Category:

Steganography

Name:

steg1.png

Message:

You are provided with an image named “steg1.png”. The flag for this challenge is embedded in this image in the form of “flag.txt”. However, a passphrase is required to extract “flag.txt”!

Hints:

- Tried your hand at LSB manipulation yet? It’s where the passphrase for flag.txt is hiding, waiting to be unlock with OpenStego!
- Using LSB, The image can hold the hidden information inside of the color/bit planes by slightly modifying the pixel value. Remember, each pixel’s got three partners in crime: Red, Green, and Blue.

Objective:

Your task is to retrieve the hidden passphrase from “steg1.png”, and then using this passphrase to extract “flag.txt” with OpenStego to capture the flag. This requires understandings of basic steganography tools and mechanism, especially LSB manipulation.

Instructions:

1. Start by loading “steg1.png” in your preferred environment. You will see the blue image of a person carrying a flag.

2. Look at the meta data of “steg1.png” with tools such as ExifTool, Strings etc. to see the basic file

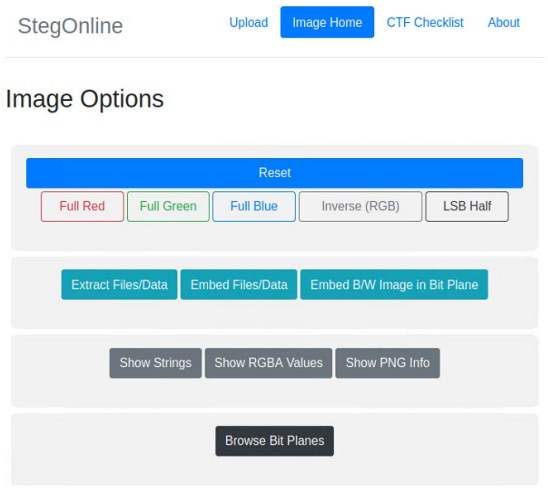
information. For example, using ExifTool, you will find the description saying, “this image contains a passphrase for OpenStego”.

```
$ exiftool steg1.png
```

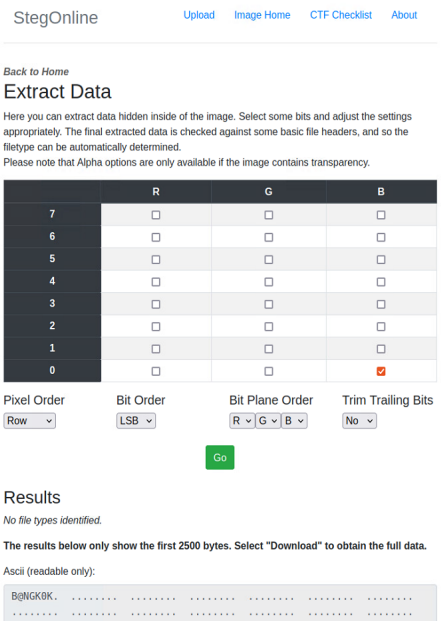
```
Title                           : steg1.png
Description                     : This image contains the passphrase for OpenStego.
Copyright                       : AJCCBC_CTF2024
Image Size                      : 548x592
```

This description suggests that you can use OpenStego to extract “flag.txt” from “steg1.png”, but you need a passphrase for it.

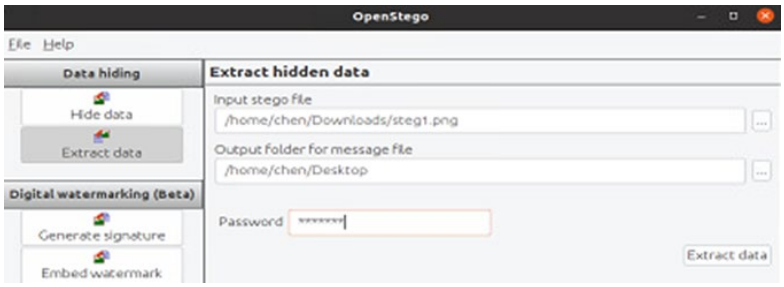
3. Let’s find out the passphrase first. The image can hold the hidden information like passphrase inside of the color/bit planes by slightly modifying the pixel value. This steganography technique is known as **Least Significant Bit** (LSB) and it leverages the unavailability of humans to recognize the subtle changes in image pixel. Each pixel in image is composed of three color components: Red, Green and Blue, each represented by 8 bits. In this case, as the color of the image indicates, the least significant bits in the Blue channel were modified to hold the binary data of the passphrase.
4. You can use any steganography tool to retrieve the data from the modified bits in the Blue channel. 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 Blue channel. It retrieves the binary data in each 0 bit in the Blue channel and then translate the extracted binary to string. The result should show the passphrase “B@NGK0K”.



5. Using the obtained passphrase, you should be able to extract the flag from “steg1.png” on OpenStego. Choose Extract Data and then select the appropriate paths.



If you correctly specify the file paths and the password, a file “flag.txt” is extracted, where you can find the final flag!

Flag is:

CSG_FLAG{A_picture_is_worth_@_thousand_words}

References:

- StegOnline (https://georgeom.net/StegOnline/upload)
- OpenStego (https://www.openstego.com/)