



## 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:

103	13.419446	host	1.9.1	USBMS	28187 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
104	13.421707	1.9.1	host	USB	27 URB_BULK out
105	13.421718	host	1.9.2	USB	27 URB_BULK in
106	13.421754	1.9.2	host	USBMS	40 SCSI: Response LUN: 0x00 (Write(10)) (Good)

> Frame 103: 28187 bytes on wire (225496 bits), 28187 bytes captured (225496 bits)  
 > USB URB  
 > USB Mass Storage  
 > SCSI Payload (Write(10) Request Data)

0000	1b 00 70 27 8e f6 8e dd ff ff 00 00 00 00 09 00	..p'....
0010	00 01 00 09 00 01 03 00 6e 00 00 61 62 6f 75 74	..... n..about
0020	0d 0a 61 66 74 65 72 0d 0a 61 67 61 69 6e 0d 0a	..after..again..
0030	61 69 72 0d 0a 61 6c 6c 0d 0a 61 6c 6f 6e 67 0d	air..all ..along..
0040	0a 61 6c 73 6f 0d 0a 61 6e 0d 0a 61 6e 64 0d 0a	..also..a n..and..
0050	61 6e 6f 74 68 65 72 0d 0a 61 6e 79 0d 0a 61 72	another..any..ar
0060	65 0d 0a 61 72 6f 75 6e 64 0d 0a 61 73 0d 0a 61	e..aroun d..as..a

Figure 1

At frame 103, there is one file to export:

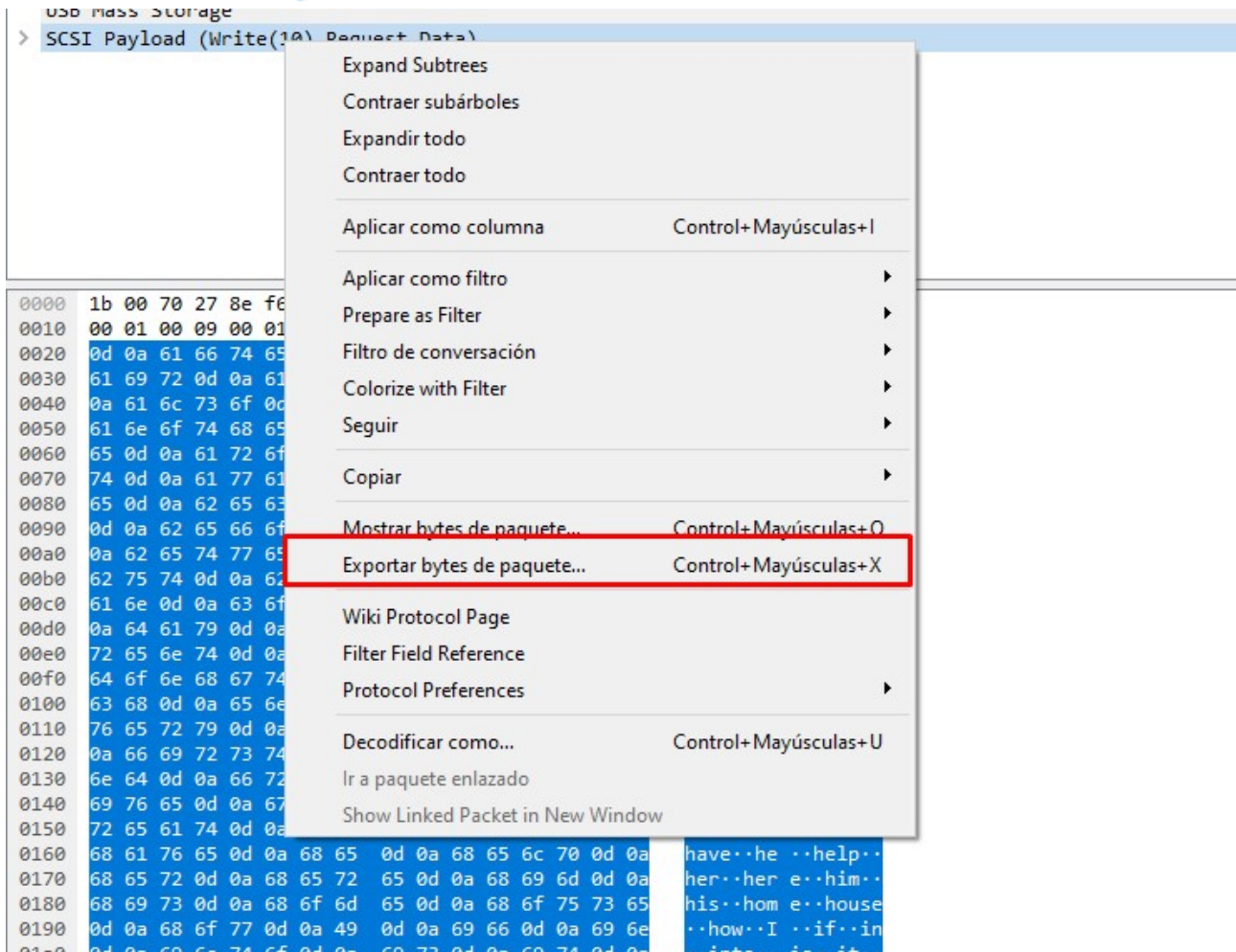


Figure 2

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:

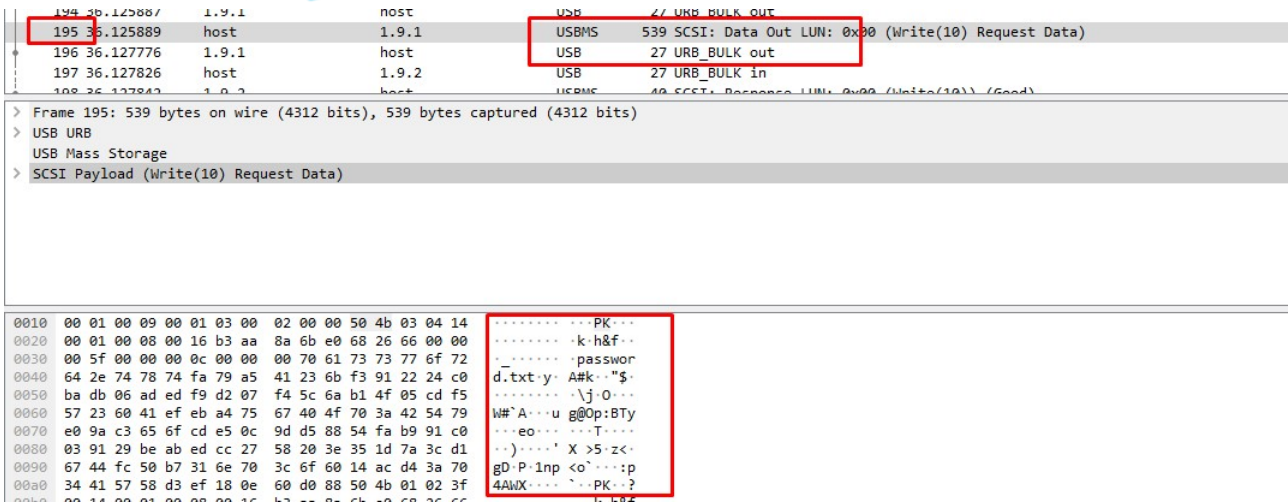


Figure 4

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

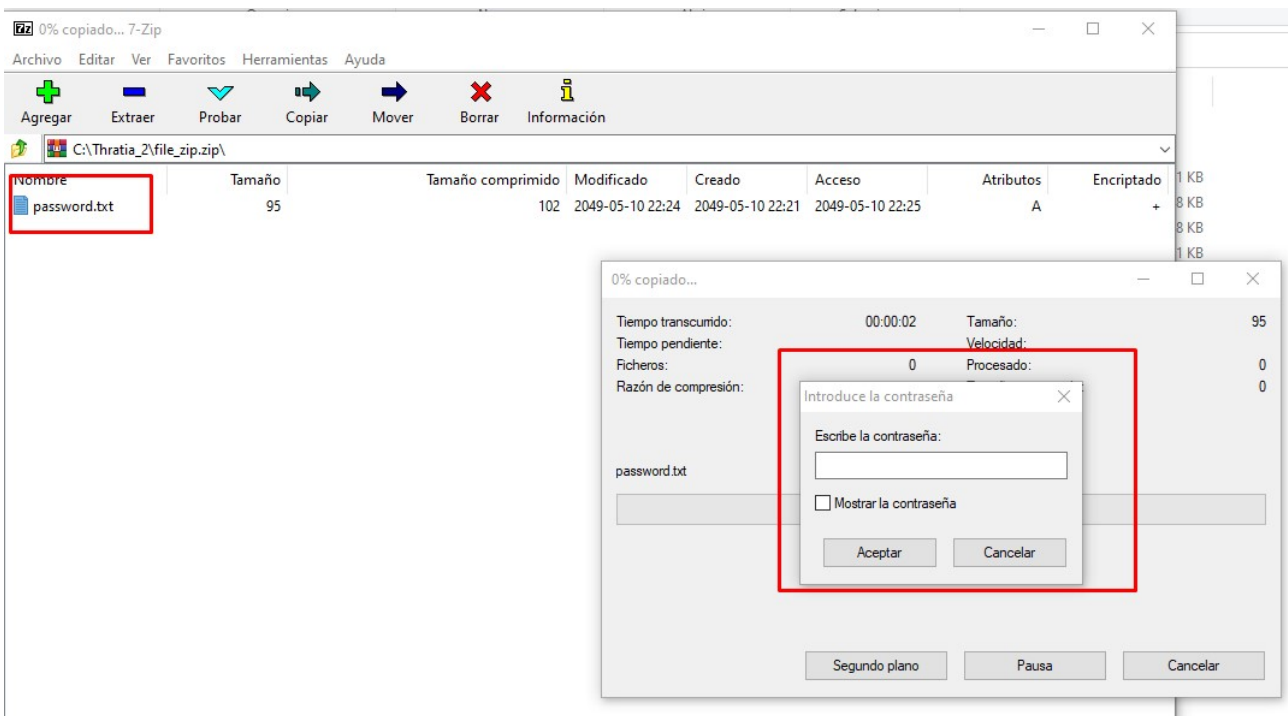


Figure 5

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:

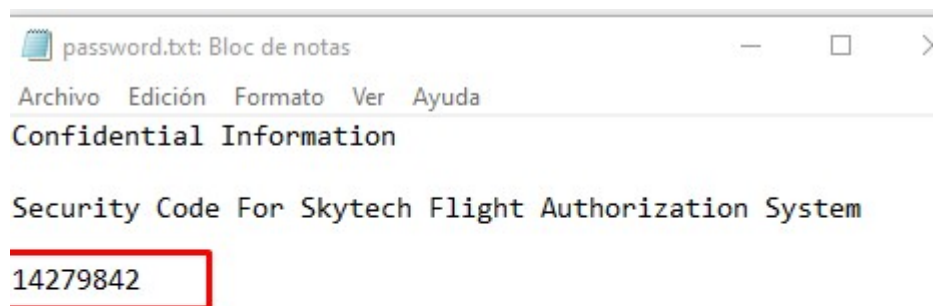


Figure 7

Finally player could get the security code : 14279842

## Flag Information

flag{14279842}