BUUCTF：喵喵喵

原创

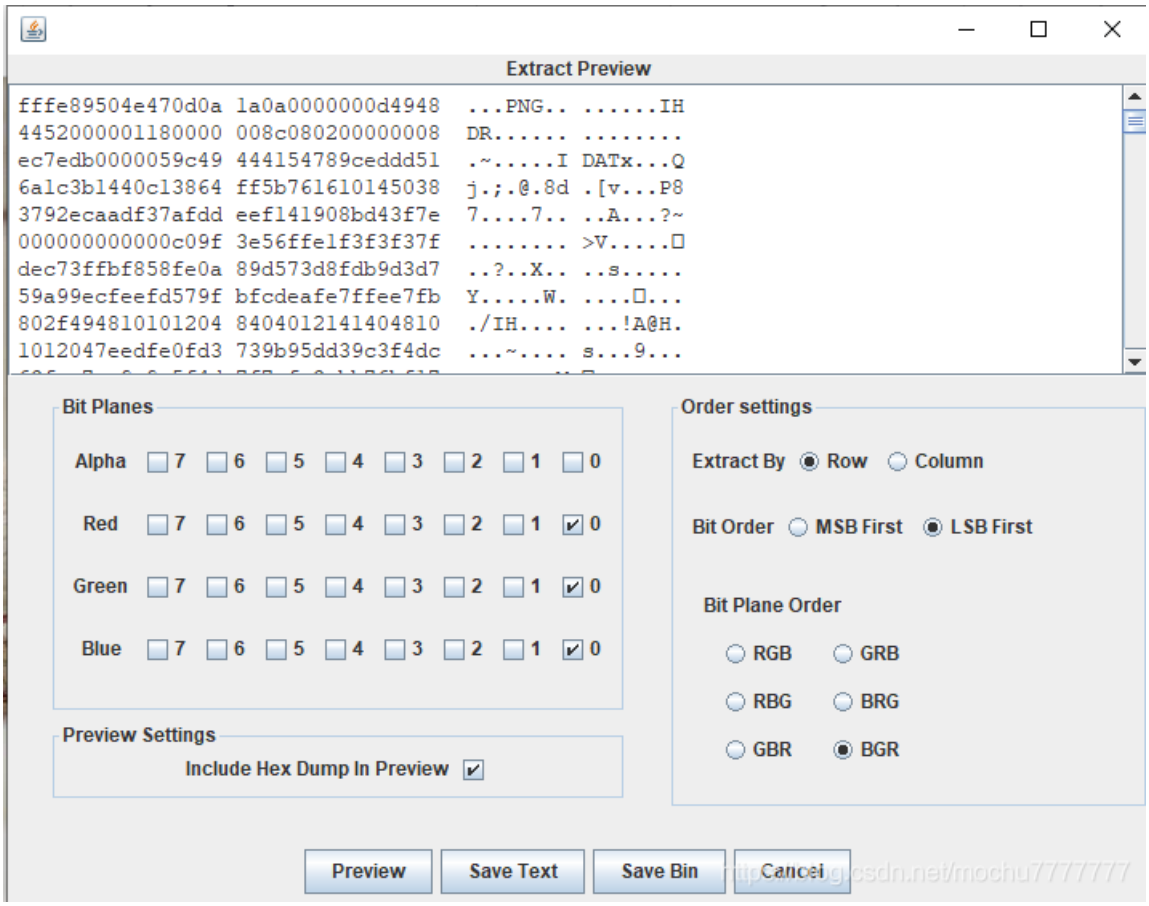
末 初 于 2020-10-29 20:57:03 发布 2200 收藏 4

分类专栏： CTF_MISC_Writeup

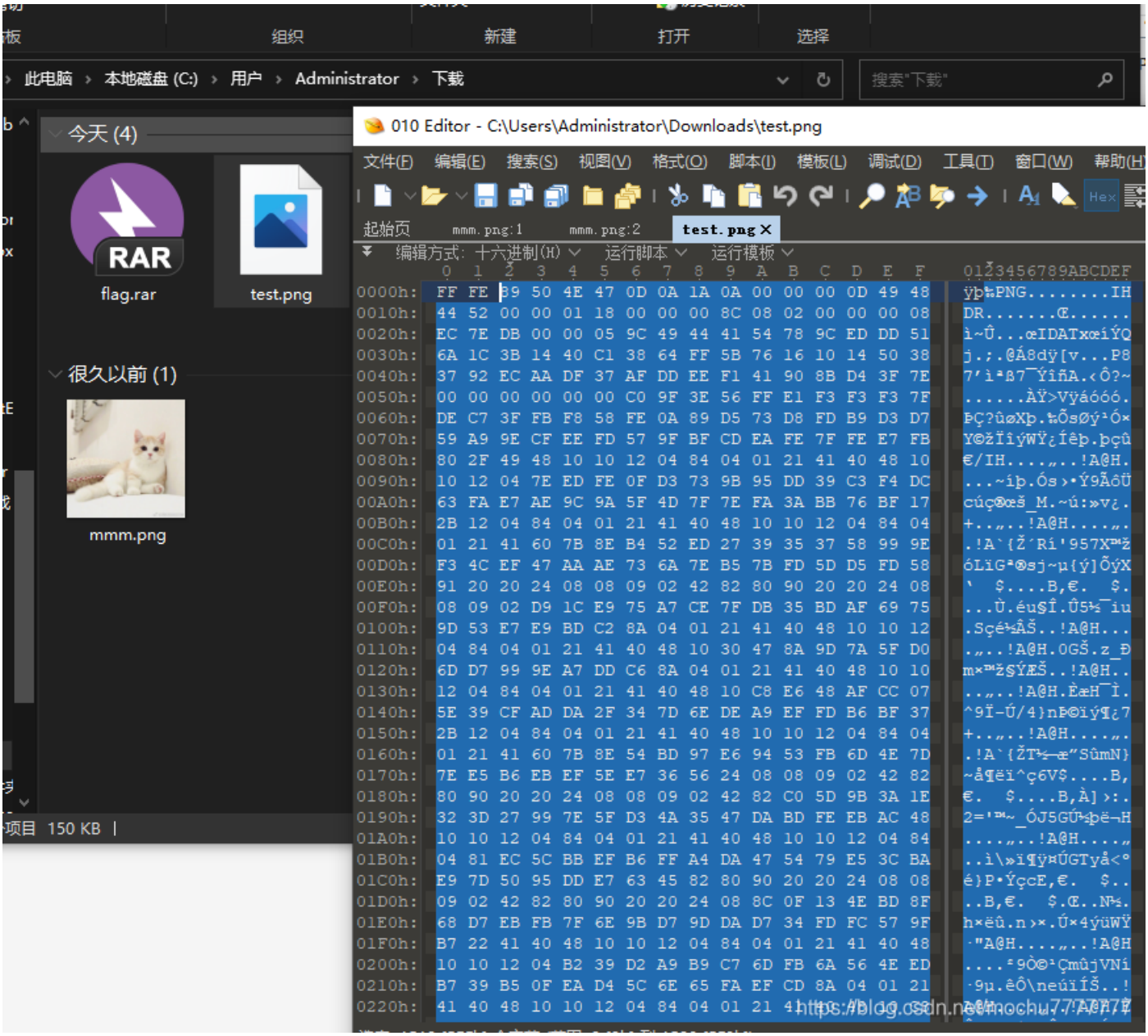
本文链接：https://blog.csdn.net/mochu7777777/article/details/109368451

> 题目地址：https://buuoj.cn/challenges#%E5%96%B5%E5%96%B5%E5%96%B5

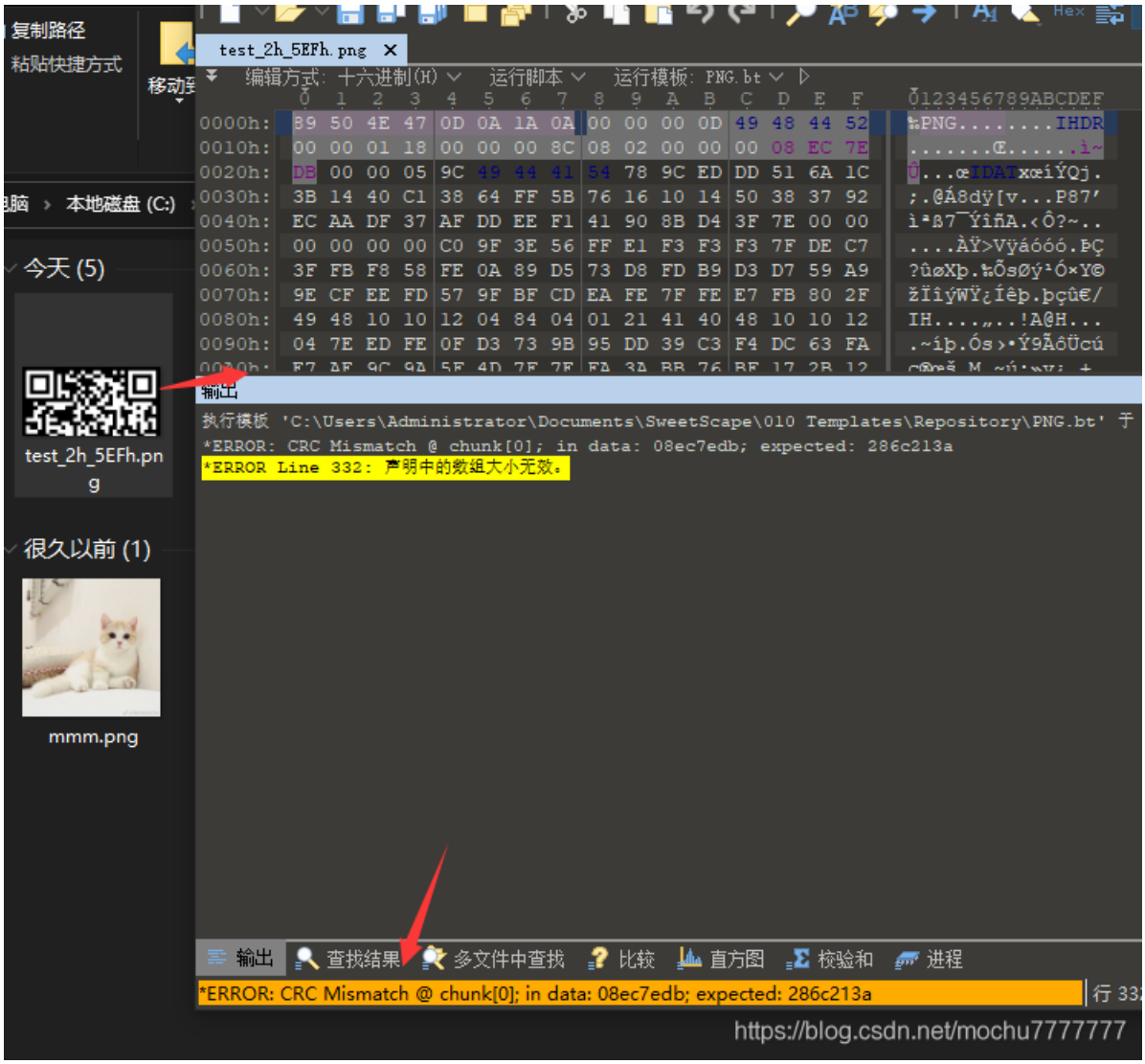
`stegslove` 打开，发现 `RGB` 的 `0通道` 存在异常， `LSB隐写` 发现 `png`

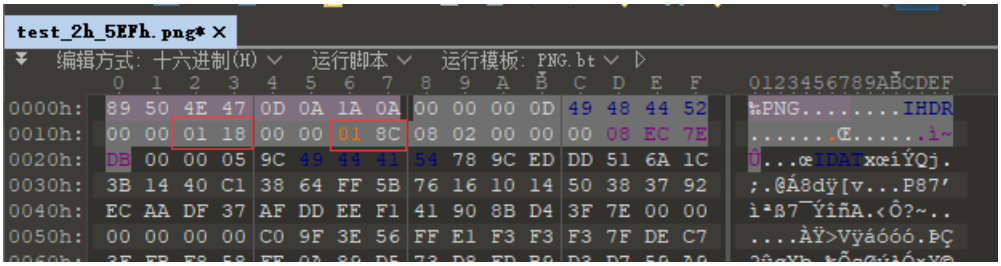


保存为`test.png`，无法正常显示的，因为文件头前面多了些东西导致无法识别为PNF，另存从`PNG`文件头开始到`IEND`结束的数据即可



保存得到半张二维码，用`010 Editor`打开出现CRC不匹配，明显修改了宽高



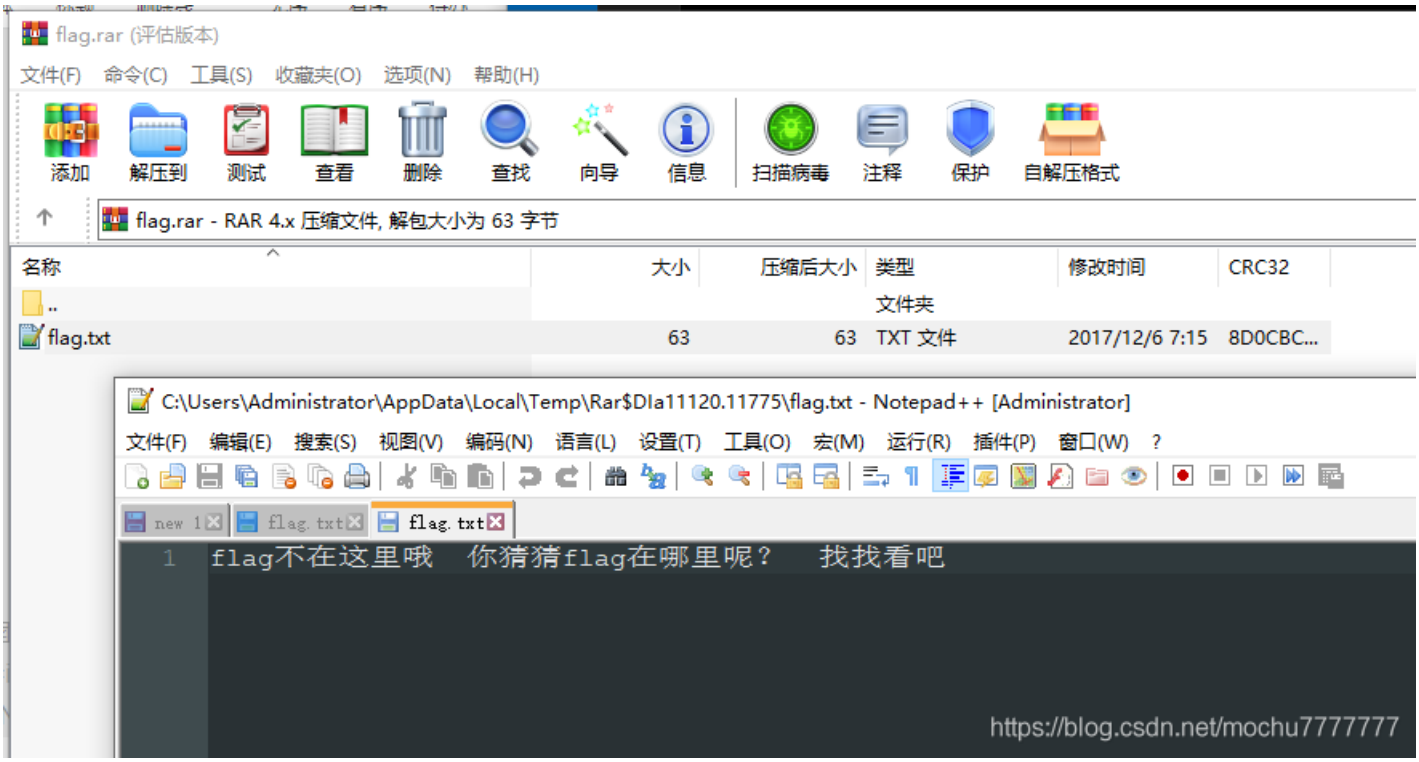


得到完整的二维码，扫描得到信息

```
https://pan.baidu.com/s/1pLT2J4f
```

下载`flag.rar`

`flag.txt`打开没有发现flag



这里猜测有`NTFS`文件流隐写，将`flag.txt`解压到一个新建的文件夹内，利用`NtfsStreamsEditor`

果然藏了东西，导出`flag.pyc`

利用`Pyc反编译`在线网站进行反编译：https://tool.lu/pyc/

得到如下代码

```python
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import base64

def encode():
    flag = '**********'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i ^ ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))

    return ciphertext[::-1]

ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '97',
    '88',
    '80',
    '82',
    '137',
    '90',
    '109',
    '99',
    '112']
```

写个脚本把`ciphertext`解出来

```python
#Author: mochu7
def decode(arg1):
 ciphertext = arg1[::-1]
 flag = ''
 for i in range(len(ciphertext)):
  if i % 2 == 0:
   s = int(ciphertext[i]) - 10
  else:
   s = int(ciphertext[i]) + 10
  s = s ^ i
  flag += chr(s)
 print(flag)

if __name__ == '__main__':
 ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '97',
    '88',
    '80',
    '82',
    '137',
    '90',
    '109',
    '99',
    '112']
 decode(ciphertext)
```

```
PS C:\Users\Administrator\Downloads\新建文件夹> python .\decode.py
flag{Y@e_Cl3veR_C1Ever!}
```