Category

Cryptography / Forensics

Challenge description

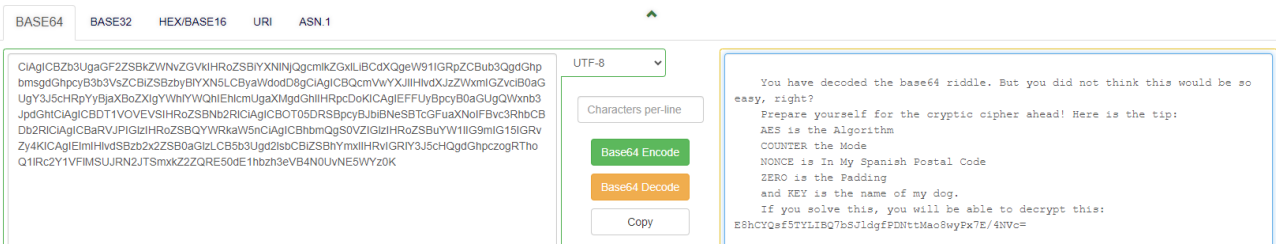
Some time ago, Victoria hid their master password in her PC. But she needs it now and she cannot remember what she must do to recover it from their data. Can you help her? Her password is the flag you are looking for 😉.

Hints

- {LEVEL 1} Try to explore the folders and find suspicious files. The information might be encoded so anyone cannot access it accidentally.
- {LEVEL 2} After decoding the first message you will get a lot of information. Just try to find the missing things you need for decrypt the password.
- {LEVEL 3} Use Base64 to decode the file and then use AES algorithm in CTR mode to decrypt the password. To get the parameters that you need for the algorithm just look in the rest of the files of the folder using the puzzle message you decode in the first step.

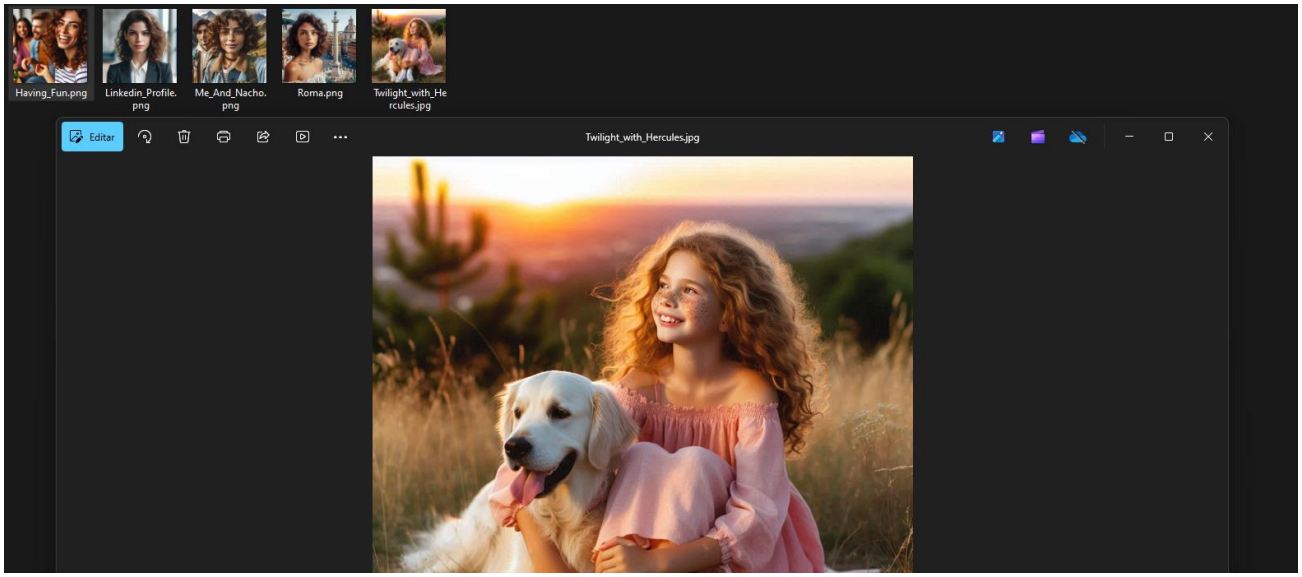
Write Up

Looking at the folders we can find a file called “my_best_secret.txt” which takes our attention. If we open it, we will discover that the file is not readable by humans. But if we enter the text in a base64 decoder …



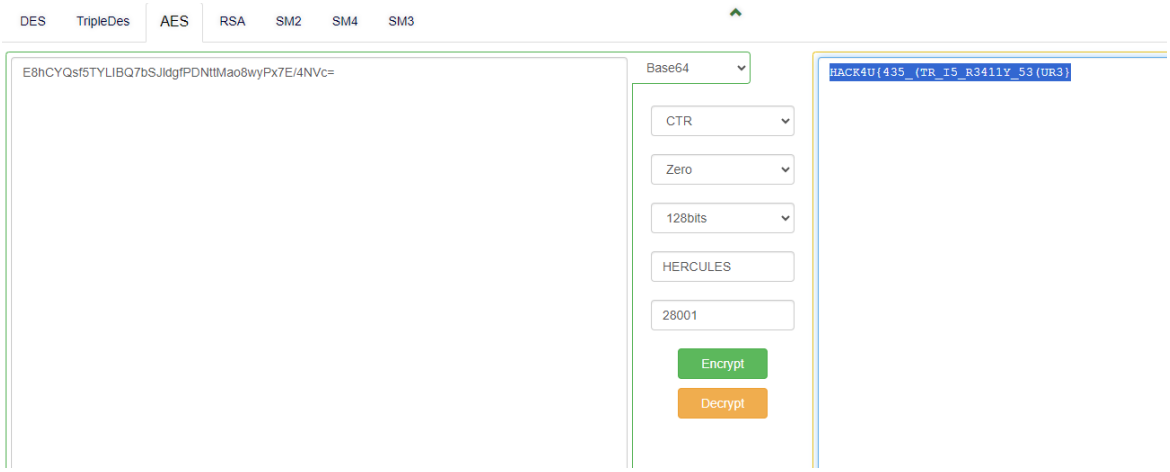
So we can look information about AES algorithm and their modes of operation, and every other thing that we don’t understand in the text. Once we understand what we need, we will look in the rest of the files looking for the information we are missing.

We can find that the name of the dog is **Hercules** in a photography.



And in their CV we can find that their postal code is 28001.

So, with this information, we can go to any decryption tool that supports AES CTR and using it with the appropriate configuration, we will finally get the flag.



Flag

`HACK4U{435_(TR_I5_R3411Y_53(UR3}`