Mission Name

TheFencesDataCard

History Background

Claire and Ethar are in Asuncion (Paraguay) with she (The Fence). Claire must analyze The Fence´s datacard in order to get any relationship among The Fence and SHAX community.

Technical High-Level Overview

The Fence´s Datacard is provided as an iPhone evidence. The aim is to analyse in depth to locate any clue that allow Claire to identify SHAX community. There is an email from SHAX community located in Protonmail App.

Short Description

You´re going to analyse The Fence´s Datacard based on an iPhone evidence. Your goal is to locate any clue related to SHAX, if you find it, please give us the SHAX Contact.

Mission Description

The Fence´s Datacard is provided based on an iPhone evidence. The aim is to analyse in depth to locate any clue that allow Claire to identify SHAX community. Your goal is to locate any clue related to SHAX, if you find it, please give us the SHAX contact.

Location

ASUNCION | PARAGUAY

Tools

- 7Z
- iLEAPP - https://github.com/abrignoni/iLEAPP
- SQLite Studio
- CyberChef

Questions

How many emails contains ProtonMail App?

- 2

Which day of the week was installed ProtonMail App?

- Wednesday

Hints

1. Use iLEAPP to find any strange App installed.
2. Analyse ProtonMail App.
3. ProtonMail SQLITE could be tampered and using a XOR encryption.

Write Up

First of all, player must unzip Fence´s data card. In this scenario, player is going to face an iPhone evidence. Considering that there are a lot of pieces of information from Apps, and iOS, this challenge is more complicated than others. The first step, would be to use iLEAPP tool to analyse which apps are installed on the Iphone:

```
jmma@demowindows:/mnt/c/THREATIA/Iphone/iLEAPP-1.9.4/iLEAPP-1.9.4$ python3 ileapp.py
usage: ileapp.py [-h] [-t {fs,tar,zip,gz,itunes}] [-o OUTPUT_PATH] [-i INPUT_PATH] [-p]
ileapp.py: error: No OUTPUT folder path provided
```

Figure 1

Player must launch the previous command using "-t fs" -o output_path and -i path_to_extract evidence. Once iLEAPP finishes, an index.html is created. This file has all the necessary information:

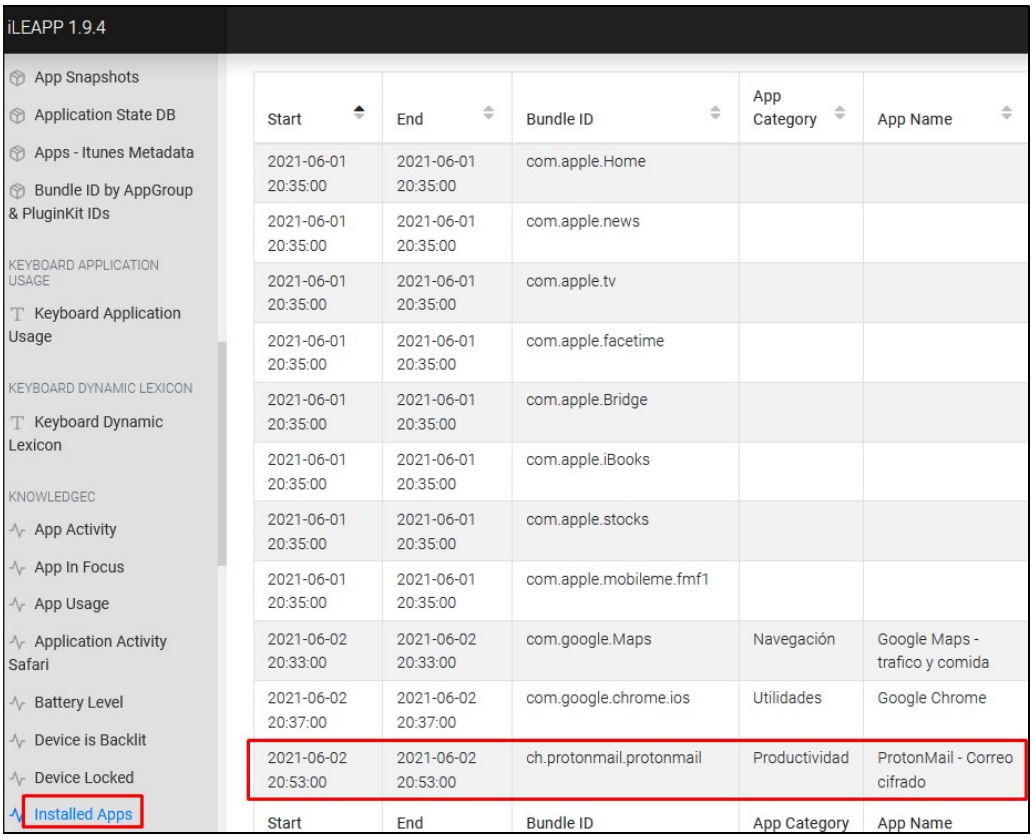

Figure 2

Above picture shows that Proton Mail is installed on the iPhone among other Apps.
Last time that protonmail was focused :

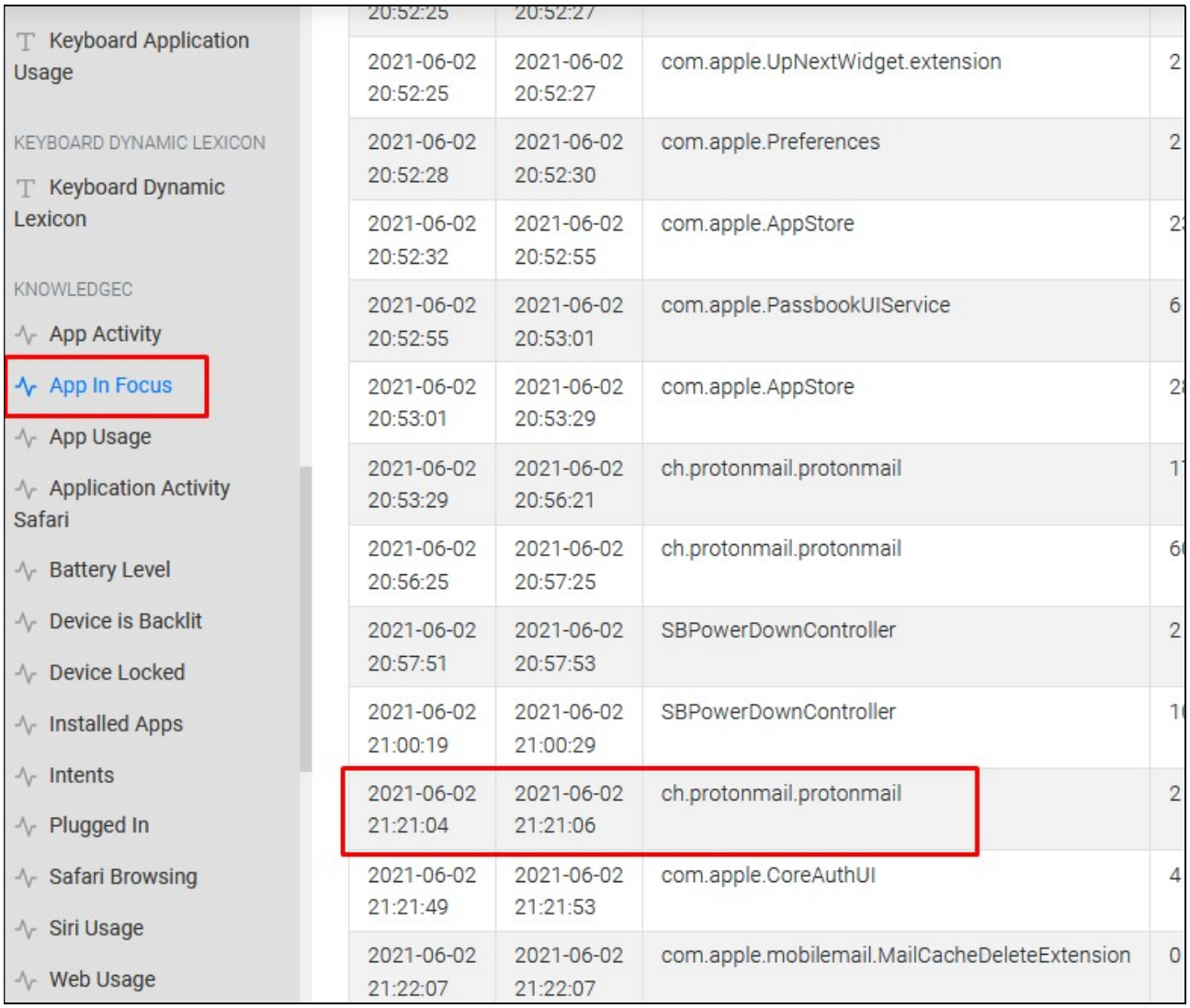
Keyboard Application Usage
KEYBOARD DYNAMIC LEXICON
Keyboard Dynamic Lexicon
KNOWLEDGEC
App Activity
App In Focus
App Usage
Application Activity Safari
Battery Level
Device is Backlit
Device Locked
Installed Apps
Intents
Plugged In
Safari Browsing
Siri Usage
Web Usage
2021-06-02 20:52:25 | 2021-06-02 20:52:27 | com.apple.UpNextWidget.extension
2021-06-02 20:52:28 | 2021-06-02 20:52:30 | com.apple.Preferences
2021-06-02 20:52:32 | 2021-06-02 20:52:55 | com.apple.AppStore
2021-06-02 20:52:55 | 2021-06-02 20:53:01 | com.apple.PassbookUIService
2021-06-02 20:53:01 | 2021-06-02 20:53:29 | com.apple.AppStore
2021-06-02 20:53:29 | 2021-06-02 20:56:21 | ch.protonmail.protonmail
2021-06-02 20:56:25 | 2021-06-02 20:57:25 | ch.protonmail.protonmail
2021-06-02 20:57:51 | 2021-06-02 20:57:53 | SBPowerDownController
2021-06-02 21:00:19 | 2021-06-02 21:00:29 | SBPowerDownController
2021-06-02 21:21:04 | 2021-06-02 21:21:06 | ch.protonmail.protonmail
2021-06-02 21:21:49 | 2021-06-02 21:21:53 | com.apple.CoreAuthUI
2021-06-02 21:22:07 | 2021-06-02 21:22:07 | com.apple.mobilemail.MailCacheDeleteExtension

Figure 3

Considering other apps and installed, and checking that proton App was the last application, it would be a good way to start the analysis. Player must locate folder which contains App protonmail:

- \private\var\mobile\Containers\Shared\AppGroup\16A0E996-690B-4BEE-BE80-AE37A6C986AD**ProtonMail.sqlite**

Next step, would be to open **ProtonMail.sqlite** using SQLite Studio and locate the following table:

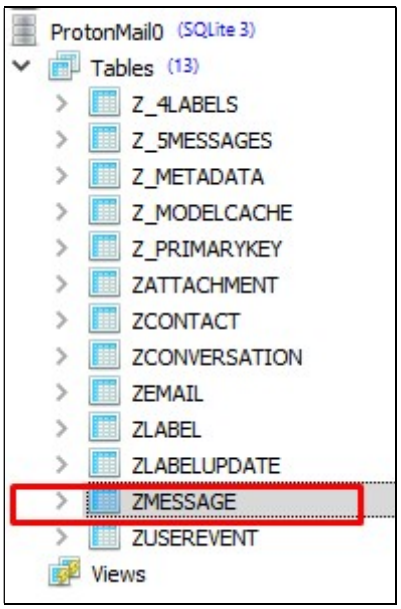

Figure 4

Then locate ZSENDER column:

Figure 5

AZSJ2Q]\FSQF(## # +*'&&#

Player must try to decrypt this information applying his best efforts. This piece of information it´s a XOR encryption.

The key it´s unknown, so player has to launch a little brute force. To accomplish this way, player could use CyberChef. Player doesn´t know anything about the key, so player will go step by step, increasing until key 12:

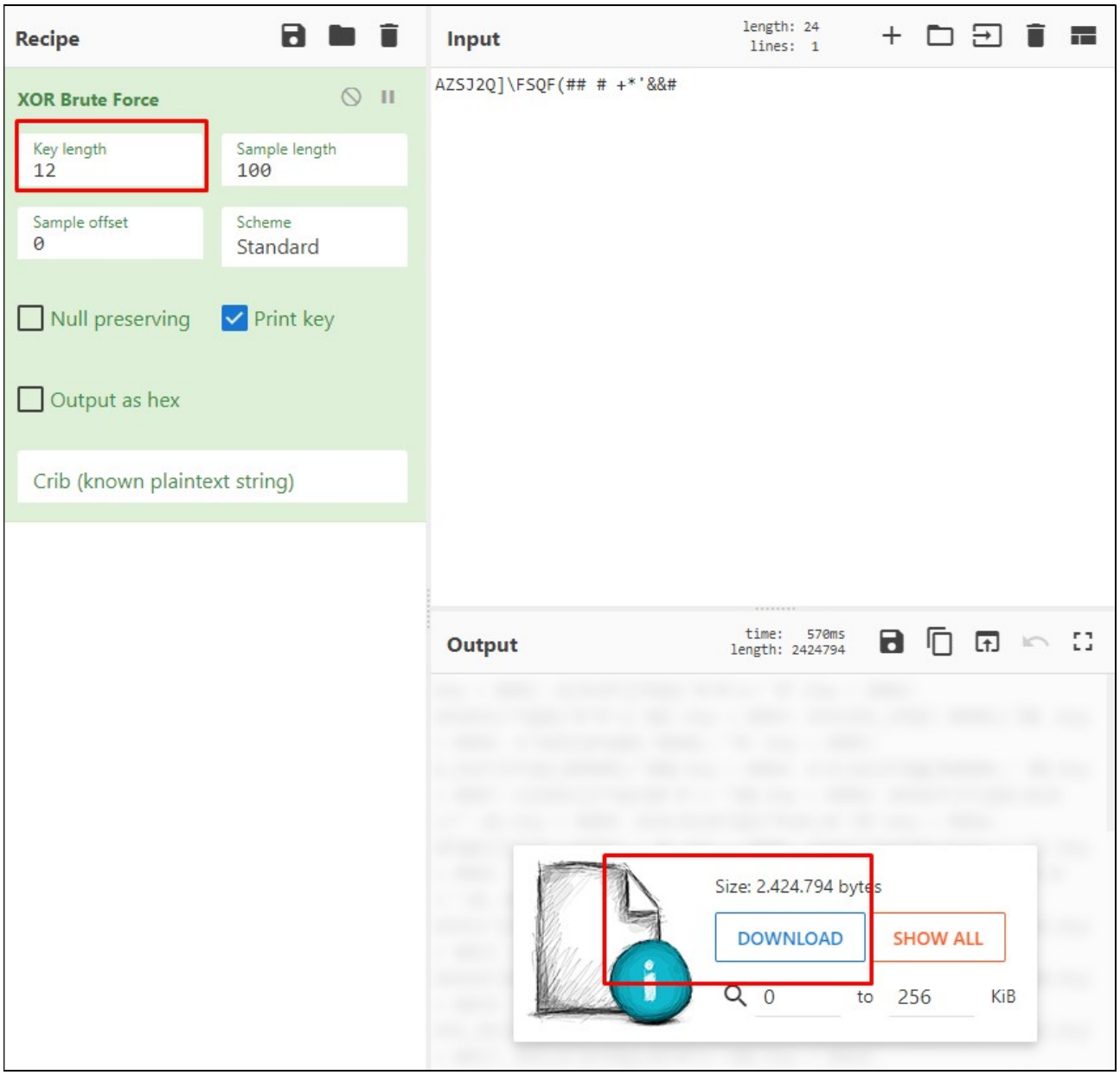

Figure 6

Player must download created file with all possibilities:

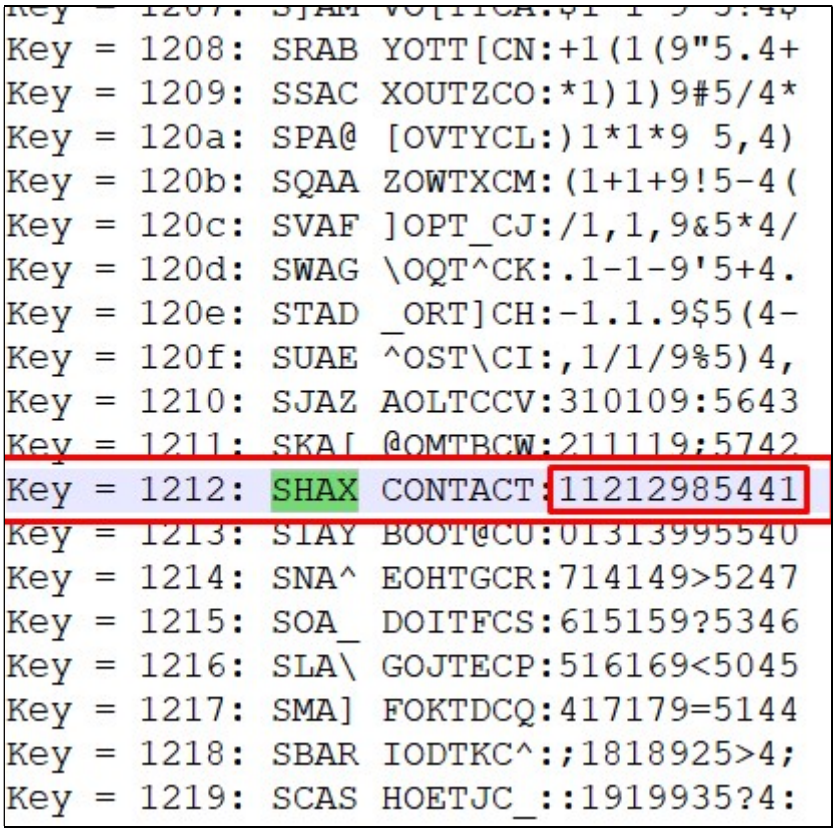

Figure 7

Finally, the SHAX CONTACT is located:
11212985441

Flag Information

flag{11212985441}