Operation: Operation Euston

1. Overview of the Case

1.1 Narrative of the case

An thief steal a sports car without the owner's knowledge. They used a target person as a victim to demonstrate the responsible party. The thief and their group hack the victim's phone in order to obtain his credit card information. Without knowing the victim, they purchase a sports car from a website run by a sports car selling authority using the victim's credit card information. We infiltrated and confiscated the offender's device, and from his bootable pendrive, we retrieved some evidence to support our claims. We seize the pendrive in order to substantiate this case about the thieves' theft of the victim's sports automobile.

1.2 Timeline of key evidence

Image Information:
Acquisition started: Wed Nov 9 12:23:51 2022
Acquisition finished: Wed Nov 9 12:29:43 2022
Segment list:
F:\Foysal Mohammad\Encase_Evidence_File\Sports.E01
F:\Foysal Mohammad\Encase_Evidence_File\Sports.E02
F:\Foysal Mohammad\Encase_Evidence_File\Sports.E03

Image Verification Results:
Verification started: Wed Nov 9 12:29:43 2022
Verification finished: Wed Nov 9 12:31:13 2022

1.3 Details of the offenders, victims and witnesses

A targeted victim ziraffe phone hacked by offenders. Witness is victim image & Project_car.pdf file collected from seizure device of offender.

1.4 Photographs of any physical evidence, clues or supplemental material

1.5 Scenario Rules

A ziraffe represent a victim image. Car class represent the Sports car.
Sample Pendrive represent the seizure device from the offenders.

2. Legislation Analysis

2.1 Legislation

Motor vehicle theft, as defined by the Federal Bureau of Investigation (FBI), is the taking or attempted taking of a motor vehicle without the owner's consent. They continue by defining a motor vehicle as any self-propelled, land-based, non-rail vehicle. This excludes watercraft, airplanes, farm machinery, bulldozers, and construction tools.

2.2 Points to prove

A target victim acknowledge by offender by hacked his phone & stealing a sports car using victim credit card.

2.3 What the Digital Forensics case can prove

This Digital Forensics case can prove that who is the victim, 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 Sports car authority & offender that can prove, offender plan to buy a sports car using a credit card and the credit card they hacked from a victim phone . Attachment Below:

Hi.

Hello sir
Thanks for reaching out!
What is your model!

Hello
Its sports version
MC-01234

When you want to checkout!

By today!

Ok

Can I check out using my credit card!

Yeah sure!

Send me the Site link!

https://****.**.*

Okay we will check out!

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: 956
Evidence Number: 545
Unique Description:
Examiner: Sample Group
Notes: Seizure Devices about of Stealing sports Car

Information for F:\Foysal Mohammad\Encase_Evidence_File\Sports:
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: 388bd93d61f10cc19480af53ea1e5565
SHA1 checksum: d03984f707e660f577b35ee65639067447526f68

Image Information:
Acquisition started: Wed Nov 9 12:23:51 2022
Acquisition finished: Wed Nov 9 12:29:43 2022
Segment list:
F:\Foysal Mohammad\Encase_Evidence_File\Sports.E01
F:\Foysal Mohammad\Encase_Evidence_File\Sports.E02
F:\Foysal Mohammad\Encase_Evidence_File\Sports.E03

Image Verification Results:
Verification started: Wed Nov 9 12:29:43 2022
Verification finished: Wed Nov 9 12:31:13 2022
MD5 checksum: 388bd93d61f10cc19480af53ea1e5565 : verified
SHA1 checksum: d03984f707e660f577b35ee65639067447526f68 : verified

3.2 Hash value of the Evidence File

[Computed Hashes]
MD5 checksum: 388bd93d61f10cc19480af53ea1e5565 : verified
SHA1 checksum: d03984f707e660f577b35ee65639067447526f68 : verified

```
File  Edit  Format  View  Help
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 956
Evidence Number: 545
Unique Description:
Examiner: Sample Group
Notes: Seizure Devices about of Stealing sports Car

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

Information for F:\Foysal Mohammad\Encase_Evidence_File\Sports:

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:    388bd93d61f10cc19480af53ea1e5565
 SHA1 checksum:   d03984f707e660f577b35ee65639067447526f68

Image Information:
 Acquisition started:   Wed Nov  9 12:23:51 2022
 Acquisition finished:  Wed Nov  9 12:29:43 2022
 Segment list:
  F:\Foysal Mohammad\Encase_Evidence_File\Sports.E01
  F:\Foysal Mohammad\Encase_Evidence_File\Sports.E02
  F:\Foysal Mohammad\Encase_Evidence_File\Sports.E03

Image Verification Results:
 Verification started:  Wed Nov  9 12:29:43 2022
 Verification finished: Wed Nov  9 12:31:13 2022
 MD5 checksum:    388bd93d61f10cc19480af53ea1e5565 : verified
 SHA1 checksum:   d03984f707e660f577b35ee65639067447526f68 : 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_car.pdf target.jpg	Files containing the victim image & Clarification.
DRF	Document File & Picture File	4.2.2	Project_car_2.pdf Target_2.jpg	Files containing the victim image & Clarification.
DRA	Picture File	4.2.3	Conversation.png	File containing some social media chat logs between car authority & offender.
DRA	Text file	4.2.4	Browsing_history.txt	File containing info that target stealing sports car site link
DROS	Registry File	4.2.5	Software_Hive	File containing the information about offender save the browsing historyin notepad.
DROS	Registry File	4.2.6	Software_Hive_2	File containing the information about offender edited the victim image set.
DRFS	Document File	4.2.7	Deleted Files	Files containing information about cyberspace identity article
DRFS	Document File	4.2.8	BBS.pdf	Files containing information about credit card fraud and detection technique article
DHU	White text on white background	4.3.1	Hives.docx	Contains information about electronic hive & car value.
DHU	White text on white background	4.3.2	Secret.txt Hives_2.pdf	Contains information about Victim credit card info.
DHA	Audio file	4.3.3	Morse_1.wav	File Containing sports car news that targeted by the offender and hide in secret audio
DHA	Audio file	4.3.4	Morse_2.wav	File Containing sports car code that targeted by the offender and hide in secret audio
DHOS	Unknown File(.oi)	4.3.5	Phissy_1.oi	File containing Data secret data hiding by changing the file extension

DHOS	Unknown File(.oi)	4.3.6	Phissy_2.oi	File containing Data secret data hiding by changing the file extension
DHFS	Picture File	4.3.7	Its_me.jpg	File containing offender real image information.
DHFS	Picture File	4.3.8	Partner.jpg	File containing offender partner real image information.
DHU_1	Compressed File	4.4.1	Our_Client.zip	File Containing the offender targeted client image by the secure zip file.
DHU_2	Text file	4.4.2	What_is_the_issues.txt	File Containing the information of offender threat.
DHU_3	Image File	4.4.3	Plan-date.jpg	File containing information that the stealing plan date of a sports car.
DR_1	Image File	4.4.	Next_Target.png	Here is Some secret message under this image. Containing information about another target by the offender.

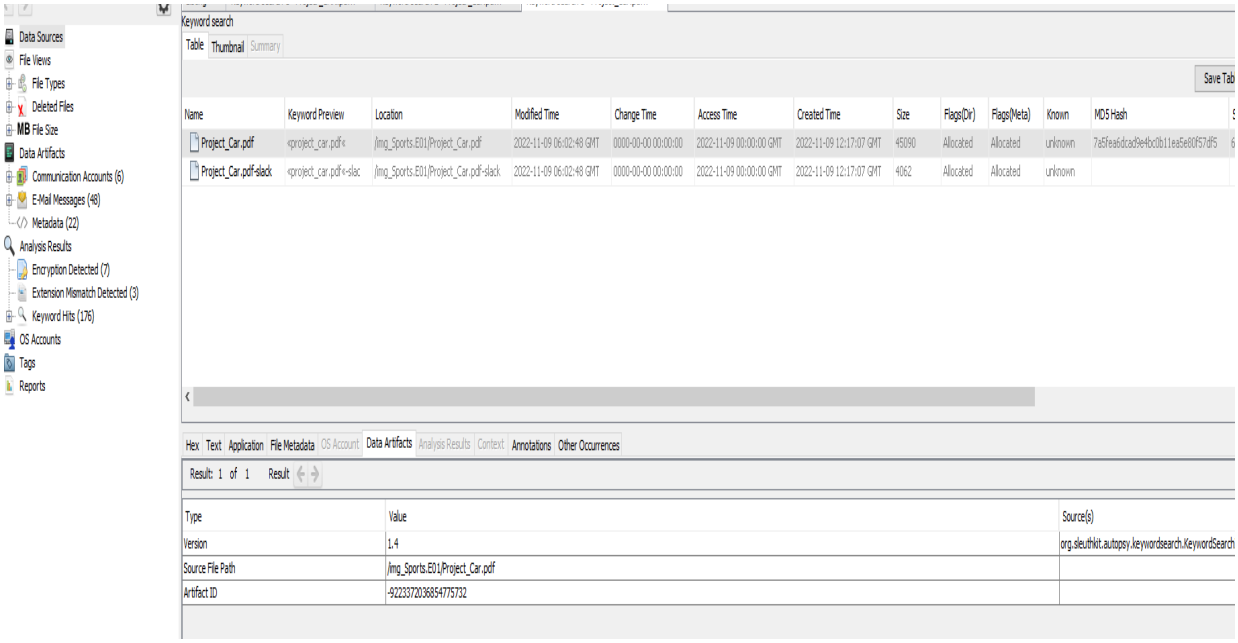
Table 4.2 – Summary Table of Artefacts

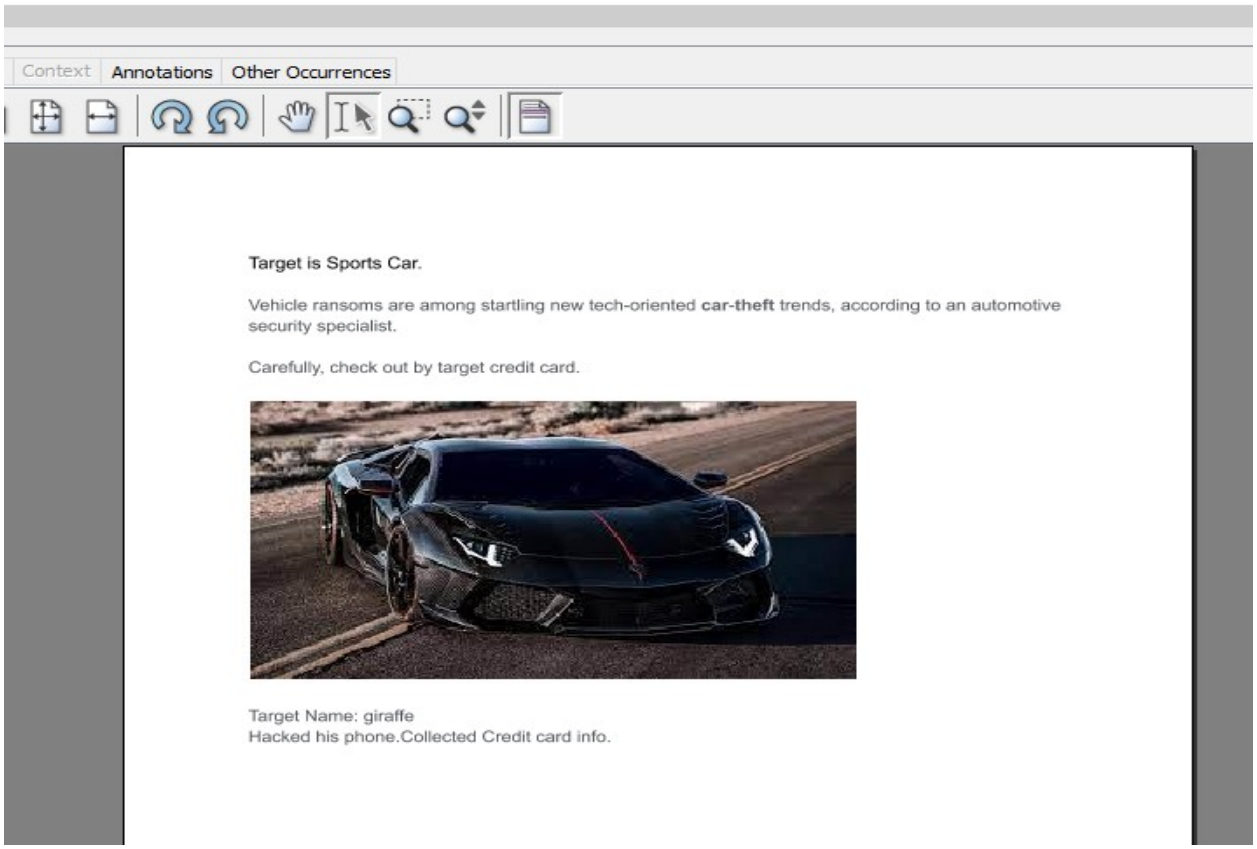
4.2 Data Recovery Artefacts

4.2.1 Category DRF

Screenshot of the artefact:

Content- Target is Sports Car. Vehicle ransoms are among startling new tech-oriented car-theft trends, according to an automotive security specialist. Carefully, check out by target credit card.
Target Name: giraffe Hacked his phone.Collected Credit card info


Data Sources
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Communication Accounts (6)
E-Mail Messages (48)
Metadata (22)
Analysis Results
Encryption Detected (7)
Extension Mismatch Detected (3)
Keyword Hits (176)
OS Accounts
Tags
Reports
Keyword search
Table Thumbnail Summary
Save Tab
Name Keyword Preview Location Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known MD5 Hash
Project_Car.pdf «project_car.pdf« /img_Sports.E01/Project_Car.pdf 2022-11-09 06:02:48 GMT 0000-00-00 00:00:00 2022-11-09 00:00:00 GMT 2022-11-09 12:17:07 GMT 45090 Allocated Allocated unknown 7a5fea6dcad9e4bc0b11ea5e60f57df5
Project_Car.pdf-slack «project_car.pdf«-slac /img_Sports.E01/Project_Car.pdf-slack 2022-11-09 06:02:48 GMT 0000-00-00 00:00:00 2022-11-09 00:00:00 GMT 2022-11-09 12:17:07 GMT 4062 Allocated Allocated unknown
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 1 Result
Type Value Source(s)
Version 1.4 org.sleuthkit.autopsy.keywordsearch.KeywordSearch
Source File Path /img_Sports.E01/Project_Car.pdf
Artifact ID -9223372036854775732


Context Annotations Other Occurrences
Target is Sports Car.
Vehicle ransoms are among startling new tech-oriented car-theft trends, according to an automotive security specialist.
Carefully, check out by target credit card.
Target Name: giraffe
Hacked his phone.Collected Credit card info.

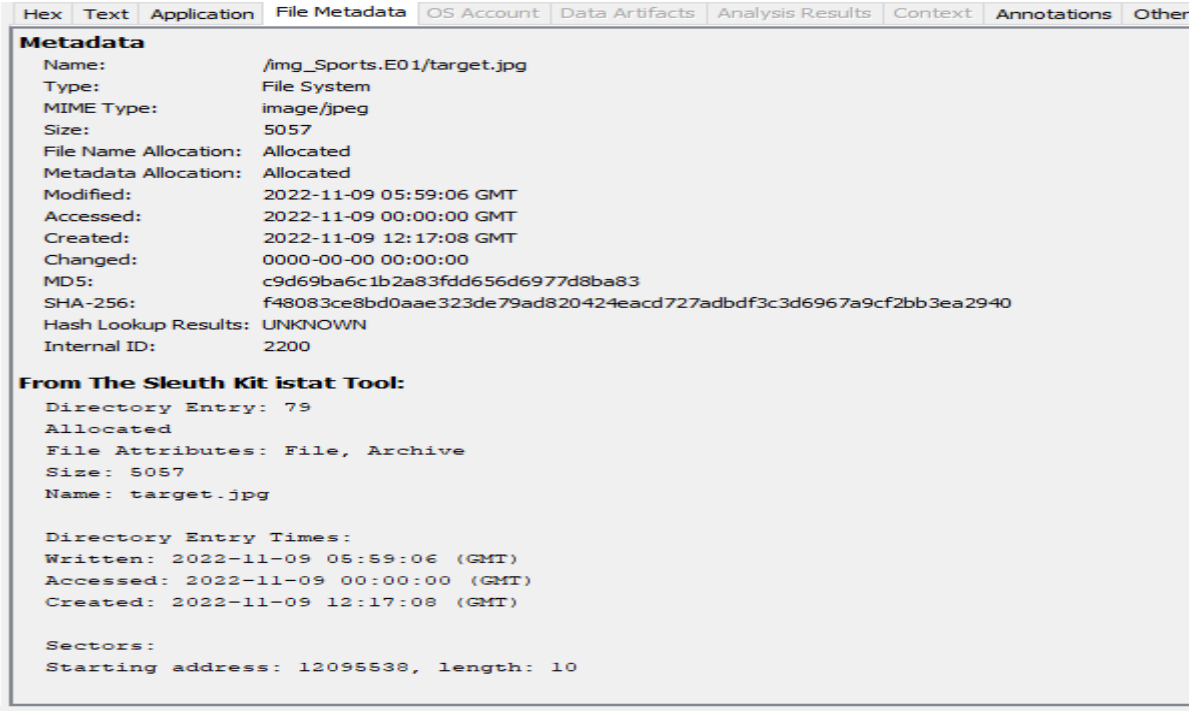
A screenshot of artefact evidence details:

Metadata

Name:	/img_Sports.E01/Project_Car.pdf
Type:	File System
MIME Type:	application/pdf
Size:	45090
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 06:02:48 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:17:07 GMT
Changed:	0000-00-00 00:00:00
MD5:	7a5fea6dcad9e4bc0b11ea5e80f57df5
SHA-256:	63c1c74cf22a4ee24ba38769450eccd07e698fb5e0f8f877b8b977fb347fc2fe
Hash Lookup Results:	UNKNOWN
Internal ID:	2196

From The Sleuth Kit istat Tool:

```
Directory Entry: 75
Allocated
File Attributes: File, Archive
Size: 45090
Name: PROJEC~1.PDF

Directory Entry Times:
Written: 2022-11-09 06:02:48 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:17:07 (GMT)

Sectors:
Starting address: 12095370, length: 89
```



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

Metadata

Name:	/img_Sports.E01/target.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	5057
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 05:59:06 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:17:08 GMT
Changed:	0000-00-00 00:00:00
MD5:	c9d69ba6c1b2a83fdd656d6977d8ba83
SHA-256:	f48083ce8bd0aae323de79ad820424eacd727adbdf3c3d6967a9cf2bb3ea2940
Hash Lookup Results:	UNKNOWN
Internal ID:	2200

From The Sleuth Kit istat Tool:

```
Directory Entry: 79
Allocated
File Attributes: File, Archive
Size: 5057
Name: target.jpg

Directory Entry Times:
Written: 2022-11-09 05:59:06 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:17:08 (GMT)

Sectors:
Starting address: 12095538, length: 10
```

Description and implications of the artefact:

Target is Sports Car. Vehicle ransoms are among startling new tech-oriented car-theft trends, according to an automotive security specialist. Carefully, check out by target credit card. That means they plan to hack the target victim phone and hack the credit card info then they use this credit card for steal the sports car.

4.2.2 Category DRF

Screenshot of the artefact:

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kr
Project_Car_2.pdf	«project_car_2.pdf«	/img_Sports.E01/Project_Car_2.pdf	2022-11-09 06:13:30 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 12:17:08 GMT	35825	Allocated	Allocated	un
Project_Car_2.pdf-slack	«project_car_2.pdf«-slac	/img_Sports.E01/Project_Car_2.pdf-slack	2022-11-09 06:13:30 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 12:17:08 GMT	1039	Allocated	Allocated	un

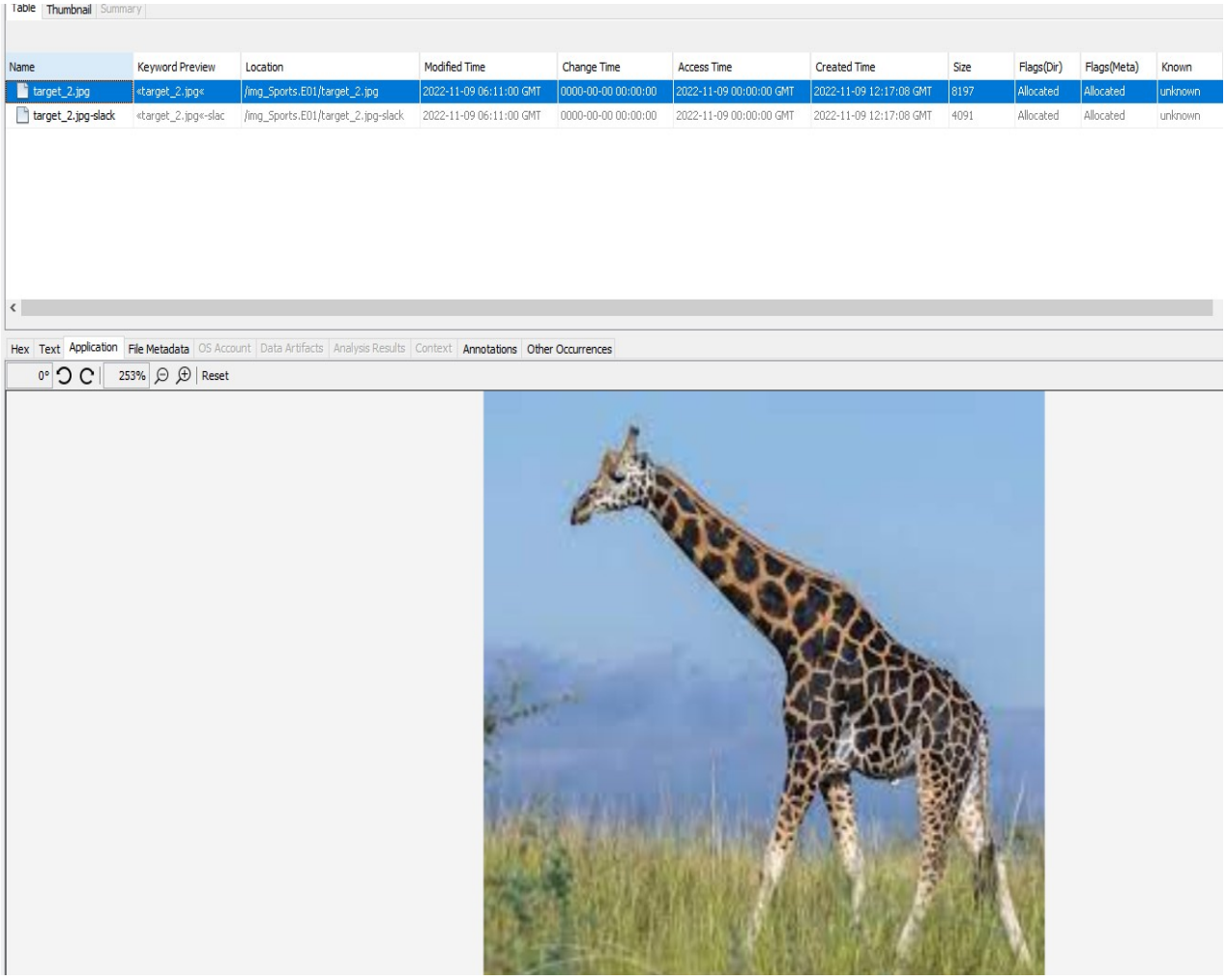
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

1 of 1 100%

What is the point of stealing cars?

As a tool to commit another crime: Thieves are frequently in need of vehicles to help commit other crimes — usually robberies. Most of these vehicles are recovered soon after the illegal acts, abandoned, and sometimes with substantial damage. To take for a ride: Sometimes cars are stolen just to take "joyrides."

Target: Giraff_2



A screenshot of artefact evidence details:

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

Metadata

Name:	/img_Sports.E01/Project_Car_2.pdf
Type:	File System
MIME Type:	application/pdf
Size:	35825
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 06:13:30 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:17:08 GMT
Changed:	0000-00-00 00:00:00
MD5:	19a05407dd891e89f4bc43f1e43b550f
SHA-256:	7d5c1971ae80ed01b42939631b6a3a99aef92d4eba8f353735b96f5bbf2f32f1
Hash Lookup Results:	UNKNOWN
Internal ID:	2198

From The Sleuth Kit istat Tool:

```
Directory Entry: 78
Allocated
File Attributes: File, Archive
Size: 35825
Name: PROJEC~2.PDF

Directory Entry Times:
Written: 2022-11-09 06:13:30 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:17:08 (GMT)

Sectors:
Starting address: 12095466, length: 70
```

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

Metadata

Name:	/img_Sports.E01/target_2.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	8197
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 06:11:00 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:17:08 GMT
Changed:	0000-00-00 00:00:00
MD5:	ee7f54b62c5d672bbb3c960b83f8d089
SHA-256:	9acc1977620c31a7603e888d4286ec1a021a4c3c5b886b92348c93d37295d124
Hash Lookup Results:	UNKNOWN
Internal ID:	2202

From The Sleuth Kit istat Tool:

```
Directory Entry: 80
Allocated
File Attributes: File, Archive
Size: 8197
Name: target_2.jpg

Directory Entry Times:
Written: 2022-11-09 06:11:00 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:17:08 (GMT)

Sectors:
Starting address: 12095554, length: 17
```

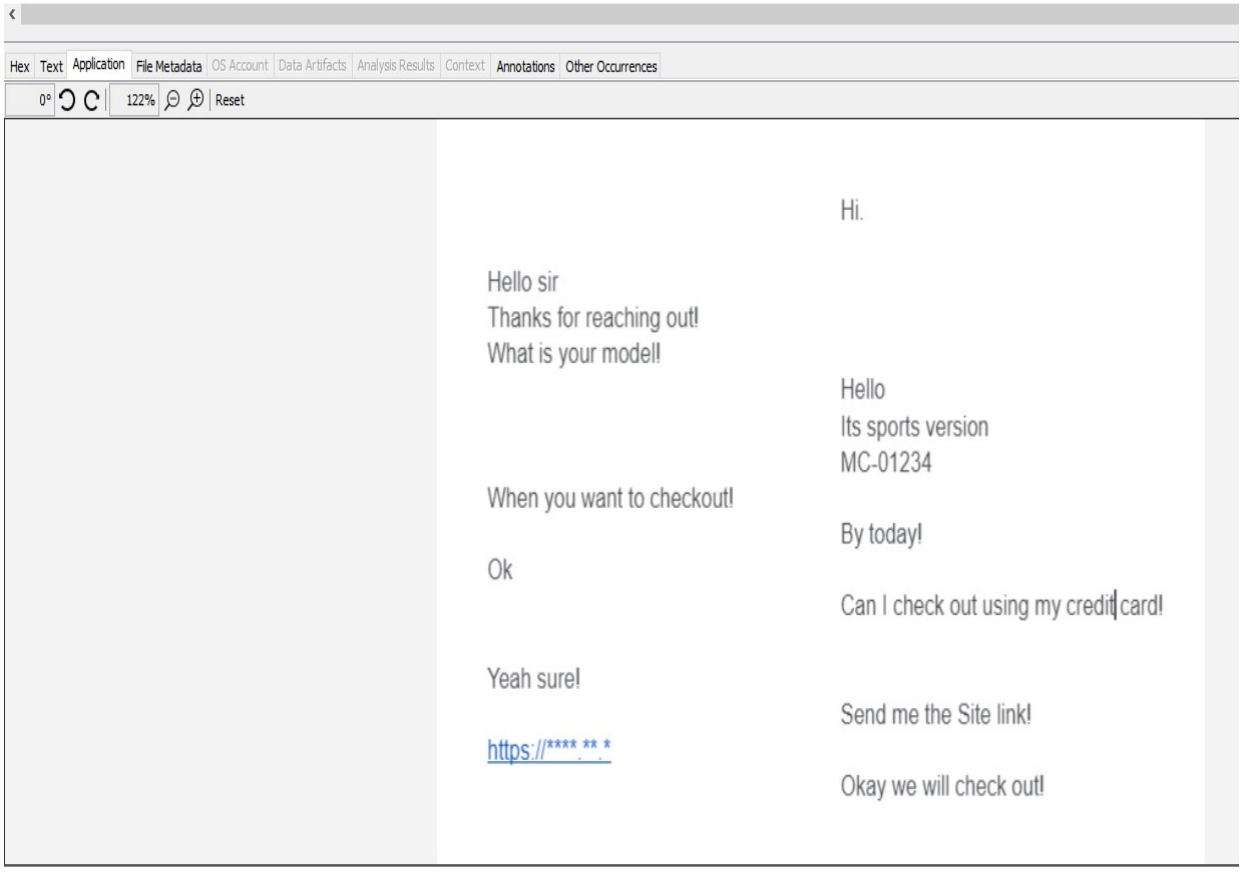
Description and implications of the artefact:

What is the point of stealing cars? As a tool to commit another crime: Thieves are frequently in need of vehicles to help commit other crimes — usually robberies. Most of these vehicles are recovered soon after the illegal acts, abandoned, and sometimes with substantial damage. To take for a ride: Sometimes cars are stolen just to take "joyrides." Target: Giraff_2

4.2.3 Category DRA

Screenshot of the artefact:

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Conversation.PNG	«conversation.png«	/img_Sports.E01/efi/Conversation.PNG	2022-11-09 06:09:32 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 12:18:11 GMT	12866	Allocated
Conversation.PNG-slack	«conversation.png«-slac	/img_Sports.E01/efi/Conversation.PNG-slack	2022-11-09 06:09:32 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 12:18:11 GMT	3518	Allocated



A screenshot of artefact evidence details:

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

Metadata

Name:	/img_Sports.E01/efi/Conversation.PNG
Type:	File System
MIME Type:	image/png
Size:	12866
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 06:09:32 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:18:11 GMT
Changed:	0000-00-00 00:00:00
MD5:	596fd8d059a92537b70696424bf5771d
SHA-256:	6cbfb6f9803f5e7d96b0472bc055876d3667e56777fc326bab0a208100d2d43a
Hash Lookup Results:	UNKNOWN
Internal ID:	2044

From The Sleuth Kit istat Tool:

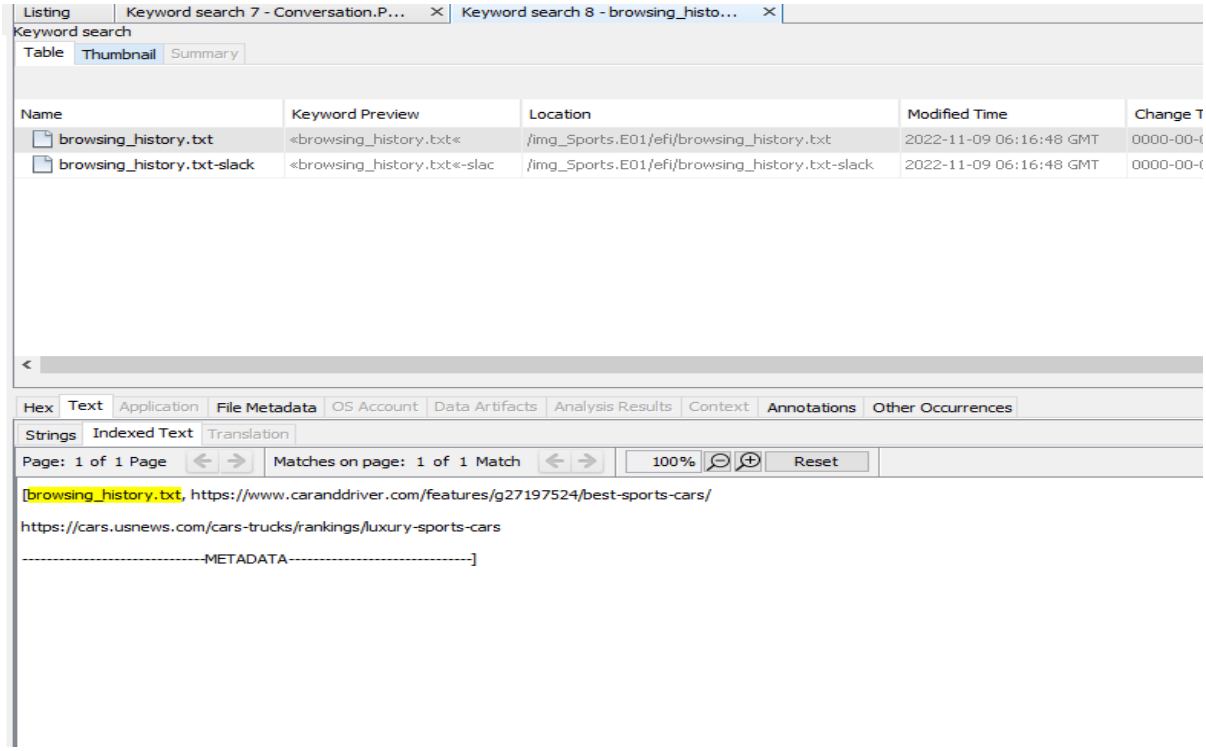
```
Directory Entry: 189934865
Allocated
File Attributes: File, Archive
Size: 12866
Name: CONVER~1.PNG

Directory Entry Times:
Written: 2022-11-09 06:09:32 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:18:11 (GMT)

Sectors:
Starting address: 12095626, length: 26
```

Description and implications of the artefact:

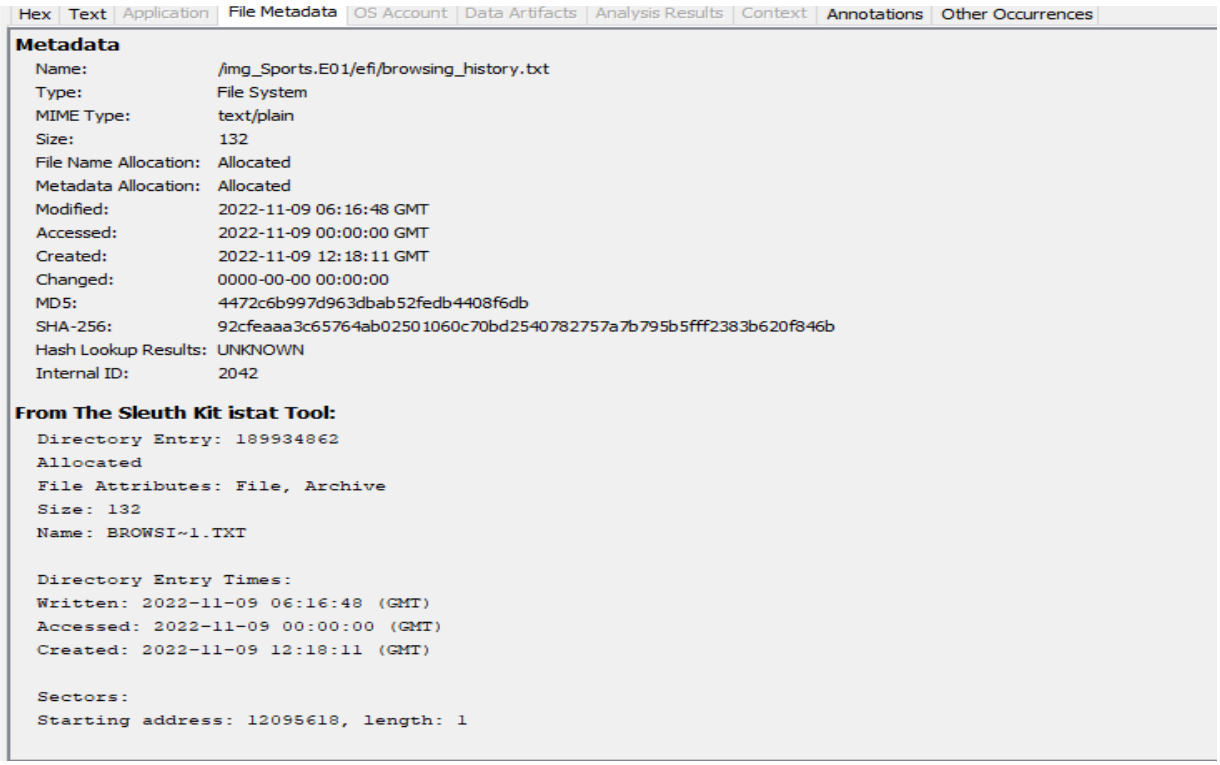
Offender planning to sports car & they chat with authority via website chat or social media site..

4.2.4 Category DRA

Screenshot of the artefact:



A screenshot of artefact evidence details:

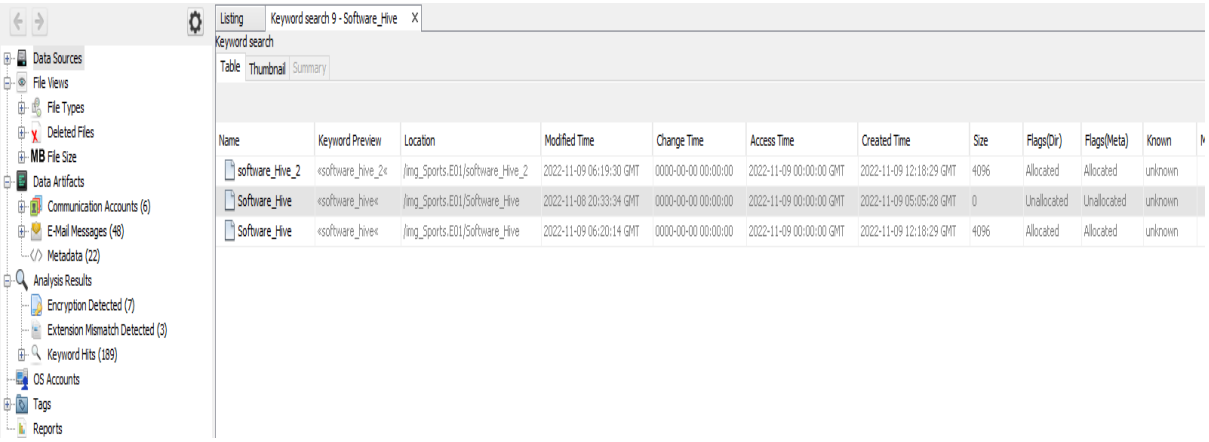


Description and implications of the artefact:

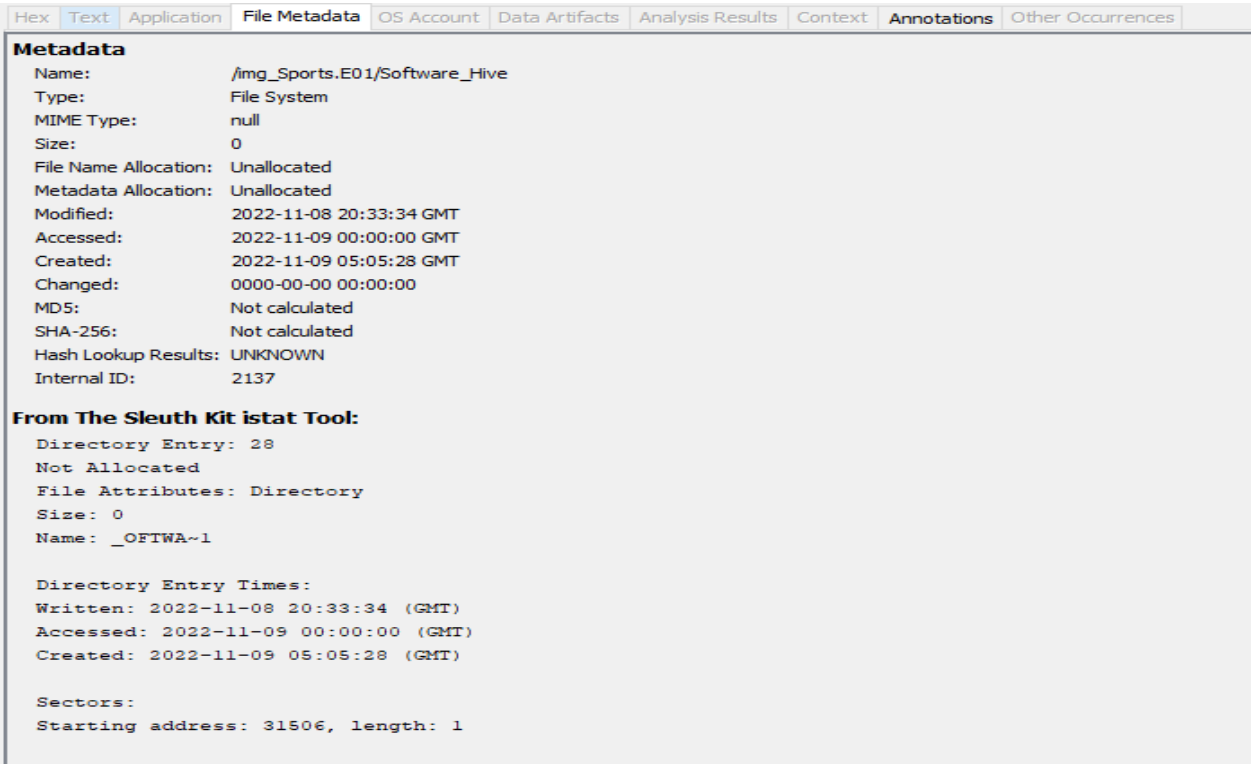
This Section clarify that offenders analysis the browing search for a sports car authority site visit to execute the plan.They saved the history in their device.

4.2.5 Category DROS

Screenshot of the artefact:



A screenshot of artefact evidence details:



Description and implications of the artefact:

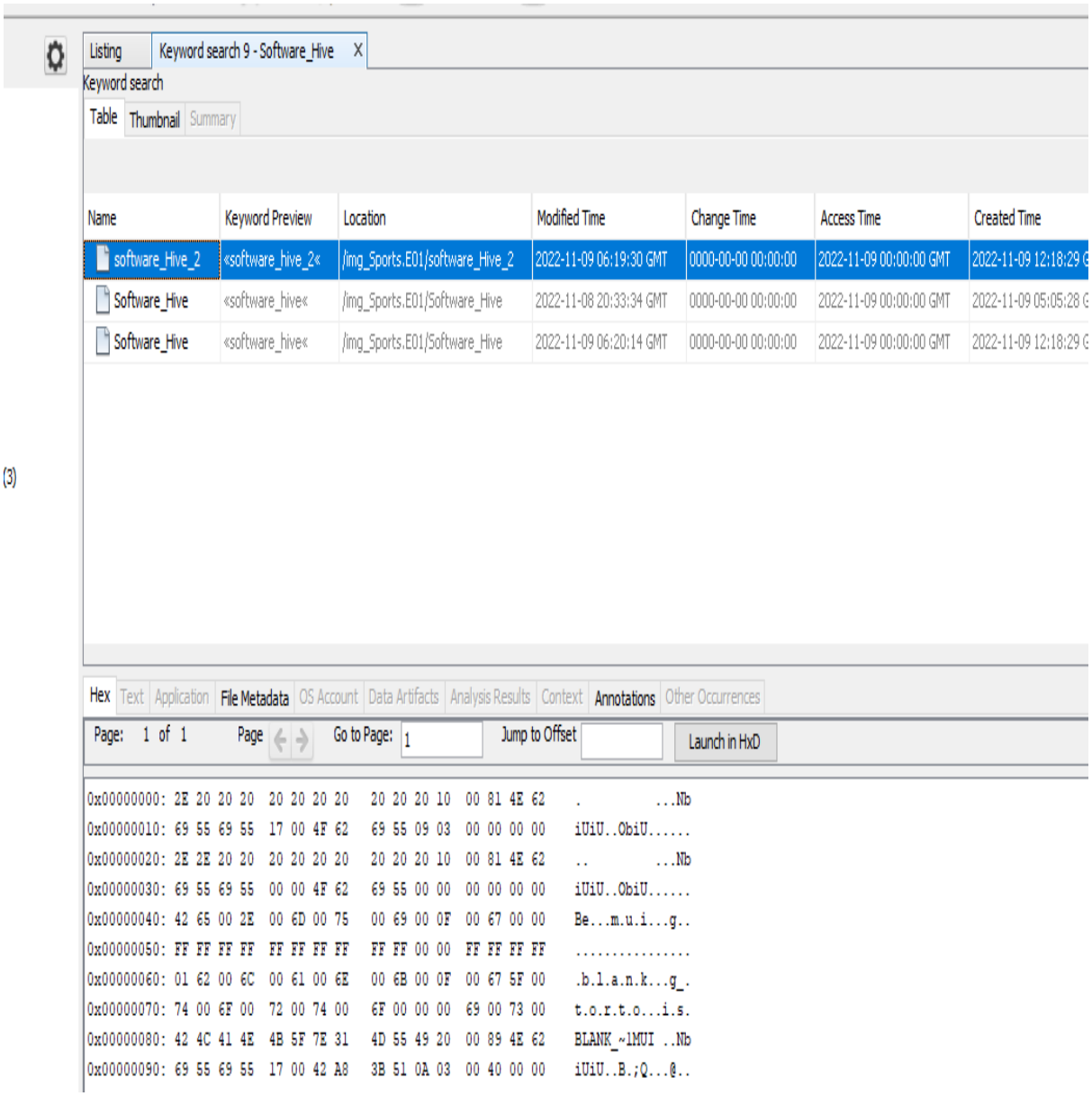
This Section clarify that File containing the information about offender save the browsing historyin notepad.

.

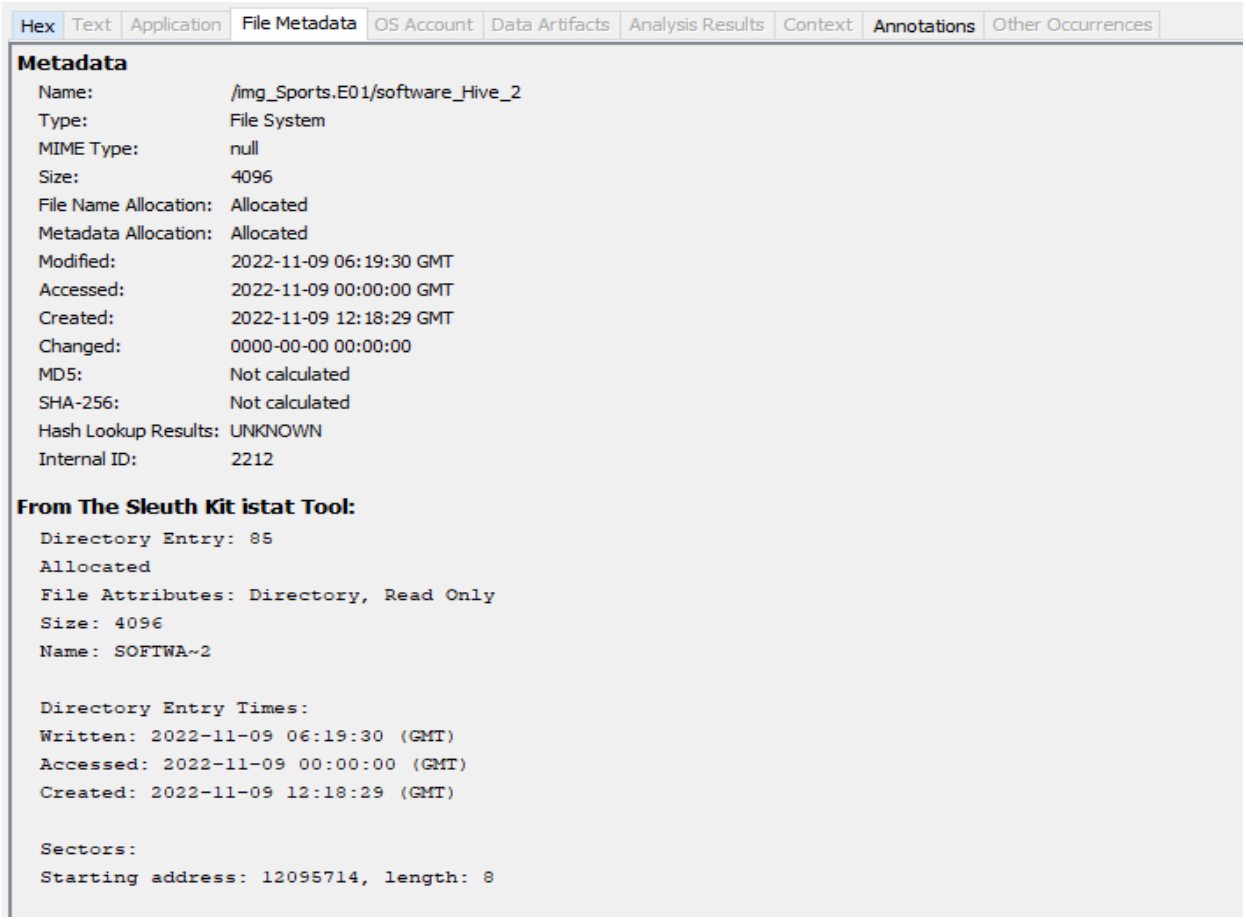
4.2.6 Category DROS

Screenshot of the artefact:

(3)



A screenshot of artefact evidence details:



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

Metadata

Name:	/img_Sports.E01/software_Hive_2
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 06:19:30 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:18:29 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	2212

From The Sleuth Kit istat Tool:

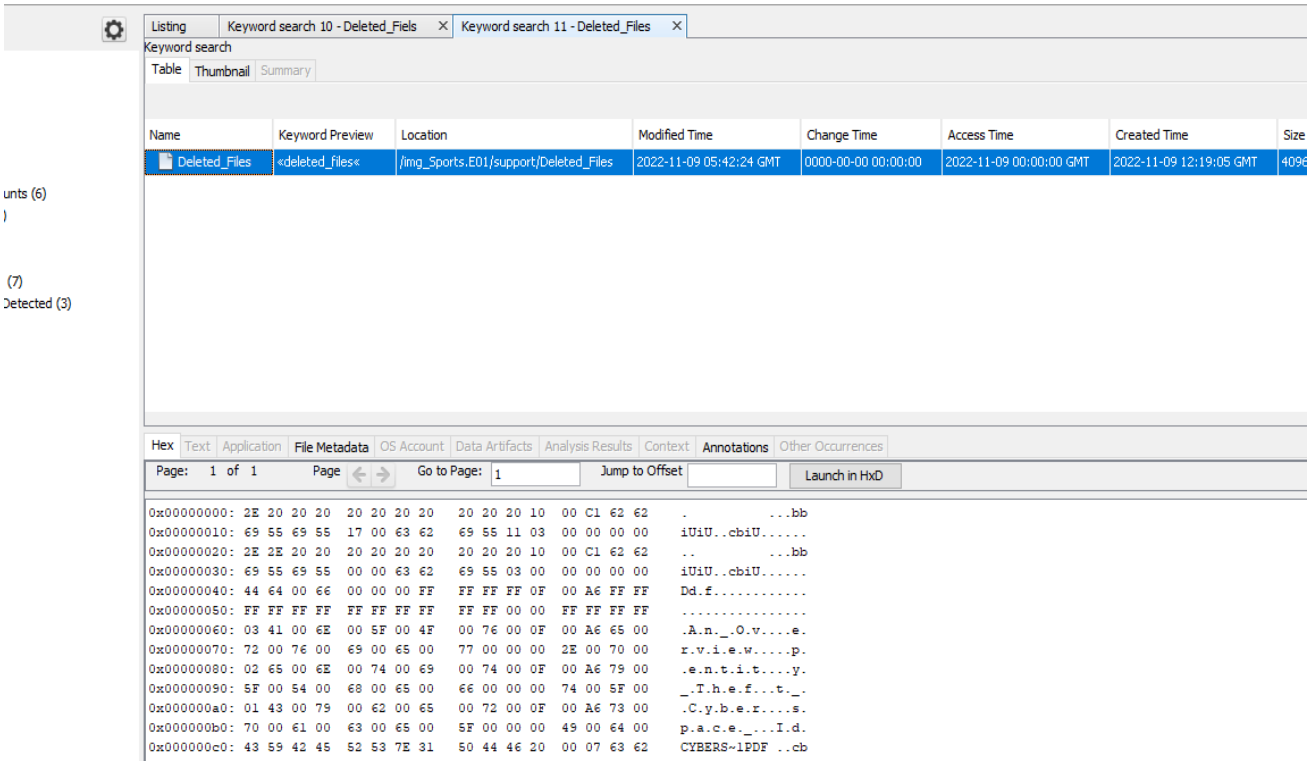
```
Directory Entry: 85
Allocated
File Attributes: Directory, Read Only
Size: 4096
Name: SOFTWA~2

Directory Entry Times:
Written: 2022-11-09 06:19:30 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:18:29 (GMT)

Sectors:
Starting address: 12095714, length: 8
```

Description and implications of the artefact:

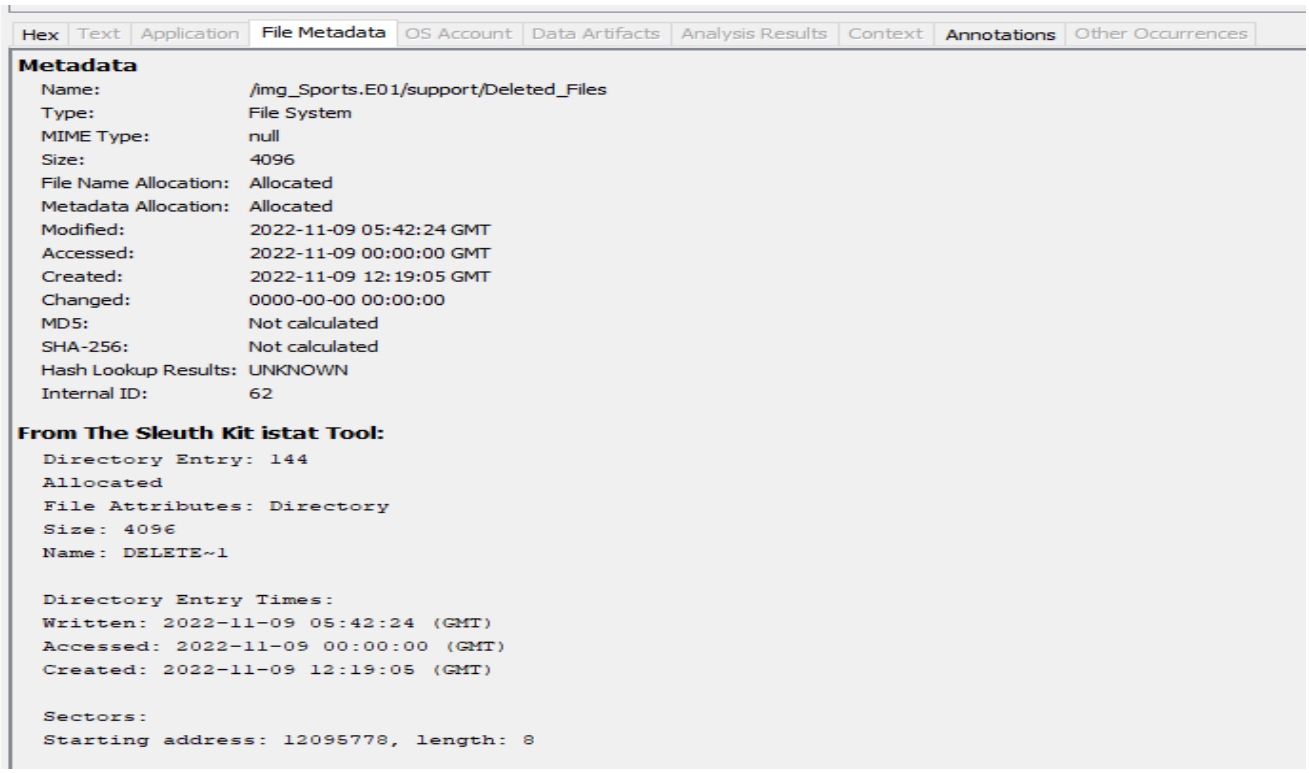
This Section clarify that offenders analysis about offender edited the victim image set.

4.2.7 Category DRFS

Screenshot of the artefact:



A screenshot of artefact evidence details:

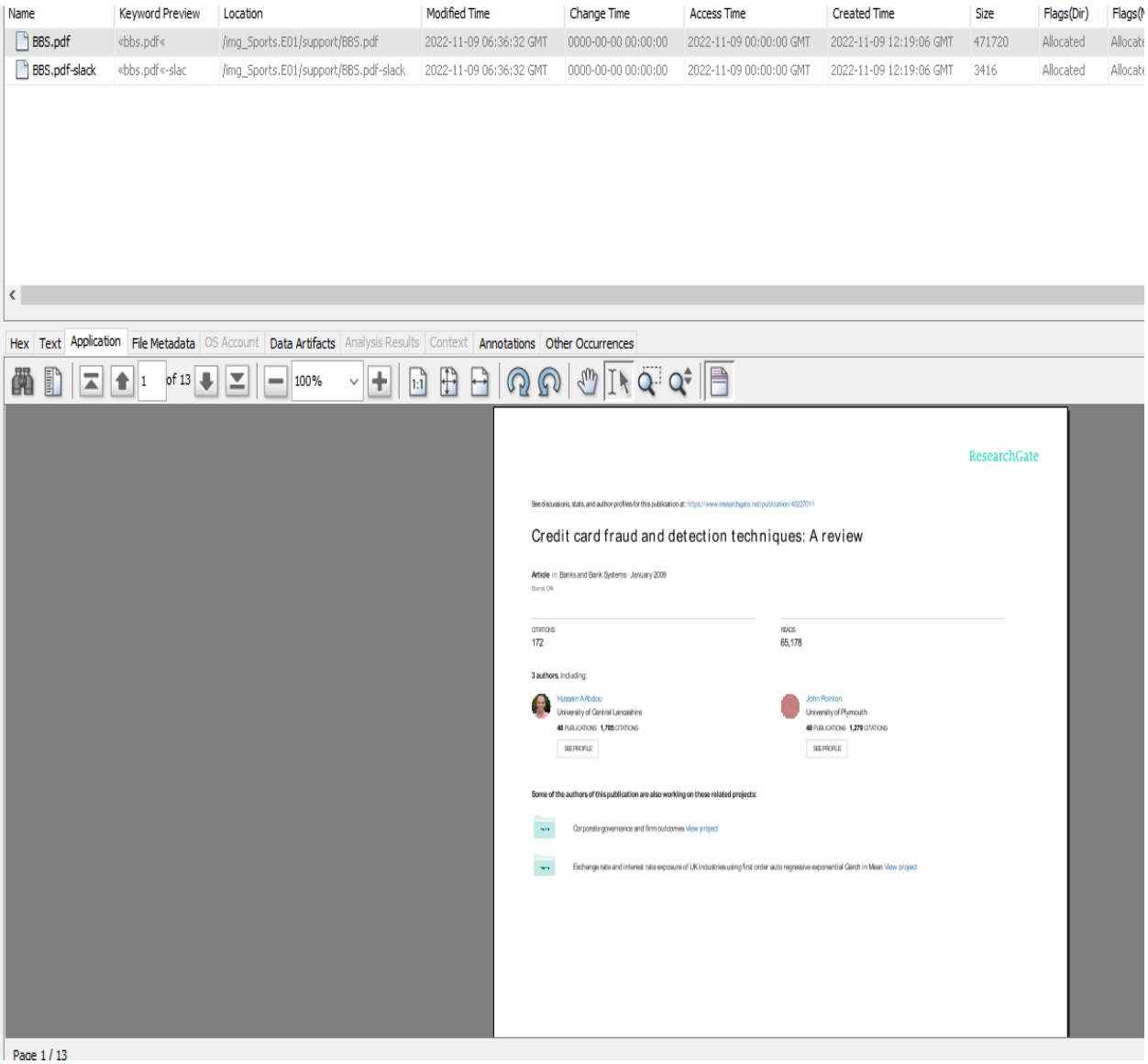


Description and implications of the artefact:

This Section clarify that offenders analysis the about the sports car news article for theft legislation for do the plan safe.

4.2.8 Category DRFS

Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M
BBS.pdf	«bbs.pdf«	/img_Sports.E01/support/BBS.pdf	2022-11-09 06:36:32 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 12:19:06 GMT	471720	Allocated	Allocat
BBS.pdf-slack	«bbs.pdf«-slac	/img_Sports.E01/support/BBS.pdf-slack	2022-11-09 06:36:32 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 12:19:06 GMT	3416	Allocated	Allocat

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

1 of 13 100%

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/40227011

Credit card fraud and detection techniques: A review

Article in Banks and Bank Systems · January 2009

Source: OAI

CITATIONS 172

READS 65,178

3 authors, including:

Hussein A Abdou
University of Central Lancashire
48 PUBLICATIONS 1,785 CITATIONS
SEE PROFILE

John Pointon
University of Plymouth
48 PUBLICATIONS 1,279 CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Corporate governance and firm outcomes View project

Exchange rate and interest rate exposure of UK industries using first order auto regressive-exponential Garch in Mean View project

Page 1 / 13

A screenshot of artefact evidence details:

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

Metadata

Name:	/img_Sports.E01/support/BBS.pdf
Type:	File System
MIME Type:	application/pdf
Size:	471720
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 06:36:32 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:19:06 GMT
Changed:	0000-00-00 00:00:00
MD5:	6a36703d491c488ca754df743465c6ba
SHA-256:	f837e1dbb509215dfd665d42924023340fe7f5d9b319053b4ef5c21343661548
Hash Lookup Results:	UNKNOWN
Internal ID:	67

From The Sleuth Kit istat Tool:

```
Directory Entry: 145
Allocated
File Attributes: File, Archive
Size: 471720
Name: BBS.pdf

Directory Entry Times:
Written: 2022-11-09 06:36:32 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:19:06 (GMT)

Sectors:
Starting address: 12096282, length: 922
```

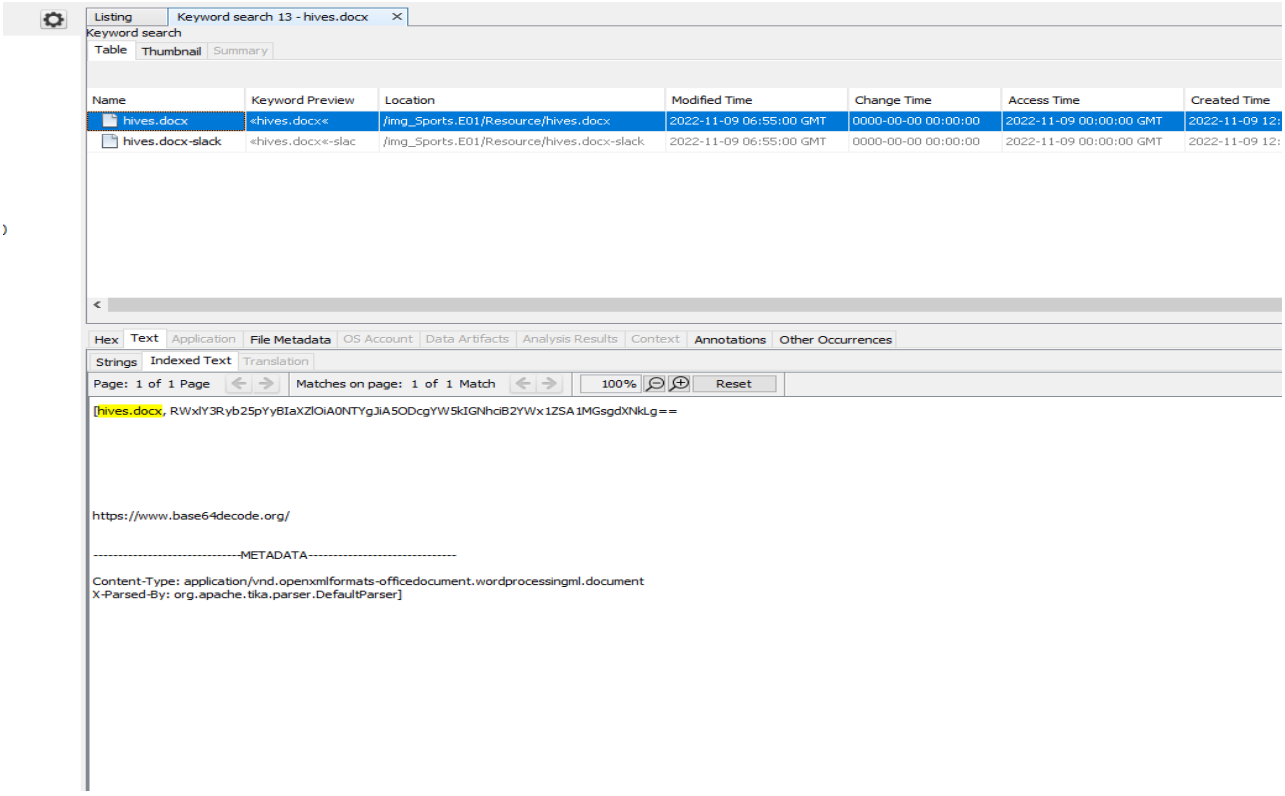
Description and implications of the artefact:

This Section clarify that offenders analysis the credit card fraud detection technique article.

4.3 Data Hiding Artefacts

4.3.1 Category DHU

Screenshot of the artefact:



Content:

RWxlY3Ryb25pYyBIaXZlOiA0NTYgJiA5ODcgYW5kIGNhciB2YWx1ZSA1MGsgdXNkLg==

https://www.base64decode.org/

A screenshot of artefact evidence details:

Description and implications of the artefact:

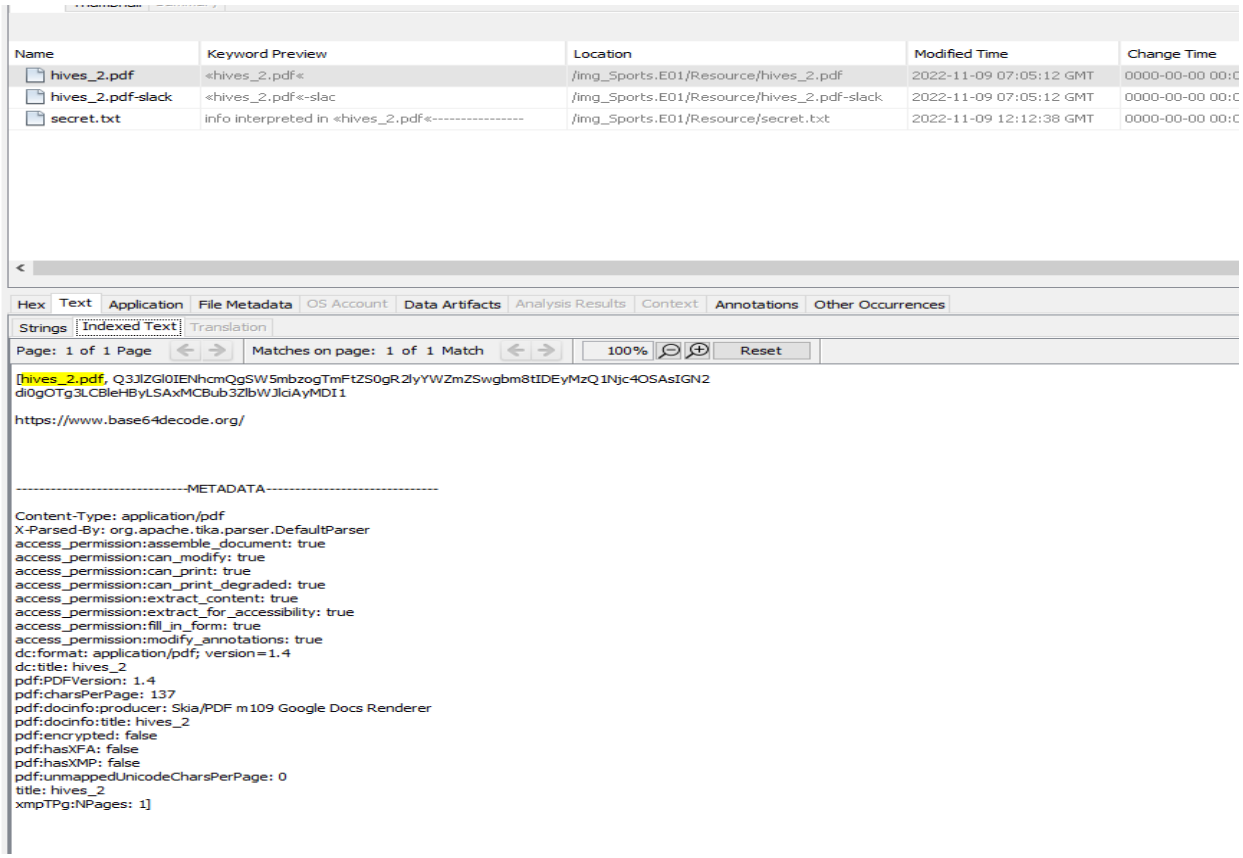
Offender Hide some secret data in a docx file by encrypting to a hash code like base64 format.
After decode the hash found that text “Electronic Hive: 456 & 987 and car value 50k usd.”. We clarify that they are planning to steal car and the value of the car with the electronic hive number.

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 DHU

Screenshot of the artefact:

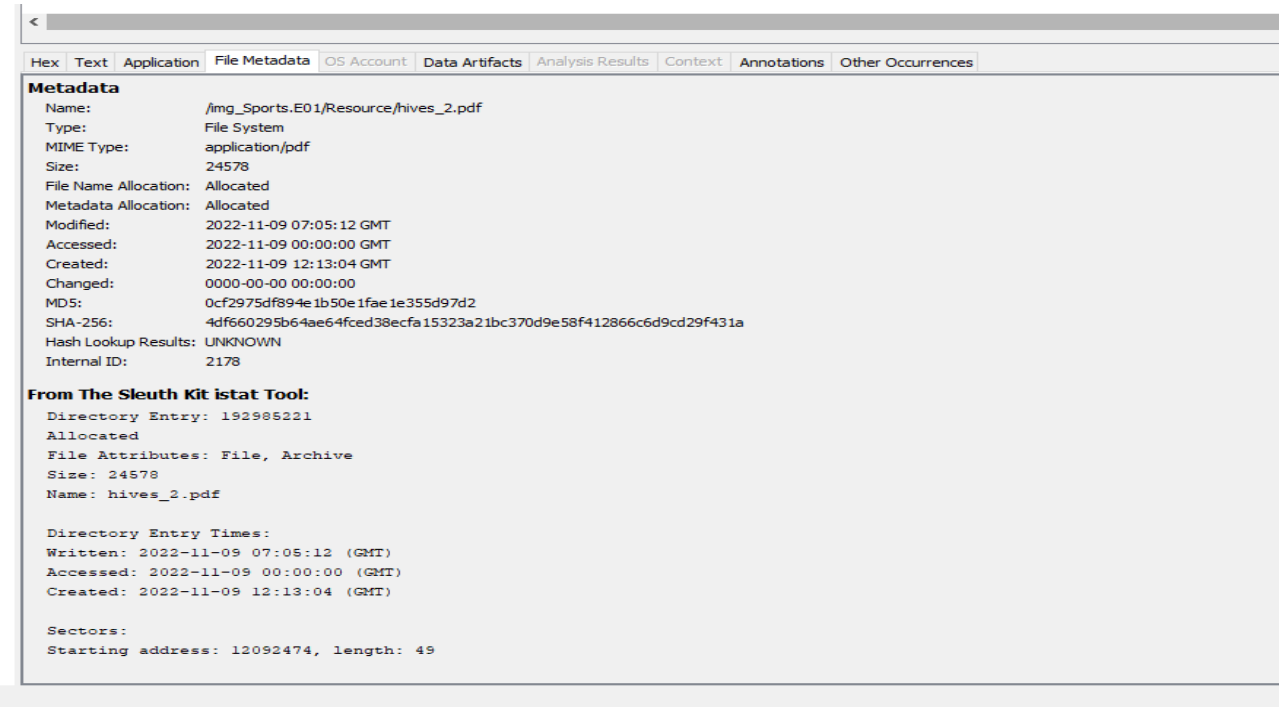


Content:


```
Q3JlZGl0IENhcmQgSW5mbzogTmFtZS0gR2lyYWZmZSwgbm8tIDEyMzQ1Njc4OSAsIGN2
di0gOTg3LCBleHByLSAxMCBub3ZlbWJlciAyMDI1
```

https://www.base64decode.org/

A screenshot of artefact evidence details:



Description and implications of the artefact:

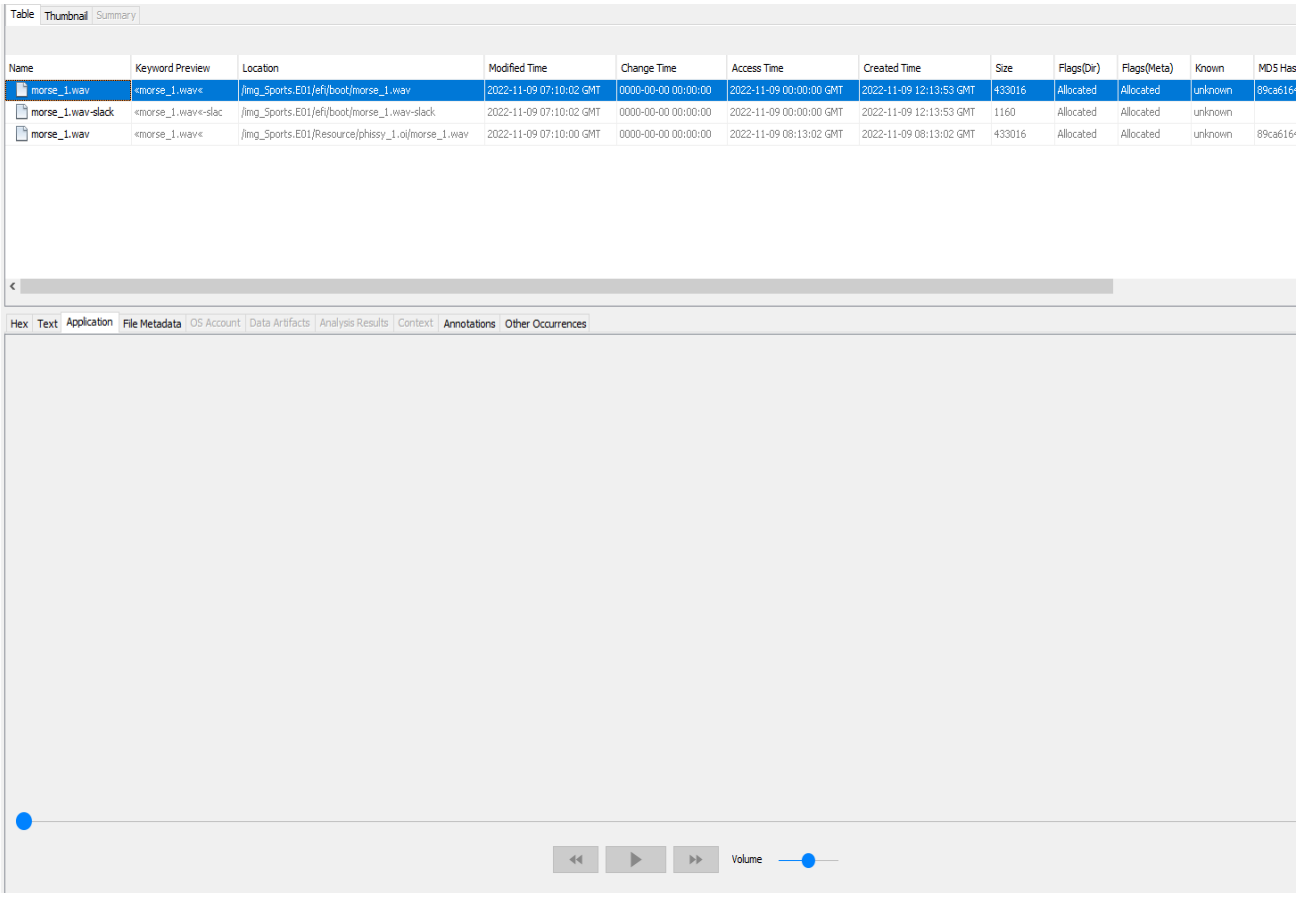
Offender Hide some secret data in a docx file by encrypting to a hash code like base64 format.
After decode the hash found that text “Credit Card Info: Name- Giraffe, no- 123456789 , cvv- 987, expr- 10 november 2025”. We clarify that they were hacked the victim phone and they got it his credit card info in details and they hide the info in blank docx file.

Description of the hiding/unhiding process:

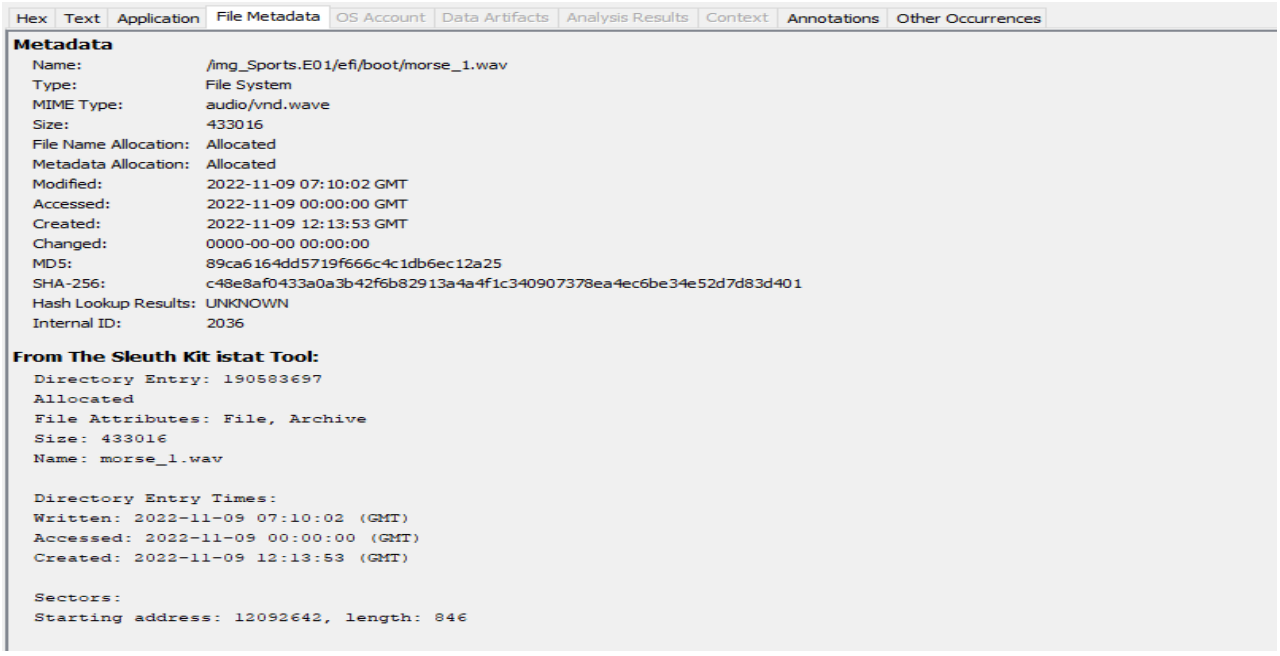
Hide the characters in a docs file by a white background. Basically when it is opened then it can view by blank but mark the page and change the colour then we found the text that is hash value like base64. We decode from base64 decoder.

4.3.3 Category DHA

Screenshot of the artefact:



A screenshot of artefact evidence details:



Description and implications of the artefact:

Offender Hide some secret data in audio file via using steganography technique using a morse code adaptive audio encoder technique. After decode we see that here is the sports car rankings site that they are target for their planning to stealing.
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

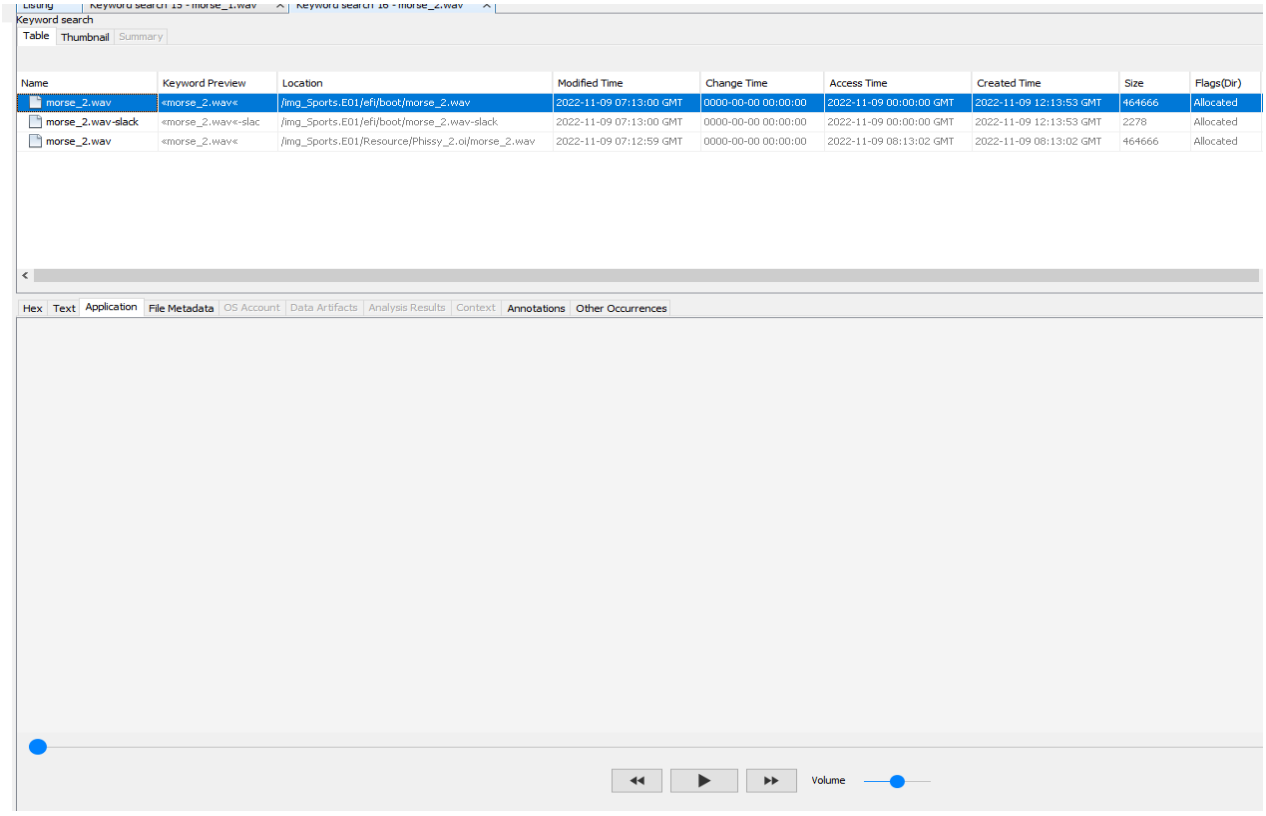
Select	File	Speed (wpm)	Min volume (dB)	Max volume (dB)	Min frequency (Hz)	Max frequency (Hz)	Volume threshold	FFT size
◉	Morse	20	-100	-30	700	700	200	256
○	Alphabet	30	-100	-30	600	600	200	256
○	Alphabet	40	-60	-30	700	700	200	256
○	Fox (via mic)	23	-60	-30	600	700	225	256
○	Inspector Morse	10	-60	-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.

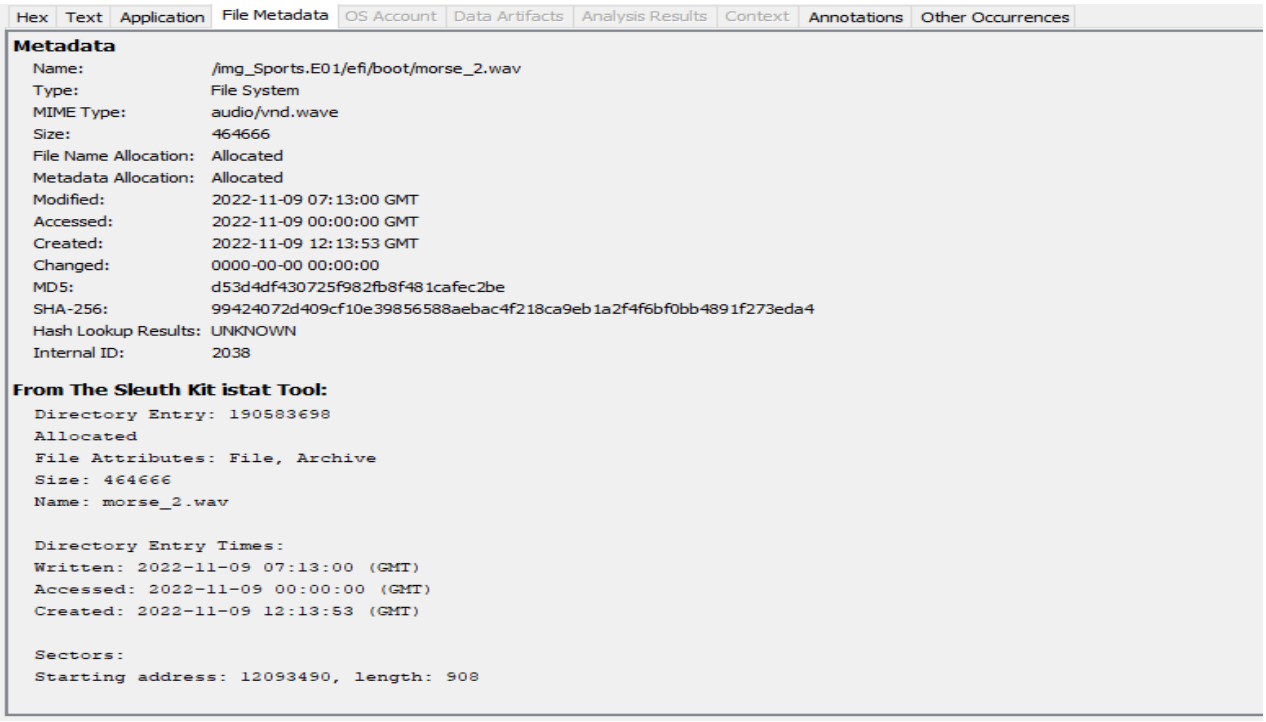
Step-3: Click the Play button and wait to finish the morse audio. Then we got our message from below

4.3.4 Category DHA

Screenshot of the artefact:



A screenshot of artefact evidence details:

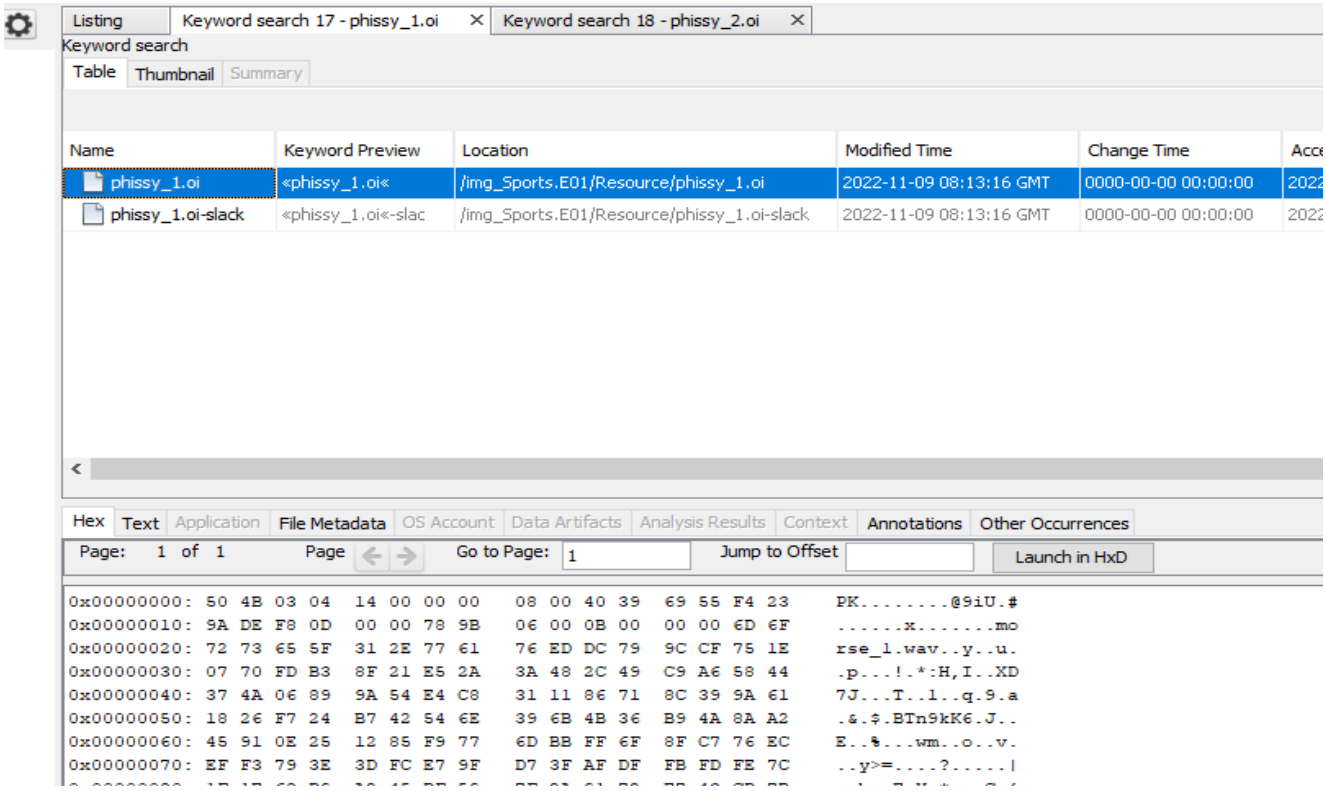


Description and implications of the artefact:

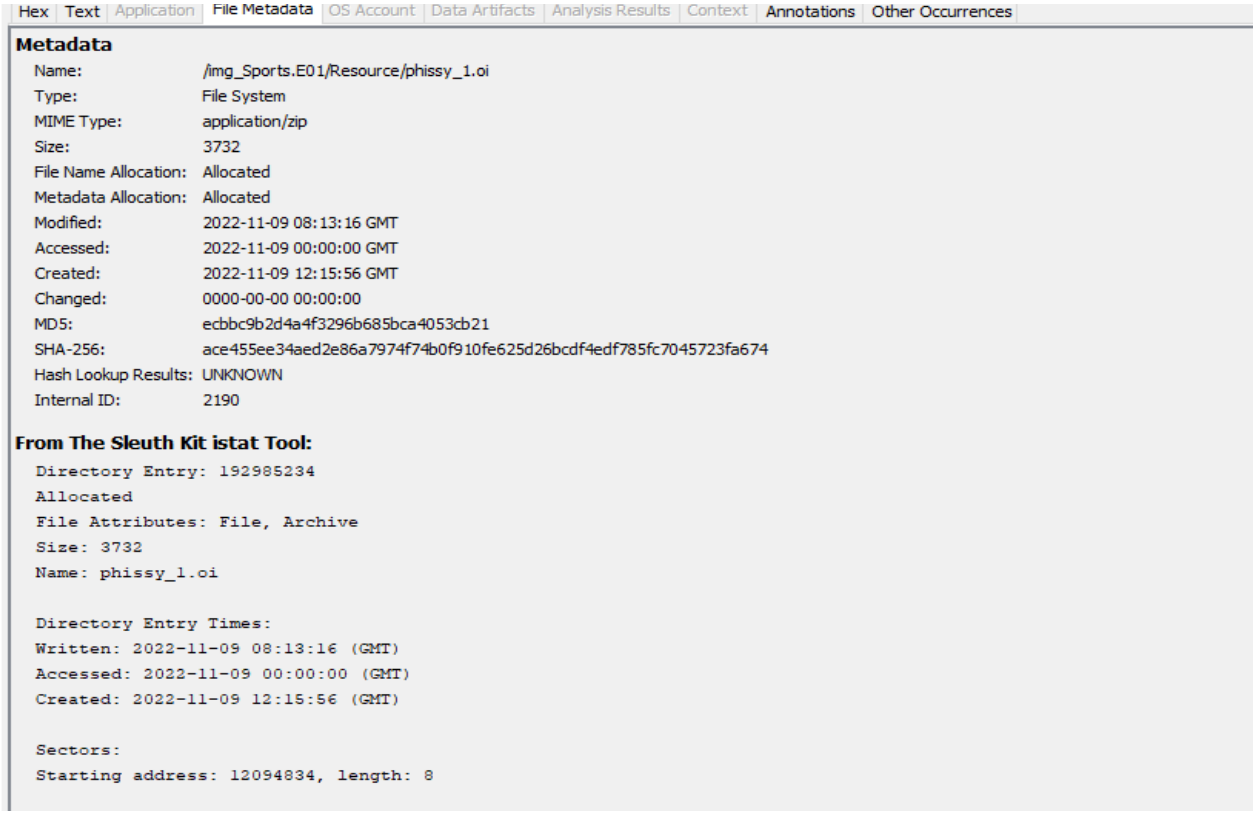
Offender Hide some secret data in audio file via using steganography technique using a morse code adaptive audio encoder technique. After decode we see that File Containing sports car code that targeted by the offender and hide in secret audio.
They used morse code adaptive audio for hide the text.

4.3.5 Category DHOS

Screenshot of the artefact:



A screenshot of artefact evidence details:



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

Metadata

Name:	/img_Sports.E01/Resource/phissy_1.oi
Type:	File System
MIME Type:	application/zip
Size:	3732
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 08:13:16 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:15:56 GMT
Changed:	0000-00-00 00:00:00
MD5:	ecbbc9b2d4a4f3296b685bca4053cb21
SHA-256:	ace455ee34aed2e86a7974f74b0f910fe625d26bcdf4edf785fc7045723fa674
Hash Lookup Results:	UNKNOWN
Internal ID:	2190

From The Sleuth Kit istat Tool:

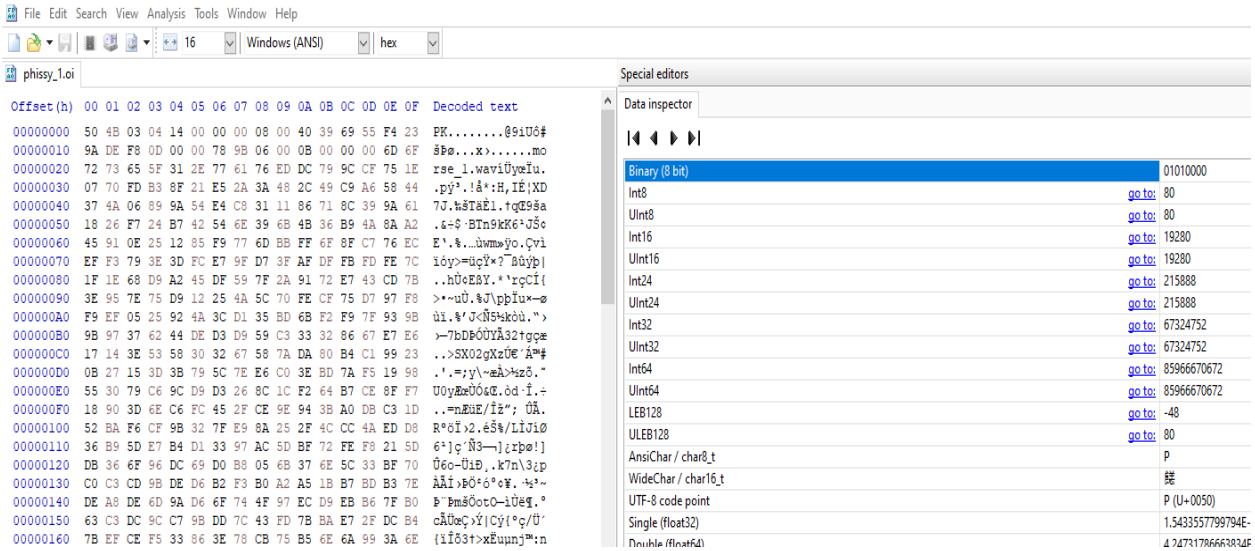
```
Directory Entry: 192985234
Allocated
File Attributes: File, Archive
Size: 3732
Name: phissy_1.oi

Directory Entry Times:
Written: 2022-11-09 08:13:16 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:15:56 (GMT)

Sectors:
Starting address: 12094834, length: 8
```

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 phissy_1.wav to phissy_1.oi

Description of the hiding/unhiding process:

Check the extension by matchinfg header signature.



File Edit Search View Analysis Tools Window Help

16 | Windows (ANSI) | hex

phissy_1.oi

```
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 40 39 69 55 F4 23  PK........@9iUô#
00000010  9A DE F8 0D 00 00 78 9B 06 00 0B 00 00 00 6D 6F  šÞø...x›......mo
00000020  72 73 65 5F 31 2E 77 61 76 ED DC 79 9C CF 75 1E  rse_1.waví Ütyœ Ïu.
00000030  07 70 FD B3 8F 21 E5 2A 3A 48 2C 49 C9 A6 58 44  .pý³.!å*:H,IÉ¦XD
00000040  37 4A 06 89 9A 54 E4 C8 31 11 86 71 8C 39 9A 61  7J.‰šTäÈ1.†qŒ9ša
00000050  18 26 F7 24 B7 42 54 6E 39 6B 4B 36 B9 4A 8A A2  .&÷$·BTn9kK6¹JŠ¢
00000060  45 91 0E 25 12 85 F9 77 6D BB FF 6F 8F C7 76 EC  E'.%.…ùwm»ÿo.Çvì
00000070  EF F3 79 3E 3D FC E7 9F D7 3F AF DF FB FD FE 7C  ïóy>=üçŸ×?¯ßûýþ|
00000080  1F 1E 68 D9 A2 45 DF 59 7F 2A 91 72 E7 43 CD 7B  ..hÙ¢EßY.*'rçCÍ{
00000090  3E 95 7E 75 D9 12 25 4A 5C 70 FE CF 75 D7 97 F8  >•~uÙ.%J\pþÏu×—ø
000000A0  F9 EF 05 25 92 4A 3C D1 35 BD 6B F2 F9 7F 93 9B  ùï.%'J<Ñ5½kòù."›
000000B0  9B 97 37 62 44 DE D3 D9 59 C3 33 32 86 67 E7 E6  ›—7bDÞÓÙYÃ32†gçæ
000000C0  17 14 3E 53 58 30 32 67 58 7A DA 80 B4 C1 99 23  ..>SX02gXzÚ€´Á™#
000000D0  0B 27 15 3D 3B 79 5C 7E E6 C0 3E BD 7A F5 19 98  .'.=;y\~æÀ>½zõ.˜
000000E0  55 30 79 C6 9C D9 D3 26 8C 1C F2 64 B7 CE 8F F7  U0yÆœÙÓ&Œ.òd·Î.÷
000000F0  18 90 3D 6E C6 FC 45 2F CE 9E 94 3B A0 DB C3 1D  ..=nÆüE/Îž"; ÛÃ.
00000100  52 BA F6 CF 9B 32 7F E9 8A 25 2F 4C CC 4A ED D8  R°öÏ›2.éŠ%/LÌJíØ
00000110  36 B9 5D E7 B4 D1 33 97 AC 5D BF 72 FE F8 21 5D  6¹]ç´Ñ3—¬]¿rþø!]
00000120  DB 36 6F 96 DC 69 D0 B8 05 6B 37 6E 5C 33 BF 70  Û6o–ÜiÐ¸.k7n\3¿p
00000130  C0 C3 CD 9B DE D6 B2 F3 B0 A2 A5 1B B7 BD B3 7E  ÀÃÍ›ÞÖ²ó°¢¥.·½³~
00000140  DE A8 DE 6D 9A D6 6F 74 4F 97 EC D9 EB B6 7F B0  Þ¨ÞmšÖotO–ìÙë¶.°
00000150  63 C3 DC 9C C7 9B DD 7C 43 FD 7B BA E7 2F DC B4  cÃÜœÇ›Ý|Cý{°ç/Ü´
00000160  7B EF CE F5 33 86 3E 78 CB 75 B5 6E 6A 99 3A 6E  {ïÎõ3†>xËuµnj™:n
```

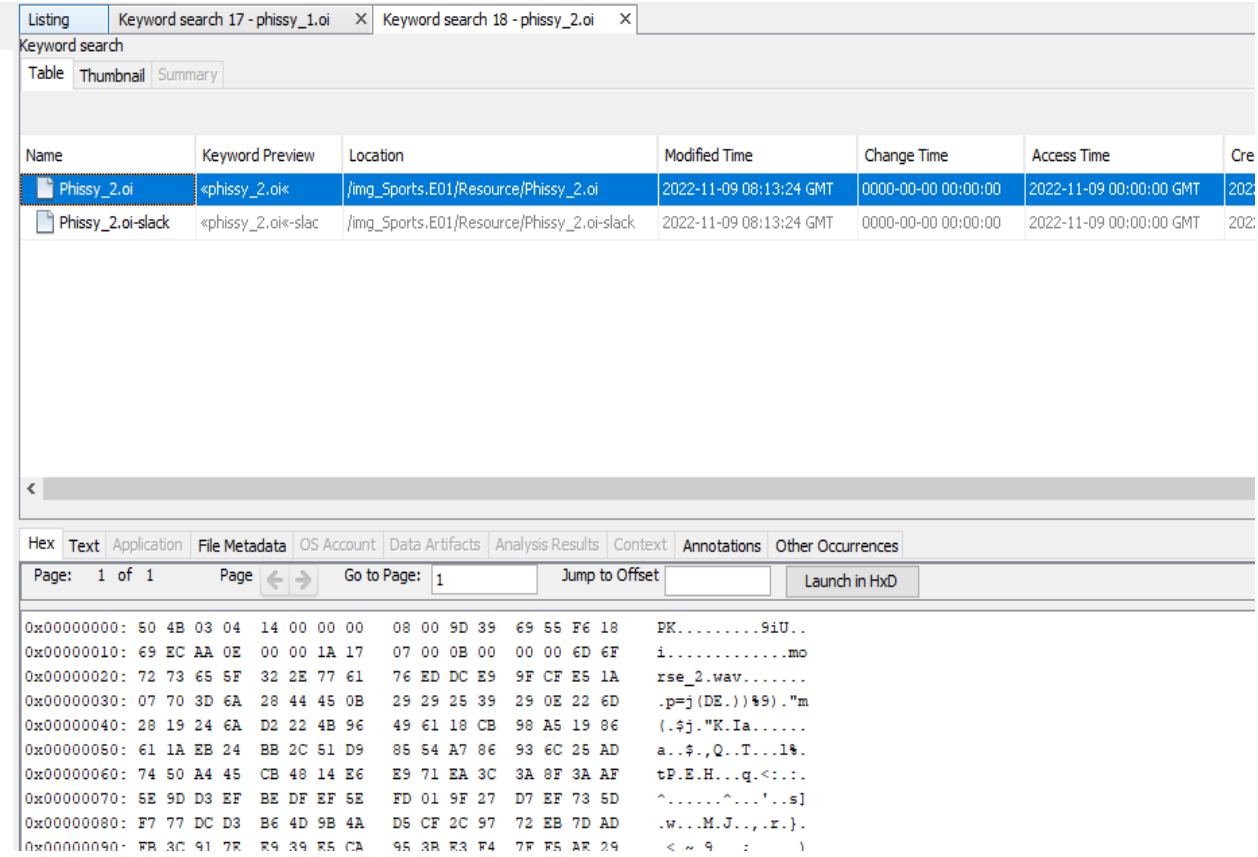
Special editors

Data inspector

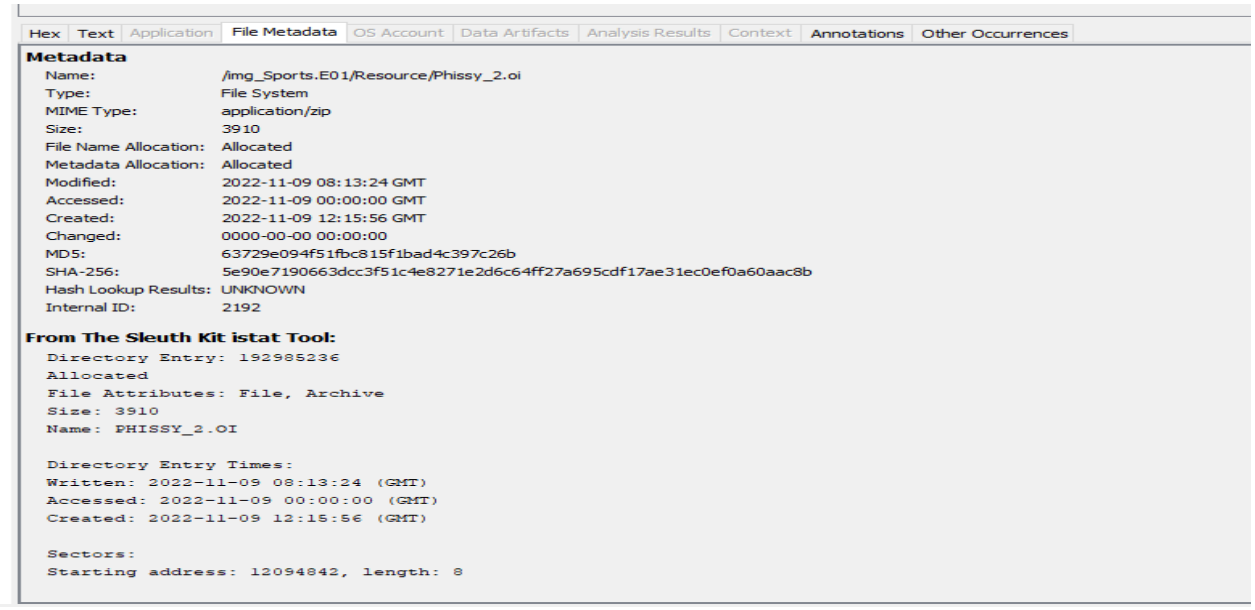
Binary (8 bit)		01010000
Int8	go to:	80
UInt8	go to:	80
Int16	go to:	19280
UInt16	go to:	19280
Int24	go to:	215888
UInt24	go to:	215888
Int32	go to:	67324752
UInt32	go to:	67324752
Int64	go to:	85966670672
UInt64	go to:	85966670672
LEB128	go to:	-48
ULEB128	go to:	80
AnsiChar / char8_t		P
WideChar / char16_t		鈀
UTF-8 code point		P (U+0050)
Single (float32)		1.5433557799794E-
Double (float64)		4.2473178666383

4.3.6 Category DHOS

Screenshot of the artefact:



A screenshot of artefact evidence details:

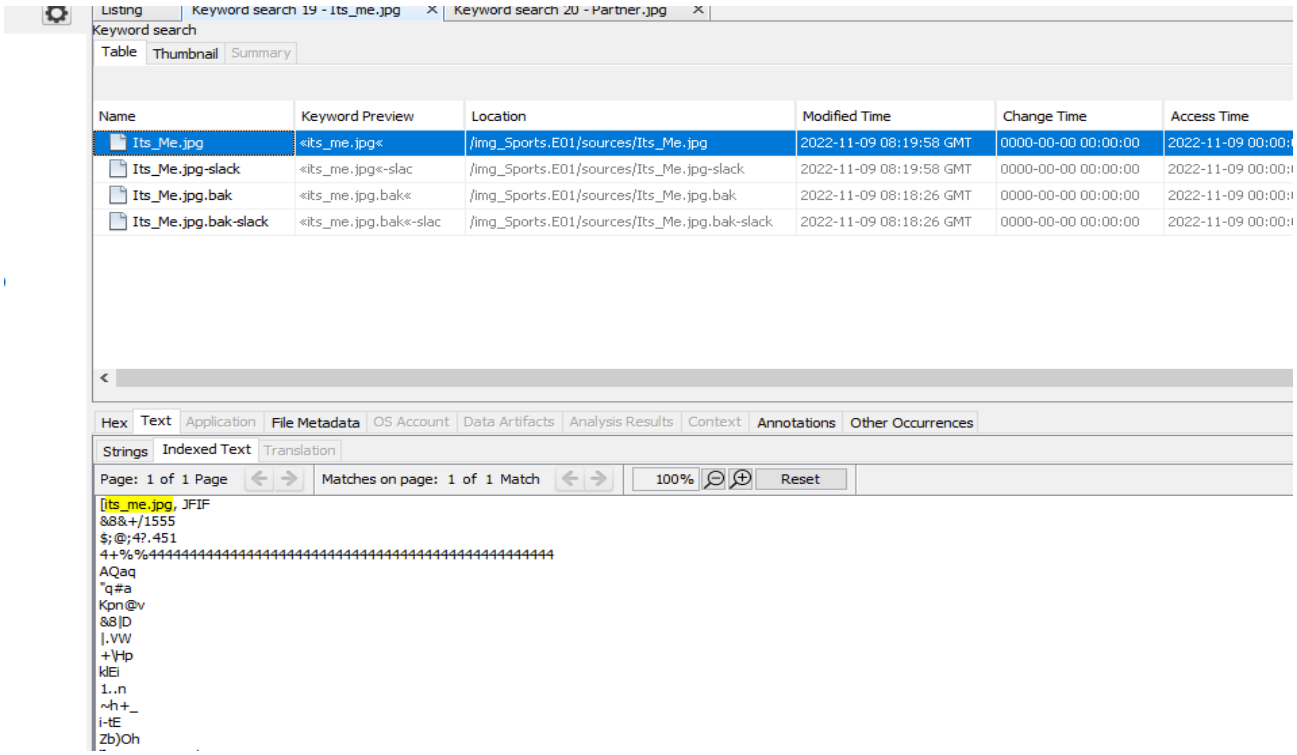


Description and implications of the artefact:

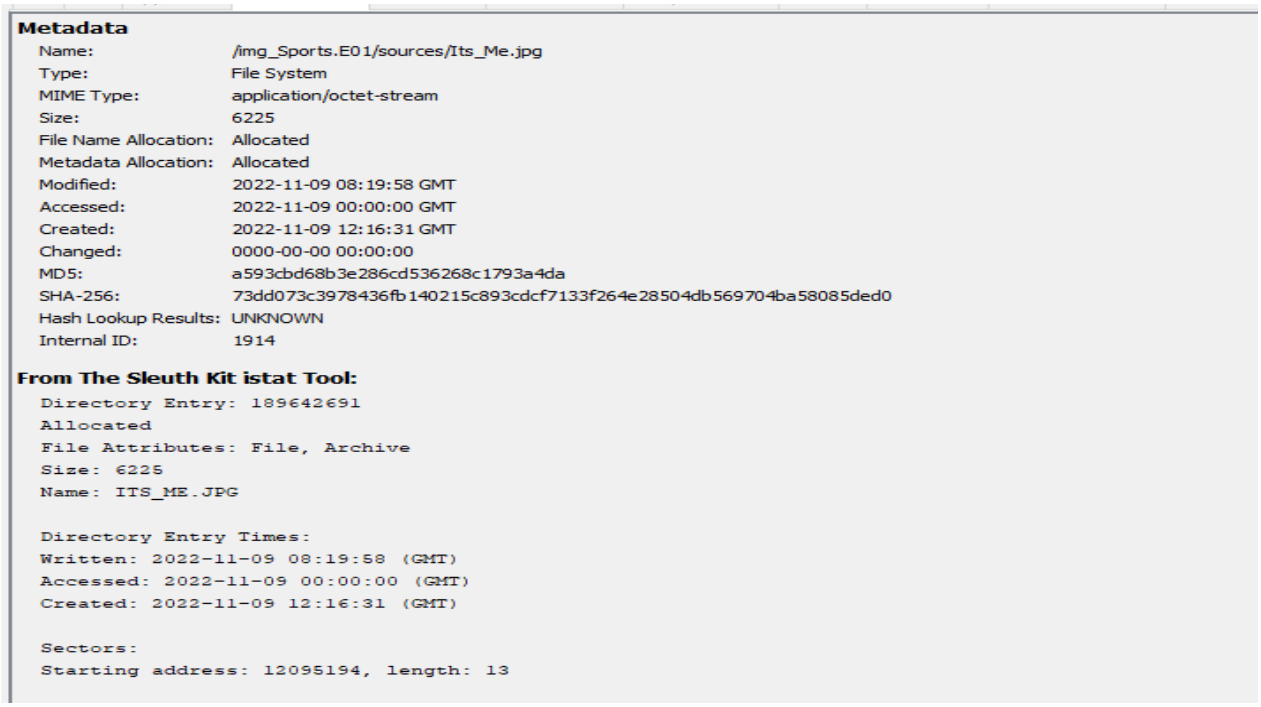
In this section Offender Make corrupt the file by change the extension of the previous section file Compressed like phissy_2.wav to phissy_2.oi

4.3.7 Category DHFS

Screenshot of the artefact:



A screenshot of artefact evidence details:



Metadata

Name:	/img_Sports.E01/sources/Its_Me.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	6225
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 08:19:58 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:16:31 GMT
Changed:	0000-00-00 00:00:00
MD5:	a593cbd68b3e286cd536268c1793a4da
SHA-256:	73dd073c3978436fb140215c893cdcf7133f264e28504db569704ba58085ded0
Hash Lookup Results:	UNKNOWN
Internal ID:	1914

From The Sleuth Kit istat Tool:

```
Directory Entry: 189642691
Allocated
File Attributes: File, Archive
Size: 6225
Name: ITS_ME.JPG

Directory Entry Times:
Written: 2022-11-09 08:19:58 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:16:31 (GMT)

Sectors:
Starting address: 12095194, length: 13
```

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

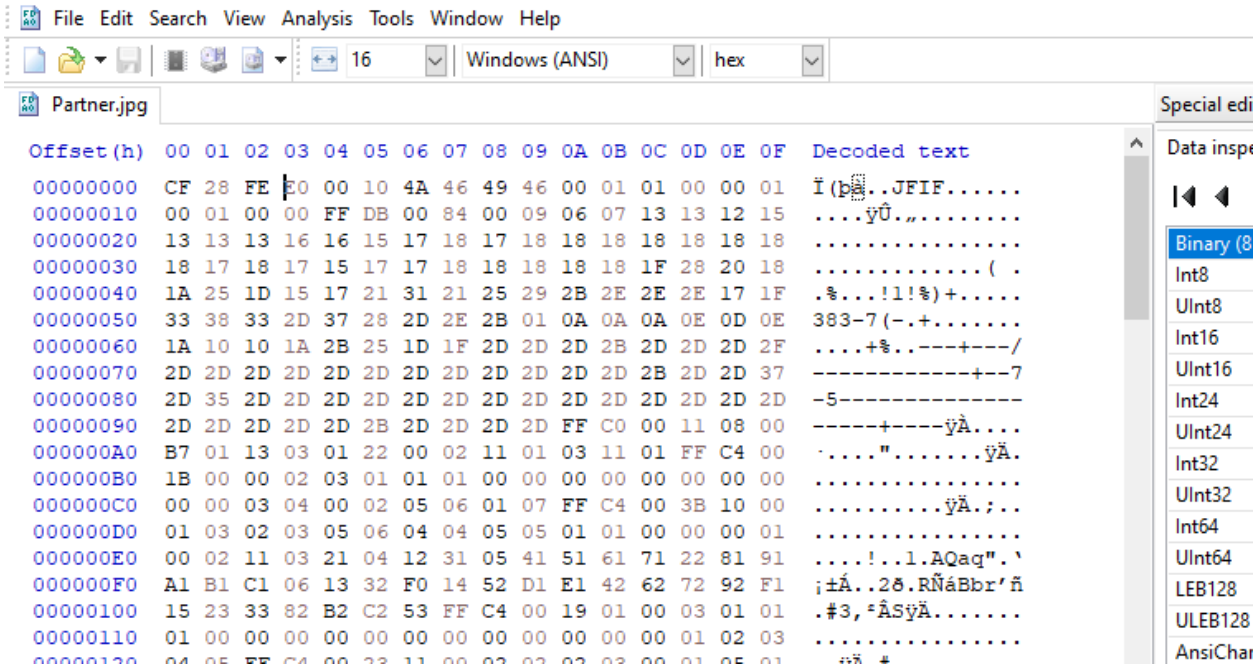
For the “Partner & Its_me” jpg file, we showed that the file does not open due to a signature or extension mismatched. This image extension we show that it's a jpg file but not opened. Using HxD tools, we can open it to check the signature with a detailed hex view with ascii value. After Open in HxD,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

We noticed that the hex value ended with FF D9.

```
000017F0  D5 62 C5 98 10 35 7F ED EA AE AD AF 80 F6 0B 16  ÕbÅ˜.5.íê®. €ö..
00001800  2E AE 2F 88 41 A9 7C CA D3 AA DA C5 58 0A 07 AB  .®/ˆA©|ÊÓªÚÅX..«
00001810  AA C5 8B 12 57 60 34 11 47 E4 58 B1 3F 1F B0 8B  ªÅ‹.W`4.GäX±?.°‹
00001820  96 D6 2C 50 11 06 6C FF 00 9D BD 51 B8 CF 9D DD  –Ö,P..lÿ..½Q¸Ï.Ý
00001830  56 96 2B F1 F4 52 7A 3A AA 9F 28 E8 3D 82 5B 53  V–+ñôRz:ªŸ(è=‚[S
00001840  7A C5 8B 86 BE 4C 28 59 53 52 B1 62 C4 A6 3F FF  zÅ‹†¾L(YSR±bÄ¦?ÿ
00001850  D9                                               Ù
```

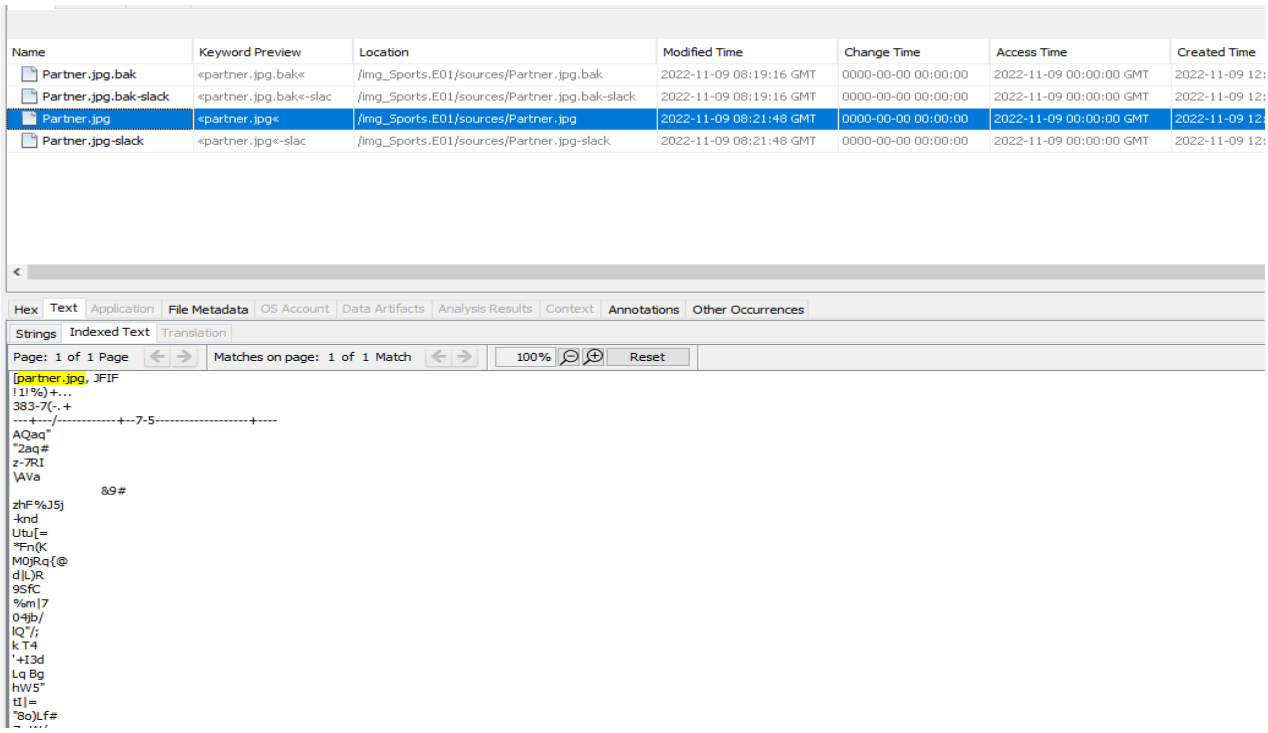
And start with some wrong hex like this.

```
File  Edit  Search  View  Analysis  Tools  Window  Help
16   Windows (ANSI)   hex
Its_Me.jpg

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  EF 08 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ï.ÿà..JFIF......
00000010  00 01 00 00 FF DB 00 84 00 0A 07 08 16 16 15 18  ....ÿÛ.„........
00000020  16 16 15 19 18 18 1A 1A 1C 18 18 1A 1A 1A 1A 1A  ................
00000030  1C 1A 21 1C 1C 1A 1C 18 1C 1A 1A 1C 21 2E 25 1C  ..!.........!.%.
00000040  1E 2B 21 1A 1A 26 38 26 2B 2F 31 35 35 35 1A 24  .+!..&8&+/1555.$
00000050  3B 40 3B 34 3F 2E 34 35 31 01 0C 0C 0C 10 0F 10  ;@;4?.451.......
00000060  1F 12 12 1E 34 2B 25 25 34 34 34 34 34 34 34 34  ....4+%%44444444
00000070  34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34  4444444444444444
00000080  34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34  4444444444444444
00000090  34 34 34 34 34 34 34 34 34 34 FF C0 00 11 08 00  4444444444ÿÀ....
000000A0  C2 01 03 03 01 22 00 02 11 01 03 11 01 FF C4 00  Â....".......ÿÄ.
000000B0  1B 00 00 02 02 03 01 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 04 05 02 03 00 01 06 07 FF C4 00 3C 10 00  ..........ÿÄ.<..
000000D0  01 03 02 03 05 06 04 04 06 02 02 03 00 00 00 01  ................
000000E0  00 02 11 03 21 04 12 31 05 41 51 61 71 06 22 81  ....!..1.AQaq.".
000000F0  91 A1 B1 13 32 C1 F0 52 62 D1 E1 14 15 23 42 72  '¡±.2ÁðRbÑá..#Br
00000100  F1 07 33 B2 D2 24 92 A2 FF C4 00 1A 01 00 03 01  ñ.3²Ò$'¢ÿÄ......
```

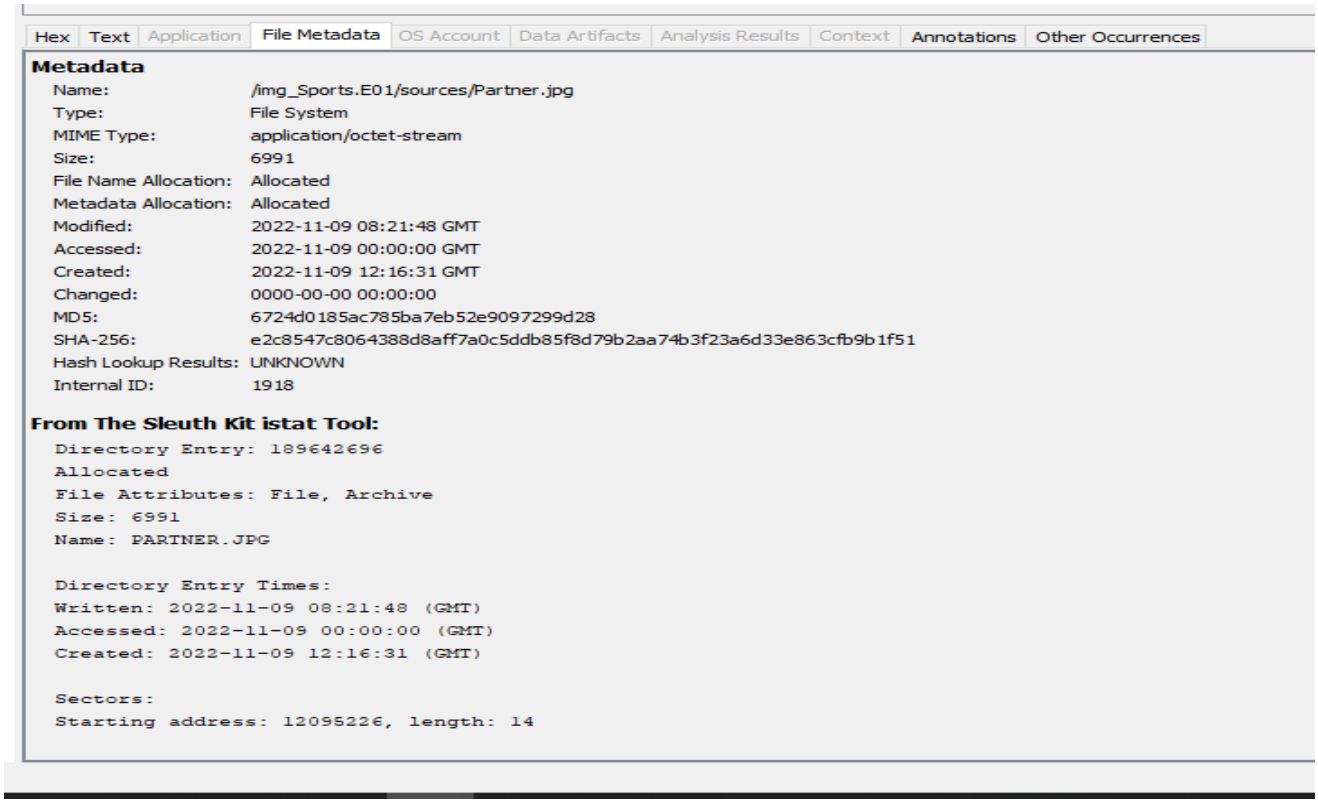


4.3.8 Category DHFS

Screenshot of the artefact:



A screenshot of artefact evidence details:



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

Metadata

Name:	/img_Sports.E01/sources/Partner.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	6991
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 08:21:48 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:16:31 GMT
Changed:	0000-00-00 00:00:00
MD5:	6724d0185ac785ba7eb52e9097299d28
SHA-256:	e2c8547c8064388d8aff7a0c5ddb85f8d79b2aa74b3f23a6d33e863cfb9b1f51
Hash Lookup Results:	UNKNOWN
Internal ID:	1918

From The Sleuth Kit istat Tool:

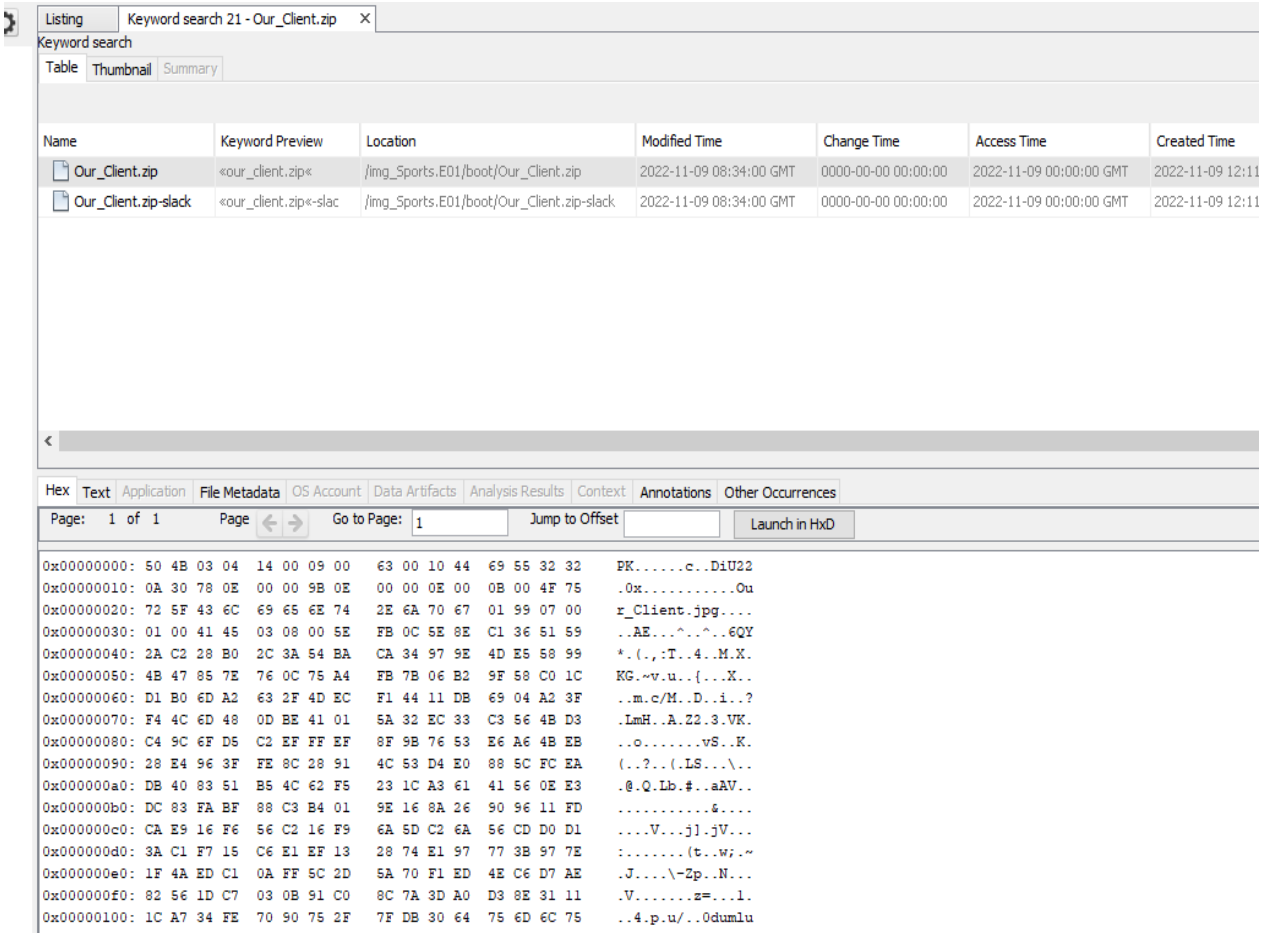
```
Directory Entry: 189642696
Allocated
File Attributes: File, Archive
Size: 6991
Name: PARTNER.JPG

Directory Entry Times:
Written: 2022-11-09 08:21:48 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:16:31 (GMT)

Sectors:
Starting address: 12095226, length: 14
```

Description and implications of the artefact:

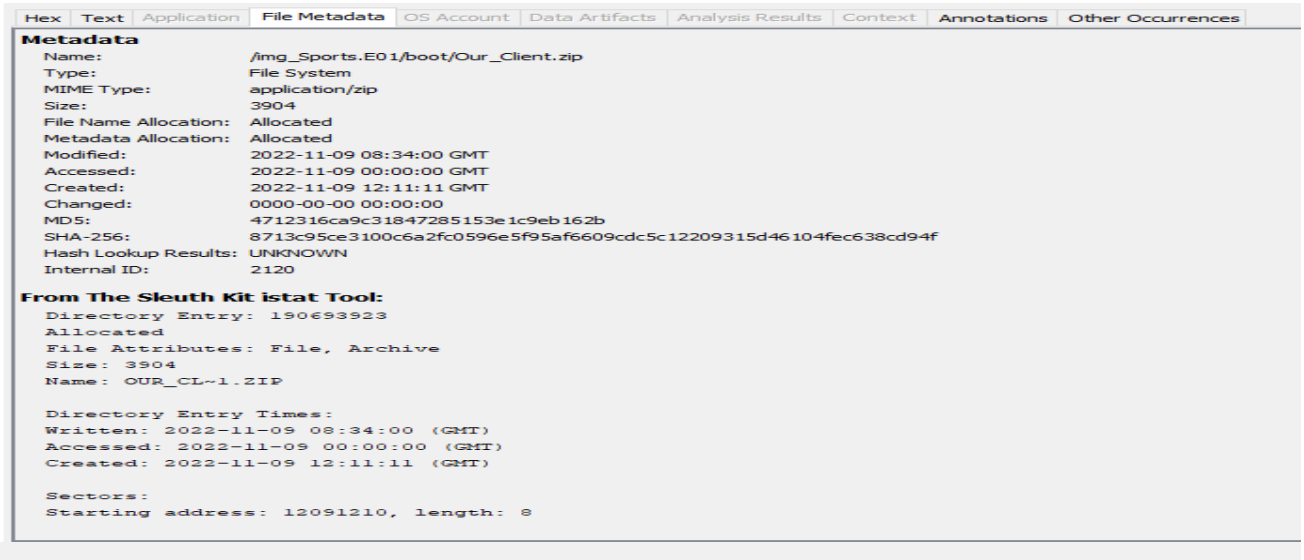
Finally we noticed that this is the offender image and information. But the image is being corrupted. We need to correct it. Here is, they do the file signature change for hide the real image. This is a offenders jpg image but not opened. So after correct the header signature of jpg file then it will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

4.4.1 Category DHU_1

Screenshot of the artefact:



A screenshot of artefact evidence details:

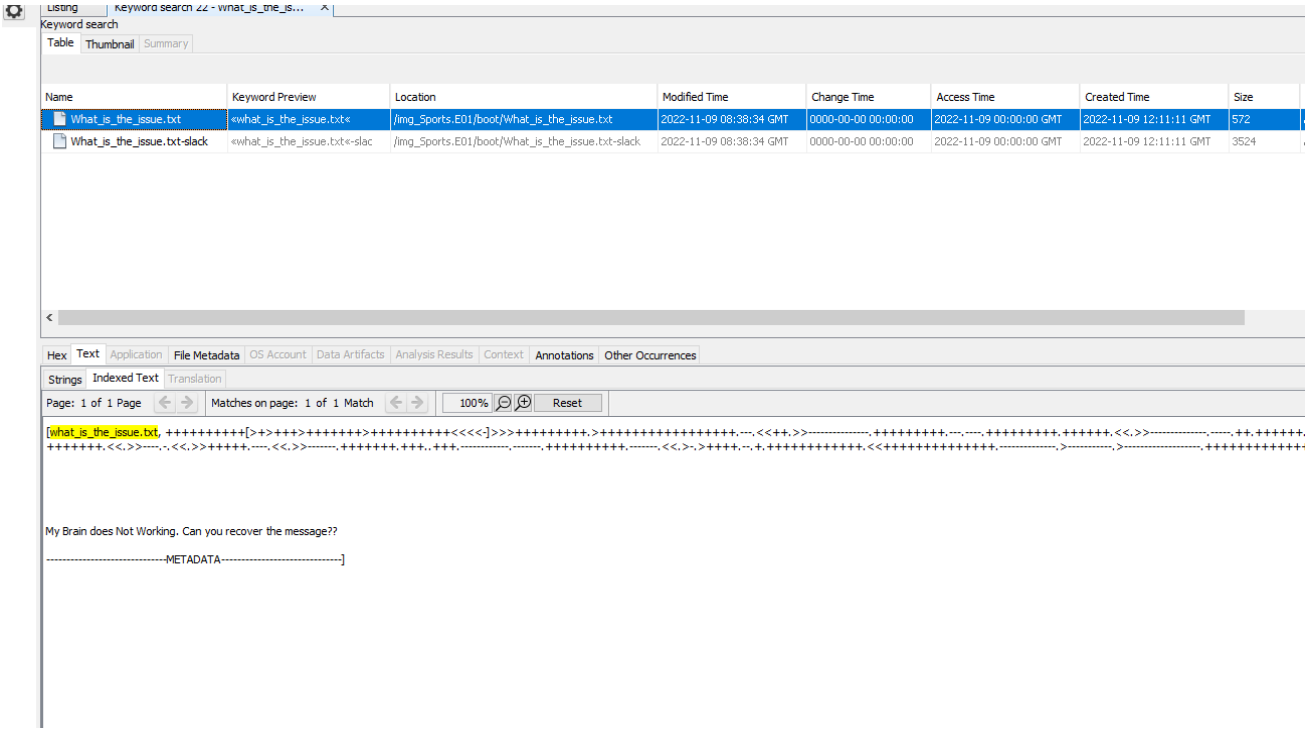


Description and implications of the artefact:

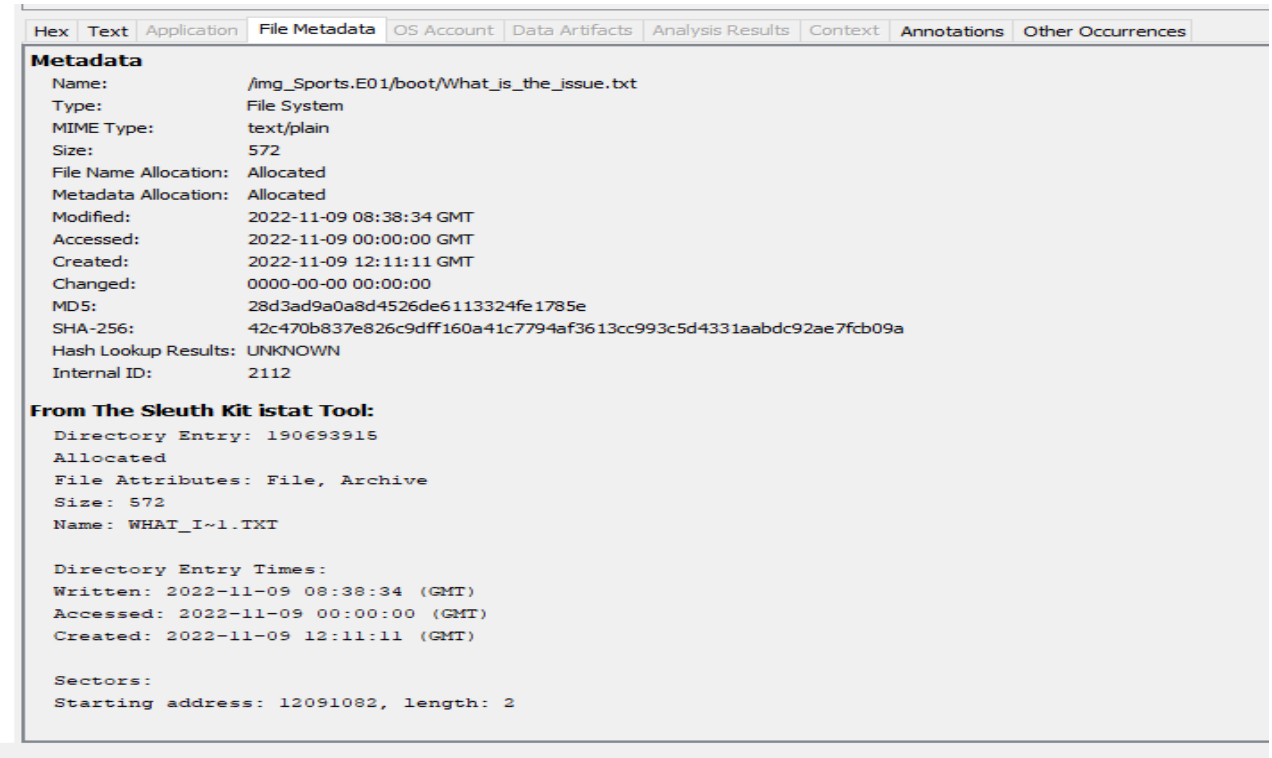
In this section we found a notes text file & a zip file for password protectied that is define that a client information. We found the image zip file that is password protected. Offender hide the image in a zip file by password protect. Notes file define us that the zip file password can be found from chats like car model number. That can prove against offender by a strong proof.

4.4.2 Category DHU_2

Screenshot of the artefact:



A screenshot of artefact evidence details:



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

Metadata

Name:	/img_Sports.E01/boot/What_is_the_issue.txt
Type:	File System
MIME Type:	text/plain
Size:	572
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 08:38:34 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:11:11 GMT
Changed:	0000-00-00 00:00:00
MD5:	28d3ad9a0a8d4526de6113324fe1785e
SHA-256:	42c470b837e826c9dff160a41c7794af3613cc993c5d4331aabdc92ae7fcb09a
Hash Lookup Results:	UNKNOWN
Internal ID:	2112

From The Sleuth Kit istat Tool:

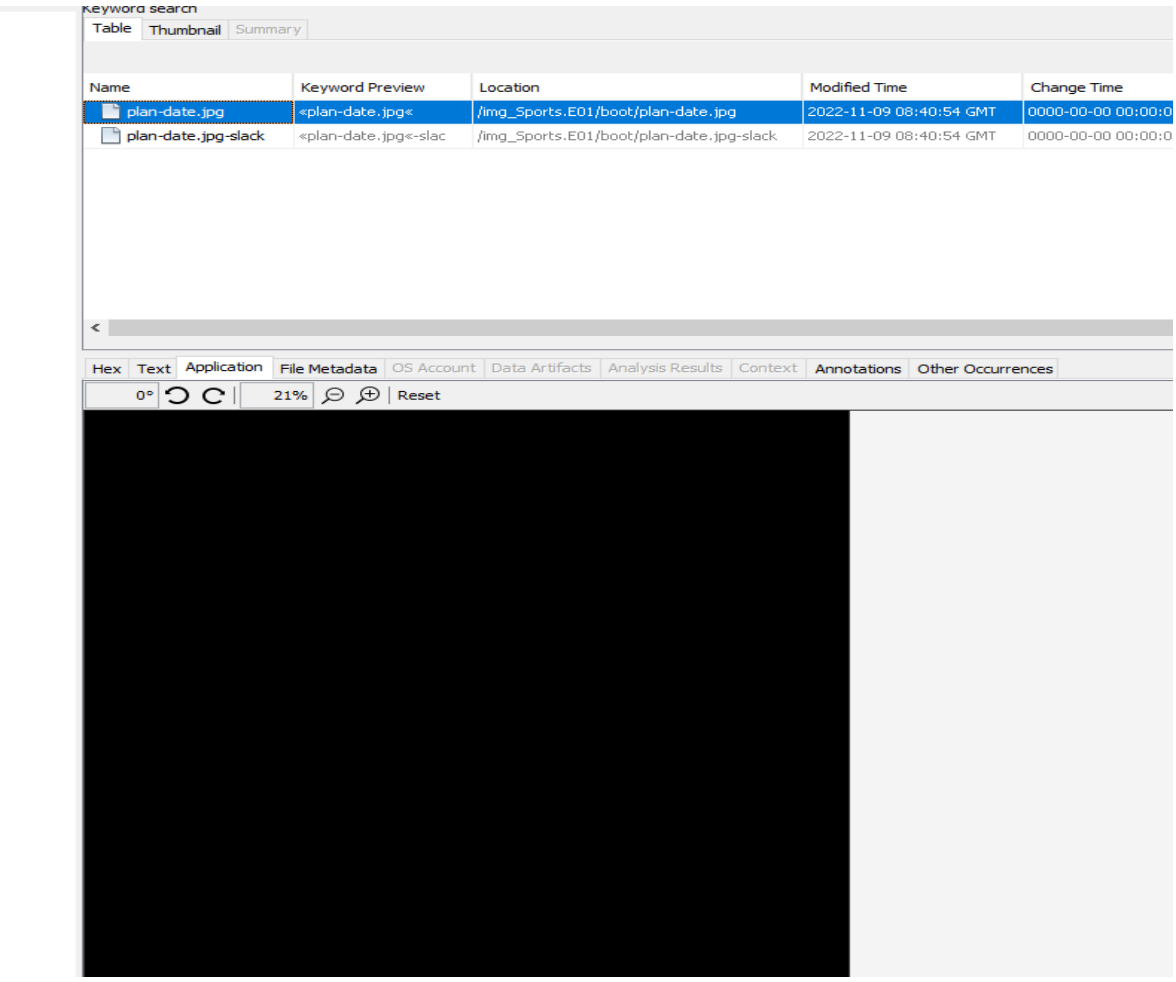
```
Directory Entry: 190693915
Allocated
File Attributes: File, Archive
Size: 572
Name: WHAT_I~1.TXT

Directory Entry Times:
Written: 2022-11-09 08:38:34 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:11:11 (GMT)

Sectors:
Starting address: 12091082, length: 2
```

Description and implications of the artefact:

In this section, after decode the brainfuck language code we found File Containing the information of offender threat about client issues. They hide the secret info using a cryptographic cipher named as brainfuck algorithm.

4.4.3 Category DHU_3

Screenshot of the artefact:



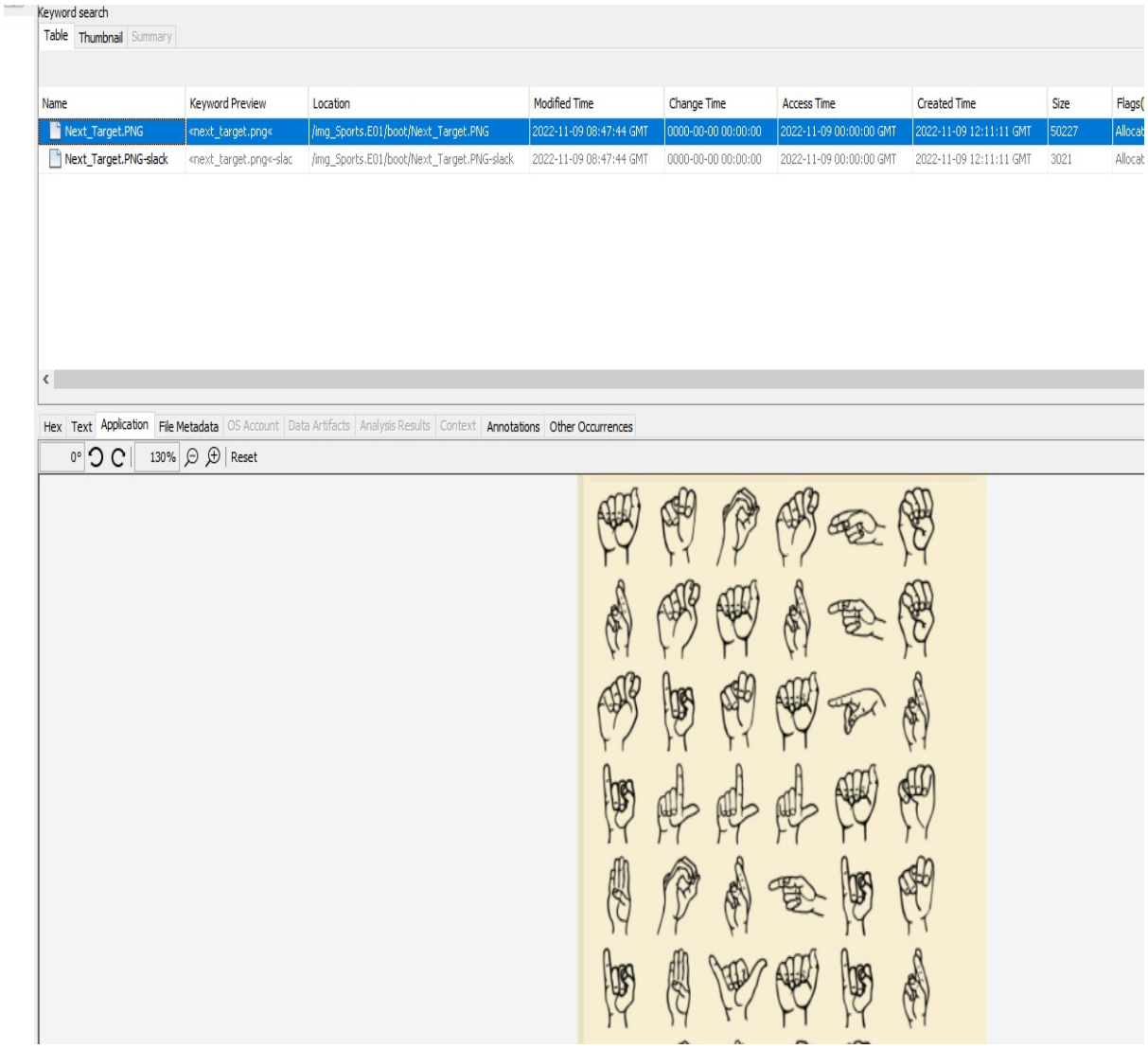
A screenshot of artefact evidence details:

Description and implications of the artefact:

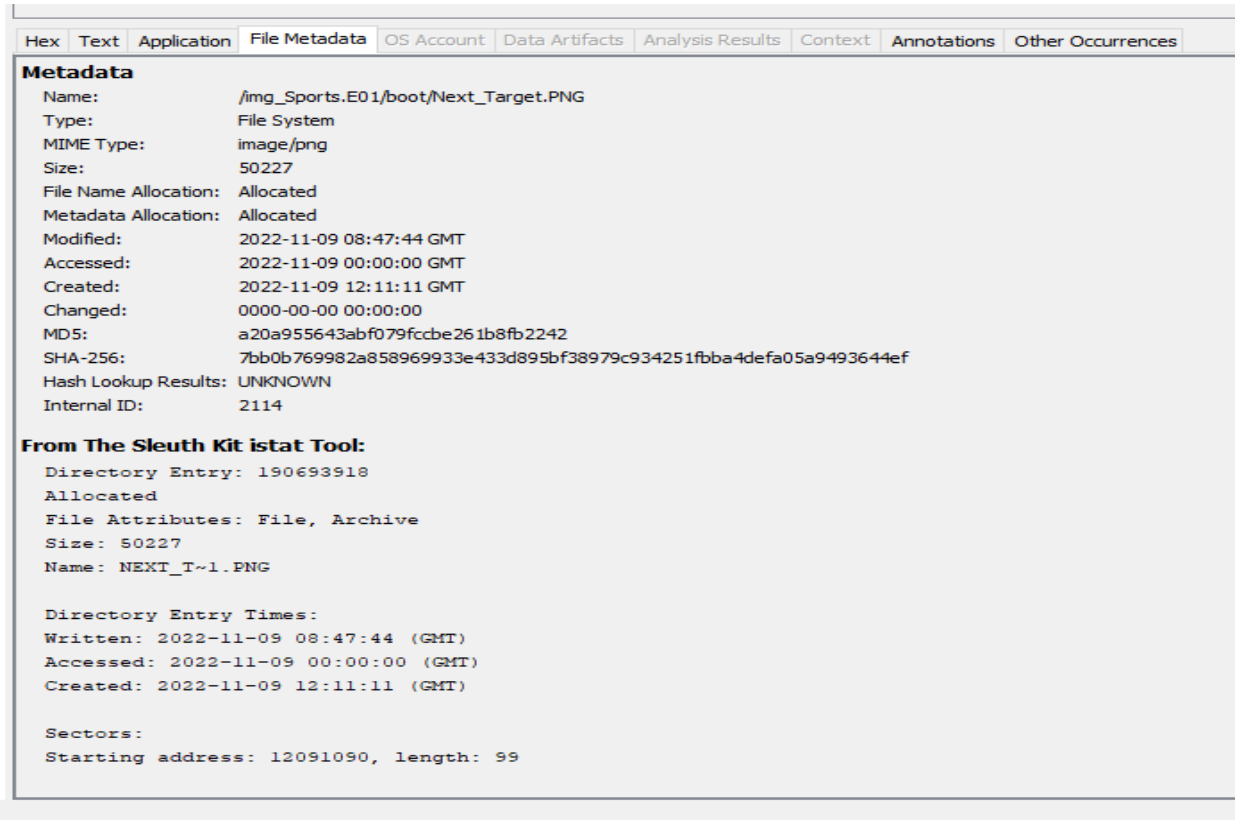
In this section we will found stealing sports car planning date by the offende & their partner. we found a image file named plan-date.png but its also not opened. But here we found a another text file that is related to this png file. We noticed that plan-date.png file string compromised by this encase. 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 Plan date of the sports car stealing.

4.3.8 Category DR_1

Screenshot of the artefact:



A screenshot of artefact evidence details:



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

Metadata

Name:	/img_Sports.E01/boot/Next_Target.PNG
Type:	File System
MIME Type:	image/png
Size:	50227
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 08:47:44 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 12:11:11 GMT
Changed:	0000-00-00 00:00:00
MD5:	a20a955643abf079fccbe261b8fb2242
SHA-256:	7bb0b769982a858969933e433d895bf38979c934251fbba4defa05a9493644ef
Hash Lookup Results:	UNKNOWN
Internal ID:	2114

From The Sleuth Kit istat Tool:

```
Directory Entry: 190693918
Allocated
File Attributes: File, Archive
Size: 50227
Name: NEXT_T~1.PNG

Directory Entry Times:
Written: 2022-11-09 08:47:44 (GMT)
Accessed: 2022-11-09 00:00:00 (GMT)
Created: 2022-11-09 12:11:11 (GMT)

Sectors:
Starting address: 12091090, length: 99
```

Description and implications of the artefact:

In this section, we found a image that is related to sign language. That means another some secret message encoded in sign language.after extracted the message we found “Another Target in Aprill : Lamborgini by AirHouse” that is the offender & his partners next target about sports car stealing.

Description of the hiding/unhiding process:

https://www.dcode.fr/american-sign-language

Using this site we decode the sign language cipher code to plain text.

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

6.1.1 Reflection

Digital crime stealing services is very bad things in this time. Digital crime is the most common factors for this time & victim can easily the target by the social media or hacked by phising.

6.1.2 Strengths/major contributions to the group

Completed the full Project on 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 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.