Mission Name

LazarusForensics

History Background

The Level 7 citizen is plugged into the jack, but he does not have the DATACARD:

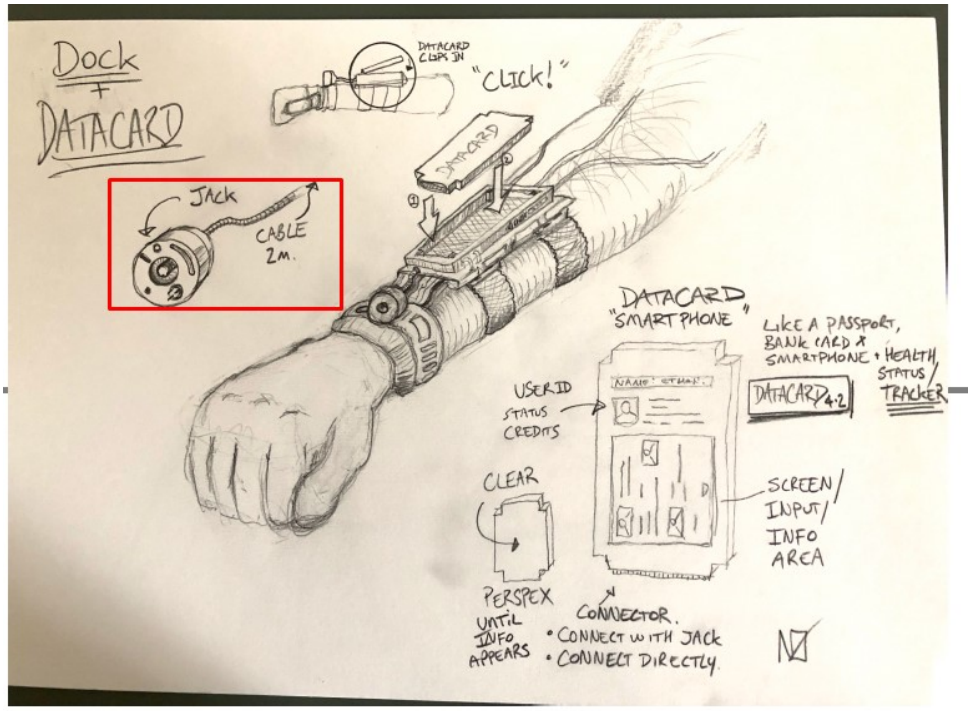


Figure 1

Claire finally gets from the citizen the following evidence.

- Attempts to Change Vaccine Records
- Bank Records
- Code Snippets

Once the forensic procedure has finished, Claire obtains information about where ETHAN lives. Block 44 - SUFU, as this is the address that appears to Claire when Ethan is connected to the Level 7 Dock. Again, depending on how the evidence is provided, it will determine the difficulty of the mission.

Technical High-Level Overview

Player must carry out several recovery task to get files from the provided evidence. In this case, Citizen´s dock has information inside itself and this information is provided to the player. The goal of this mission would be to recover an SQLite database located inside Citizen´s dock.

Short Mission Description

Claire is jacking to Citizen and getting a full dump of him. Your goal is to locate Citizen´s vaccine name.

Mission Description

Player must carry out several recovery task to get files from the provided evidence. In this case, Citizen´s dock has information inside. Claire is jacking to Citizen and getting a full dump of him. Your goal is to locate Citizen´s vaccine name.

Tools

- Photorec for recovering sqlite databases.
- SQLite viewer to read the database and get de necessary information to complete the mission.
- HxD to identify headers of files.

Questions

Which is the bank account of the target?

- US526003453361086800859615O2

Which is the magic header string of the recovered SQLite file? Please provide the whole header in hex

- 53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00

How many types of files were you able to recover? Insert the number.

- 3

Hints

1. Identify if any partition exists on Citizen´s dock.
2. Use carving techniques to recover data.
3. Use Photorec to get an SQLite file.

Location

- SYLVARCON | ANUTM DISTRICT | LEVEL 7 CLIENT'S APARTMENT

Write Up

First step would be to recover the SQL database using Photorec for Windows or Linux, to accomplish this, you must launch Photorec from Defensive tools:

Linux Method.

- apt install gnome-disk-utility
- testdisk needs root access

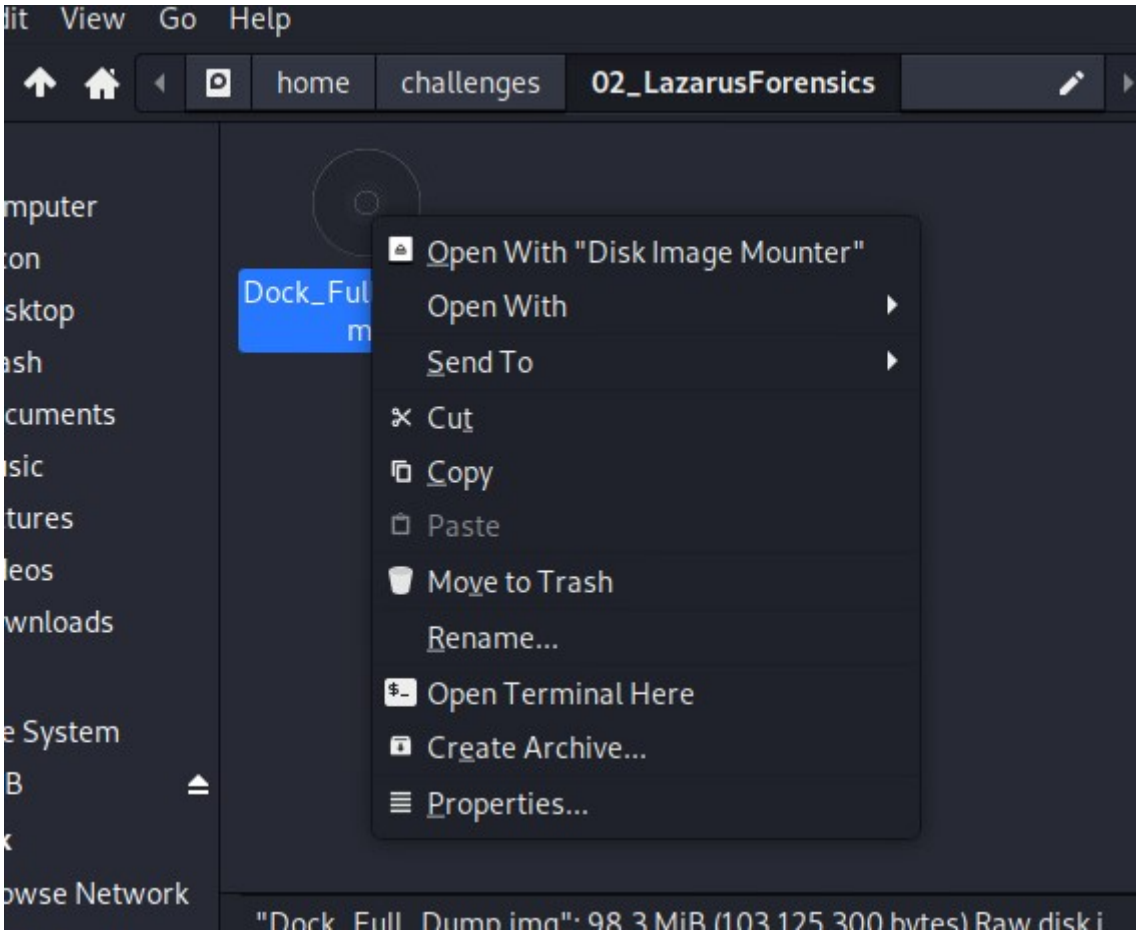


Figure 2

We selected create and select the partition that we have mounted with Open Disk Mount

1. Create
2. None
3. Fat32
4. Image Creation

5. Select the folder where we will extract the content

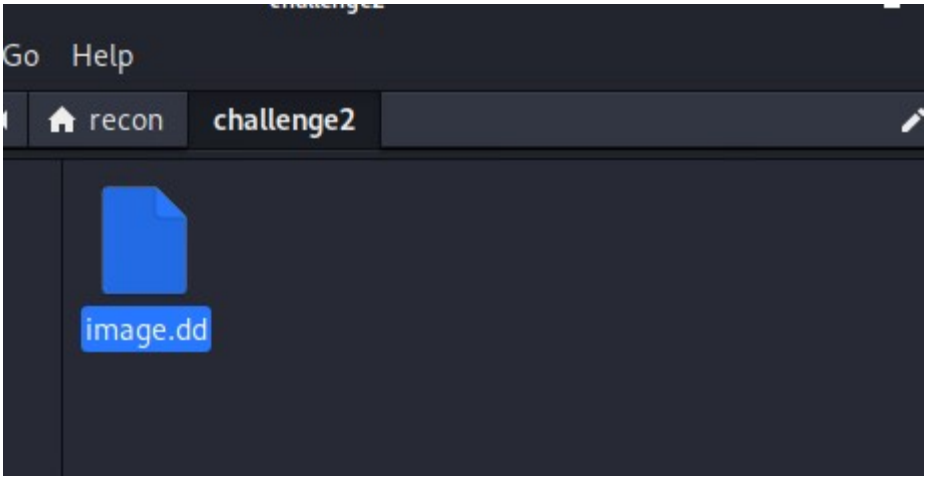


Figure 3

Open it with DB Browser for SQLite

Windows Method

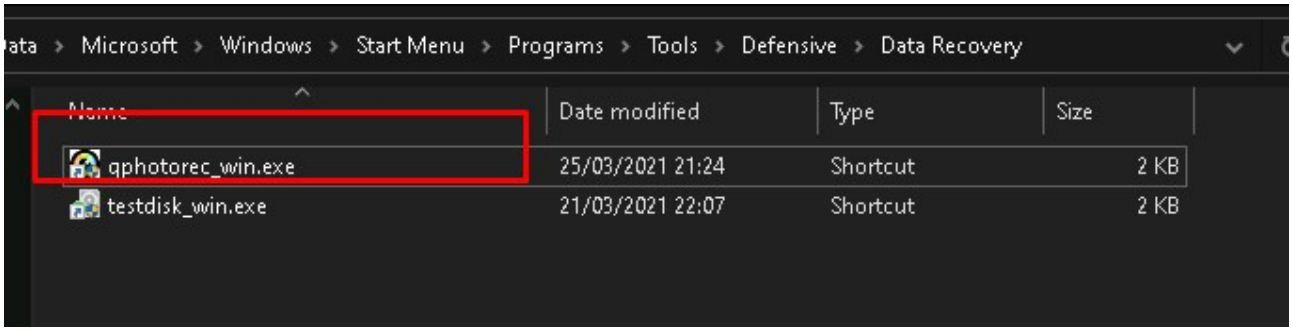


Figure 4

Open it:

Figure 5

1. Select evidence downloaded.
2. Select FAT/NTFS
3. Select destination folder to save the recovered files
4. Press "Start"

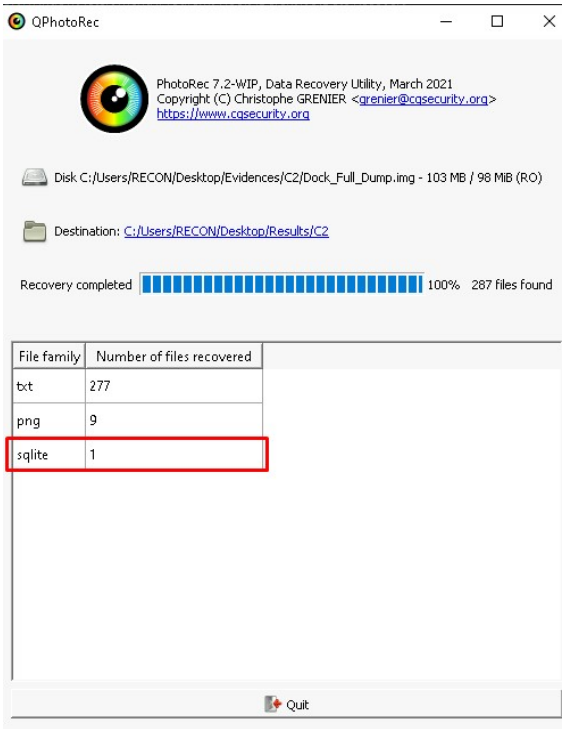


Figure 6

Once you had got SQLite database, next step would be to use a sqlite reader to fetch data:

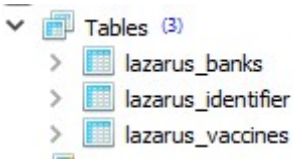
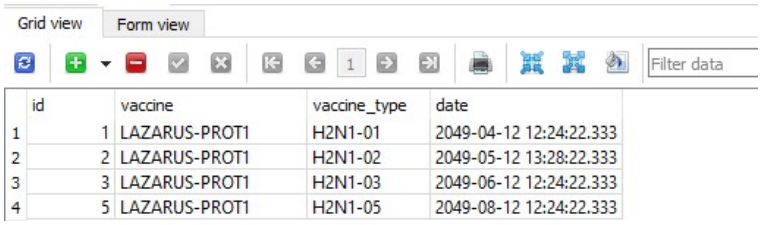


Figure 7

Our goal is to find out which is Citizen´s vaccine name, so we must analyse Lazarus_vaccines table:



	id	vaccine	vaccine_type	date
1	1	LAZARUS-PROT1	H2N1-01	2049-04-12 12:24:22.333
2	2	LAZARUS-PROT1	H2N1-02	2049-05-12 13:28:22.333
3	3	LAZARUS-PROT1	H2N1-03	2049-06-12 12:24:22.333
4	5	LAZARUS-PROT1	H2N1-05	2049-08-12 12:24:22.333

Figure 8

And finally, you can get Citizen´s vaccine name: LAZARUS-PROT1

Flag Information

flag{LAZARUS-PROT1}