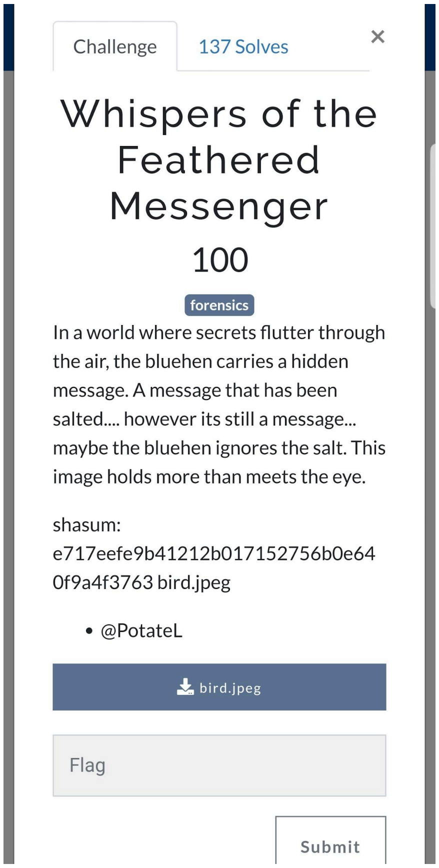


Challenge 137 Solves ×

Whispers of the Feathered Messenger

100

forensics

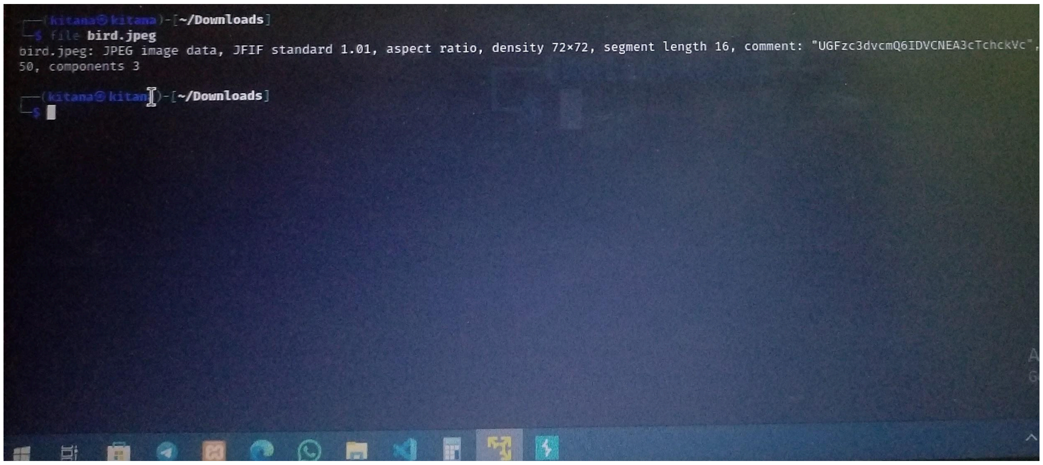
In a world where secrets flutter through the air, the bluehen carries a hidden message. A message that has been salted.... however its still a message... maybe the bluehen ignores the salt. This image holds more than meets the eye.

shasum: e717eefe9b41212b017152756b0e640f9a4f3763 bird.jpeg

- @PotateL

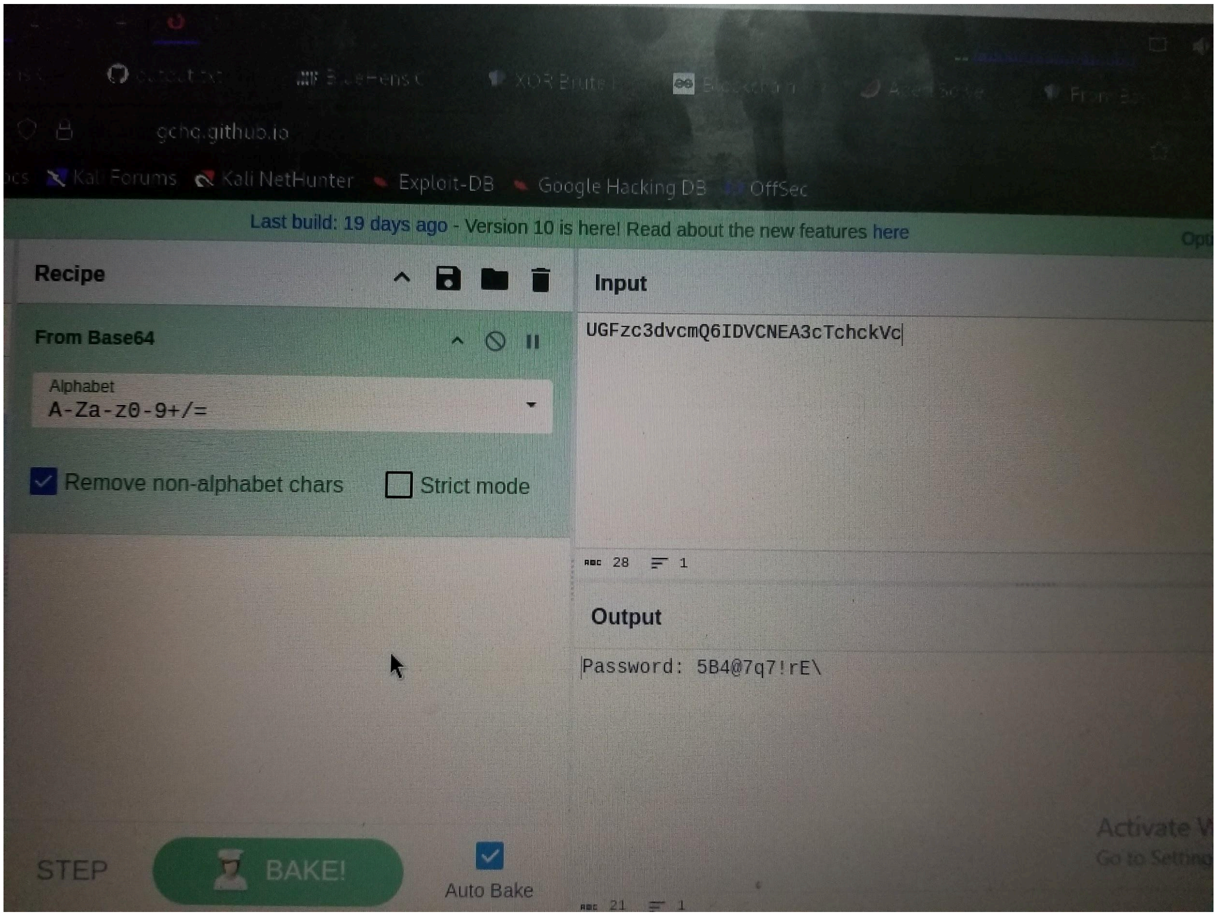
>in this challenge there was a jpeg image

>running files on this image revealed a note encoded in base64



```
┌──(kitana㉿kitana)-[~/Downloads]
└─$ file bird.jpeg
bird.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 72×72, segment length 16, comment: "UGFzc3dvcmQ6IDVCNEA3cTchckVc",
50, components 3

┌──(kitana㉿kitana)-[~/Downloads]
└─$ 
```

>decoding the base64 using cyberchef we get that it is a password



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

Input

```
UGFzc3dvcmQ6IDVCNEA3cTchckVc
```

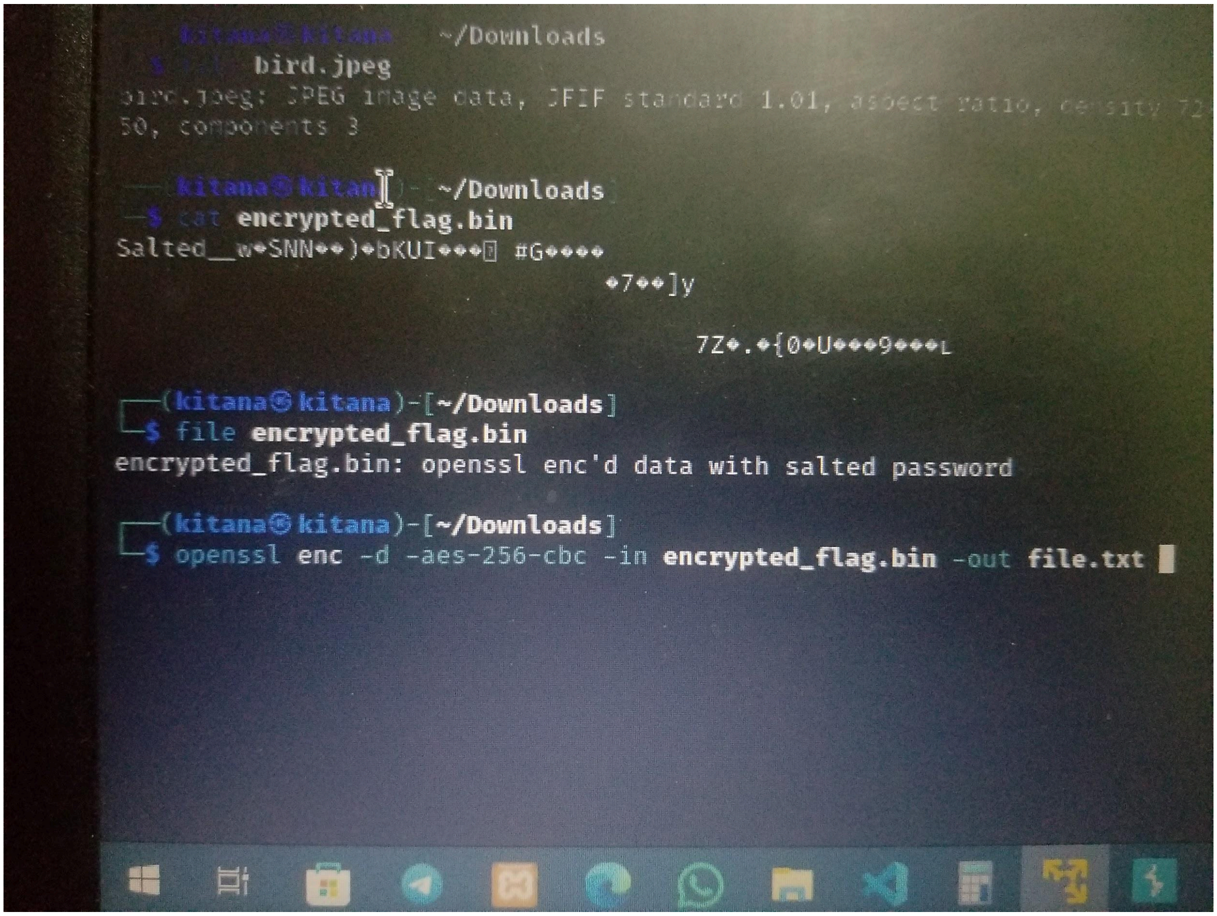
28 1

Output

```
Password: 5B4@7q7!rE\
```

21 1

>now we run steghide with the password to get the embedded file(encrypted flag.bin) which is encrypted using openssl

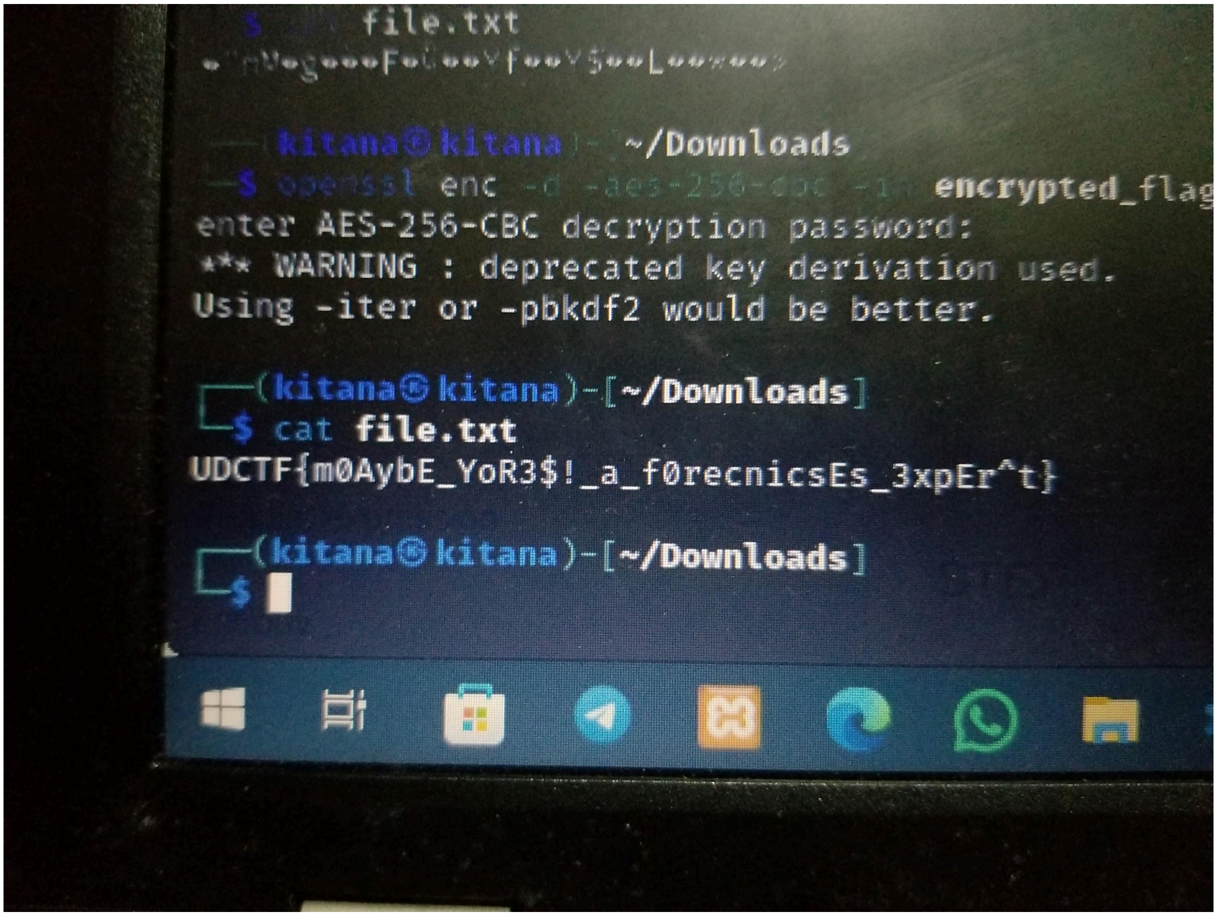


```
  kitana㉿kitana  ~/Downloads
  $ file bird.jpeg
bird.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 72
50, components 3

┌──(kitana㉿kitana)-[~/Downloads]
└─$ cat encrypted_flag.bin
Salted__w◆SNN◆◆)◆bKUI◆◆◆▯ #G◆◆◆◆
                                                ◆7◆◆]y

                                                              7Z◆.◆{0◆U◆◆◆9◆◆◆L

┌──(kitana㉿kitana)-[~/Downloads]
└─$ file encrypted_flag.bin
encrypted_flag.bin: openssl enc'd data with salted password

┌──(kitana㉿kitana)-[~/Downloads]
└─$ openssl enc -d -aes-256-cbc -in encrypted_flag.bin -out file.txt
```

>After reading how to decrypt openssl i used the code above and when it asks for password use the one provided

>my decrypted output was stored in file.txt

>so i cat the file.txt to reveal the flag



```
  $ cat file.txt
[illegible]

┌──(kitana㉿kitana)-[~/Downloads
└─$ openssl enc -d -aes-256-cbc -in encrypted_flag
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kitana㉿kitana)-[~/Downloads]
└─$ cat file.txt
UDCTF{m0AybE_YoR3$!_a_f0recnicsEs_3xpEr^t}

┌──(kitana㉿kitana)-[~/Downloads]
└─$ █
```

UDCTF{m0AybE_YoR3$!_a_f0recnicsEs_3xpEr^t}