

# 攻防世界-杂项-Misc

转载

[weixin\\_30551963](#) 于 2019-08-07 15:41:00 发布 258 收藏 1  
原文链接: <http://www.cnblogs.com/yichen115/p/11315696.html>  
版权

长期更新一波 攻防世界 的杂项题解

这东西主要靠积累吧

攻防世界: <https://adworld.xctf.org.cn>

新手练习区

## 1、this\_is\_flag

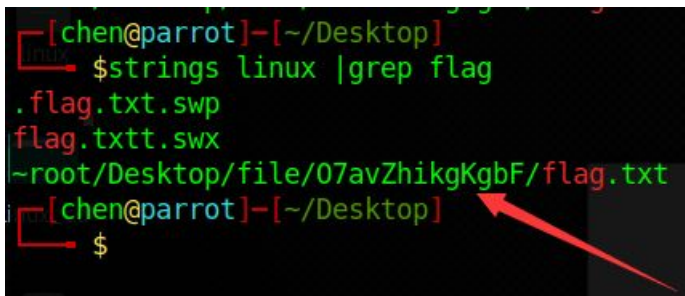
题目直接给出了 flag

## 2、ext3

主要考察 linux 下光盘的挂载

strings 文件名 | grep flag

搜索文件中的可打印字符 grep: 全面搜索正则表达式并把行打印出来



```
[chen@parrot]-[~/Desktop]
└─$ strings linux | grep flag
.flag.txt.swp
flag.txtt.swx
~root/Desktop/file/07avZhikgKgbF/flag.txt
[chen@parrot]-[~/Desktop]
└─$
```

使用命令: mount linux ./linux\_cd

将 linux(文件名) 挂载到 linux\_cd 目录下, 正常访问 O7avZhikgKgbF 文件夹即可看到 flag 文件, 再经过 base64 解码得到最终 flag

### 3、give\_you\_flag



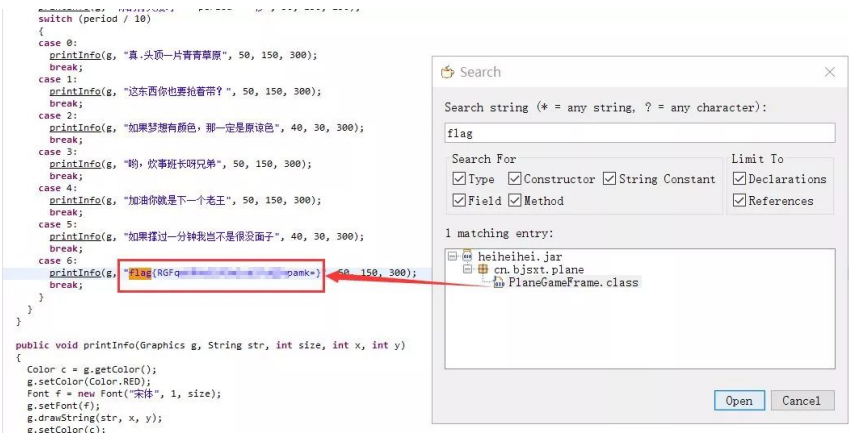
动态图，一帧一帧看（我用的是爱奇艺万能播放器），在第50帧有个二维码，但是少了三个定位图案，用 PS 补上，扫码得到 flag

### 4、pdf

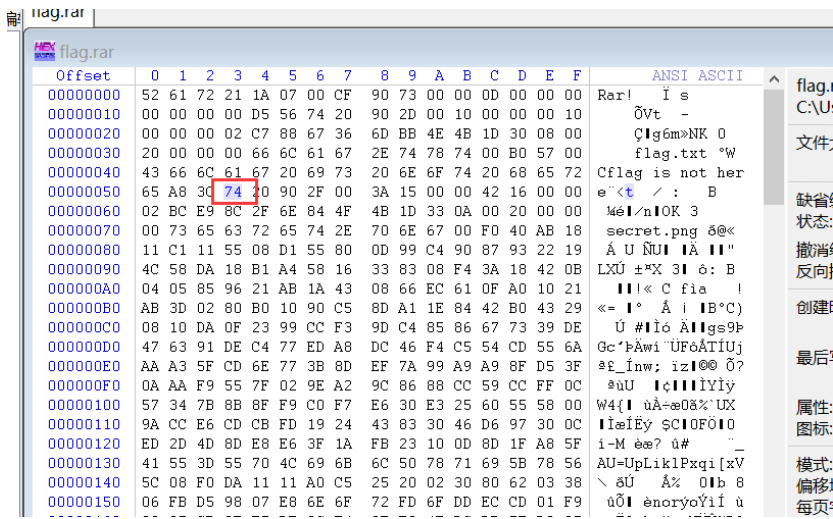
下载下来直接把编辑 PDF，把图片拿开就可以看到 flag

### 5、坚持60s

一个 java 小游戏，用 **jd-gui** 打开，直接搜索：flag，得到，结果需要 base64 解码

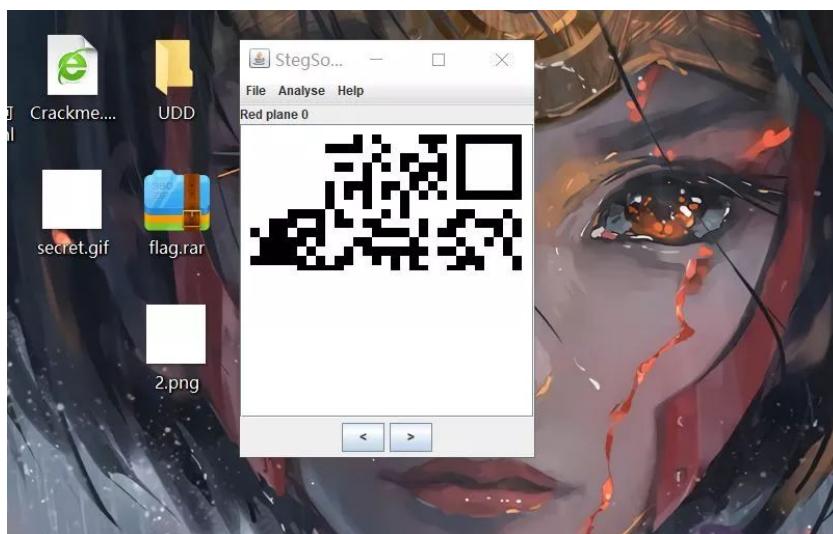
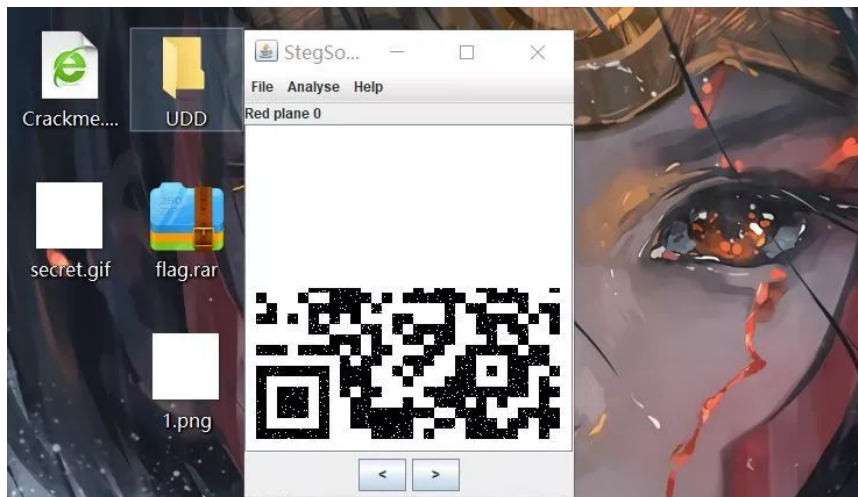






再打开就看到了 png 文件，winhex 发现其实是个 gif 将后缀改成 gif

分离出来（我用的是 PS），然后用 Stegsolve 查看



把这个二维码拼起来，再把定位标志补上扫码得到 flag

## 9、掀桌子

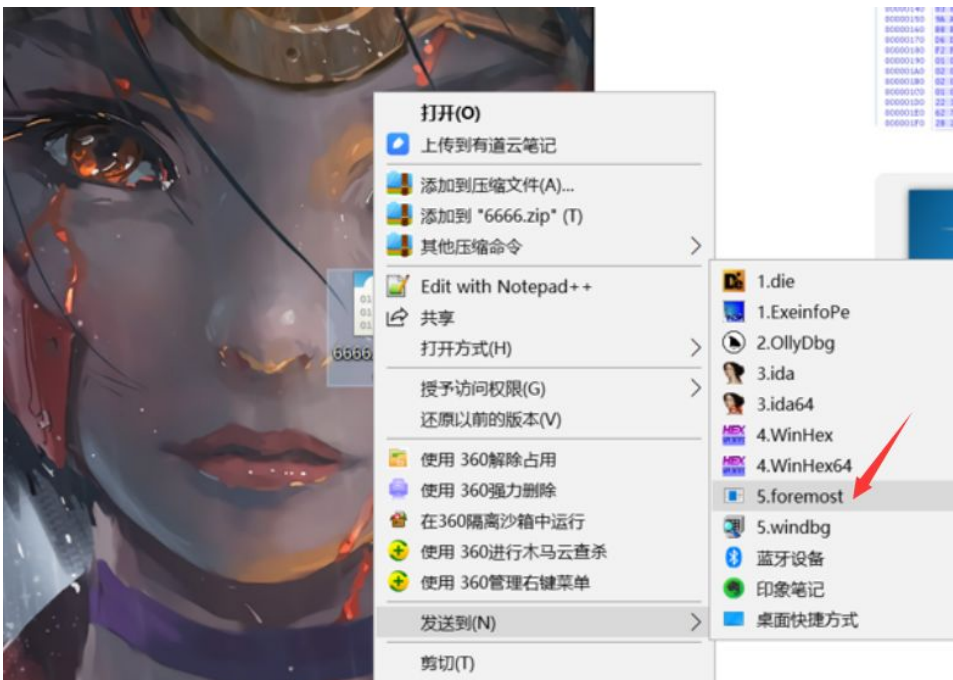
网上师傅们给出的解密代码

```
string =  
"c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9e  
af3e2e4e6f2"  
flag = ''  
for i in range(0,len(string), 2):  
    s = "0x" + string[i] + string[i+1]  
    flag += chr(int(s, 16) - 128)  
print(flag)
```

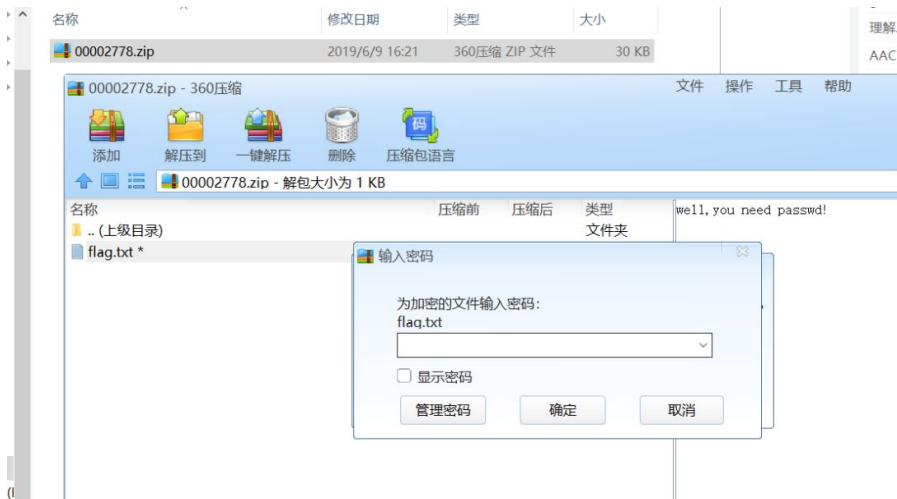
每两个一组，将16进制转换为10进制，减去128以后输出 ascii

## 10、功夫再高也怕菜刀

下载到一个流量包，有 foremost 分离一下

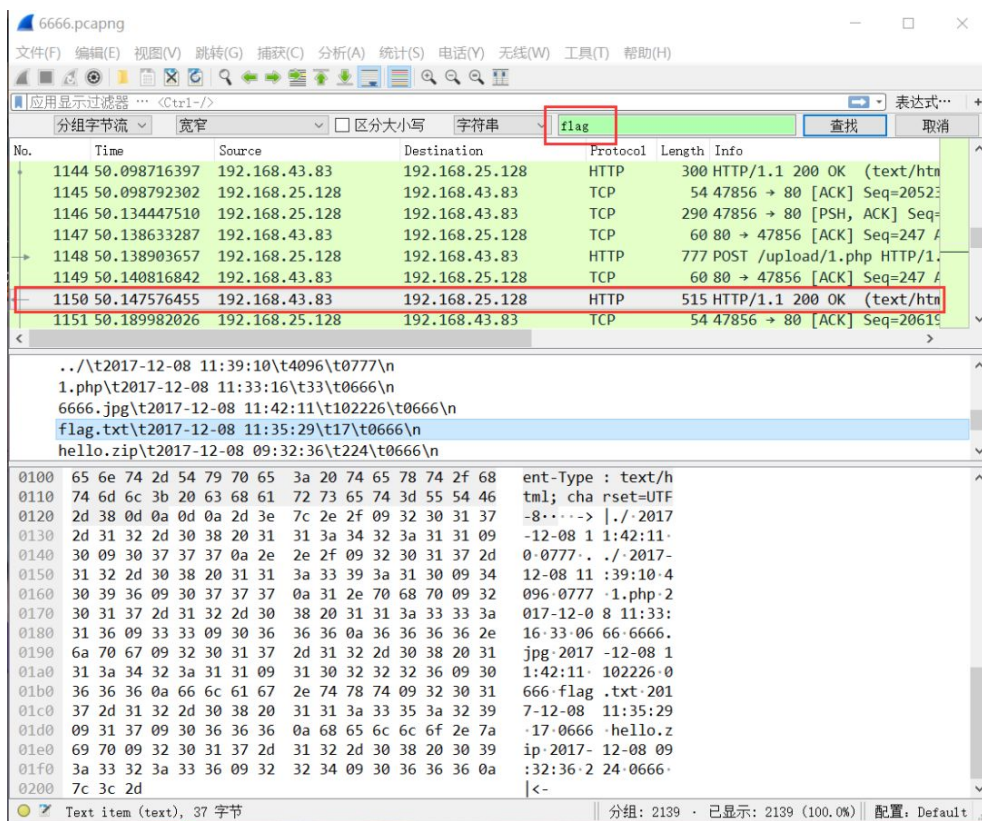


得到一个压缩包，里面有 flag 文件，爆破就别想了（太复杂），



分析流量包！！

ctrl+F 搜索字符



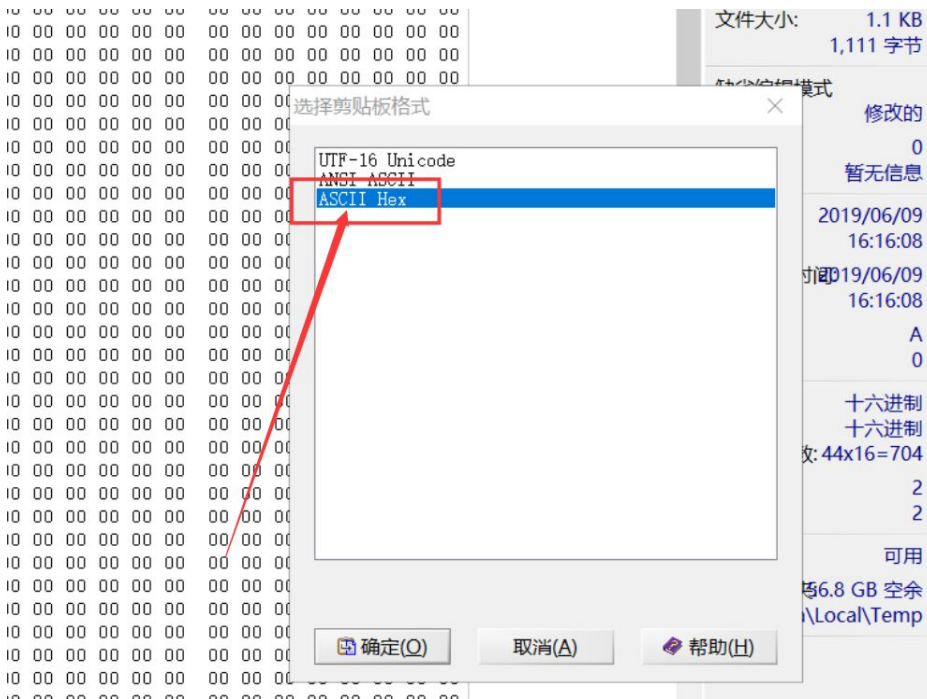
选择第1150个，右键，追踪流 -> TCP 流

把这些保存下来



```
AC4F3E7CDDC9BD48DADB41C016E521B39C094801447E38D0DE480FF0099F5747B9
0B4EB1E6EABFF0060E7FE42BCCAD75A76F2B6B74AE97CB4E8BDD4EE9352F630E9
FBD05FE4CF2D79723EF48D93930C648EBC608CE0935893BE771399079983839FB
F005E32FF0027ACA3D6D3FEB85CFF00296BC6ACF5F9A5F7FB3FFE4FE6959FC53E
C8BA9000DB89705BF798CE679C1F96043FF3CE3EA5BA7191FC158B70E4F98643B
EA83A72FDFB3FF7DFFF0066AC83D2D3FEBEA4FF00D0C578F8896CBBC53FBD5376
5F0E96DBDD690465CEF8326FE08C7DA197A20E365B47D831C00DE9DF201CE3DC
DD83CEEAD297FD5A7FD7F37F4AC8B8E92FF00D7E8FE46BC5AD276BFCFEFF7B57F
6693E6C9BA90E580C21D9866FF009F780F1B467A4926E00FF176E0B3118731C7C
0480356EFEEDCFF00D7D27F37ACAD47A5FF00FBF07F235E3577A7AB7F85FF001F
6D39FEE56FB526F0EE1CB30D9F28018C00E3F751F57B8931FF002D1B191E99E32
2E7B8183F2F37EE7EFDCCFFD7383F9C758F77D65FF00AF78FF00F408EBC6C4DD4A
DD41EBD5FC7AF7F7BAC9B59E658327293B9CF2E1BEF7FB5FF02EBF8D15763FF57
E9E65DA5FF81BFF002F5FE96BFFD9HTTP/1.1 200 OK
10 Date: Fri, 08 Dec 2017 11:42:07 GMT
11 Server: Apache/2.4.23 (Win64) PHP/5.6.25
12 X-Powered-By: PHP/5.6.25
13 Content-Length: 7
```

打开 winhex 新建一个文件，把上面的粘贴进去，注意，选择 hex



可以看出是个 jpg 了



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	78	y0ya JFIF x
00000010	00	78	00	00	FF	DB	00	43	00	01	01	01	01	01	01	01	x yÜ C
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000040	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000050	01	01	01	01	01	01	01	01	FF	DB	00	43	01	01	01	01	yÜ C
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000070	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000080	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000090	01	01	01	01	01	01	01	01	01	01	01	01	01	01	FF	C0	yÄ
000000A0	00	11	08	01	39	01	E2	03	01	22	00	02	11	01	03	11	g ä "
000000B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	yÄ
000000C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	
000000D0	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	yÄ µ
000000E0	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21	} !
000000F0	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23	1A Qa "q 2 'i #
00000100	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	B±Ä Rñ\$3br!
00000110	18	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	%&'()*456789:
00000120	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	CDEFGHIJSTUVWXYZ
00000130	63	64	65	66	67	68	69	6A	73	74	75	76	77	78	79	7A	cdefghijstuvwxyz
00000140	83	84	85	86	87	88	89	8A	92	93	94	95	96	97	98	99	!!!!!!'!!!!!!
00000150	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	!çèé!\$@*~µñ.
00000160	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	.'9AAAAÇEE0000
00000170	D6	D7	D8	D9	DA	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	F1	Ö×@Uuääääæçèéêë
00000180	F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4	00	1F	01	00	03	ööööö+öüüyÄ
00000190	01	01	01	01	01	01	01	01	01	00	00	00	00	00	00	01	
000001A0	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	11	00	yÄ µ
000001B0	02	01	02	04	04	03	04	07	05	04	04	00	01	02	77	00	w
000001C0	01	02	03	11	04	05	21	31	06	12	41	51	07	61	71	13	! ! A0 aq
000001D0	22	32	81	08	14	42	91	A1	B1	C1	09	23	33	52	F0	15	"2 B'!±Ä #3R\$
000001E0	62	72	D1	0A	16	24	34	E1	25	F1	17	18	19	1A	26	27	brÑ \$4&%& &!
000001F0	28	29	2A	35	36	37	38	39	3A	43	44	45	46	47	48	49	()*56789:CDEFGHI

未命名  
未命名

文件大小: 101 KB  
103,337 字节

缺省编辑模式  
状态: 修改的

撤销级数: 1  
反向撤销: 数据粘贴

创建时间: 2019/06/09  
16:16:08

最后写入时间: 2019/06/09  
16:16:08

属性: A  
图标: 0

模式: 十六进制  
偏移地址: 十六进制  
每页字节数: 44x16=704

当前窗口: 2  
窗口总数: 2

剪贴板: 可用  
暂存文件: 6.8 GB 空余  
S:\AppData\Local\Temp

保存后打开图片:



用这个密码打开压缩包里的 flag.txt

### 11、stegano

下载 PDF 在火狐浏览器打开，控制台输入：

```
document.documentElement.textContent
```

看一下内容，会有一串

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA AB BBB BA AAAB AB BBB  
AAAAA AB BBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB



```

#coding=utf-8
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res

def solve_stego():
    with open('1.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)

def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str

if __name__ == '__main__':
    solve_stego()

```

## 高手进阶区

### 1、Excaliflag

使用 Stegsolve 在蓝色通道为0的时候发现 flag

### 2、签到题

base64 -> 凯撒 -> 栅栏

注意根据题目背景，是SSCTF，凯撒的时候看到 ssC 选择那一个进行栅栏

未完待续...



转载于:<https://www.cnblogs.com/yichen115/p/11315696.html>