攻防世界Misc(下)

原创

[她叫常玉莹](#) 于 2021-07-27 00:40:39 发布 52 收藏 1
分类专栏： [CTF](#) 文章标签： [CTF](#) [writeup](#) [攻防世界](#) [ctf刷题](#) [网络安全](#)


[CTF 专栏收录该内容](#)
18 篇文章 0 订阅
订阅专栏

> 博客新地址: c7ay.top

掀桌子

题目给出一串
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2
试了下16进制转字符串不行

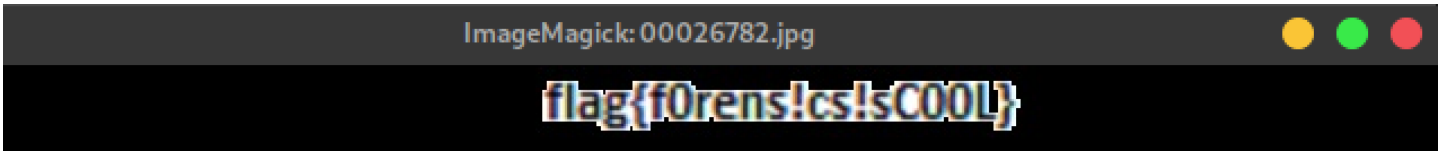
搞了半天是两个一组减128转ascii码(技术太菜)

```
s = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2"
flag = ""
for i in range(0,len(s),2):
    flag+=chr(int(s[i:i+2],16)-128)
print(flag)
```

```
~/CTF_practice/攻防世界_Misc
❯ python3 掀桌子.py
Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr
```

ext3

先foremost得到章写着flag的图片，好像签到题，一提交md不对…



题目里说生日收到个linux系统光盘，挂载下看一下。没发现可疑的直接find下flag得到个base64解码提交正确

```
root@kali:~/Desktop/ctf_GFMisc/abc# find -name flag*
./O7avZhikgKgbF/flag.txt
root@kali:~/Desktop/ctf_GFMisc/abc# cat ./O7avZhikgKgbF/flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=
root@kali:~/Desktop/ctf_GFMisc/abc#
```


stegano

给了个pdf文件,打开全是英文后面水印提示这没有flag
浏览器打开pdf控制台document.documentElement.textContent查看下全部文本

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB
有间隔不是二进制，可能是摩斯电码

```
str = 'BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB A
AAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB'
str = str.replace("B","-")
str = str.replace("A",".")
print(str)
```

```
~/CTF_practice/攻防世界_Misc
❯ python3 摩斯电码.py
-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- ..... ..... ....- --. ...--
```

摩斯密码解密得到 CONGRATULATIONS,FLAG:1NV151BL3M3554G3 flag小写

SimpleRAR

附件给了个RAR压缩包，解压后得到个flag.txt文件（肯定没这么简单）用hex fiend看了下压缩包，看到了secret.png

RAR文件码流分析

标记块：HEAD_TYPE=0x72

压缩文件头：HEAD_TYPE=0x73

文件头：HEAD_TYPE=0x74

旧风格的注释头：HEAD_TYPE=0x75

旧风格的用户身份信息：HEAD_TYPE=0x76

旧风格的子块：HEAD_TYPE=0x77

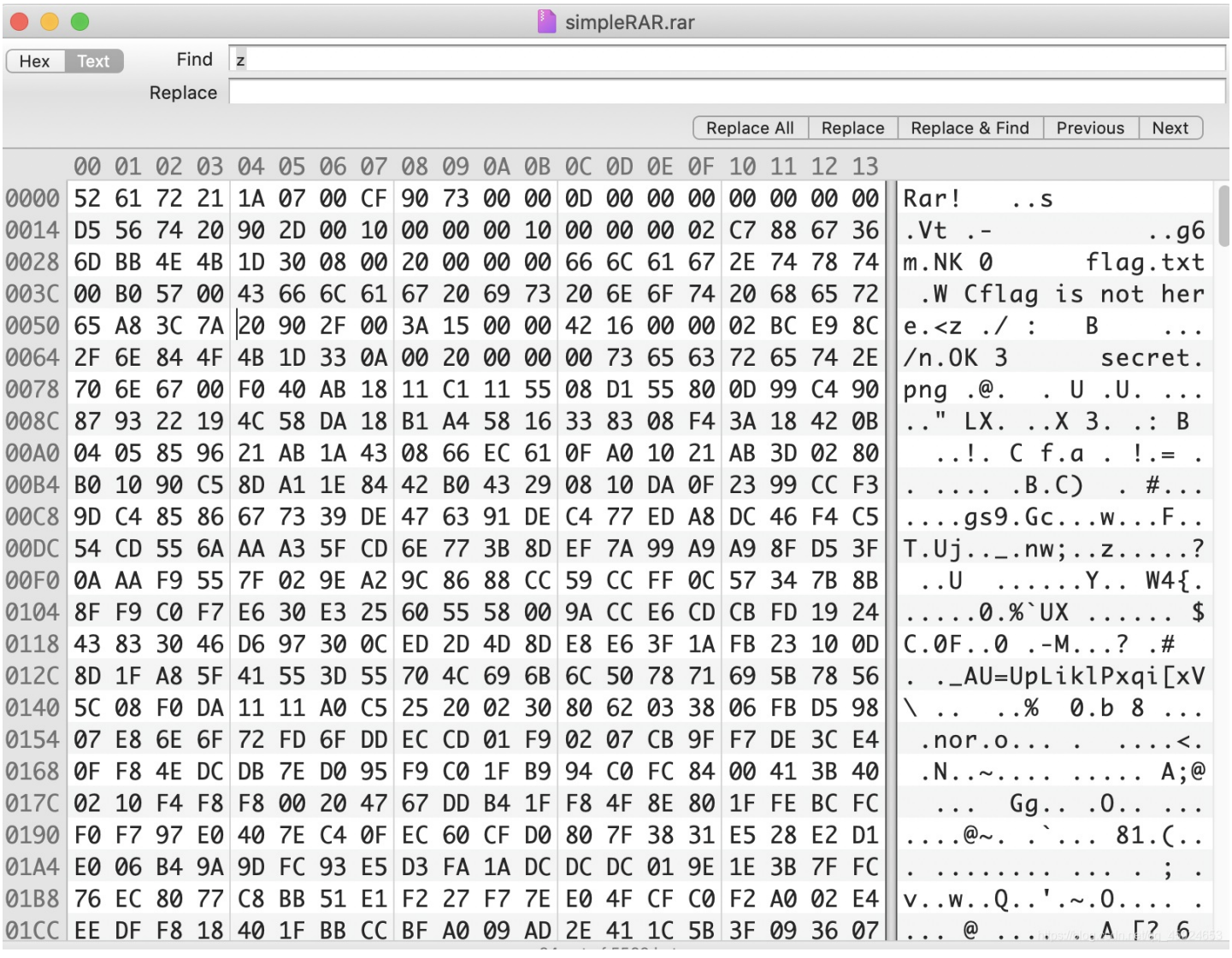
旧风格的恢复记录：HEAD_TYPE=0X78

旧风格的用户身份信息：HEAD_TYPE=0X79

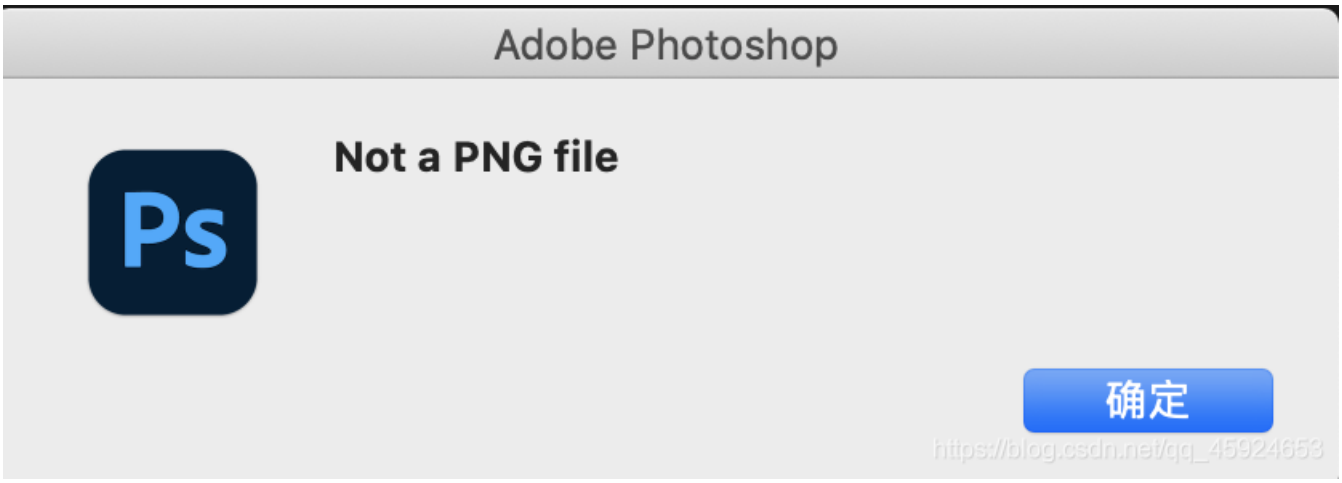
子块：HEAD_TYPE=0x7A

最后的结束块：HEAD_TYPE=0x7B

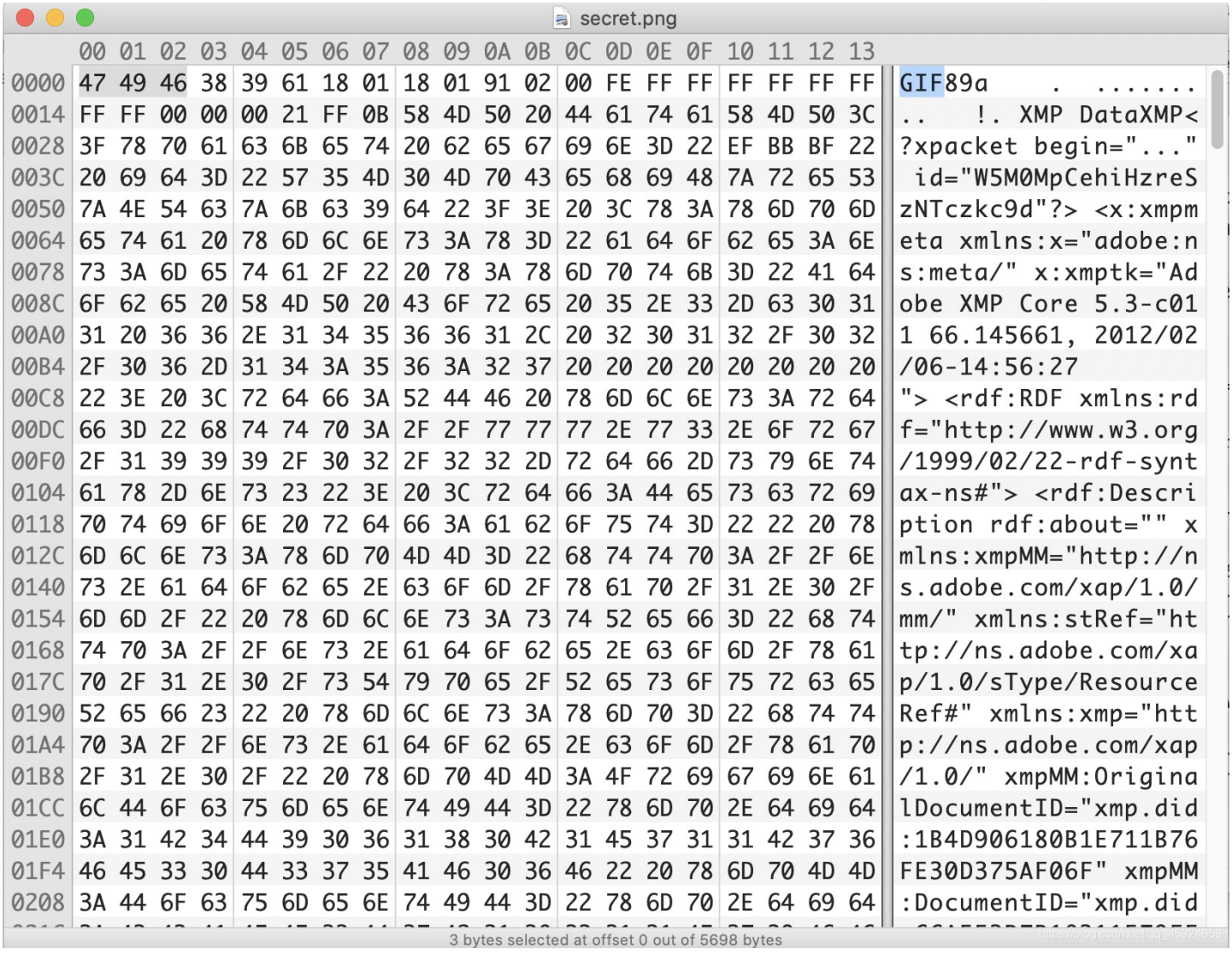
将7A改为74文件头



解压后有一张png图片，提示中说双图层用ps打开后报错

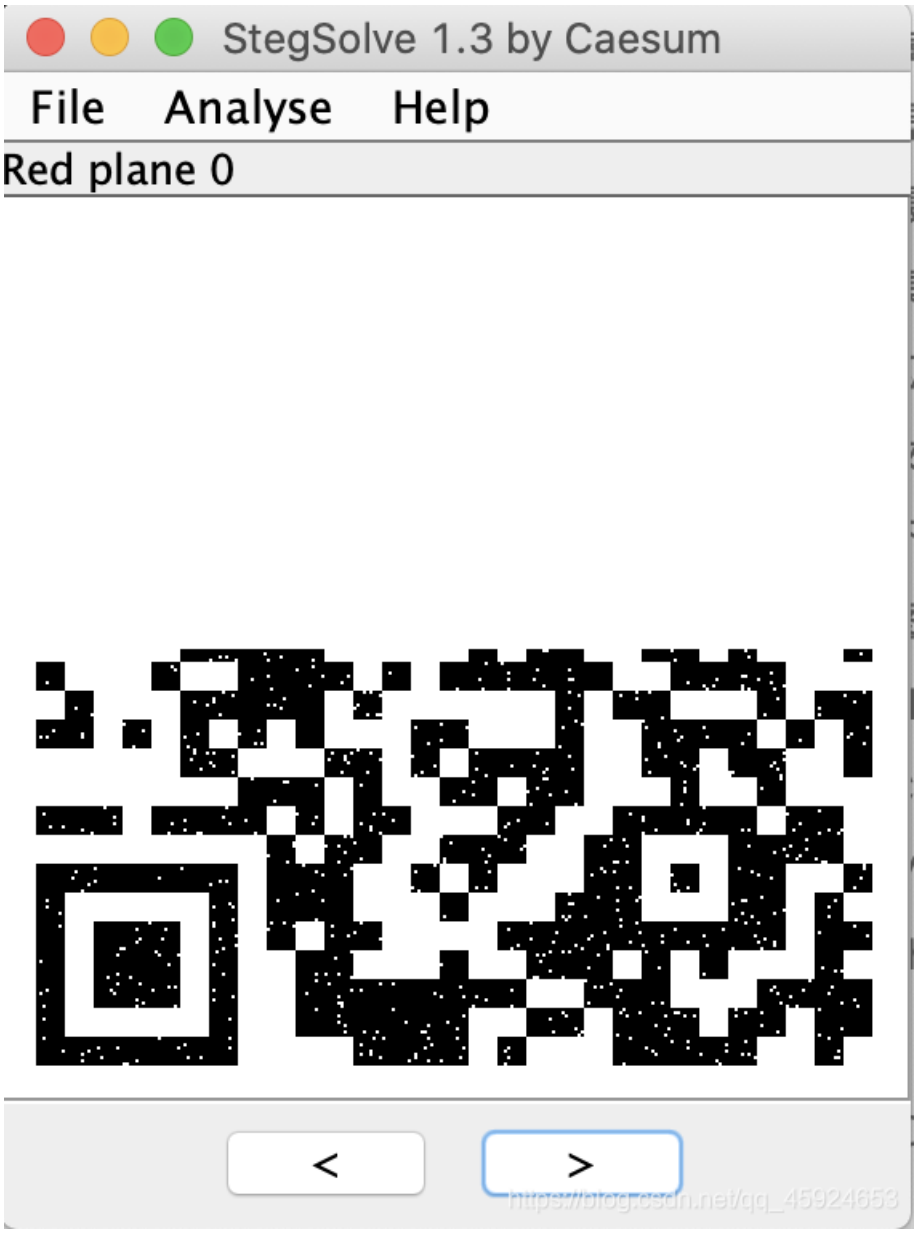


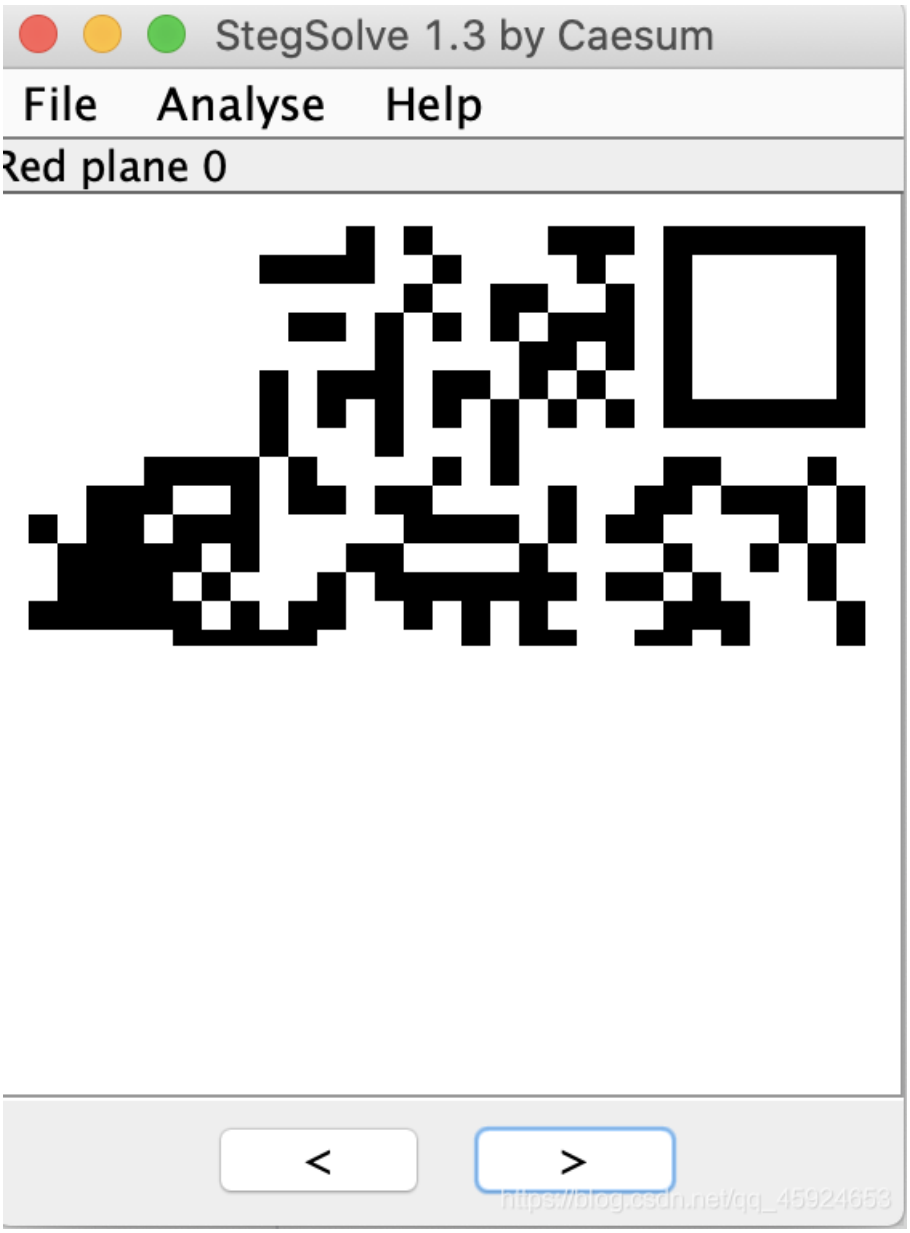
接着用hex fiend看一下 头是gif



重命名后用ps打开 有两个空白图层

将两个图层保存打开stegsolve看一下，得到二维码，补全定位角得到flag





base64stego

base64隐写

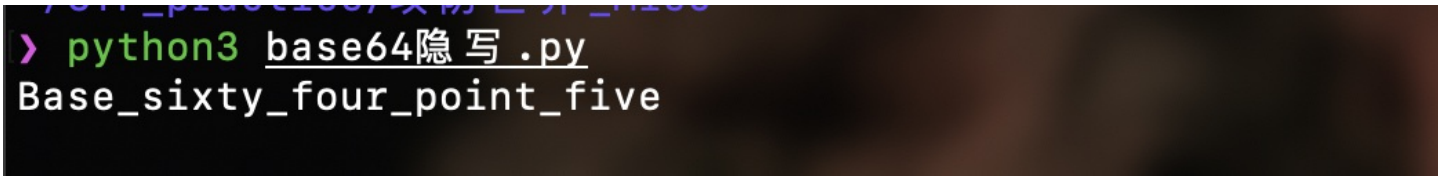
隐写原理：base64编码再解码这个过程中，会出现"="个数*2bit的字节数的无效字节，也就是说这些字节无论填充什么，都不会影响结果

```
import base64
b = ''
for i in range(26):
    b = 'U' + chr(65 + i) + '=='
    print(b)
    print(base64.b64decode(b))
>>>
UA==
b'P'
UB==
b'P'
UC==
b'P'
UD==
b'P'
UE==
b'P'
UF==
b'P'
UG==
b'P'
UH==
b'P'
UI==
b'P'
UJ==
b'P'
UK==
b'P'
UL==
b'P'
UM==
b'P'
UN==
b'P'
UO==
b'P'
UP==
b'P'
UQ==
b'Q'
UR==
b'Q'
US==
b'Q'
UT==
b'Q'
UU==
b'Q'
UV==
b'Q'
UW==
b'Q'
UX==
b'Q'
UY==
b'Q'
UZ==
b'Q'
```

要是发P UA==可以UB==也可以
拿隐写脚本跑一下

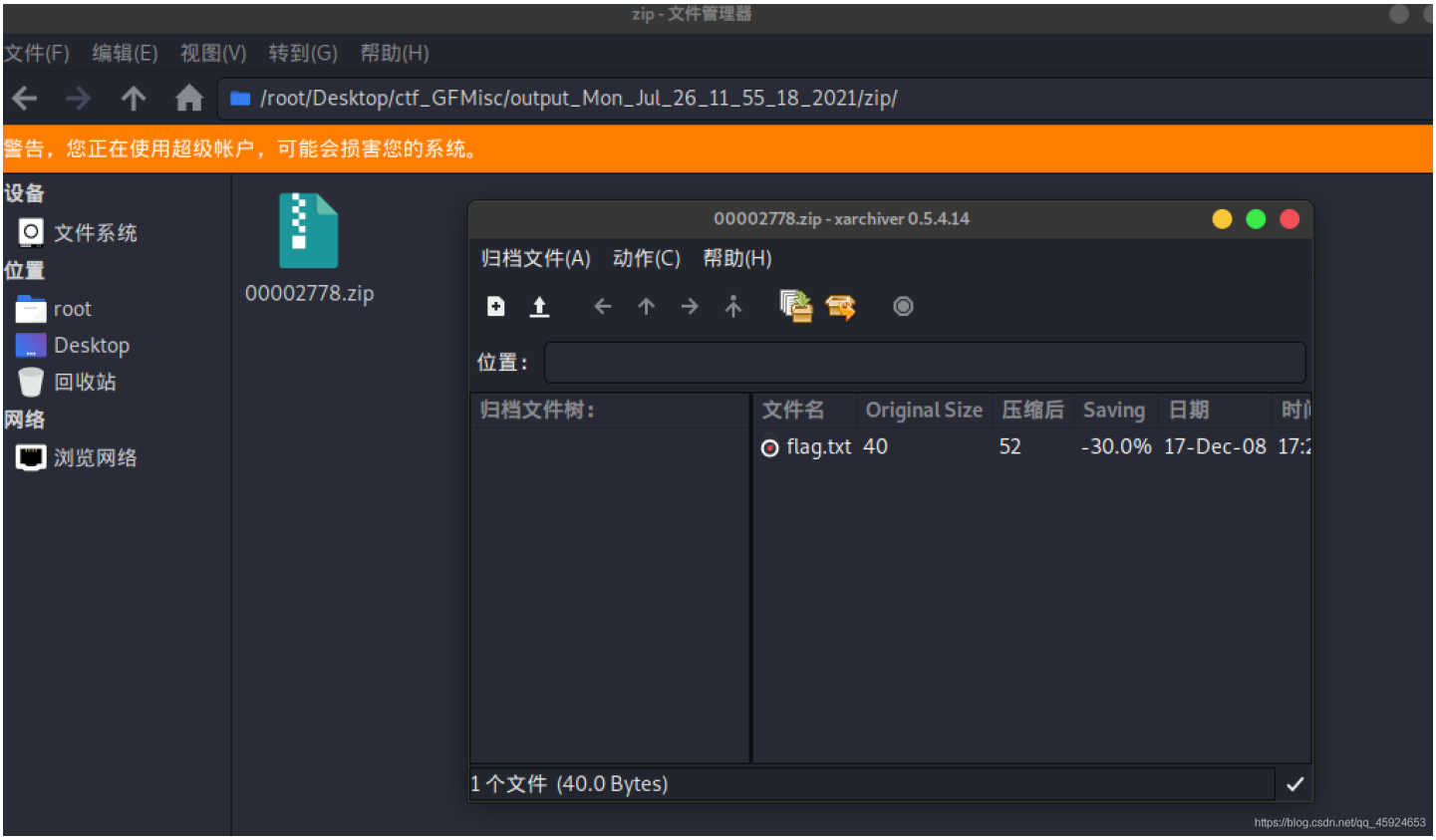
```
import base64
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 =  str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")#删除首尾换行

        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1]))
        #把末尾的'='去掉,offset = |给定字符串在b64表中的位置-解码字符串在b64表中的位置|
        equalnum = stegb64.count('=') #计算等号个数
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)#返回offset的二进制形式
            print(''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])) #8 位一组
```

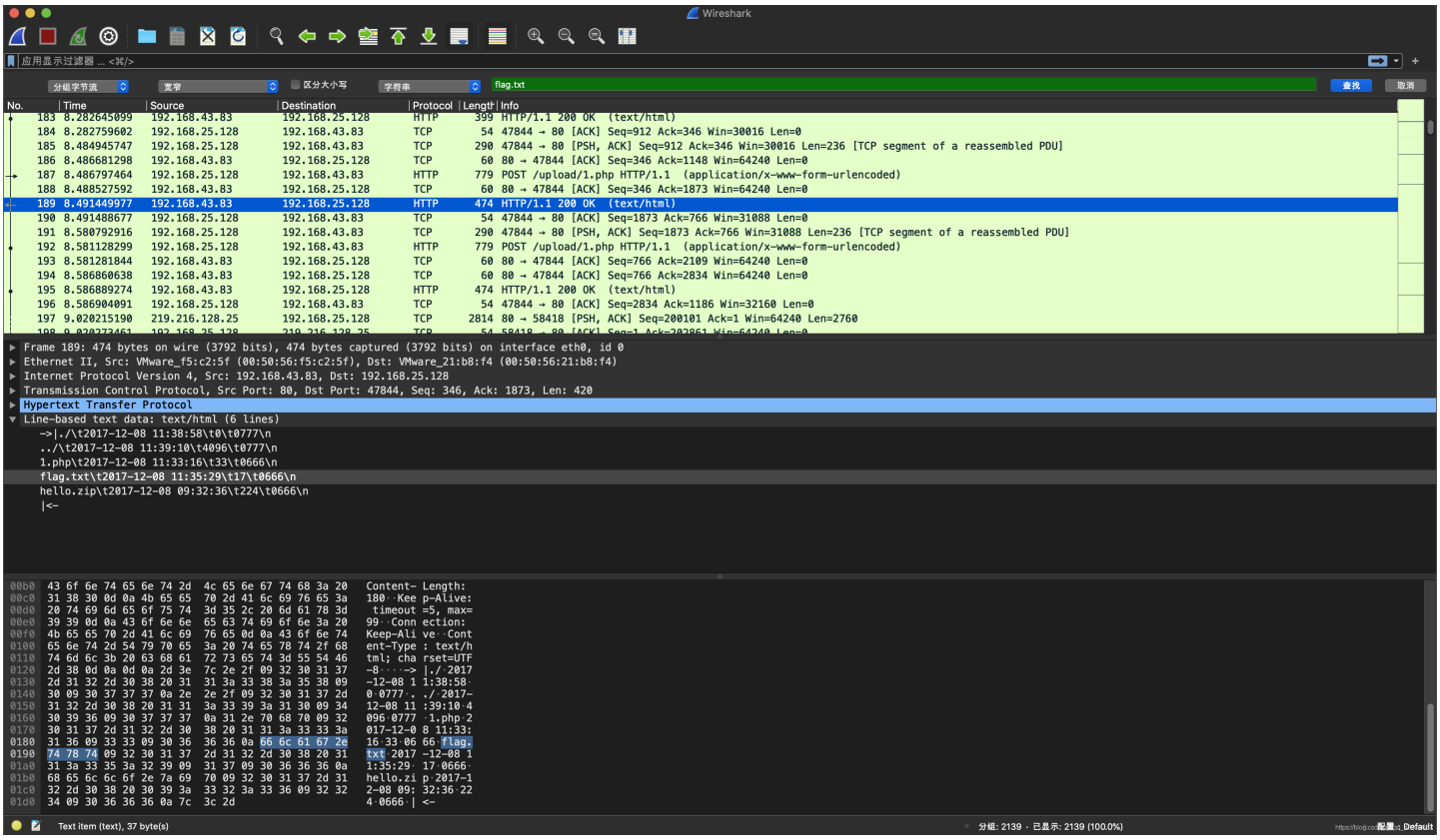


功夫再高也怕菜刀

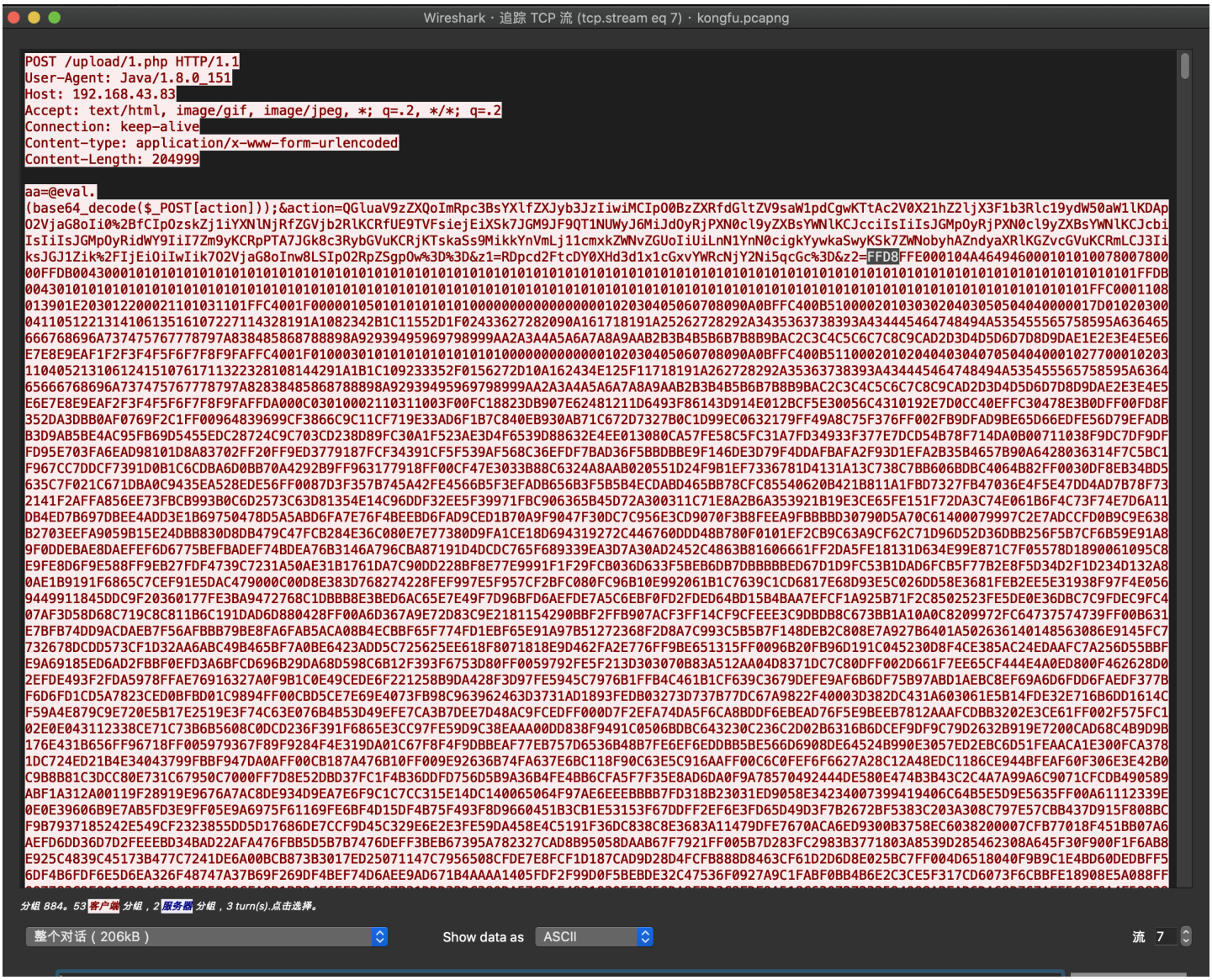
下载附件得到个pcapng文件，foremost一下有个压缩包，里面有flag.txt文件可是需要密码

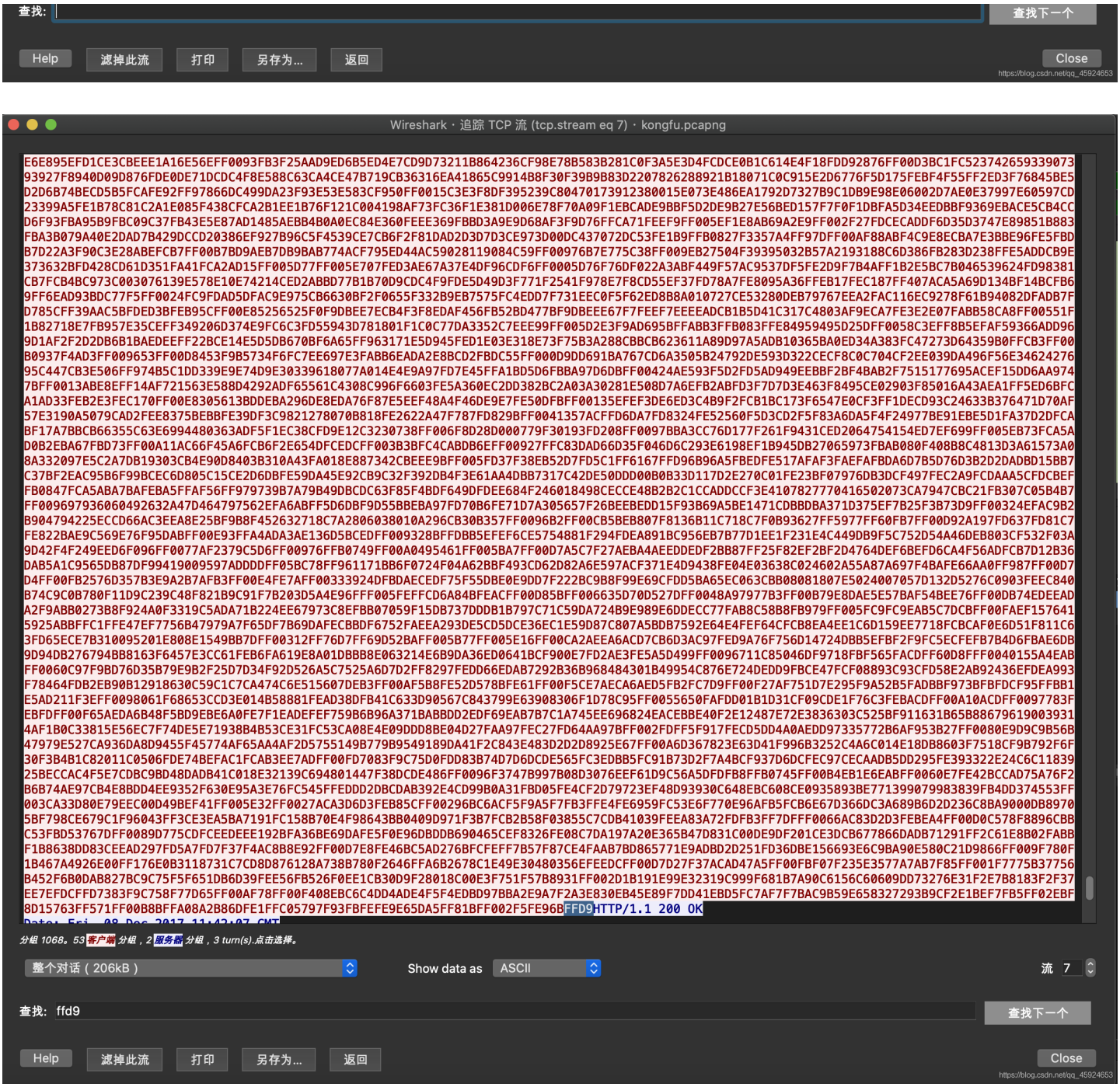


先打开wireshark看一下，搜索下关键字



跟踪TCP流，发现ffd8是jpg文件





FFD8到最后一个FFD9复制到HexFiend，ASCII形式保存位jpg文件

打开图片这应该就是解压密码

解压flag.txt中得到flag

> 人生漫漫其修远兮，网安无止境。
> 一同前行，加油！