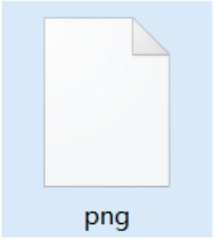
bugkuCTF—杂项—猫片(安恒)

转载

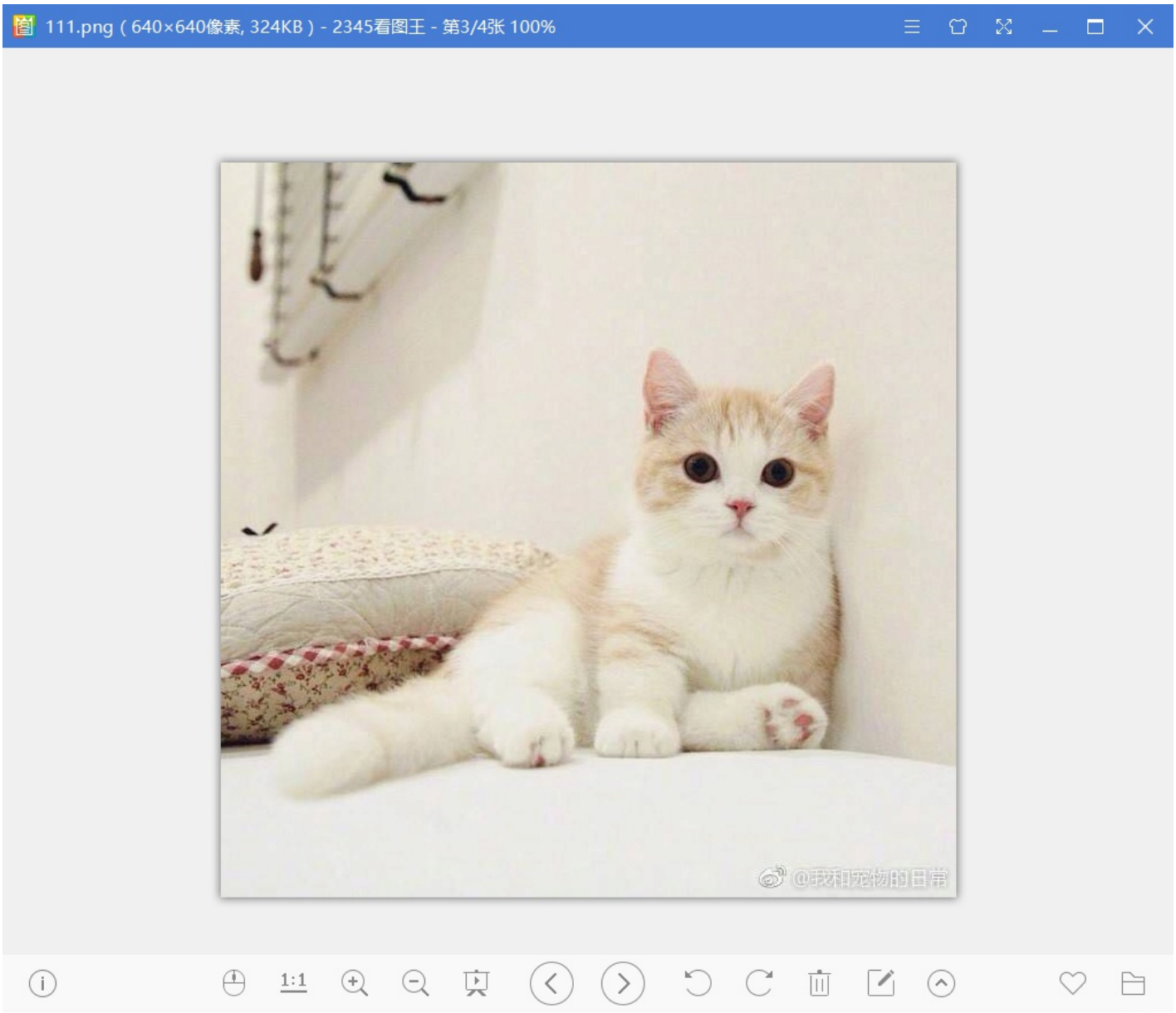
ana35287 于 2018-11-28 17:22:00 发布 244 收藏 1
文章标签： python 运维
原文链接：http://www.cnblogs.com/liuzeyu12a/p/10033384.html

根据题目提示

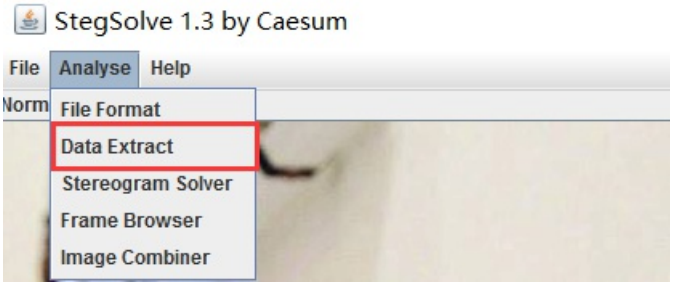
可以判断出来出来这很可能是一个LSB的图片隐写，下载下来



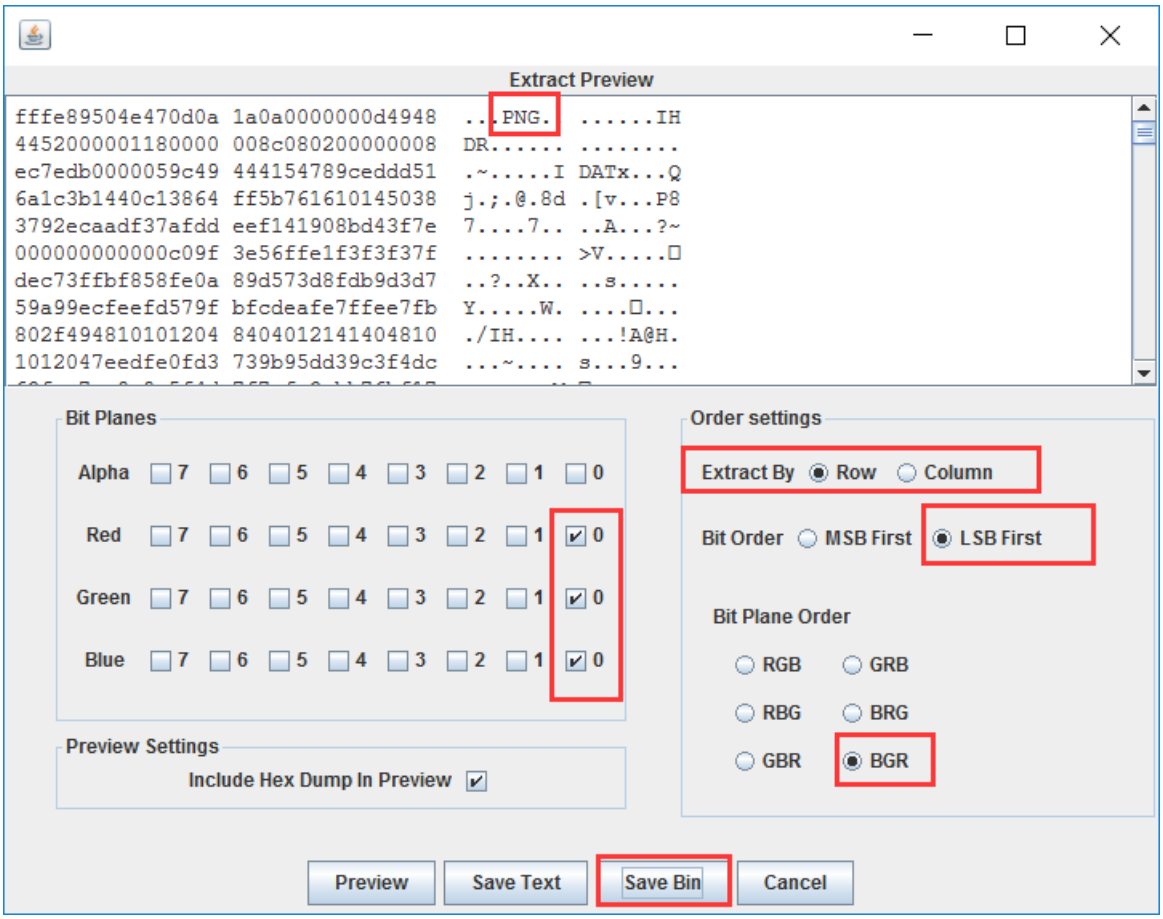
很明显是一个png的图片文件，只是被删掉了后缀名，我们将它补上



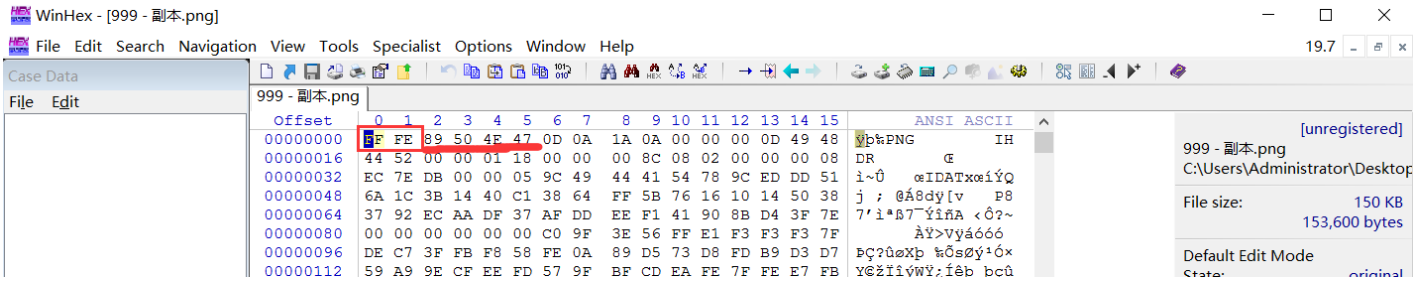
根据题目提示我们直接打开stegsolve的图片数据信息提取



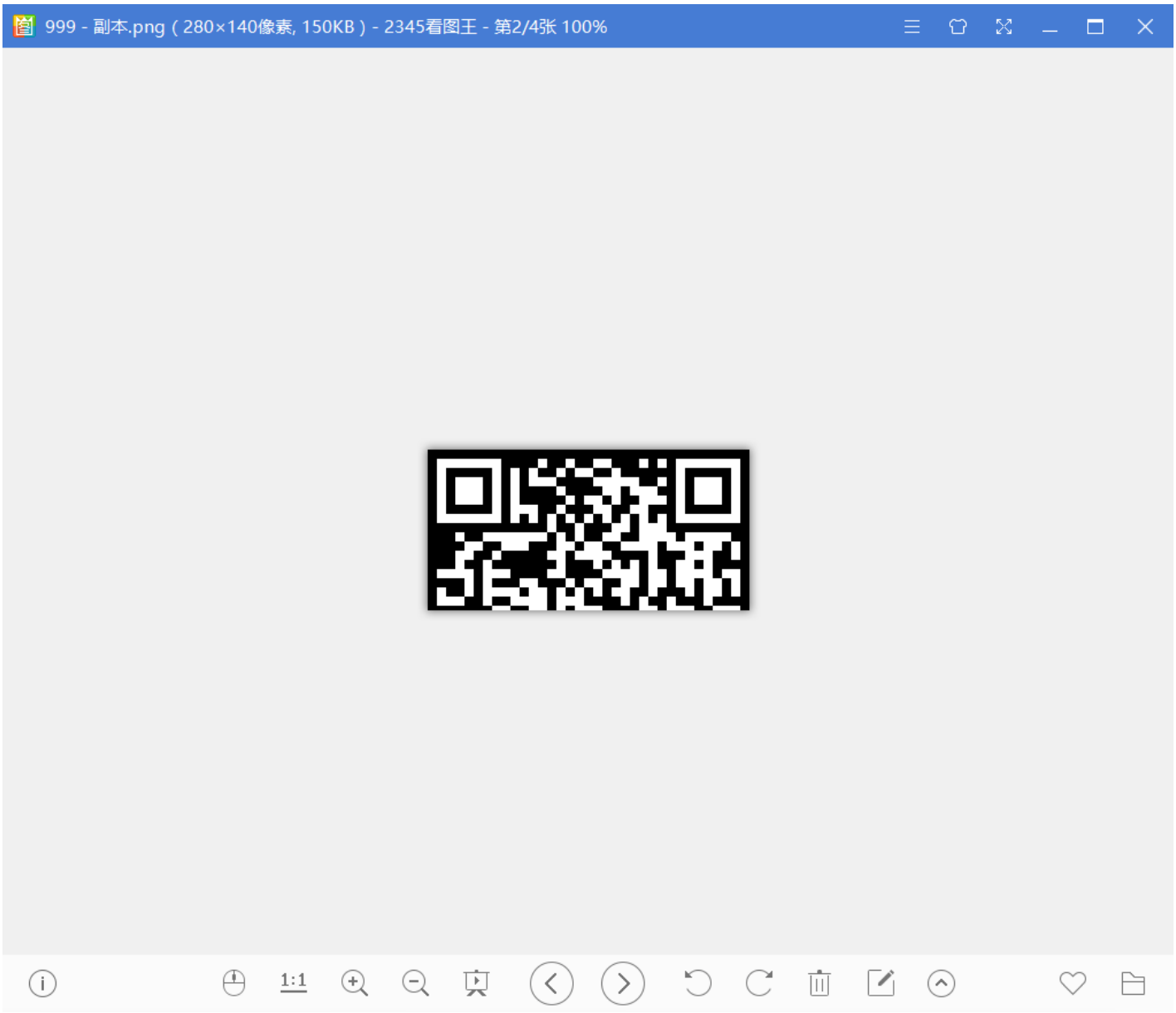
根据题目提示我们选择LSB和BGR



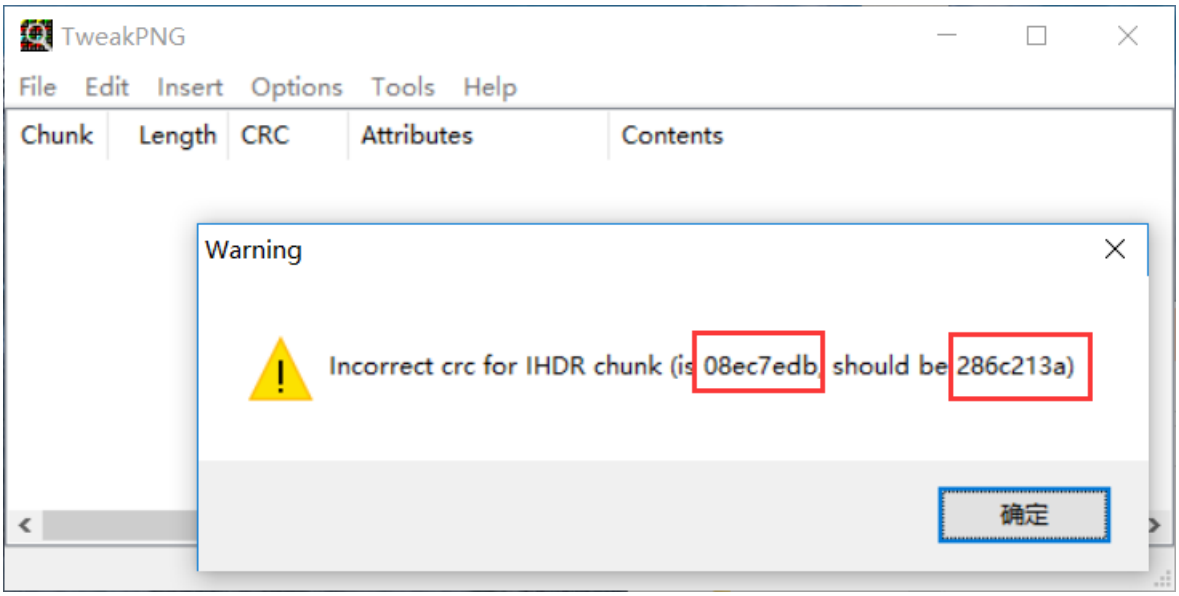
发现了里面隐藏了一张图片png我们将其提取出来，保存的格式bin(txt格式用winhex和010Editor打开都是乱码)，然后我们修改文件的后缀为png，然后发现图片打不开，用winhex打开



发现了并不是我们预期的png文件头，PNG (png)的正常的文件头：89504E47，所以们将他前面的FFFF删掉保存退出。



额 半张二维码@@，CRC值出错，很明显是高度出错引起的



这个时候我们用一个py脚本算出正确的宽度和高度

```python
import os
import binascii
import struct
crcbp = open("999.png","rb").read()   #文件名
for i in range(1024):
    for j in range(1024):
        data = crcbp[12:16] + struct.pack('>i',i) + struct.pack('>i',j) +
crcbp[24:29]
        crc32 = binascii.crc32(data) & 0xffffffff
        if crc32 == 0x08ec7edb:   #当前的CRC值
            print i,j
            print "hex",hex(i),hex(j)   #输出宽度和高度
```

在有python环境的kali下面跑一下脚本

```
root@kali:~/桌面/python跑脚本/图片隐写(png)# python calWidthHeight.py
280 280
hex 0x118 0x118
root@kali:~/桌面/python跑脚本/图片隐写(png)# A
```

在winhex里面修改保存即可。

999 - 副本.png

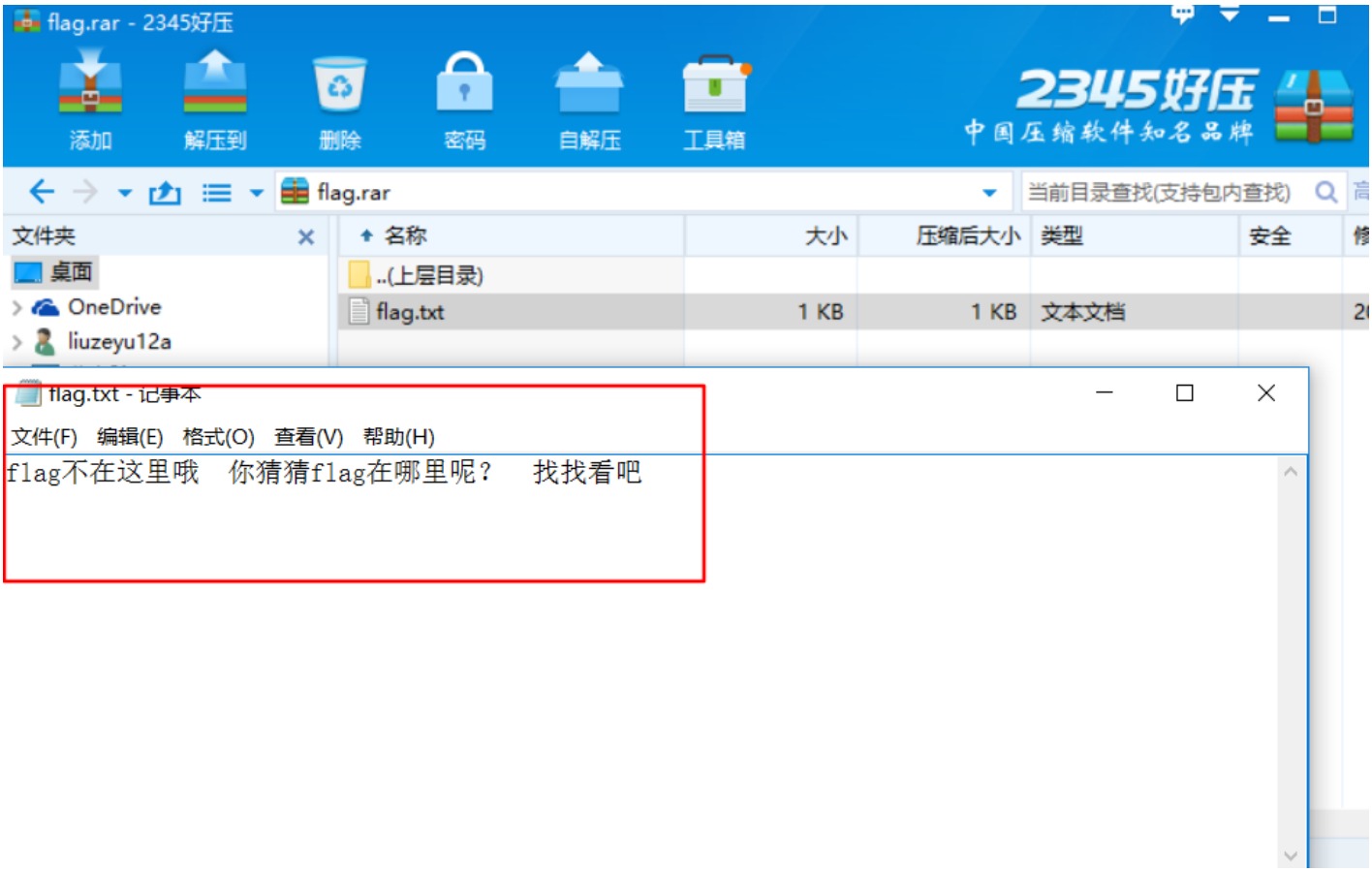
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52
00000016	00	00	01	18	00	00	01	18	08	02	00	00	00	28	6C	21
00000032	3A	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C

发现一个问题这个二维码和我们平时见到的不太一样，正常正方形中间应该是黑色的。所以还要用画图工具进行反色

反色后的图片用QR二维码扫一下

发现一个百度云链接，我也是醉了，还没出来 - -

打开链接下载一个压缩包



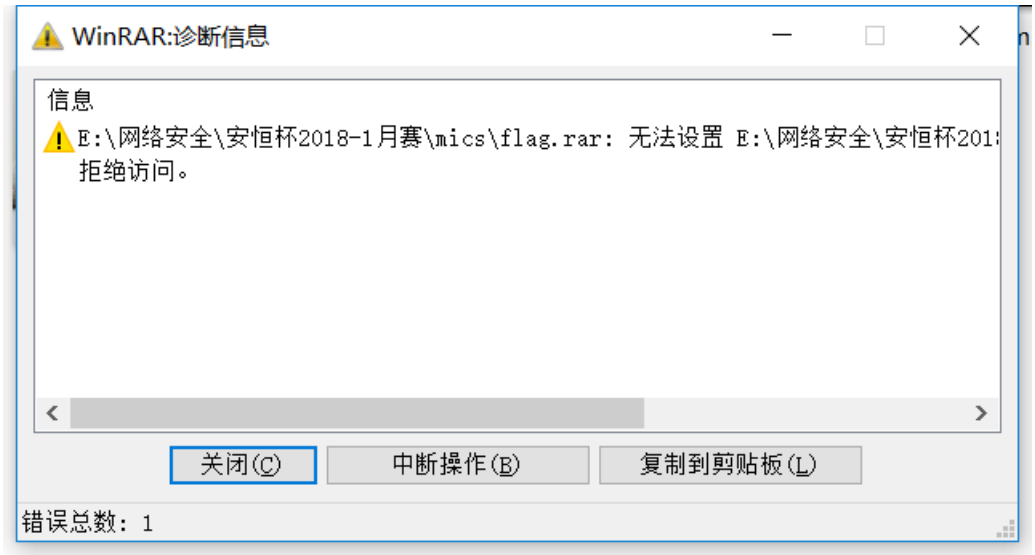
mmp flag竟然不在里面，真TM。。。无语。。现在呢？？我无从下手了 ，开始参考网上大佬的wp

度娘搜了下，发现另一位老铁写的writeup

https://www.jianshu.com/p/abc44c54857a

最后根据hint里面的提示“NTFS”，根据大佬的说法，这是一种流隐写，需要用到工具

ntfstreamseditor，然而。。这里还有一个坑就是，这压缩文件一定要用winrar来解压才会产生这样的效果

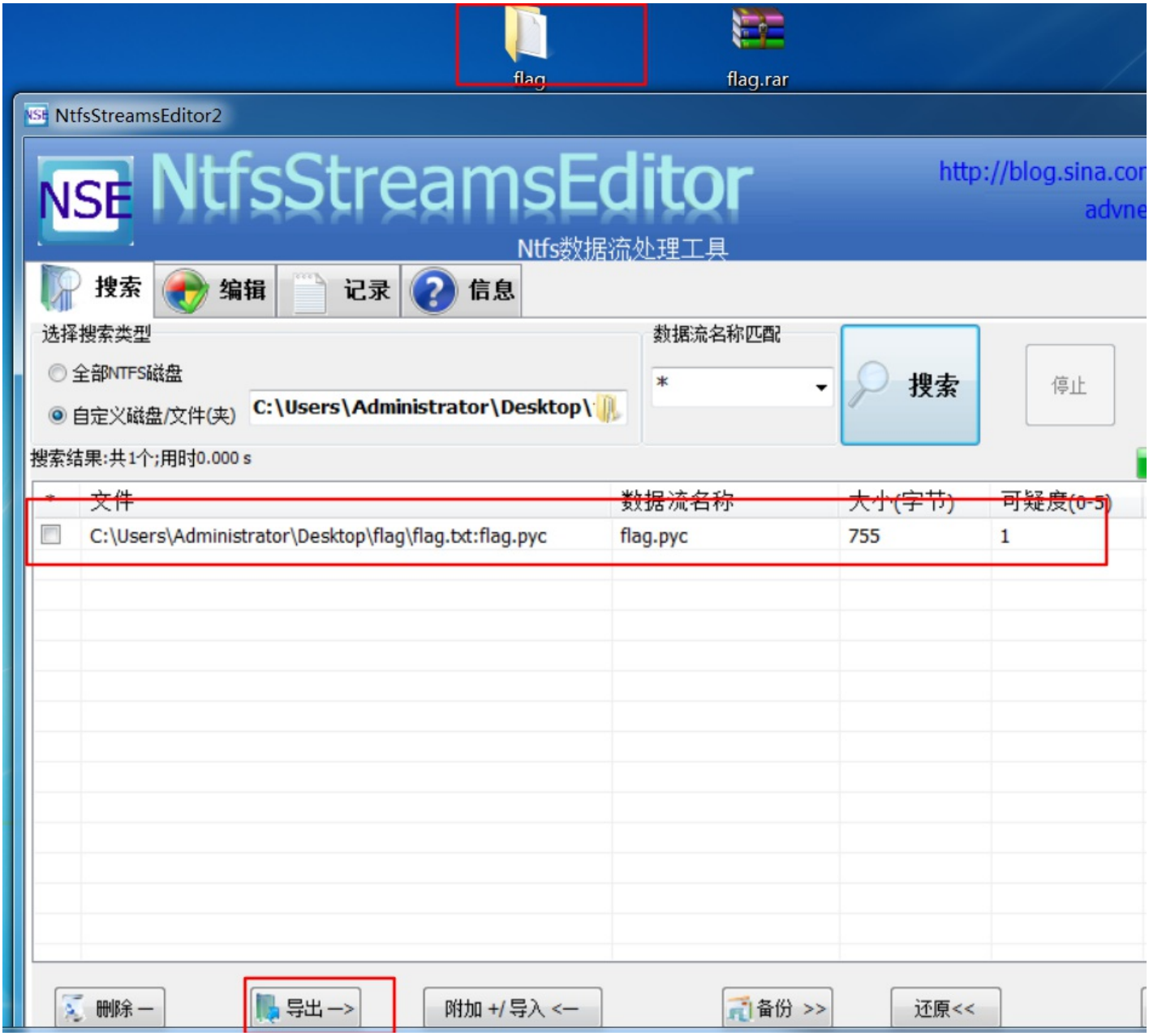


接着用ntfstreamseditor，查看解压的文件夹里面的数据流，然后把他导出来，而且更可恶的是解压的时候必须使用的是winrar来解压(我是在win7的虚拟机里面做的，

我也不知道win10为什么不能不能扫出来@@)

不然的话扫不出文件夹里面的数据流，，真的是坑爹到了极致@@

得到一个pyc文件，也就是py编译后的文件，因此需要扔到网上去在线反编译一下



这里推荐一个网站，可以反编译py， https://tool.lu/pyc/

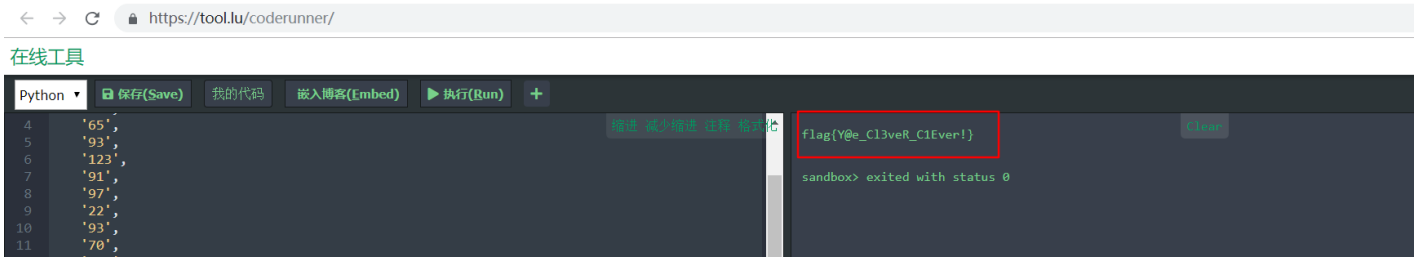
根据他这个加密的脚本再写出一个解密的脚本，运行一下就可以得到flag了

```python
def decode():
    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']
    ciphertext.reverse()
    flag = ''
    for i in range(len(ciphertext)):
        if i % 2 == 0:
            s = int(ciphertext[i]) - 10
        else:
            s = int(ciphertext[i]) + 10
        s=chr(i^s)
        flag += s
    return flag

def main():
    flag = decode()
    print(flag)

if __name__ == '__main__':
    main()
```

拿到这个网上去跑一下就出来了



吐槽一番：

我只能想吐一口血在出题人脸上，没写过py，这个脚本和还是参考网上大佬写的，好刚嘎，刚刚那个软件ntfstreamseditor也是花了很长时间才找到的，网上这种软件都快绝种了。。这个题目解题的一个转折点就是从数据流中提取出来那个已经编译过的py程序，我们需要拿去反编译，

然后呢？就是要看得懂这个加密脚本了，再然后呢，就是写解密脚本了，这个是真的没写过@@,一波三折， +写博客=花了4个小时 - 感觉dei找个时间去学一下py --人生苦短，我用python。

转载于:https://www.cnblogs.com/liuzeyu12a/p/10033384.html