Writeup For XOR

Name : XOR

Domain : Steganography

Difficulty : Medium

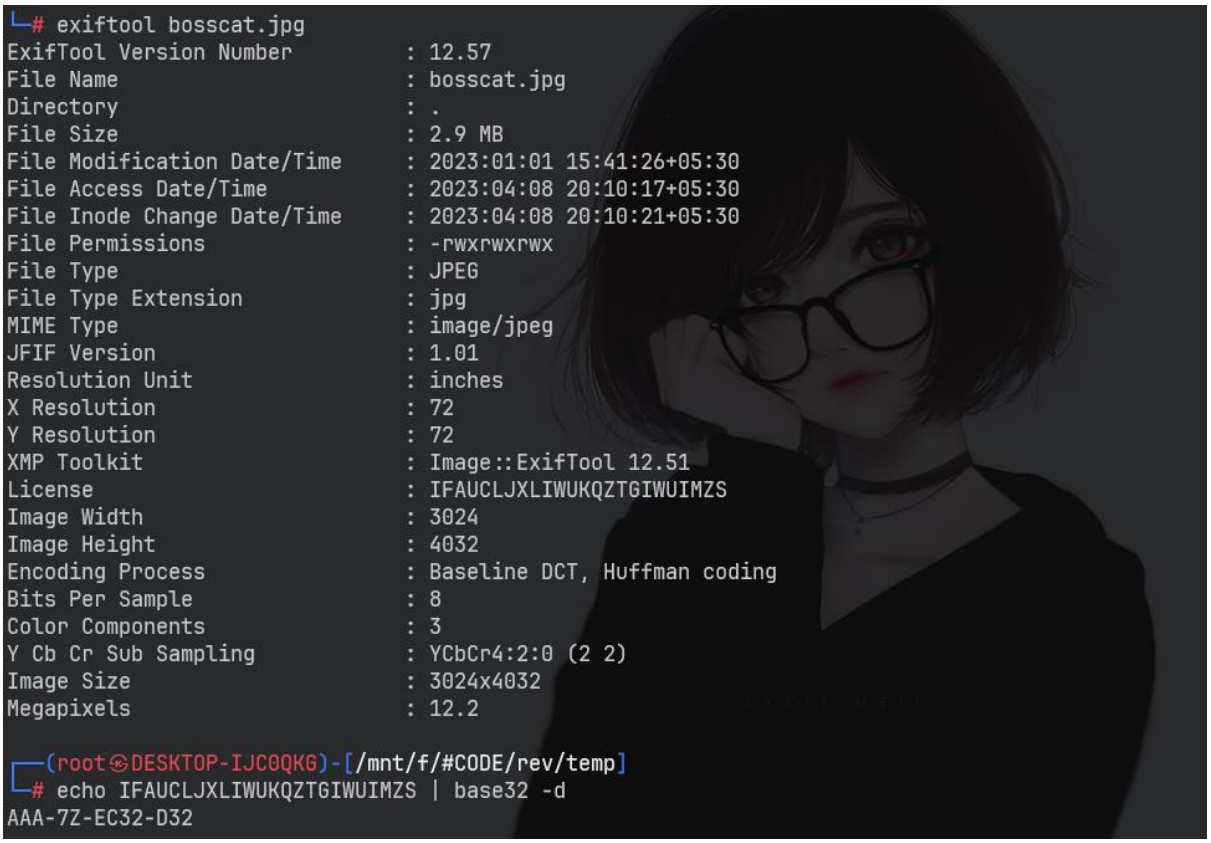
Description : My friend sent me a clip and I found it to be very interesting. I wanted to watch the full video but before I could rewatch the clip, he deleted it!! All I have right now is this image he sent me afterwards. Can you help me find the video link?

Points : 296

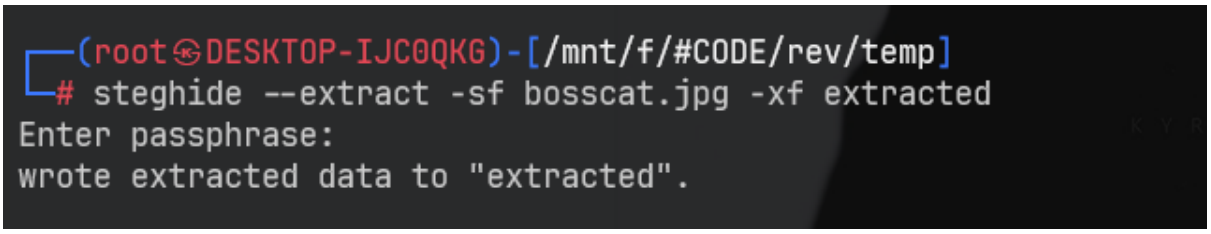
Author : Yogesh Rathod

File given : BossCat.jpg

We have been given a file BossCat.jpg use exiftool on the image and look at the metadata. The license field in metadata is encoded in base32 decode it. We get the string AAA-7Z-EC32-D32.



Now use this string we got as password to extract hidden data from BossCat.jpg using steghide.

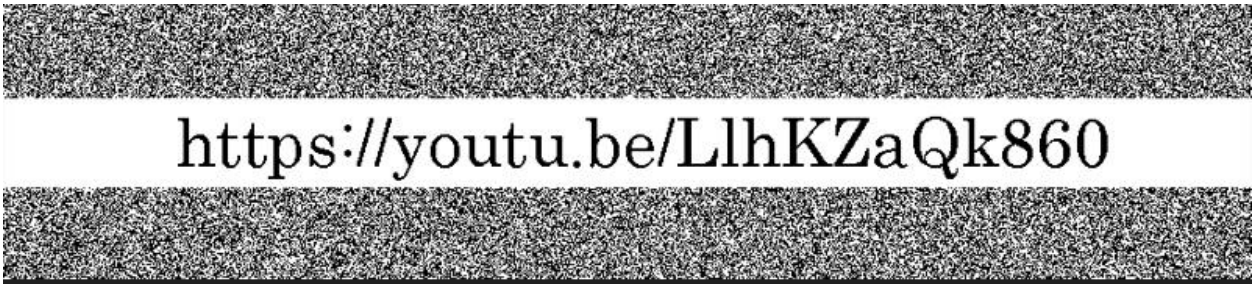


We get a zip file after using steghide, we can simply unzip it. After unzipping we get two files n1.png, n2.png.

Now to get the flag we need to xor the rgb values pixel by pixel of n1.png with n2.png and use that value as the pixel value of a new image. We can use python to do that. Here is a simple script to do that.

```
#!/usr/bin/python3

from PIL import Image

image1 = Image.open('n1.png')

image2 = Image.open('n2.png')

print(image1.mode, image2.mode)

size = width, height = image1.size

new = Image.new('RGBA', size)

img1 = image1.load()

img2 = image2.load()

data = new.load()

for x in range(width):

    for y in range(height):

        one = img1[x,y]

        two = img2[x,y]

        new_color = (one[0] ^ two[0],

                     one[1] ^ two[1],

                     one[2] ^ two[2],

                     one[3])

        data[x,y] = new_color

new.save('flag.png')
```

Above script creates a new file flag.png in the current working directory. This file contains the flag.



Flag is: `VishwaCTF{https://youtu.be/LlhKZaQk860}`