



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

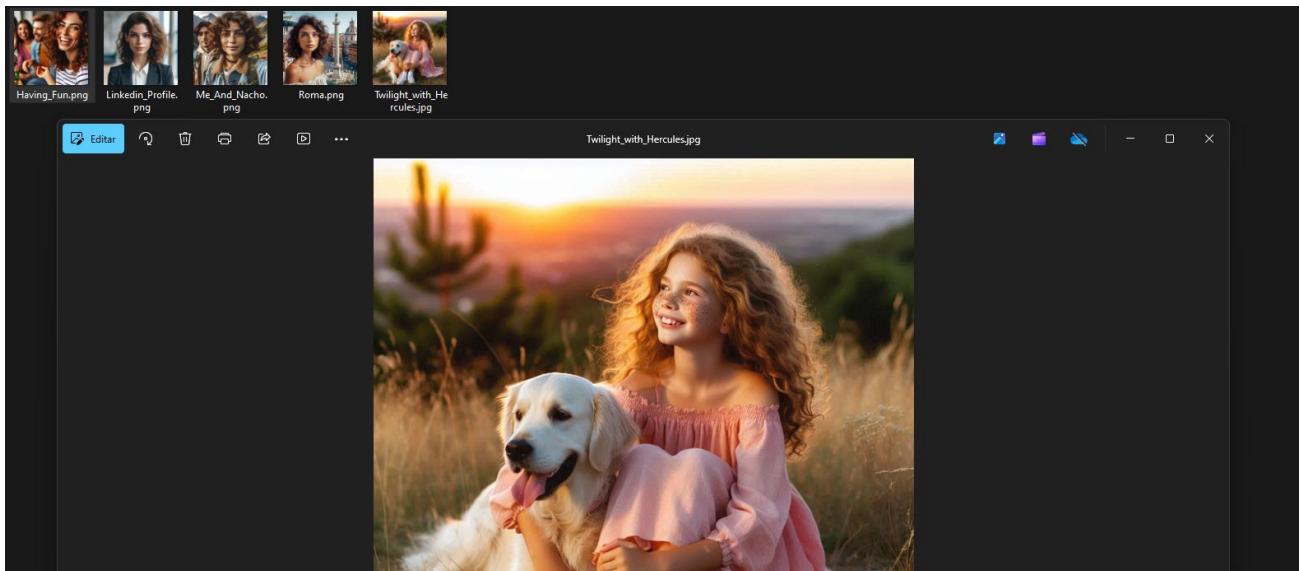
Looking at the folders we can find a file called “my_best_secret.txt” which takes our attention. If we open it, we will discover that the file is not readable by humans. But if we enter the text in a base64 decoder ...

The screenshot shows a web-based base64 decoder interface. At the top, there are tabs for BASE64, BASE32, HEX/BASE16, URI, and ASN.1. The BASE64 tab is selected. Below the tabs is a text input field containing a long base64 encoded string. To the right of the input field is a dropdown menu set to "UTF-8" and a "Characters per-line" input field set to 80. Below these are three buttons: "Base64 Encode" (disabled), "Base64 Decode" (highlighted in orange), and "Copy". To the right of the buttons is a text area containing the decoded message:

```
You have decoded the base64 riddle. But you did not think this would be so easy, right?  
Prepare yourself for the cryptic cipher ahead! Here is the tip:  
AES is the Algorithm  
COUNTER is the Mode  
NONCE is In My Spanish Postal Code  
ZERO is the Padding  
and KEY is the name of my dog.  
If you solve this, you will be able to decrypt this:  
E8hCYQsF5TYLJzQ7bsJldgfPmNttMa8wyFx7E/4NVc=
```

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.

The screenshot shows a web-based AES decryption tool. At the top, there are tabs for DES, TripleDes, AES, RSA, SM2, SM4, and SM3. The AES tab is selected. Below the tabs, there is a large input field containing the ciphertext: E8hCYQsf5TYLIBQ7bSJldgfPDNttMao8wyPx7E/4NVc=. To the right of this field is a dropdown menu set to "Base64". Further down, there are several configuration options: "Mode" (set to "CTR"), "IV" (set to "Zero"), "Key Length" (set to "128bits"), "Key" (containing the hex value "HERCULES"), and "Nonce" (containing the hex value "28001"). Below these options are two buttons: a green "Encrypt" button and an orange "Decrypt" button. To the right of the configuration area, the decrypted flag is displayed in a blue-bordered box: HACK4U{435_(TR_I5_R3411Y_53(UR3)}.

Flag

HACK4U{435_(TR_I5_R3411Y_53(UR3)}