攻防世界misc高手进阶篇教程（2）

原创

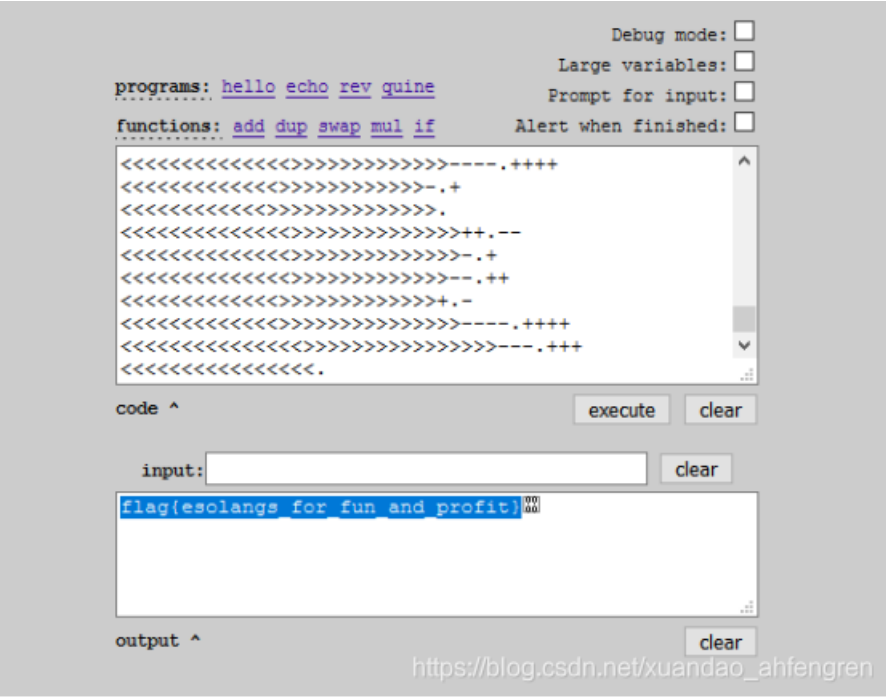
锋刃科技 于 2020-05-26 12:31:14 发布 1740 收藏 6
文章标签： ctf攻防世界

本文链接：https://blog.csdn.net/xuandao_ahfengren/article/details/106353523

can_has_stdio?

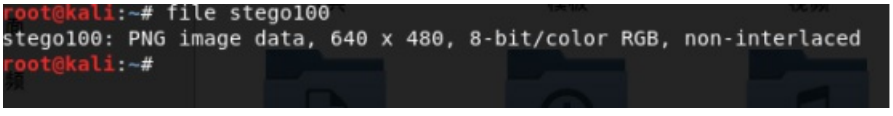
通过brainfuck在线工具打开即可

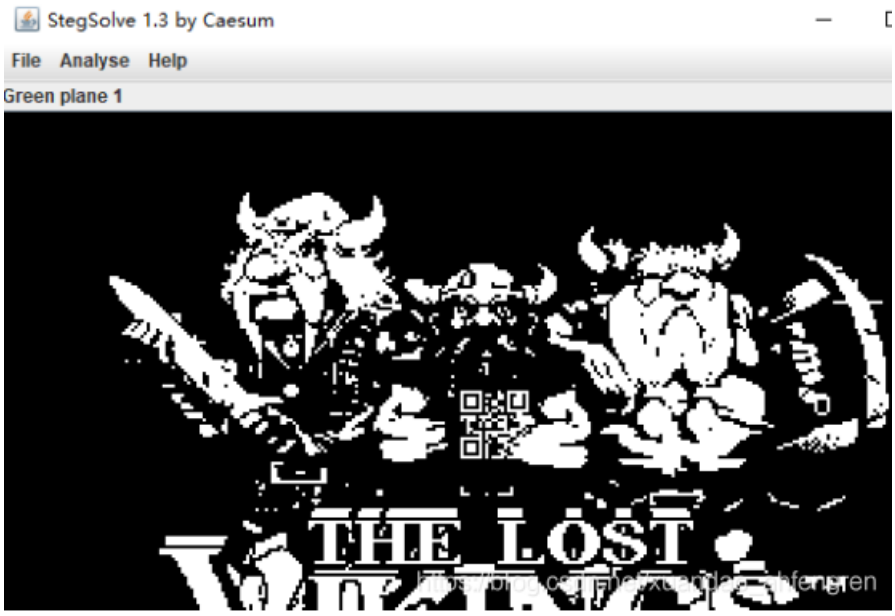
http://esoteric.sange.fi/brainfuck/impl/interp/i.html



Erik-Baleog-and-Olaf

file发现是png格式，根据图片名字联想到使用Stegsolve工具



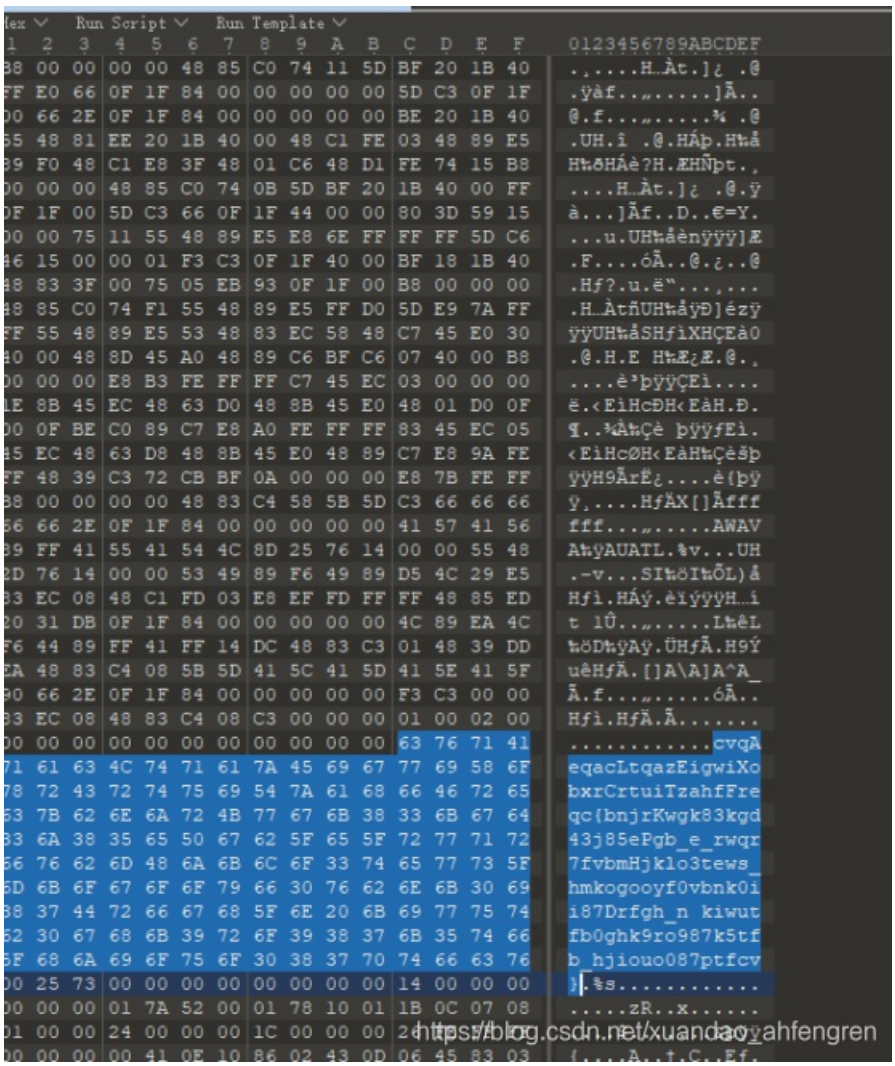


使用ps进行补全，扫描二维码得到flag

flag{#justdiffit}

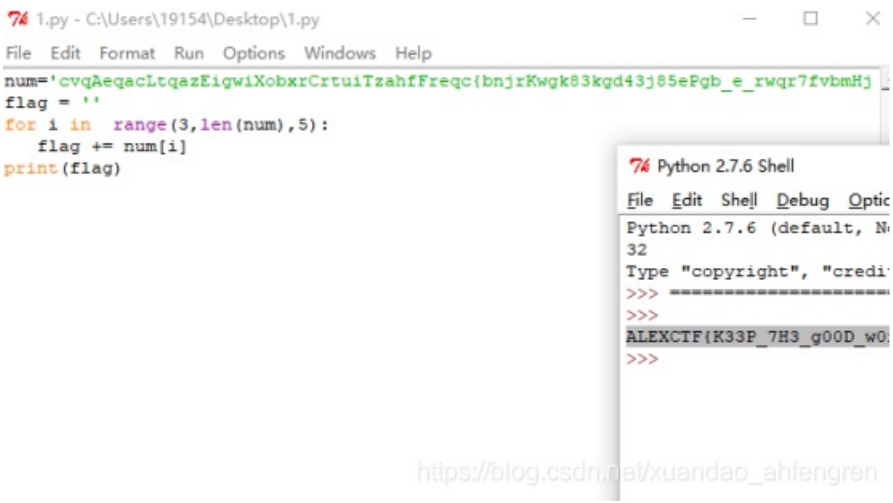
hit-the-core

用010editor打开，发现关键字符串



然后我们发现大写的XCTF每个字母之间只隔了四个字母，使用python提取一下，得到flag。

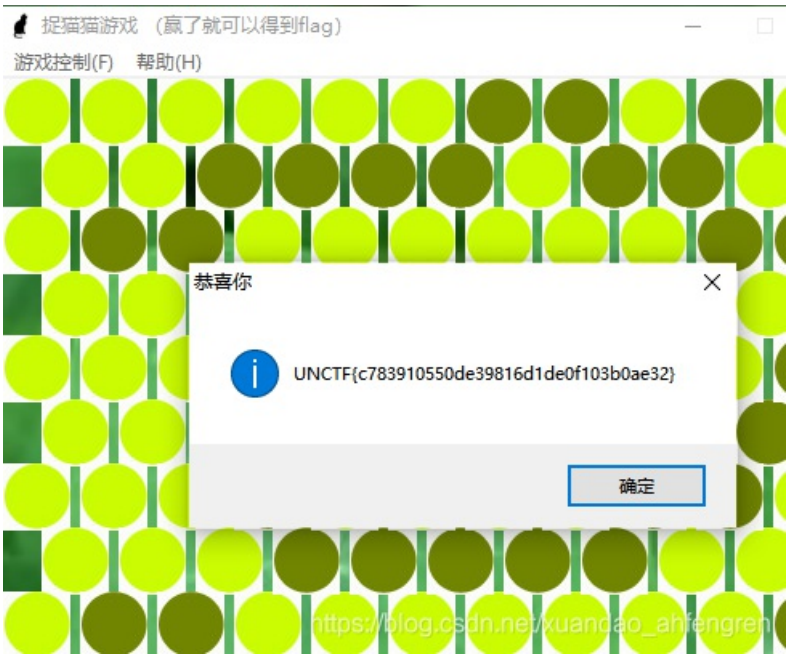
```
num='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii8
flag = ''
for i in  range(3,len(num),5):
   flag += num[i]
print(flag)
```



快乐游戏题

直接通关就可以了

提示：flag是固定的可以直接提交，UNCTF{c783910550de39816d1de0f103b0ae32}



glance-50

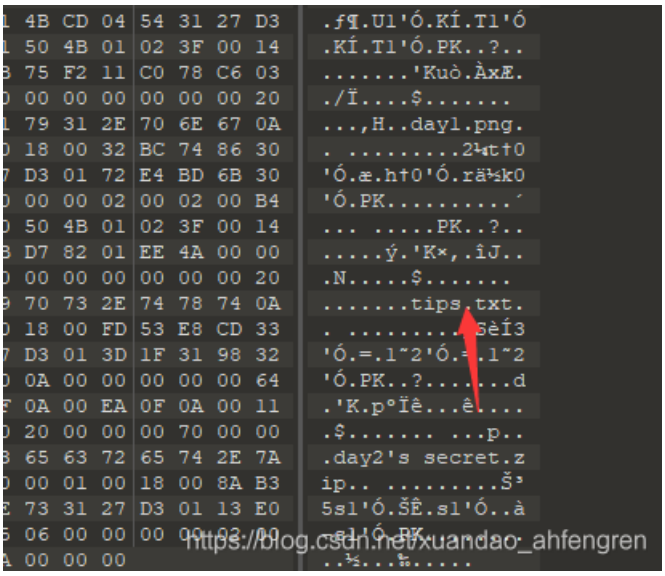
用在线网站直接拼接

https://tu.sioe.cn/gj/fenjie/

TWCTF{Bliss by Charles O'Rear}

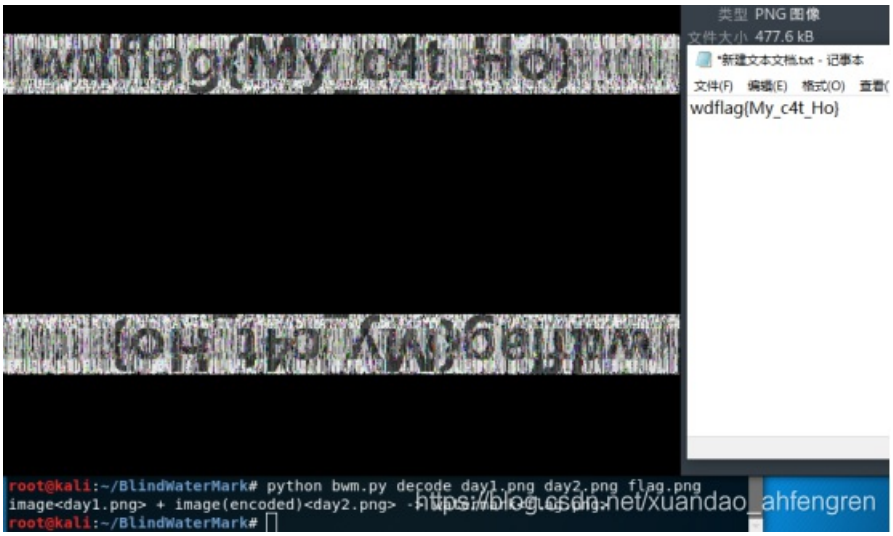
4-1

先用010editor编辑图片，发现txt文件，直接把后缀修改成zip把文件压缩出来



解压后txt中提示flag在day2.png中，猜想是盲水印

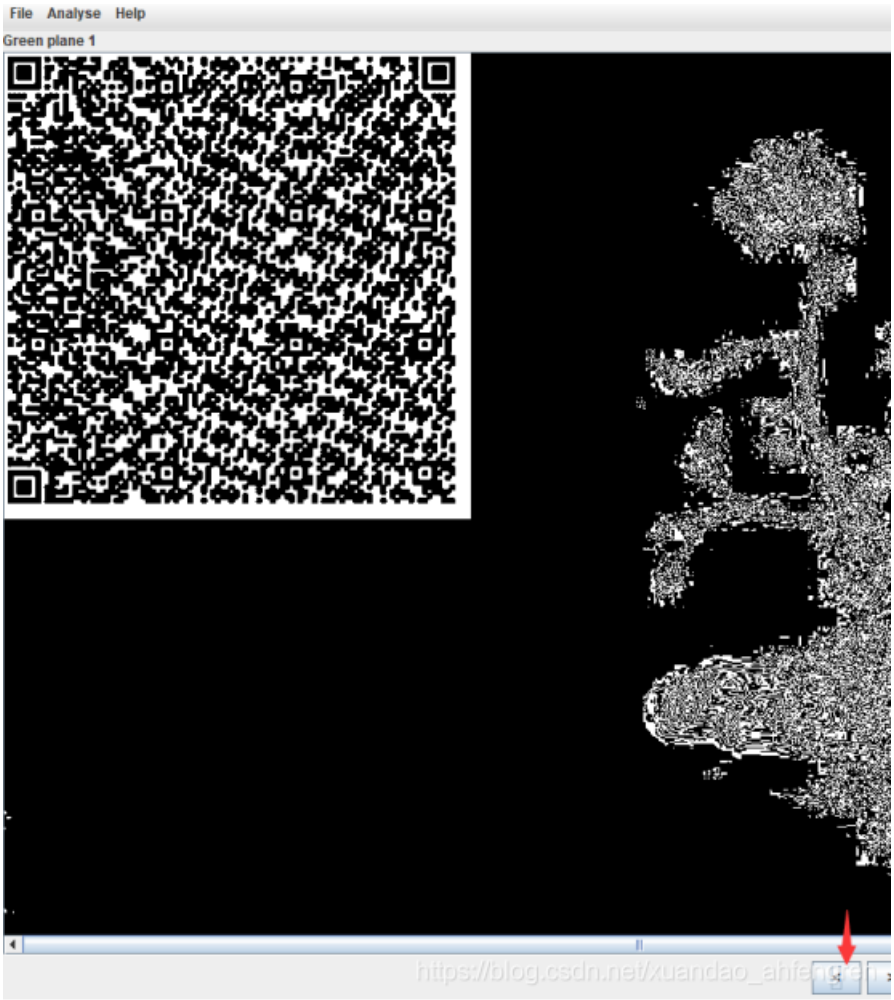
```
安装环境
sudo pip install matplotlib
pip install opencv-python

然后安装解密脚本
git clone https://github.com/chishaxie/BlindWaterMark

解密操作：
python bwm.py decode day1.png day2.png flag.png
```



适合作为桌面

用Stegsolve打开左右调节即可出现二维码

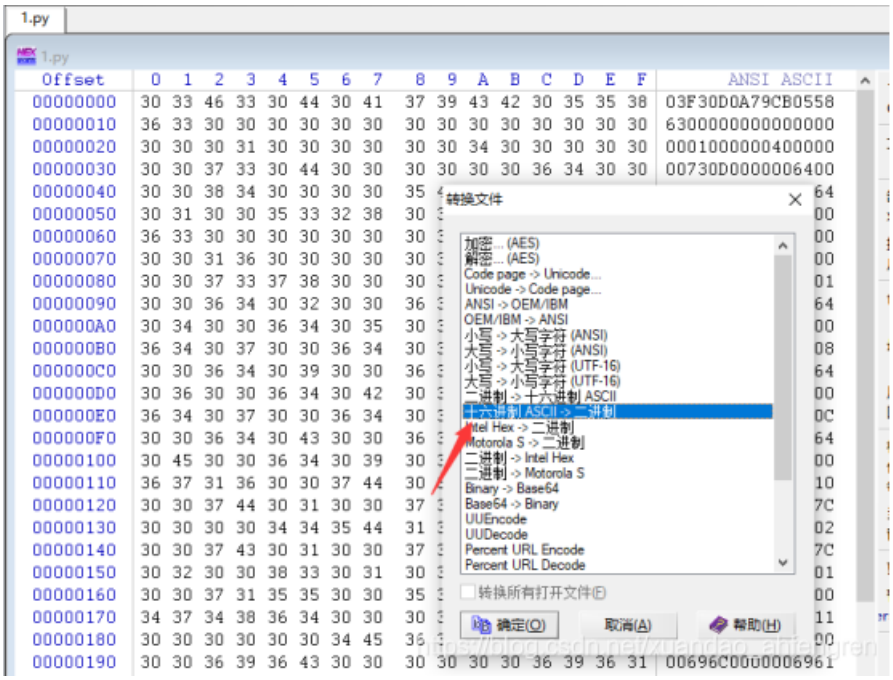
再放在QR上面扫描二维码出现疑似十六进制的内容



内容:

```
03F30D0A79CB055863000000000000000001000000400000000730D0000006400008400
005A000064010053280200000063000000000300000016000000430000007378000000640
0100640200640300640400640500640600640700640300640800640900640A00640600640
0B00640A00640700640800640C00640C00640D00640E00640900640F006716007D0000
6410007D0100781E007C0000445D16007D02007C01007400007C0200830100377D0100
715500577C0100474864000053281100000004E696600000096C0000006961000000696
7000000697B000000693300000069380000006935000000693700000069300000006932C
0000069340000006931000000696500000697D000000740000000028010000007403000
0006368722803000000740300000073747274040000006660C6167740100000069280000C
0002800000000730400000031 2E70795203000000010000007 30A000000000148010601
0D0114014E2801000000520300000028000000002800000000280000000073040000003
```

我们放在winhex里面，按Ctrl+r，转换成二进制，然后保存位1.pyc进行反编译python文件

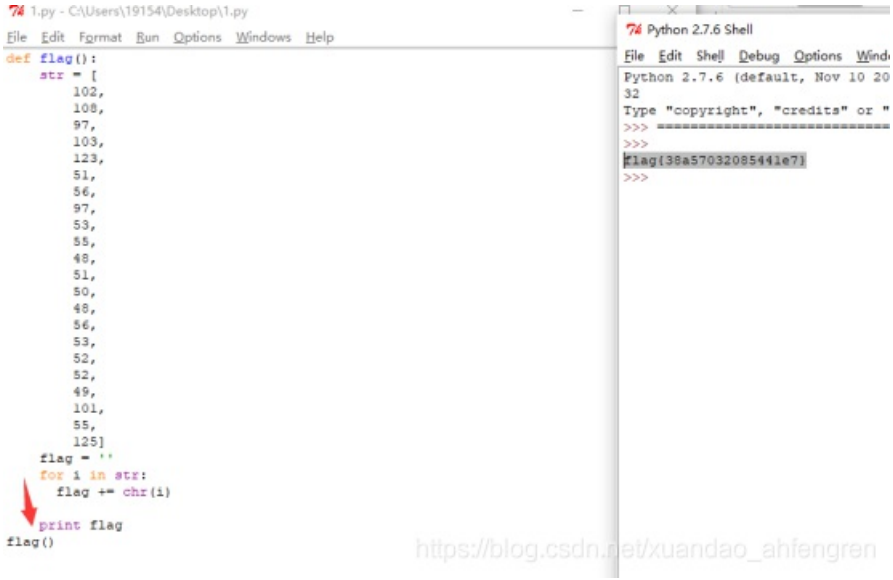


请选择pyc文件进行解密。支持所有Pyt

浏览... 未选择文件。

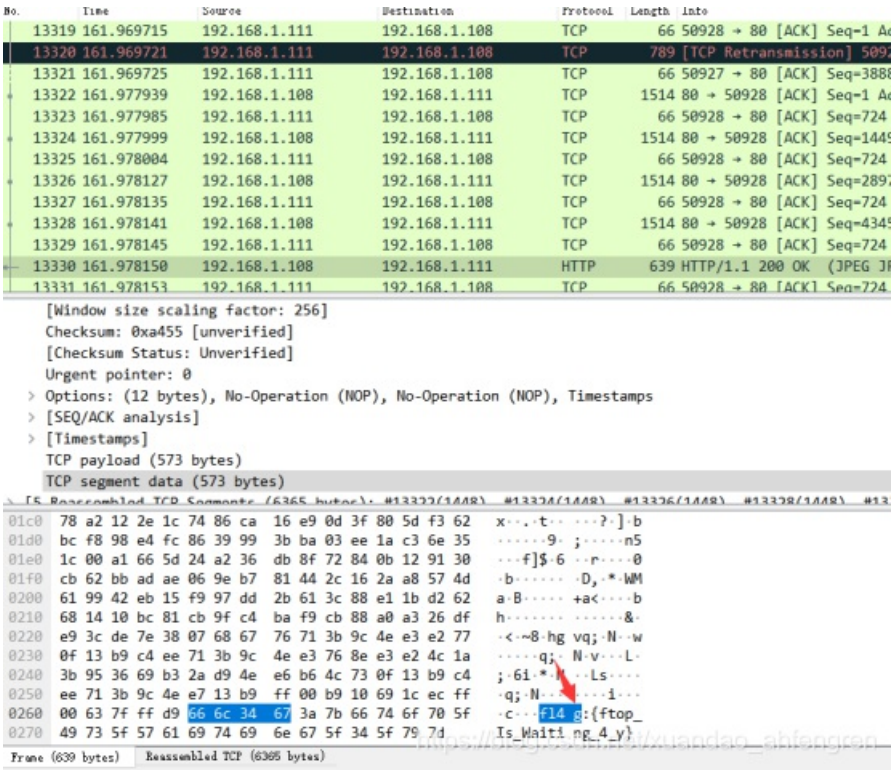
```
#!/usr/bin/env python
# encoding: utf-8
# 如果觉得不错，可以推荐给你
def flag():
    str = [
        102,
        108,
        97,
        103,
        123,
        51,
        56,
        97,
```

加多一个flag()即可运行得到flag



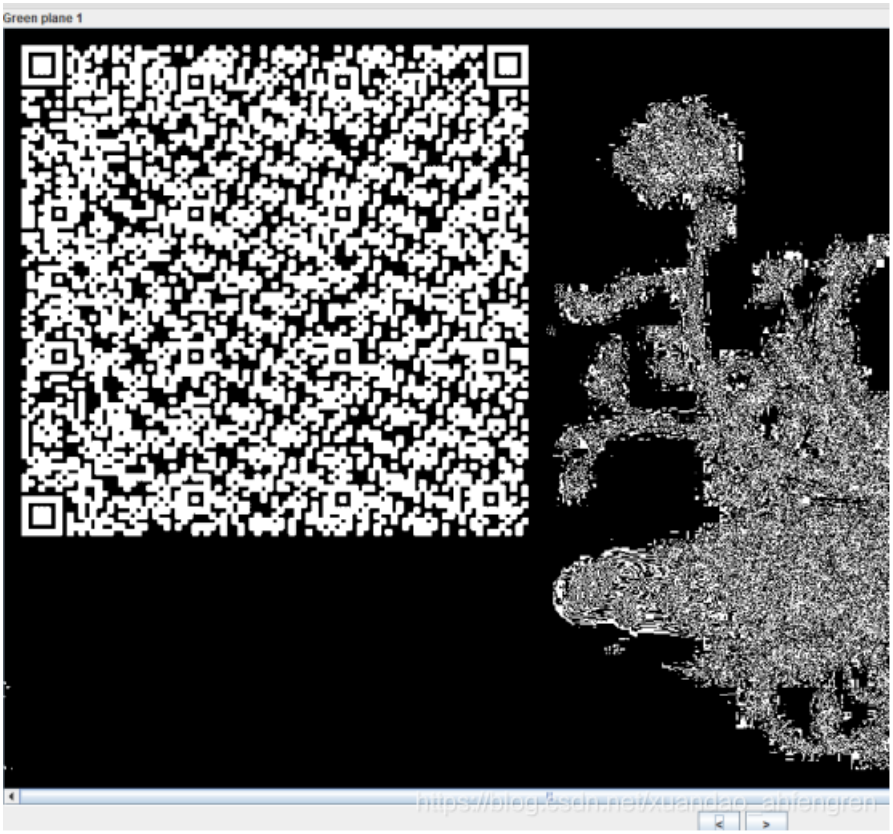
心仪的公司

在tcp流中发现fl4g



stage1

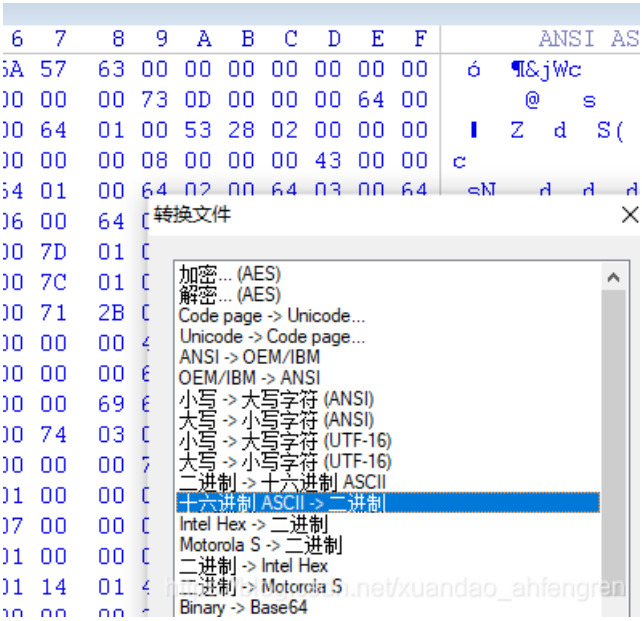
放进Stegsolve里左右调整



保存再放在RQ分析二维码，然后放进winhex转换为二进制，保存为pyc进行反编译python文件后运行即可

版本: 18
纠错等级:L, 掩码:3
内容:

```
03F30D0AB6266A576300000000000000000010000004000000730D0000006400008400
005A000064010053280200000063000000003000000080000004300000073 4E0000006
401006402006403006404006405006406006405006407006708007D00006408007D0100
781E007C0000445D16007D02007C01007400007C0200830100377D0100712B00577C0
1004748640000532809000000 4E6941000000696C000006970000000696800000069 61
000000694C000000696200000074000000002801000000740300000063687228030000
74030000007374727404000000666C6167740100000069280000000028000000007307 0
0000746573742E707952030000000
```




```
def flag():
    str = [
        65,
        108,
        112,
        104,
        97,
        76,
        97,
        98]
    flag = ''
    for i in str:
        flag += chr(i)

    print flag
flag()
```

```
Python 2.7.6 Shell
File Edit Shell Debug Option
Python 2.7.6 (default, Nov
32
Type "copyright", "credits
>>> ======================
>>>
AlphaLab
>>>
```

Easycap

打开数据包，追踪tcp流即可

双色块

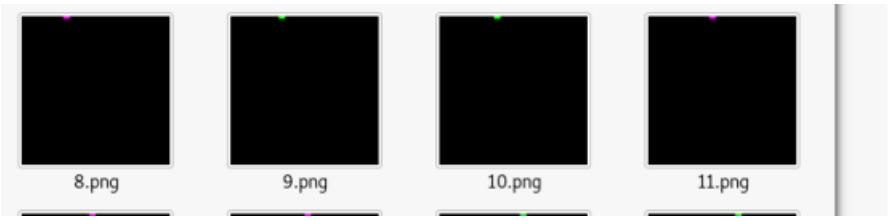
binwalk分析发现尾部有png，用foremost分离出来

拿出来是□个密码

gif轮播之后发现是□个24*24的像素点，每个像素为1*0，每个点颜□为00ff00或是ff00ff 先把gif分离成单帧

```
#! /usr/bin/env python2
# -*- coding: utf-8 -*-

import os
from PIL import Image

def main(gif_file):
    png_dir = 'frame/'
    img = Image.open(gif_file)
    while True:
        current = img.tell()
        img.save(png_dir + str(current + 1) + '.png')
        img.seek(current + 1)
if __name__ == '__main__':
    gif_file = 'out.gif'
main(gif_file)
```

会出先很多图片



然后读取每个png中的对应点的信息，并按照8bit转换为ascii

```
#! /usr/bin/env python2
# -*- coding: utf-8 -*-

import os
from PIL import Image

def main():
    png_dir = 'frame/'
    ret = ""
    for i in range(0,24):
        line = ""
        for j in range(0,24):
            file_name = "frame/" + str(i * 24 + j + 1) + ".png"
            x = j * 10 + 5
            y = i * 10 + 5
            img = Image.open(file_name)
            img = img.convert("RGB")
            img_array = img.load()
            r, g, b = p = img_array[x, y]
            if g == 255:
                line += "0"
            if r == 255 and b == 255:
                line += "1"
            if len(line) == 8:
                ret += chr(int(line, 2))
                line = ""
    print ret
if __name__ == '__main__':
main()
```

两个等会后面的hhh去除掉然后进□DES解密即可得到flag

```
root@kali:~# python 1.py
o8DlxK+H8wsiXe/ERFpAMaBPiIcj1sHyGOMmQDkK+uXsVZgre5DSXw==hhhhhhhhhhhhhhhh
```

很普通的数独

将有数字的格子写成0，没有的写成1

```
11111110101010100010100000111111000010111111
10000010110011110101001110110001100100 1000001
10111010111001111101001111110100010100 1011101
10111010110110001000101000001111000110101 1101
10111010001110010000111110111111101110101 1101
10000010110010000001100010000111010000 1000001
11111110101010101010101010101010111011111111
00000000001100110100100011010011001110000 0000
11001110010010000111111111001001010000001011 11
10100100101111111111011101010111101011010011 00
10000011110010010000011000110100110101000 1010
00110001001101000101001100010000001011001 0000
01011010101000111111010001110100111010110 1111
10001100010001110011101110110110010101101110001
00110011010000000001001000011110010110101 1010
10100000101101011111001101111111010011101 00011
11011111011101100110110001010000111000010 0000
11010100001010100001110110110111010110100 1100
01001111111000101111101000100001101110110 1100
01100101100101010110001111010100110000101 0010
01011111111111010111111111101101101111111111 1100
01111000110000010000100010100010010010001 1110
11111010111001110011101011010011010010101 0010
11001000101110101110100011110000001110001 0000
10101111101110011110111111110000101011111 0010
11010001100011100010011110110111110100010 0010
11110111111000100100001101011000111111011 1110
01100101010100011001010001000100010110101 0001
01110111010110110110010000110110100011110 1001
11011000100110110001010110111111010010110 0110
00001110011100000000010000101010111110001 0010
11101001001111001110111001010000101111101 0010
10100110001011111111010000010000101010101 0100
00001001100100110111010100111110010111110 1101
00001011110111000110101100000100010111010 0110
01111001101010001010000001101100000111001 0000
10011010010000110111111111011001011101111 0011
00000000111111010110100010101110010010001 1010
11111110001111101101101010110111001110101 1110
10000010111010110110100011111001000110001 0001
10111010101110000111111111011010010001111 1011
10111010011011111011010000010011011000111 0110
10111010000001110110000110101011001001001 0001
10000010101100101111101100101100001101011 0000
11111110101010100111101111010110111000010 1101
```

然后使用python写个脚本来生成图片。

```
from PIL import Image
x = 45
y = 45
im = Image.new('RGB', (x, y))
white = (255, 255, 255)
black = (0, 0, 0)
with open('ss.txt') as f:
    for i in range(x):
        ff = f.readline()
        for j in range(y):
            if ff[j] == '1':
                im.putpixel((i, j), black)
            else:
                im.putpixel((i, j), white)
im.show()
```

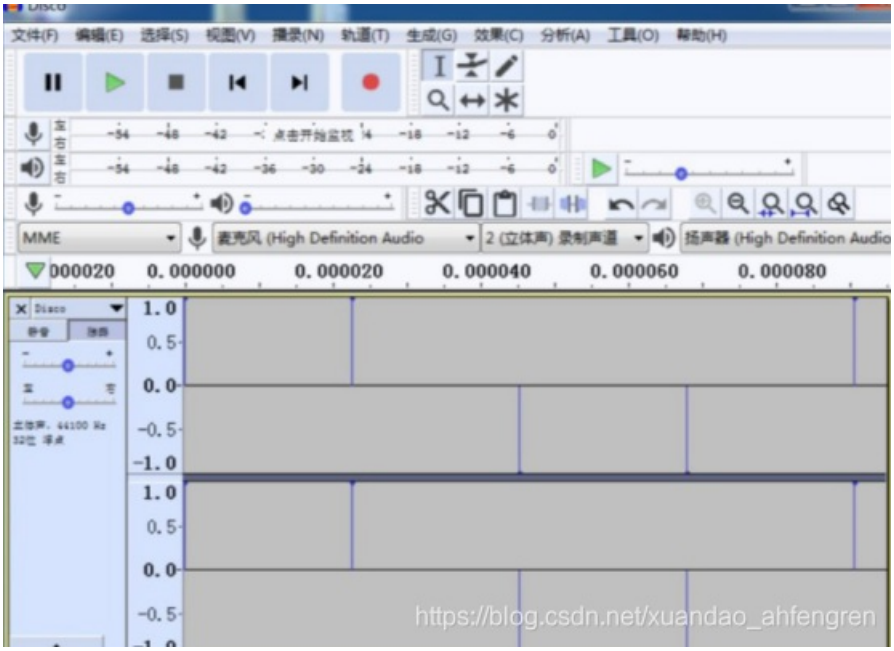
扫出来是：

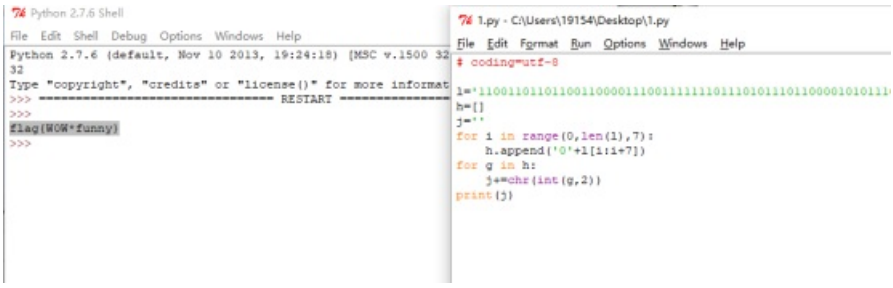
Vm0xd1NtUXlWa1pPVldoVFlUSlNjRlJVVGtOamJGWnlWMjFHVlUxV1ZqTldNakZIWVcxS1IxTnNhRmhoTVZweV

是多个base64加密的，解密出来是flag{y0ud1any1s1}

很普通的Disco

峰值高的点为1，峰值低的点为0。抠出来，是105个二进制数，每7个数为一组，刚好15组，也就是15个字母，最后用python跑出来即可





flag{W0W*funny}

就在其中

打开数据包发现，找到了key

还有一些文件，果断用foremost分离出来

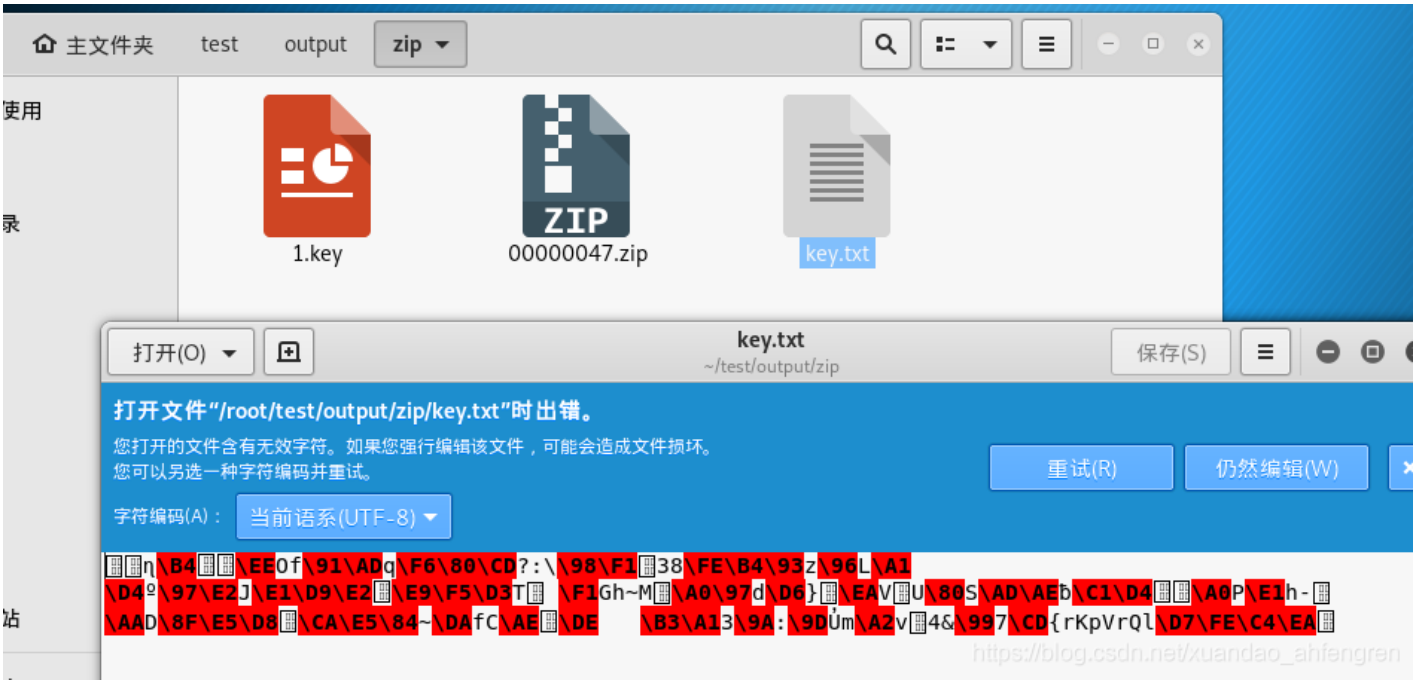
```
Line-based text data (15 lines)
    -----BEGIN RSA PRIVATE KEY-----\n
    MIICXgIBAAKBgQD0UN0A+70iM0VCJ1ni0n/U1BRj0u8yMWH4Qi+xTbjHgbE7wOuk\n
    OaO+2PyQXiqIzZnf5jCkJuVDYjALGcKrZM4OCQBBd85B/LTc36XZ7JVfX5kGy5tI\n
    R3tquuPIVKNdAsH1Sqh9S7YSS39RdnSa5rOUyGhrLzxwzzM9IO4e+QQ+CQIDAQAB\n
    AoGADiaw5mGubtCxbkeBOVYf+V/fXnjVSf76QbrzsD1kOooUjfV6sKR2C5Pd7S7H\n
    H+1owENBBgEKvoBtb/cqA2tvU9vQ415TMBJcHv6LEcb9WPpnMxPV2GNjO+DTPGPy\n
    Xnu1UZlZjwx+NaF5rESoSSVS2ZaaIixBs4RWRXk+1HEbTFECQQD6Rp6jMweRgPHO\n
    pR3mgIK83zL+kzqYM5isIPv3DIC5JQN2kXqK73IDQCFVlfXnr91AAVRzLDsAXLqv\n
    le/o6yQLAkEA+edY+GER1LuD1t2k9Js0Dc7EwnLcxoFUE60ivj8Gf9jzLskGHxsv\n
    0IV6J5OHwPh54kAxAnqCjSqNRAWGNzr+uwJBALYEjDUm1LdGrxXZ0jAkgHC6Z0zs\n
    aK3uwHdXGcinqCp+t9EQpq3KzQF+L4AeKxRQONEq5m9I2LQ/vGocwrmD4dcCQQDb\n
    rTyOinWz8upAFPKOe2hUwvA/pkzgyosoCMhDyI9kD0gmV1vlODbd7Jem9o8dWM97\n
```

```
40  3d 1f 2d 2d 2d 2d 2d 42  45 47 49 4e 20 52 53 41   =-----B EGIN RSA
50  20 50 52 49 56 41 54 45  20 4b 45 59 2d 2d 2d 2d    PRIVATE  KEY----
60  2d 0a 4d 49 49 43 58 67  49 42 41 41 4b 42 67 51   --MIICXg IBAAKBgQ
70  44 30 55 4e 30 41 2b 37  30 69 4d 30 56 43 4a 31   D0UN0A+7 0iM0VCJ1
80  6e 69 30 6e 2f 55 31 42  52 6a 30 75 38 79 4d 57   ni0n/U1B Rj0u8yMW
90  48 34 51 69 2b 78 54 62  6a 48 67 62 45 37 77 4f   H4Qi+xTb jHgbE7wO
a0  75 6b 0a 4f 61 4f 2b 32  50 79 51 58 69 71 49 7a   uk·OaO+2 PyQXiqIz
b0  5a 6e 66 35 6a 43 6b 4a  75 56 44 59 6a 41 4c 47   Znf5jCkJ uVDYjALG
c0  63 4b 72 5a 4d 34 4f 43  51 42 42 64 38 35 42 2f   cKrZM4OC QBBd85B/
d0  4c 54 63 33 36 58 5a 37  4a 56 66 58 35 6b 47 79   LTc36XZ7 JVfX5kGy
e0  35 74 49 0a 52 33 74 71  75 75 50 49 56 4b 4e 64   5tI·R3tq uuPIVKNd
f0  41 73 48 6c 53 71 68 39  53 37 59 53 53 33 39 52   AsH1Sqh9 S7YSS39R
00  64 6e 53 61 35 72 4f 55  79 47 68 72 4c 7a 78 77   dnSa5rOU yGhrLzxw
10  7a 7a 4d 39 49 4f 34 65  2b 51 51 2b 43 51 49 44   zzM9IO4e +QQ+CQID
20  41 51 41 42 0a 41 6f 47  41 44 69 61 77 35 6d 47   AQAB·AoG ADiaw5mG
30  75 62 74 43 78 62 6b 65  42 4f 56 59 66 2b 56 2f   ubtCxbke BOVYf+V/
```

```
s)
    142588562 IDA Pro 6.5 Setup.exe\r\n
          128 key.txt\r\n
```

```
 20 20 31 31 3a 31 35 41    08-09-16   11:15A
 20 20 20 20 20 20 20 20    M
 65 79 2e 74 78 74 0d 0a       128 k ey.txt··
 20 20 31 31 3a 32 39 41    08-10-16   11:29A
```

有个压缩包，里面的key.txt文件被加密过了，我们有密码就可以直接解密



openssl rsautl -decrypt -in key.txt -inkey 1.key -out flag.txt

in为要解密的加密文档-inkey为密钥-out为输出文档

```
hi, boys and girls! flag is {haPPy_Use_0penSsI}
```

再见李华

用winhex打开看到key.txt，把后缀改成zip

```
14 00 01 ▌- ▌[»¹yUPK
00 00 1A    íi I  q %
74 1F B8        key.txt ¸
```

打开需要密码。

没有特殊字符，是指密码中没有特殊字符。而不少于1000个字，这个1000是8的二进制，所以密码是9位或9位以上，最后署名，意思是密码中后面5位数是Lihua，最后用Advanced ZIP Password Recovery_4.0进行破解。最后密码为15CCLiHua

```
import string
from hashlib import md5
a = string.ascii_letters + string.digits

for a1 in a:
    for a2 in a:
        for a3 in a:
            for a4 in a:
                if '1a4fb3fb5ee' in md5(bytes(a1 + a2 + a3 + a4 + 'LiHua').encode('ascii')).hexdigest():
                    print a1+ a2 + a3 + a4 + 'LiHua'
                    break
```

```
port string
om hashlib import md5
= string.ascii_letters + string.digits

r a1 in a:
  for a2 in a:
      for a3 in a:
          for a4 in a:
              if '1a4fb3fb5ee' in md5(bytes(a1 + a2 + a3 + a4 + 'LiHua').
                  print a1+ a2 + a3 + a4 + 'LiHua'
                  break
```

```
Python 2.7.6 Shell
File  Edit  Shell  Debug  Options  Windows  Help
Python 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (I
32
Type "copyright", "credits" or "license()" for more information.
>>> ========== RESTART ==========
>>>
15CCLiHua
>>>
```


肥宅快乐题

打通关后获取base64加密后的falg，解密即可

warmup

先将 open_forum.png 压缩为 open_forum.zip，然后明文破解

python bwm.py encode fuli.png fuli2.png res.png

flag{bWm_Are_W0nderfu1}