

Open in app ↗



Search



★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#) ✕

# Intigriti CTF write up for OSINT , Cryptography challenges



dnelsaka · Follow

5 min read · 1 day ago



Listen



Share

... More

Hello It's me youssef a Web/OSINT CTF player and currently learning cryptography

##Challenge 1 : ( OSINT ) Difficulty : Medium

Challenge

54 Solves

✕

## Photographs

### 388

Can you help us track down this photographer? 📷

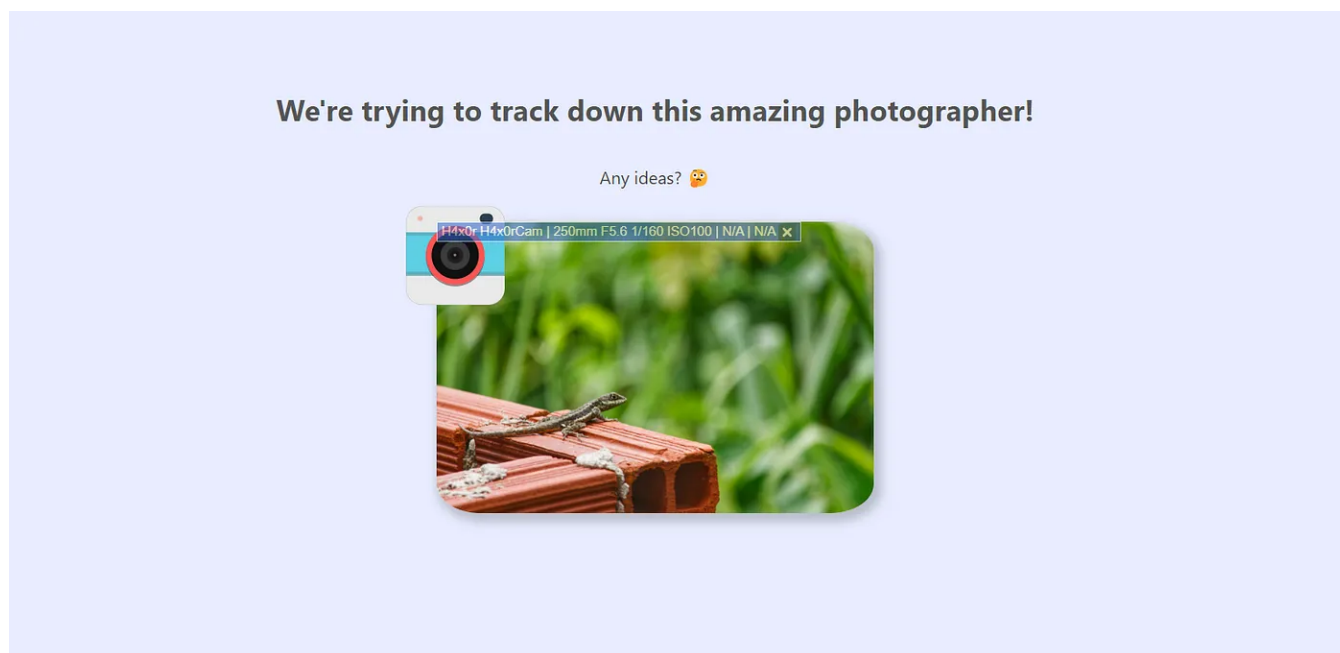
Author: therealbrenu

<https://photographs.ctf.intigriti.io> ||  
<https://photographs2.ctf.intigriti.io>

Flag

Submit

After opening the challenge photo which is a lizard I tried as everyone would do in the first thing to lookup at this image using **\*\*Google Index Research\*\*** but we found nothing so that it's not about image research it's maybe could be a **METADATA**



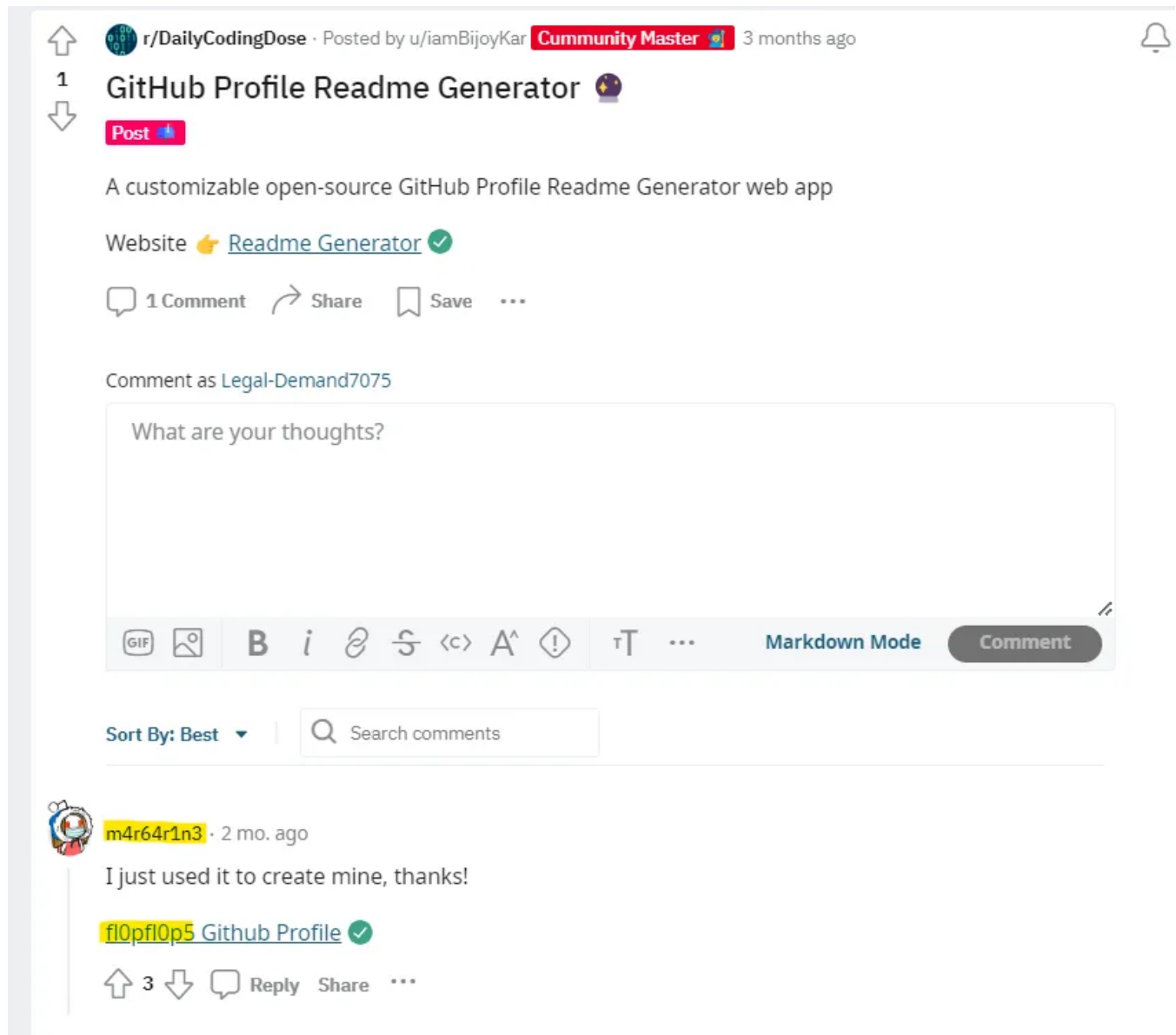
so after downloading the image and opened any tool that may extract photo details I'm always using this website [aperisolve](https://www.aparisolve.com/)

after uploading here we can see the artist name is : **f10pf10p5**

A screenshot of the ExifTool application interface. The title "ExifTool" is in the top left. The main area displays a list of metadata fields and their values. The "Artist" field is highlighted in green and contains the value "f10pf10p5".

Resolution	72
YResolution	72
ResolutionUnit	inches
ModifyDate	2023:09:25 23:42:32
Artist	f10pf10p5
Padding	(Binary data 2060 bytes, use -b option to extract)
EXIFIFD	
ExposureTime	1/160

so i thought that is the end of the challenge but it's not they are asking for an actual flag so we need to lookup at this username we didn't find much social media accounts just (reddit and an empty medium account) but after investigating and watching his profile we found that we have another account name !



then the artist have another name which is **m4r64r1n3** so after looking up on this name we found a Twitter account using googling

so after opening his Twitter account at the first sight you'll notice nothing same as I but I remembered that this challenge is about a photographer and he have a post said that "*A picture of just a little bird that I recently took :)*" then i started to suspect that this is the challenge completion



## Post

**m4r64r1n3**

@m4r64r1n3



A picture of just a little bird that I recently took :)

#photography #birds #birdphotography #telephotography  
#blackandwhitephotography



and yeah nothing actually surprising I took the same photo and tried the same process again

1. Image Reverse Using google hell no we got another username called : **v1ck1v4l3**



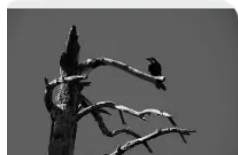
Reddit

v1ck1v4l3 (u/v1ck1v4l3)

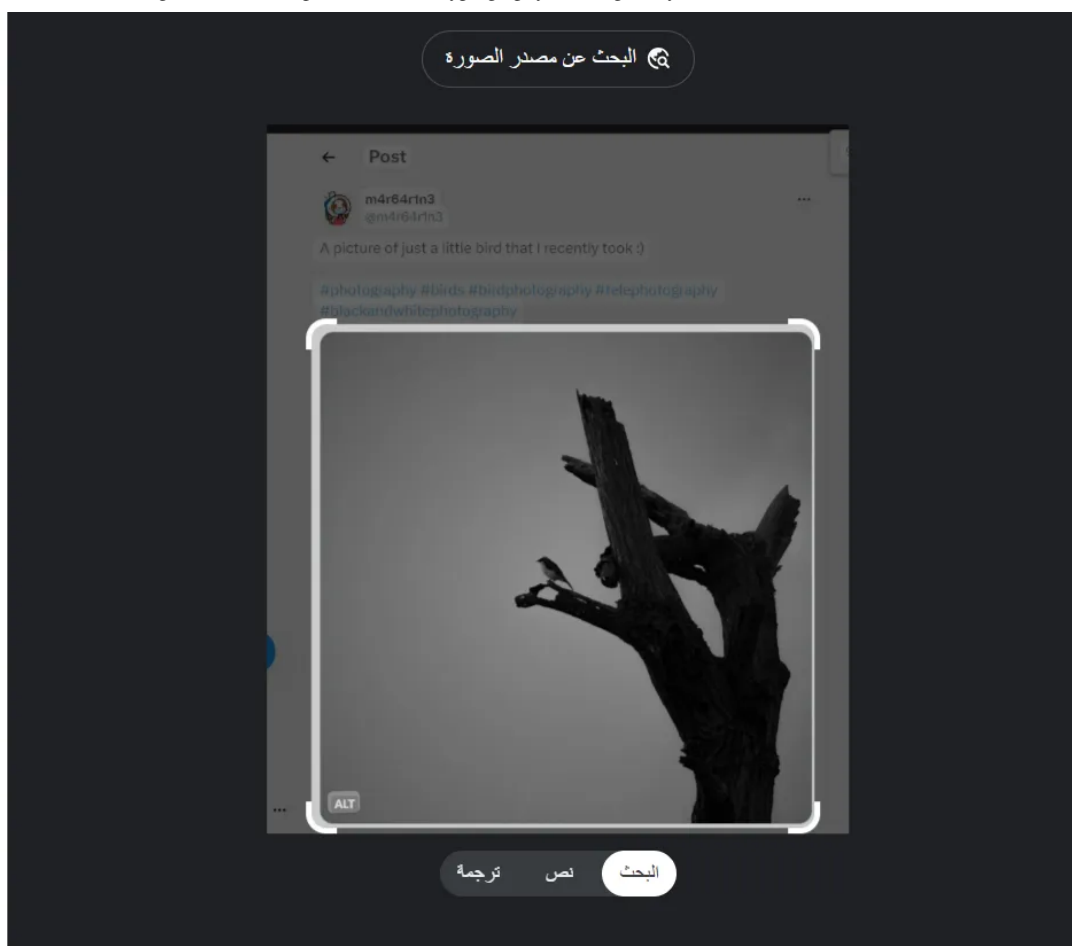
- Reddit



Flickr

tree 3 | during a small  
vacation i met this...

ما الجوانب التي يمكن تحسينها؟



after looking at his reddit account we found literally nothing so here I started to lose control and started to ignore that challenge but i said there's maybe anything else that related to this image and started again doing the image reverse but we found an Personal blog !!

which is : <https://v1ck1pictures.blogspot.com>

## Just a Little Bird



setembro 18, 2023

This one is just a picture of a little bird I took!



---

**Anônimo** 3 de outubro de 2023 às 04:46

I don't think it's a good idea to share your location online.

**RESPONDER**



**rinstaff** 17 de novembro de 2023 às 09:14

Este comentário foi removido pelo autor.

**RESPONDER**

Não é permitido fazer novos comentários.

if we noticed in the comments there's someone telling him that it's not a good idea to share his location ??

but there is no location in the post .... uhhh wayback machine Archive

after looking up on this website we found 1 result in 2 October 2023

and we opened it then ..... finally we got the flag

## Just a Little Bird



setembro 18, 2023

This one is just a picture of a little bird I took when I was in INTIGRITI{D3F1N173LY\_N07\_60TH4M\_C17Y}



---

##INTIGRITI{D3F1N173LY\_N07\_60TH4M\_C17Y}

=====

Challenge 2 : Cryptography (Really Secure Apparently) Difficulty : Easy

Clearly It's an Basic RSA but we need to get the d Value First



# Really Secure Apparently 100

Apparently this encryption is "really secure" and I don't need to worry about sharing the ciphertext, or even these values..

$n =$

6890610373394836368517448715648683799800611519  
9190407381405721687341258348472076869490584105  
3416938972235588548525570270575285633894975913  
7171300705444074805478262273980398314099291297  
4200710167185175745365603216144394681768570828  
2221883187089692065998793742064551244403369599  
965441075497085384181772038720949  $e =$   
9816100162324594645537145997227063704894709674  
0867123960987426843075734419854169415217693040  
6039439856145778547509284536848409297552542482  
0116124837535023862891741329120112503051450097  
7409961838501076015838508082749034318410808298  
0258581817116133728702894828900740725552653826  
00388541381732534018133370862587

Author: CryptoCat



ciphertext

Flag

Submit

I solved many RSA Challenges in [Cryptohack](#) so I remember that i saw this idea before and this depends on an attack called Wiener Attack by using this tool we can get the D value easy



## GitHub - zweisamkeit/RSHack: RSHack - Tool for RSA CTF's challenges

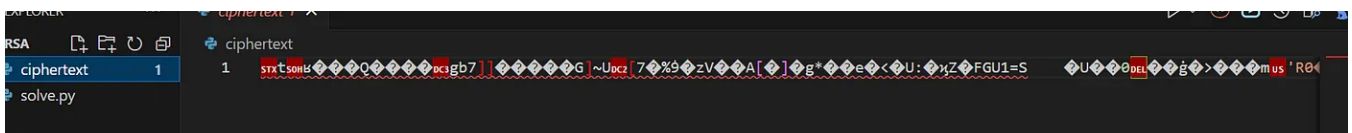
RSHack - Tool for RSA CTF's challenges. Contribute to zweisamkeit/RSHack development by creating an account on...

github.com

```
./RS./rshack.py -n $N Value -e $E Value
```

Then after getting the D value which is the private key

we need to get the C value and in the challenge there's a given file called plaintext but as it shown it's an Bytes and we need to convert it into Int



```
from Crypto.Util.number import bytes_to_long , long_to_bytes
c = open('ciphertext', 'rb').read()
c= bytes_to_long(c)

n = 689061037339483636851744871564868379980061151991904073814057216873412583484
e = 981610016232459464553714599722706370489470967408671239609874268430757344198
d = 653994415707479966122460879586443902420890730143890608823697555250579490695

x = pow(c,d,n)
print(long_to_bytes(x))
#FLag: INTIGRITI{0r_n07_50_53cur3_m4yb3}
```

```

1 from Crypto.Util.number import bytes_to_long, long_to_bytes
2 c = open('ciphertext', 'rb').read()
3 c = bytes_to_long(c)
4
5 n = 68906103733948363685174487156486837998006115199190407381405721687341258348472076869490584105341693897223558854852
6 e = 98161001623245946455371459972270637048947096740867123960987426843075734419854169415217693040603943985614577854750
7 d = 6539944157074799661224608795864439024208907301438906088236975525057949069503
8
9 x = pow(c,d,n)
10 print(long_to_bytes(x))

```

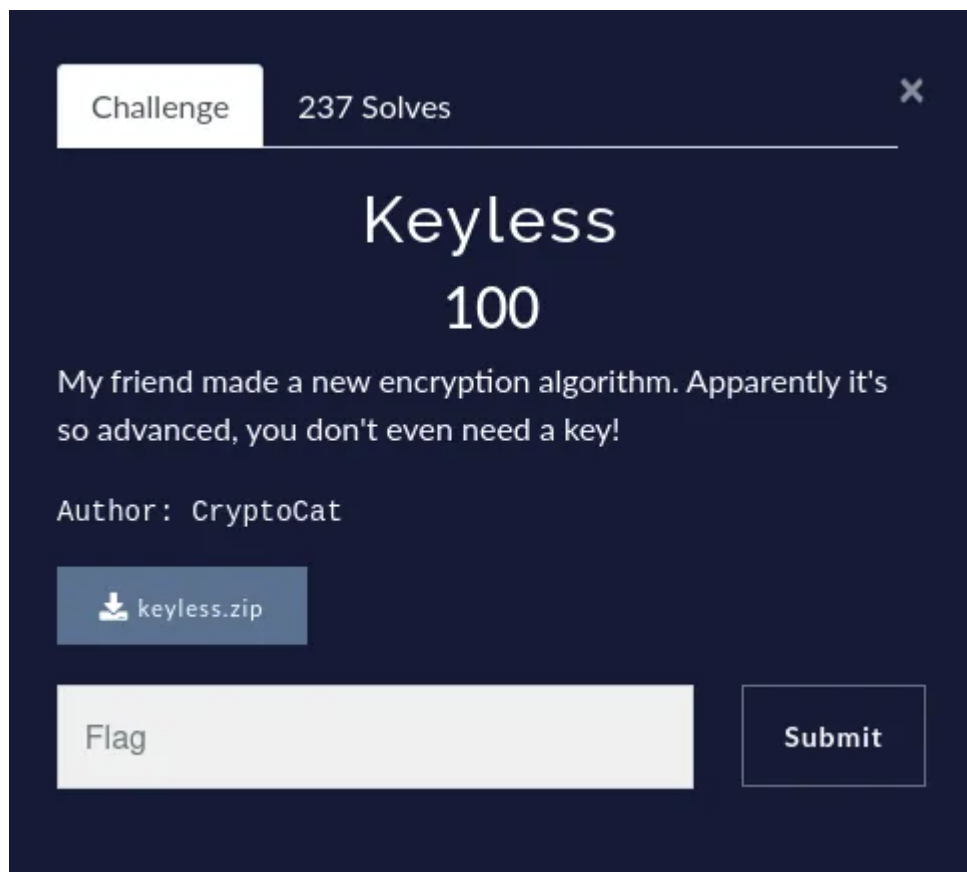
```

PS C:\Users\ahmed\Downloads\RSA> & C:/Users/ahmed/AppData/Local/Microsoft/WindowsApps/python3.11.exe c:/Users/ahmed/Downloads/RSA/solve.py
b'\x02\xa2\xf2\x97^\x10\xdb\xb3}\xf3\xf9ZI%\xc0*\x94\x0c=\x11S\x13\x04\xec\xbb\xb3\x7f\x97)\x1c\xf1\xb8\xe1\x0b\x97\xbbN\x7f\xca8\xb4\x89\xbc\xa9i\xb4\xc8V_\xd2\xf4k\xac\x7ft"\xaeqqH\xd6\xfe\x00Well done! Here is your flag: INTIGRITI{0r_n07_50_53cur3_m4yb3}'
PS C:\Users\ahmed\Downloads\RSA>

```

##INTIGRITI{0r\_n07\_50\_53cur3\_m4yb3}

### Challenge 3 : Keyless (Cryptography) Difficulty : Easy



after downloading the challenge file and unzipped it we got that python file

```
def encrypt(message):
    encrypted_message = ""
    for char in message:
        a = (ord(char) * 2) + 10
        b = (a ^ 42) + 5
        c = (b * 3) - 7
        encrypted_char = c ^ 23
        encrypted_message += chr(encrypted_char)
    return encrypted_message

flag = "INTIGRITI{REDACTED}"
encrypted_flag = encrypt(flag)

with open("flag.txt.enc", "w") as file:
    file.write(encrypted_flag)
```

---

*so here the python encrypts the flag and outputting it in the flag.txt.enc*

---

we can decrypt this file by reversing the process

```
def encrypt(message):
    encrypted_message = ""
    for char in message:
        a = (ord(char) * 2) + 10
        b = (a ^ 42) + 5
        c = (b * 3) - 7
        encrypted_char = c ^ 23
        encrypted_message += chr(encrypted_char)
    return encrypted_message

from string import printable

key = {}
for c in printable:
    key[encrypt(c)] = c

chipht = open('flag.txt.enc', 'rb').read().decode()
flag=""
for c in chipht:
    flag += key[c]

print(flag) # INTIGRITI{m4yb3_4_k3y_w0uld_b3_b3773r_4f73r_4ll}
```

so here we imported the printable library and then we created the dictionary “Key” and It associates each encrypted character with its corresponding original character from the printable ASCII characters. It uses the `encrypt` function defined earlier to generate the keys.

```
chiphrt = open('flag.txt.enc', 'rb').read().decode()
flag = ""
for c in chiphrt:
    flag += key[c]

print(flag) ##INTIGRITI{m4yb3_4_k3y_w0uld_b3_b3773r_4f73r_4ll}
```

Here, the encrypted message is read from the file ‘flag.txt.enc’, and each character is looked up in the `key` dictionary to find its corresponding original character. The resulting characters are concatenated to form the decrypted `flag`, which is then printed.

##INTIGRITI{m4yb3\_4\_k3y\_w0uld\_b3\_b3773r\_4f73r\_4ll}

kind regards, Hope you enjoyed this write up <’3

[Ctf Writeup](#)[Ctf](#)[Ctf Walkthrough](#)[Intigriti](#)[Cryptography](#)[Follow](#)

## Written by dnelsaka

228 Followers

CNSS | eJPT | 18 yrs | engineering student | bughunter