

## 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.

```
# exiftool bosscat.jpg
ExifTool Version Number      : 12.57
File Name                    : bosscat.jpg
Directory                   : .
File Size                    : 2.9 MB
File Modification Date/Time  : 2023:01:01 15:41:26+05:30
File Access Date/Time       : 2023:04:08 20:10:17+05:30
File Inode Change Date/Time  : 2023:04:08 20:10:21+05:30
File Permissions             : -rwxrwxrwx
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit              : inches
X Resolution                 : 72
Y Resolution                 : 72
XMP Toolkit                  : Image::ExifTool 12.51
License                     : IFAUCLJXLIWUKQZTGIWUIMZS
Image Width                 : 3024
Image Height                : 4032
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                  : 3024x4032
Megapixels                  : 12.2
```

```
(root@DESKTOP-IJCQK6)-[/mnt/f/#CODE/rev/temp]
# echo IFAUCLJXLIWUKQZTGIWUIMZS | base32 -d
AAA-7Z-EC32-D32
```

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

```
(root@DESKTOP-IJCQK6)-[/mnt/f/#CODE/rev/temp]
# steghide --extract -sf bosscat.jpg -xf extracted
Enter passphrase:
wrote extracted data to "extracted".
```

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)

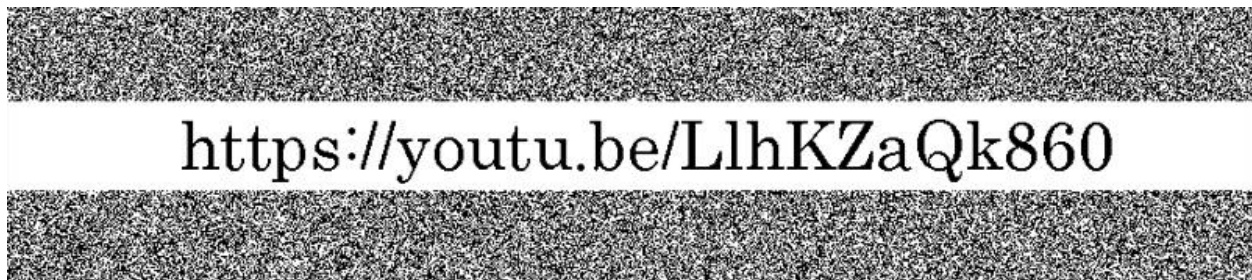
img1 = image1.load()
img2 = image2.load()

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}