

# **b01lers CaptureTheFlag**



**Completed Challenge :**

**Granular Data (Misc.)**

**Zima Blue (Misc.)**

**Dream Stealing (Crypto)**

**Completed Challenge outside the time limit :**

**Echoes of Reality (Misc.)**

**Needle in a Haystack (Misc.)**

**Troll Hunt (Misc.)**

## Granular Data (Misc.)

We have to download the given photo to advance the challenge, so after we download the photo and open it we could see this



So after I see this the first thing I do is check the metadata through exiftool


Authors Position	Software Engineer	<a href="#">✎</a>
Creator	Garrett Scholes	<a href="#">✎</a>
Title	Cute Selfie	<a href="#">✎</a>
Creator City	flag{h4t3d_1n_th3_n4t10n_0MTBu}	<a href="#">✎</a>
Creator Country	United Kingdom	<a href="#">✎</a>
Image Size	400x400	
Megapixels	0.16	
Category	image	

So we got the flag now,

**flag{h4t3d\_1n\_th3\_n4t10n\_0MTBu}**

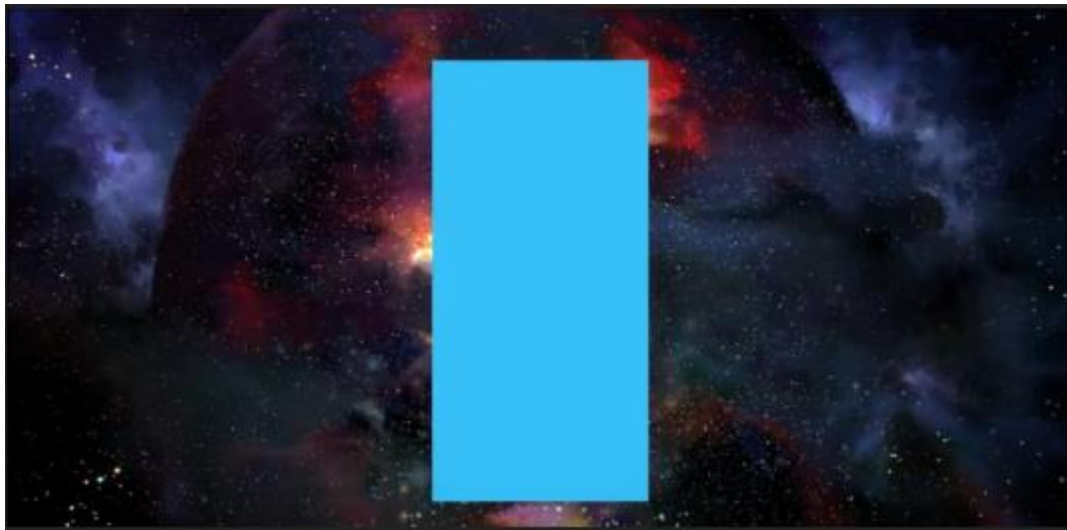
**Granular Data** 100 Points **SOLVED** ✓

A disgruntled ex-employee of Granular is the prime suspect behind recent killings in the nation. We've received his manifesto, which included this photo of him. Is there anything here that could help us figure out his location?

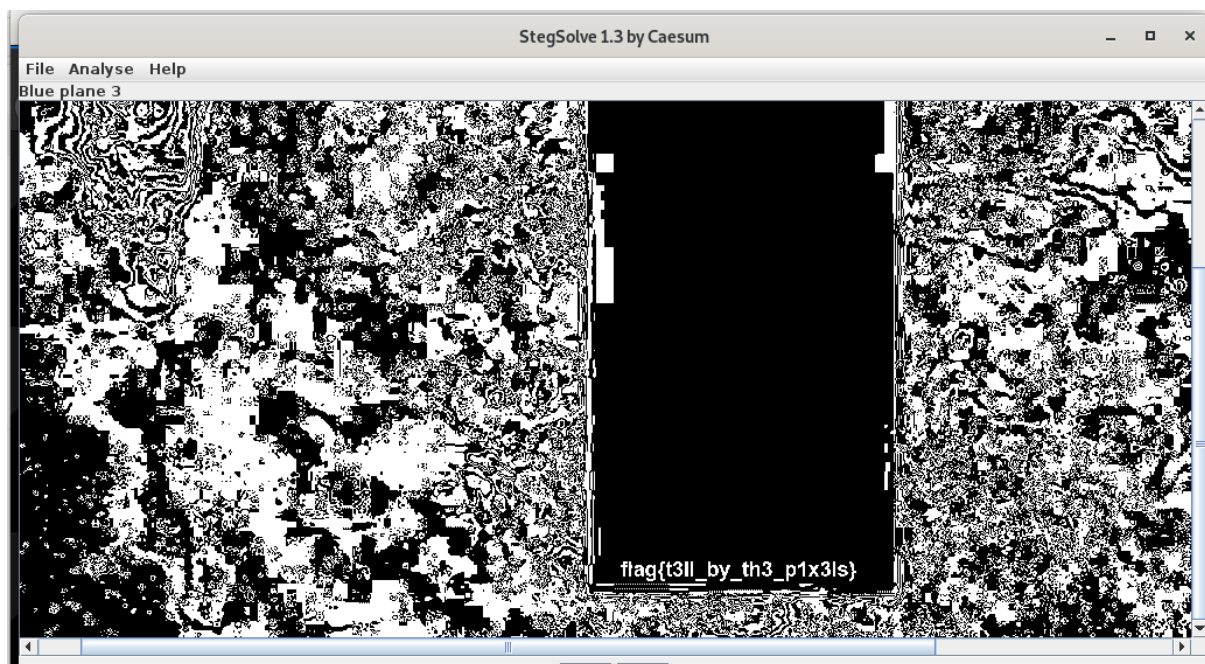
 **GarrettScholes.png** Size: 86.31 KB MD5: df317e3519426b22c71c81e87aed2412

## Zima Blue (Misc.)

After we downloaded the file, we could see something weird in the photos



We could see a galaxy but being covered with weird blue rectangle, I tried to use the stegsolver to see whats behind the blue rectangle



After few tries, and we got the glimpses of the flag when use filter blue plane 3.

**flag{t3ll\_by\_th3\_p1x3ls}**

**Zima Blue** 100 Points

**SOLVED** ✓

The mysterious artist Zima has unveiled his latest piece, and once again, it features his signature shade of blue. I honestly don't get it. Is he hiding a message in his art somehow?



**zima blue.png**

Size: 730.22 KB MD5: 2646021495d79dc860ea59316dcdcf046

## Dream Stealing (Misc.)

We could see from the downloaded file there is a cipher text,

```
root@opacite:~/Downloads# cat ciphertext-bb416c708f242b0c70d6f2c07d646d9f.txt
Modulus: 98570307780590287344989641660271563150943084591122129236101184963953890
61051528634218264323651412432567205330437435528194545599300145414546944964060210
28082870186198964941442218894119604188290670009444089109778572465492396175405881
05788633268030690222998939690024329717050066864773464183557939988832150357227
One factor of N: 96954776120978141436346859758954863650122112560672369881841514
82923787800058653259439240377630508988251817608592320391742708529901158658812320
088090921919
Public key: 65537
Ciphertext: 75665489286663825011389014693118717144564492910496517817351278852753
25905305273253566328550181428167815891398961591977649177794594562714723207311629
57584003656655262644382028251710128742665197522075225808333007892710160654647677
71248100896706714555420620455039240658817899104768781122292162714745754316687483
root@opacite:~/Downloads#
```

After I discuss with my friend who knows a lot of Cryptography, he said the content of ciphertext.txt is Classic RSA, and then we using the python to code the decryption of the cipher.

```
root@opacite:~/Documents# cat decrypt.py
from Crypto.Util.number import inverse, long_to_bytes

N = 9857030778059028734498964166027156315094308459112212923610118496395389061051
52863421826432365141243256720533043743552819454559930014541454694496406021028082
87018619896494144221889411960418829067000944408910977857246549239617540588105788
633268030690222998939690024329717050066864773464183557939988832150357227
e = 65537
p = 9695477612097814143634685975895486365012211256067236988184151482923787800058
653259439240377630508988251817608592320391742708529901158658812320088090921919
c = 7566548928666382501138901469311871714456449291049651781735127885275325905305
27325356632855018142816781589139896159197764917779459456271472320731162957584003
65665526264438202825171012874266519752207522580833300789271016065464767771248100
896706714555420620455039240658817899104768781122292162714745754316687483

q = N//p

totient = (p-1)*(q-1)

d = inverse(e,totient)

m = pow(c,d,N)

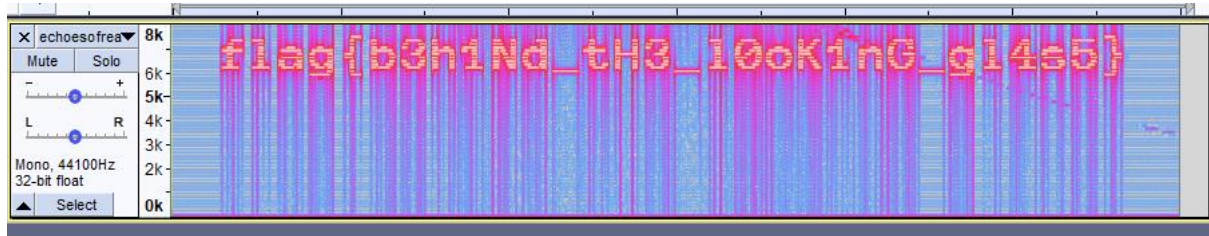
print(long_to_bytes(m))
```

Then we got the flag after we run the python.

**flag{4cce551ng\_th3\_subc0nsc10us}**

## Echoes of Reality (Misc.)

We only got a audio file, and when we play the audio we got some beeping sound, first I thought it was a beeping cipher but I don't get the result, so I thought again about sound and I think we have to analyze the sound because I thought it was about the frequency called spectrogram.



Using the audacity, I could get the **flag{b3h1Nd\_tH3\_l0ok1nG\_g14s5}**

## Needle In A Haystack (Misc.)

we need to download the file, and after that we have to extract the file then we got 400 text file with some random string each file as a hay. Its quite simple actually, we just need to run a command like this `"ls -l | grep -r "flag{"`.

```
root@opacite:~/Downloads/haystack# ls -l NeedleInAHayStack/ | grep -r "flag{"
NeedleInAHayStack/haystack269.txt:F0lgQaT1DgTzK3B0+xkuAIRHKflag{y0u_f0unD_Th3_n3
3d1e!}
root@opacite:~/Downloads/haystack#
```

Then we got the flag, **flag{y0u\_f0unD\_Th3\_n33d1e!}**

## Troll Hunt (Misc.)

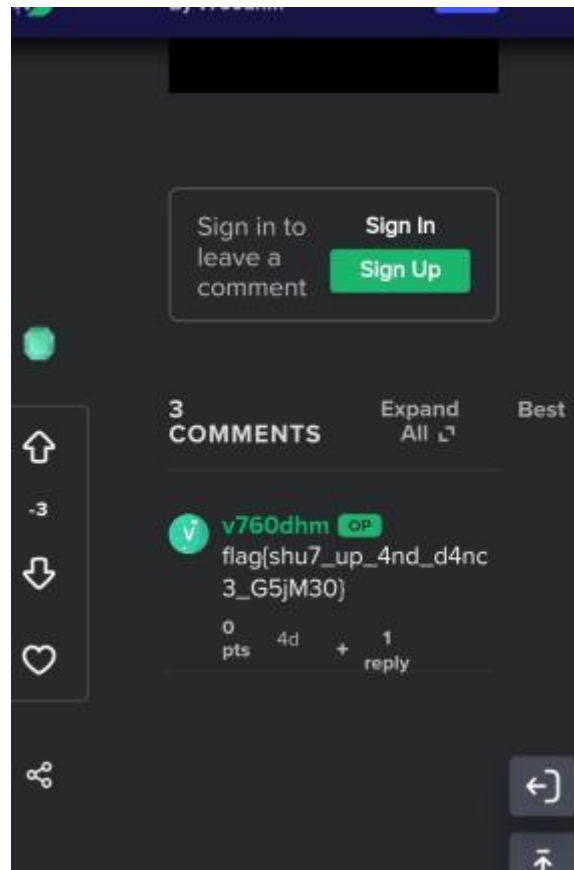
From the description of the challenge, we know there is a popular hashtag **#shrive** and the first social media I went to it **Twitter**, because the hashtag is popular on Twitter.



And we got the Twitter account, I know it because of the **date of tweets** almost as the starting time of CTF. After scrolling through his tweets, I got the link to imgur



Then after opening the link, I got the profile of **V760DHM** on [imgur.com](https://imgur.com) then after scrolling through that account I got the flag as shown below.



flag{shu7\_up\_4nd\_d4nc3\_G5jM30}