Bugku writeup 猫片（安恒）

转载

FrancisQiu 于 2019-03-10 23:24:07 发布 1996 收藏 1

分类专栏： CTF CTFwriteup Bugku misc

CTF 同时被 3 个专栏收录

7 篇文章 0 订阅

订阅专栏

CTFwriteup

8 篇文章 0 订阅

订阅专栏

Bugku

3 篇文章 0 订阅

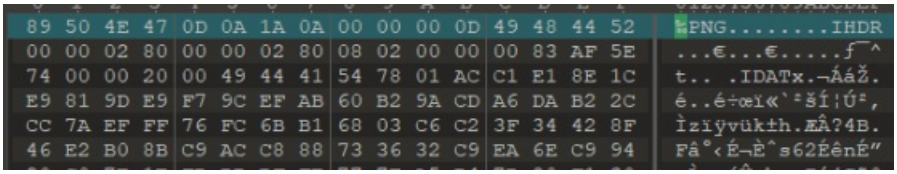
订阅专栏

Bugku writeup 猫片（安恒）

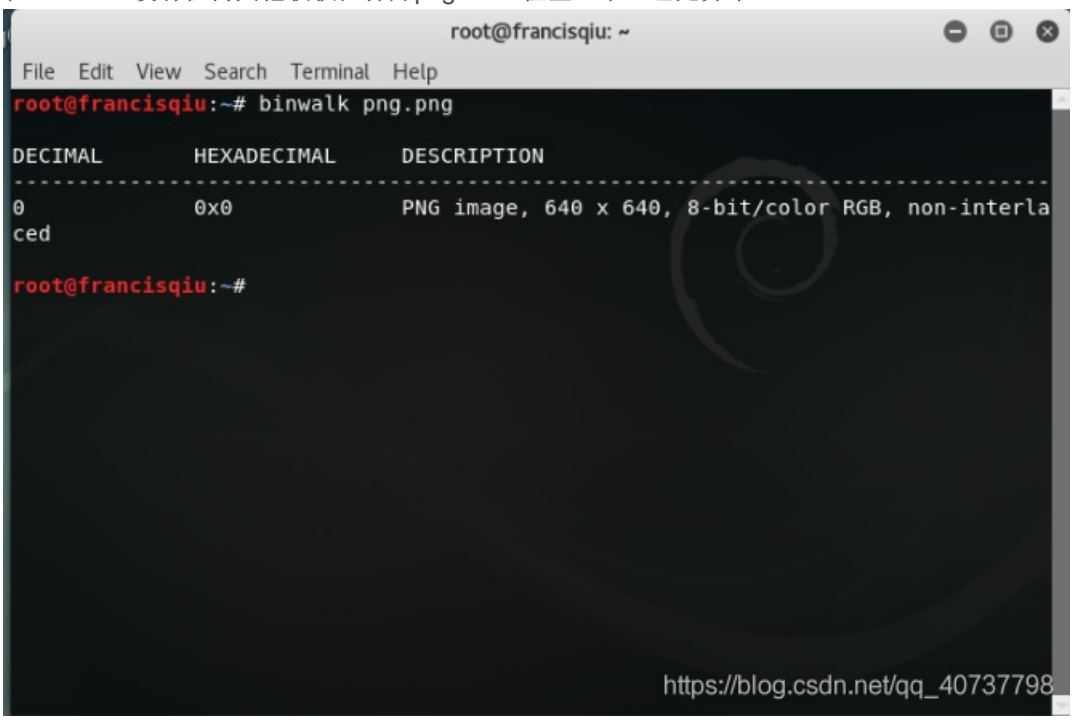
题目：

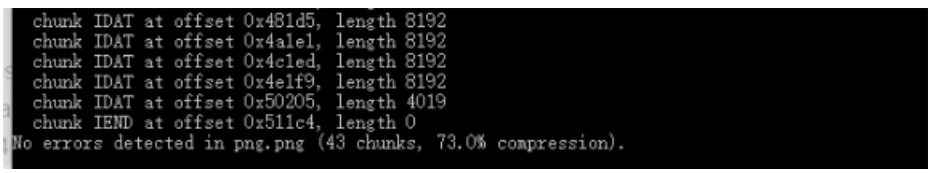
解题：

1、首先打开题目附件，得到一个png的二进制文件。用010editor打开，发现头部内容显示为png，因此修改文件后缀，得到一张图片。



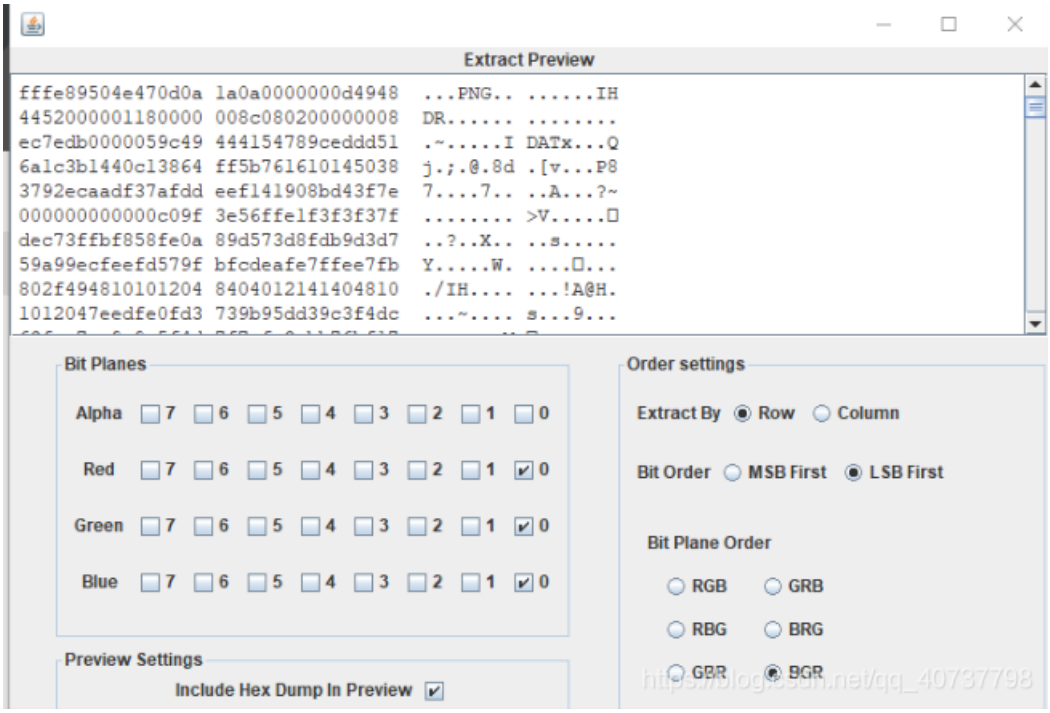
打开虚拟机跑一下binwalk，没有任何其他收获；打开pngcheck检查一下，也无异常。



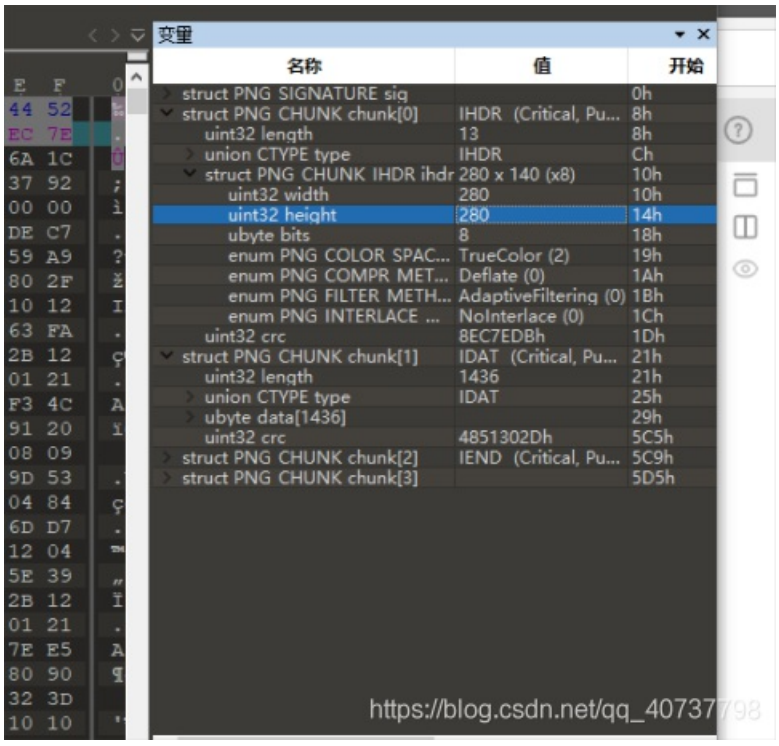


2、在这时，思考hint内容：LSB、BGR，故使用Stegsolve，在Data Extract内勾选LSB、BGR、Red 0、Green 0、Blue 0，发现

了preview部分出现了“PNG"信息，因此选择“Save bin”，保存为png文件。



用010editor将头部信息矫正，将“FFFE”删除并保存，打开修改后的图片，发现是一张二维码，但是此二维码高度需要修改。再次运行010editor，通过变量窗口修改高度。



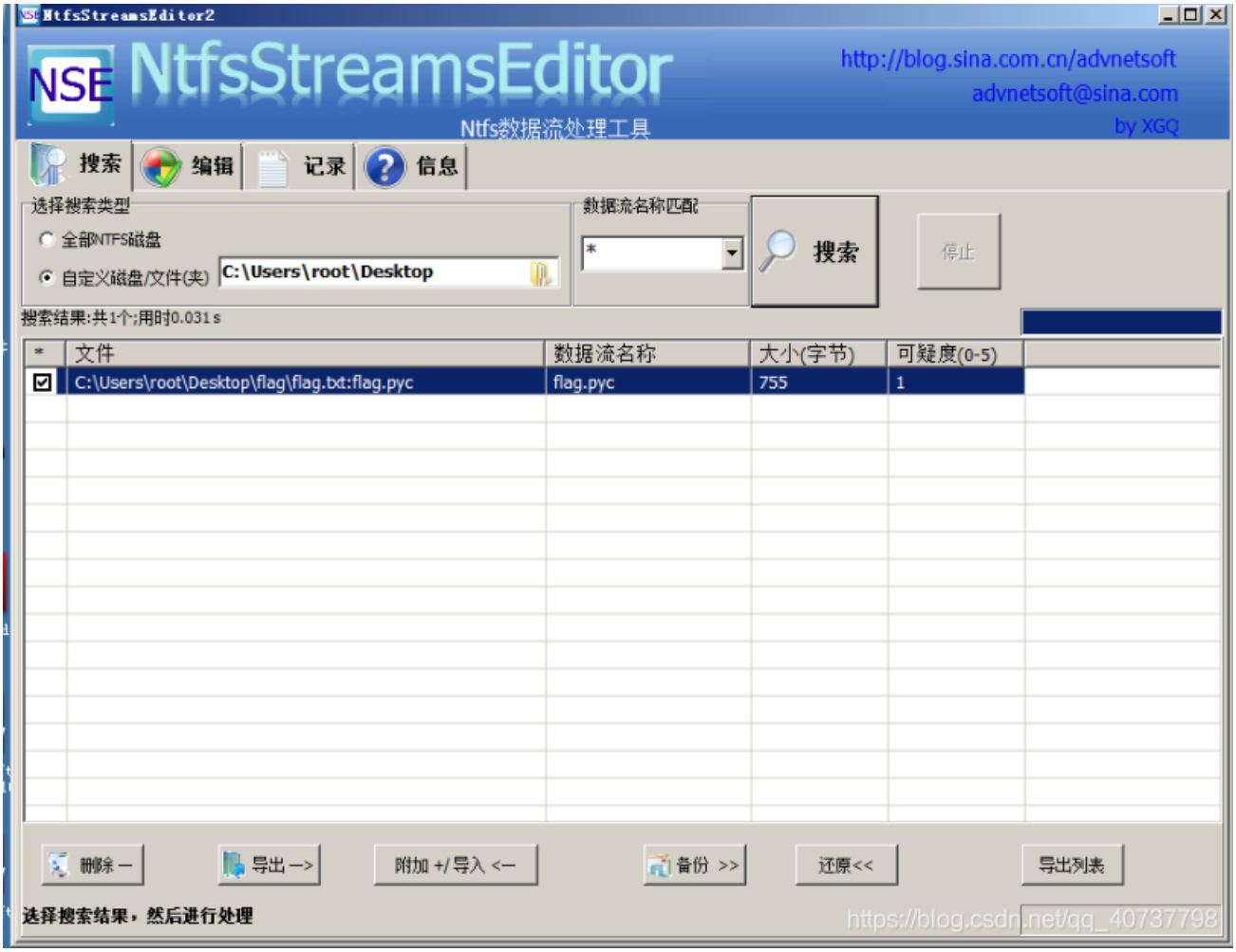
得到一张完整的二维码，但是此二维码却需要反色处理，可以使用画板按“shift”+“ctrl”+“i”进行反色之后再扫码，也可以直接使用

QR Research直接打开获取内容，得到一个百度网盘链接：

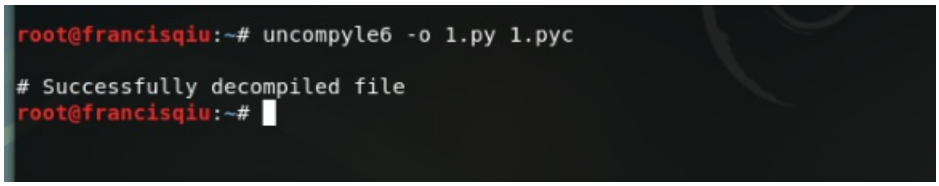
3、打开网盘后，发现是个flag.rar文件，下载之后打开压缩包，里面有个flag.txt文件。直接打开txt文件，却发现：

> flag不在这里哦 你猜猜flag在哪里呢？ 找找看吧

尝试解压，也没问题；打开binwalk跑，也没结果。苦想想不出，就直接去看大手子写的WP了，发现这居然是个坑：用winrar解压会提示解压错误（PS：本人一向来只用7-zip，这个坑我fo了）。这时还剩一个hint：NTFS，根据大佬的WP，这是一个NTFS文件流隐写的问题，可以使用ADS或者NtfsStreamEditor。下载NtfsStreamEditor这软件之后win10内打不开，于是又临时搞了个win7虚拟机。打开之后导入flag.txt，发现确实隐含了一个pyc文件，但是开头用的是v1.0版本又导出不出来，于是只能去下v2.0版本，得到以下结果：



4、将得到的pyc文件用uncompyle6反编译之后得到py文件。



得到的py文件内容如下：

```
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']
```

这显然是个对称加密，因此写个解密函数：

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

最终获取得到flag。

```
D:\code\CTF-tools\venv\Scripts\python.exe
flag{Y@e_Cl3veR_C1Ever!}

Process finished with exit code 0
```