ESC-32-33-12

Final Exam Report – Appareils Mobiles et Smartphone Apps

Caroline Moutiez

UNIL | École des Sciences Criminelles

Introduction

On the 25th of February 2019, two persons were arrested in Lausanne : Mr Francesco Sforza and Mr Tim Pressive. They were both subject to an international arrest warrant as they are suspected to be part of a criminal organization responsible for stealing the US Declaration of Independence.

Caroline Moutiez was mandated to answer five questions and present the results in a report for the 31st of May 2019 (**Annex I**) :

1. Where was Mr Sforza in January and February 2019 ?
2. Where was Mr Pressive in January and February 2019 ?
3. Did Mr Sforza and Mr Pressive meet during this period?
4. Did Mr Sforza and/or Mr Pressive take part in any illegal activities during this period?
5. In particular, are Mr Sforza and/or Mr Pressive implicated in the theft of the US Declaration of Independence?

To answer these questions, different extractions were performed on two smartphones :

- ESC-32-33-12_P001 : a Samsung Galaxy S6 Edge, that was seized on Mr Tim Pressive
  - ESC-32-33-12_P001_R001 : a logical extraction was performed, but no operable data was obtained (25 February 2019)
  - ESC-32-33-12_P001_R002 : the phone was rooted and a physical extraction was performed (26 February 2019)
- ESC-32-33-12_P002 : an iPhone 6, that was seized on Mr Francesco Sforza
  - ESC-32-33-12_P002_R001 : a logical extraction was performed (1 March 2019)
  - ESC-32-33-12_P002_R002 : the phone was rooted and a file system extraction was performed (5 April 2019)
  - ESC-32-33-12_P002_R003 : the content of the Telegram application was captured with the screen recording function of the phone

The following table shows the communications in the context of this case :

Date	From	To	Annex
17 May 2019	Group of experts	The Prosecutor	**Annex II**
20 May 2019	The Prosecutor	Group of experts	**Annex III**

The chosen propositions are :

1. *Where was Mr Sforza in January and February 2019 ?*

H_1 : Mr Sforza was in Switzerland and in the United States in January and February 2019.
H_2 : Mr Sforza was somewhere else in January and February 2019.

2. *Where was Mr Pressive in January and February 2019 ?*

H_1 : Mr Pressive was in Switzerland and in the United States in January and February 2019.
H_2 : Mr Pressive was somewhere else in January and February 2019.

3. *Did Mr Sforza and Mr Pressive meet during this period ?*

H_1 : Mr Sforza and Mr Pressive met during this period.
H_2 : Mr Sforza and Mr Pressive did not meet during this period.

4. *Did Mr Sforza and/or Mr Pressive take part in any illegal activities during this period ?*

H_1 : Mr Sforza and/or Mr Pressive took part in illegal activities during this period.
$H_{1,1}$: Mr Sforza took part in illegal activities during this period.

$H_{1,2}$: Mr Pressive took part in illegal activities during this period.

H_2 : Mr Sforza and/or Mr Pressive did not take part in any illegal activities during this period.
$H_{2,1}$: Mr Sforza did not take part in any illegal activities during this period.
$H_{2,2}$: Mr Pressive did not take part in any illegal activities during this period.

5. *In particular, are Mr Sforza and/or Mr Pressive implicated in the theft of the US Declaration of Independence ?*

H_1 : Mr Sforza and/or Mr Pressive are implicated in the theft of the US Declaration of Independence.
$H_{1,1}$: Mr Sforza is implicated in the theft of the US Declaration of Independence.
$H_{1,2}$: Mr Pressive is implicated in the theft of the US Declaration of Independence.

H_2 : Mr Sforza and/or Mr Pressive are not implicated in the theft of the US Declaration of Independence.
$H_{2,1}$: Mr Sforza is not implicated in the theft of the US Declaration of Independence.
$H_{2,2}$: Mr Pressive is not implicated in the theft of the US Declaration of Independence.

Methodology

The data from the extractions was retrieved from an external hard drive (ESC-32-33-12_National_Treasure.zip). The compressed file was unzipped, and the resulting folder was copied. The analysis was performed on the copied data to prevent the original data from being modified and secure the integrity of the case's data.
To analyze the data, various tools were used. The files from the file system extraction were previewed via the windows file explorer and using JPEG Snoop for the images files. The extractions made with Cellebrite could be displayed with UFED Reader. To view the databases files, the software DB Browser for SQLite was used and PListExplorer for the .plist files.
The GPS coordinates for the locations were entered in Google Maps in order to visualize the corresponding address.
Finally, some timestamps formats, especially those that can be found in databases files, could be converted in a readable human format using the software DCode.
The diagrams in annex were created using i2 Analyst's Notebook.

The process that was followed for analyzing the data is described in the document Smartphone Forensic Analysis, Step-by-Step (Casey and Maguire, 2015).
First, the different associated accounts were searched for the two phones. Then, the focus was on the applications installed. The content of the databases and the media files was analyzed.
After the analysis phase, a comparison between the data from the two phones is made and the information extracted from the analysis was crossed. This step is important for the reconstruction of the events.
To finish, an evaluation is performed based on the information that was found and the degree of confidence that the expert puts in these. This allows to review the probability of observing the observations under each proposition.

Note : The two smartphones are set on the America/New York time zone (UTC-5). However, all the timestamps will be presented in UTC+0 time zone to ensure the consistency between the devices and the files from the extraction and harmonize the reconstruction of the events.

Results

The following table presents the different accounts and usernames used on the two devices :

Samsung Galaxy S6 Edge (P001)	iPhone 6 (P002)
Francesco Sforza	Tim Pressive
Francesco Sforz	Obi Wan Kenobi
Han Solo	+18572149152
+41792245315	tim.pressive@icloud.com
+15712749998	tpressive@gmail.com
sforzafrancesco01@gmail.com	gokenobi66@gmail.com
falconsolo1m@gmail.com	helpdesk.nara@gmail.com
George Anderson	
abigailchase76@gmail.com	

The links between these accounts are presented in a Relational Diagram to help understand the connection between the entities mentioned in the Results (**Annex IV**).

The results are presented here in a chronological order, according to the timeline that was reconstructed for a better understanding of the case. To help the comprehension of the results, a diagram showing the timeline of the main events is provided in **Annex V**.

Some screenshots of messages were put in the **Annex VI** to not weigh down the presentation of the results.

On the 25th of January 2019, there are SMS messages received on the Samsung from the Swiss phone service provider Swisscom. This leads to think that the owner of the Samsung was in Switzerland.

One of the first relevant information on the iPhone is an event in the calendar name "Jedi Order", that can be observe in the Calendar's database "Calendar.sqlite.db". The event is called "Meeting G. Secura" and is set for the 31/01/19 at 14:00:00, at the address : 77 Massachusetts Ave, Cambridge, MA 02139, United States".
By crossing with the location of the first photos, the owner of the iPhone was in Cambridge, Massachusetts on the 30th and the 31st of January. However, nothing could link the phone at place of the meeting at 14:00.
On the 1st of February, the location of the photos shows that the owner of the iPhone was in Boston, Massachusetts.

In the conversation on WhatsApp between "Francesco Sforza" and "Tim Pressive" (the content can be seen in both phone's extraction), it is possible to learn that "Tim Pressive" is in the United States and Francesco intends on joining him there : "Should I worry and take lots of warm things?" (31/01 at 06:39), "I'm getting everything ready to join you" (01/02 at 19:30), from "Tim Pressive" "Nice have a safe trip to Washington! I'm flying there on Sunday" (01/02 at 20:33.
On the 3rd of February, the location of photos places the owner of the iPhone in Washington around 00:20:00.
A location of a photo places the owner of the Samsung in Washington at 17:59:49.

On the 4th of February, a SMS message is received on the Samsung at 15:42:21 from the phone operator service T-Mobile. This message indicates that the owner changed the SIM card (Swisscom) to an American phone number (T-Mobile).
Also, in WhatsApp, a few minutes later the phone number changes at some point, and "Han Solo" tells "Tim Pressive" that he got a new number (see **Figure 1 of Annex VI**).
This is consistent with the line in the page "Extraction Summary" when opening the UFED Reader for the Samsung ; saying that there was a SIM card change.

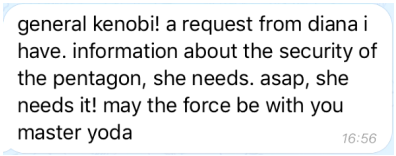
The owner of the iPhone connects to a wifi called "FlyReagan", which is the wifi of the Reagan National Airport, in Washington at 16:17:00. The iPhone then connects to a wifi called "gogoinflight", which is an in-flight wifi service.
The location of a photo on the iPhone indicates that the owner was at the Reagan National Airport at 16:38:36.
The location of a photo on the Samsung indicates that the owner was at the Reagan National Airport at 19:20:10.
Then the iPhone is located via a photo in Orlando, Florida at 19:38:39.
At 19:38:09, a photo's GPS coordinates locates the owner of the Samsung in Orlando, Florida.
The two suspects flew from Washington to Orlando, Florida on the 4th of February.

On the 5th of February, according to the Telegram conversation between "Wonder Woman" and the two phones, the owner of the phones met a waitress called Michele who was supposed to hand them a package : a USB stick. This USB stick, according to "Wonder Woman" contains a piece of malware that retrieves data and put it on the key (see **Figure 2 of Annex VI**).
A photo of a USB stick on the Samsung shows with its GPS position that the owner was at a restaurant called Krystal at 13:14:30. But nothing on the iPhone locates the owner of the iPhone was there. In the Telegram group with the two devices and "Wonder Woman", "Tim Pressive" says "We met with Michele" (at 13:14), which supports the location above.
After that, there are photos taken from inside a car (passenger seat) that locates the owner of the Samsung at different places in Florida. He was at the Kennedy Space Center (KSC) in Florida at least from 14:11:15 to 21:26:08.
A series of photos places the owner of the iPhone also at KSC at least from 15:15:14 and 21:26:13. The last photos mentioned here for each phone show a very similar content : a plane in an exhibition, from the same point of view. However, the photos are not the same since the shape of the people in front of the plane are not at the same place.
A piece of a Telegram conversation between the two devices describes the event when the owner of Samsung is placing the USB Key at KSC while the owner of the iPhone watches for guards (see **Figure 3 of Annex VI**).

On the 7th of February at 18:01:06, the iPhone auto connects to the wifi "FlyReagan" after connecting to "gogoinflight". This information indicates that the owner was at the Reagan National Airport of Washington.
There isn't any indication concerning the Samsung.
However, "Francesco Sforza" sends messages on WhatsApp at 17:26 to "Tim Pressive" : "Gotta love wifi on the plane and last minute check-ins", "I know I could just walk up to your seat and tell you". The content of these messages suggests that they are both in the same plane.

On the 8th of February, at 23:45:22, a photo on the Samsung is taken, showing a basketball game in the stadium Capital One Arena in Washington.
At 00:13:20 (the 9th of February), a similar photo is taken on the iPhone, from the same point of view, but the photos are not the same.

On the 9th of February at 15:56, "Wookie Translator" (which signs "master yoda" in its message) gives a mission to "Obi Wan Kenobi" :



Then, "Tim Pressive" informs "Han Solo" on Telegram that they were given a new mission by "Master Yoda" (see **Figure 4 of Annex VI**). "Tim Pressive" tells "Han Solo" to meet at the WWII memorial around 16:50.

The iPhone was located at the World War II Memorial in Washington using the GPS coordinates of the photo IMG_0061.jpg, at 16:53:00. Moreover, the photo shows something that seems to be a commemorative plaque in a park. This is consistent with its location in the World War II Memorial, since, when using the function "street view" on Google Maps on the location, the same commemorative plaque can be spotted. "Han Solo" sends to "Tim Pressive" on Telegram : "Now at the memorial" with a photo the commemorative plaque also at 16:52.
After 20 :25, both phones are located with photos' GPS coordinates close to the Pentagon in Washington.

On the 10th of February, "Obi Wan Kenobi" contacts "Wonder Woman" on Telegram regarding her need for intel and sends her pictures. Those pictures are the one mentioned above.

On the 12th of February, at 18:50:46, the iPhone is located at the Steven F. Udvar-Hazy Center, Air and Space Musem Pkwy (Chantilly, VA 20151, United States) with a photo. The Samsung is located at the Steven F. Udvar-Hazy Center, Air and Space Musem Pkwy (Chantilly, VA 20151, United States) at 18:51:22.
The two photos are similar ; they both show the same plane from the same point of view.

On the 13rd of February at 16:28, "Wonder Woman" charges "Han Solo" and "Tim Pressive" to retrieve the US Declaration of Independence :

```
De: From: 695862679 Wonder Woman
Horodateur: 13.02.2019 16:28(UTC+0)
App Source: Telegram (41792245315)
Corps:
Hi guys!
I need you again...
I have intel telling me that there is an invisible map behind the Declaration of Independence !!
I'll need to take a look at it!
Could you take care of it ?
```

From this day, an important amount of google searches are found in the Google Chrome History of the iPhone on the matter of the Declaration and its preservation. It appears that the owner was looking for where the US Declaration of Independence was stored :

On the 14th of February, from 00:24, "Han Solo" and "Tim Pressive" exchange about the National Archives and an event to go in (see **Figure 5 of Annex VI**).
They found an event and want to find the email account of the organizer Abigail Chase ; the event is called "Inauguration of Restored Bill of Rights Display", when opening the link on Facebook (see **Figure 6 of Annex VI**).

Abigail Chase's profile on LinkedIn is consulted the at 02:03:23 on the iPhone. There is a screenshot of Abigail Chase's profile on LinkedIn on the Samsung taken at 02:07:04. This is how "Han Solo" found her email, as it can be read in the WhatsApp conversation between "Han Solo" and "Tim Pressive" :

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 02:07(UTC+0)
App Source: Telegram (41792245315)
Corps:
Got the email on linkedin
```

In a gmail database found in the Samsung, there is an email addressed to Abigail Chase from the mail helpdesk.nara@gmail.com from "IT National Archives". The content of the email informs Abigail Chase that there was a security breach in the personal email accounts of some employees of the NARA.
At 22:27, Abigail Chase contacts live:helpdesk.nara on Skype : "Hi, Helpdesk NARA, I'd like to add you as a contact".
At 22:28:01, there was a call on Skype between live:helpdesk.nara and Abigail Chase that lasted 01:41 minutes.
At 22:30, "Tim Pressive" informs "Han Solo" on WhatsApp that he just did a call on Skype with Abigail Chase (see **Figure 7 of Annex VI**).
At 22:37:50, the gmail account from Abigail Chase (abigailchase76@gmail.com) is opened. At 22 :44 :40, the website Bitwarden Web Vault is opened (https://vault.bitwarden.com/#/). At 22:46:43, the page https://vault.bitwarden.com/@/vault is opened. An email from hello@bitwarden to abigailchase76@gmail.com informs her that another device logged into her account at 22:46, which supports the previous observations.
The conversation between "Han Solo" and "Tim Pressive" in Telegram supports these observations.
At 22:38, so right after the gmail account is accessed, "Han Solo" tells "Tim Pressive" that he logged in (see **Figure 8 of Annex VI**).

"Obi Wan Kenobi" sends to "Wonder Woman" on Telegram a message with the address where the USB key was dropped (see **Figure 9 of Annex VI**). The USB key was left in a mailbox on Raoul Wallenberg SW, Washington.

On the 15th of February, from 17:46 to 18:15, there is a series of audios sent between "Han Solo" and "Tim Pressive" on Telegram. Those audios can be found in the file system extraction of the Samsung as audio files that can be played. The timestamps match the ones of the Telegram's messages and the content matches the audios that can be seen in the screen recording of the iPhone .
When retranscribing the content, the conversation appears. They are describing what they do during the event at the National Archives. "Han Solo" is entering the vault using the password and retrieves the US Declaration of Independence, while "Tim Pressive" watches for security.
The iPhone connects to a wifi called "National Archives I" at 17:58:06.
There is also a wifi connection to "National Archives I" on the Samsung, but there is no timestamp.
This date is consistent for what took place at NARA on the 15th of February. In a conversation on Telegram between "Han Solo" and "Tim Pressive" that took place on the 14th of February, they conclude with "That's perfect for tomorrow!". It supports the proposition that the theft was planned for the 15th of February :

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:48(UTC+0)
App Source: Telegram (41792245315)
Corps:
That's perfect for tomorrow!
----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 22:49(UTC+0)
App Source: Telegram (41792245315)
Corps:
Yep I think we have everything we need
```

On the 16th of February, "Tim Pressive" informs "Wonder Woman" on the group on Telegram that they have the US Declaration of Independence and sends a photo of it the next day (IMG_0094.jpg). The messages and the photo are illustrated in the **Figure 10 of Annex VI**.
The last message implies that "Tim Pressive" and "Francesco Sforza" will be in Europe from the 25th or the 26th of February.

On the 23rd of February, there are messages between "Francesco Sforza" and "Tim Pressive" on WhatsApp, but they provide no information.

Discussion

There was no really inconsistency between the information found on both devices and also between the different extractions. The timeline of the events can be constructed easily by crossing the data.
However, there was some aspects that needed further searches to explain. They are presented in the paragraphs below.

The accounts and usernames associated to the phones show that the two suspects may have switch their phones with each other before the arrestation. Another explanation could be that they used the name of the other one on their phone. However, the observation of the photos on the phones and the photo of the suspect Tim Pressive provided by the prosecutor (see Annex III) indicates that the first explanation is most likely since the selfies on the iPhone allow to link the user of the iPhone with the suspect Tim Pressive.
Linking accounts to a physical identity is difficult. It requires contextual information. As said above, a link can be done between Tim Pressive and the accounts on the iPhone because a photo of the suspect was provided by the prosecutor. But the link between Francesco Sforza and the accounts on the Samsung is less certain, even if there is similarity between the names this is not enough.

Another difficulty is that on the Samsung, the conversations on Telegram are with "Han Solo" and "Tim Pressive" whereas on the iPone they are with "Francesco Sforza" and "Obi Wan Kenobi", names that are associated to the same phone numbers respectively. The screen recording of the content of the application Telegram (ESC-32-33-12_P002_R003) shows that on the Samsung, the name chosen in the application by the owner is "Obi Wan Kenobi". While searching on the internet[1] an explanation is found : when the person is in the phone's contacts, the name on the application is automatically changed to the name in the contacts. This can be why even if they chose a display name, as there are saved in each other's contacts, the name on the other one's phone will not be the same. Or it's also possible that they simply changed locally the names to "Francesco Sforza" and "Tim Pressive" instead of keeping "Han Solo" and "Obi Wan Kenobi" respectively.

"Francesco Sforza" told "Tim Pressive" that he hacked Abigail Chase. One method that seems consistent with the observations is social engineering. With this kind of attack, no technologic vulnerability is used at the beginning, but simply a conversation between two persons where one tries to obtain information pretending to be someone else. In this case, a gmail address helpdesk.nara@gmail.com was created on the iPhone. There was an email sent to Abigail Chase saying that there has been a security breach. Later, "live:helpdesk.nara" calls Abigail Chase on Skype. There is a message from "Tim Pressive" to "Francesco Sforza" saying that he spoke with

[1] https://www.reddit.com/r/Telegram/comments/52tl8x/telegram_automatically_set_my_contact_names_based/

her, so this is consistent. He then continues by saying that she gave him her gmail password and that she uses a password manager service.
On the Samsung, there are traces of a gmail connection to Abigail Chase's email address.
"Francesco Sforza" tells "Tim Pressive" that the password for Bitwarden was saved in Chrome's password managers. After that, the Samsung owner goes on Bitwarden on internet and logs in. He recovers the password for the Vault's door.
So, by pretending at the beginning that someone from the IT helpdesk contacts Abigail Chase for a security matter, she communicates her password and they managed to, from one step to another, recover the password for the vault's door.

Evaluation

As a reminder, those are the chosen propositions :

1. *Where was Mr Sforza in January and February 2019 ?*

H_1 : Mr Sforza was in Switzerland and in the United States in January and February 2019.
H_2 : Mr Sforza was somewhere else in January and February 2019.

2. *Where was Mr Pressive in January and February 2019 ?*

H_1 : Mr Pressive was in Switzerland and in the United States in January and February 2019.
H_2 : Mr Pressive was somewhere else in January and February 2019.

3. *Did Mr Sforza and Mr Pressive meet during this period ?*

H_1 : Mr Sforza and Mr Pressive met during this period.
H_2 : Mr Sforza and Mr Pressive did not meet during this period.

4. *Did Mr Sforza and/or Mr Pressive take part in any illegal activities during this period ?*

H_1 : Mr Sforza and/or Mr Pressive took part in illegal activities during this period.
$H_{1,1}$: Mr Sforza took part in illegal activities during this period.
$H_{1,2}$: Mr Pressive took part in illegal activities during this period.

H_2 : Mr Sforza and/or Mr Pressive did not take part in any illegal activities during this period.
$H_{2,1}$: Mr Sforza did not take part in any illegal activities during this period.
$H_{2,2}$: Mr Pressive did not take part in any illegal activities during this period.

5. *In particular, are Mr Sforza and/or Mr Pressive implicated in the theft of the US Declaration of Independence ?*

H_1 : Mr Sforza and/or Mr Pressive are implicated in the theft of the US Declaration of Independence.
$H_{1,1}$: Mr Sforza is implicated in the theft of the US Declaration of Independence.
$H_{1,2}$: Mr Pressive is implicated in the theft of the US Declaration of Independence.

H_2 : Mr Sforza and/or Mr Pressive are not implicated in the theft of the US Declaration of Independence.
$H_{2,1}$: Mr Sforza is not implicated in the theft of the US Declaration of Independence.
$H_{2,2}$: Mr Pressive is not implicated in the theft of the US Declaration of Independence.

To evaluate the different observations under the propositions, the verbal scale from ENFSI (ENFSI, 2015) was used.

The questions of the mandate mention two persons : Francesco Sforza and Tim Pressive. However, when analyzing digital traces, the link to a physical person is not direct. It is difficult to link accounts and pseudonyms with certitude to a person without contextual information.
This is why the following propositions are also interesting to evaluate :

H1 : The Samsung belongs to Francesco Sforza.	**H1** : The iPhone belongs to Tim Pressive.
H2 : The Samsung belongs to someone else.	**H2** : The iPhone belongs to someone else.

At the moment of the arrestation, the Samsung is seized on the suspect Tim Pressive and the iPhone is seized on the suspect Francesco Sforza. However, when searching the accounts and photos, it can be seen that on the Samsung there are selfies of the same man and some accounts contains the name "Francesco Sforza". No photo of the suspect Francesco Sforza was provided so there is no way to know if the selfies represent the suspect. There isn't a lot of information to link the Samsung and Francesco Sforza. This allows to give a weight to the propositions above.
The observations are more probable given the proposition H1 ("The Samsung belongs to Francesco Sforza) rather than the proposition H2 ("The Samsung belongs to someone else.").
When searching the accounts and photos on the iPhone, it can be seen that there are selfies of the same man and he looks very similar to the person on the photo of Tim Pressive provided by the prosecutor. Moreover, some accounts contain the name "Tim Pressive".
The photo known to represent Tim Pressive allows a stronger link between the iPhone's owner and Tim Pressive. **The observations are much more probable given the proposition H1 ("The iPhone belongs to Tim Pressive.) than the proposition H2 ("The iPhone belongs to someone else.").**

The Samsung device was connected to a Swiss network in January and February and had a Swiss phone number. The phone was receiving SMS messages from the Swiss phone service provider Swisscom. Various locations associated to the photos on the Samsung shows that the phone's owner travels to Washington on the 3rd of February. On the 4th of February, another SIM card is put in the phone and the device now has an American phone number, provided by the American phone service provider T-Mobile, as the SMS messages sent by the latest shows and "Francesco Sforza" tells "Tim Pressive" in a WhatsApp conversation. The phone's owner travels in February in Florida and goes back to Washington. This is supported by various photo's location and the content of messages. No location can place the owner in Switzerland at the end of February, but a message indicates that it is planned. Mr Sforza was arrested in Lausanne, Switzerland on the 25th of February.
Each step of his travel is easily constructed and there is no inconsistency between the diverse sources of information.
No information show that the owner of the Samsung was somewhere else during that period.
This leads to think that **the observations are much more probable given the proposition H1 ("Mr Sforza was in Switzerland and in the United States in January and February 2019.") than the proposition H2 ("Mr Sforza was somewhere else in January and February 2019.").**

The owner of the iPhone is in the United States in January. He travels to Cambridge, Massachusetts and Boston, Massachusetts. He then travels to Washington on the 3rd of February. The flights are supported by the wifi connections to the Reagan National Airport of Washington and the photos' location. He goes to Florida at the beginning of February and then goes back to Washington. No location can place the owner in Switzerland at the end of February, but a message indicates that it is planned. Mr Pressive was arrested in Lausanne, Switzerland on the 25th of February.
Again, each step of his travel is easily constructed and there is no inconsistency between the diverse sources of information.

No information show that the owner of the iPhone was somewhere else during that period. This leads to think that **the observations are much more probable given the proposition H1 ("Mr Pressive was in Switzerland and in the United States in January and February 2019.") than the proposition H2 ("Mr Pressive was somewhere else in January and February 2019.").**

By crossing the timestamp, the very similar content of photos at close hours, the messages, and photos' location, it can be seen that the owner of the Samsung and the owner of the iPhone met multiple times during February. These meetings are illustrated with red links on the spatiotemporal diagram of **Annex V**.
The multiplicity of the sources of information concording leads to conclude that **the observations are far more probable given the proposition H1 ("Mr Sforza and Mr Pressive met during this period") than the proposition H2 ("Mr Sforza and Mr Pressive did not meet during this period.").**

Two illegal activities happened during February.
The first one is the use of a malware contained on a USB key to retrieve information from the Kennedy Space Center internal network. Both device's owners were put on the mission via the Telegram group with "Wonder Woman". GPS location from photos and the audios where each describes what they do put the two owners at the Kennedy Space Center on the 5th of February.
The second one is the theft of the US Declaration of Independence. On the iPhone's web history, there are multiple searches on the Declaration and where it is stored. The Samsung's owner found the email address of the organizer of an event that took place on the 15th of February at the National Archives and Records Administration. The phone's owners then use a type of attack called "social engineering" on the organizer of the event Abigail Chase. In the end, they managed to retrieve the password for the vault's door logging as Abigail Chase in her password manager.
The amount of details on how they proceeded that can be seen in the conversations between "Francesco Sforza" and "Tim Pressive", and the concordance with the web history and cache of the iPhone and the ones from the Samsung that shows the connections on Gmail and Bitwarden as Abigail Chase's accounts, and the trace of the Skype call, lead to say that **the observations are far more probable given the proposition H1 ("Mr Sforza and/or Mr Pressive took part in illegal activities during this period.") than the proposition H2 ("Mr Sforza and/or Mr Pressive did not take part in any illegal activities during this period."). The observations support both sub-propositions ($H_{1,1}$ and $H_{1,2}$)** since both devices can be linked to the two illegal activities that took place, and from the data it appears that they were together the two times.

As mentioned previously, one of the illegal activities that took place is the theft of the US Declaration of Independence. For the same reasons, **the observations are far more probable given the proposition H1 ("Mr Sforza and/or Mr Pressive are implicated in the theft of the US Declaration of Independence.") than the proposition H2 ("Mr Sforza and/or Mr Pressive are not implicated in the theft of the US Declaration of Independence."). Both sub-propositions $H_{1,1}$ and $H_{1,2}$ are strongly supported by the observations. But the observations provide very strong support for $H_{1,2}$** because "Tim Pressive" sends "Wonder Woman" a photo showing the Declaration of Independence and says that there is nothing behind it. This indicates a possession and a potential contact between Tim Pressive and the Declaration of Independence. It might be interesting for the case to search for DNA on the document and it could allow to re-evaluate the propositions.

Conclusion

On the 25th of February 2019, two persons were arrested in Lausanne : Mr Francesco Sforza and Mr Tim Pressive. They were both subject to an international arrest warrant as they are suspected to be part of a criminal organization responsible for stealing the US Declaration of Independence.

Caroline Moutiez was mandated to answer five questions and present the results in a report for the 31st of May 2019 (**Annex I**) :

1. Where was Mr Sforza in January and February 2019 ?
2. Where was Mr Pressive in January and February 2019 ?
3. Did Mr Sforza and Mr Pressive meet during this period?
4. Did Mr Sforza and/or Mr Pressive take part in any illegal activities during this period?
5. In particular, are Mr Sforza and/or Mr Pressive implicated in the theft of the US Declaration of Independence?

The result of the analysis provides information on the case. With the evaluation phase, the information is evaluated under each propositions.

As a reminder, those are the propositions that were chosen :

1. *Where was Mr Sforza in January and February 2019 ?*

H_1 : Mr Sforza was in Switzerland and in the United States in January and February 2019.
H_2 : Mr Sforza was somewhere else in January and February 2019.

2. *Where was Mr Pressive in January and February 2019 ?*

H_1 : Mr Pressive was in Switzerland and in the United States in January and February 2019.
H_2 : Mr Pressive was somewhere else in January and February 2019.

3. *Did Mr Sforza and Mr Pressive meet during this period ?*

H_1 : Mr Sforza and Mr Pressive met during this period.
H_2 : Mr Sforza and Mr Pressive did not meet during this period.

4. *Did Mr Sforza and/or Mr Pressive take part in any illegal activities during this period ?*

H_1 : Mr Sforza and/or Mr Pressive took part in illegal activities during this period.
$H_{1,1}$: Mr Sforza took part in illegal activities during this period.
$H_{1,2}$: Mr Pressive took part in illegal activities during this period.
H_2 : Mr Sforza and/or Mr Pressive did not take part in any illegal activities during this period.
$H_{2,1}$: Mr Sforza did not take part in any illegal activities during this period.
$H_{2,2}$: Mr Pressive did not take part in any illegal activities during this period.

5. *In particular, are Mr Sforza and/or Mr Pressive implicated in the theft of the US Declaration of Independence ?*

H_1 : Mr Sforza and/or Mr Pressive are implicated in the theft of the US Declaration of Independence.
$H_{1,1}$: Mr Sforza is implicated in the theft of the US Declaration of Independence.
$H_{1,2}$: Mr Pressive is implicated in the theft of the US Declaration of Independence.
H_2 : Mr Sforza and/or Mr Pressive are not implicated in the theft of the US Declaration of Independence.
$H_{2,1}$: Mr Sforza is not implicated in the theft of the US Declaration of Independence.
$H_{2,2}$: Mr Pressive is not implicated in the theft of the US Declaration of Independence.

Regarding the matter of the owners of the smartphones, the following was concluded.
The observations are more probable given the proposition H1 ("The Samsung belongs to Francesco Sforza) rather than the proposition H2 ("The Samsung belongs to someone else.").

The observations are much more probable given the proposition H1 ("The iPhone belongs to Tim Pressive.) than the proposition H2 ("The iPhone belongs to someone else.").

On the matter of the location of Francesco Sforza, the observations are much more probable given the proposition H1 ("Mr Sforza was in Switzerland and in the United States in January and February 2019.") than the proposition H2 ("Mr Sforza was somewhere else in January and February 2019.").

For Tim Pressive, the observations are much more probable given the proposition H1 ("Mr Pressive was in Switzerland and in the United States in January and February 2019.") than the proposition H2 ("Mr Pressive was somewhere else in January and February 2019.").

The multiplicity of the sources of information goes in the same way. The observations are far more probable given the proposition H1 ("Mr Sforza and Mr Pressive met during this period") than the proposition H2 ("Mr Sforza and Mr Pressive did not meet during this period.").

Two illegal activities took place in February. After analyzing and crossing the information, the observations are far more probable given the proposition H1 ("Mr Sforza and/or Mr Pressive took part in illegal activities during this period.") than the proposition H2 ("Mr Sforza and/or Mr Pressive did not take part in any illegal activities during this period."). The observations support both sub-propositions ($H_{1,1}$ and $H_{1,2}$).
One of the illegal activities is the theft of the Declaration of Independence. The observations are far more probable given the proposition H1 ("Mr Sforza and/or Mr Pressive are implicated in the theft of the US Declaration of Independence.") than the proposition H2 ("Mr Sforza and/or Mr Pressive are not implicated in the theft of the US Declaration of Independence."). Both sub-propositions $H_{1,1}$ and $H_{1,2}$ are strongly supported by the observations. But the observations provide very strong support for $H_{1,2}$.

A reevaluation could be necessary if more information on the case comes.

Bibliographie

1. Casey E and Maguire T (2015) Smartphone Forensic Analysis, Step-by-Step. In : *Appareils mobiles et Smartphone Apps* (course), University of Lausanne, CH, semester of Spring 2019.

2. ENFSI (2015) *ENFSI Guideline for Evaluative Reporting in Forensic Science, European Network of Forensic Science Institutes*, p. 17.

Annexes :

I. Mandat
II. Mail from the group of experts to the prosecutor
III. Mail from the prosecutor to the group of experts
IV. Relational Diagram
V. Spatiotemporal Diagram
VI. Figures to illustrate the results

Annex I : Mandate

UNIL | Université de Lausanne
Ecole des Sciences criminelles
bâtiment Batochime
CH - 1015 Lausanne - Dorigny

Final Exam – National Treasure (ESC-32-33-12)

Appareils Mobiles et Smartphone Apps – 09.05.2019

Description

Following an international arrest warrant, two individuals, Mr Francesco Sforza and Mr Tim Pressive, were arrested in Lausanne on 25 February 2019. They are suspected to be part of a criminal organization responsible for stealing the US Declaration of Independence.

Two phones were taken from the suspects: (1) a Samsung Galaxy S6 Edge from Mr Pressive, and (2) an iPhone 6 from Mr Sforza.

The phones were sent to the ESC for examination.

Transmitted items

The ESC received the items on 25 February. The case ESC-32-33-12 was created. The items were labelled as follows:

> Samsung Galaxy S6 Edge (ESC-32-33-12_P001)

> iPhone 6 (ESC-32-33-12_P002)

A logical extraction of the Samsung (item P001) was performed on 25 February (ESC-32-33-12_P001_R001). Because no operable data was obtained with this technique, the phone was rooted on 26 February and a physical extraction was performed (ESC-32-33-12_P001_R002).

A logical extraction of the iPhone (item P002) was performed on 1 March (ESC-32-33-12_P002_R001). After rooting the phone, a file system extraction was also performed on 5 April (ESC-32-33-12-P002_R002). Some messages from the Telegram application were also captured using the screen recording function of the phone (ESC-32-33-12_P002_R003).

Traces Numériques
Ecole des Sciences criminelles

Tél.+41 (0)21 692 46 11 | esc-cyber@unil.ch | www.unil.ch/esc

Annex II : Mail from the group of experts

Case ESC-32-33-12

Alexandrine Briaux

ven. 17/05/2019 10:30

À : Eoghan Casey <eoghan.casey@unil.ch>;

Cc : Alexis Jacquin <alexis.jacquin@unil.ch>; Neila-Amor Leonor <neila-amor.leonor@unil.ch>; Kilian Hoffmeyer <kilian.hoffmeyer@unil.ch>; Morgane Muratori <morgane.muratori@unil.ch>; Nadia Meichtry <nadia.meichtry@unil.ch>; Justine Guérin <justine.guerin@unil.ch>; Caroline Moutiez <caroline.moutiez@unil.ch>; Jean Lathion <jean.lathion@unil.ch>; Romain Berthod <romain.berthod@unil.ch>; Déborah Francisco <deborah.francisco@unil.ch>; Lionel Notari <lionel.notari@unil.ch>; Andrea Turrisi <andrea.turrisi@unil.ch>; Jonathan Maurer <jonathan.maurer@unil.ch>;

Mr Prosecutor,

Following the mandate that was given to the class regarding the case "National Treasure", we were wondering if it would be possible to get a photography of each suspect.

Indeed, during the analysis of the phones, several pictures of individuals were found and some of the mandates's questions request some evaluation of a potential link between the suspect and the phone.

Therefore, knowing what the suspects look like would be of great help for said evaluation.

Best regards,

The Master's class.

Annex III : Mail from the prosecutor

29/05/2019 Courrier - caroline.moutiez@unil.ch

Re: Case ESC-32-33-12

Eoghan Casey

lun. 20/05/2019 20:03

À : Alexandrine Briaux <alexandrine.briaux@unil.ch>;

Cc : Alexis Jacquin <alexis.jacquin@unil.ch>; Neila-Amor Leonor <neila-amor.leonor@unil.ch>; Kilian Hoffmeyer <kilian.hoffmeyer@unil.ch>; Morgane Muratori <morgane.muratori@unil.ch>; Nadia Meichtry <nadia.meichtry@unil.ch>; Justine Guérin <justine.guerin@unil.ch>; Caroline Moutiez <caroline.moutiez@unil.ch>; Jean Lathion <jean.lathion@unil.ch>; Romain Berthod <romain.berthod@unil.ch>; Déborah Francisco <deborah.francisco@unil.ch>; Lionel Notari <lionel.notari@unil.ch>; Andrea Turrisi <andrea.turrisi@unil.ch>; Jonathan Maurer <jonathan.maurer@unil.ch>; Alain Iglesias Borrajo <alain.iglesiasborrajo@unil.ch>; Bryan Renner <bryan.renner@unil.ch>; Jérémy Corcoba <jeremy.corcoba@unil.ch>; Philippe Jansen <philippe.jansen@unil.ch>; Thomas Pineau <thomas.pineau@unil.ch>; Romain Berthod <romain.berthod@unil.ch>;

1 pièce(s) jointe(s) (1 Mo)

sujet1.JPG;

Dear Alexandrine (and others),

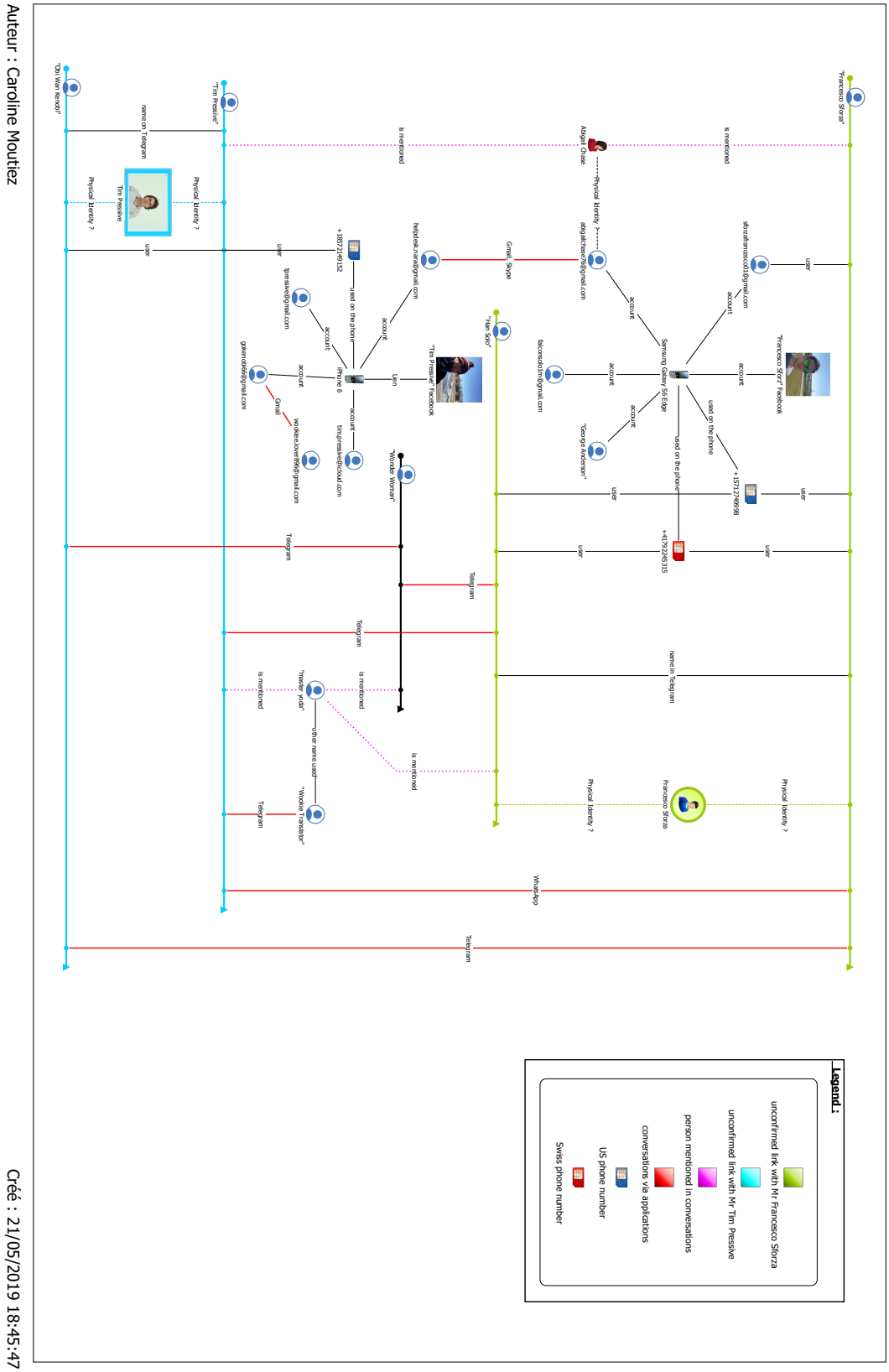
Here is the photograph "mugshot" of Mr Tim Pressive.

The second individual is under a witness protection program because he became an informant for the police, so his photograph cannot be provided at this time.

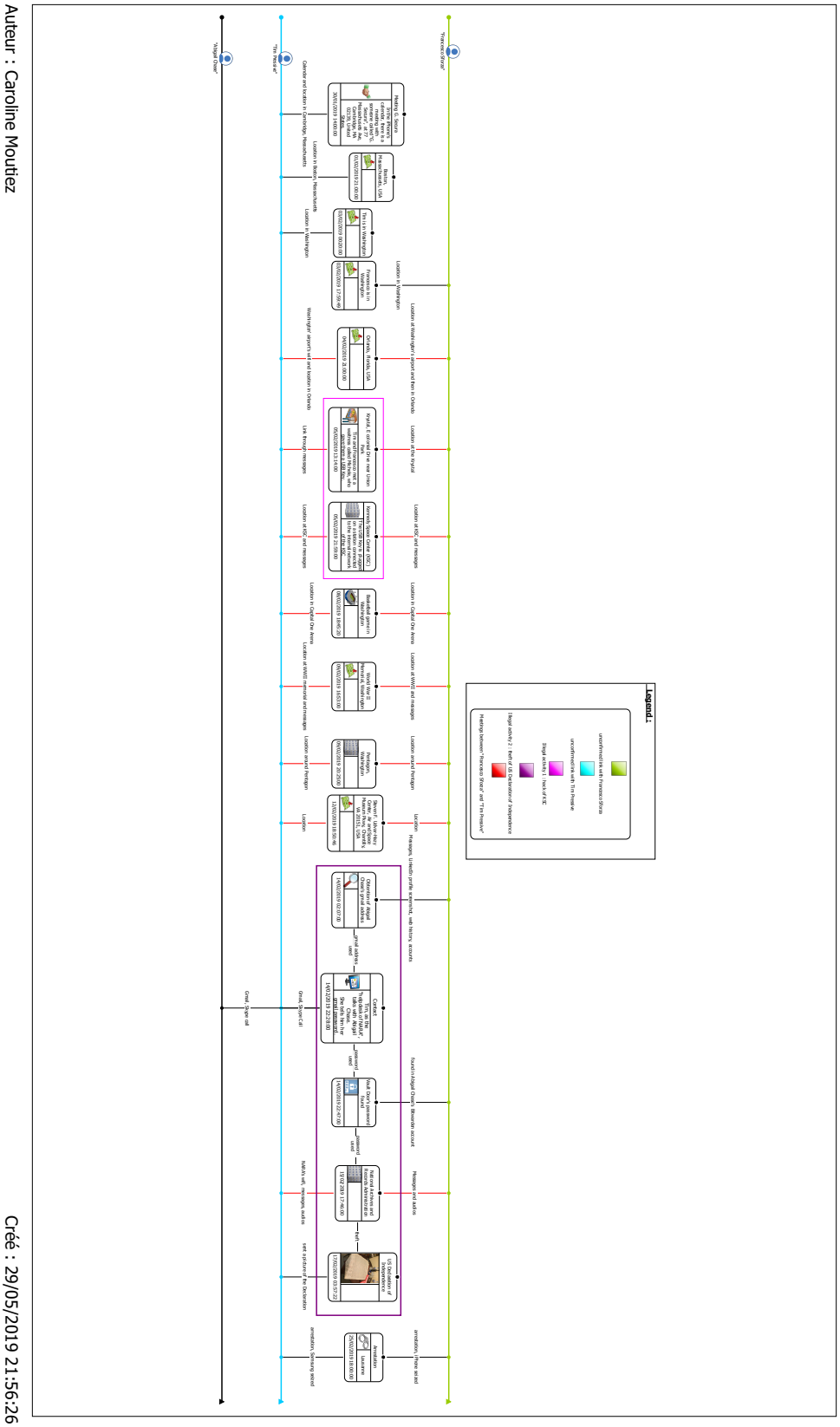
Eoghan Casey
Professor of Digital Forensic Science and Investigation

Sujet1.JPG :

Annex IV : Relational Diagram



Annex V : Spaciotemporal Diagram



Annex VI : Figures

```
De: From: 41792245315@s.whatsapp.net Francesco Sforza
Horodateur: 04.02.2019 15:52(UTC+0)
App Source: WhatsApp
Corps:
Got a new number!
------------------------------
De: From: 18572149152@s.whatsapp.net Tim Pressive
Horodateur: 04.02.2019 16:38(UTC+0)
App Source: WhatsApp
Corps:
Yay what is it?
------------------------------
De: From: 41792245315@s.whatsapp.net Francesco Sforza
Horodateur: 04.02.2019 17:35(UTC+0)
App Source: WhatsApp
Corps:
1-571-274-9998
```

Figure 1 : Messages between "Francesco Sforza" and "Tim Pressive" on WhatsApp (04/02/19)

```
De: From: 695862679 Wonder Woman
Horodateur: 05.02.2019 12:16(UTC+0)
App Source: Telegram (41792245315)
Corps:
Han, Obi Wan,
This mission will be tricky and we need the best!
------------------------------
De: From: 695862679 Wonder Woman
Horodateur: 05.02.2019 12:17(UTC+0)
App Source: Telegram (41792245315)
Corps:
A package is waiting for you at the Krystal on E colonial Drive near Union Park.
------------------------------
De: From: 695862679 Wonder Woman
Horodateur: 05.02.2019 12:18(UTC+0)
App Source: Telegram (41792245315)
Corps:
Ask Michele the waitress, she will give it to you.
```

```
De: From: 695862679 Wonder Woman
Horodateur: 05.02.2019 12:19(UTC+0)
App Source: Telegram (41792245315)
Corps:
It contains a USB key with a piece of Malware.
------------------------------
De: From: 695862679 Wonder Woman
Horodateur: 05.02.2019 12:20(UTC+0)
App Source: Telegram (41792245315)
Corps:
You have to plug it to a station connected to the internal network of the KSC.
```

```
De: From: 695862679 Wonder Woman
Horodateur: 05.02.2019 12:22(UTC+0)
App Source: Telegram (41792245315)
Corps:
This is very important. The malware will retrieve some data and copy it on the key.
```

Figure 2 : Messages between "Wonder Woman", "Francesco Sforza"/"Han Solo" and "Tim Pressive"/"Obi Wan Kenobi" on Telegram (05/02/19)

```
Heure de début: 05.02.2019 21:59(UTC+0)
Dernière activité: 15.02.2019 18:15(UTC+0)
Participants: 713796950 Tim Pressive, 663470243 Han Solo
De: To: 663470243 Han Solo
Horodateur: 05.02.2019 21:59(UTC+0)
App Source: Telegram (41792245315)
Corps:
Placing USB now
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 05.02.2019 22:03(UTC+0)
App Source: Telegram (41792245315)
Corps:
Hurry up the guards are coming back!
------------------------------
De: To: 663470243 Han Solo
Horodateur: 05.02.2019 22:04(UTC+0)
App Source: Telegram (41792245315)
Corps:
Its done! Comin back now!!!
------------------------------
De: To: 663470243 Han Solo
Horodateur: 05.02.2019 22:05(UTC+0)
App Source: Telegram (41792245315)
Corps:

------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 05.02.2019 22:06(UTC+0)
App Source: Telegram (41792245315)
Corps:
Nice meet me at the atlas rocket!
```

Figure 3 : Messages between "Tim Pressive" and "Han Solo" on Telegram (05/02/19)

```
De: From: 713796950 Tim Pressive
Horodateur: 09.02.2019 15:58(UTC+0)
App Source: Telegram (41792245315)
Corps:
I received a message from Master Yoda
------------------------------
De: To: 663470243 Han Solo
Horodateur: 09.02.2019 16:00(UTC+0)
App Source: Telegram (41792245315)
Corps:
A new mission?
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 09.02.2019 16:01(UTC+0)
App Source: Telegram (41792245315)
Corps:
Yes
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 09.02.2019 16:01(UTC+0)
App Source: Telegram (41792245315)
Corps:
I will explain it you in person
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 09.02.2019 16:03(UTC+0)
App Source: Telegram (41792245315)
Corps:
Met me on the 17th street in front of the WWII memorial in 45min
------------------------------
De: To: 663470243 Han Solo
Horodateur: 09.02.2019 16:08(UTC+0)
App Source: Telegram (41792245315)
Corps:

------------------------------
De: To: 663470243 Han Solo
Horodateur: 09.02.2019 16:08(UTC+0)
App Source: Telegram (41792245315)
Corps:
Meet you there
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 09.02.2019 16:09(UTC+0)
App Source: Telegram (41792245315)
Corps:

------------------------------
De: To: 663470243 Han Solo
Horodateur: 09.02.2019 16:52(UTC+0)
App Source: Telegram (41792245315)
Corps:
Now at the memorial
```

Figure 4 : Messages between "Tim Pressive" and "Han Solo" on Telegram (09/02/19)

```
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 00:53(UTC+0)
App Source: Telegram (41792245315)
Corps:
When we was at the national archives the other day I saw that there was a an event on Friday
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 00:54(UTC+0)
App Source: Telegram (41792245315)
Corps:
It may be the good time to go in?
------------------------------
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 00:55(UTC+0)
App Source: Telegram (41792245315)
Corps:
Good idea, i'll search for it
```

Figure 5 : Messages between "Tim Pressive" and "Han Solo" on Telegram (14/02/19)

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 01:02(UTC+0)
App Source: Telegram (41792245315)
Corps:
https://m.facebook.com/events/2232396137022610/
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 01:25(UTC+0)
App Source: Telegram (41792245315)
Corps:
Nice
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 01:27(UTC+0)
App Source: Telegram (41792245315)
Corps:
The organisator of the event, Abigail Chase, seems easy to hack...
------------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 01:27(UTC+0)
App Source: Telegram (41792245315)
Corps:
We should try to access her email account to see what's in it
------------------------------
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 01:28(UTC+0)
App Source: Telegram (41792245315)
Corps:
Yup, great idea, i'll see what I can find on her
```

Figure 6 : Messages between "Tim Pressive" and "Han Solo" on Telegram (14/02/19)

```
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 22:30(UTC+0)
App Source: Telegram (41792245315)
Corps:
I just Skyped her
-----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 22:30(UTC+0)
App Source: Telegram (41792245315)
Corps:
Very nice girl
-----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 22:30(UTC+0)
App Source: Telegram (41792245315)
Corps:
The password is nationaltreasure for her gmail
-----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 14.02.2019 22:31(UTC+0)
App Source: Telegram (41792245315)
Corps:
And she said that she just started to use a pwd manager
-----------------------------
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:33(UTC+0)
App Source: Telegram (41792245315)
Corps:
That's great! I'm gonna check her gmail and this thing about the password manager, it could be exactly what we need! 😎
```

Figure 7 : Messages between "Tim Pressive" and "Han Solo" on Telegram (14/02/19)

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:38(UTC+0)
App Source: Telegram (41792245315)
Corps:
I'm in
```

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:41(UTC+0)
App Source: Telegram (41792245315)
Corps:
Gonna login and see what it holds
```

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:40(UTC+0)
App Source: Telegram (41792245315)
Corps:
She setup bitwarden as password manager
```

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:46(UTC+0)
App Source: Telegram (41792245315)
Corps:
She saved it into chrome's password manager
```

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:47(UTC+0)
App Source: Telegram (41792245315)
Corps:
It's a goldmine!
-----------------------------
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:47(UTC+0)
App Source: Telegram (41792245315)
Corps:
There are all hers accounts
```

```
De: To: 663470243 Han Solo
Horodateur: 14.02.2019 22:47(UTC+0)
App Source: Telegram (41792245315)
Corps:
...THE VAULT PASSWORD!
```

Figure 8 : Messages between "Tim Pressive" and "Han Solo" on Telegram (14/02/19)

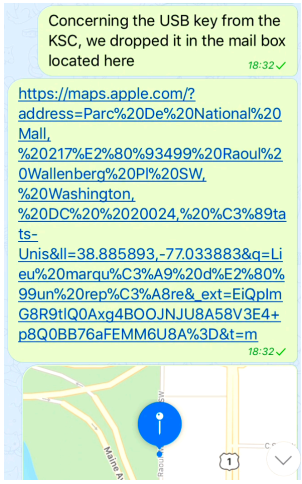


Figure 9 : The location of the USB key, message from "Obi Wan Kenobi" to "Wonder Woman on Telegram (14/02/19)

```
De: To: 663470243 Han Solo
Horodateur: 16.02.2019 04:36(UTC+0)
App Source: Telegram (41792245315)
Corps:
We got the declaration, now getting to a safe place, will be back in touch soon!
----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 17.02.2019 03:57(UTC+0)
App Source: Telegram (41792245315)
Corps:
Here it is!
----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 17.02.2019 03:58(UTC+0)
App Source: Telegram (41792245315)
Corps:
We can’t see anything on the back
----------------------------
De: From: 713796950 Tim Pressive
Horodateur: 17.02.2019 03:58(UTC+0)
App Source: Telegram (41792245315)
Corps:
We will bring it to you in 8-9 days when we come back to Europe
```

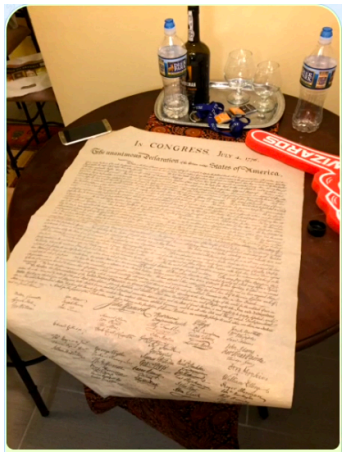


Figure 10 : Messages between "Han Solo", "Tim Pressive" and "Wonder Woman" on Telegram, and on the right is the photo sent with the message "Here it is!" (IMG_0094.jpg).