Category:

Steganography

Name:

Steg2.png

Message:

You are provided with an image named “steg2.png”. The flag for this challenge is written in this image. However, the image dimensions were altered by mistake! Your mission is to capture the flag by diving into the binary depths and restoring “steg2.png”!

Hint:

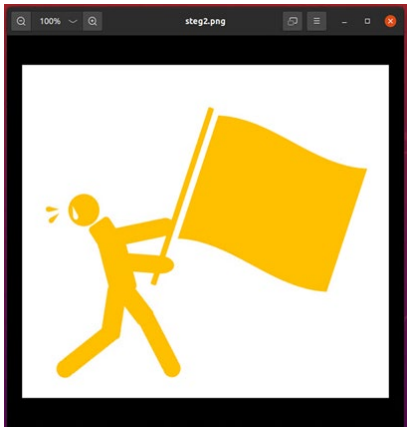
- Tried poking around with LSB decoding yet? It might reveal more than you expect! Psst… the original height of “steg2.png” could be your clue!
- Ever wondered what makes a PNG tick? Dive into the PNG file structure and pinpoint which bytes hold the height information. Once you tweak that, you're one step closer.
- CRC errors raining on your parade? Recalculate the CRC and give “steg2.png” a second life. pngcheck might just be a good company!

Objective:

Your task is to restore the image dimension by editing the binary file of “steg2.png” to read the flag. This requires understandings of LSB manipulation and PNG image structure.

Instructions:

1. Start by loading “steg2.png” in your preferred environment. You will see the yellow image of a person carrying a flag.

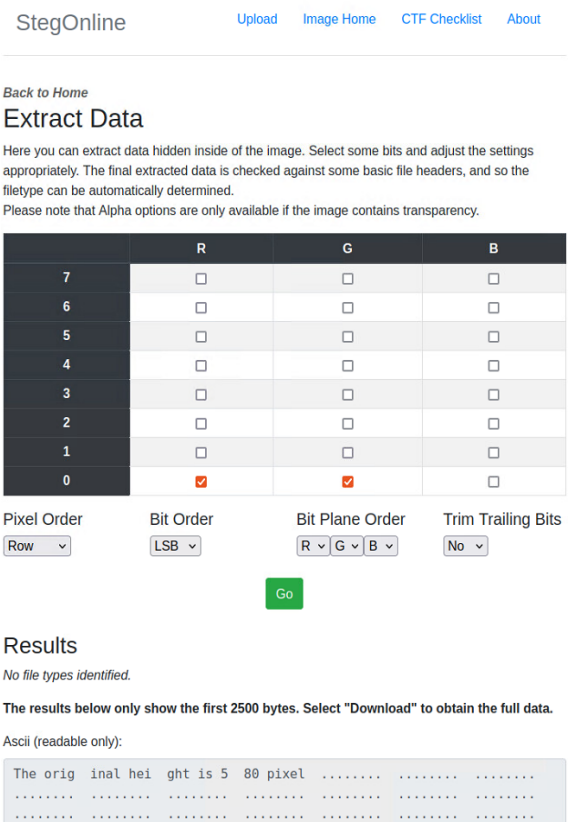


2. Look at the meta data of “steg2.png” with tools such as ExifTool, Strings, pngcheck etc. to see the basic file information. For example, using ExifTool, you will find the image size as 636 (width) and 555 (height) pixels.

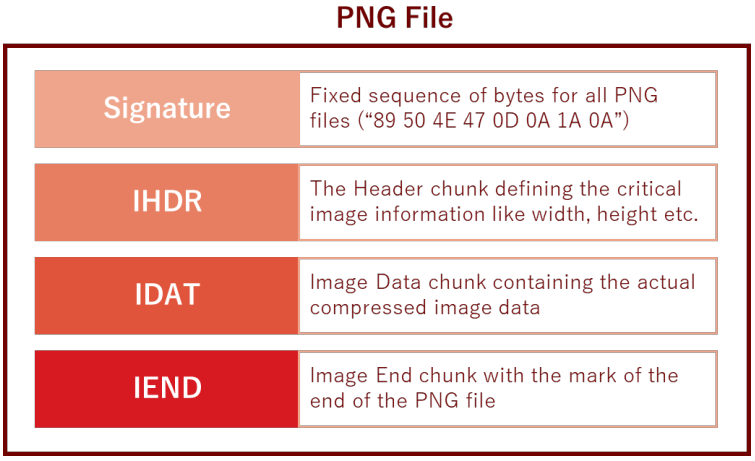
```
$ exiftool steg2.png
```

```
Title                           : steg2.png
Copyright                       : AJCCBC_CTF2024
Image Size                      : 636x555
Megapixels                      : 0.353
```

3. Like the previous challenge with "steg1.png," the image hides a string using the LSB technique. In this case, the least significant (0) bits are modified in the Red and Green channels, as hinted by the yellow color (the combination of Red and Green light) the original image.
4. In StegOnline, one of the most popular tools, upload the image and then choose Extract Files/Data. In the window, select the least significant bit (0 bit) in Red and Green channels. The result should show the string “**The original height is 580 pixel**”. This suggests that the current height 555 pixel should be restored to 580 pixels to capture the flag.

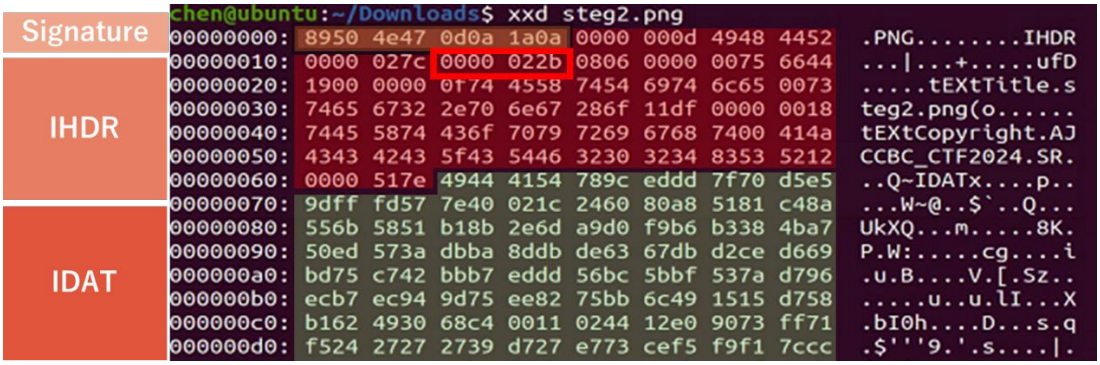


5. Although there are several ways to modify the image size, let’s edit the binary data in this scenario as the challenge message requests. Speaking about the PNG file structure, it is made up of several chunks to form an image as shown below.

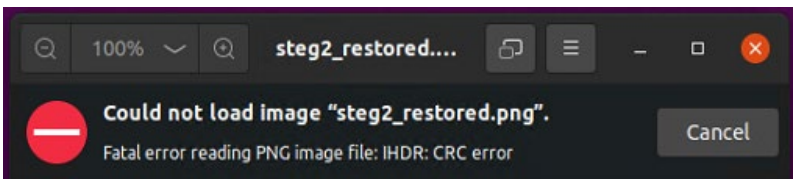


The IHDR chunk contains important file information such as width, height, bit depth etc. In another word, you can modify the image height by properly editing this chunk.

6. Open preferred Hex editor and load “steg2.png”. Following to PNG file signature (“89 50 4E 47 0D 0A 1A 0A”), the IHDR chunk starts. IHRD chunk starts from length (13 bytes represented as “00 00 00 0D”) and then the chunk type code for IHDR (“49 48 44 52”). The next 4 bytes (“00 00 02 7C”) represent the image width (636 pixel), while another 4 bytes (“00 00 02 2B”) represent the image height (555 pixel). Note that 636 and 555 are interpreted to 27C and 22B in hex respectively. To resize the height from 555 to 580 pixel, modify the 4 bytes from “00 00 02 2B” to “00 00 02 44” as 580 is interpreted to 244 in hex. Use any Hex/Binary editor to modify the binary such as Ghex, HxD and so forth.



7. In some cases, the modified PNG file is recognized as corrupted. This error is detected by the checksum function CRC stored in IHDR chunk which detects the lack of data integrity. It is caused because the height related binary data in IHDR chunk was modified.

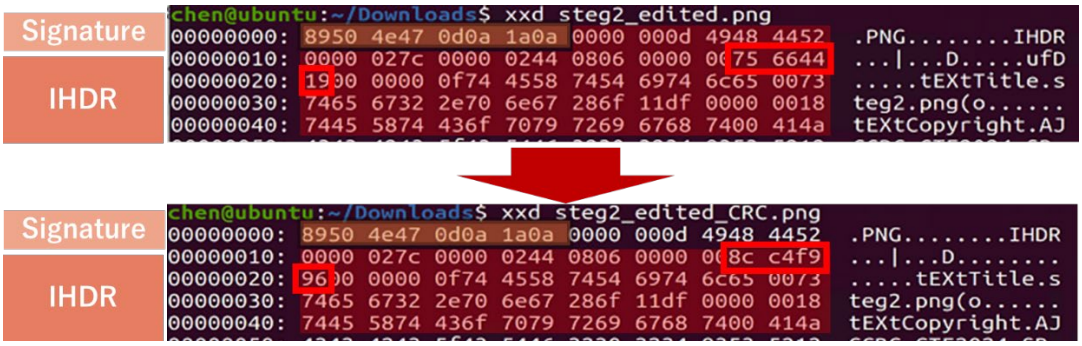


You need to recalculate the CRC value before opening the modified image. Using pngcheck, a

tool to verify the integrity of PNG files, you can see the current CRC value is “8cc4f996”. As the predefined CRC value is “75664419”, modify it into “8cc4f996” using Hex/Binary editor.

```
$ pngcheck <modified_steg2.png>
```

```
chen@ubuntu:~/Downloads$ pngcheck steg2_edited.png
steg2_edited.png  CRC error in chunk IHDR (computed 8cc4f996, expected 75664419)
ERROR: steg2_edited.png
```



8. Now you should be able to see the original image with flag written at the bottom.

Flag is:

CSG_FLAG{Broaden_your_horizons_to_find_the_FLAG!35}