

For this challenge, we got at our disposal a png file, named here “pokedex.png”.

Une image contenant texte

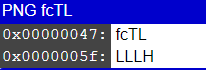
Description générée automatiquementFirst thing we do is check the metadatas of this file, and that’s we find :

Now we know that our file isn’t a simple png, but an animated png, AKA apng. Next, I’ve tried a lot of things on this file, like disassemble it and look deeper in the images that are in the apng file, but nothing very interesting...

After several hours of tearing my hair out, I realized that the solution maybe wasn’t in the png files inside de apng. I tried more things on the apng file directly, and I read about the structure of an apng file, from which I didn’t knew a lot.

I leaned that the apng structure is a succession of fcTL and fDAT chunks, which is what we probably need to focus on. I managed to find this website : <https://fotoforensics.com>

Next thing is to upload the apng file into the website and see what it will find.

If we go in the “Strings” section in the analysis section, we can see that the website has separated all the chunks. If we look in the fcTL chunks, we can see that most of the time, one letter stands out from the rest. Now, I tried to concatenate all the letters that I manage to get from these chunks.

I first found this :

I putted blank spaces when the chunk was empty, so I thought that some letters were missing at these emplacements. I tried to guess all the missing letters to finally get the flag :