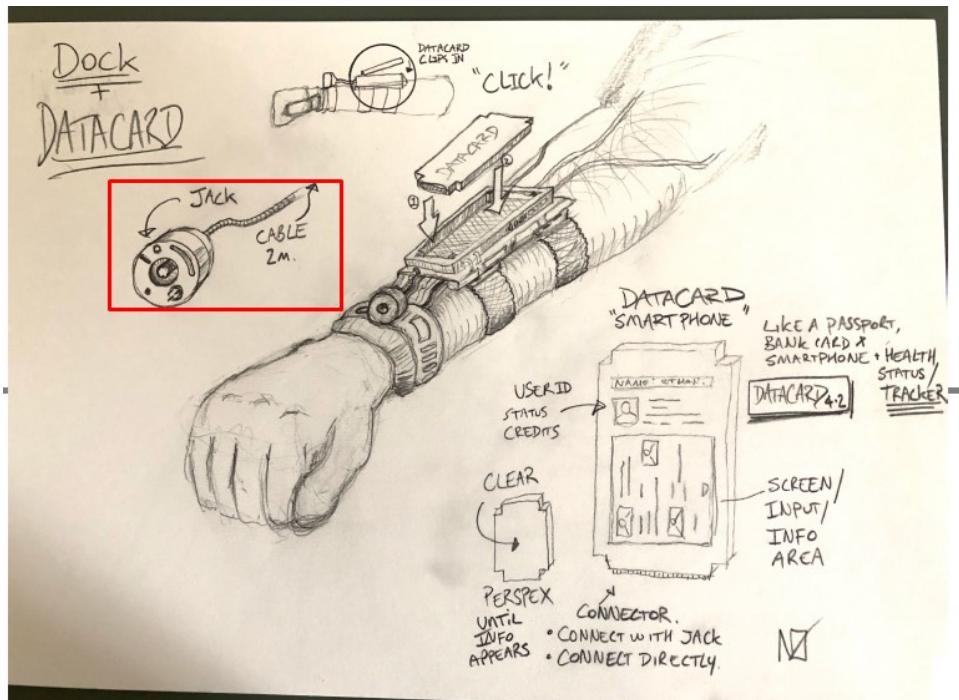


Mission Name

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.



IN GAME INFORMATION

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 COVID19 vaccine injected.

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 **COVID19** vaccine injected. Insert: YYYY-MM-DD HH:MM:SS

Tools

- Photorec for recovering files: https://www.cgsecurity.org/testdisk-7.2-WIP.linux26-x86_64.tar.bz2
- Wxhexeditor: <https://howtoinstall.co/es/wxhexeditor>
- Whatsapp Parser Tool set: <https://github.com/B16f00t/whapa>
- Exiftool: <https://www.poftut.com/how-to-install-and-use-exiftool-in-linux-windows-kali-ubuntu-mint-with-examples/>
- SQLite viewer tool to read the database extracted.

Credentials

- N/A

Questions

Which is the first two hex bytes of the 7Z file?

- 377A

Which is the Primary Platform of the JPG file extracted?

- Microsoft Corporation

How many bytes were needed to decrypt the database?

- 158

Hints

1. Check header and footer of the evidence provided.
2. Extract the JPG file based on the footer.
3. Decrypt the content of the 7Z file based on the JPC picture.

Location

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

Write Up

First step would be to identify header and footer of the evidence provided. To accomplish this, use wxHexEditor:

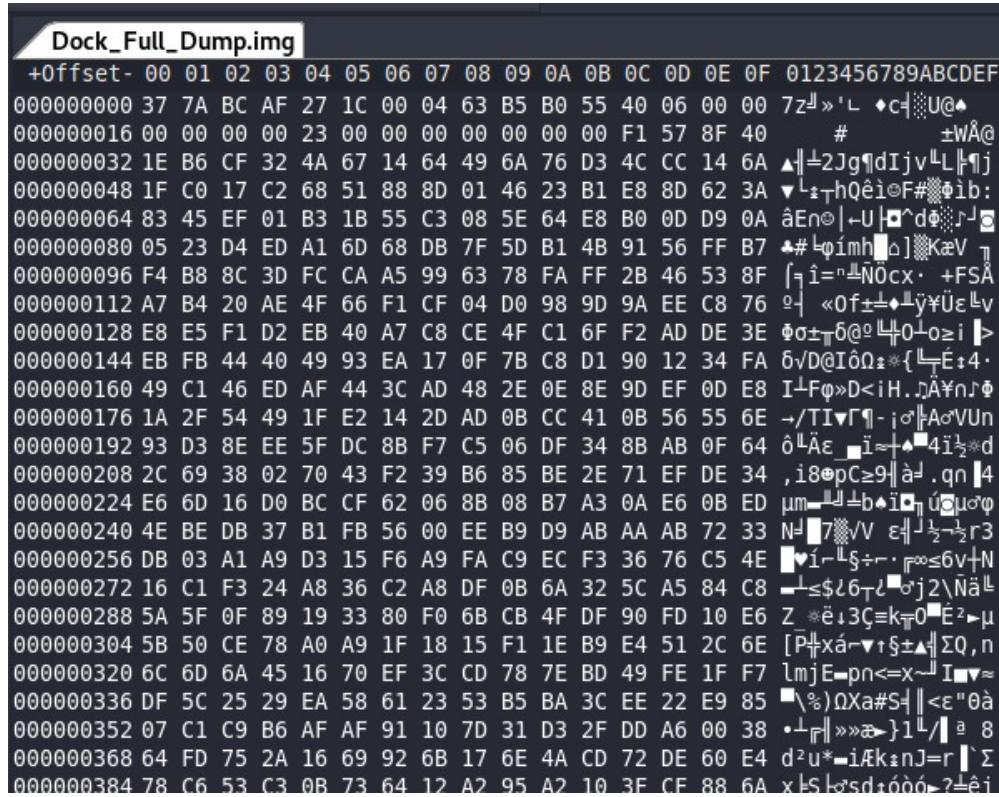


Figure 1

Above image represents the header of the evidence. It's a 7Z file.



The following image represents the footer of the evidence:

Figure 2

The footer has FF D9 values. It's necessary to discover which file is, so searching on Google would be easy to find it:

Google

FF D9 footer

X |

[Todo](#) [Videos](#) [Imágenes](#) [Noticias](#) [Shopping](#) : Más Herramientas

Aproximadamente 411.000 resultados (0,62 segundos)

<https://www.file-recovery.com/jp...> ▾ Traducir esta página

JPG Signature Format: Documentation & Recovery Example

... a length of the file embedded, thus we need to find JPEG trailer, which is **FF D9**. ... Camera RAW files DESCRIPTION = Primitive JPG files **FOOTER=FOOTER-**.

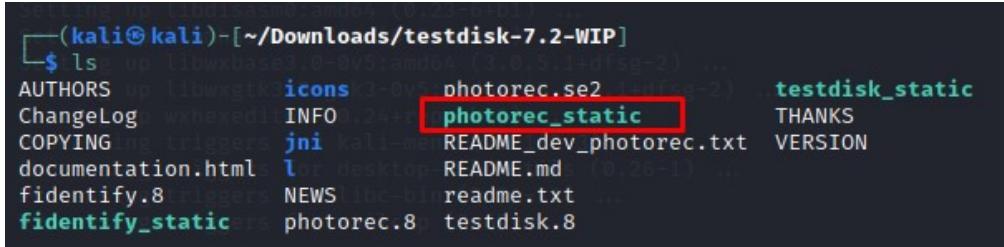
<https://www.garykessler.net/library> ▾ Traducir esta página

File Signatures - Gary Kessler

1 jun 2021 — [6 byte offset] 00 00 FF FF FF FF, [6 byte offset] ... FF FF FF FF FF FF FF FF 00 00 02 00 01 .ÿÿÿÿÿÿ ... A6 D9 00 AA 00 62 CE 6C, 0&#u.fl. ¡Ú.º.bñ.

Figure 3

To sum up: we've found out two files: 7Z file and JPG file. To extract them, it would be essential to use a tool like Photorec. Once downloaded Photorec for Linux, we have the following binaries:

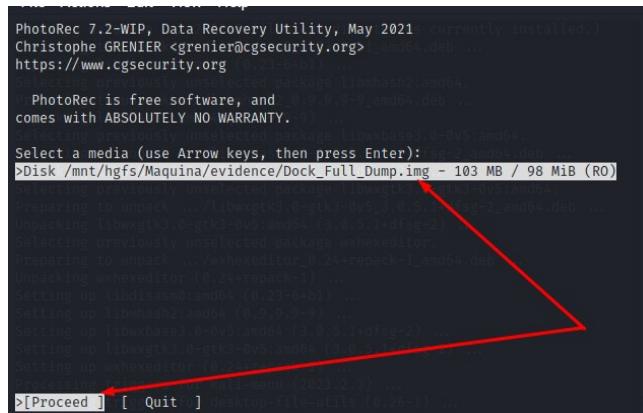


```
(kali㉿kali)-[~/Downloads/testdisk-7.2-WIP]
$ ls
AUTHORS      icons      photorec.se2      testdisk_static
ChangeLog    INFO       photorec_static
COPYING      jni        README_dev_photorec.txt THANKS
documentation.html  l          README.md      VERSION
fidentify.8   NEWS       readme.txt
fidentify_static photorec.8  testdisk.8
```

Figure 4

Photorec_static is the main binary to execute. `./photorec_static Dock_Full_Dump.img`

Once executed, let's forward to the recovery phase, selecting:



```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021 (currently installed.)
Christophe GRENIER <grenier@cgsecurity.org> libhexedit_0.24+repack-1_amd64.deb ...
https://www.cgsecurity.org
Selecting previously unselected package libhash2:amd64 ...
libhash2:amd64 (0.9.9-9) ...
PhotoRec is free software, and ...
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /mnt/hgfs/Maquina/evidence/Dock_Full_Dump.img - 103 MB / 98 MiB (RO)
Preparing to unpack .../libhexedit_0.24+repack-1_amd64.deb ...
Unpacking libhexedit_0.24+repack-1_amd64.deb ...
Selecting previously unselected package wxhexeditor ...
Preparing to unpack .../wxhexeditor_0.24+repack-1_amd64.deb ...
Unpacking wxhexeditor (0.24+repack-1) ...
Setting up libisasm0:amd64 (0.23-6+b1) ...
Setting up libhash2:amd64 (0.9.9-9-9) ...
Setting up libhexedit_0.24+repack-1_amd64 ...
Preparing to unpack .../wxhexeditor_0.24+repack-1_amd64.deb ...
Unpacking wxhexeditor (0.24+repack-1) ...
Setting up libisasm0:amd64 (0.23-6+b1) ...
Setting up libhash2:amd64 (0.9.9-9-9) ...
Setting up libhexedit_0.24+repack-1_amd64 ...
Preparing to unpack .../desktopfilerecovery_0.26-1 ...
Unpacking desktopfilerecovery_0.26-1 ...
Setting up desktopfilerecovery_0.26-1 ...
>[Proceed] [ Quit ]
```

Figure 5

And now, file Opt:

```
Disk /mnt/hgfs/Maquina/evidence/Dock_Full_Dump.img - 103 MB / 98 MiB

Partition      Start    End  Size in sectors
> P Unknown          0     1    12 140 23    201622

Unpacking libwxbase3.0-0v5:amd64 (3:0.5.1+dfsg-2) ...
Selecting previously unselected package libwxgtk3.0-gtk3-0v5:amd64.
Preparing to unpack .../libwxgtk3.0-gtk3-0v5_3.0.5.1+dfsg-2_amd64.deb ...
Unpacking libwxgtk3.0-gtk3-0v5:amd64 (3:0.5.1+dfsg-2) ...
Selecting previously unselected package wxhexeditor.
Preparing to unpack .../wxhexeditor_0.24+repack-1_amd64.deb ...
Unpacking wxhexeditor (0.24+repack-1) ...
Setting up libdidasim0:amd64 (0.23-6+b1) ...
Setting up libmhash2:amd64 (0.9.9.9-9) ...
Setting up libwxbase3.0-0v5:amd64 (3:0.5.1+dfsg-2) ...
Setting up libwxgtk3.0-gtk3-0v5:amd64 (3:0.5.1+dfsg-2) ...
Setting up wxhexeditor (0.24+repack-1) ...
Processing triggers for kali-menu (2021.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for libc-bin (2.31-11) ...
Processing triggers for mailcap (0.100.0) ...

[ Search ] [ Options ] >[File Opt] [ Quit ]
Modify file options
```

Figure 6

Leave all selected files, in order to recovery the whole content:

```
File Actions Edit View Help
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021 (currently installed.)
Christophe GRENIER <grenier@cgsecurity.org>_amd64.deb ...
https://www.cgsecurity.org

Selecting previously unselected package libmhash2:amd64.
Preparing to unpack .../libmhash2_0.9.9.9-9_amd64.deb ...
libmhash2:amd64 (0.9.9.9-9) ...
>[X] custom Own custom signatures
[X] 1cd Russian Finance 1C:Enterprise 8.0.5.1+dfsg-2_amd64.deb ...
[X] 3dm Rhino / openURBS
[X] 3ds 3d Studio
[X] 7z 7zip archive file
[X] DB Microsoft Database 0.0.0.0-0v5:amd64 (3:0.5.1+dfsg-2) ...
[X] a Unix Archive/Debian package
[X] abr Adobe Brush
[X] acb Adobe Color Book +repack-1) ...
[X] accdb Access Data Base (0.23-6+b1) ...
[X] ace ACE archive
[X] ab MAC Address Book
[X] ado Adobe Duotone Options
[X] afdesign afdesign
[X] ahd Ahnenblatt
[X] aif Audio Interchange File Format
[X] all Cubase Song file: .all

Next
Press s to disable all file families, b to save the settings
>[ Quit ] /mnt/hgfs/Maquina/evidence
Return to main menu
```

Figure 7

Select **b**, to save settings and then **Quit** to return to main window. Then, leave **P Unknown** option and select **Search**:



```
kali㉿kali: ~/Downloads/testdisk-7.2-WIP
File Actions Edit View Help
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021 currently installed.
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /mnt/hgfs/Maquina/evidence/Dock_Full_Dump.img - 103 MB / 98 MiB (RO)

Partition Start End Size in sectors
> P Unknown 0 0 1 12 140 23 201622

Preparing to unpack .../libwxgtk3.0-gtk3-0v5_3.0.5.1+dfsg-2_amd64.deb ...
Unpacking libwxgtk3.0-gtk3-0v5_amd64 (3.0.5.1+dfsg-2) ...
Selecting previously unselected package wxhexeditor.
Preparing to unpack .../wxhexeditor_0.24+repack-1_amd64.deb ...
Unpacking wxhexeditor (0.24+repack) ...
Setting up libidn2-0:amd64 (0.23-0+deb11u1) ...
Setting up liblmbase3-0-0v5:amd64 (0.9.9-9-9) ...
Setting up libwxbase3-0-0v5:amd64 (3.0.5.1+dfsg-2) ...
Setting up libwxgtk3.0-gtk3-0v5:amd64 (3.0.5.1+dfsg-2) ...
Setting up wxhexeditor (0.24+repack-1) ...
Processing triggers for kali-menu (2021.2.3) ...
Processing triggers for desktop-file-utils (0.29-1) ...
Processing triggers for libc-bin (2.31-11) ...

[ Search ] [ Options ] [ File Opt ] [ Quit ]
Start file recovery
```

Figure 8
Figure 9

Select other:

```
kali@kali: ~/Downloads/testdisk-7.2-WIP
File Actions Edit View Help
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021 currently installed.
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
Selecting previously unselected package libmhash2:amd64...
P Unknown unpack .../libmhash2:amd64_0.9.9.9-9
Unpacking libmhash2:amd64 (0.9.9.9-9)...
To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
[ ext2/ext3 ] ext2/ext3/ext4 filesystem
>[ Other ] FAT/NTFS/HFS+/ReiserFS/ ...

```

Figure 10

And finally, player must select folder to extract recovered files:



```
File Actions Edit View Help
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021 (currently installed.)
Preparing to unpack .../libdbsm0_0.23-6+01_amd64.deb ...
Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /mnt/hgfs/Maquina/evidence/recovery2
>drwxrwxrwx    0      0   0 Jul 15 2021 05:47 .
drwxrwxrwx  recovery2  0      0   0 Jul 15 2021 05:47 ..
Unpacking libwxgtk3.0-gtk3-0v5:amd64 (3.0.5.14dfsg-2) ...
Unpacking libwxgtk3.0-gtk3-0v5:amd64 (3.0.5.14dfsg-2) ...

```

Figure 11

Last step would be select **C** to confirm the folder. After Photorec finishes, Quit it. In the same folder that you must analyse recovered files. 7Z file was recovered but the JPG wasn't recovered:

```
(kali㉿kali)-[~/mnt/.../Maquina/evidence/recovery2/recup_dir.1] stalled.
$ ls
f0000000.7z  f0011246.txt  f0015438.txt  f0020009.txt  f0051077.txt
f0000444.txt  f0011248.txt  f0015439.txt  f0020220.txt  f0051078.txt
f0000447.txt  f0011249.txt  f0015441.txt  f0020262.txt  f0051079.txt
f0000448.txt  f0011251.txt  f0015445.txt  f0020264.txt  f0051082.txt
f0000449.txt  f0011252.txt  f0015447.txt  f0020321.txt  f0051083.txt
f0000489.txt  f0011255.txt  f0015448.txt  f0020332.txt  f0051084.txt
f0000729.txt  f0011256.txt  f0015449.txt  f0020333.txt  f0051087.txt
f0001205.txt  f0011258.txt  f0015469.txt  f0020381.txt  f0051088.txt
f0001376.txt  f0011259.txt  f0015471.txt  f0020429.txt  f0051089.txt
```

Figure 12

To extract the JPG file, it's mandatory to use wxHexEditor, to locate the header of the JPG file. Searching on Internet, you will find: https://www.garykessler.net/library/file_sigs.html

```
FF D8          ýØ
                   JPE, JPEG, JPG  Generic JPEGimage file
                   Trailer: FF D9 (ÿÙ)

NOTES on JPEG file headers: The proper JPEG header is the two-byte sequence, 0xFF-D8, aka Start of Image (SOI) marker. JPEG files end with the two-byte sequence, 0xFF-D9, aka End of Image (EOI) marker.

Between the SOI and EOI, JPEG files are composed of segments. Segments start with a two-byte Segment Tag followed by a two-byte Segment Length field and then a zero-terminated string identifier (i.e., a character string followed by a 0x00), as shown below with the JFIF, Exif, and SPIFF segments.

Segment Tags of the form 0x-FF-Ex (where x = 0..F) are referred to as APP0-APP15, and contain application-specific information. The most commonly seen APP segments at the beginning of a JPEG file are APP0 and APP1 although others are also seen. Some additional tags are shown below:

• 0xFF-D8-FF-E0 — Standard JPEG/JFIF file, as shown below.
• 0xFF-D8-FF-E1 — Standard JPEG file with Exif metadata, as shown below.
• 0xFF-D8-FF-E2 — Canon Camera Image File Format (CIF) JPEG file (formerly used by some EOS and Powershot cameras).
• 0xFF-D8-FF-E8 — Still Picture Interchange File Format \(SPIFF\), as shown below.

FF D8 FF E0 xx xx 4A 46          ýØÿà..JF
49 46 00                      IF.
                   JFIF, JPEG, JPG  JPEG/JFIF graphics file
                   Trailer: FF D9 (ÿÙ)

FF D8 FF E1 xx xx 45 78          ýØÿà..Ex
69 66 00                      if.
```

Figure 13

We don't know anything about the JPG file, so the main pattern to find the header would be: FF D8 FF. Use wxHexEditor to find it: Select the **magnifying glass**, and then insert the pattern, **find all**:

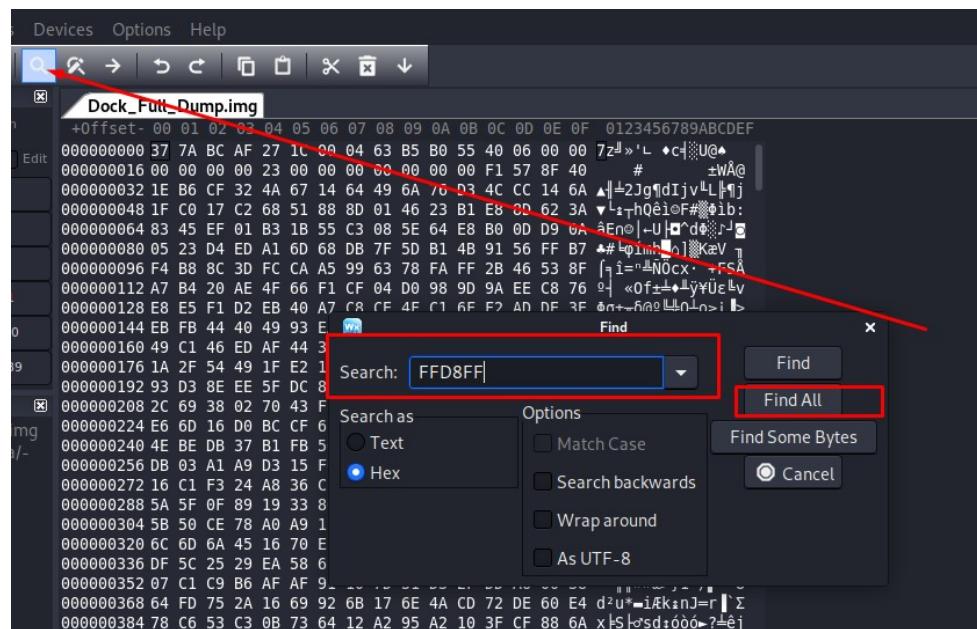


Figure 14

Finally found 334 matches:

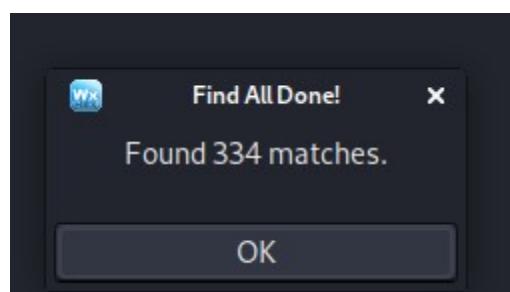


Figure 15

The key to extract the specific JPG file, would be to locate the last match. This means that the last match is the header of the file. (Keeping in mind, the footer is JPG file, and the footer of the evidence provided). On Search results windows you will find the results: OFFSET 103125280



- 330. Offset 100013535
- 331. Offset 100013537
- 332. Offset 100013539
- 333. Offset 100013541
- 334. Offset 103125280**

Figure 16

Figure 17



On this offset, right click and select:

- Copy Ctrl+C
- CopyAs Shift+Ctrl+C
- Paste Ctrl+V
- Cut Ctrl+X
- Delete
- Insert
- Save As Dump Ctrl+Alt+S
- Fill Selection
- Set Selection Block Start
- Quick Tag Ctrl+T
- New Tag Shift+Ctrl+T
- Tag Edit

Figure 18

Go to the end of the file, and repeat the step:

6272B10h 28 A ₂	CA CC CC AD CA CC CC AD CA CC CC AD CA CC CC	
6272B20h 28 A ₂	Copy	Ctrl+C
6272B30h 28 A ₂		
6272B40h 28 A ₂	CopyAs	Shift+Ctrl+C
6272B50h 28 A ₂	Paste	Ctrl+V
6272B60h 28 A ₂		
6272B70h 28 A ₂	Cut	Ctrl+X
6272B80h 28 A ₂		
6272B90h 28 A ₂	Delete	
6272BA0h 28 A ₂		
6272BB0h 28 A ₂	Insert	
6272BC0h 28 A ₂	Save As Dump	Ctrl+Alt+S
6272BD0h 28 A ₂		
6272BE0h 28 A ₂	Fill Selection	
6272BF0h 28 A ₂	Set Selection Block End	
6272C00h 28 A ₂		
6272C10h 28 A ₂	Quick Tag	Ctrl+T
6272C20h 28 A ₂		
6272C30h FF D _E	New Tag	Shift+Ctrl+T
	Tag Edit	

Figure 19



You will able to see the whole JPG file select, ready to extract from the evidence provided:

The screenshot shows a hex editor window titled "Dock_Full_Dump.img". The left side displays the offset of each byte, ranging from 00 to 0F. The right side shows the binary data as a grid of hex values (00-FF) and their corresponding ASCII representation. The file starts with a standard JPEG header (0xFF, 0xD8, 0xFF, 0xE0, etc.) followed by a large amount of compressed image data.

Figure 20

Finally extract the JPG file, selecting Edit -> Save as dump. There we, We've got it!

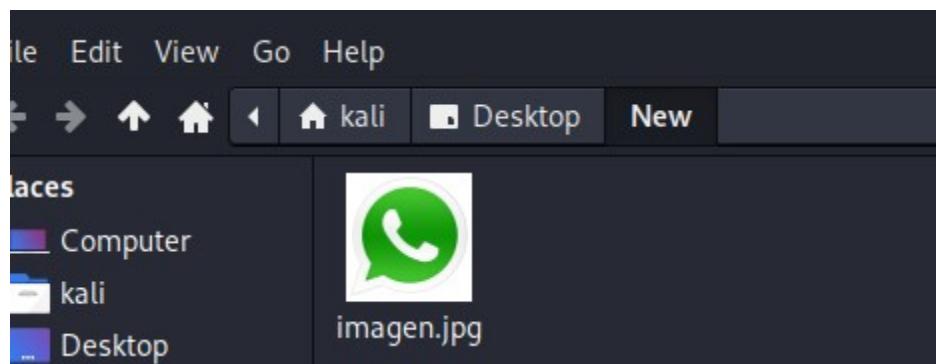


Figure 21

It's a whatsapp picture. This is the key to the following steps. A good one forensicator will test medata of the JPG files, using exiftool tool: `exiftool imagen.jpg`

```

File inode Change Date/Time      . 2021.07.15 00:38:32 +04:00
File Permissions : rw-r--r-- /libwxbase3.0-0v5:amd64.
File Type       : JPEG
File Type Extension : jpg
MIME Type      : image/jpeg
JFIF Version   : 1.01
Resolution Unit: inches
X Resolution   : 72
Y Resolution   : 72
Exif Byte Order: Big-endian (Motorola, MM)
Make           : This is the clue
Camera Model Name: file and file2
Warning        : Invalid EXIF text encoding for UserComment
User Comment   : cmp3.9.27.3q4 0xcdcf0d34
Padding        : (Binary data 2060 bytes, use -b option to e
xtract)

```

Figure 22

Pay attention on the above results: "This is the clue" and "file and file2". If you compare these clues with the content of the 7Z file, you will guess, that the image extracted is related to the 7Z file:

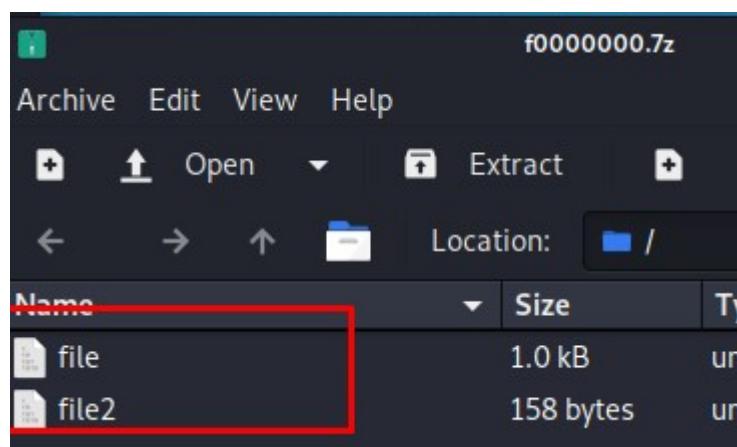


Figure 23

At this point, player has:

- File
- File 2
- Whatsapp JPG file pointing to file1 and file 2



File it's an SQLite Database encrypted using the steps like WhatsApp encryption. File2 , it's the key to decrypt the SQLite database.

File2:

file file2

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000000h	AC	ED	00	05	75	72	00	02	5B	42	AC	F3	17	F8	06	08	40 4ur @ [B ₄ ≤ ₁ ° A
000010h	54	E0	02	00	00	78	70	00	00	83	00	01	02	2B	9A	Ta@ xp â œœÜ	
000020h	FE	87	65	7E	34	94	18	D9	E7	8F	80	41	68	F3	33	8B ■ce~4öt τÅÇAh≤3i	
000030h	DE	9E	43	BD	54	68	D7	11	66	3E	50	4B	49	BD	D6	D7 ■sC Th f>PKI r	
000040h	6C	81	9B	F7	BE	70	4B	A6	3B	09	14	F9	6C	3A	77	47 lüç=PK@;o·l:wG	
000050h	44	0A	69	0E	90	3A	10	E1	72	8E	57	57	44	19	FF	C9 DgiñÉ:►BrÄWWd+ F	
000060h	3B	69	EF	E3	D8	F7	D8	DB	65	A5	B8	06	7B	26	00	00 ;innt=leÑ♦{&	
000070h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	D4	CF L	
000080h	9F	AE	2F	DF	C9	73	E9	C2	A0	D2	0A	A4	E9	C9	FF	15 f«/■fs0tåTçñ0F §	
000090h	49	17	7E	56	FB	FC	33	AC	C3	E7	BD	D0	CD	2D	I	z~V'n34 τJL=-	

Figure 24

File:

Figure 25



In this phase of the challenge, player could use a user friendly tool like WhatsApp parsers tools. The command to launch the tool would be: `python3 whapa-gui.py`

To use this tool, player must try to rename the file for the following options:

- file.crypt14
- file.crypt13
- file.crypt12

And so on... The correct option is **file.crypt12**. The ending of the file, indicate the type of the encryption. There is no other way to find out unless you try manually.



Figure 26

Select WhaCipher, locate the renamed file "file.crypt12", locate the key to decrypt and the output folder. Finally check the last button. Open an SQLite Data browser on Kali, and select the unencrypted database:

id	vaccine	vaccine_type	date
1	LAZARUS-PROT1	H2N1-01	2049-04-12 12:24:22.333
2	LAZARUS-PROT1	H2N1-02	2049-05-12 13:28:22.333
3	LAZARUS-PROT1	H2N1-03	2049-06-12 12:24:22.333
4	LAZARUS-PROT1	H2N1-05	2049-08-12 12:24:22.333
5	LAZARUS - PROT1	COVID19	2049-12-12 23:59:58

Figure 27

The flag would be: 2049-12-12 23:59:58



Flag

flag{2049-12-12 23:59:58}