Audio misc challenge

Categories: forensics, miscellaneous Solves: 16 Points: 380 Author: lVitaD

My friend Martin, a radio enthusiast, is on a trip to Europe. He promised me a picture of a place he liked a lot, but instead of images, he sent me only an incomprehensible audio! Can you help me, please?

The flag must be submitted in srdnlen{} format: wrap the found flag in srdnlen{}

The flag is a meaningful sentence.

By reading the description we can find two big hints: the friend's name is **Martin** and he is a **radio enthusiast**. This information is very helpful because – if we have any previous experience with SSTV (Slow-Scan Television) – we can already tell that it is, in fact, an **SSTV audio** created using the **Martin mode**.

In case we couldn't already tell, in the file's **EXIF data** we can find this comment: *SGludCA6IFNsb3cgU2xvdyBSYWRpbyBUcmFuc21pc3Npb24g*

If we decode this string from Base64, we get: *Hint :* ***Slow Slow Radio Transmission***

Wikipedia shows this definition of what SSTV is:

Slow-scan television (SSTV) is a picture transmission method, used mainly by amateur radio operators, to transmit and receive static pictures via radio in monochrome or color.[1]

So, what do we do now? It's simple, we need a decoder to show us what is the image!

For this challenge, I used a program called **QSSTV**[2], which is an SSTV open-source software, and, after decoding the WAV audio, it showed me an image (Figure 1) in which we can see the Sardinian flag and a string in front of it, *{MQ}4Af,T5q7JHx*.

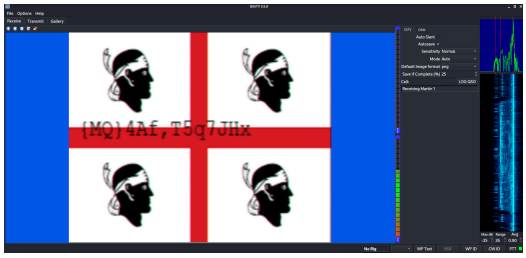

Figure 1: SSTV scan result

At first, I didn't know what this string meant... I thought, *maybe it is a crypted message containing the flag?* But after trying out various methods of decyphering and decoding, none of them seemed to give me a result so I just gave up.

Figure 2: Image containing the flag

Then, I started analyzing the file and I found a hidden RAR archive thanks to **binwalk**[3]. I tried opening it but it was protected by a password... Then, I tried using the string I saw on the image (Figure 1) and... Bingo! I found an image containing the flag (Figure 2). I just had to copy it and wrap it in the flag format (srdnlen{}).

Flag: **srdnlen{Wh4t_4_W0nd3rful_c1ty!!!}**

References

[1] Wikipedia. *Slow-scan television*. DOI: `https://en.wikipedia.org/wiki/Slow-scan_television`.

[2] GitHub. *QSSTV*. DOI: `https://github.com/ON4QZ/QSSTV`.

[3] Kali Linux. *binwalk*. DOI: `https://www.kali.org/tools/binwalk/`.