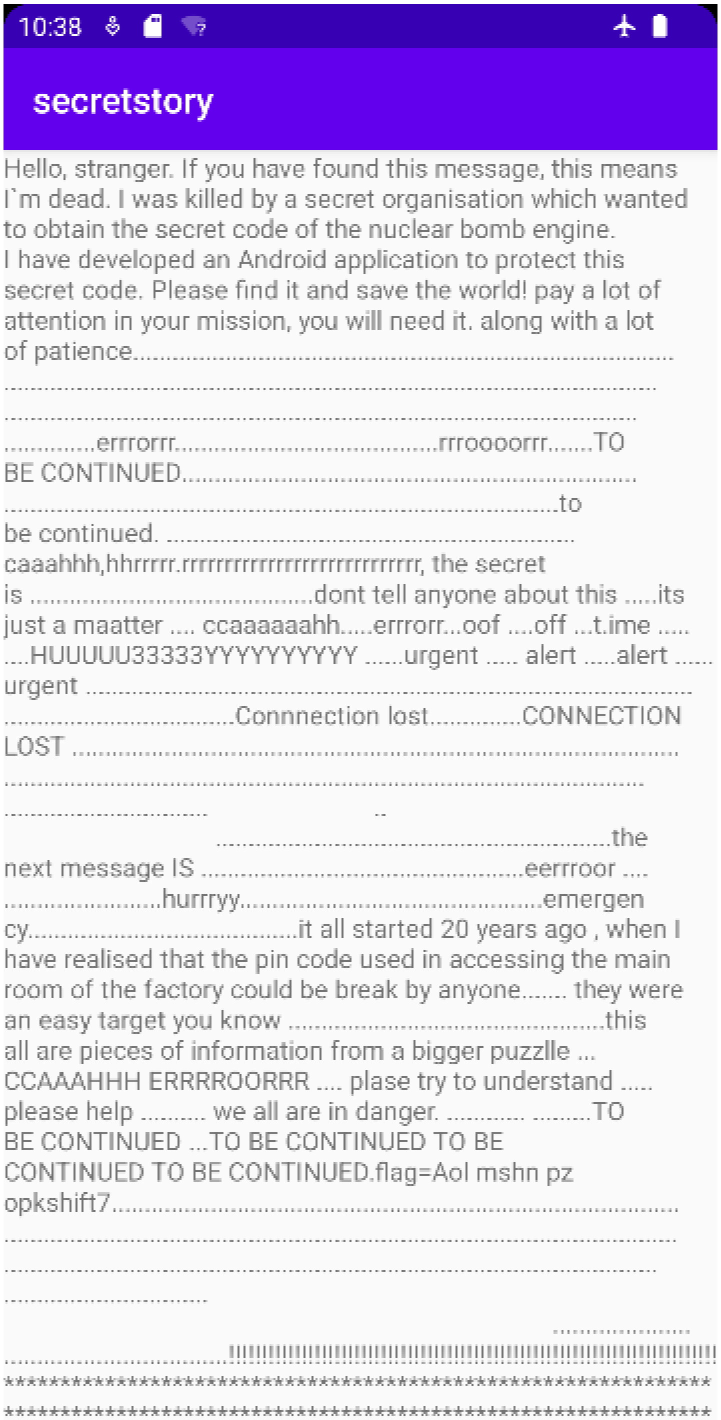
We have and apk. This means there are 2 essentials things we need to do. This is true anytime we have an apk.

1. Emulate it. Personally, I use Android Studio since it's the most reliable. The trick is to Profile/Debug apk, not just open it. Anyway, let's see what this app do!



Ok….. So, as general pieces of info, we know there might be a **PIN** code, and **flag=Aol mshn pz opkshift7** might mean something.

Turns out, the entire text is in **activity_main.xml**

The difference? **flag=Aol mshn pz opkklu pu aol zhtwsl dhc mpsl. Thfil zuhrlz jhu olsw //shift7**

The flag is obviously encoded with Caesar Shift or ROT, so we simply need to use dcode.fr to decode it:

→7 (←19)	The flag is hidden in the sample wav file. Maybe snakes can help

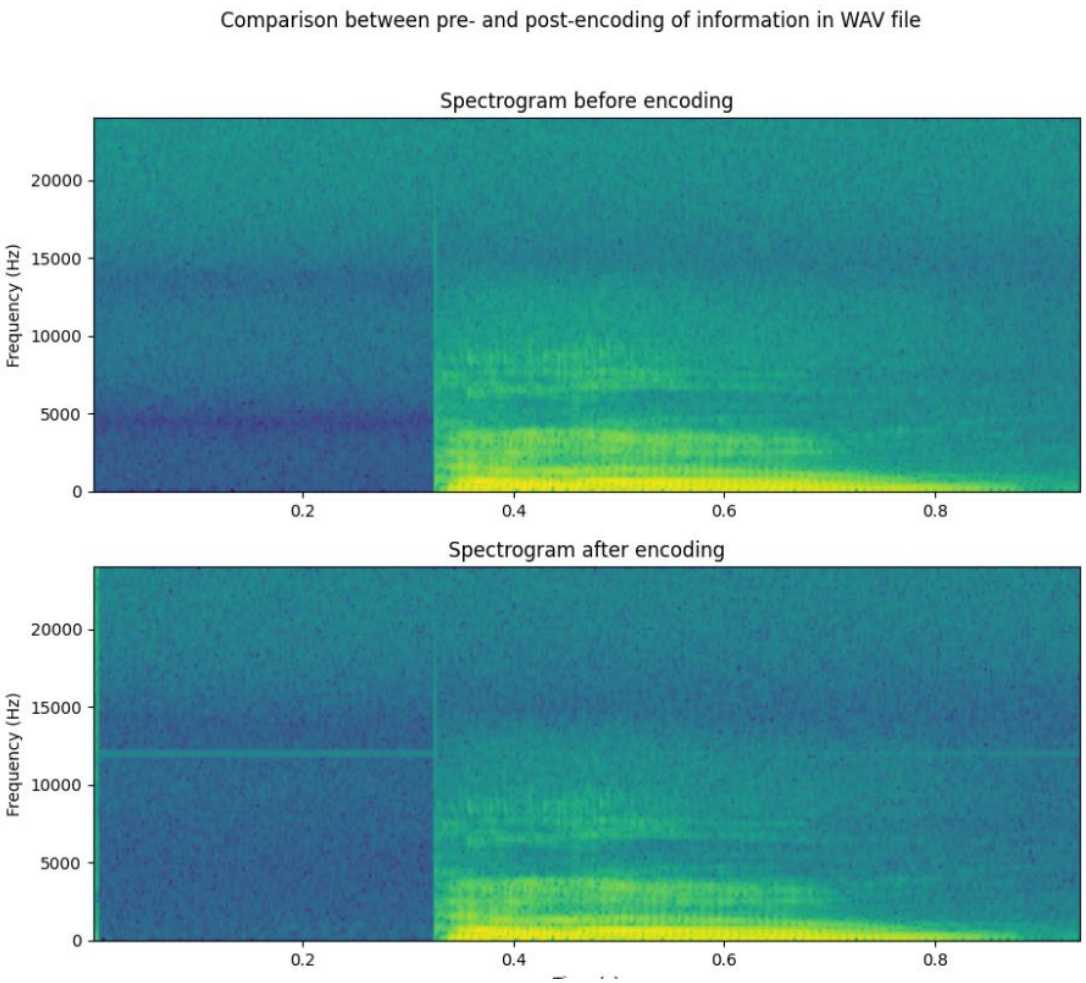
Ok, so next up we need to investigate a wav file.

And the wav file is… an explosion? That doesn't trick me, time to look at the spectrogram.

Nothing… well, we were told "snakes" can help, so we may need to make a script. This leads me to think something along the lines of LSB/MSB steganography, or something hidden in the text composing the audio file anyway.

While researching, I found something particularly interesting: https://github.com/LiquidFun/stegowav.

Namely:



See that “line” in the after encoding image? WE HAVE THAT TOO!

Using https://github.com/techchipnet/HiddenWave/blob/main/ExWave.py we can easily recover the flag. The main trick is that we need to extract LSB of each byte, not each pair of 2 bytes as it is more commonly done.

Made with love by: AndreiCat