INVESTIGATION REPORT

HEXA OSINT CTF v2

CASE N°02: L.DUMARQUAIS

Investigation conducted by:

hashp4
baddhack
WildPasta
Lwo

Classification level:

CONFIDENTIAL

Date: 29/01/2023	Référence : Report_CS_02 (v1)

Table of contents

Introduction.....3
#1 - Mission Analysis.....3
#2 Action man Analysis - Oleg VOKOLSKI.....5
#3 Associate Analysis - Minca H.....13
#4 Mastermind Analysis.....17
Conclusion.....19
Appendix.....20

Introduction

As a reminder, last year we worked on a criminal organization called Manipar. This group is composed of friends who met during an Erasmus course. Their business is based on the theft and resale of strategic data for personal gain. This year, Lucilhe Dumarquais, the leader of Manipar escaped during a transfer. The convoy transporting L. Dumarquais from "Maison d'arrêt de Versailles" was hijacked on the 30th of November 2022. She was planning to give information about the people to whom she was selling the data but she disappeared from the scene after this event.

We answered the ministry call to help the government to recover the group's tracks. This report highlights the elements that our investigators gathered following the escape of Lucilhe Dumarquais.

#1 - Mission Analysis

In this part, we detail how we could establish a link between Mastermind and Oleg VOLOSKI (also known as the "**action man**") involvement in the course of events.

Oleg VOLOSKI aka "Action Man" kidnaped Lucilhe Dumarquais when she was headed towards the tribunal of Versailles on the 30th of November 2022. They stayed in a safehouse for a while and crafted fake passports to take off by plane later.

On the 14th of December 2022, they took the plane **FSF145P** from Paris (France) to Payerne (Switzerland). They moved to Zurich and met Minca H. (head of Mastermind) at Kaufleuten on the 16th of December 2022. At this time, their safehouse was located at Limmatquai Street.

After some time, they took a train to Cadenazzo, drove through Italy and navigated to reach Crete (Greece). From this point they waited three days in a safehouse. After this short break, they took a plane from Heraklion airport to Singapore. Then, they went to a safe house in Malaysia where they were intercepted thanks to our precious help to the case.

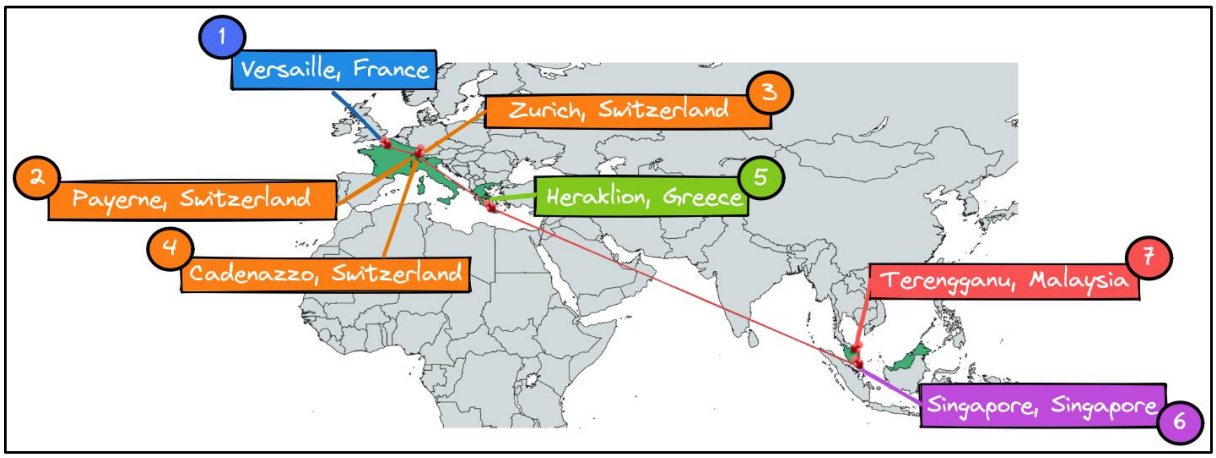


Exhibit 1 : Map of the different accessed key location (sorted by time)

This map represents all the different locations where Lucilhe and Oleg traveled. They have been sorted by time. For clarity purposes only the city and the country are displayed. More details will be given in the different categories.

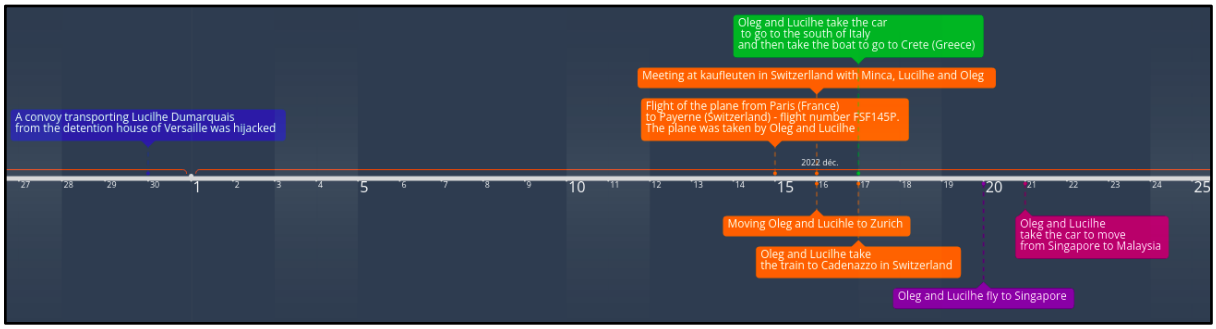


Exhibit 2 : Events timeline

Please note that the dates after the appointment are approximate. Only the gap of 3 days between the creation and the taking of the plane to go to singapore is certain.

The benefits for Mastermind are quite clear. On one hand, they have a financial objective in mind. It’s actually the source of motivation for any criminal organization. Money rules the world. We’ve been able to notice thanks to Minca H. who clearly mentioned it on the phone while we were doing an identity usurpation of Lian Nussbaumer. She also unintentionally leaked the contract arrangement with the A-Team in Mauritia to make profits out of the stock exchange. On another hand, it’s more a strategic and prosperous aim. A client always judges on the quality of the service provided. In that case, they want to give their client, Tsuzune Y. the best experience possible.

#2 Action man Analysis - Oleg VOKOLSKI

Exhibit 3 : Oleg VOKOLSKI printed picture

Individual description

- Name: **Oleg**
- Surname: **VOKOLSKI**
- Sex: **Male**
- Nationality: **Polish**
- Height: **1m88**
- Particularities & accessories:
- Right arm: **Rose tattoo and a scar**

Oleg Vokolski is the so-called **action man**. He seems to be strong, professional, brave enough to accomplish any type of mission and cold-hearted enough to kill someone if needed. That said, we managed to find the lever that will make him talk during the next police interrogation. This lever is his 19 year old daughter named **Olga VOKOLSKA**. She's a developper and appears to have developed Nelexat's website. Thanks to her social media presence, we managed to find a link between her and her father.

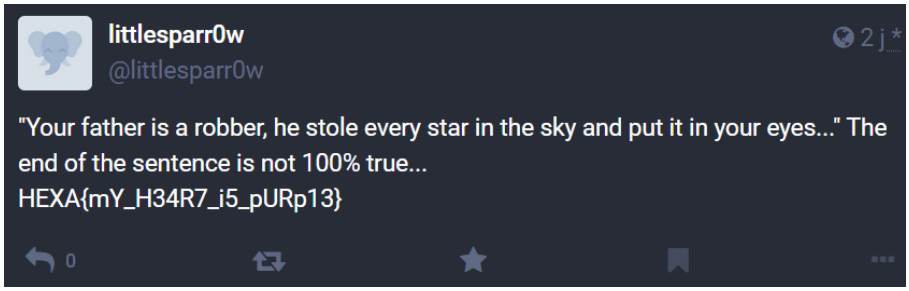


Exhibit 4 : One of Olga Vokolska's Mastodon messages

In this message she posted, she's saying that the end of the sentence is not 100% true, meaning the beginning is. Indeed, her father is not stealing stars but humans in our case eh… Also, it's essential to note that in Polska, the suffix for boys is **SKI** and **SKA** for girls. As a matter of fact, it confirms that they have the same surname, meaning they are from the same family.

Investigation Technical Details

A convoy transporting Lucilhe Dumarquais from the detention house of Versaille was hijacked on the 30th of November 2022. A picture indicating the destination of the police escort was provided (Exhibit 5). The location is the **tribunal of Versaille**, where the convo was initially heading.

Exhibit 5: Original destination of the convoy

The hijacked convoy was witnessed driving at top speed by a pedestrian that took the picture in Exhibit 6. Using the traffic sign we managed to find that they took the road **Avenue de l'Europe**.

Exhibit 6: Road taken by the hijacked convoy transporting Lucilhe Dumarquais

The investigators found the place where the "Action Man" brought Lucilhe Dumarquais. The apartment was searched and Exhibit 3 was

found. The printed email found in the bin reads that the "Action Man" first name is **Oleg** and that they took a flight.

The flight ID they took on the 14-12-2021 is **FSF145P** and its destination was **Payerne** (Switzerland) according to FlightAware (Exhibit 7-2). Two pictures are also attached for the craft of fake passports, we have the portrait of Oleg aka "Action Man".

Note: "See ya" expression is used. It is typically british.

Exhibit 7: Flight information and passport photography

JOURNAL DE L'ACTIVITE — Vous voulez une recherche complète sur l'historique de FSF145P depuis 1998? Achetez maintenant. Recevez-le dans l'heure.

Date	Avion	Provenance	Destination	Départ	Arrivée	Durée
15-12-2022	PC24	Paris-Le Bourget (LBG / LFPB)	Payerne Air Base (LSMP)	06:36PM CET	07:40PM CET	1:03

Exhibit 7-2: Flight information

The investigators found a text message and a picture attached while searching the previous safehouse (Exhibit 8). Oleg aka "Action Man" and Lucilhe Dumarquais took public transport after arriving at Payerne. Investigation on the railway network resulted in finding that the picture was taken in **Limmatquai Street** near the Münsterbrücke bridge.

Notes:
By cross-referencing the information with **The Lawyer** timeline, we discover we discover that they met Minca H. in Kaufleuten on the 16th of December 2022.

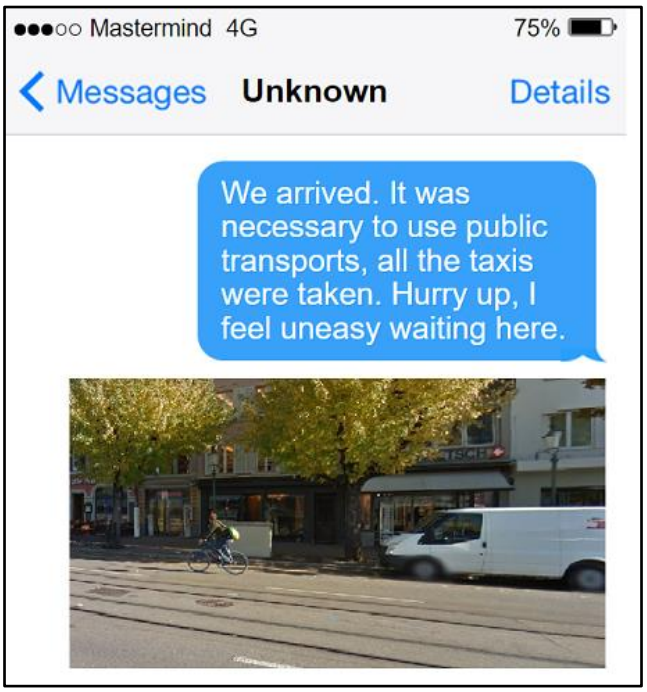


Exhibit 8: Zurich location information

In the safehouse located in Limmatquai Street, investigators found a message sent by Oleg aka "Action Man" reading that they left Zurich by train (Exhibit 9). According to the message, the trip was a direct connection and lasted exactly 3:07. Using direktbahn we determined that the train was heading to **Cadenazzo** where they will meet a contact.

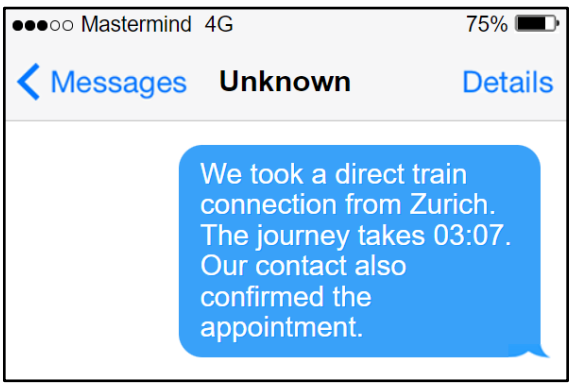


Exhibit 9: Trip information to Cadenazzo

A message read that Oleg aka "Action Man" is about to take a flight with Lucilhe Dumarquais (Exhibit 10). The metadata of the picture locate the **safehouse in Crete** (Greece) as shown in Exhibit 10-2. The airport mentioned in the message is the Heraklion International Airport but referred to as **Nikos Kazantzakis Airport**. It is located near the Heraklion Fortress.

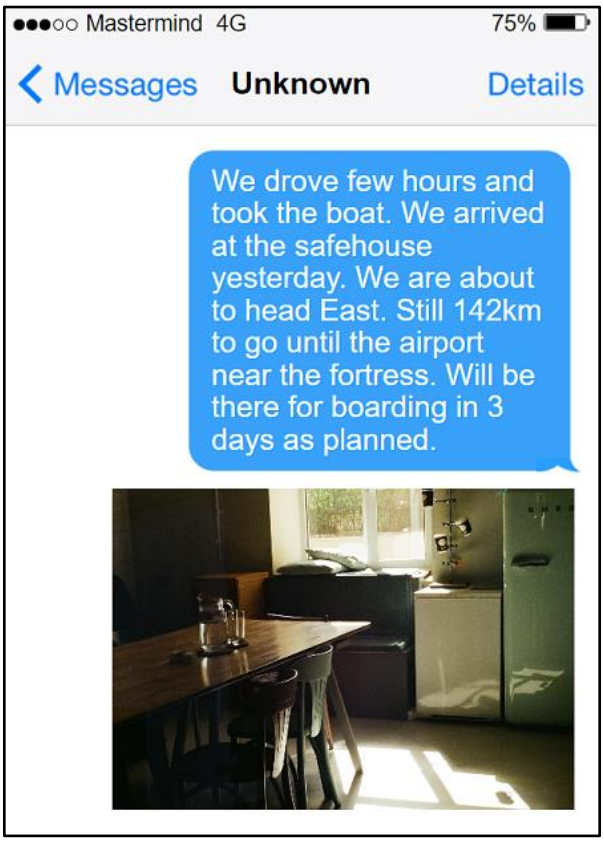


Exhibit 10: Information about airport destination

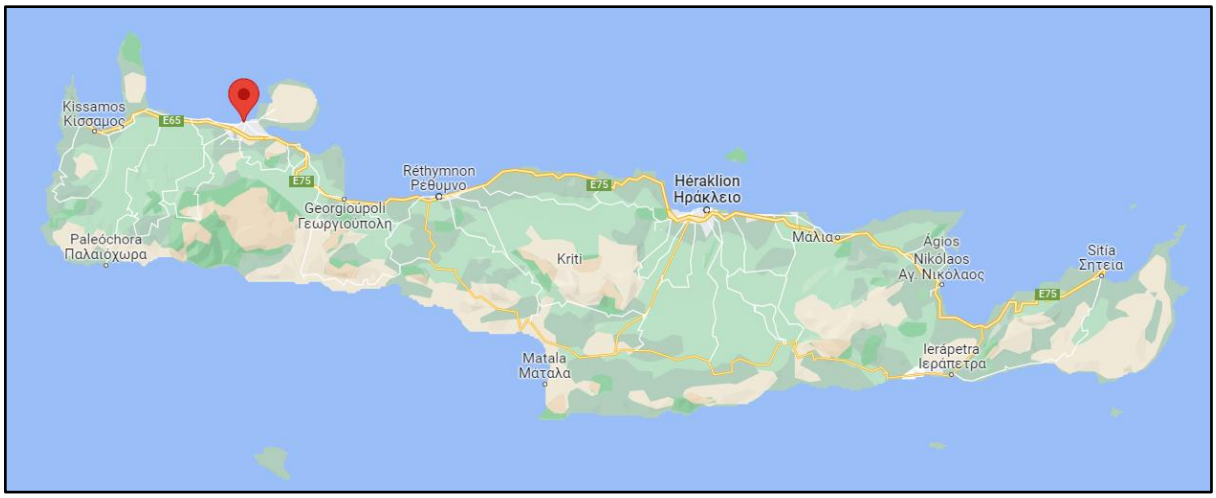


Exhibit 10-2: Location of the safehouse in Crete

Sovereign City: they landed in Singapore and hid in the neighborhood of Hougang. After that, they changed their car on the Marsiling Lane before leaving the city and heading to Johor Bahru in Malaysia.

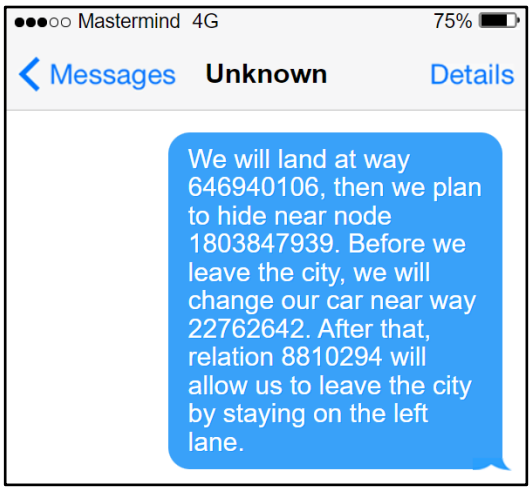
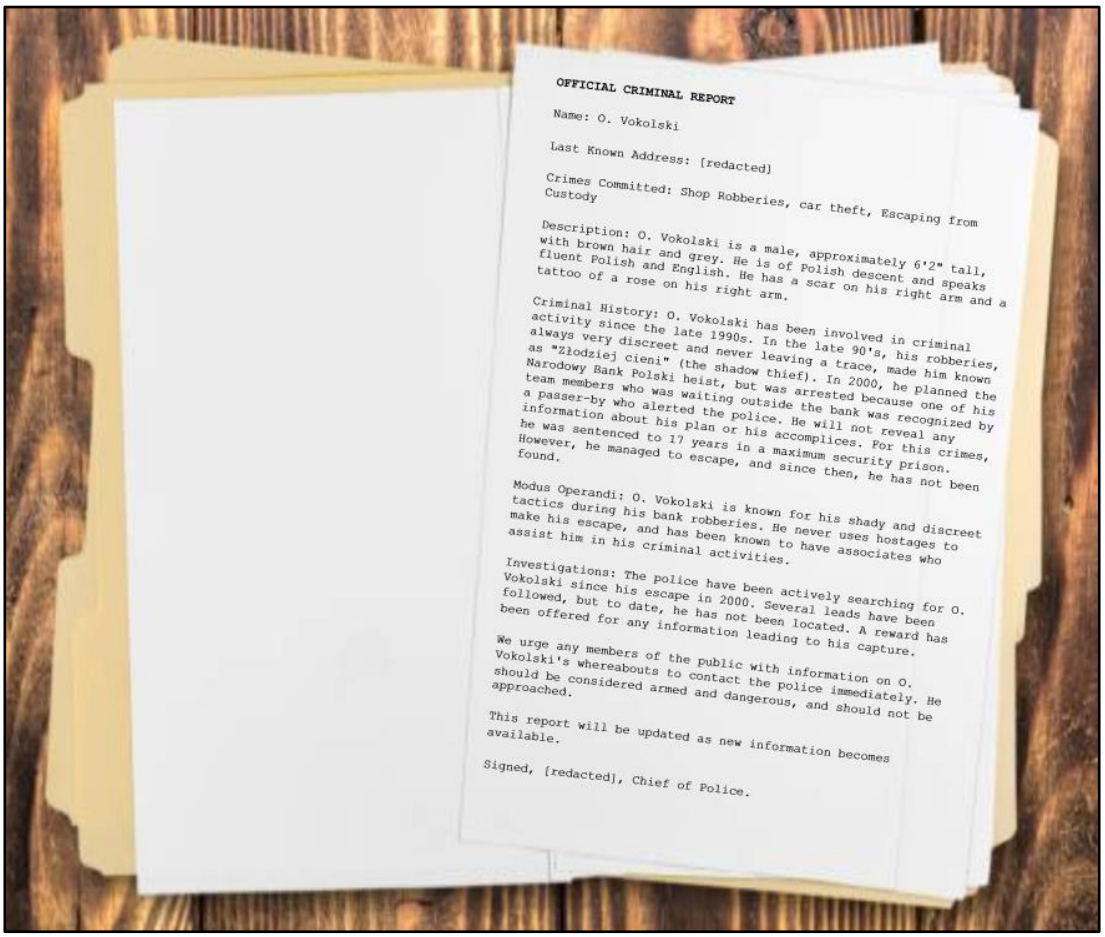


Exhibit 11: Trip planned by Oleg aka "Action Man"

Meanwhile, Interpol provided the biography record of Oleg aka "Action Man". Unfortunately, something (or someone) erased and rewrote the biography record several times. We managed to retrieve the correct file. We learned that the Action Man is actually called **Oleg Vokolski** and that he's known for the following:

- Shop robberies
- Car theft
- Escape from custody

He has been in the wild since 2000, the year when he escaped. With the Exhibit 8 and the Exhibit 3, we now have a full description of Oleg Vokolski so we are able to identify him easily.



OFFICIAL CRIMINAL REPORT

Name: O. Vokolski

Last Known Address: [redacted]

Crimes Committed: Shop Robberies, car theft, Escaping from Custody

Description: O. Vokolski is a male, approximately 6'2" tall, with brown hair and grey. He is of Polish descent and speaks fluent Polish and English. He has a scar on his right arm and a tattoo of a rose on his right arm.

Criminal History: O. Vokolski has been involved in criminal activity since the late 1990s. In the late 90's, his robberies, always very discreet and never leaving a trace, made him known as "Zlodziej cieni" (the shadow thief). In 2000, he planned the Narodowy Bank Polski heist, but was arrested because one of his team members who was waiting outside the bank was recognized by a passer-by who alerted the police. He will not reveal any information about his plan or his accomplices. For this crimes, he was sentenced to 17 years in a maximum security prison. However, he managed to escape, and since then, he has not been found.

Modus Operandi: O. Vokolski is known for his shady and discreet tactics during his bank robberies. He never uses hostages to make his escape, and has been known to have associates who assist him in his criminal activities.

Investigations: The police have been actively searching for O. Vokolski since his escape in 2000. Several leads have been followed, but to date, he has not been located. A reward has been offered for any information leading to his capture.

We urge any members of the public with information on O. Vokolski's whereabouts to contact the police immediately. He should be considered armed and dangerous, and should not be approached.

This report will be updated as new information becomes available.

Signed, [redacted], Chief of Police.

Exhibit 12: Interpol report on Oleg Vokolski aka "Action Man"

A last message about Oleg Vokolski's current location was retrieved. While investigating **The Lawyer**, we found a map with different zones in Malaysia. The Zone 4 mentioned by Oleg Vokolski aka "Action Mac" is the one near **Terengganu** (Exhibit 13-2). A soccer field and a religious building are mentioned as well as an "unsafe place". It happens that their safehouse was the **Masjid Kampung Kuala Telemong mosque** next to a police station (Exhibit 13-3).
French secret service agency, with the help of Malaysian police forces, managed to intercept and retrieve the two individuals.

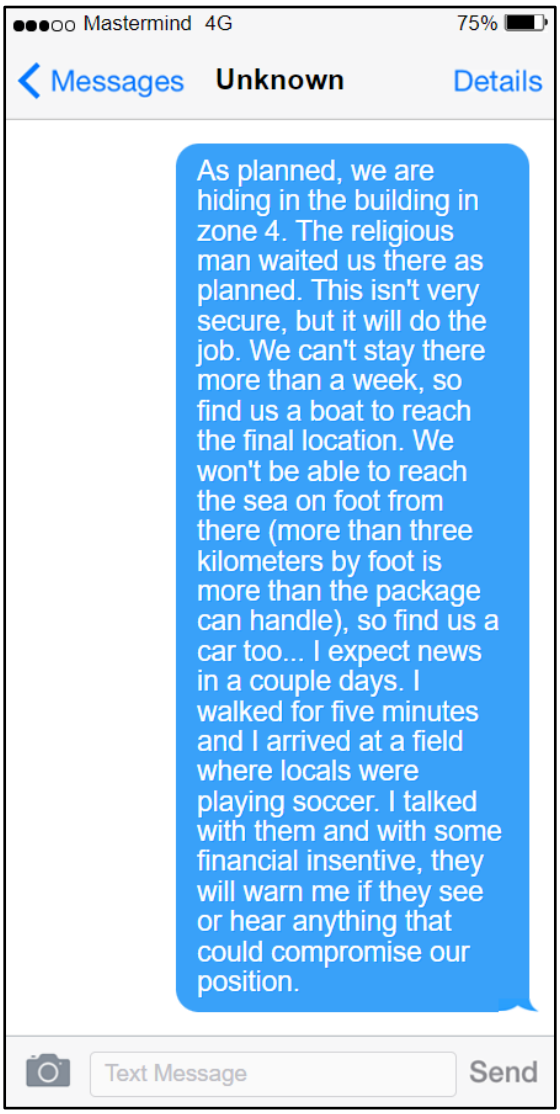


Exhibit 13: Message about the malaysian safehouse

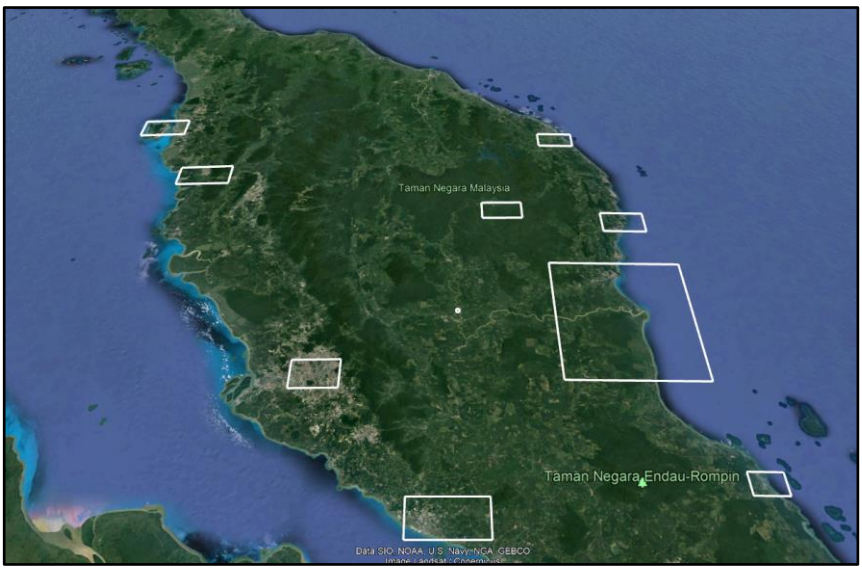


Exhibit 13-2: Malaysia map with safehouse locations

Exhibit 13-3: Safehouse location where we found L. Dumarquais and Oled Vokolski

#3 Associate Analysis - Minca H.

Exhibit 14: Minca H. robot portrait generated with AI

Individual description

- Name: **Minca**
- Surname: **H.**
- Sex: **Female**
- Nationality: **British**
- Height: **1m87**
- Facial traits / particularities: **Slavic**

- Hair: **wavy red hair with venetian reflection**
- Particularities & accessories
    - Watch model : Festina F20286/3 Timeless Chronographe 41mm 5ATM
    - Possible house location: Chelsea neighborhood, London
- Username & accounts
    - Username: **Minca H, micah_mm**
    - Email: micah_mm@proton.me

This is Minca H. She is the so-called "*long-time associate*" of **Lian Nussbaumer**, the lawyer . We've been able to recover several pieces of information on her thanks to Lian's phone we found in one of their safehouses located in Zurich. We found she went to Mauritius to sign a contract with the company *A-Team Security Ltd* in order to manipulate markets and make profits by reselling their actions. Thus, it reinforces the fact that their business is becoming more and more lucrative.

Investigation technical details

Below is the bribe of conversation that was remaining on the phone. It contained the following picture.

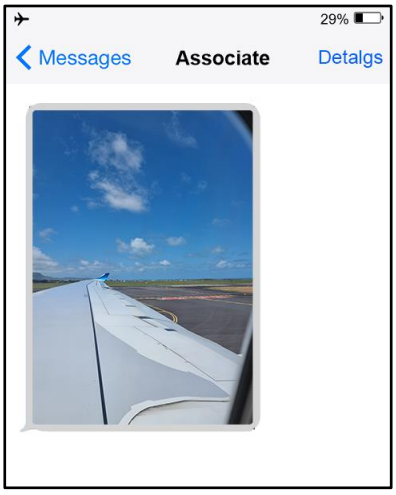
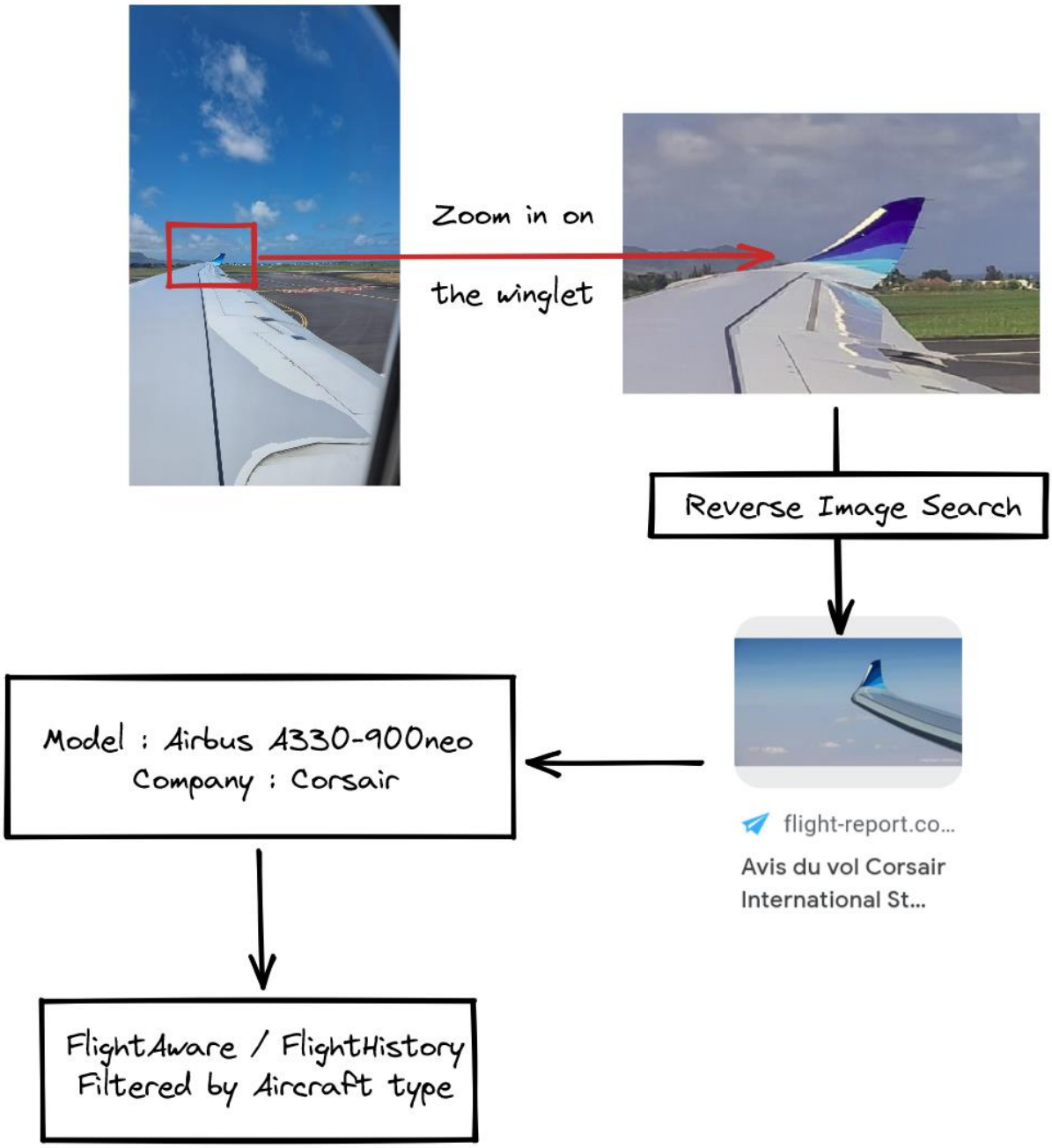
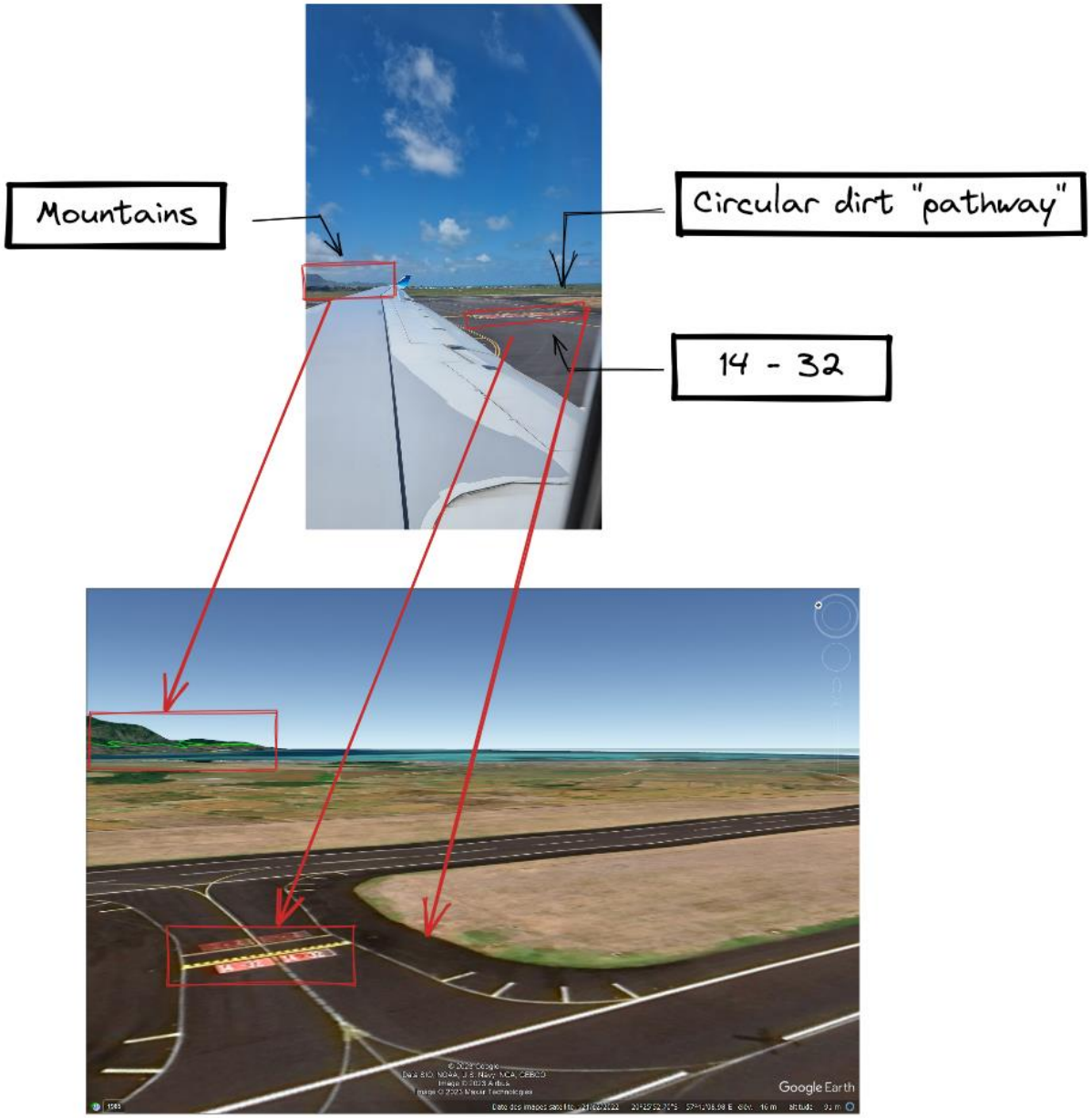


Exhibit 15: Photo sent by Minca to Lian

From there, we analyzed this picture to determine the location of Minca. Here's a quick summary of what we have been able to find.



From there, we conducted further analysis on the picture. Thanks to the landscape, we were able to make hypotheses on the airport's location which should be located on an island. We quickly found Mauritius to be a good candidate. We could confirm that thanks to the landscape as well as some information in the background like numbers on the plane track, as you can see below.



Thus, we could determine that she was in **Mauritius** at the time of the received text message. More importantly, thanks to a private source we met on this case, we know that she went to Mauritiusas she has been recognized by a Mauritian friend of ours. Indeed, she has an atypical and easily recognizable profile compared to the local inhabitants.

#4 Mastermind Analysis

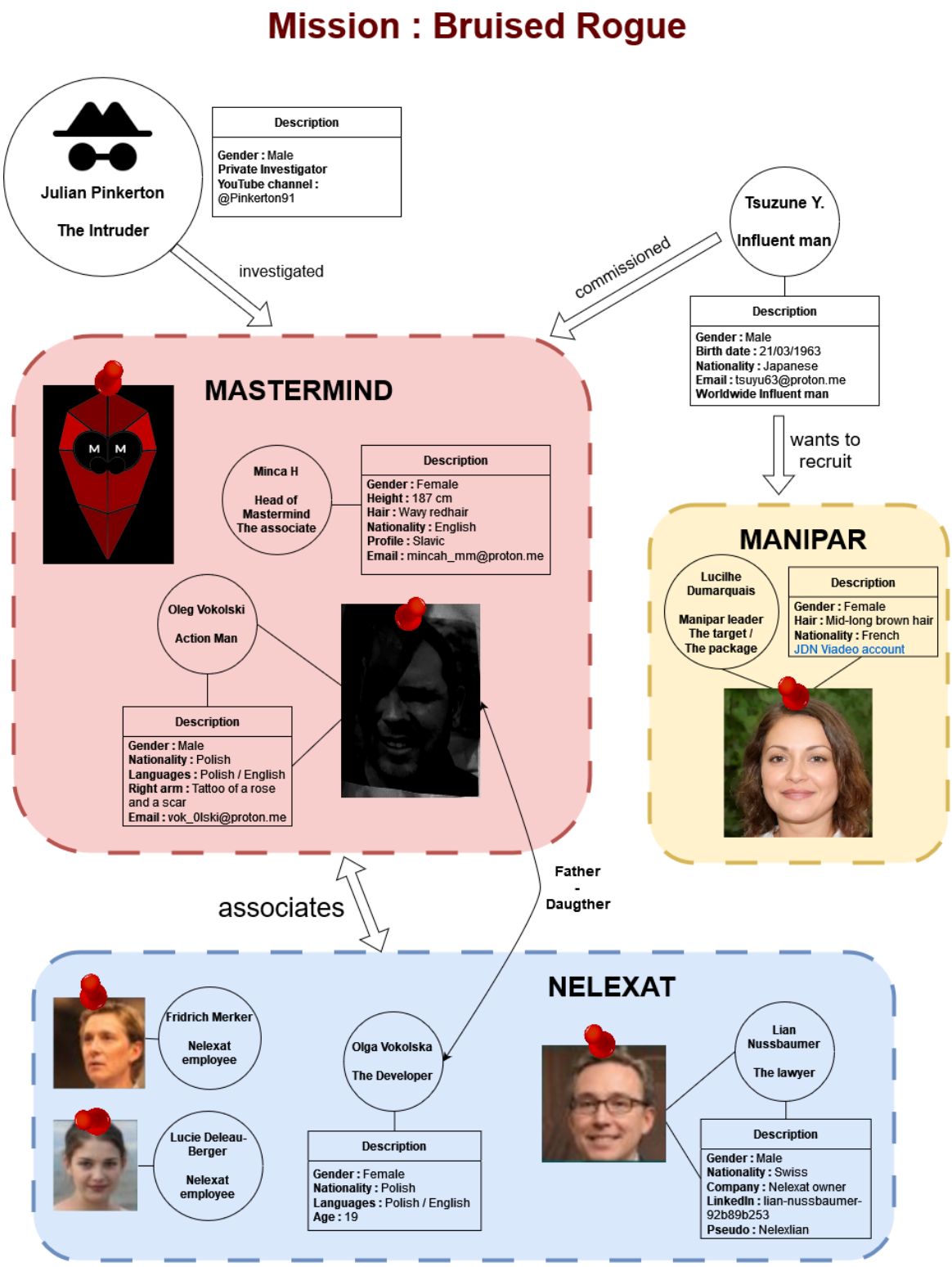


Exhibit 16: Mastermind case illustration

In this part, we want to illustrate the people who were directly or indirectly involved in this case investigation.

The worldwide influential Japanese guy who commissioned the Bruised Rogue Mission is defined as an external component of the Mastermind organization. He wanted to recruit Lucilhe Dumarquais for her skills as mentioned in the mission description.

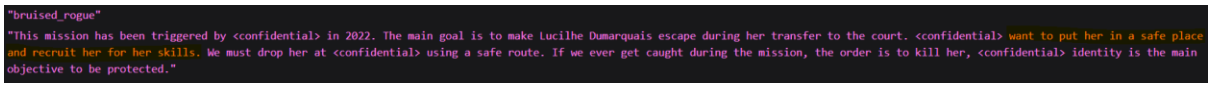


Exhibit 17: Mission purpose

We were able to retrieve some information about Minca.H. This businesswoman is the head of the Mastermind. She is an english red headed woman of 187cm, a bit "Slavic". She is linked with Oleg Vokolski who has a criminal background and he is acting like a mercenary for Minca.

Lian Nussbaumer is a Swiss man and works as a lawyer specialist in the company he runs, Nelexat. He studied international business, commercial and tax law at the University of Neuchâtel Faculty of Law. According to his linkedin profile. In addition he was Lucilhe’s lawyer and he managed to reduce her jail sentence without having to give any information about the people she was working with. We assume that Lian's defense of Lucilhe was also part of the plan to cause a movement of Lucilhe. Indeed, the trial allowed for a movement between the “Maison d'arrêt” and the court of Versailles. Also, we supposed that the people present at one of the Nelexat conferences are Lian employees but they might not be aware of the relationship between Lian and Minca. Finally, we managed to link the Nelexat developer with “Action Man” in the previous part due to their name and messages.

The intruder is also an external component who investigated the same case as us. He tried to access our investigative information but in the end we were the ones who were able to get the investigation information out of him.

Finally, as we said Lucilhe Dumarquais was freed by Mastermind to answer Tsuzune Y. request. He wanted to recruit her for her cybersecurity skills and maybe others because she was also the leader of the Manipar organization.

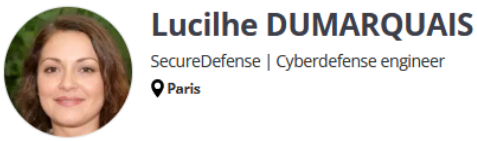


Exhibit 17: Mission purpose

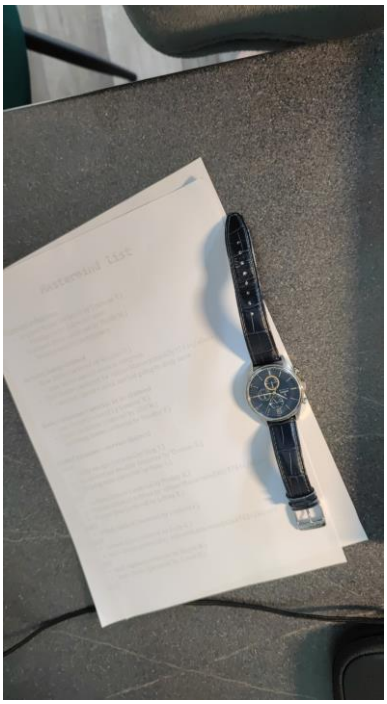
Conclusion

This new investigation case was as complex as the Manipar case last year and we hope that all the elements brought by our agents will allow the investigators and the Ministry of Justice to do their job. We will support the government in all its actions to reduce crime and provide a safer world for everyone.

Appendix

In the mission concerning The Associate we have a picture with the watch of Minca H. The information was to get the watch Model but we can see that text is written on the sheet where it lies on.

After analysis, it contains information about Mastermind organization and ongoing missions.



Current missions:
Bruised Rogue (ordered by Tsuzune Y.)
- Package to be delivered soon

Northern Silver (ordered by Basile M.)
- Waiting mission description

Service being claimed
Blue strike (ordered by Senator O.)
- Law under examination at congress

Aero Fusion (ordered by <alias>MastermindAlly3743</alias>)
- Contract signed - stock market going to drop soon

Ended mission - service to be claimed
- Lost ???? (ordered by General K.)
- Final encounter (ordered by CEO M.)
- Lightnening ascent (ordered by Senator P.)

Ended mission - service claimed
2000
- ???y escape (ordered by Oleg V.)
- vertised shadow (ordered by Thomas K.)
- Su?ping echo (ordered by Hans L)

2001
- Carbon contact (ordered by Preddy K.)
- Private convoy (ordered by <alias>MastermindAlly3743</alias>)
- Pr????? kiss (ordered by Jeffrey E.)

2002
- Fried chicken (ordered by Gustavo F)

2003
- Drown lake (ordered by Lady G.)
- New down (ordered by <alias>MastermindAlly3743</alias>)

2004
- Red caption (Mayor N.)
- New order (ordered by Coum D.)

HEXA OSINT CTF V2

X