Greenwich Police Hi-Tech Forensics Unit

Operation Archway (2023)

Chisel Chavush *001131628*
Ekrem Said Iz *001141646*
Emir Menekshelı *001084980*

Table of Contents

EXECUTIVE SUMMARY

According to the investigation of the case, JAMES made an unauthorised effort to access a file server. A watch that looks to have an integrated cable was discovered on him during the search conducted at the time of his arrest.

Further investigation into the disk integrated within the watch has revealed that Dr. John Joshua James copied the technical specifications of the underwater drone "TESV Mk1" into his watch drive and concealed it within an image using steganography techniques. Additionally, text files and emails have been found on the disk. The contents of these reveal that Dr. John Joshua James was threatened to obtain the technical information of the drone. It has also been proven that, under the name of the "The Family" group, they arranged for inappropriate children to be given as rewards to their members for successfully completing their tasks. Furthermore, it has been discovered that they shared illegal images of children using steganography techniques, encoding, and encryption storage methods among themselves. There were many cats "inappropriate children" pictures within the disk that had been encrypted, encoded, or their file formats changed to hide them.

During the interview, JAMES claimed that he was not aware that he should not access the file server and only attempted to do so to transfer files to his workstation. However, based on the evidences found during the investigation, it is believed that JAMES had more sinister motives for accessing the file server and attempting to copy technical specification of the defence drone. Addition to that, the investigation also uncovered illegal images of children stored within the disk.

INTRODUCTION

1. At 1800hrs on Friday the 10th of February 2023, DS Aanika AHMED of Greenwich Police Special Branch arrested JAMES on the premises of his employment, Marine Exploration and Defence (Greenwich) Ltd., under suspicion of Section 1 of the Computer Misuse Act (1990).

2. JAMES is alleged to have attempted to access a file server which he did not have legitimate authorisation to do so, and attempted to copy files containing Defence material relating to MOD-related programmes. This activity caused a security alert and detectives from SB were called to attend the scene before he could leave the premises.

3. JAMES was searched at the time of his arrest, and a watch that appears to contain an integrated cable was identified on his person (Exhibit AXA/1).

4. Upon interview JAMES has stated that he was not aware that he should not access the file server and he only tried to do so, so he could transfer files across to his workstation as he needed to work on the files first thing the next day, and he was having problems connecting through the network.

VICTIM AND SUSPECT DETAILS

Victim Details

5. Marine Exploration and Defence (Greenwich) Ltd.

Suspect Details

6. Dr. John Joshua JAMES (DOB: 1/Jan/1995) of Park Row, Greenwich Peninsula, London SE10 9NW. He is a propulsion Engineer for Underwater Autonomous Vehicles.

DETAILS OF EXHIBITS

Exhibit descriptions

7. AXA/1 a Laks branded watch, seized at Marine Exploration and Defence (Greenwich) Ltd. At 1800hrs on 10/Feb/2023 by DS AHMED.

TECHNICAL DETAILS OF THE EXHBITS

Exhibit AXA/1 – File System Details

8. NTFS File system

Exhibit AXA/1 – Operating System Details

9. N.A.

PRESERVATION OF EVIDENCE

Exhibit AXA/1 - Imaging of Original Evidence

```
Created By AccessData® FTK® Imager 4.3.0.18

Case Information:
Acquired using: ADI4.3.0.18
Case Number: Operation Archway
Evidence Number: AXA-1
Unique description: USB Watch
Examiner: AAA
Notes: Live Acquisition no write blocker

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

Information for E:\Op Archway AXA-1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 524,288
[Image]
 Image Type: Raw (dd)
 Source data size: 256 MB
 Sector count:    524288
[Computed Hashes]
 MD5 checksum:    3732822066629c21308c670ad18c3ac5
 SHA1 checksum:   d3f983b4327b67a336baa3251bb8088402b80169

Image Information:
 Acquisition started:   Mon Feb 20 14:00:23 2023
 Acquisition finished:  Mon Feb 20 14:00:24 2023
 Segment list:
  E:\Op Archway AXA-1.E01

Image Verification Results:
 Verification started:  Mon Feb 20 14:00:24 2023
 Verification finished: Mon Feb 20 14:00:25 2023
 MD5 checksum:    3732822066629c21308c670ad18c3ac5 : verified
 SHA1 checksum:   d3f983b4327b67a336baa3251bb8088402b80169 : verified
```

Figure 1: FTK Imager Image Details

Metadata

Name:	/img_Op Archway AXA-1.E01
Type:	E01
Size:	268435456
MD5:	3732822066629c21308c670ad18c3ac5
SHA1:	d3f983b4327b67a336baa3251bb8088402b80169
SHA-256:	Not calculated
Sector Size:	512
Time Zone:	Europe/London
Acquisition Details:	Description: USB Watch
:	Case Number: Operation Archway
:	Evidence Number: AXA-1
:	Examiner Name: AAA
:	Notes: Live Acquisition no write blocker
:	Acquired Date: Mon Feb 20 14:00:23 2023
:	System Date: Mon Feb 20 14:00:23 2023
:	Acquiry Operating System: Win 201x
:	Acquiry Software Version: ADI4.3.0.18
Device ID:	6bc93bdb-d2df-4055-8b83-e9a90addab95
Internal ID:	1
Local Path:	C:\Users\ekrem\Desktop\III\Op Archway AXA-1.E01

Figure 2: Autopsy Image Details

TOOLS USED

AUTOPSY V4.19.3*: Open source digital forensics investigation tool for all types mobile devices and digital media (Basis Technology, n.d.)*.

FTK Imager V4.3.0.18: *Software used for previewing and creating images of electronic data (Exterro, 2021).*

HxD V2.5.0.0*: HxD is a fast and versatile hex editor that supports editing of memory, disks, and files of any size (Hörz, 2003).*

OpenPuff V4.01: *OpenPuff is a steganography and watermarking tool to hide secret messages or file withint other digital media (Embedded SW, 2020).*

CyberChef V9.55.0: *CyberChef is a user-friendly web application for analyzing and decoding data (Government Communications Headquarters of the United Kingdom, 2016)*.

VeraCrypt V1.25.9: *VeraCrypt is an opensource disk encryption tool (IDRIX , 2019)*.

Web Page used:

https://md5.gromweb.com/ →

Date Accessed: 17/03/2023

Detail: A web site that provides md5 hash reverse look up table.

Screenshot:

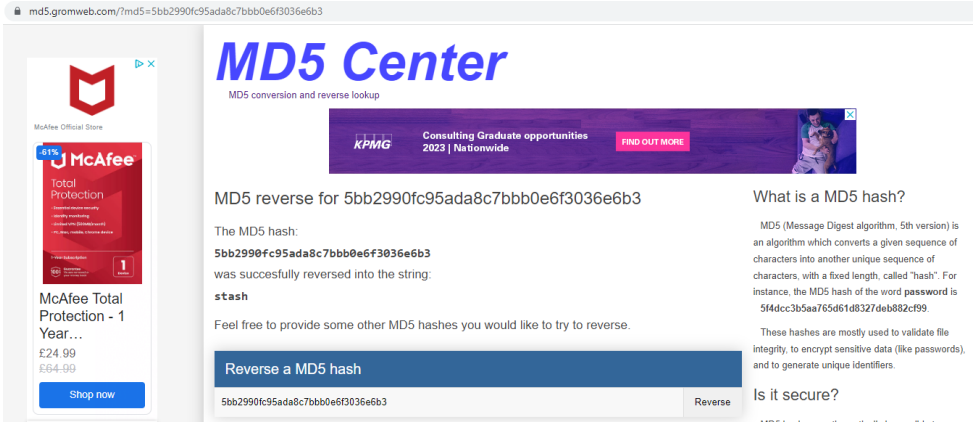


Figure 3:MD5.gromweb

RESULTS AND FINDINGS

Information Artefacts

Information 1: a lovely.txt

The file {a lovely.txt} on path { /img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/a lovely. txt} has been investigated that content of the text file has been saved as hex version of ASCII code (see Figure 4: A lovely.txt (Encrypted) on page 9). After converting the hex characters into ASCII characters, a hidden message was revealed (see Figure 5:A lovely.txt (Decrypted) on page 10).The content of the file is about how the person needs to be carefull about the pictures and specific preferences called “blondtje” and shared that they have couple of sets the blondtje is a reference term for a word blonde and there is an encrypted file called blondtje within the same directory { /img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/}. Also receipent has been warned to keep themselves out of any pictures they take.

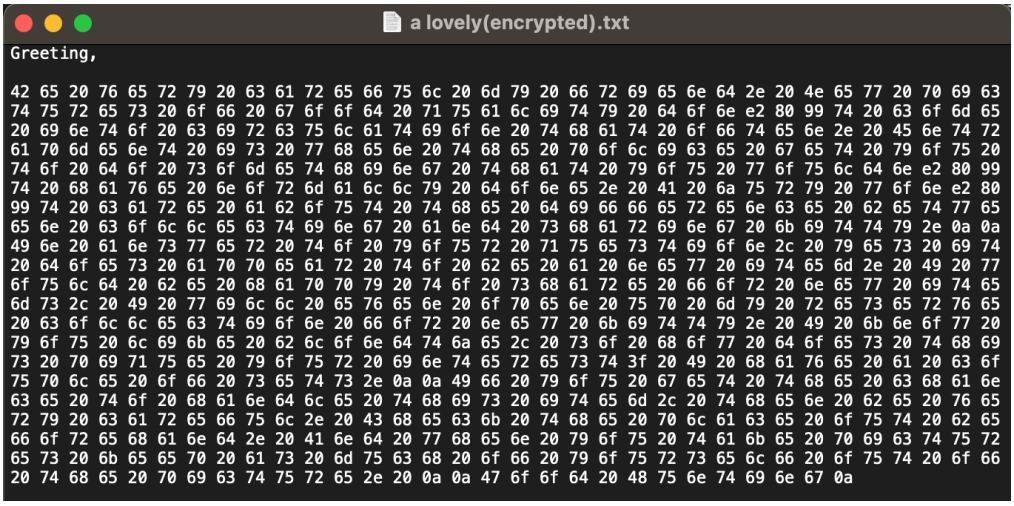


Figure 4: A lovely.txt (Encrypted)

a lovely.txt

Be very careful my friend. New pictures of good quality don't come into circulation that often. Entrapment is when the police get you to do something that you wouldn't have normally done. A jury won't care about the difference between collecting and sharing kitty.

In answer to your question, yes it does appear to be a new item. I would be happy to share for new items, I will even open up my reserve collection for new kitty. I know you like blondtje, so how does this pique your interest? I have a couple of sets.

If you get the chance to handle this item, then be very careful. Check the place out beforehand. And when you take pictures keep as much of yourself out of the picture.

Good Hunting

Figure 5:A lovely.txt (Decrypted)

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/a lovely.txt
Type:	File System
MIME Type:	text/plain
Size:	2139
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-05 03:00:00 GMT
Accessed:	2023-02-05 03:00:00 GMT
Created:	2023-02-05 03:00:00 GMT
Changed:	2023-01-21 11:05:35 GMT
MD5:	02ed349f37c44dce3b7fad82975036b6
SHA-256:	f65b551fd01cbf47f8ddf056e71a61fc25c891bfd215d321eb7519879844ea4c
Hash Lookup Results:	UNKNOWN
Internal ID:	212

Figure 6: Metadata of a lovely.txt

INFORMATION 2: draft.txt

The file {draft.txt} on path {/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/draft. txt} has been investigated that content of the text file has been saved as hex version of ASCII characters where it starts with “Hello old friend,” (see Figure 7:draft.txt Encrypted on page 11). The message has been decrypted by converting hex values into ASCII characters (see Figure 8:draft.txt Decrypted on page 12).

When content of the file has been decrypted, the message was saying that picture has been send by associate. The sender was claiming that full access to that picture has been offered. The sender acknowledges that it may sound like a setup, but they don't think it involves law enforcement, as it would be a serious entrapment case if it was. The sender is seeking the recipient's opinion on whether the picture is new in the market, as they consider the recipient to have a better collection. They offer to swap a higher-resolution version of the picture for one of the recipient's candid photos, but they first want the recipient's opinion based on the low-resolution version they've shared. The sender concludes the message by mentioning that it has been a weird day.

draft(encrypted).txt

```
Hello old friend,

49 e2 80 99 76 65 20 62 65 65 6e 20 73 65 6e 74 20 74 68 69 73 20 70 69 63 74 75 72 65 20 62 79 20 61
6e 20 61 73 73 6f 63 69 61 74 65 2e 20 49 74 20 6c 6f 6f 6b 73 20 67 65 6e 75 69 6e 65 2e 20 49 e2 80
99 76 65 20 6e 65 76 65 72 20 73 65 65 6e 20 69 74 20 62 65 66 6f 72 65 20 61 6e 64 20 49 e2 80 99 76
65 20 62 65 65 6e 20 6f 66 66 65 72 65 64 20 61 63 63 65 73 73 20 74 6f 20 69 74 20 61 73 20 77 65 6c
6c 2e 20 43 61 6e 20 79 6f 75 20 62 65 6c 69 65 76 65 20 74 68 61 74 3f 0a 49 20 6b 6e 6f 77 20 77 68
61 74 20 79 6f 75 20 61 72 65 20 67 6f 69 6e 67 20 74 6f 20 73 61 79 3a 20 49 74 20 73 6f 75 6e 64 73
20 6c 69 6b 65 20 61 20 73 65 74 2d 75 70 20 49 20 6b 6e 6f 77 2c 20 62 75 74 20 49 20 68 61 76 65 20
72 65 61 73 6f 6e 20 74 6f 20 62 65 6c 69 65 76 65 20 69 74 73 20 6e 6f 74 20 74 68 65 20 63 6f 70 73
2e 20 49 74 20 77 6f 75 6c 64 20 62 65 20 61 20 73 65 72 69 6f 75 73 20 65 6e 74 72 61 70 6d 65 6e 74
20 69 66 20 69 74 20 77 61 73 2c 20 62 65 6c 69 65 76 65 20 6d 65 2e 0a 59 6f 75 20 68 61 76 65 20 61
20 6d 75 63 68 20 62 65 74 74 65 72 20 63 6f 6c 6c 65 63 74 69 6f 6e 20 74 68 61 74 20 49 20 68 61 76
65 2e 20 49 20 63 61 6e 20 73 77 61 70 20 74 68 65 20 68 69 67 68 65 72 20 72 65 73 20 76 65 72 73 69
6f 6e 20 66 6f 72 20 6f 6e 65 20 6f 66 20 79 6f 75 72 20 63 61 6e 64 69 64 73 2c 20 49 20 6a 75 73 74
20 77 61 6e 74 65 64 20 79 6f 75 72 20 6f 70 69 6e 69 6f 6e 20 66 72 6f 6d 20 74 68 69 73 20 6c 6f 77
20 72 65 73 2c 20 69 66 20 69 74 20 69 73 20 61 20 6e 65 77 20 6f 6e 65 20 6f 6e 20 74 68 65 20 6d 61
72 6b 65 74 3f 20 0a 49 74 20 68 61 73 20 62 65 65 6e 20 61 20 77 65 69 72 64 20 64 61 79 2e 0a
```

Figure 7:draft.txt Encrypted

draft.txt

I've been sent this picture by an associate. It looks genuine. I've never seen it before and I've been offered access to it as well. Can you believe that?
I know what you are going to say: It sounds like a set-up I know, but I have reason to believe its not the cops. It would be a serious entrapment if it was, believe me.
You have a much better collection that I have. I can swap the higher res version for one of your candids, I just wanted your opinion from this low res, if it is a new one on the market?
It has been a weird day.

Figure 8:draft.txt Decrypted

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/draft.txt
Type:	File System
MIME Type:	text/plain
Size:	1646
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-04 13:00:00 GMT
Accessed:	2023-02-04 13:00:00 GMT
Created:	2023-02-04 13:00:00 GMT
Changed:	2023-01-21 11:04:42 GMT
MD5:	92c67cfd4763b2efc5d317bc23feeead
SHA-256:	9075018e271cd05b63ba2f801da316917cb300213b6227229ce1b4cd19c60bfa
Hash Lookup Results:	UNKNOWN
Internal ID:	216

Figure 9:Metadata of draft.txt

INFORMATION 3: UNALLOCATED DISK SPACE E-MAILS

Within the unallocated disk space (the disk space that is free to use to fill in with other files, this space might have some deleted files' left behinds) on path {/img_Op Archway AXA-1.E01/vol_vol2//$Unalloc/Unalloc_8_8421376_265351168}, it has been investigated that three emails left behind in this disk space (see

Figure 10:Unallocated disk sapce E-mails on page 13). The emails were between the person called Lucian(speaker-of-thedb@gmail.com) and JJ(tripplejay@protonmail.com). Most likely the triplejay being Dr. John Joshua JAMES. The conversation was about the person called JJ was forced to steal technical details of the engine on the TESTV. "JJ" emailed about that he wanted to get out of the situation and Lucian replied back with they will take him out of the situation no matter what.

On Thur, 9 Feb 2023 at 20:45, Lucian <speaker-of-thedb@gmail.com> wrote:
Brother,
We will take you out of the situation, one way or the other.
Collect the files and let us know when you have them. They will be too big for Open Puff.
The Family
On Thur, 9 Feb 2023 at 20:30, JJ <tripplejay@protonmail.com> wrote:
You can drop the act, brother, I just need to get out of this situation.
What you are asking means I have to go onto the primary file server. Just getting a chance to be alone with that is non-trivial!
On Thur, 9 Feb 2023 at 19:00, Lucian <speaker-of-thedb@gmail.com> wrote:
Brother,
We have need of your services again.
We need precise technical details of the engine on the TESV. Power levels. Especially noise of operation and the noise made when they are being vectored.
We enclose a picture to remind you of what awaits when you complete this task.
The Family

Figure 10:Unallocated disk sapce E-mails

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2//$Unalloc/Unalloc_8_8421376_265351168
Type:	Unallocated Blocks
MIME Type:	application/octet-stream
Size:	85327872
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	9

Figure 11:Metadata of "unallocated"

INFORMATION 4: <u>UNALLOCATED DISK SPACE Getty Images(website)</u>

Within the unallocated disk space {Unalloc_8_8421376_265351168} on path {/img_Op Archway AXA-1.E01/vol_vol2//$Unalloc/Unalloc_8_8421376_265351168} an information about a picture has been found (see Figure 12:Photo by Werner Layer via Getty Images on page 14). This picture was edited by Adobe Photoshop in windows 2019 operating system. As Adobe tagged in its metadata, it was indicated that the picture has been gotten from the "Getty Images" global stock photography and editorial image service. There was an identification number of the picture (see Figure 13: Identification number on page 14). After doing the reverse engineering on the "Getty Images" website with the identification number (862755394) found, a Siamese cat with a seal-point coloring taken by Werner Layer and published by Gamma-Rapho picture has been found (see Figure 14:Siamese cat on page 15).

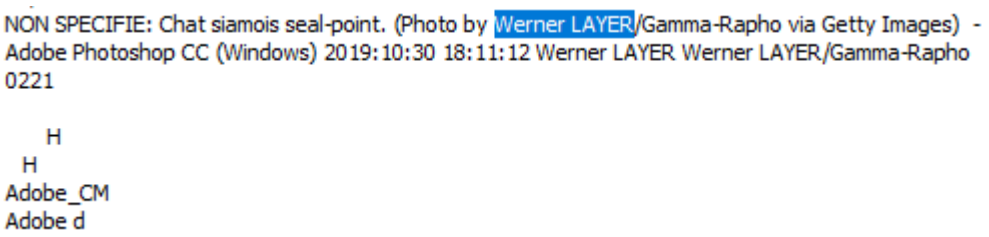


Figure 12:Photo by Werner Layer via Getty Images

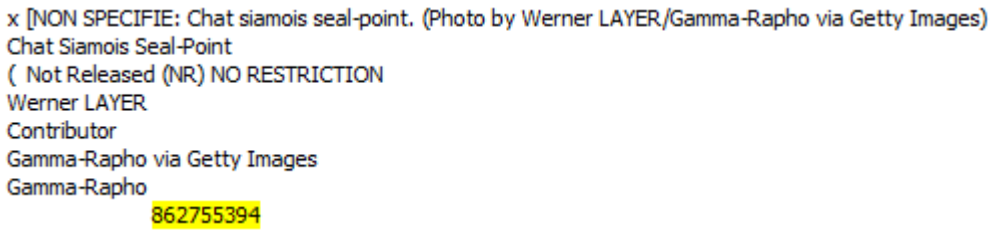


Figure 13: Identification number

Figure 14:Siamese cat

DETAILS

Restrictions:	Contact your local office for all commercial or promotional uses.NO RESTRICTION
Credit:	Werner LAYER / Contributor
Editorial #:	862755394
Collection:	Gamma-Rapho
Date created:	01 January, 1900
Licence type:	Rights-managed
Release info:	Not released. More information
Source:	Gamma-Rapho
Object name:	gamma_jka001011.jpg
Max file size:	4843 x 3528 px (41.00 x 29.87 cm) - 300 dpi - 9 MB

Figure 15: Picture Details

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2//$Unalloc/Unalloc_8_8421376_265351168
Type:	Unallocated Blocks
MIME Type:	application/octet-stream
Size:	85327872
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	9

Figure 16: Unallocated disk space Metadata

Document Artefacts

DOCUMENT 1: <u>For The Personal Attention of Dr.James.zip</u>

The zip file called { For The Personal Attention of Dr.James.zip } in path {/img_Op Archway AXA-1.E01/vol_vol2/Personal/} had two files. A text file {InnocenceMyBrother.txt}(see Figure 17:InnocenceMyBrother.txt on page 17) and a jpg file {WeKnow.jpg}(see Figure 18:WeKnow.jpg on page 17). After investigating the {InnocenceMyBrother.txt }, the person is asked to get technical specifications for the TESV Mk1 and there was a password given within the file “InnocenceMyBrother” to use in OpenPuff steganography application. Using the password in OpenPuff for {WeKnow.jpg} (see Figure 19:OpenPuff output for "WeKnow.jpg" on page 18), a hidden text file called {A Blade of Woe.txt}(see Figure 20:A Blade of Woe.txt on page 18) has been found. In the file there was a phrase saying that they know {Dr. John Joshua JAMES} address and they mention that they believe in him to do the task.

InnocenceMyBrother.txt

```
You like playing games. Then you know what this means. From now on you will need the password
InnocenceMyBrother.

We know, you think “it can’t hurt anyone” or maybe you are thinking that if you look at those
pictures, then you are stopping yourself from hurting someone.

We don’t care. But we do know.

We know you’d never survive in prison. We know that everyone you know will turn their backs on you.
All you have worked for, your degrees, everything, will be taken away from you.

We know.

You are thinking you can wipe your computer. Or you can throw it in the Thames.
It is too late. We know.

Send us the technical specifications for the TESV Mk1. You will encode it using Open Puff and use the
same password we have given you here.

You can email back only once, or everyone will know.

The Family
```

Figure 17:InnocenceMyBrother.txt

Figure 18:WeKnow.jpg

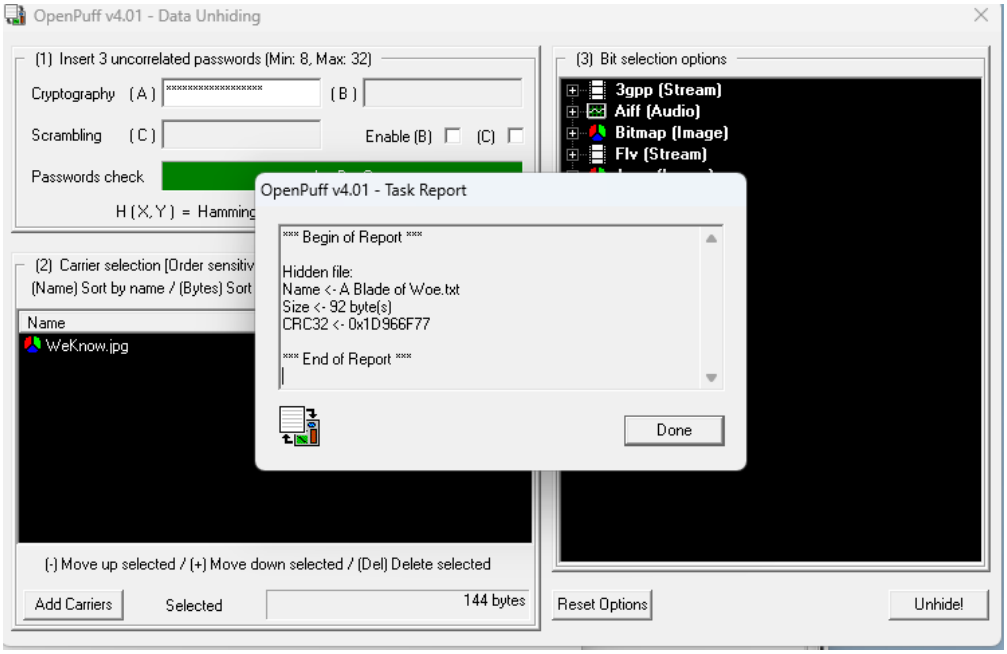


Figure 19:OpenPuff output for "WeKnow.jpg"

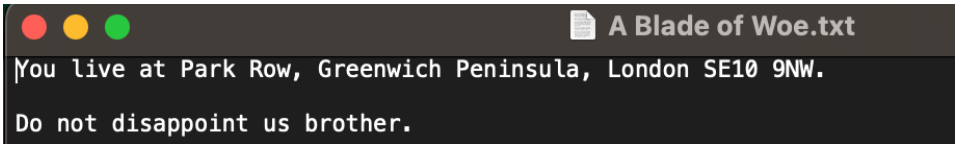


Figure 20:A Blade of Woe.txt

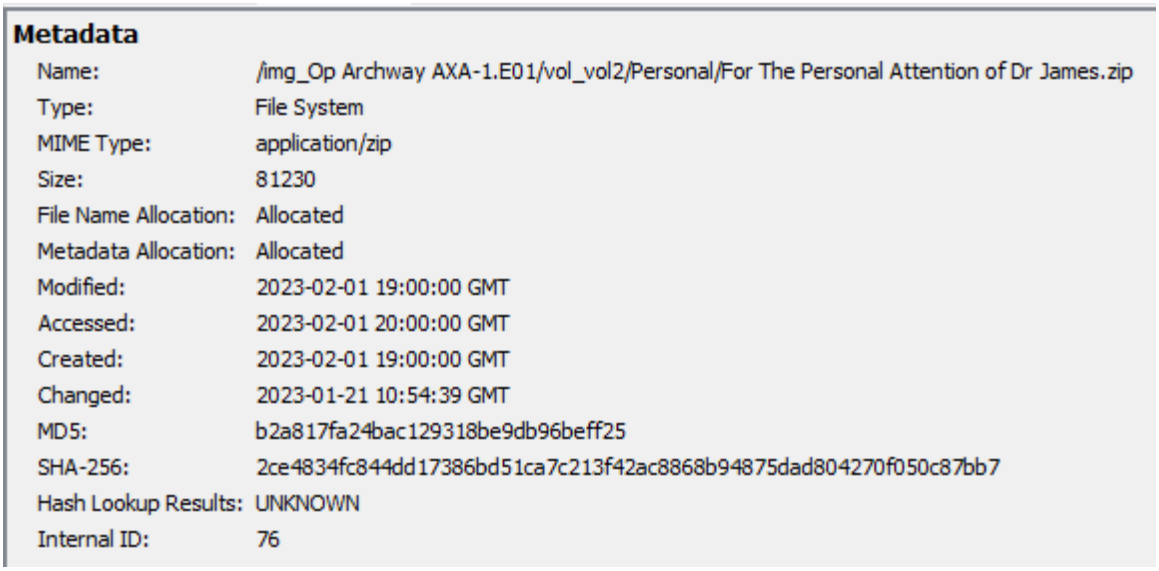


Figure 21:Metadata of For The Personal Attention of Dr James.zip

DOCUMENT 2: whatisthelife'sgreatestillusion-mkv1.txt

The file {sithis.bmp} on path {/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Sithis.bmp} has the same hand figure that was indicating a file could be hidden by using the steganography technic with openpuff (see Figure 22:sithis.bmp on page 19). After using the same password "InnocenceMyBrother" a hidden text file {TESV Mk1.txt} is obtained. the text file consists of the technical specifications for the TESV Mk1 (see Figure 24:TESV Mk1.txt Technical Spesificationson page 20).

Figure 22:sithis.bmp

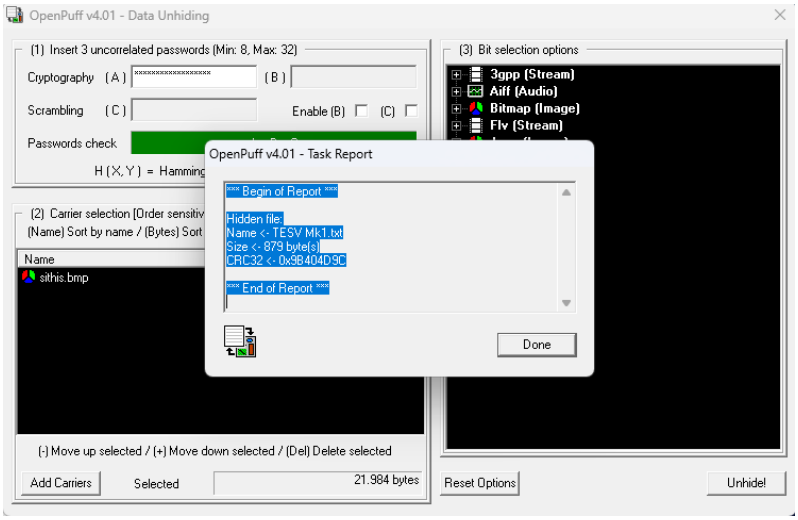


Figure 23: OpenPuff "sithis.bmp"

TESV Mk1.txt

```
TECHNICAL SPECIFICATIONS UNDERWATER DRONE

Hull design Hydrodynamic and hydrobalanced hull
for stability and performance in ocean
conditions. Ruggedized exterior for im-
pact resistance.

Pressure rating         150m.

Weight  8,6 kg.
Speed   1.5 m/s (3 knots).
Boost mode for efficiency.
Slow mode for precision.

Run-time        hours normal operation.

Thrusters       powerful thrusters (350 W on each).
rear, 1 vertical center, 1 lateral.
User replaceable.

Automation      Auto heading. Auto depth.

Camera  Light sensitive Full HD 1080p 25/30 fps, wide angle lens.

Search light    Powerful 3300 lumen LED below camera. Fittings for extra lights as payload.

Sensors
Accelerometer.
Gyroscope.
Magnetometer.
Water temperature.
Depth.
Internal pressure.

Payload         Standard fittings for payload on both top and bottom side of drone.
```

Figure 24:TESV Mk1.txt Technical Spesifications

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/sithis.bmp
Type:	File System
MIME Type:	image/bmp
Size:	2764854
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-03 21:00:00 GMT
Accessed:	2023-02-03 23:00:00 GMT
Created:	2023-02-03 21:00:00 GMT
Changed:	2023-01-21 11:01:35 GMT
MD5:	9652d178f689e9963529d1bb02f38c6e
SHA-256:	3b68a7f4679253e4543ee4cc768f0aa78054948030766abd6ebca8e322052da7
Hash Lookup Results:	UNKNOWN
Internal ID:	224

Figure 25:Metadata of sithis

DOCUMENT 3: KITTY LOVERS

The file {K____Lovers Rules.jpg} on path {/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/backups/K__ Lovers Rules.jpg} has been investigated that the actual file extension is not a jpg but a Microsoft Word file (docx). After changing the file extension to ".docx" the Microsoft Word file (see Figure 27: Hidden text. on page 21) has been found. There are some hidden texts within the file. The text has been changed to windings format (see Figure 26 : Wingdings on page 21). There is also a hidden text that the colour of the text was changed to background colour and it was a tiny size. After revealing the hidden texts the final word document looking like (see Figure 28: K____Lovers Rules.docx on page 22). The content of the file is talking about the how to encrypt the files or how the group members encrypt their own files. The term "kitty" has been used to tell if they don't follow the rules they will not provide kitties anymore. The text is in windings format means "kitty".
Additionally, in the text it was mentioned that some of the files are encrypted by using Vigenère encryption technique with key "kittylovers" and the file format has been changed to base64. This is going to be a hint for other encrypted files.

Figure 26 : Wingdings

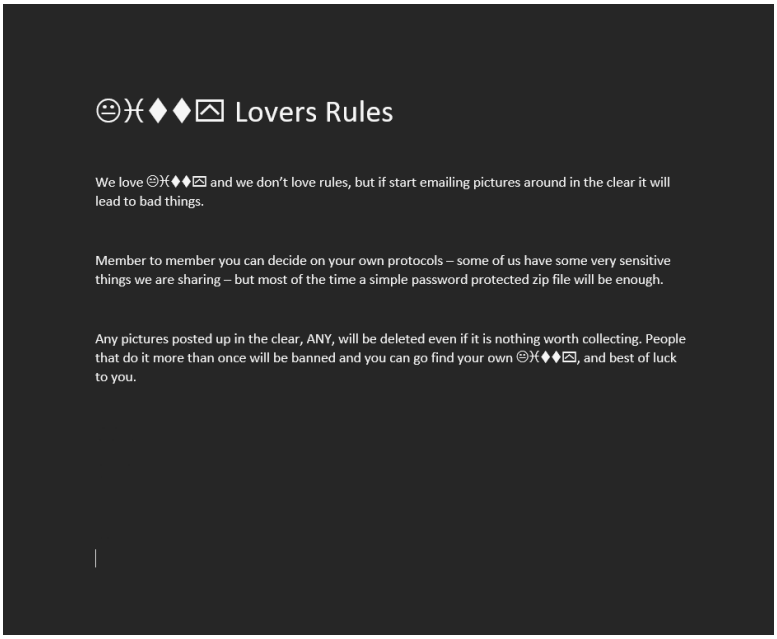
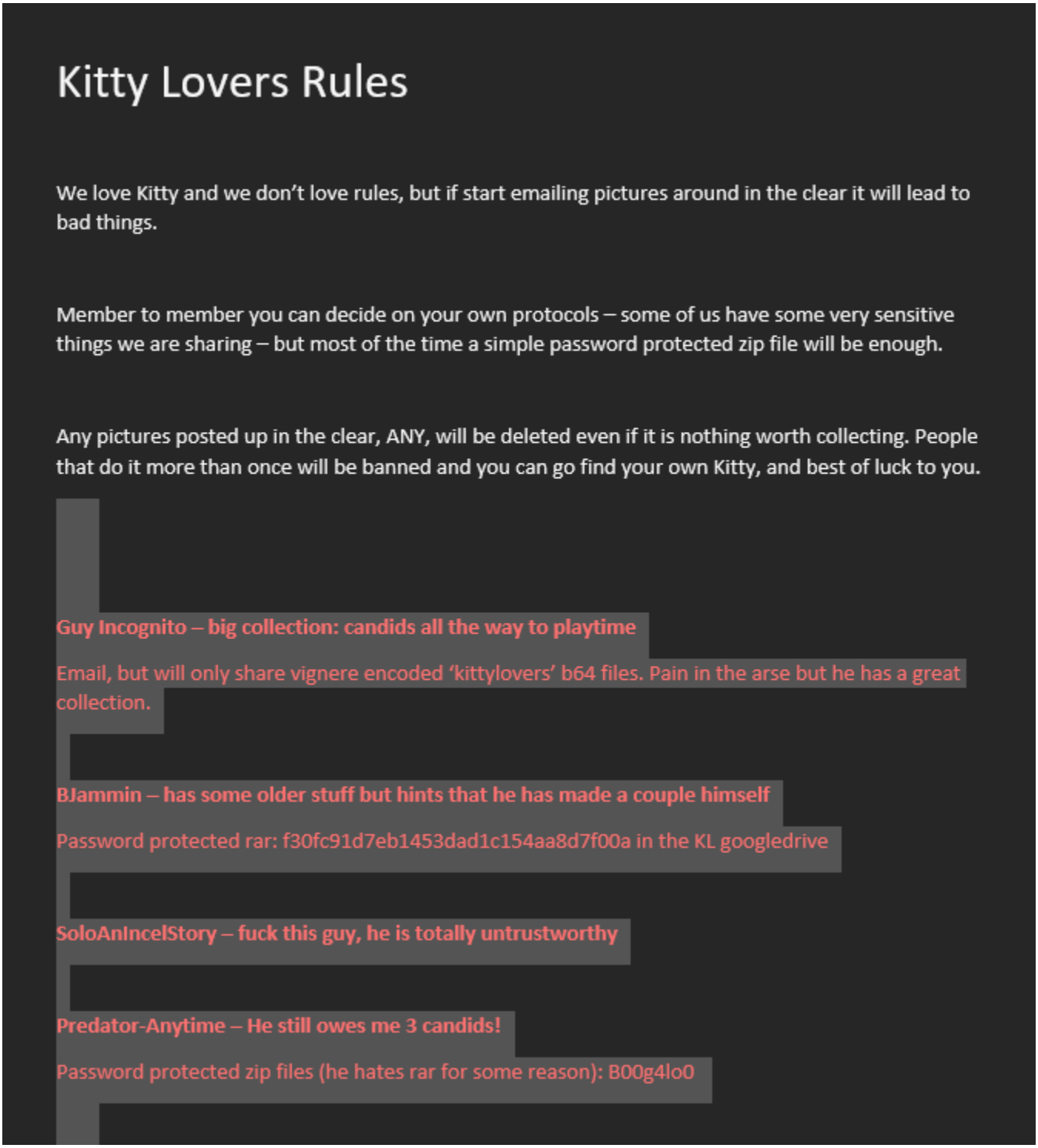


Figure 27: Hidden text.



Kitty Lovers Rules

We love Kitty and we don't love rules, but if start emailing pictures around in the clear it will lead to bad things.

Member to member you can decide on your own protocols – some of us have some very sensitive things we are sharing – but most of the time a simple password protected zip file will be enough.

Any pictures posted up in the clear, ANY, will be deleted even if it is nothing worth collecting. People that do it more than once will be banned and you can go find your own Kitty, and best of luck to you.

Guy Incognito – big collection: candids all the way to playtime

Email, but will only share vignere encoded 'kittylovers' b64 files. Pain in the arse but he has a great collection.

BJammin – has some older stuff but hints that he has made a couple himself

Password protected rar: f30fc91d7eb1453dad1c154aa8d7f00a in the KL googledrive

SoloAnIncelStory – fuck this guy, he is totally untrustworthy

Predator-Anytime – He still owes me 3 candids!

Password protected zip files (he hates rar for some reason): B00g4lo0

Figure 28: K____Lovers Rules.docx

Picture Artefacts

Picture 1: Would you like intoduction my brother.jpg

{Would you like to introduction my brother.jpg} on path {limg_Op Archway AXA 1.E01/vol_vol2/Personal/In Deep/Would you like an introduction my brother.jpg} was a broken jpg file. After investigating the file, the first 32 bytes of the file header was broken (zeroed) (see; Figure 30:Broken Header Hex, Would you like introduction my Brother(Hex) on page 24). This was fixed by using HxD and a picture of a cat (see Figure 29:Would you like intoduction my brother.jpg on page 23) found.

The other file within the same directory { /img_Op Archway AXA-1.E01/vol_vol2/Personal/In Deep / } was { OpenTheDoorMyBrother.bmp }. Using the openpuff on this file with the same password "InnocenceMyBrother", a hidden text file {Excellent Work.txt} is obtained. In this text file, there is a reference attached saying that if the person does what has been asked, the reward will be the picture of the cat that has been found.

Figure 29:Would you like intoduction my brother.jpg

```
0x00000000: 00 00 00 00  00 10 4A 46   49 46 00 01  01 00 00 01    ......JFIF......
0x00000010: 00 01 00 00  FF DB 00 43   00 06 04 05  06 05 04 06    .......C........
0x00000020: 06 05 06 07  07 06 08 0A   10 0A 0A 09  09 0A 14 0E    ................
0x00000030: 0F 0C 10 17  14 18 18 17   14 16 16 1A  1D 25 1F 1A    .............%..
0x00000040: 1B 23 1C 16  16 20 2C 20   23 26 27 29  2A 29 19 1F    .#... , #&')*)..
```

Figure 30:Broken Header Hex, Would you like introduction my Brother(Hex)

FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿàNULDLEJFIFNULSOH	0	jpg jpeg
FF D8 FF EE	ÿØÿî		

Figure 31: Expected Hex

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Personal/In Deep/Would you like an introduction my brother.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	120060
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-03 22:00:00 GMT
Accessed:	2023-02-04 13:00:00 GMT
Created:	2023-02-03 22:00:00 GMT
Changed:	2023-01-21 11:03:20 GMT
MD5:	175a0448f1c6af6ba772a3ffd6042d70
SHA-256:	e6d5363724ed97b2497066549050885a4aa7012f3b57c75cf14ea03516e14760
Hash Lookup Results:	UNKNOWN
Internal ID:	98

Figure 32:Meta Data of Would you like an introduction my brother.jpg

Figure 33:OpenTheDoorMyBrother.bmp

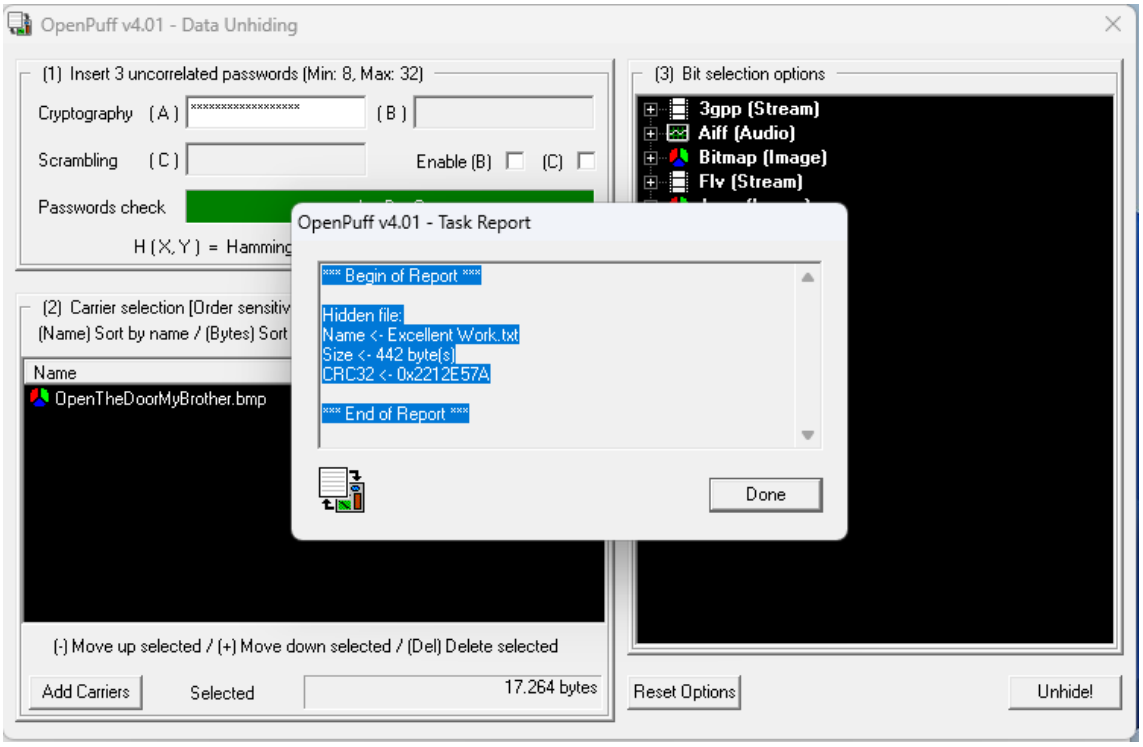


Figure 34: OpenPuff "OpenTheDoorMyBrother" file.

Excellent Work.txt — Edited

```
Well done my brother.

You did as you were commanded, and you did it well.

Do not misunderstand us, we do not judge you for your dark urges. We are beyond that now you are one
of us. We enclose a small reward, the promise of more if you complete more of our tasks.

We know you your prefer blonde, but we have this one available for you to play with if you continue
to provide us with what our Mother requires from us.

The Family
```

Figure 35:Excellent Work.txt

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Personal/In Deep/OpenTheDoorMyBrother.bmp
Type:	File System
MIME Type:	image/bmp
Size:	1552374
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-03 22:00:00 GMT
Accessed:	2023-02-04 13:00:00 GMT
Created:	2023-02-03 22:00:00 GMT
Changed:	2023-01-21 11:03:20 GMT
MD5:	6f55209acd2c42c2f77ff76b476ec18b
SHA-256:	e22f4b4cbd13b664c7e75fe287c1e32cf26dd8fb7830cbc9cb88f323668b9ba9
Hash Lookup Results:	UNKNOWN
Internal ID:	96

Figure 36:Metadata of "Excellent Work"

Picture 2: BLONDTJE

The file {blondtje.txt} on path {/limg_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/blondtje. Txt} has been investigated and found that the text file has been encrypted with Vigenère encryption technique (see Figure 37: blondtje.txt (Encrypted) on page 27). After decrypting the file with the key “kittylovers” that has been found on section (Document 3 on page 21) by using CyberChef, it has been determined that the file was transformed into base64 format. Changing the format back to its original form from base64 again with CyberChef has given that the file is actually a jpeg. Therefore, the extension of the file has also been changed and the blonde cat picture has been found (see Figure 38: blondtje.jpeg (Decrypted) on page 27).

Figure 37: blondtje.txt (Encrypted)

Figure 38: blondtje.jpeg (Decrypted)

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/blondtje.txt
Type:	File System
MIME Type:	text/plain
Size:	79636
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-05 03:00:00 GMT
Accessed:	2023-02-05 03:00:00 GMT
Created:	2023-02-05 03:00:00 GMT
Changed:	2023-01-21 11:05:35 GMT
MD5:	a2823b737a0a783bfe947269d3747e05
SHA-256:	ce2fc79be4674dd86e86ada6d665c0b36c6a9dcccc5c41bf73d8503013daf98d
Hash Lookup Results:	UNKNOWN
Internal ID:	214

Figure 39: Metadata of blondtje.txt

Picture 3: SEND FILE

The file {send.data} on path {/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/send.data } has been investigated that the the file with ".data" is encrypted by Vigenère encryption with key "kittylovers" that has been found on section (Document 3 on page 21) and encoded with base 64 format. After decrypting and decoding the file by using the tool called CyberChef, it has been found that the original file is a jpeg file. Changing the extension back to its original format has given a cat picture (see Figure 40: send.jpeg on page 28).

Figure 40: send.jpeg

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/send.data
Type:	File System
MIME Type:	text/plain
Size:	27212
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-04 13:00:00 GMT
Accessed:	2023-02-04 13:00:00 GMT
Created:	2023-02-04 13:00:00 GMT
Changed:	2023-01-21 11:04:42 GMT
MD5:	b08fc577c507c3de838513456ac6f258
SHA-256:	2f7deba094c091f1cfe3c8d95d605e6beadd2c60d250b14d8940c685b131190b
Hash Lookup Results:	UNKNOWN
Internal ID:	218

Figure 41:Metadata of send.data

Picture 4:STEP 1 FILE

The file {step1.txt} on path {/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/step1.txt} has been investigated that the format of the file has been changed to base64. Using the Cyber Chef the format has been changed to its original. It has been seen that the original data is a ".jpeg" file. However, it has been saved as a ".txt" file. After changing the extension to ".jpeg" a blonde cat picture is found.

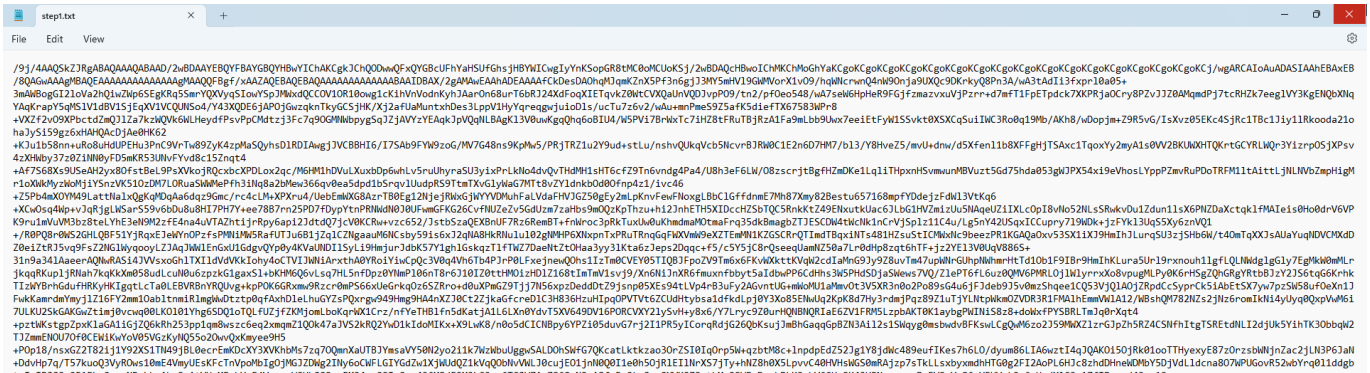


Figure 42: step1.txt (base64 encoded)

Figure 43: step1.jpeg

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/step1.txt
Type:	File System
MIME Type:	text/plain
Size:	79636
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-05 03:00:00 GMT
Accessed:	2023-02-05 03:00:00 GMT
Created:	2023-02-05 03:00:00 GMT
Changed:	2023-01-21 11:05:35 GMT
MD5:	0fc98cfdc552f9d4b64e931c42c25de0
SHA-256:	ea0e796f7d7be31e0e813a67df2c15d350692242f94e9fb15325c4fb7f56de51
Hash Lookup Results:	UNKNOWN
Internal ID:	220

Figure 44: Metadata of step1.txt

Picture 5:STEP 2 FILE

The file {step2.txt} on path { /img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/step2.txt } has been investigated that the text file has been saved as txt but the metadata shows the extension as jpeg. So this file was actually a jpeg file but it has been saved as txt. This picture contains indecent picture of a child (blonde cat).

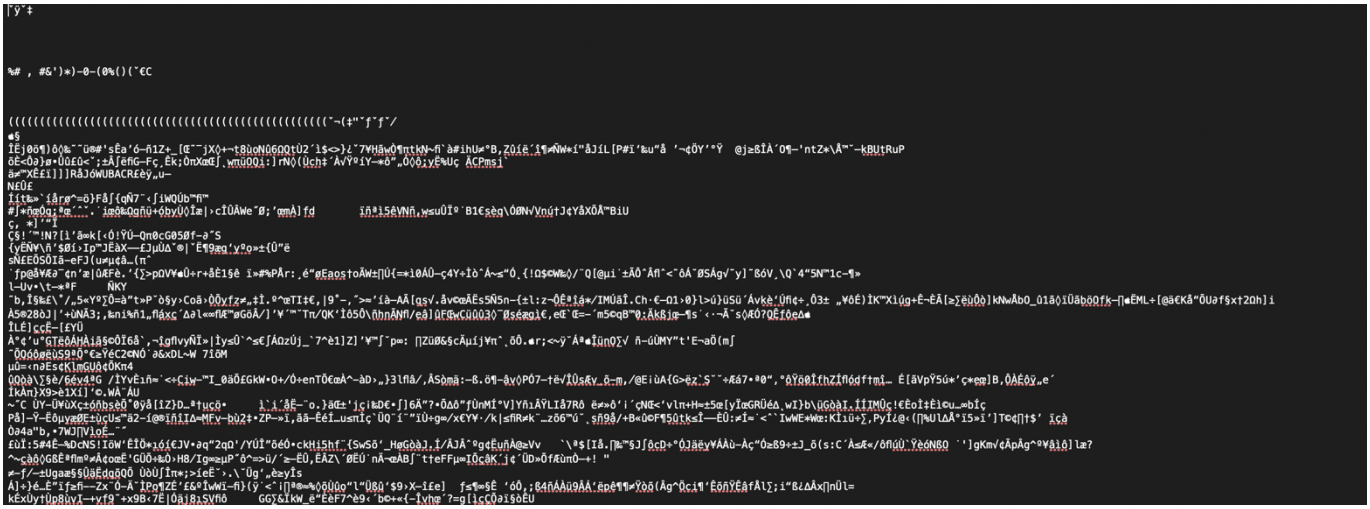
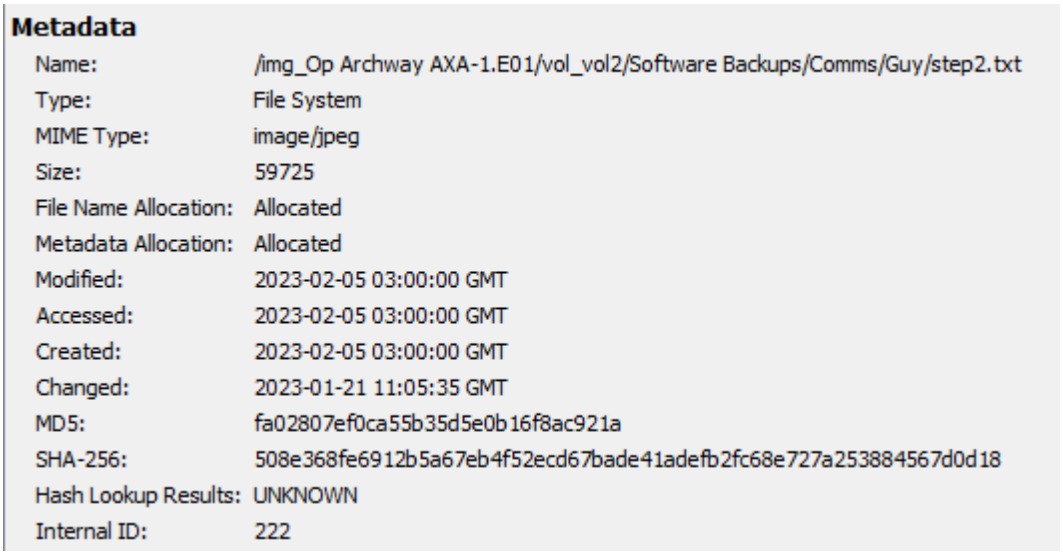


Figure 45:step2.txt

Figure 46:step2.jpeg



Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/Comms/Guy/step2.txt
Type:	File System
MIME Type:	image/jpeg
Size:	59725
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-05 03:00:00 GMT
Accessed:	2023-02-05 03:00:00 GMT
Created:	2023-02-05 03:00:00 GMT
Changed:	2023-01-21 11:05:35 GMT
MD5:	fa02807ef0ca55b35d5e0b16f8ac921a
SHA-256:	508e368fe6912b5a67eb4f52ecd67bade41adefb2fc68e727a253884567d0d18
Hash Lookup Results:	UNKNOWN
Internal ID:	222

Figure 47:Metadata of step2.txt

Picture 6:VERA CRYPT

A file called {5bb2990fc95ada8c7bbb0e6f3036e6b3} on path {/img_Op Archway AXA-1.E01/vol_vol2/work/5bb2990fc95ada8c7bbb0e6f3036e6b3} has been investigated since the file has high entropy, which is suspicious. After the investigation it has been found that the file is a container file (a disk has been encrypted within the file). In the {Software Backups} directory on path {/img_Op Archway AXA-1.E01/vol_vol2/Software Backups} “VeraCrypt Setup 1.25.9.exe” file has been found. Matching the pieces together, it was realised that the container file {5bb2990fc95ada8c7bbb0e6f3036e6b3} has been encrypted by using “VeraCrypt” tool. The encryption key was the file name. However, the file name was hashed by md5. By using the reverse hash lookup table on a website called md5.gromweb, the password "stash" has been found {see Figure 48: Key “stash” on page 34}, and virtual disk has been accessed. Inside of the disk many “cat” (inappropriate children) pictures and file called “Vault” which also contains “cat” (inappropriate children) pictures has been found.

MD5 reverse for 5bb2990fc95ada8c7bbb0e6f3036e6b3

The MD5 hash:

5bb2990fc95ada8c7bbb0e6f3036e6b3

was succesfully reversed into the string:

stash

Figure 48: Key "stash"

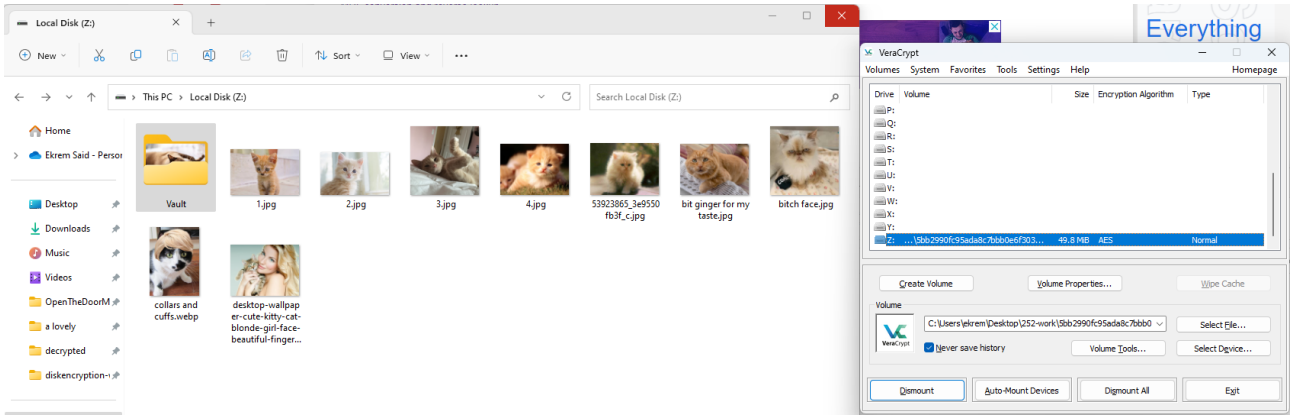


Figure 49: Virtual Disk (Decrypted)

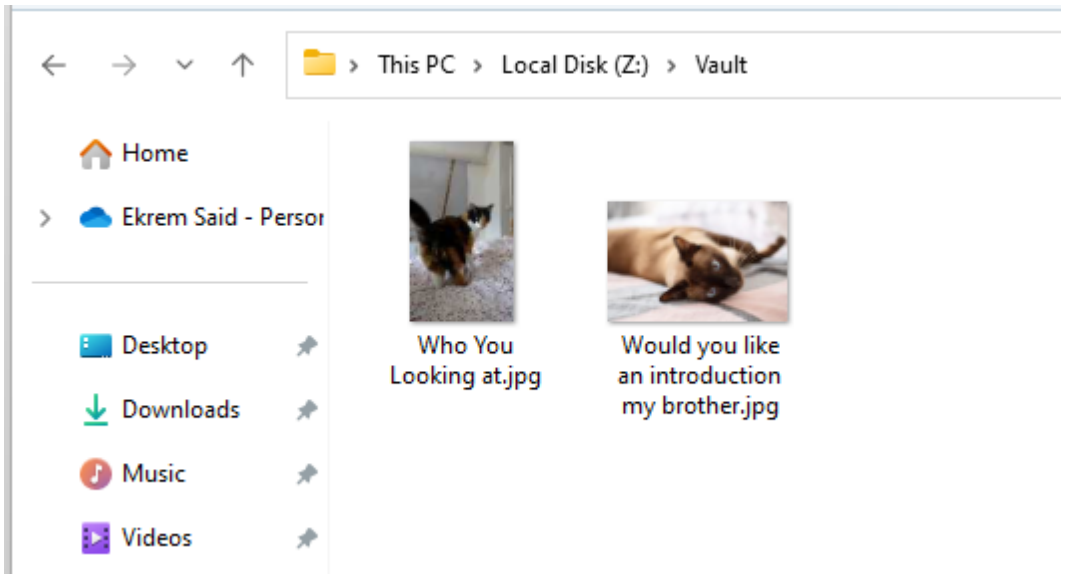


Figure 50: Vault file

Figure 51: 1.jpg

Figure 52: 2.jpg

Figure 53: 3.jpg

Figure 54: 4.jpg

Figure 55: 53923865_3e9550fb3f_c.jpg

Figure 56: bit ginger for my taste.jpg

Figure 57: bitch face.jpg

Figure 58: collars and cuffs.webp

Figure 59: desktop-wallpaper-cute-kitty-cat-blonde-girl-face-beautiful-fingers.jpg

Figure 60: Who You Looking at.jpg (Vault directory)

Figure 61: Would you like an introduction my brother.jpg (Vault directory)

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/work/5bb2990fc95ada8c7bbb0e6f3036e6b3
Type:	File System
MIME Type:	application/octet-stream
Size:	52428800
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-02-03 23:00:00 GMT
Accessed:	2023-02-03 23:00:00 GMT
Created:	2023-01-21 10:46:54 GMT
Changed:	2023-01-21 11:11:02 GMT
MD5:	43b6d447ab5c363917d411871de9cc65
SHA-256:	ae77d9847b2b79a3f5bd55f6daf66d8e297f28f11349c0437632423f2fb20238
Hash Lookup Results:	UNKNOWN
Internal ID:	255

Figure 62:Metadata of container file {5bb2990fc95ada8c7bbb0e6f3036e6b3}

Metadata

Name:	/img_Op Archway AXA-1.E01/vol_vol2/Software Backups/VeraCrypt Setup 1.25.9.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	22165328
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-01-21 10:44:15 GMT
Accessed:	2023-02-09 23:00:00 GMT
Created:	2023-01-21 10:46:53 GMT
Changed:	2023-02-20 11:43:11 GMT
MD5:	a7869a41d85f83d661fa3bea431e78f7
SHA-256:	9328f69fe8cca3377b66783fbae4405d764e77eae75cc2b62ac082c551d93a0e
Hash Lookup Results:	UNKNOWN
Internal ID:	244

Figure 63: VeraCrypt Setup 1.25.9.exe Metadata

CONCLUSION

To conclude, after examining the 'Op Archway AXA-1.E01' image file, emails, and some encrypted text files containing directives and instructions, it was determined that 'Dr. John Joshua James' was threatened in order to obtain technical specifications for the underwater drone 'TESV Mk1' and send them to the perpetrators. Specifically, INFORMATION 3: UNALLOCATED DISK SPACE E-MAILS within the Information Artefacts section shows the emails between “Dr. John Joshua JAMES” and person called Lucian that “Dr. John Joshua JAMES” has been asked to get specifications of the drone. The artefact DOCUMENT 1: For The Personal Attention of Dr.James.zip within the Document Artefacts section, clearly shows that “Dr. John Joshua JAMES” was threatened to get the specifications for “TESV Mk1” and a text file was hidden inside of the picture (Figure 18:WeKnow.jpg on page 17) which contains the home address of “Dr. John Joshua JAMES” to demonstrate the seriousness of the threat. The specifications of the “TESV Mk1” has been found hidden within the artefact DOCUMENT 2: whatisthelife'sgreatestillusion-mkv1.txt in section Document Artefacts with using the Steganography technique (OpenPuff). The artefact Picture 1: Would you like intoduction my brother.jpg in Picture Artefacts, a text file was hidden inside a picture, which contained a message congratulating the person for successfully completing the task. The actual reward was displayed in another picture within the same folder, which was a cat (inappropriate child picture). This is not the only cat picture that has been appeared. The term “The Family” what they refer their selves, seems like a network that shares pictures of cats and they make people to be able to have cats to play with. These can be clearly seen in artefact DOCUMENT 3: KITTY LOVERS in Document Artefacts that they use Vigenère encryption techniques and hide the pictures they share to eachother. The pictures of inappropriate children.

Overall, It can be proven from the investigation that the technical specifications of the "TESV Mk1" have been leaked through the use of the "watch drive". However, it's important to note that illegal content, such as child pornography and related materials, were found within the drive along with text files indicating arrangements of children to individuals.

Appendix A

Complete the declaration below

This version applies from 3rd April 2019

WE (**Chisel Chavush / Ekrem Said Iz / Emir Menekshelі**) DECLARE THAT:

1. I understand that my duty is to help the court to achieve the overriding objective by giving independent assistance by way of objective, unbiased opinion on matters within my expertise, both in preparing reports and giving oral evidence. I understand that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied with and will continue to comply with that duty.
2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.
3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report.
4. I do not consider that any interest which I have disclosed affects my suitability as an expert witness on any issues on which I have given evidence.
5. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affect my answers to points 3 and 4 above.
6. I have shown the sources of all information I have used.
7. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.
8. I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.
9. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others including my instructing lawyers.
10. I will notify those instructing me immediately and confirm in writing if for any reason my existing report requires any correction or qualification.
11. I understand that:
    1. my report will form the evidence to be given under oath or affirmation;
    2. the court may at any stage direct a discussion to take place between experts;
    3. the court may direct that, following a discussion between the experts, a statement should be prepared showing those issues which are agreed and those issues which are not agreed, together with the reasons;
    4. I may be required to attend court to be cross-examined on my report by a cross-examiner assisted by an expert.
    5. I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.
12. I have read Part 19 of the Criminal Procedure rules and I have complied with its requirements.
13. I confirm that I have acted in accordance with the code of practice or conduct for experts of my discipline, namely [identify the code].

14. [For Experts instructed by the Prosecution only] I confirm that I have read guidance contained in a booklet known as Disclosure: Experts' Evidence and Unused Material which details my role and documents my responsibilities, in relation to disclosure as an expert witness. I have followed the guidance and recognise the continuing nature of my responsibilities of revelation. In accordance with my duties of disclosure, as documented in the guidance booklet, I confirm that:
    1. I have complied with my duties to record, retain and reveal material in accordance with the Criminal Procedure and Investigations Act 1996, as amended;
    2. I have compiled an Index of all material. I will ensure that the Index is updated in the event I am provided with or generate additional material;
    3. in the event my opinion changes on any material issue, I will inform the investigating officer, as soon as reasonably practicable and give reasons.

STATEMENT OF TRUTH

I confirm that the contents of this report are true to the best of my knowledge and belief and that I make this report knowing that, if it is tendered in evidence, I would be liable to prosecution if I have wilfully stated anything which I know to be false or that I do not believe to be true.

Notes on Codes of Practice & Conduce can be found at the following link
https://www.academyofexperts.org/guidance/experts-declaration/experts-declaration-criminal-proceedings-england-wales

REFERENCES

Basis Technology, n.d.. *Autopsy.* [Online]
Available at: https://www.autopsy.com/about/
[Accessed 01 04 2023].
Embedded SW, 2020. *OpenPuff - Steganography & Watermarking.* [Online]
Available at: https://embeddedsw.net/OpenPuff_Steganography_Home.html
[Accessed 01 04 2023].
Exterro, 2021. *FTK Imager.* [Online]
Available at: https://www.exterro.com/ftk-imager
[Accessed 01 04 2023].
Government Communications Headquarters of the United Kingdom, 2016. *CyberChef - the Cyber "Swiss Army Knife".* [Online]
Available at: https://www.gchq.gov.uk/news/cyberchef-cyber-swiss-army-knife
[Accessed 01 04 2023].
Hörz, M., 2003. *mh-nexus.* [Online]
Available at: https://mh-nexus.de/en/hxd/
[Accessed 01 04 2023].
IDRIX , 2019. *VeraCrypt - Free Open source disk encryption with strong security for the Paranoid.* [Online]
Available at: https://www.veracrypt.fr/en/Home.html
[Accessed 01 04 2023].