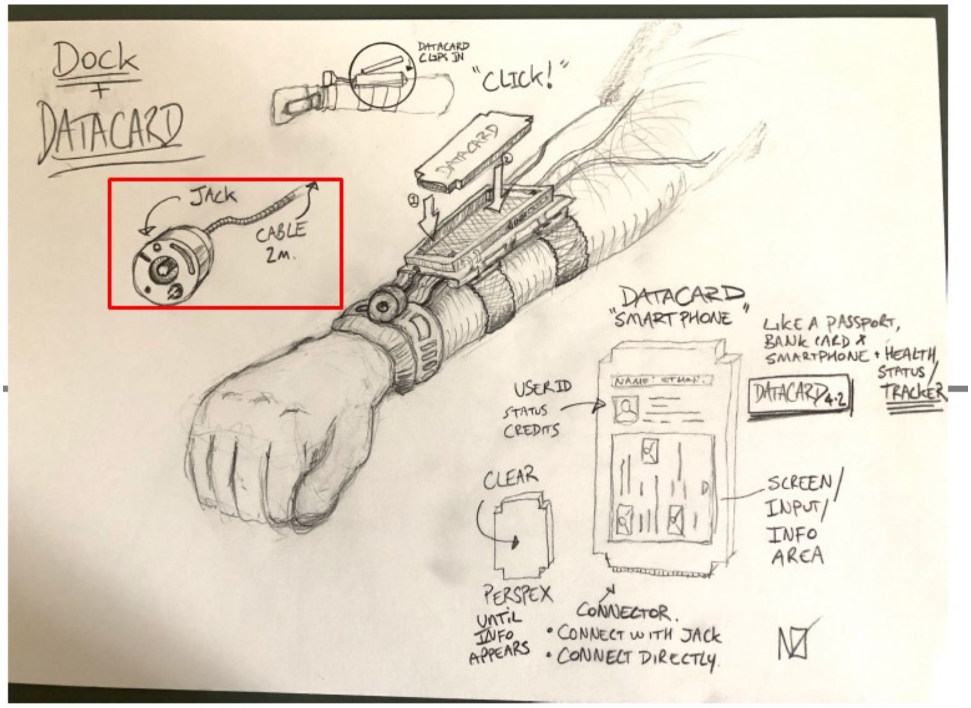
Mission Name

LazarusForensics

History Background

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



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 get de exact date of the vaccine injected between June 2049 and August 2049.

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 get de exact date of the vaccine injected between June 2049 and August 2049. Insert: YYYY-MM-DD HH:MM:SS

Tools

- Photorec for recovering sqlite databases.
- Tsk_recover
- SQLite viewer to read the database and get de necessary information to complete the mission.
- HxD to identify headers of files.
- https://github.com/mdegrazia/SQLite-Deleted-Records-Parser to recover deleted registers inside SQLite

Questions

Which is the free block that contains the exact date?

- 8038

How many unallocated blocks did you find?

- 7838

Hints

1. Use carving techniques to recover data.
2. Check in depth the SQLite Database, specially dates of injected vaccines.
3. Use any tool which allow you recover deleted register on the SQLite Database

Location

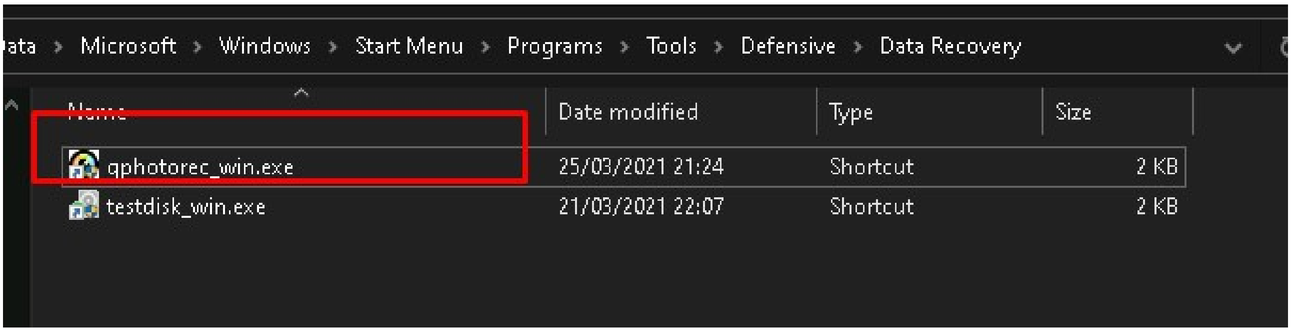
- SYLVARCON | ANUTM DISTRICT | LEVEL 7 CLIENT'S APARTMENT

Write Up

Linux Method.

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

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

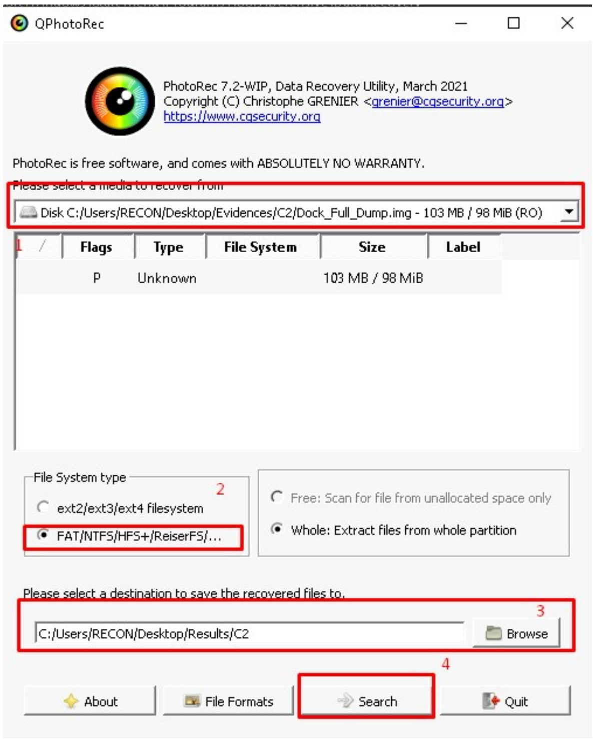


ata › Microsoft › Windows › Start Menu › Programs › Tools › Defensive › Data Recovery

Name	Date modified	Type	Size
qphotorec_win.exe	25/03/2021 21:24	Shortcut	2 KB
testdisk_win.exe	21/03/2021 22:07	Shortcut	2 KB

Figure 1

Open it:



QPhotoRec

PhotoRec 7.2-WIP, Data Recovery Utility, March 2021
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.

Please select a media to recover from

Disk C:/Users/RECON/Desktop/Evidences/C2/Dock_Full_Dump.img - 103 MB / 98 MiB (RO)

/	Flags	Type	File System	Size	Label
	P	Unknown		103 MB / 98 MiB	

File System type
○ ext2/ext3/ext4 filesystem
● FAT/NTFS/HFS+/ReiserFS/...

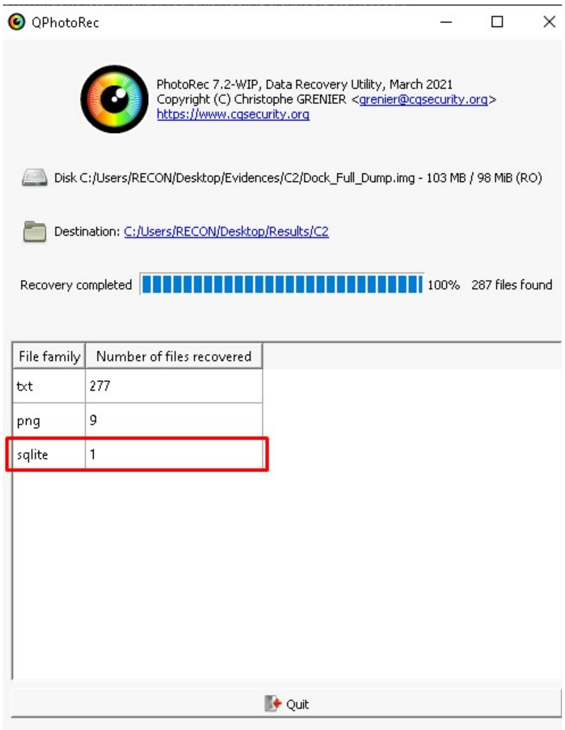
○ Free: Scan for file from unallocated space only
● Whole: Extract files from whole partition

Please select a destination to save the recovered files to.

C:/Users/RECON/Desktop/Results/C2

Figure 2

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



QPhotoRec

PhotoRec 7.2-WIP, Data Recovery Utility, March 2021
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk C:/Users/RECON/Desktop/Evidences/C2/Dock_Full_Dump.img - 103 MB / 98 MiB (RO)

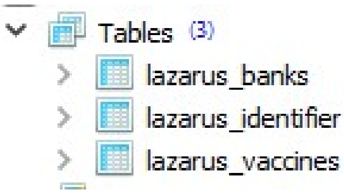
Destination: C:/Users/RECON/Desktop/Results/C2

Recovery completed 100% 287 files found

File family	Number of files recovered
txt	277
png	9
sqlite	1

Figure 3

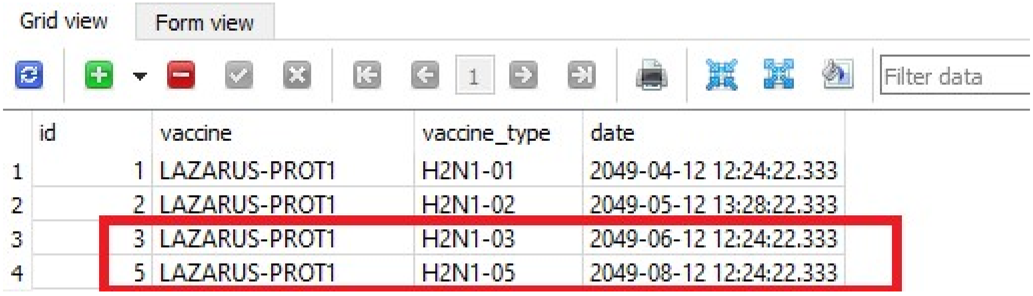
Once you had got SQLite database, next step would be to use a sqlite reader to fetch data:



Tables (3)
- lazarus_banks
- lazarus_identifier
- lazarus_vaccines

Figure 4

Our goal is to find out which is exact date between June and Augusut, so we must analyse Lazarus_vaccines table:

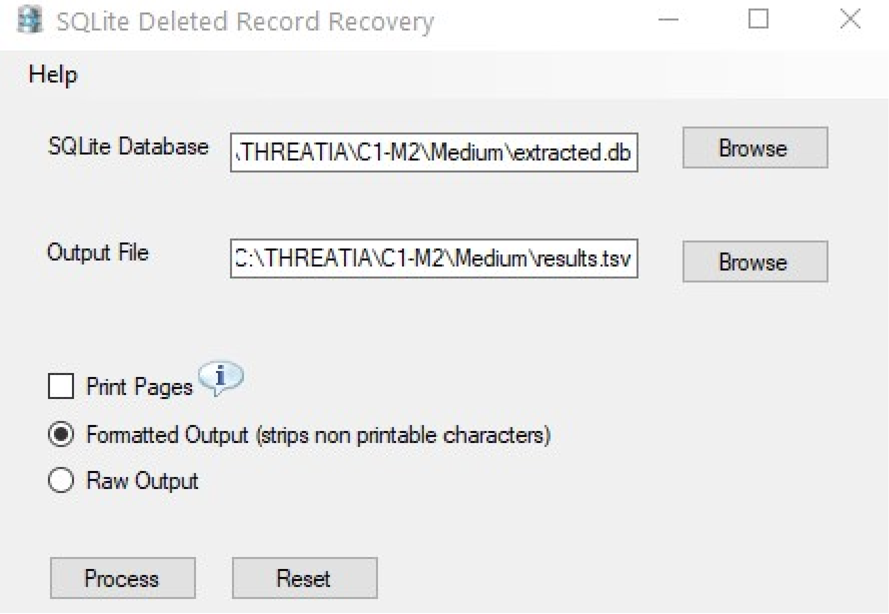


	id	vaccine	vaccine_type	date
1	1	LAZARUS-PROT1	H2N1-01	2049-04-12 12:24:22.333
2	2	LAZARUS-PROT1	H2N1-02	2049-05-12 13:28:22.333
3	3	LAZARUS-PROT1	H2N1-03	2049-06-12 12:24:22.333
4	5	LAZARUS-PROT1	H2N1-05	2049-08-12 12:24:22.333

Figure 5

The key is to identify that there is a shadow register deleted. So, it´s necessary to use a tool which extracts free blocks from the SQLite Database: https://github.com/mdegrazia/SQLite-Deleted-Records-Parser.

Player must insert SQLite Database and execute the tool:



SQLite Deleted Record Recovery

Help

SQLite Database: .THREATIA\C1-M2\Medium\extracted.db

Output File: C:\THREATIA\C1-M2\Medium\results.tsv

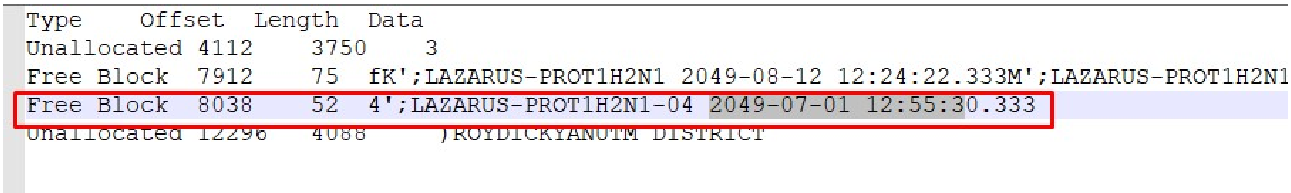
□ Print Pages

● Formatted Output (strips non printable characters)

○ Raw Output

Figure 6

Finally, the output file will show which is the exact date of the vaccine injected in July:



```
Type     Offset  Length  Data
Unallocated 4112    3750    3
Free Block  7912    75   fK';LAZARUS-PROT1H2N1 2049-08-12 12:24:22.333M';LAZARUS-PROT1H2N1
Free Block  8038    52   4';LAZARUS-PROT1H2N1-04 2049-07-01 12:55:30.333
Unallocated 12296   4088      )ROYDICKYANUTM DISTRICT
```

Figure 7

2049-07-01 12:55:30

Flag

flag{2049-07-01 12:55:30}