



Mission Name

Flying to Euphea

History Background

After being in Paris with the librarian his next step is EUPHEA. Claire and Ethan must obtain authorization in the Recon Car to travel to Euphea.

Technical High-Level Overview

A network dump from a computer connected to a system that manages authorizations is provided to the player. This dump contains communication, that simulates traffic with Recon Permissions.

Short Description

Your goal is to analyse a communication from computer connected to Skytech Flight Authorization System and get any Security Code For the Skytech Flight Authorization System

Mission Description

A dump from the Skytech Flight Authorization System is provided to the player. Your goal is to analyse to get any Security Code for the Skytech Flight Authorization System

Location

PARIS, FRANCE | PREPARING TO DEPART



Tools

- Wireshark
- Zipcrack

Questions

Which is the number of the frame that contains ZIP file?

- 195

Which is the CRC of the unencrypted file?

- 2668E06B

Items

1. It's an USB capture
2. Several files have been transmitted.
3. The key to decrypt the compressed file is found in another file.

Write Up

Player must use Wireshark application in order to analyze this USB PCAP. Once opened, player should analyse deeply, to get files. Player must pay attention to URB_BULK_OUT packets, in order to get possible files:

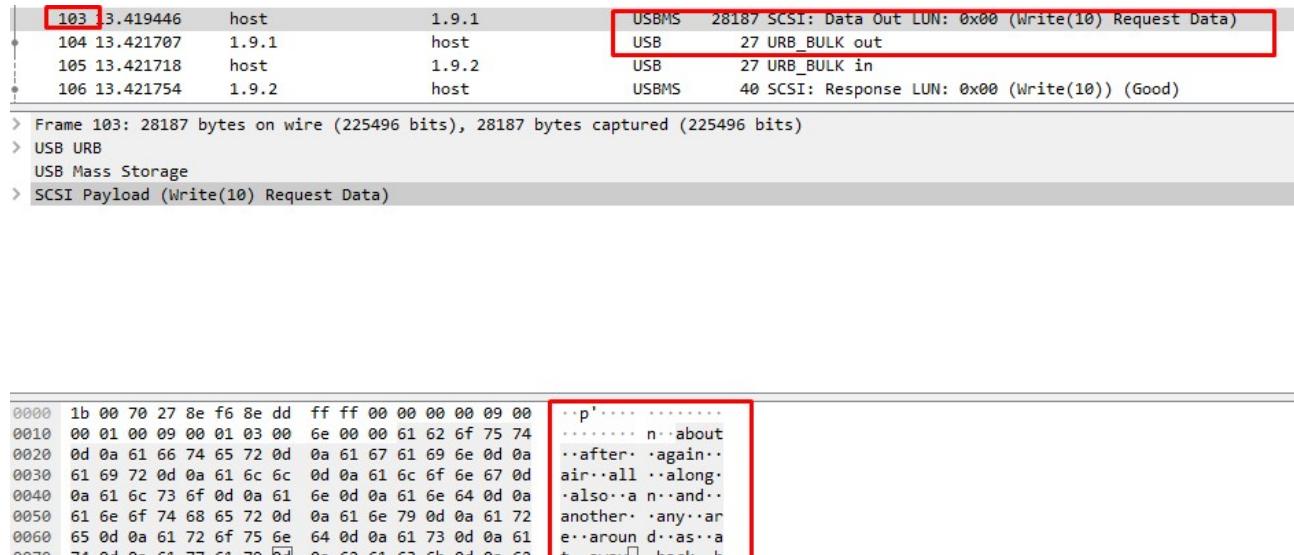


Figure 1

At frame 103, there is one file to export:

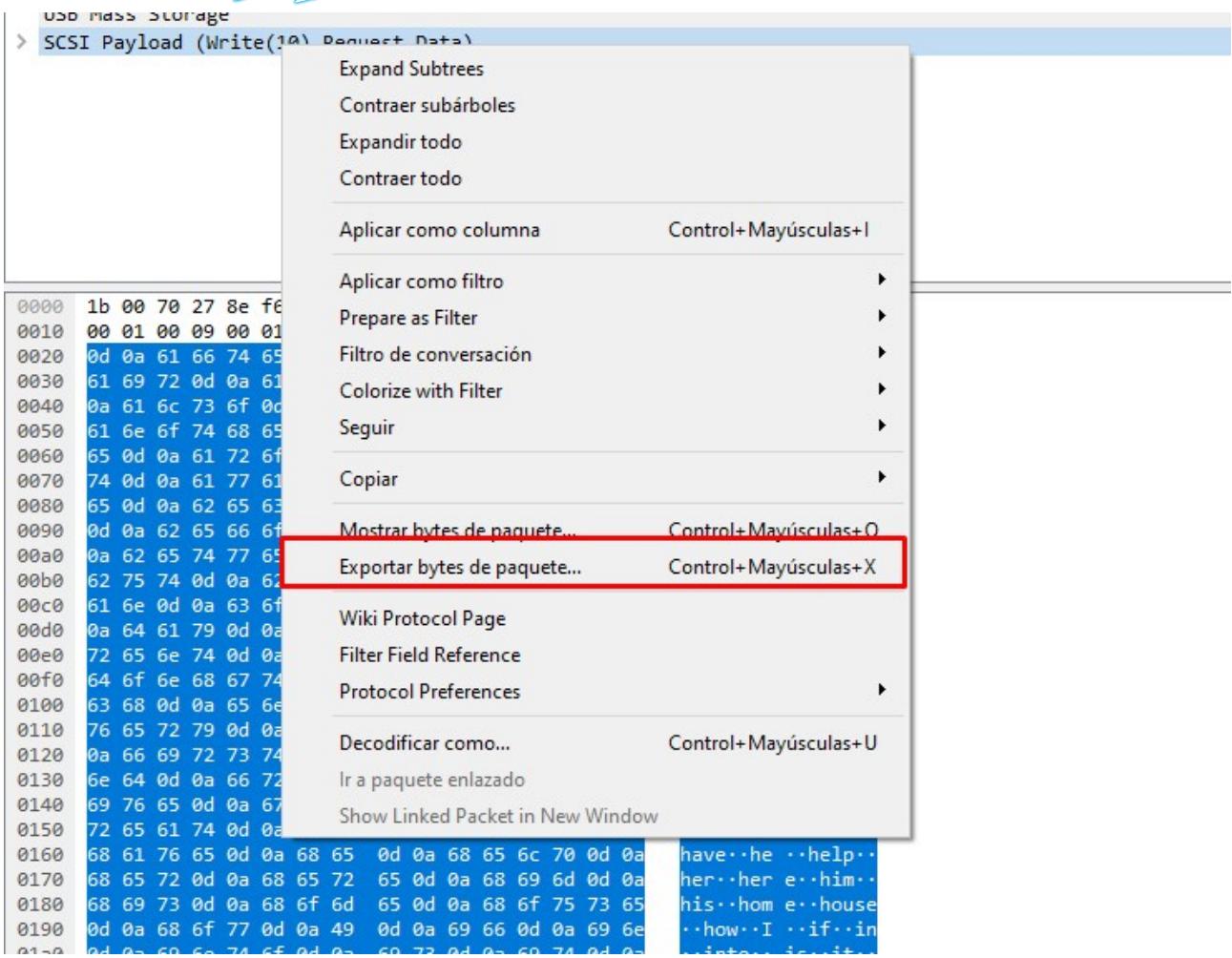


Figure 2

There we go:

```

1 about
2 after
3 again
4 air
5 all
6 along
7 also
8 an
9 and
10 another
11 any
12 are
13 around
14 as
15 at
16 away
17 back

```

Figure 3

It seems to be a dictionary.

And the last file found at frame 195:

194 3d.12588/	1.9.1	host	USB	27 URB_BULK OUT
195 3d.125889	host	1.9.1	USBMS	539 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
196 36.127776	1.9.1	host	USB	27 URB_BULK out
197 36.127826	host	1.9.2	USB	27 URB_BULK in
198 36.127842	host	1.9.2	USBCMC	10 SCSI: Response LUN0 Avail (Unit(10)) (Good)

> Frame 195: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
> USB URB
USB Mass Storage
> SCSI Payload (Write(10) Request Data)

```

0010 00 01 00 09 00 01 03 00 02 00 00 50 4b 03 04 14 .....PK...
0020 00 01 00 08 00 16 b3 aa 8a 6b e0 68 26 66 00 00 .....k-h&f...
0030 00 5f 00 00 00 0c 00 00 00 70 61 73 73 77 6f 72 .....password
0040 64 2e 74 78 74 fa 79 a5 41 23 6b f3 91 22 24 c0 d.txt y A#k- "$-
0050 ba db 06 ad ed f9 d2 07 f4 5c 6a b1 4f 05 cd f5 .....j-O...
0060 57 23 60 41 ef eb a4 75 67 40 4f 70 3a 42 54 79 W#`A- u g@Op:BTy
0070 e0 9a c3 65 6f cd e5 0c 9d d5 88 54 fa b9 91 c0 ...eo... T...
0080 03 91 29 be ab ed cc 27 58 20 3e 35 1d 7a 3c d1 ...)....' X >5 z<
0090 67 44 fc 50 b7 31 6e 70 3c 6f 60 14 ac d4 3a 70 gD·P·1np <o`...:p
00a0 34 41 57 58 d3 ef 18 0e 60 d0 88 50 4b 01 02 3f 4AwX....`PK-?
00b0 2a 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 L L82

```

Figure 4

It seems to be a ZIP file, due to file header "PK" and:

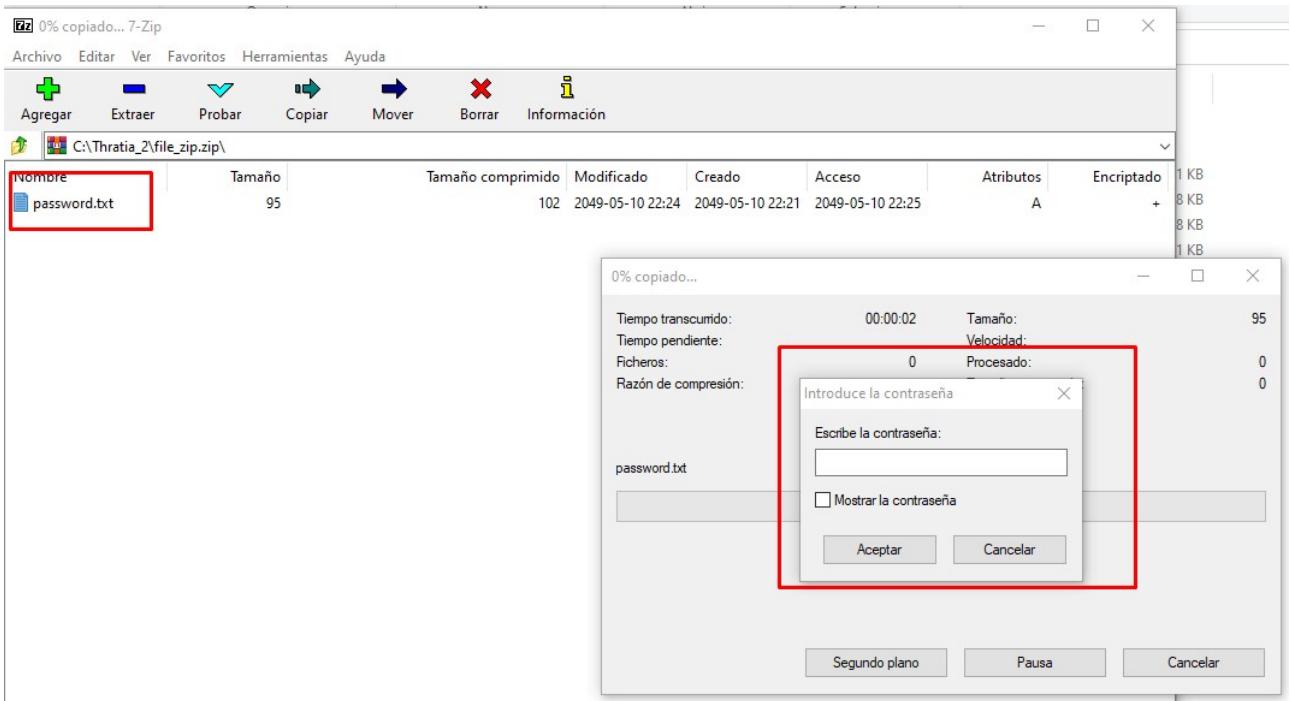


Figure 5

It's a ZIP file which needs a password. So considering dictionary found before, it's time to crack.



```
Usage: ZipCrack.exe [zip file] [dictionary file/letters] [type of attack]
Example:
- Dictionary: ZipCrack.exe ExampleFile.zip passwords.txt dictionary
- Brute force: ZipCrack.exe ExampleFile.zip abcdefghijklmnopqrstuvwxyz bruteforce

C:\Thratia 2>ZipCrack.exe file zip.zip data.bin dictionary
Starting dictionary attack..
Password matched: Flight_Authorization_System
Combinations tried: 3551
Time taken: 0.667236 seconds
```

Figure 6

Once password has been gained (Flight_Authorization_System) , next step would be to open ZIP file:

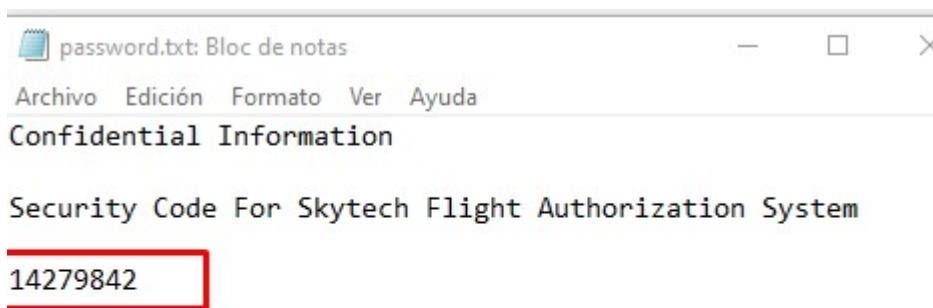


Figure 7

Finally player could get the security code : 14279842

Flag Information

flag{14279842}