**Title: Digital forensics encase image analysis**

Case Scenario: A forensic image of Rahim computer has been provide to you. A group of people killed a person. They used violence image to indicate the person. They communicate social media and share some picture. They communicate Text file messages.

Suspect: Rahim

Victim Name: Karim

1. OVERVIEW OF THE CASE
   1. Narrative of the case
   2. Time line of key evidence
   3. Details of the offenders, victims and witnesses
   4. Photographs of any physical evidence, clues or supplemental material
   5. Scenario rules
2. LEGISLATION ANALYSIS
   1. Legislation
   2. Point to prove
   3. What the digital forensics case can prove
   4. What the digital forensics case will not prove
   5. Highlight any artefacts that undermine the prosecutions case
3. EVIDENCE FILE
   1. Details of the evidence file
   2. Hash value of the evidence file
4. ARTEFACTS
   1. Summary of artefacts
   2. Data recovery artefacts
   3. Data hiding artefacts
5. SUPPORTING MATERIAL
6. PERSONAL REFLECTION
   1. Student1
7. Overview of the Case
   1. Narrative of the case

A forensic image of Rahim computer has been provide to you. A group of people killed a person. They used violence image to indicate the person. They communicate social media and share some picture. They communicate Text file messages.

* 1. Timeline of key evidence

Image Information:

Acquisition started: Sat Jan 21 21:20:43 2023

Acquisition finished: Sat Jan 21 21:48:28 2023

Segment list:

G:\ssd analysis\digital image\hacker.E01

G:\ssd analysis\digital image\hacker.E02

G:\ssd analysis\digital image\hacker.E03

G:\ssd analysis\digital image\hacker.E04

G:\ssd analysis\digital image\hacker.E05

G:\ssd analysis\digital image\hacker.E06

G:\ssd analysis\digital image\hacker.E07

G:\ssd analysis\digital image\hacker.E08

G:\ssd analysis\digital image\hacker.E09

G:\ssd analysis\digital image\hacker.E10

G:\ssd analysis\digital image\hacker.E11

G:\ssd analysis\digital image\hacker.E12

G:\ssd analysis\digital image\hacker.E13

G:\ssd analysis\digital image\hacker.E14

G:\ssd analysis\digital image\hacker.E15

G:\ssd analysis\digital image\hacker.E16

G:\ssd analysis\digital image\hacker.E17

G:\ssd analysis\digital image\hacker.E18

G:\ssd analysis\digital image\hacker.E19

G:\ssd analysis\digital image\hacker.E20

G:\ssd analysis\digital image\hacker.E21

G:\ssd analysis\digital image\hacker.E22

G:\ssd analysis\digital image\hacker.E23

G:\ssd analysis\digital image\hacker.E24

G:\ssd analysis\digital image\hacker.E25

G:\ssd analysis\digital image\hacker.E26

G:\ssd analysis\digital image\hacker.E27

G:\ssd analysis\digital image\hacker.E28

G:\ssd analysis\digital image\hacker.E29

G:\ssd analysis\digital image\hacker.E30

G:\ssd analysis\digital image\hacker.E31

G:\ssd analysis\digital image\hacker.E32

G:\ssd analysis\digital image\hacker.E33

G:\ssd analysis\digital image\hacker.E34

G:\ssd analysis\digital image\hacker.E35

G:\ssd analysis\digital image\hacker.E36

G:\ssd analysis\digital image\hacker.E37

G:\ssd analysis\digital image\hacker.E38

G:\ssd analysis\digital image\hacker.E39

G:\ssd analysis\digital image\hacker.E40

G:\ssd analysis\digital image\hacker.E41

G:\ssd analysis\digital image\hacker.E42

G:\ssd analysis\digital image\hacker.E43

G:\ssd analysis\digital image\hacker.E44

G:\ssd analysis\digital image\hacker.E45

G:\ssd analysis\digital image\hacker.E46

G:\ssd analysis\digital image\hacker.E47

G:\ssd analysis\digital image\hacker.E48

G:\ssd analysis\digital image\hacker.E49

G:\ssd analysis\digital image\hacker.E50

G:\ssd analysis\digital image\hacker.E51

G:\ssd analysis\digital image\hacker.E52

G:\ssd analysis\digital image\hacker.E53

G:\ssd analysis\digital image\hacker.E54

* 1. Details of the offenders, victims and witnesses:

A targeted person name karim threat by offenders. witness is people image & many txt file.

* 1. Scenario Rules:

A person represent a victim image. Gun represent the tools of killer.

1. Legislation Analysis:
   1. Point to prove

Many people torture a person it is ensure that crime occurred by this people.

* 1. What the Digital Forensics case can prove

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

* 1. What the Digital Forensics case will not prove

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

* 1. Highlight any artefacts that undermine the prosecution’s case.

1. Evidence File
   1. Details of the Evidence File

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: crime101

Evidence Number: 101

Unique Description:

Examiner: nishad

Notes:

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

Information for G:\ssd analysis\digital image\hacker:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Logical

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 253,073,518

[Physical Drive Information]

Removable drive: False

Source data size: 123571 MB

Sector count: 253073518

Image Information:

Acquisition started: Sat Jan 21 21:20:43 2023

Acquisition finished: Sat Jan 21 21:48:28 2023

Segment list:

G:\ssd analysis\digital image\hacker.E01

G:\ssd analysis\digital image\hacker.E02

G:\ssd analysis\digital image\hacker.E03

* 1. Hash value of the Evidence File

[Computed Hashes]

MD5 checksum: 3e6a084e097ec4f62e5f606f12fd53be

SHA1 checksum: 5ff6d3d55910055e6a9a86c3cc9c21905729f88f

1. Artefacts
   1. Summary of Artefacts

Data Recovery

|  |  |
| --- | --- |
| DRF | Content of files |
| DRA | Contents of application data structure |
| DROS | Contents of operating system data structure |
| DRFS | Content of files system |

Data Hiding

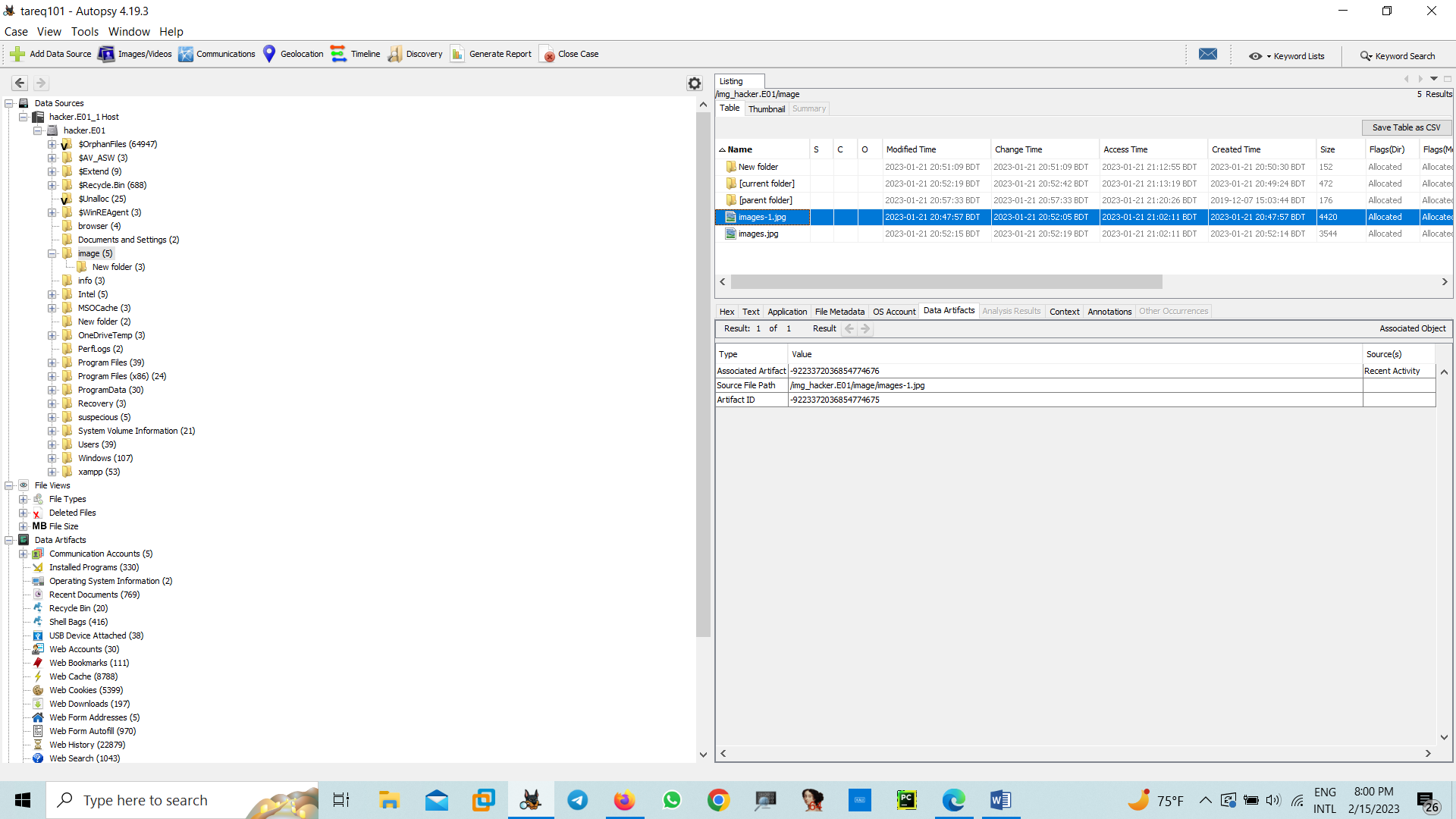
|  |  |
| --- | --- |
| DHU | User |
| DHA | Application |
| DHOS | Operating System |
| DHFS | File system |

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Type | File name | comment |
| DRF | Document File & picture file | man.txt  images-1.jpg | File contains the killer information and image |
| DRA | Picture File | Images.jpg | Contains the gun image |
| DHFS | Document File | Key.txt | keyword information and name |
| DR\_1 | Image File | Images.jpg | Social media information |
| DHU\_3 | Text File | malware.txt | Date and time provided |
| DHU\_1 | Compressed file | suspecious.zip | File contains the victim information |
| DROS | Registry File | G:\ssd analysis\digital image\hacker.E01 | File contains the information about cyber crime |

* 1. Data Recovery Artefacts

Category DRF

Screenshot of the artefact:



It’s assigned victim and killer



Description and implications of the artefact:

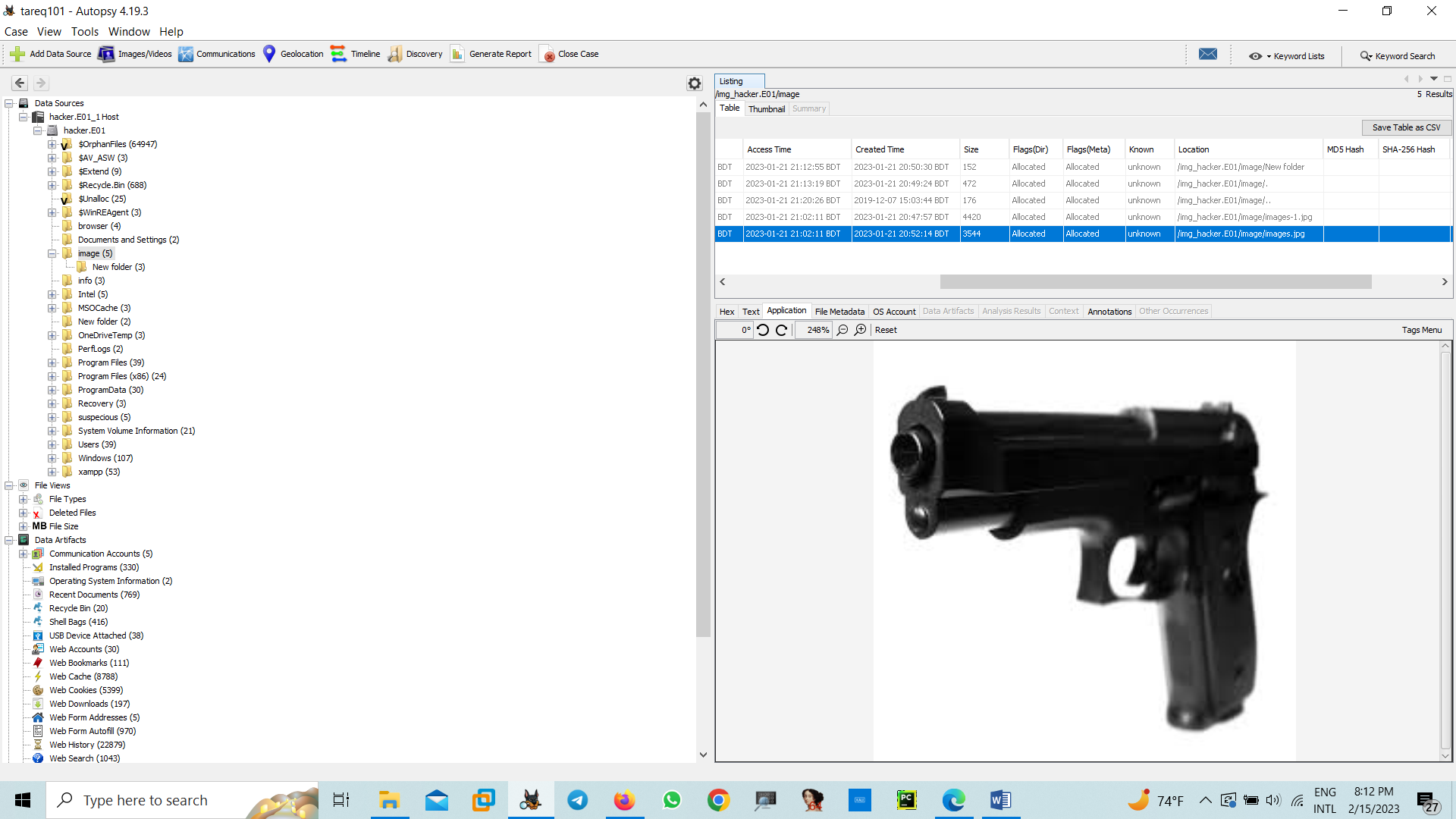
Images-1.jpg shown some people torture and they trying to killed a man. The extracted image indicate the crime activity.

**Metadata**

|  |  |
| --- | --- |
| Name: | /img\_hacker.E01/image/images-1.jpg |
| Type: | File System |
| MIME Type: | image/jpeg |
| Size: | 4420 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 2023-01-21 20:47:57 BDT |
| Accessed: | 2023-01-21 21:02:11 BDT |
| Created: | 2023-01-21 20:47:57 BDT |
| Changed: | 2023-01-21 20:52:05 BDT |
| MD5: | Not calculated |
| SHA-256: | Not calculated |
| Hash Lookup Results: | UNKNOWN |
| Internal ID: | 219590 |

4.2.2 Category DRA

Screenshot of the artefact:



A screenshot of artefact evidence details:

**Metadata**

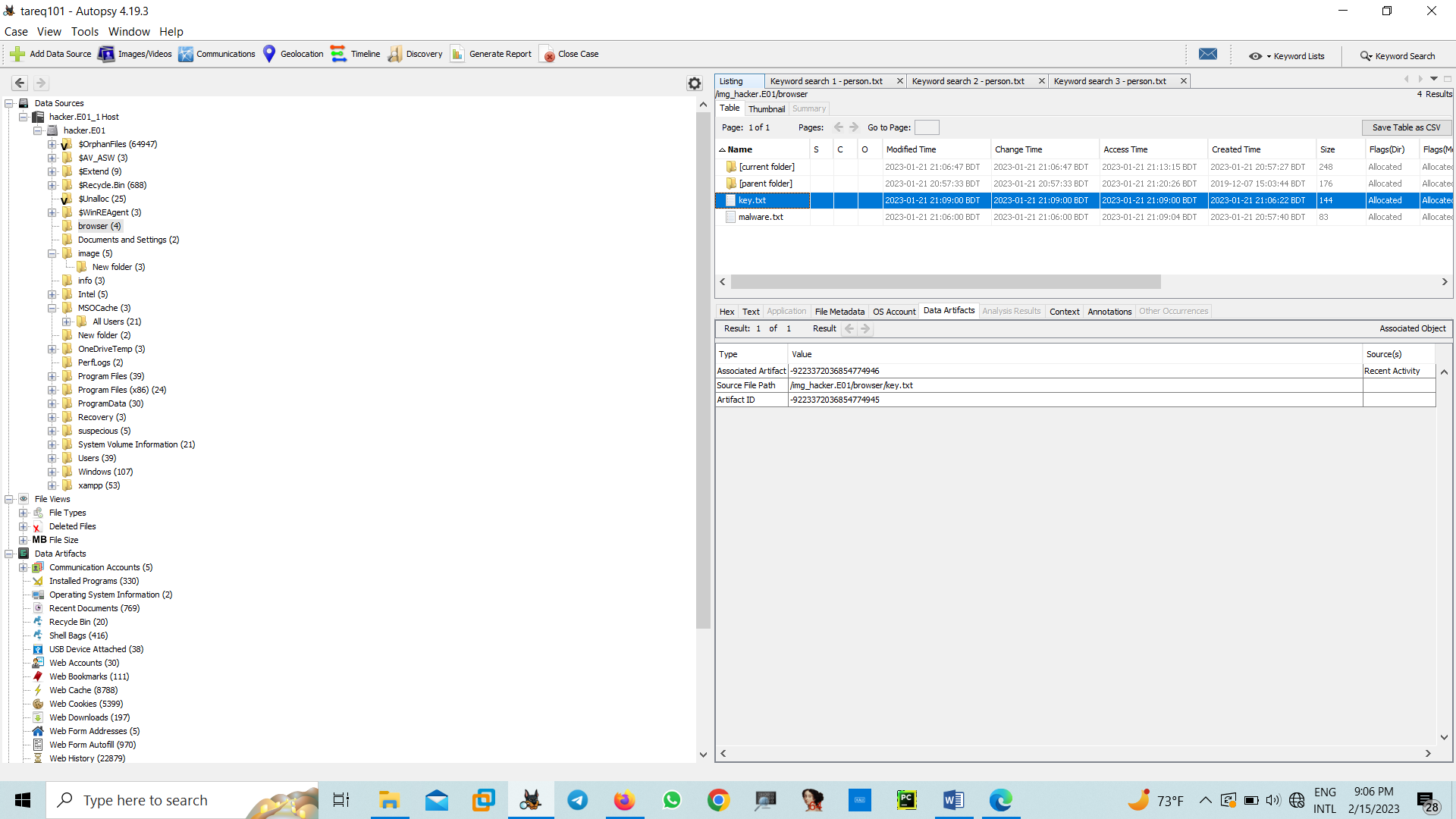
|  |  |
| --- | --- |
| Name: | /img\_hacker.E01/image/images.jpg |
| Type: | File System |
| MIME Type: | image/jpeg |
| Size: | 3544 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 2023-01-21 20:52:15 BDT |
| Accessed: | 2023-01-21 21:02:11 BDT |
| Created: | 2023-01-21 20:52:14 BDT |
| Changed: | 2023-01-21 20:52:19 BDT |
| MD5: | Not calculated |
| SHA-256: | Not calculated |
| Hash Lookup Results: | UNKNOWN |
| Internal ID: | 219592 |

Description and implications of the artefact:

Victim used to gun to killed the people. The extracted image will shown here.

4.2.4 Category DRFS

Screenshot of the artefact:



A screenshot of artefact evidence details:

**Metadata**

|  |  |
| --- | --- |
| Name: | /img\_hacker.E01/browser/key.txt |
| Type: | File System |
| MIME Type: | text/plain |
| Size: | 144 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 2023-01-21 21:09:00 BDT |
| Accessed: | 2023-01-21 21:09:00 BDT |
| Created: | 2023-01-21 21:06:22 BDT |
| Changed: | 2023-01-21 21:09:00 BDT |
| MD5: | Not calculated |
| SHA-256: | Not calculated |
| Hash Lookup Results: | UNKNOWN |
| Internal ID: | 219584 |

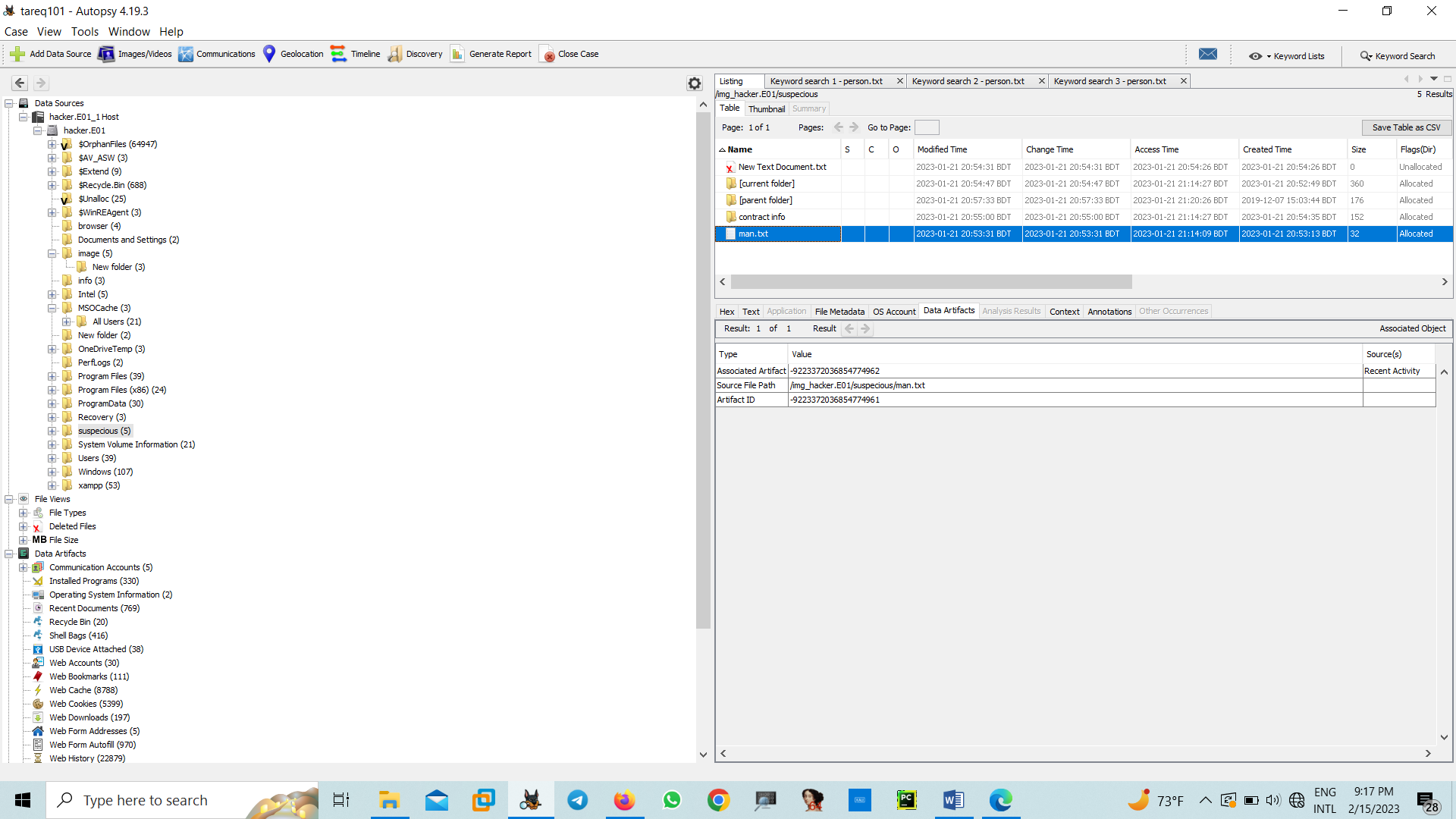
Description and implications of the artefact:

key.txt is the text file. In text file hide some data using cryptography algorithm. They used base64 encoding system for hide the text.

Cipher(key.txt): NBSWY3DPEBWWC3ROO5SSA3LBMRSSAYJAOBWGC3RAORXSAYJAOBSXE43PNYQHO2DPONSSA3TBNVSSA2LTEBVWC4TJNYXEC3TEEB3WKIDHMV2CAZTJOZSSA5DIN52XGYLOMQQHIYLLMEQC4===(base64)

4.3.7 Category DHU\_3

Screenshot of the artefact:



A screenshot of artefact evidence details:

**Metadata**

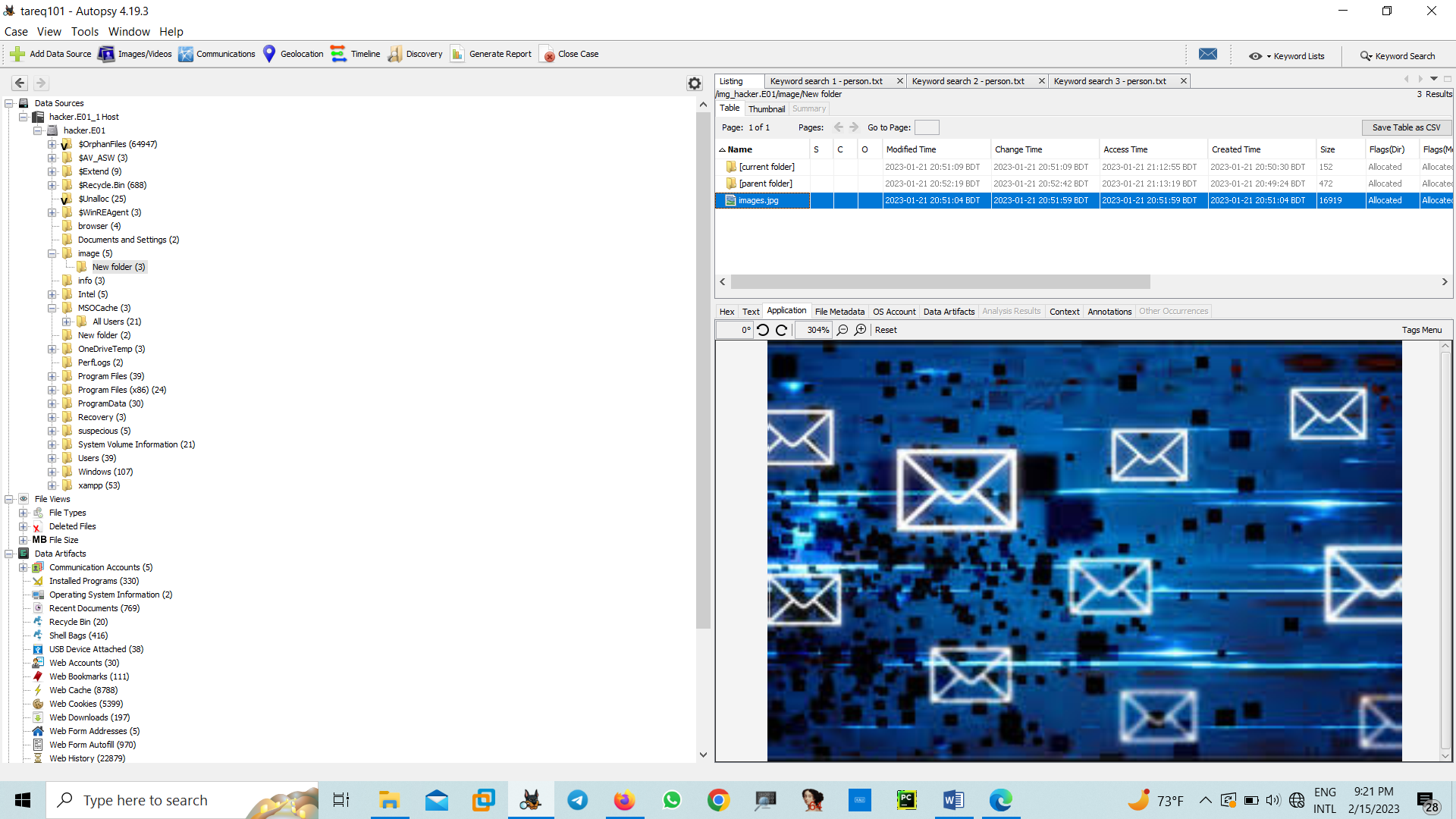
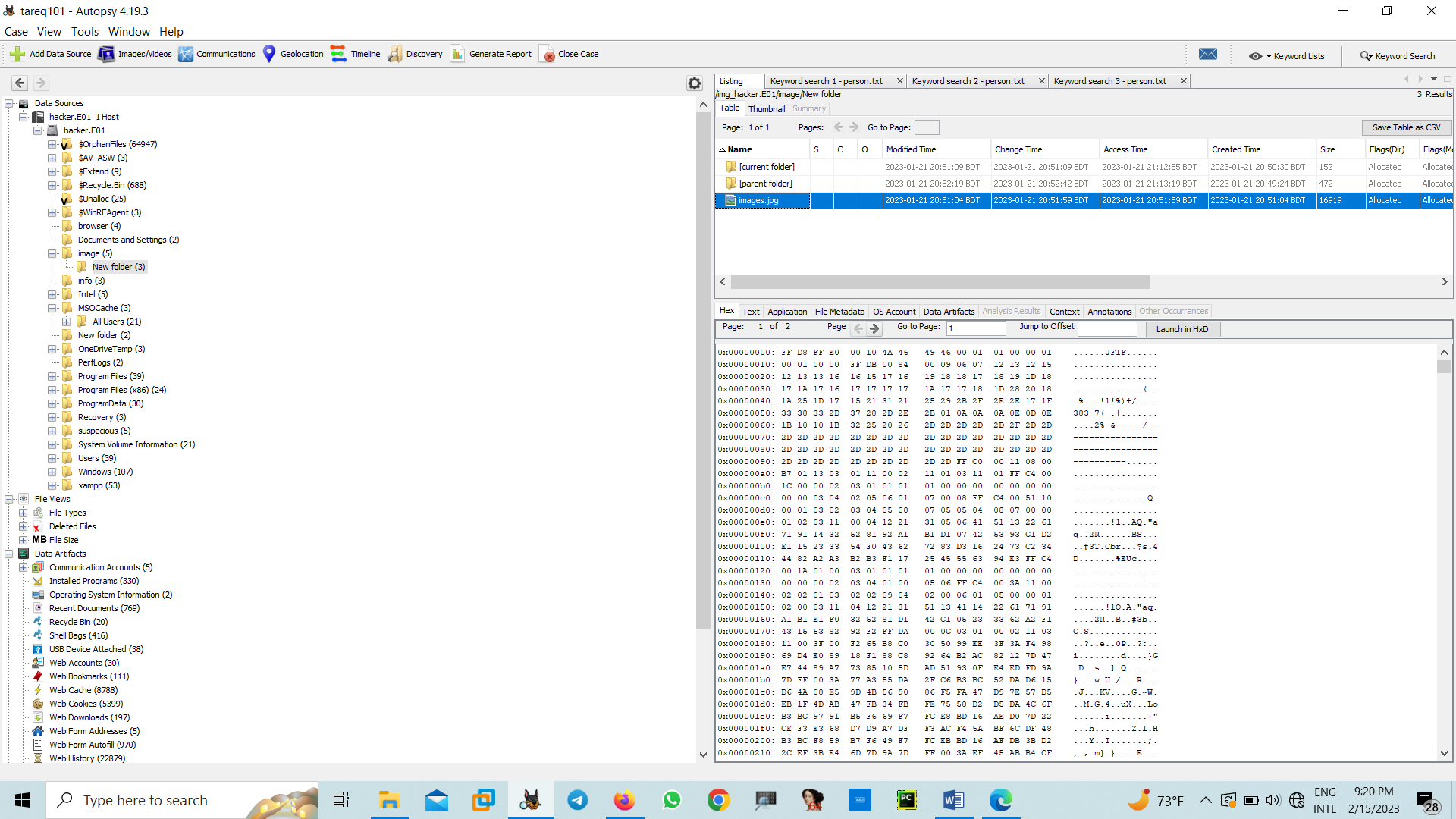
|  |  |
| --- | --- |
| Name: | /img\_hacker.E01/suspecious/man.txt |
| Type: | File System |
| MIME Type: | text/plain |
| Size: | 32 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 2023-01-21 20:53:31 BDT |
| Accessed: | 2023-01-21 21:14:09 BDT |
| Created: | 2023-01-21 20:53:13 BDT |
| Changed: | 2023-01-21 20:53:31 BDT |
| MD5: | Not calculated |
| SHA-256: | Not calculated |
| Hash Lookup Results: | UNKNOWN |
| Internal ID: | 303318 |

Description and implications of the artefact:

man.txt is a text file which has some key word and include three person name bob, jon and henry who are include the crime.

4.3.8 Category DR\_1

Screenshot of the artefact:



A screenshot of artefact evidence details:

**Metadata**

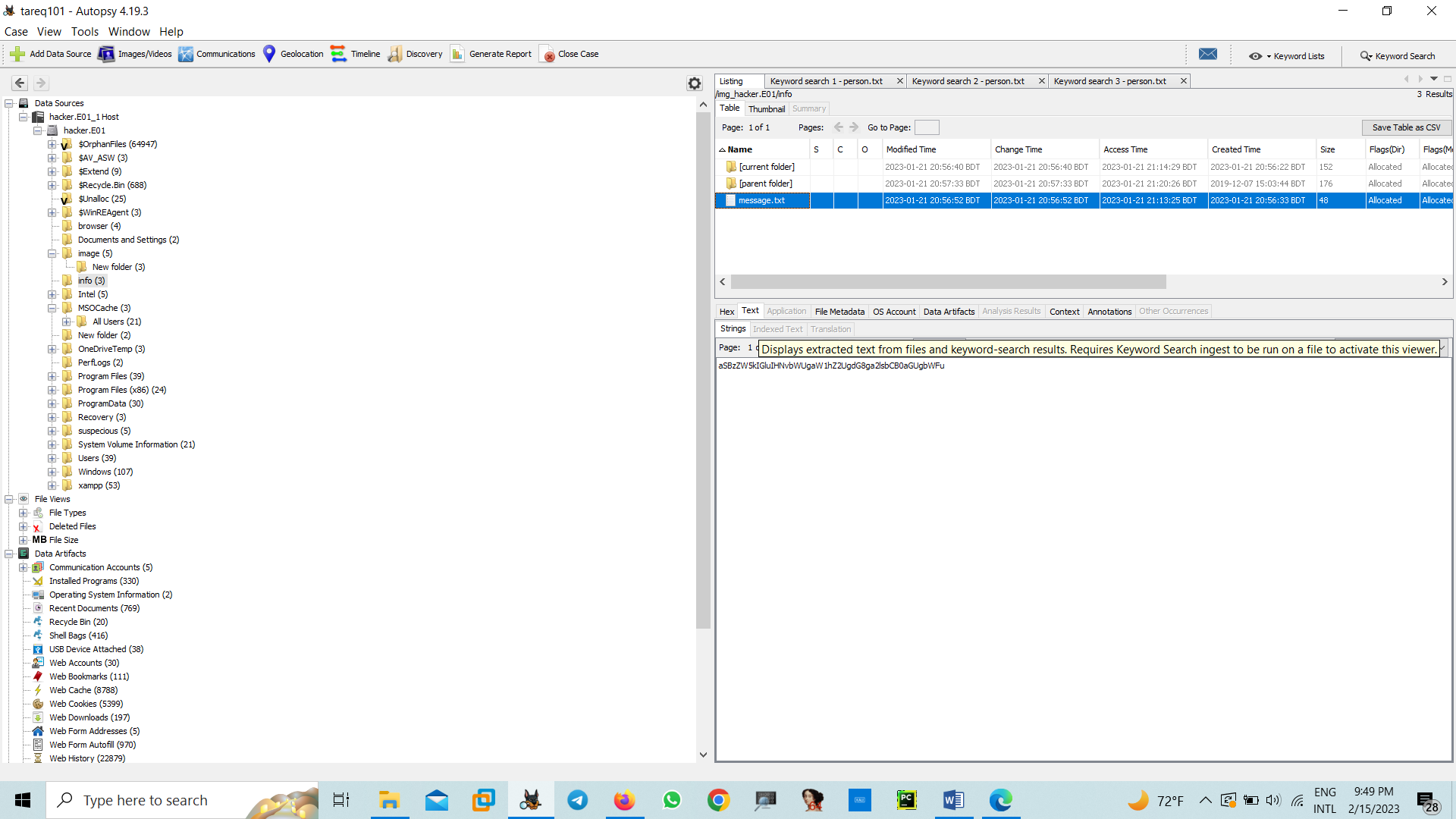
|  |  |
| --- | --- |
| Name: | /img\_hacker.E01/image/New folder/images.jpg |
| Type: | File System |
| MIME Type: | image/jpeg |
| Size: | 16919 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 2023-01-21 20:51:04 BDT |
| Accessed: | 2023-01-21 20:51:59 BDT |
| Created: | 2023-01-21 20:51:04 BDT |
| Changed: | 2023-01-21 20:51:59 BDT |
| MD5: | Not calculated |
| SHA-256: | Not calculated |
| Hash Lookup Results: | UNKNOWN |
| Internal ID: | 219597 |

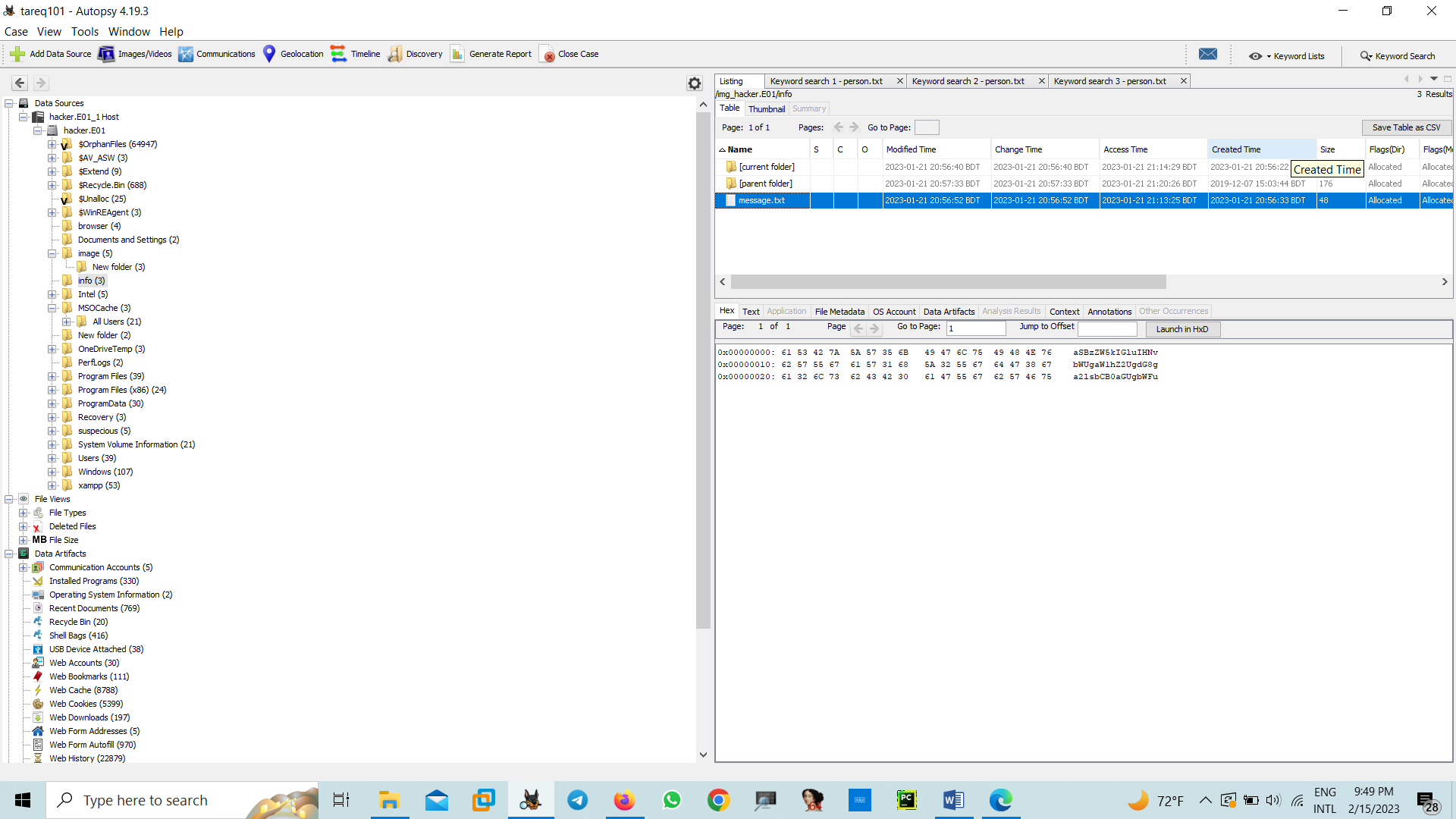
Description and implications of the artefact:

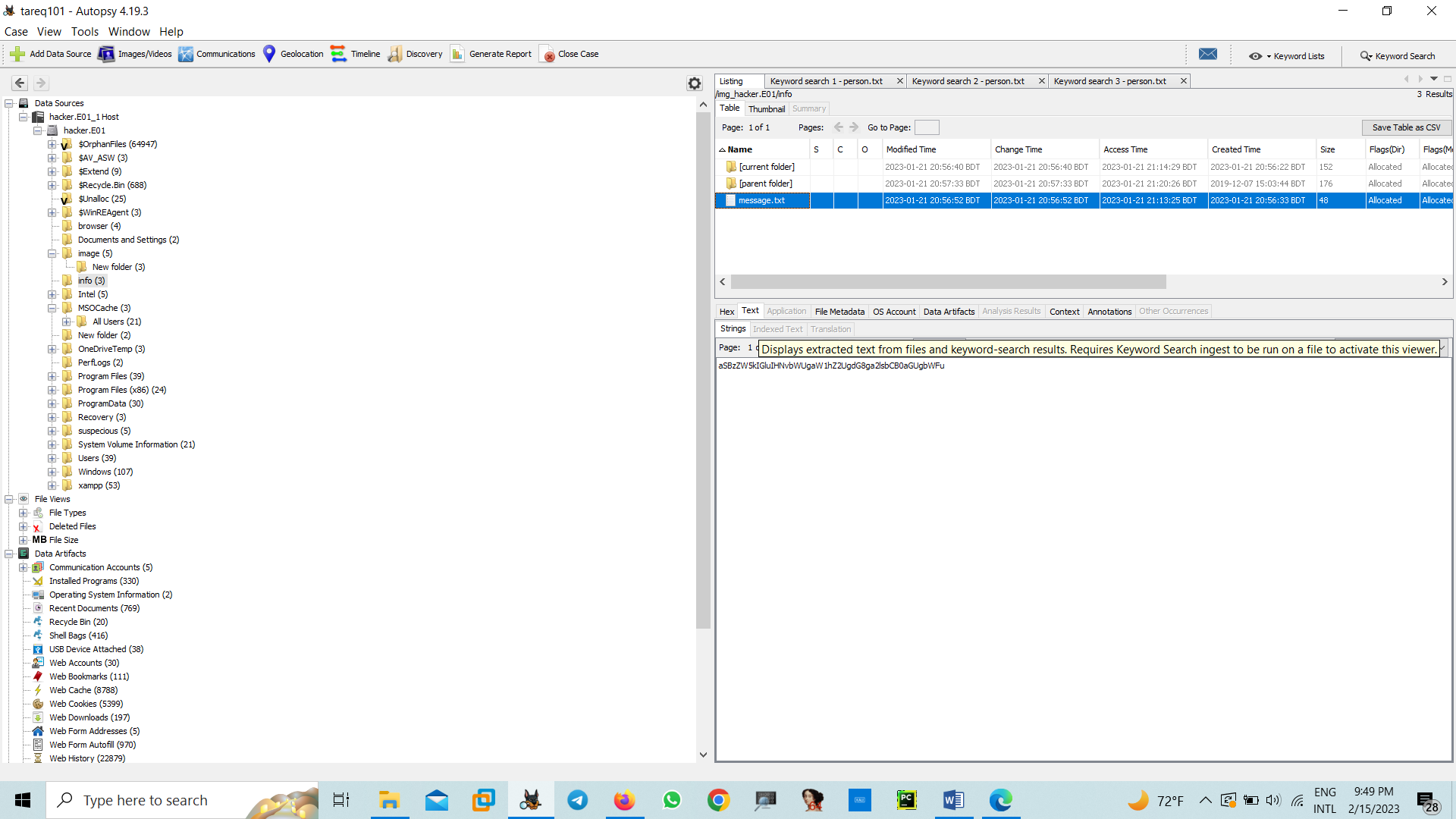
They communicate one mail([hackernishad1015@gmail.com).They](mailto:hackernishad1015@gmail.com).They) sent malicious pdf file and show some violence word.

4.3.9 DHU\_3

Screenshot of the artefact:







A screenshot of artefact evidence details:

**Metadata**

|  |  |
| --- | --- |
| Name: | /img\_hacker.E01/info/message.txt |
| Type: | File System |
| MIME Type: | text/plain |
| Size: | 48 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 2023-01-21 20:56:52 BDT |
| Accessed: | 2023-01-21 21:13:25 BDT |
| Created: | 2023-01-21 20:56:33 BDT |
| Changed: | 2023-01-21 20:56:52 BDT |
| MD5: | Not calculated |
| SHA-256: | Not calculated |
| Hash Lookup Results: | UNKNOWN |
| Internal ID: | 219602 |

Cipher (message.txt) = aSBzZW5kIGluIHNvbWUgaW1hZ2UgdG8ga2lsbCB0aGUgbWFu(base64)

Description and implications of the artefact:

This text file is cipher text. After decode the message we got plain text & hints was killing information. This text proved the killer was the Rahim.

1. Supporting Material Tools:

Autopsy

Access Data FTK Imager

Site:

<https://gchq.github.io/CyberChef/>

1. Personal Reflection
   * 1. Reflection

Digital crime is the most common factors for this time &man can easily the target by the social media.

* + 1. Strengths/major contributions to the group

Completed the full Project criminal activities on Digital Crime Scenario make and Investigation on this.

* + 1. What you found enjoyable

Data Encryption for Data Hiding. Most of cryptography Techniques Like ROT13 and base 32 &base64 and the other section is sign language.

6.1.4 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.