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. The aim is to analyse in depth to locate any clue that allow Claire to identify SHAX community. Inside the Fence´s Datacard, there is one file that has SHAX ID Citizen, but this information has been coded in Base64 format.

Short Description

You´re going to analyse The Fence´s Datacard. Your goal is to locate any clue related to SHAX, if you find it, please give us the ID Citizen.

Mission Description

The Fence´s Datacard is provided. 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 ID Citizen.

Location

ASUNCION | PARAGUAY

Tools

- Strings
- binwalk

Questions

Which is the The Fences bank account?

- PA52600345334708680085961241

When was the last creation of a folder inside The Fences Datacard? Please insert dd/mm/yyyy

- 08/12/2049

Items

1. User Arsenal Image Mounter to mount the evidence provided.
2. Locate CONTACT-01 inside the file system provided.
3. Decode the string located inside CONTACT-01 file, using "base64 -d"

Write Up

Linux Method: - root required

https://www.andreafortuna.org/2018/04/11/how-to-mount-an-ewf-image-file-e01-on-linux/

- apt install ewf-tools
- mkdir rawimage
- ewfmount IMAGE.E01 ./rawimage/
- mkdir mountpoint
- mount rawimage/ewf1 mountpoint

Windows Method

Player must mount the filesystem provided using Arsenal Image Mounter tool:
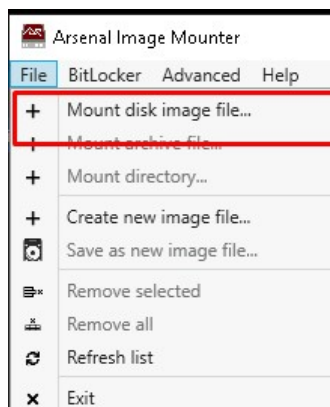

Figure 1

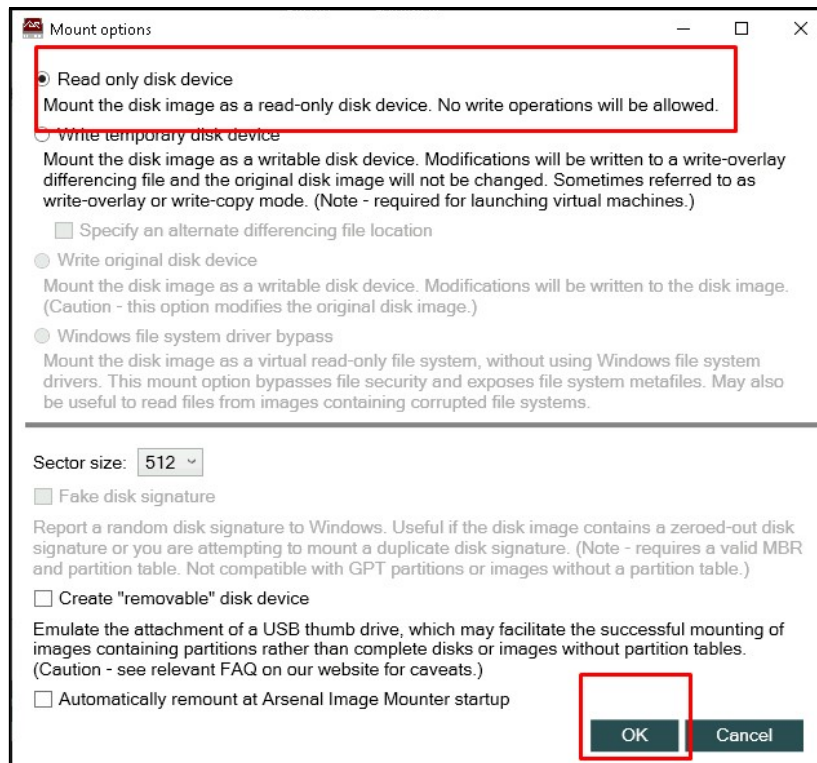Then, select appropiate options takking into account the following options:

Figure 2

Finally, you will get the image mounted on your host:
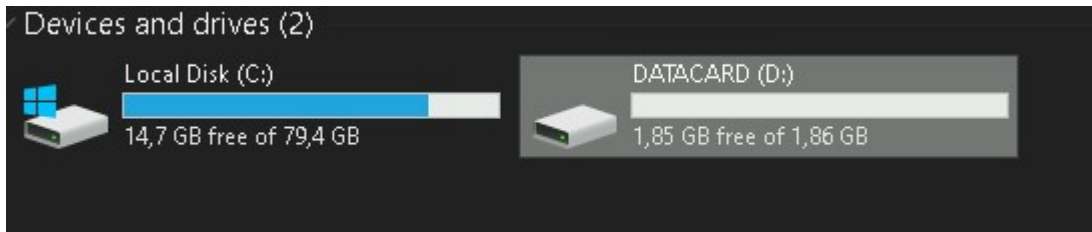
Figure 3

Having access to the filesystem of the datacard:
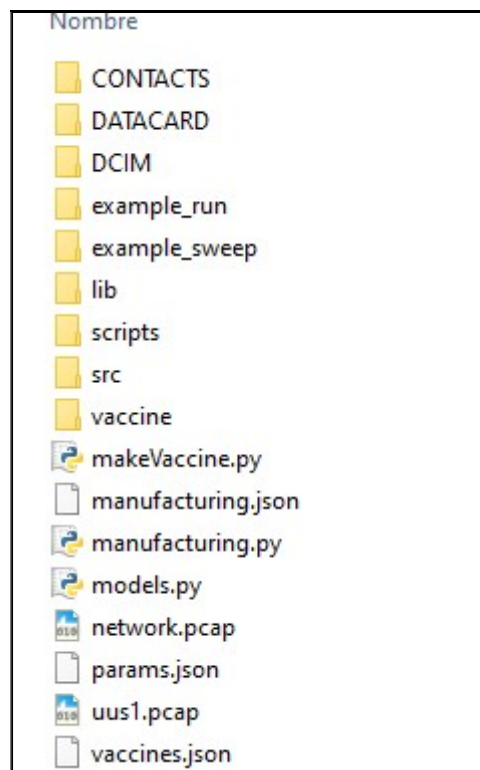

Figure 4

Once mounted, it´s easy to find a folder named "CONTACTS", and then inside there is one file:
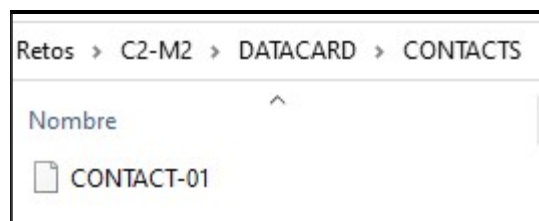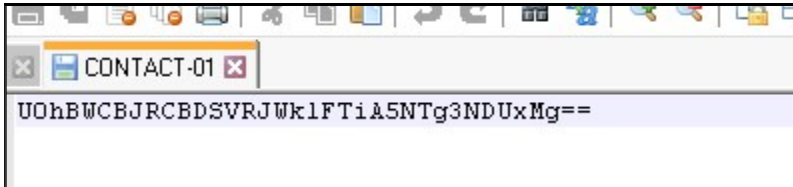

Figure 5

Open CONTACT-01 file:

Figure 6

Next step would be to decode Base64 format: echo
U0hBWCBJRCBDSVRJWklFTiA5NTg3NDUxMg== | base64 -d

Figure 7

Finally player will able to get SHAX ID citizien

Flag Information

flag{95874512}