الجامعة الإسلامية العالمية ماليزيا

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

يونيۏرسيتي إسلام انتارابغسا مليسيا

Garden of Knowledge and Virtue

KULLIYYAH OF INFORMATION & COMMUNICATION TECHNOLOGY

CSCI 4332 DIGITAL EVIDENCE FORENSICS

Group project

SEMESTER 1, 2021/2022

SECTION 1

PREPARED BY

NAME	MATRIC NUMBER
DELAMOU JACQUES	1820045
SAGAR FAKHRU UDDIN	1730753

LECTURER

DR. NORMAZIAH BINTI ABDUL AZIZ

Contents

1 INTRODUCTION:

The Wearable internet of things (Iot) Technology is getting popular day by day and when we look at the future of our daily lives, we can predict the rapid increase for the coming years. here are examples of different type of wearable technology products that people use nowadays: Smartwatches, Smart Running Shoes, Health and Fitness Trackers, Wireless Headphones, Smart Glasses, and much more. wearable technology is growing, and it is becoming a part of our lives in this modern world. Those wearable IoT devices continue to create opportunities and challenges for forensic investigators in the acquisition and analysis of evidence in scenarios where these devices witness a crime.

In this class project, we won't be performing any live investigation. This given task is a class assignment of our university, wherein we simulate the roles of forensics investigator, choosing a device that we will treat as a source of digital evidence, creating a crime and investigation scenario with evidence residing on our chosen device which will be a smartwatch and determining what methods and tools were used to our investigation. Strong evidence found at a crime scene, such as a smartwatch, can be an important factor in solving a crime. The investigation of our project attempts to prove some evidence in a smartwatch proving the link to our crime scene. One of the main objectives of our project is to explore which file location within the file systems hold the most valuable information. Furthermore, our main focus would be looking into the data relating to the smartwatch connection system since the watch was found at a crime scene without its paired phone. the question to be answer is: would the information stored on the smartwatch differ from its paired phone? and if so, would the value of the evidence stored within the smartwatch still be of value. we will be conducting several investigations, looking into the smartwatch along our forensics process, investigating the smartwatch devices performing forensic analysis.

2 : CRIME SCENE CASE

People rely on their smartwatches for many things. Most use their smartwatches to check text messages, manage their calendars and even track their heart rate as they work out. But for forensic scientists, these smart devices can do so much more. Mobile forensic teams and police agencies have recognized the value of smart technology to solve crimes and even prevent criminal activity. These experts suspected that the wealth of data smart devices collect would be a powerful crime-fighting tool, and now they have been proven right in a spectacular manner. In a recent murder case, smartwatch data proved pivotal, not only in identifying what happened but in bringing the guilty person to justice. Using mobile forensic data, police were able to identify the murder victim, narrow down the search for suspects and ultimately make an arrest in the case. In this case, it was the victim of the crime who was wearing the smartwatch, and the data collected on the device helped police get a picture of what took place in the minutes before her death. The murder took place in Australia, and the victim was a grandmother from Adelaide. When investigating the case, mobile forensic experts were able to narrow the time frame of the killing to a seven-minute window. Once investigators estimated the time of the murder, they were able to piece together the events leading up to the killing more accurately, ultimately identifying the woman's daughter-in-law as the killer and making an arrest. The details of the investigation are fascinating, especially to those with an interest in the growing field of forensic science. In investigating the case, mobile forensic experts carefully examined the data collected by the victim's smartwatch, which recorded the entire event. Instead, the data collected by the mobile forensic experts on the scene pointed to a staged home invasion, one designed to divert suspicion and cover up the crime. Now the killer is facing justice, and smart devices are getting a newfound respect. Here we try to find out important documents by our knowledge .As the use of smartwatches, smart speakers and other internet-connected devices continue to grow, police expect to see these devices play a greater role in crime solving.

3 3. DESCRIPTION

3.1 Definition of Smartwatch:

A smartwatch is similar to a minicomputer or mini smartphone because it has both the features of computer and smartphone within a single watch. It can also perform the smart task just like a computer. It has a touchscreen display interface. Applications, games, and videos can be installed via internet access in it. smartwatches have many features. on top of time keeping, the digital watch allows us to monitor many components such as heart rate, activity tracker, and reminder. smartwatches have a touch screen that allows user to do actions through tapping or swiping on the screen like a smartphone. A smartwatch requires a smartphone to function even though applications run directly on the smartwatch. in many cases the phone should be the first to receive the data and then it is sent to the watch, because most smart watches must rely on a smartphone which is compatible to provide the necessary data over Bluetooth connection. So, as a consequence, some functionality of the watch will be limited if the phone is not connected. For instance, of a smartwatch which doesn't contain a SIM card, if a messaging application on the watch allows you to send a message, the actual message is sent by the phone connected to the watch. but the message will not be sent if the connection is lost. The good news is that there are many other functionalities such as activity tracking that do not need a connection to a smart phone. In our forensics investigation project, the evidence watch being analysed can technically be a stand- alone device as it has phone like capabilities, it has a sim within itself and do not need the phone for messages or calls to have those types of features. Our evidence watch contain non-volatile memory and the OS range from Google Android Wear, Huawei wearable platform, etc…. Although they have similarities with mobile phones which already have a standardised methodology for forensic analysts in how to handle the device throughout the investigation, smartwatches are considered to be a different device that means the methodology implemented would have nuances and different from phones forensics methodology even though they look similar.

3.2 Chosen Smartwatch: Sony Smartwatch 3 SWR50

The Sony Smartwatch 3 is the evidence watch chosen for this class project as we got one sample of the device and also it one of the most commonly investigated watches mentioned in many articles and researches when reading research papers.

4 INVESTIGATION STEPS

4.1 List of devices and tools:

In this section, is listed the description of the tools and devices used in our project.

Brand	Model	Version	Specification
Sony	SWR50	TFT	**OS:** Android Wear OS **CPU:** Quad-core 1.2 GHz Cortex-A7 **MEMORY Card slot**: yes **Internal:** 4GB RAM **SIM Card slot:** Yes
Lenovo	ThinkPad		Windows OS: windows 10 Pro 64-bit(10.0, Build 18363)
Memory card	SanDisk Ultra	A1	16GB
AccessData FTK Imager			Size:1.97 KB(2.019 bytes)
MEO encryption software			To decrypt encrypted files
Cesar cipher decrypte software			To decrypt encrypted messages
ExifData			To find detailed information(metadata) of the evidences that are investigated and any forms of tampering or hidden evidences
HashCalc			Size: 1012 bytes(1.012bytes)
USB driver with card memory plug	USB2.0D		Used for for imaging the memory card

1. The smartwatch evidence:

2. **the laptop Lenovo used for Lab analysis**

3. **The USB with memory card plugs for Lab analysis**

4. **The flash drive used for copy of imaging the evidence**

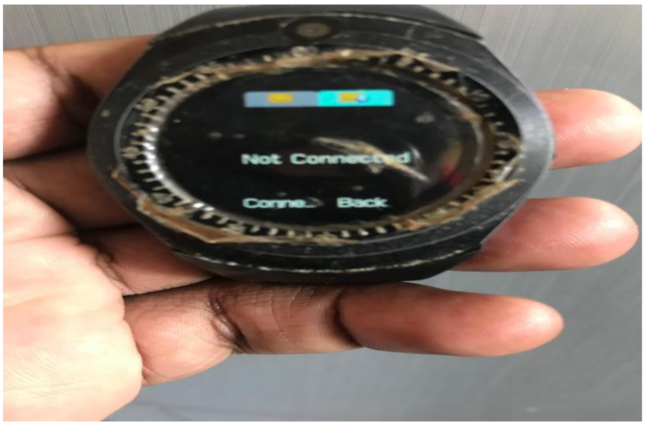
4.2 Evidence Collection

At the stage of Evidence collection, there are several considerations that should be taken into account when we get the device. Initial preservation of the device is essential to a positive result for an investigation. If our evidence is contaminated, it may not be admissible in court. Moreover, the device itself can be tampered with forever if the proper procedures are not followed. Fortunately, in our case, the evidence collection procedure was done legally and professionally. these procedures include securing, assessing, and documenting the scene. During the collection of the evidence, we opted for the isolation of the watch to prevent the activation of a password or a remote erase of the device via Wi-Fi or SMS. In our present evidence collection case, our device was found unlocked and we had to prevent it from locking due to potential evidence that we could find and for that we had to activate the airplane mode using the menu settings and activate the USB debugging mode, increasing the screen timeout, or enabling the stay awake option, ensuring that the device does not lock up while charging. Once the device was secured, we transferred it to our laboratory for processing. We were fortunate when purchasing the smartwatch that it was in an unlocked state. because there is a better chance of preserving the data necessary for our investigation.

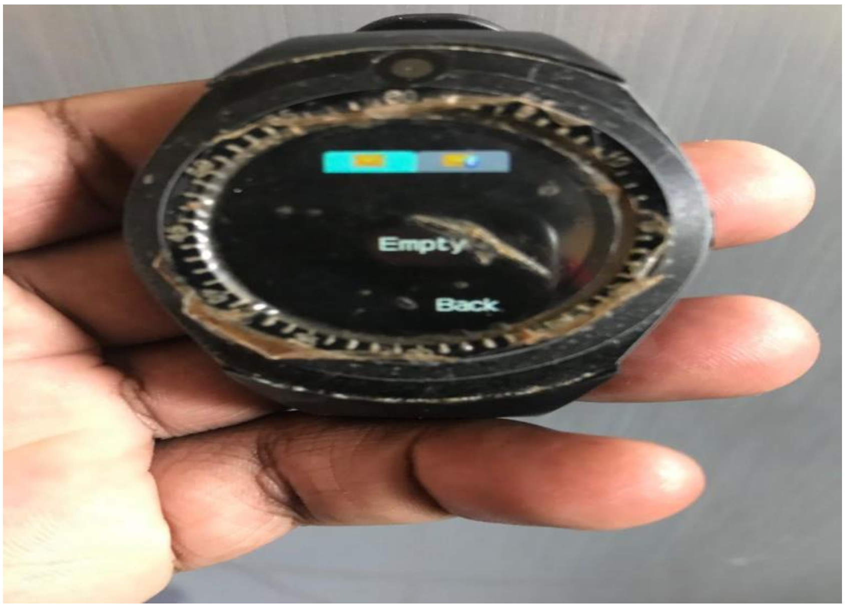
5 DATA ACQUISITON:

The collection phase is the first phase of our process, and it is to identify, label, record, and acquire data from the possible sources of relevant data, while following legal guidelines and procedures that preserve the integrity and the validity of the data. since our smartwatch is found with power on, we will have two different types of data that should be collected in our forensics investigation. we will deal firstly with volatile data and secondly the non-volatile data. According to volatile data definition, volatile data is data that exists when the system is on and erased when powered off. Random Access Memory (RAM), registry and caches are some examples of where we can find volatile data. Non-volatile data is data that exists on a system when the power is on or off, as example in our case, information, or data on memory card. Since our evidence was found without a connection with its pair phone or any other pair phone, we couldn't find much information as live data.

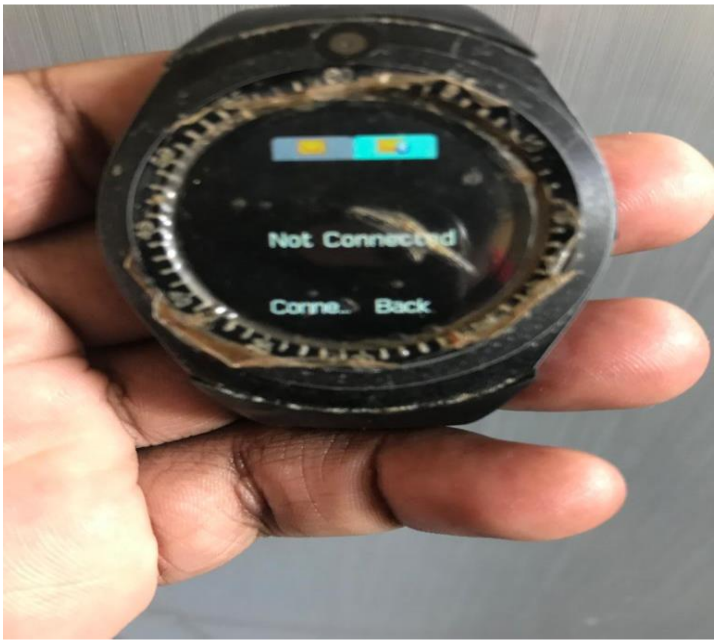
5.1 All running application were disconnected.



5.2 We couldn’t find any message in the message inbox

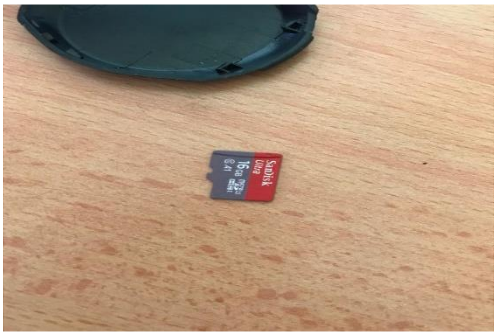


5.3 There were no messages in the sending box, that because the device was not connected.



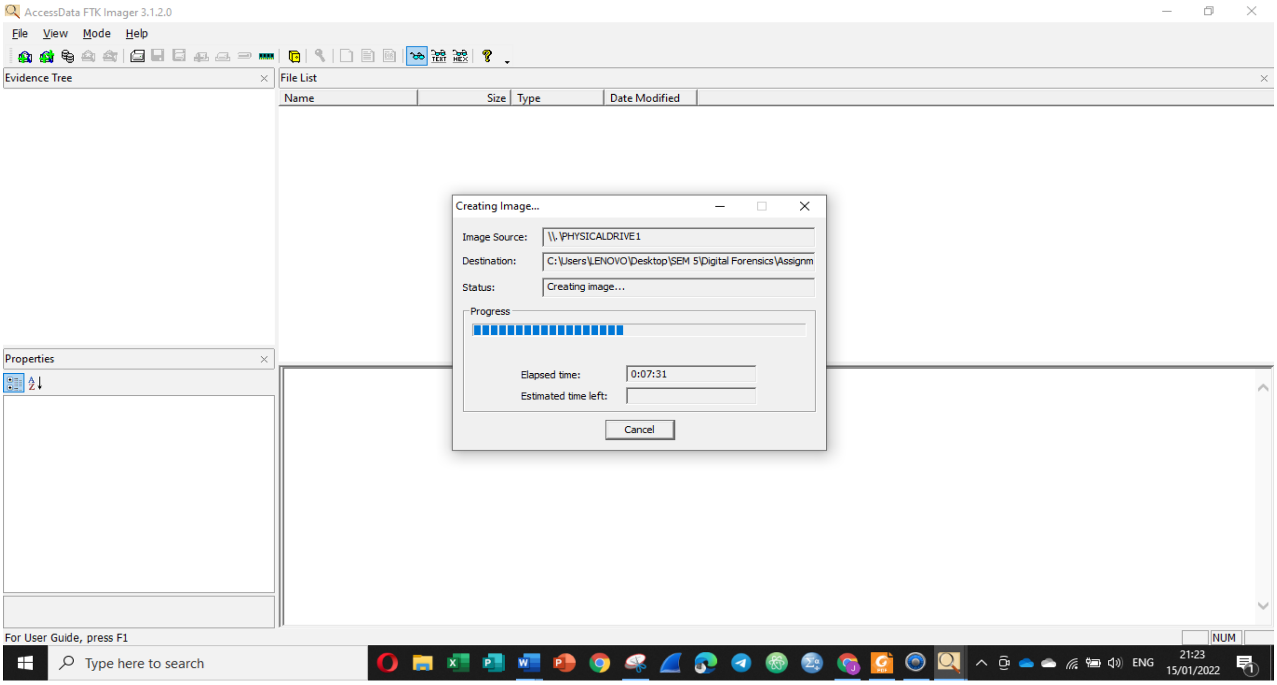
6 Non-Volatile Data collection:

In this case, we found a memory card inside the smartwatch which was brought to be analysed by our group. We supposed that though the smartwatch was not paired or connected to any phone, it would probably get some useful information inside the memory card.



Creating image of evidence is one of the first important tasks in our digital forensic investigation, because the core rule of forensic investigation says to not work on the actual evidences. For that we create bit by bit image of our evidence in terms of our project. For checking integrity of the evidence, we make sure that hash value is calculated before starting the imaging of the evidence which is our original data. At the end of the imaging, we also verify it with the calculated hash of image. this because we want to avoid any accidental modifications during the imaging process.

7 EVIDENCE IMAGING:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\LENOVO\Desktop\SEM 5\Digital Forensics\Assignm

Status: Creating image...

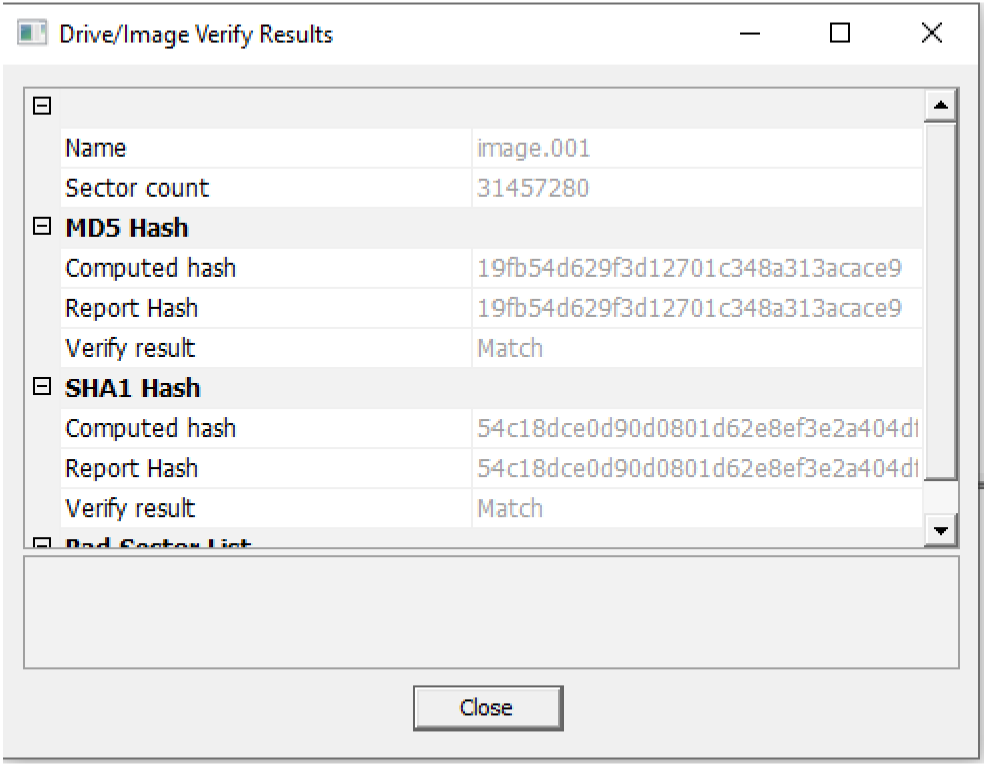
Progress

Elapsed time: 0:07:31

Estimated time left:

Cancel

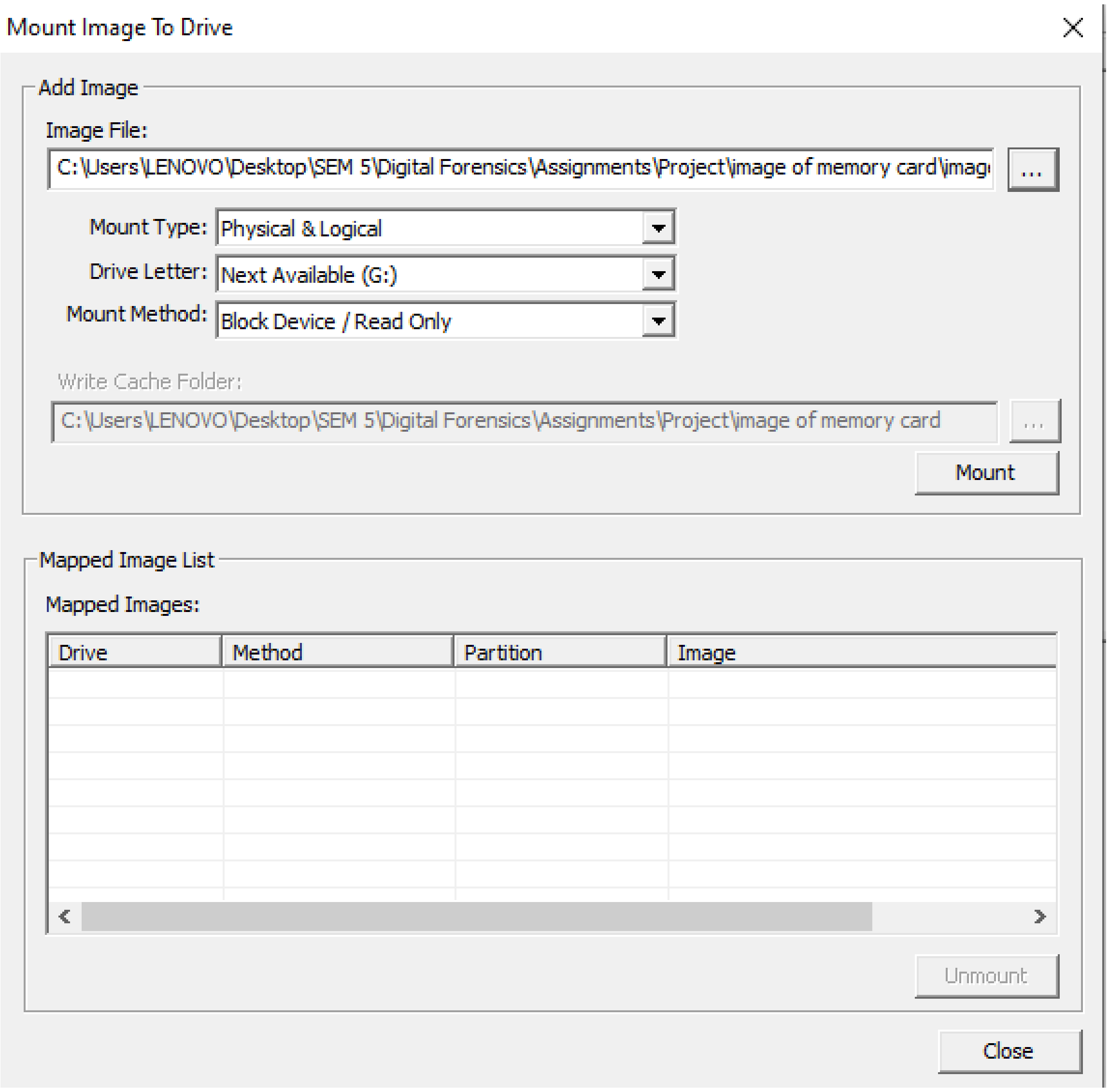
8 Hash value calculation of the original and the image copy



Drive/Image Verify Results

Name	image.001
Sector count	31457280
MD5 Hash	
Computed hash	19fb54d629f3d12701c348a313acace9
Report Hash	19fb54d629f3d12701c348a313acace9
Verify result	Match
SHA1 Hash	
Computed hash	54c18dce0d90d0801d62e8ef3e2a404d
Report Hash	54c18dce0d90d0801d62e8ef3e2a404d
Verify result	Match
Bad Sector List	

9 IMAGE MOUNTING



Mount Image To Drive

Add Image

Image File: C:\Users\LENOVO\Desktop\SEM 5\Digital Forensics\Assignments\Project\image of memory card\imag

Mount Type: Physical & Logical

Drive Letter: Next Available (G:)

Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\LENOVO\Desktop\SEM 5\Digital Forensics\Assignments\Project\image of memory card

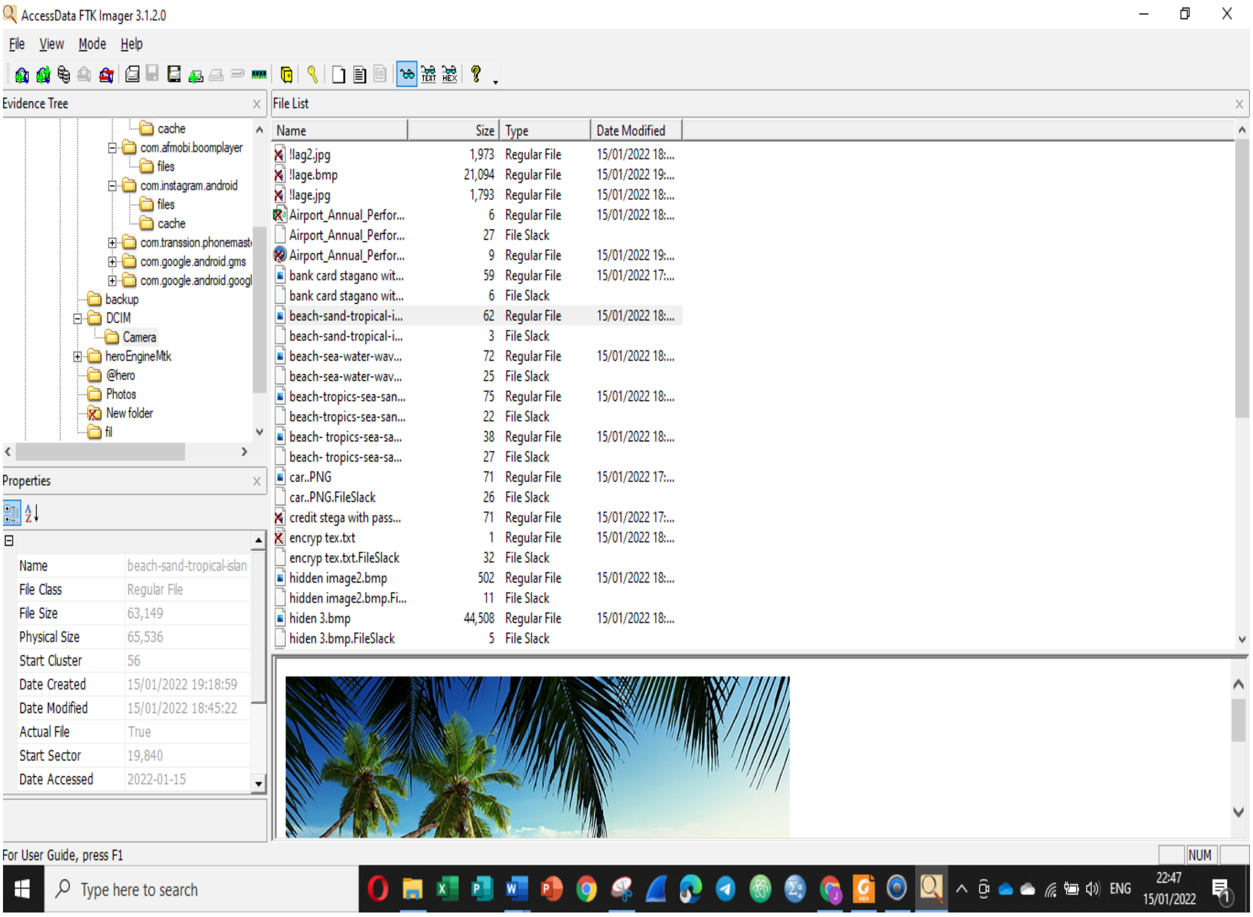
Mapped Image List

Mapped Images:

Drive	Method	Partition	Image

Deleted files: we tried to focus on deleted files as well as any other file that could get any useful information and here are what we got:

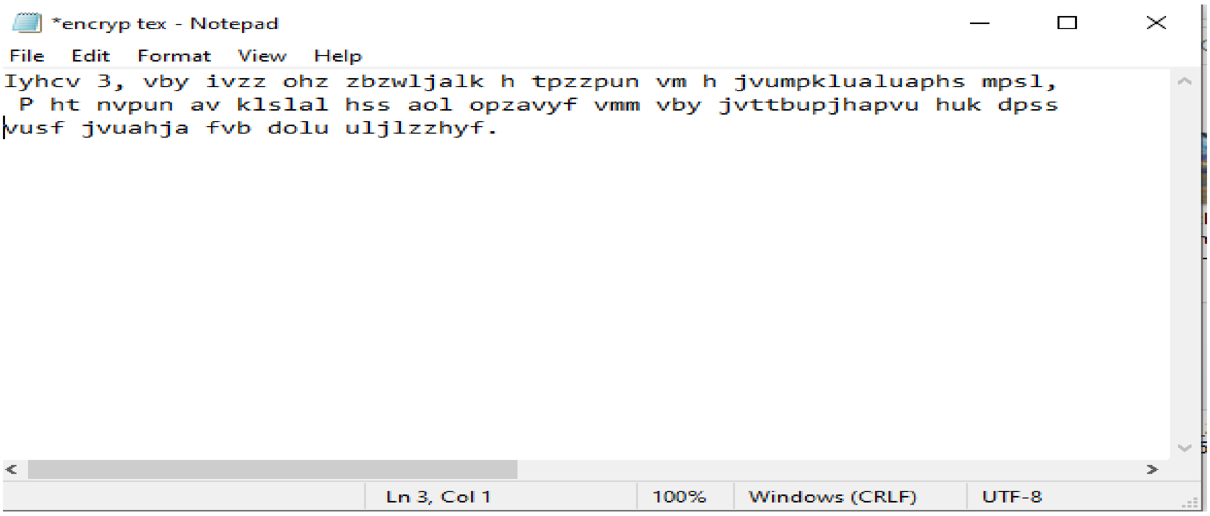
From FTK imager we could clearly see that a lot of files were deleted and we tried to recover them and find out what information could surprise us.



Name	beach-sand-tropical-islan
File Class	Regular File
File Size	63,149
Physical Size	65,536
Start Cluster	56
Date Created	15/01/2022 19:18:59
Date Modified	15/01/2022 18:45:22
Actual File	True
Start Sector	19,840
Date Accessed	2022-01-15

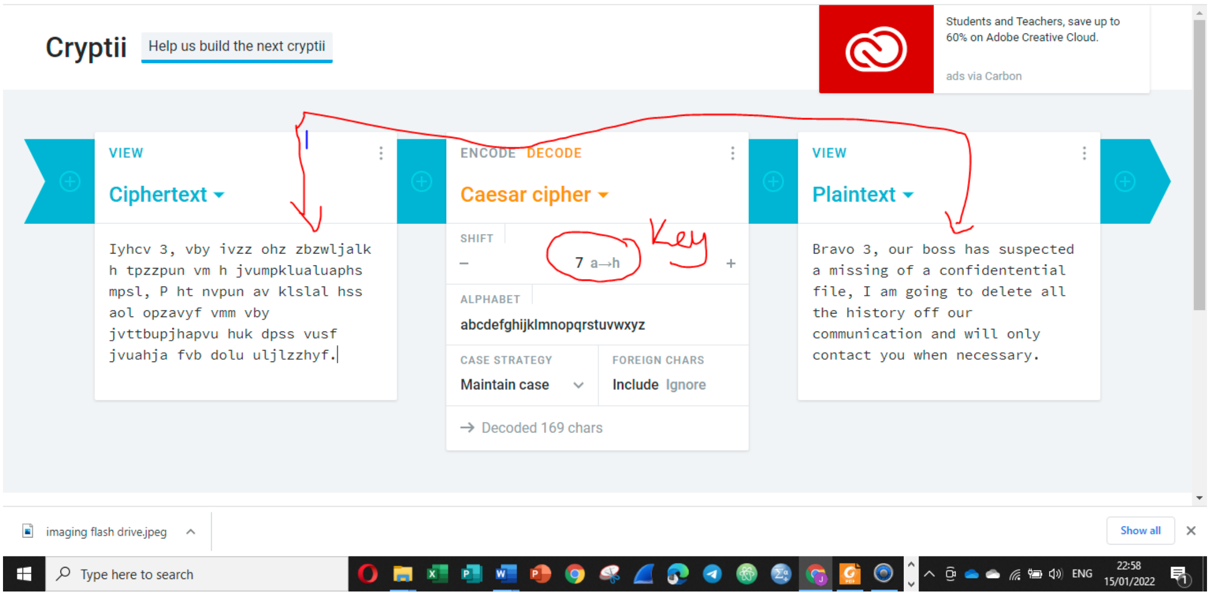
Name	Size	Type	Date Modified
!lag2.jpg	1,973	Regular File	15/01/2022 18:...
!lage.bmp	21,094	Regular File	15/01/2022 19:...
!lage.jpg	1,793	Regular File	15/01/2022 18:...
Airport_Annual_Perfor...	6	Regular File	15/01/2022 18:...
Airport_Annual_Perfor...	27	File Slack	
Airport_Annual_Perfor...	9	Regular File	15/01/2022 19:...
bank card stagano wit...	59	Regular File	15/01/2022 17:...
bank card stagano wit...	6	File Slack	
beach-sand-tropical-i...	62	Regular File	15/01/2022 18:...
beach-sand-tropical-i...	3	File Slack	
beach-sea-water-wav...	72	Regular File	15/01/2022 18:...
beach-sea-water-wav...	25	File Slack	
beach-tropics-sea-san...	75	Regular File	15/01/2022 18:...
beach-tropics-sea-san...	22	File Slack	
beach- tropics-sea-sa...	38	Regular File	15/01/2022 18:...
beach- tropics-sea-sa...	27	File Slack	
car..PNG	71	Regular File	15/01/2022 17:...
car..PNG.FileSlack	26	File Slack	
credit stega with pass...	71	Regular File	15/01/2022 17:...
encryp tex.txt	1	Regular File	15/01/2022 18:...
encryp tex.txt.FileSlack	32	File Slack	
hidden image2.bmp	502	Regular File	15/01/2022 18:...
hidden image2.bmp.Fi...	11	File Slack	
hiden 3.bmp	44,508	Regular File	15/01/2022 18:...
hiden 3.bmp.FileSlack	5	File Slack	

We found a file that contained an encrypted message and we tried to decode it and finaly we got lucky with Cesar cipher decoder because the key was hidden into a photo.



```
Iyhcv 3, vby ivzz ohz zbzwljalk h tpzzpun vm h jvumpklualuaphs mpsl,
 P ht nvpun av klslal hss aol opzavyf vmm vby jvttbupjhapvu huk dpss
vusf jvuahja fvb dolu uljlzzhyf.
```

Here is the decoded message: “Bravo 3, our boss has suspected a missing of a confidentential file, I am going to delete all the history off our communication and will only contact you when necessary.” That shows clearly that he knew that there could be an investigation at any moment of time.



Ciphertext:

```
Iyhcv 3, vby ivzz ohz zbzwljalk
h tpzzpun vm h jvumpklualuaphs
mpsl, P ht nvpun av klslal hss
aol opzavyf vmm vby
jvttbupjhapvu huk dpss vusf
jvuahja fvb dolu uljlzzhyf.
```

SHIFT: 7 a→h

ALPHABET: abcdefghijklmnopqrstuvwxyz

CASE STRATEGY: Maintain case

FOREIGN CHARS: Include Ignore

→ Decoded 169 chars

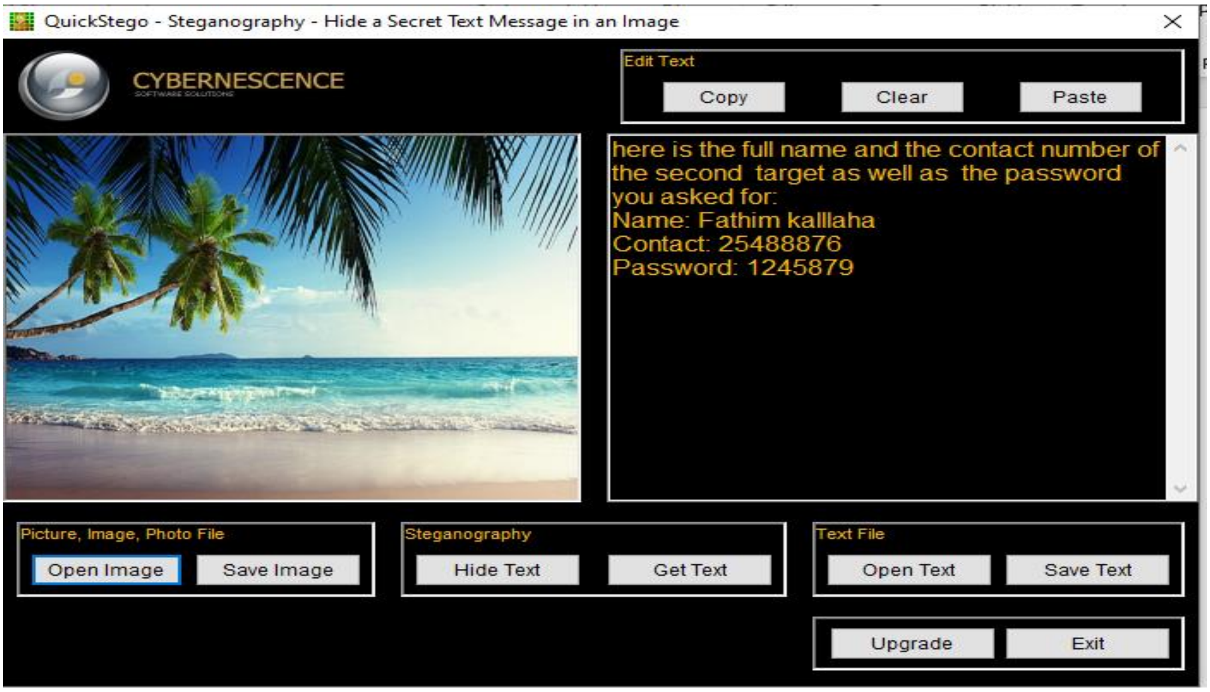
Plaintext:

```
Bravo 3, our boss has suspected
a missing of a confidentential
file, I am going to delete all
the history off our
communication and will only
contact you when necessary.
```

By using Steganography software, we found out that many hidden messages and confidential data of his coworker and even the secret key of the encrypted message.

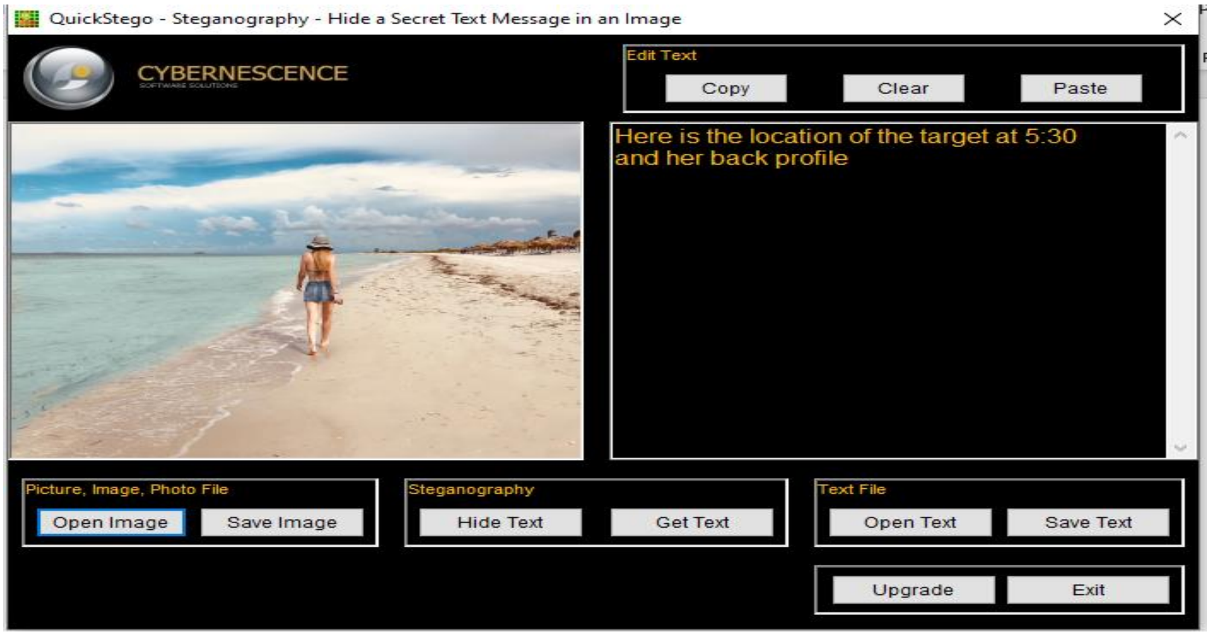
Here are what we found as evidence:

a) Here is the contact and the credit card password of his co-worker that they were using to purchase illegally online.



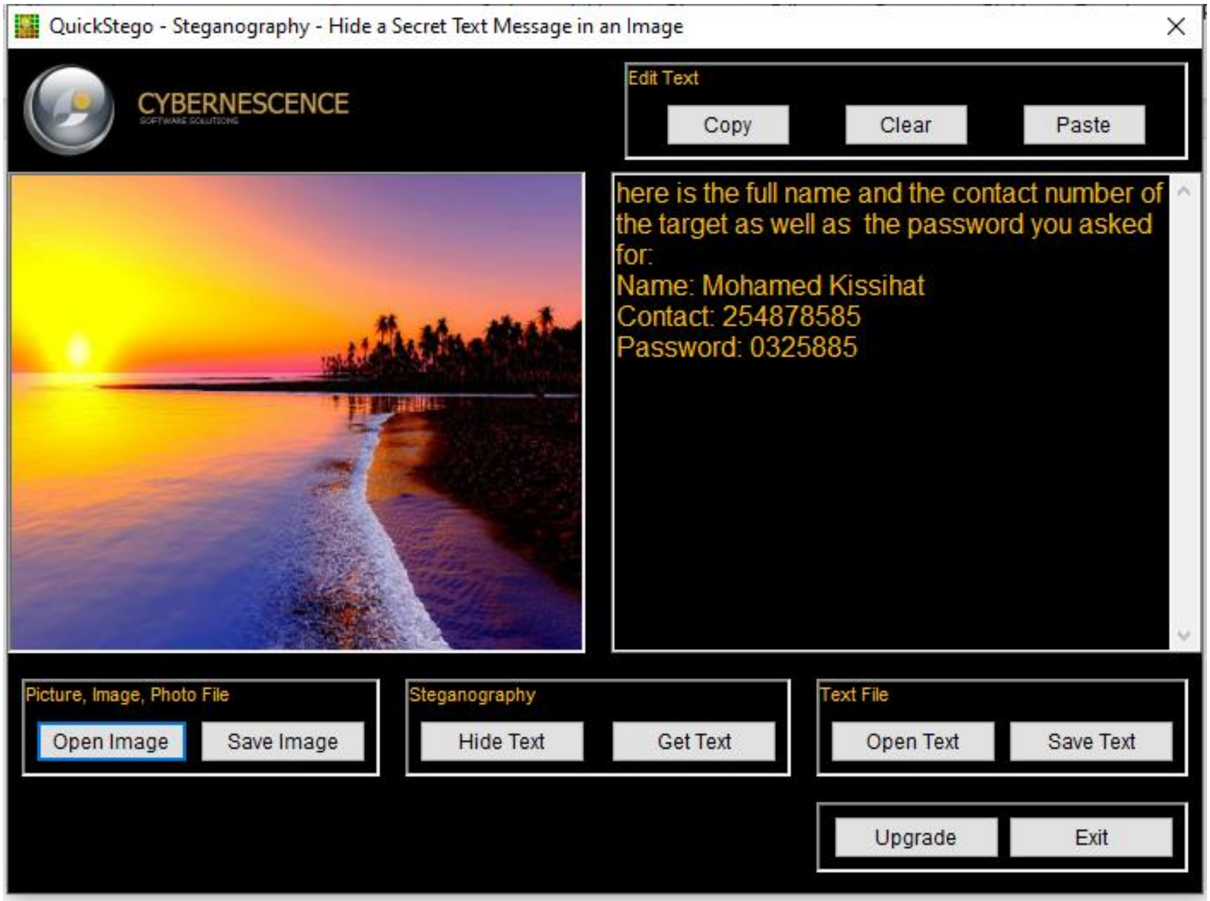
here is the full name and the contact number of the second target as well as the password you asked for:
Name: Fathim kalllaha
Contact: 25488876
Password: 1245879

b) this is clearly the place where he could have probably scanned the credit card of his co-worker



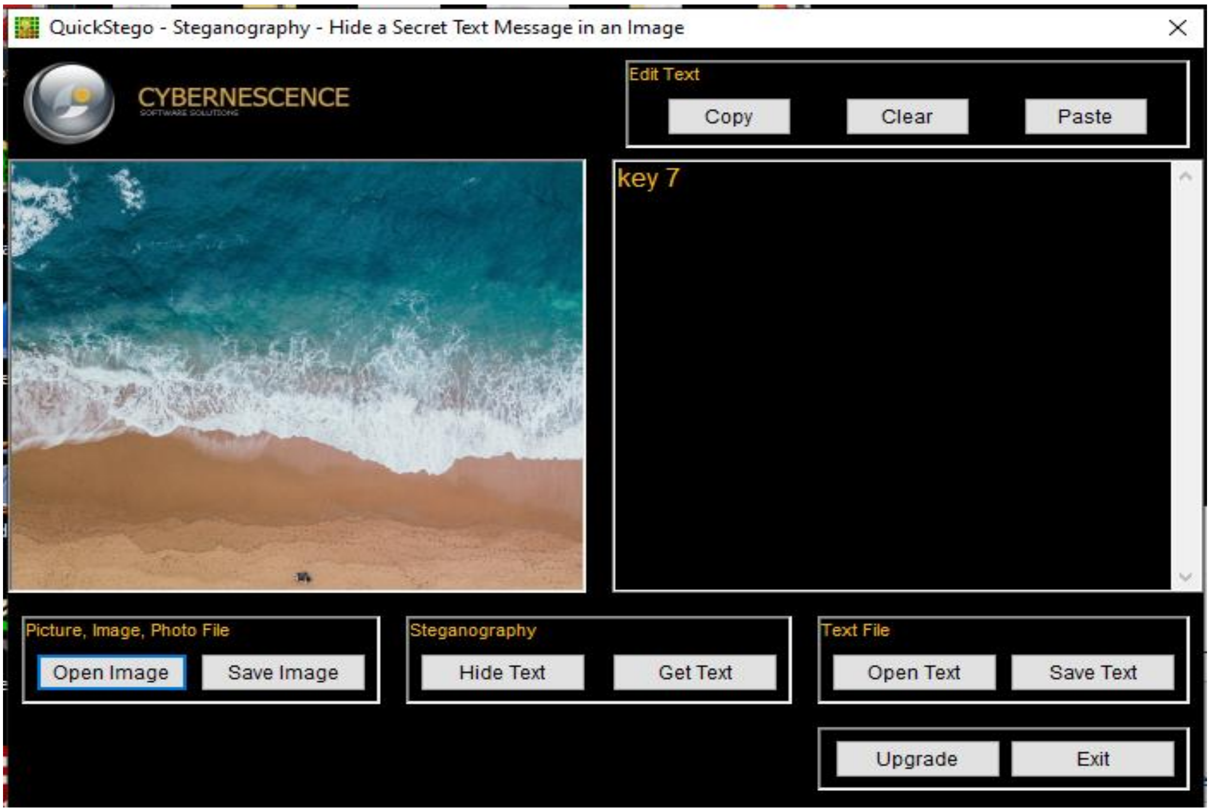
Here is the location of the target at 5:30
and her back profile

a) Here is the information of the second co-worker and his credit card password that they were using to purchase thing online.



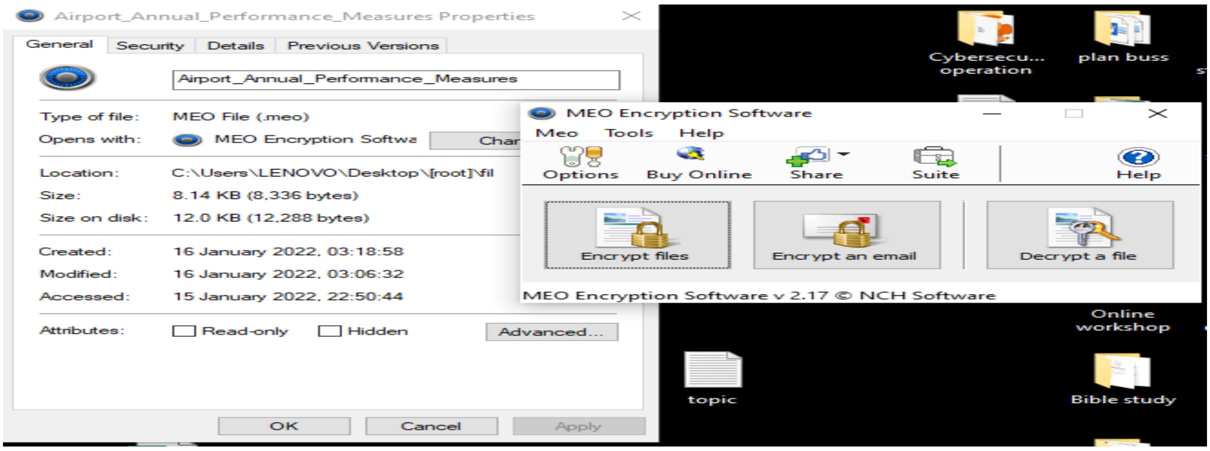
here is the full name and the contact number of the target as well as the password you asked for:
Name: Mohamed Kissihat
Contact: 254878585
Password: 0325885

d)Here is where we found luckily the encrypted Cesar cipher text message embedded into this image.



key 7

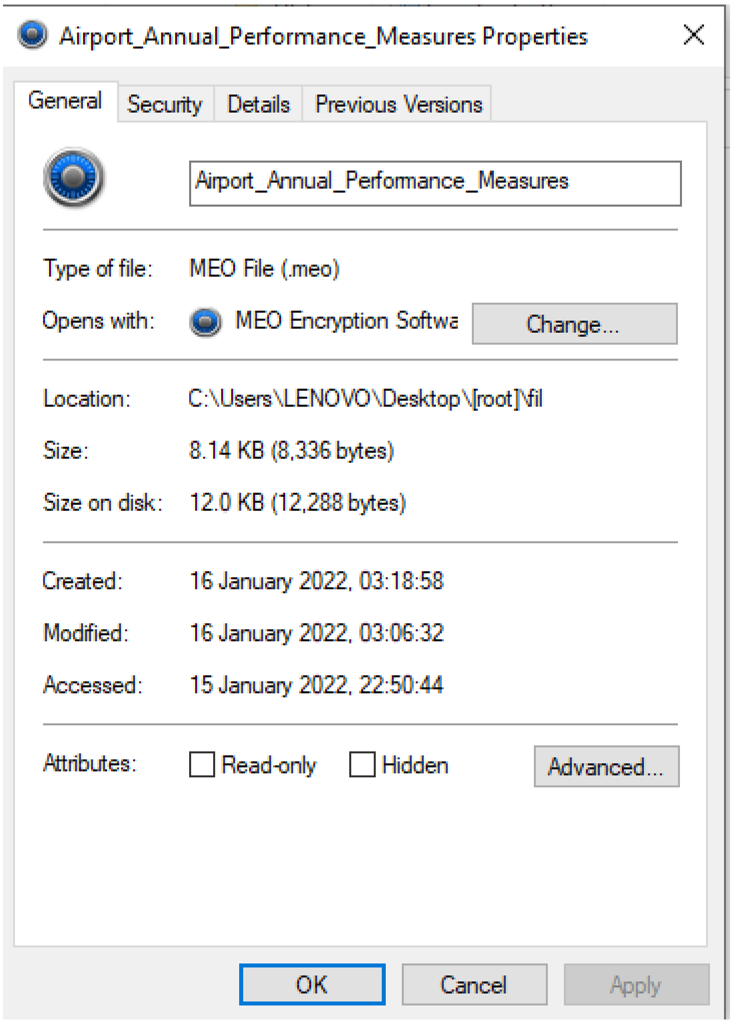
We found out also the use of MEO encryption software to encrypt a file that was containing transaction of the company. We used brute force algorithm by guessing some characters of the password and we got his name in his password to help us decrypt the file. Here is the proof that confidential data from the company were stolen.



Airport_Annual_Performance_Measures

Type of file: MEO File (.meo)
Opens with: MEO Encryption Softwa
Location: C:\Users\LENOVO\Desktop\[root]\fil
Size: 8.14 KB (8,336 bytes)
Size on disk: 12.0 KB (12,288 bytes)
Created: 16 January 2022, 03:18:58
Modified: 16 January 2022, 03:06:32
Accessed: 15 January 2022, 22:50:44
Attributes: □ Read-only □ Hidden

MEO Encryption Software v 2.17 © NCH Software



Airport_Annual_Performance_Measures Properties

Airport_Annual_Performance_Measures

Type of file: MEO File (.meo)

Opens with: MEO Encryption Softwa

Location: C:\Users\LENOVO\Desktop\[root]\fil

Size: 8.14 KB (8,336 bytes)

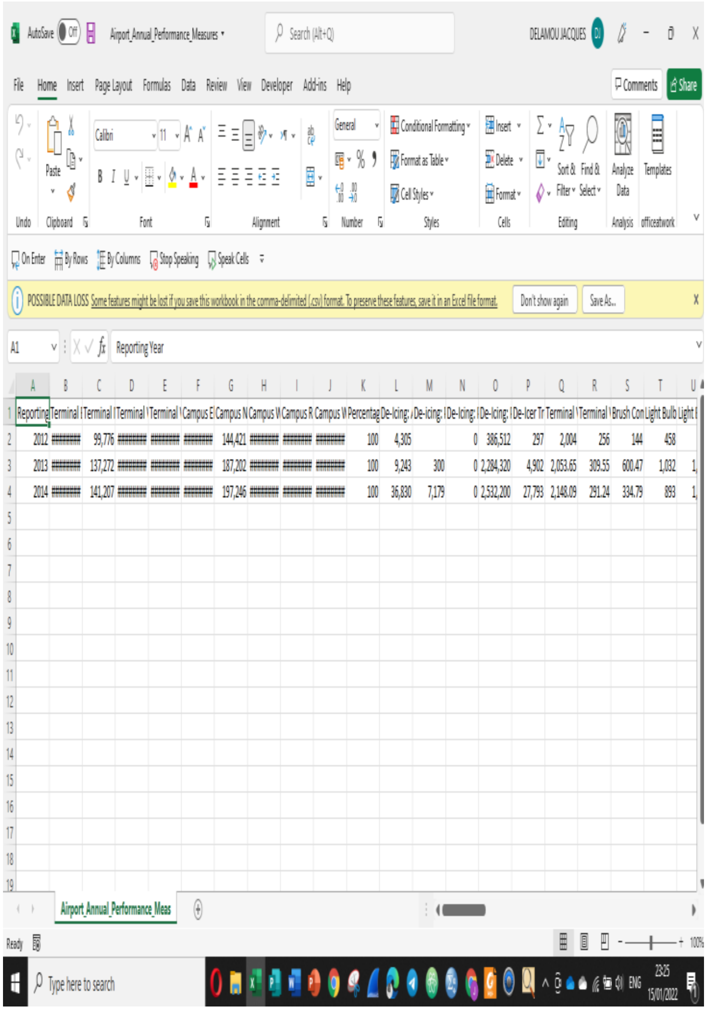
Size on disk: 12.0 KB (12,288 bytes)

Created: 16 January 2022, 03:18:58

Modified: 16 January 2022, 03:06:32

Accessed: 15 January 2022, 22:50:44

Attributes: □ Read-only □ Hidden



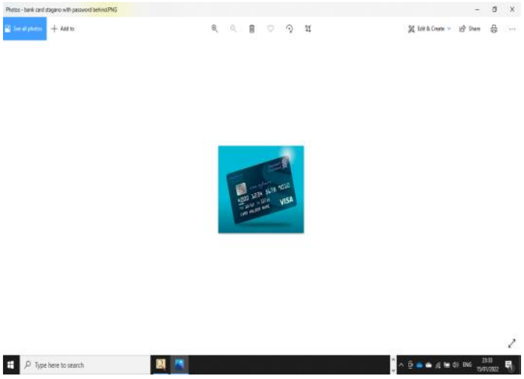
POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.

A1 fx Reporting Year

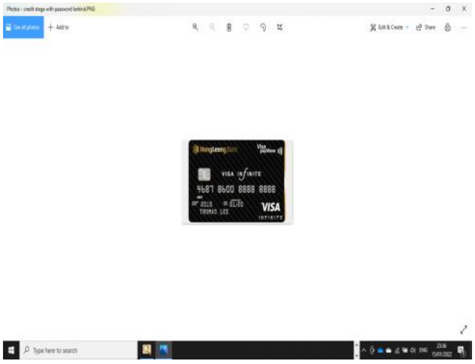
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	Reporting	Terminal	Terminal	Terminal	Terminal	Campus E	Campus N	Campus W	Campus R	Campus W	Percentag	De-Icing:	De-icing:	De-Icing:	De-Icing:	De-Icer Tr	Terminal	Terminal	Brush Con	Light Bulb	Light
2	2012	#######	99,776	#######	#######	#######	144,421	#######	#######	#######	100	4,305		0	386,512	297	2,004	256	144	458	
3	2013	#######	137,272	#######	#######	#######	187,202	#######	#######	#######	100	9,243	300	0	2,284,320	4,902	2,053.65	309.55	600.47	1,032	1,
4	2014	#######	141,207	#######	#######	#######	197,246	#######	#######	#######	100	36,830	7,179	0	2,532,200	27,793	2,148.09	291.24	334.79	893	1,

10 Deleted images recover with FTK Imager:

10.1 Two bank cards photos



Photos - bank card stagano with password behind.PNG



Photos - credit stega with password behind.PNG

1. A deleted pdf file that was containing the scanned version of these two cards

11 CONCLUSION

Implementing digital forensics on smartwatch devices is a bit challenging for forensics analyst. Data residing on unrooted smartwatch can be extracted using the right tools and processes. It is important to understand the watch architecture, its operating systems and to also understand computer forensic process and forensic tools before thinking about the data extraction and recovery of files. Data from the Contact List, Call Logs, memory card, SMS and GPS TrackPoint were not found because there was no connected phone to the smartwatch. Related data were analysed for the law enforcement to relate this evidence to the case. If real life case scenario, such digital evidence can then be brought to the court. The experience learns from this project is that the data extraction needs a lot of knowledge from many backgrounds field and requires knowing the architecture models of smartwatch and their respective manufacturer proprietary design.

12 REFERENCES:

[1] ‘Challenges and opportunities for wearable IoT forensics_ TomTom Spark 3 as a case study | Elsevier Enhanced Reader’. https://reader.elsevier.com/reader/sd/pii/S2665910721000293?token=3AC6EA4FF5FDC5F73F6A58916A5442AE8A7CF6611E44240CE439128D38285FE41796DDFBB91569C59D5F505053694B63&originRegion=eu-west-1&originCreation=20211225042433 (accessed Dec. 25, 2021).

[2] L. Dawson and A. Akinbi, ‘Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study’, *Forensic Sci. Int. Rep.*, vol. 3, p. 100198, Jul. 2021, doi: 10.1016/j.fsir.2021.100198.

[3] ‘Computer forensics investigation – A case study - Infosec Resources’. https://resources.infosecinstitute.com/topic/computer-forensics-investigation-case-study/ (accessed Dec. 25, 2021).

[4] H. Bahsi, ‘DIGITAL FORENSIC ANALYSIS OF SMART WATCHES’, p. 42, 2020.