Mission Name

Fliying 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 ir 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:

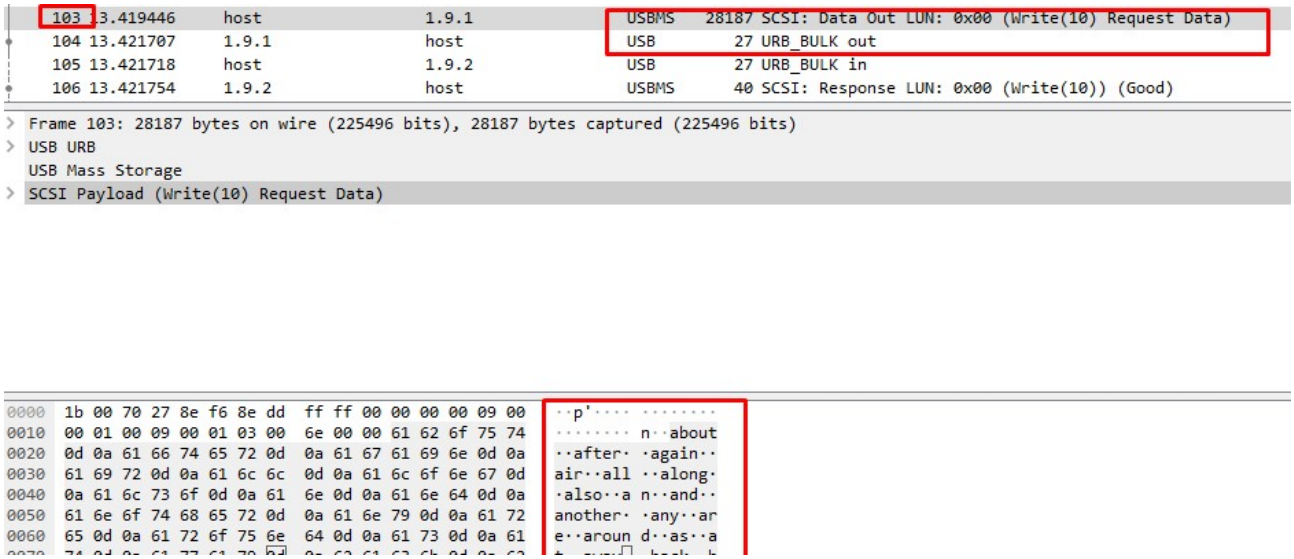

Figure 1

At frame 103, there is one file to export:

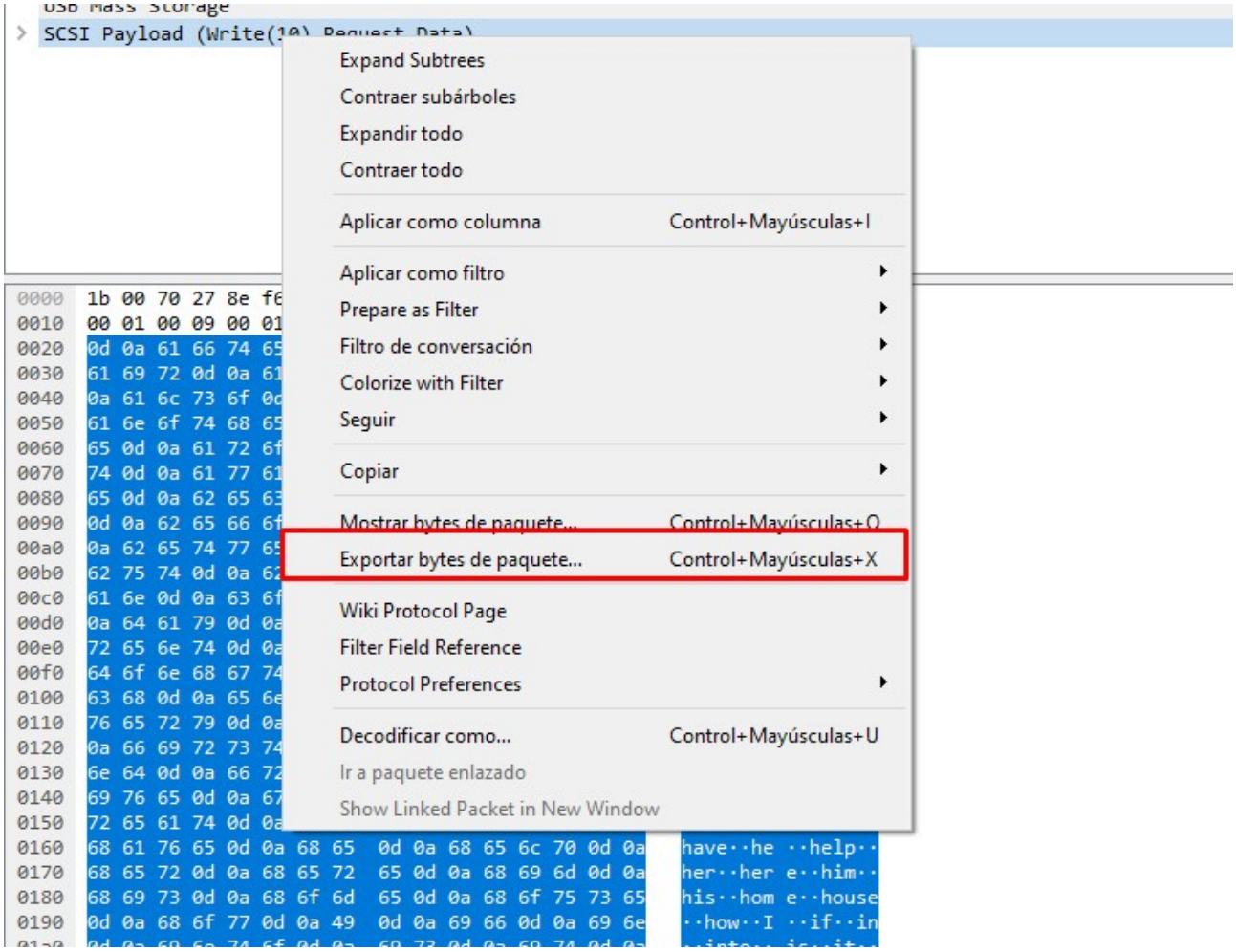

Figure 2

There we go:

```
about
after
again
air
all
along
also
an
and
another
any
are
around
as
at
away
back
```

Figure 3

It seems to be a dictionary.
And the last file found at frame 195:

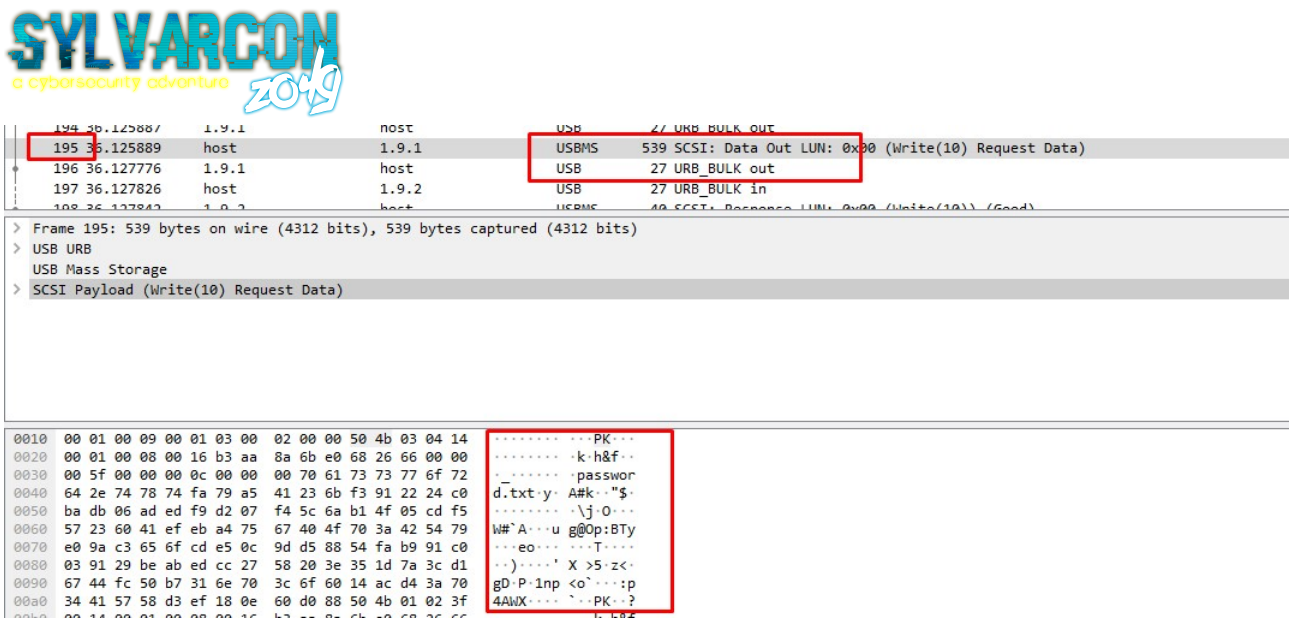

Figure 4

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

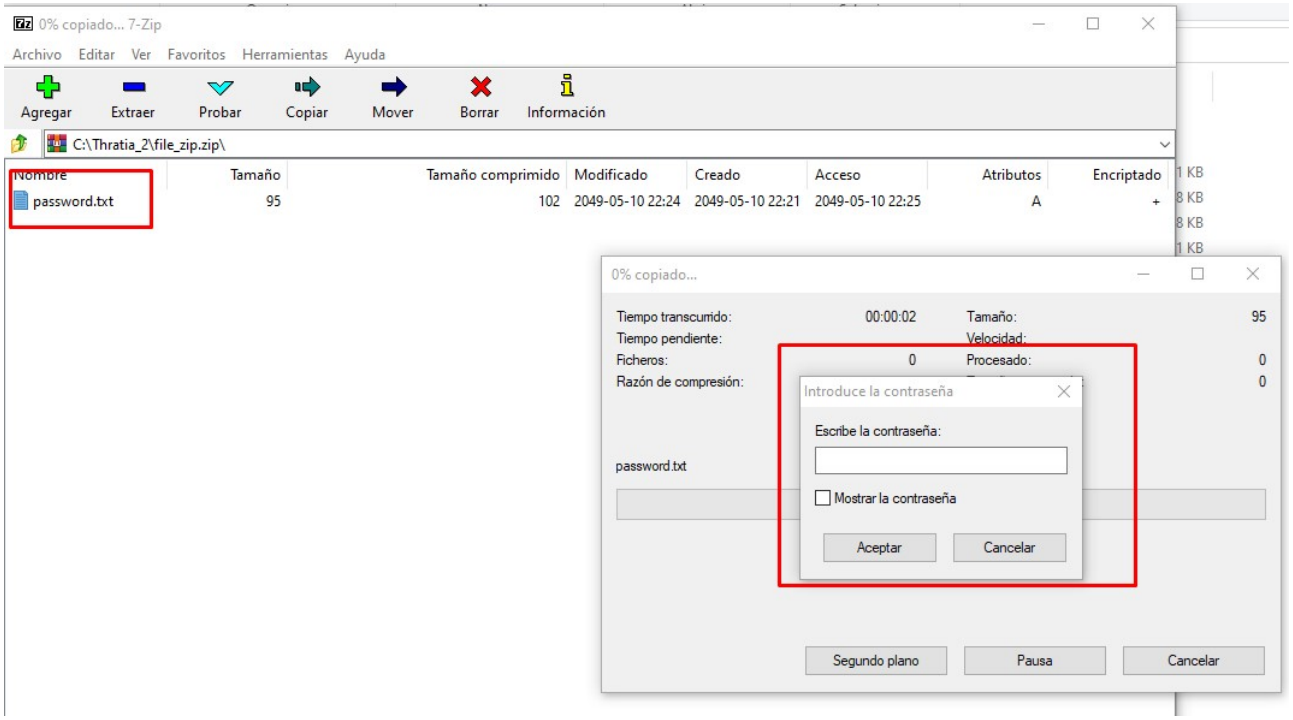

Figure 5

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:

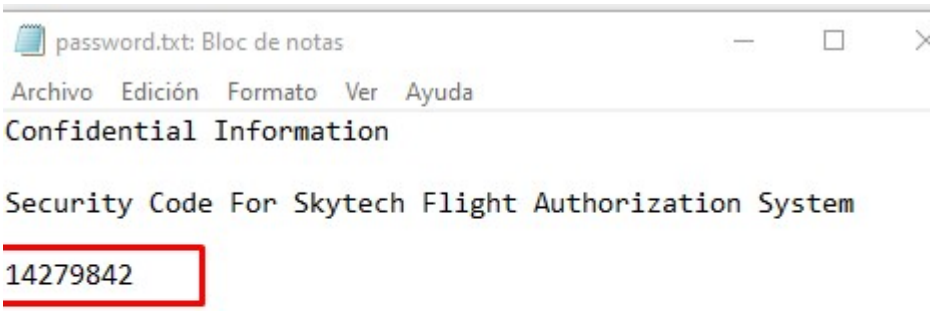

Figure 7

Finally player could get the security code : 14279842

Flag Information

flag{14279842}