

**Author : Jayesh Jaiswal; Atharva Gawas.**

**Title : Unfolded**

**Git-Hub Links :**

<https://github.com/Jayesh-2003>

<https://github.com/ATHARVA-GAWAS>

**Category : Cryptography**

**Description : My Friend Giovan Battista Bellaso was original creator but people didn't acknowledge him.**

**Flag : VishwaCTF{0r1g4m1\_1s\_4n\_rt\_856462584532}**

1. Open the file Step1.json
2. In the description, we are given "My Friend Giovan Battista Bellaso was original creator but people didn't acknowledge him". This implies it is vigenere cipher.
3. In the Step1.json file, we are provided with ciphered text

```
1  {
2      "Dmwktih": "xpdnsrw0690",
3      "Beaera": "Vrxgovg Gmznfgismix, Qtb Qhympxjextb,Jtyc sbxuki",
4      "Nxmvgbdsh": "4ih sdt",
5      "Mwmibzcoi": "Wwiawx Ksmcfz Gkvhyby",
6      "Key": "justgiveupanddie"
7 }
```

- 4.
5. Decode the text using vigenere cipher tool, also we are provided with the key.

**Vigenere Tool**

```
"Dmwktihi": "xpdnsrw0690",
"Beaera": "Vrxgovg Gmznfgismix, Qtb Qhympxjextb, Jtyc sbxuki",
"Nxmgbdsh": "aih sdlt",
"Msmlbzcoi": "Wwiawx Ksmcfz Gkvhyby",
```

Copy Paste Text Options...

justgiveupanddie Standard Mode English

Decode Encode Auto Solve (without key) Instructions

**Auto Solve Options**

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	10	100	10	Automatic

**Results**

Decoded message.

```
"Username": "dadapool0690",
"Skills": "Android Development, Web Development, Open source",
"Education": "4th fail",
"Institute": "Chintu Coding Academy",
```

Copy Text Options...

- 6.
7. Upon decoding, we get the profile of a person, it appears to be like a github repository.
8. So now, search the profile on github

dadapool0690 Create FoldMe 4f61524 3 days ago 1 commit

FoldMe Create FoldMe 3 days ago

- 9.
10. We get a repository named "fold me".
11. Check the repository

dadapool0690 Create FoldMe Latest commit 4f61524 3 days ago History

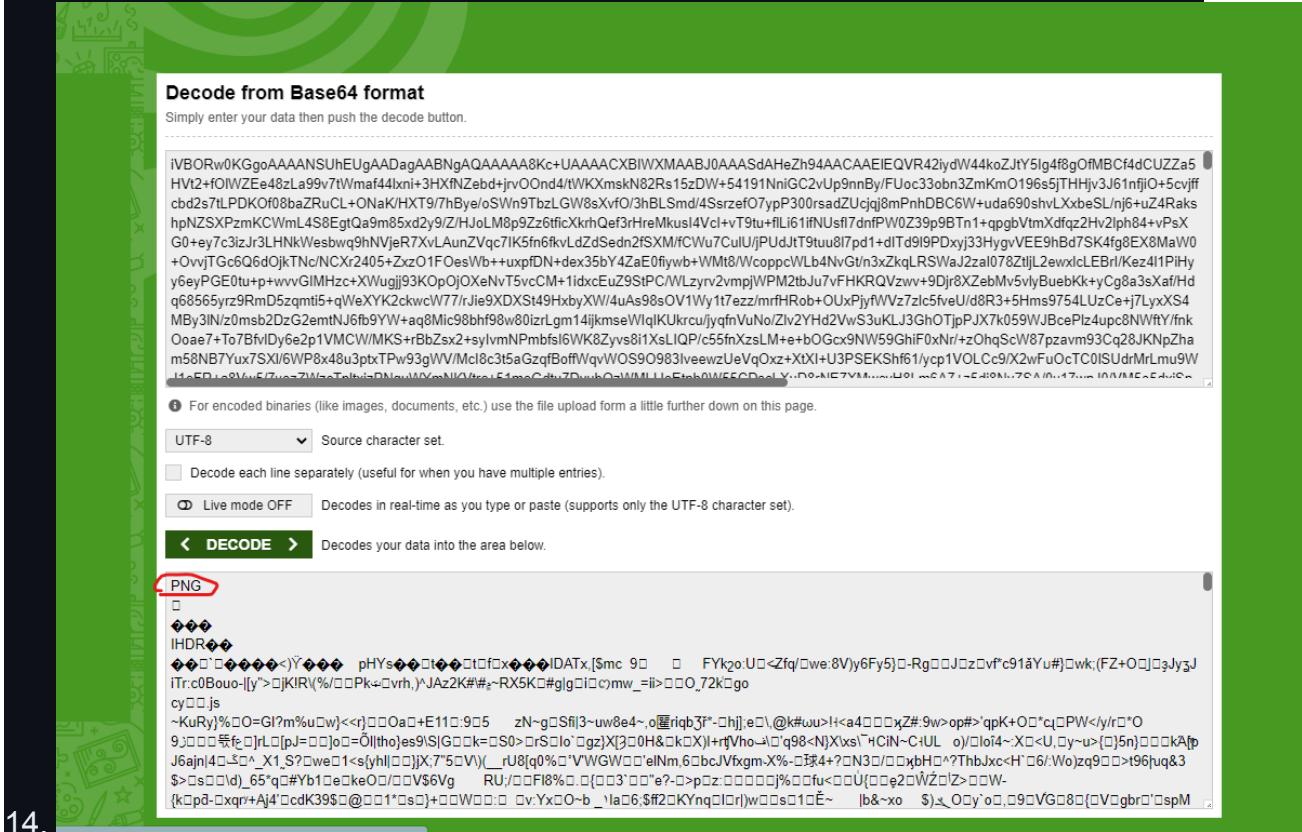
1 contributor

1 lines (1 sloc) | 1.57 MB

```
iVBORw0KGgoAAAANSUhEUgAAABNgQAAAAA8Kc+UAAAACXBIVXMAABJ0AAA5dAHeZh94AACAE1EQR42iydW44koZjtY5ig4f8gOfMBCf4dCUZZa5Hvt2+fO1WZEe48zLa99v7tWmaf441xn1+3HXfNZe...+jrvOOn4/tWIKx...
```

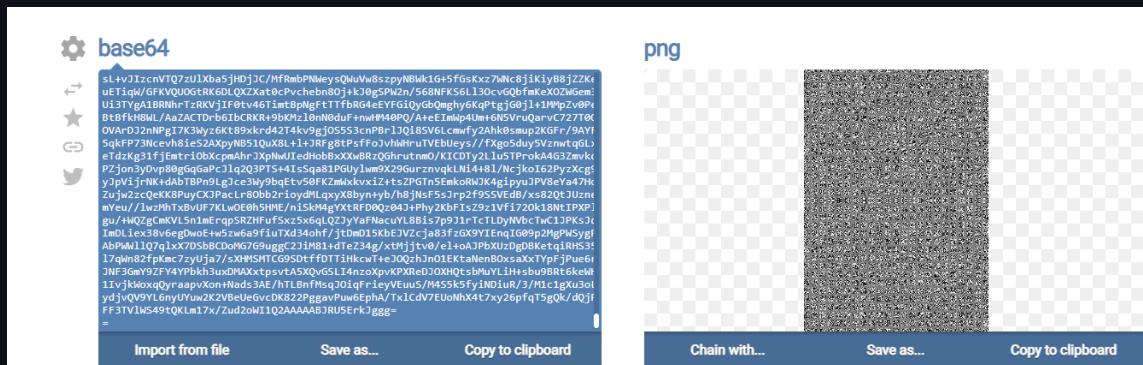
Raw Blame

- 12.
13. We get a base64 like code, we need to decode it.



14.

15. Upon decoding, it appears to be a png file, so we need to decode the base64 code to png file directly using an online tool



16.

17. Now, download the resulting image and analyze it.

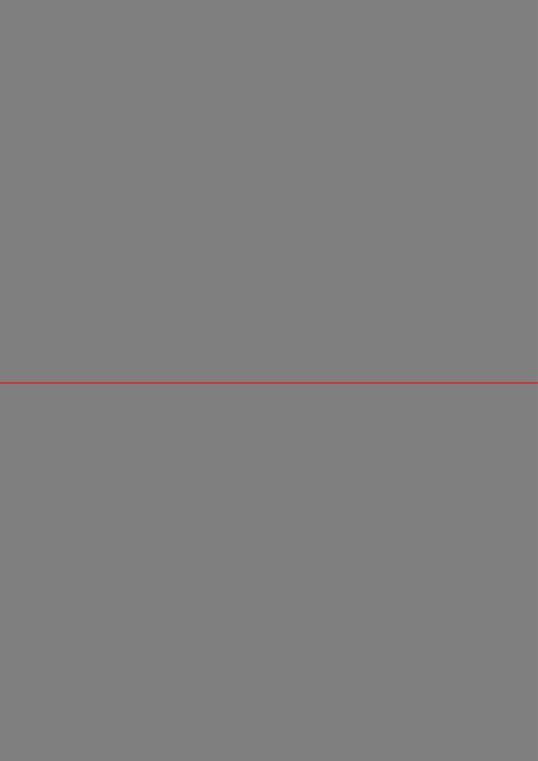


19. We are given a hint to fold the image as "fold me", just like a paper.

20. We split the image into half horizontally.

Allowed Filetypes: JPG, JPEG, GIF, PNG, BMP

Preview:



**Options**

**How to split**

How to split: **Horizontally**

Split horizontally by: **Number of blocks**

Quantity of Horizontal Blocks: **2**

**Process and Download**

21.

22. The images are

23.

24.

25. Now flip the lower image vertically.

26. The flipped image is

27.

28. Now write a code based on principle of solving visual cryptography in python

```
from PIL import Image

# Load the first share
share1 = Image.open("img1.png").convert('1')

# Load the second share
share2 = Image.open("img2flip.png").convert('1')

# Get the size of the shares
width, height = share1.size

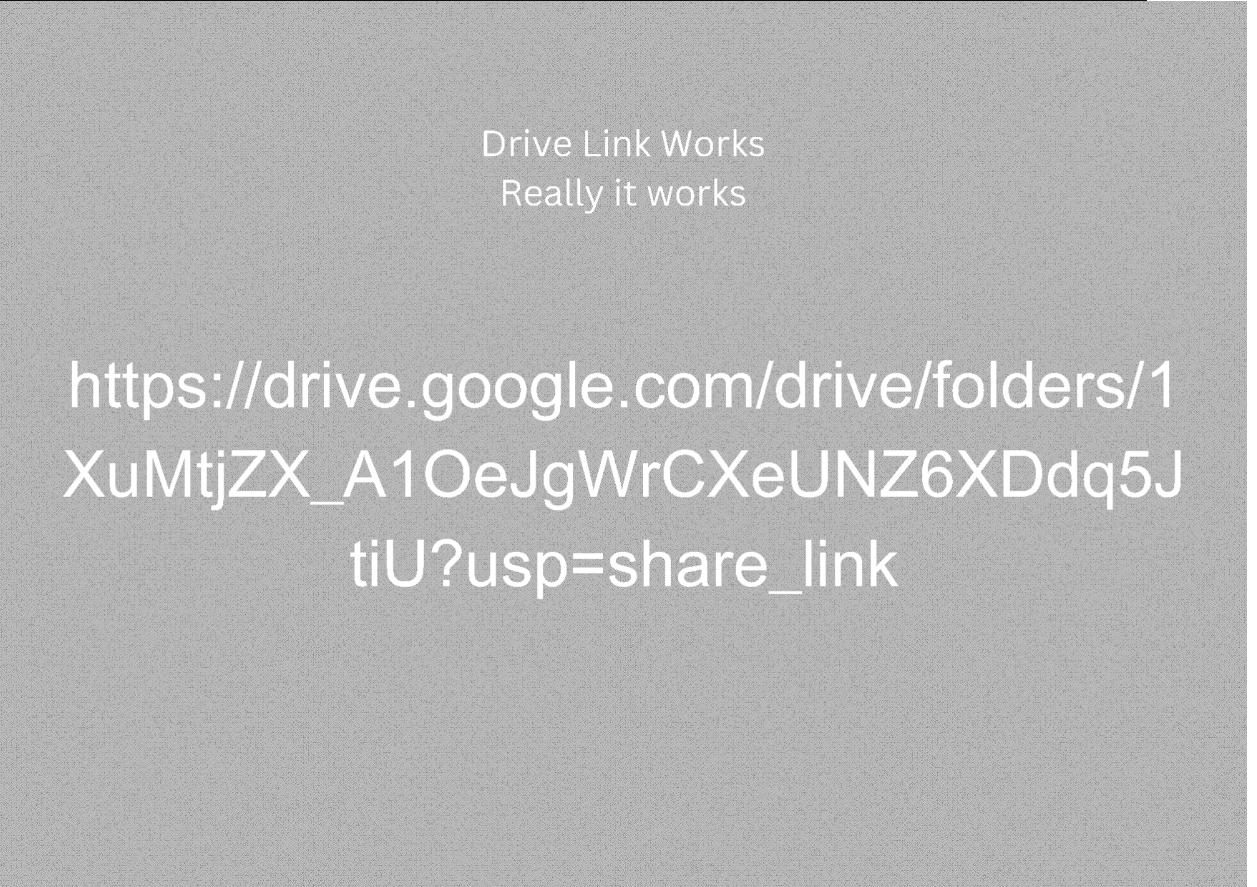
# Create a new image for the result
result = Image.new("1", (width, height))

# Loop through each pixel in the shares and combine them
for x in range(width):
    for y in range(height):
        pixel1 = share1.getpixel((x, y))
        pixel2 = share2.getpixel((x, y))

        # If both pixels are black, set the result pixel to black
        if pixel1 == 0 and pixel2 == 0:
            result.putpixel((x, y), 0)
        else:
            result.putpixel((x, y), 1)
```

```
if pixel1 == 0 and pixel2 == 0:  
    result.putpixel((x, y), 0)  
# Otherwise, set the result pixel to white  
else:  
    result.putpixel((x, y), 255)  
  
# Save the resulting image  
result.save("result.png")
```

29. Now the resulting image is,



Drive Link Works  
Really it works

[https://drive.google.com/drive/folders/1XuMtjZX\\_A1OeJgWrCXeUNZ6XDdq5JtiU?usp=share\\_link](https://drive.google.com/drive/folders/1XuMtjZX_A1OeJgWrCXeUNZ6XDdq5JtiU?usp=share_link)

30.

31. Visit the given link but before that, remove unnecessary spaces.

32. It directs us to a drive link, it has a file flag.txt

33. So the flag is VishwaCTF{0r1g4m1\_1s\_4n\_4rt\_856462584532}