BUUCTF-Misc-No.4

原创

水星Sur 于 2020-05-16 23:43:38 发布 1820 收藏 7

分类专栏： BUUCTF Misc 文章标签： python 加密解密 信息安全

本文链接：https://blog.csdn.net/pone2233/article/details/106167361

BUUCTF 同时被 2 个专栏收录

21 篇文章 2 订阅

订阅专栏

Misc

22 篇文章 0 订阅

订阅专栏

文章目录

比赛信息

内心os（蛮重要的）

- 被偷走的文件 | SOLVED |
- [GXYCTF2019]佛系青年 | SOLVED |
- 秘密文件 | SOLVED |
- [BJDCTF 2nd]TARGZ-y1ng | SOLVED |
- [BJDCTF2020]认真你就输了 | SOLVED |
- [BJDCTF2020]just_a_rar | SOLVED |
- [BJDCTF2020]你猜我是个啥 | SOLVED |
- 寂静之城 | SOLVED |
- 间谍启示录 | SOLVED |
- [GXYCTF2019]gakki | SOLVED |
- 黑客帝国 | SOLVED |
- [安洵杯 2019]吹着贝斯扫二维码 | SOLVED |
- [GXYCTF2019]SXMgdGhpcyBiYXNlPw== | SOLVED |
- [SUCTF 2019]Game | SOLVED |
- 小易的U盘 | SOLVED |
- [GUET-CTF2019]KO | SOLVED |
- [HBNIS2018]caesar | SOLVED |
- [ACTF新生赛2020]base64隐写 | SOLVED |
- [SWPU2019]Network | SOLVED |
- [GUET-CTF2019]zips | SOLVED |
- [HBNIS2018]低个头 | SOLVED |
- 百里挑一 | SOLVED |
- [RCTF2019]draw | SOLVED |
- [WUSTCTF2020]find_me | SOLVED |
- 我吃三明治 | SOLVED |
- sqltest | SOLVED |
- 弱口令 | SOLVED |
- 真的很杂 | SOLVED |
- [V&N2020 公开赛]拉胯的三条命令 | SOLVED |
- USB | SOLVED |
- 蜘蛛侠呀 | SOLVED |
- [安洵杯 2019]Attack | SOLVED |
- [ACTF新生赛2020]NTFS数据流 | SOLVED |
- [ACTF新生赛2020]swp | SOLVED |
- [安洵杯 2019]easy misc | SOLVED |
- [XMAN2018排位赛]通行证 | SOLVED |
- hashcat | SOLVED |
- Business Planning Group | SOLVED |

比赛信息

比赛地址：Buuctf靶场

内心os（蛮重要的）

我只想出手把手教程，希望大家能学会然后自己也成为ctf大佬，再来带带我QWQ

被偷走的文件 | SOLVED |

foremost分离一下

文件，发现有rar用软件跑一下有了密码


```
flag{6fe99a5d03fb01f833ec3caa80358fa3}
```

[GXYCTF2019]佛系青年 | SOLVED |

下载文件，发现有一个没加密和加密文件，发现它是伪加密

图片已做防盗链处理
请在原文件中访问该图片

图片已做防盗链处理
请在原文件中访问该图片

2处不一样，然后修改成00，就可以解压了

发现

这个图片其实是jpg，然后发现没有用，然后打开txt看到佛曰


```
flag{w0_fo_ci_Be1}
```

秘密文件 | SOLVED |

foremost，分离一下发现有rar

然后软件找密码

就有了flag

```
flag{d72e5a671aa50fa5f400e5d10eedeaa5}
```

[BJDCTF 2nd]TARGZ-y1ng | SOLVED |

他说不用爆破，我觉得是很简单密码，然后试一下他的用户名，然后成了，反复多次发现是套娃，上网找脚本

```
#Python3.7大佬超级好用的脚本
import zipfile
name = 'hW1ES89jF'
while True:
    fz = zipfile.ZipFile(name + '.tar.gz', 'r')
    fz.extractall(pwd=bytes(name, 'utf-8'))
    name = fz.filelist[0].filename[0:9]
    fz.close()
```

方便的不行

```
BJD{wow_you_can_rea11y_dance}
```

[BJDCTF2020]认真你就输了 | SOLVED |

发现文件里面既然有txt文件，然后该一个后缀zip，进入路径找到了flag


```
flag{M9eVfi2Pcs#}
```

[BJDCTF2020]just_a_rar | SOLVED |

解压文件，发现有密码

跑一下得到密码解压图片


```
flag{Wadf_123}
```

[BJDCTF2020]你猜我是个啥 | SOLVED |

发现我png格式改后缀名，在winhex最后发现了flag

```
flag{i_am_fl@g}
```

寂静之城 | SOLVED |

看来半天没找到，最后在点赞中找到了出题人


```
http://blog.sina.com.cn/s/blog_bb4702370102w4oa.html
```

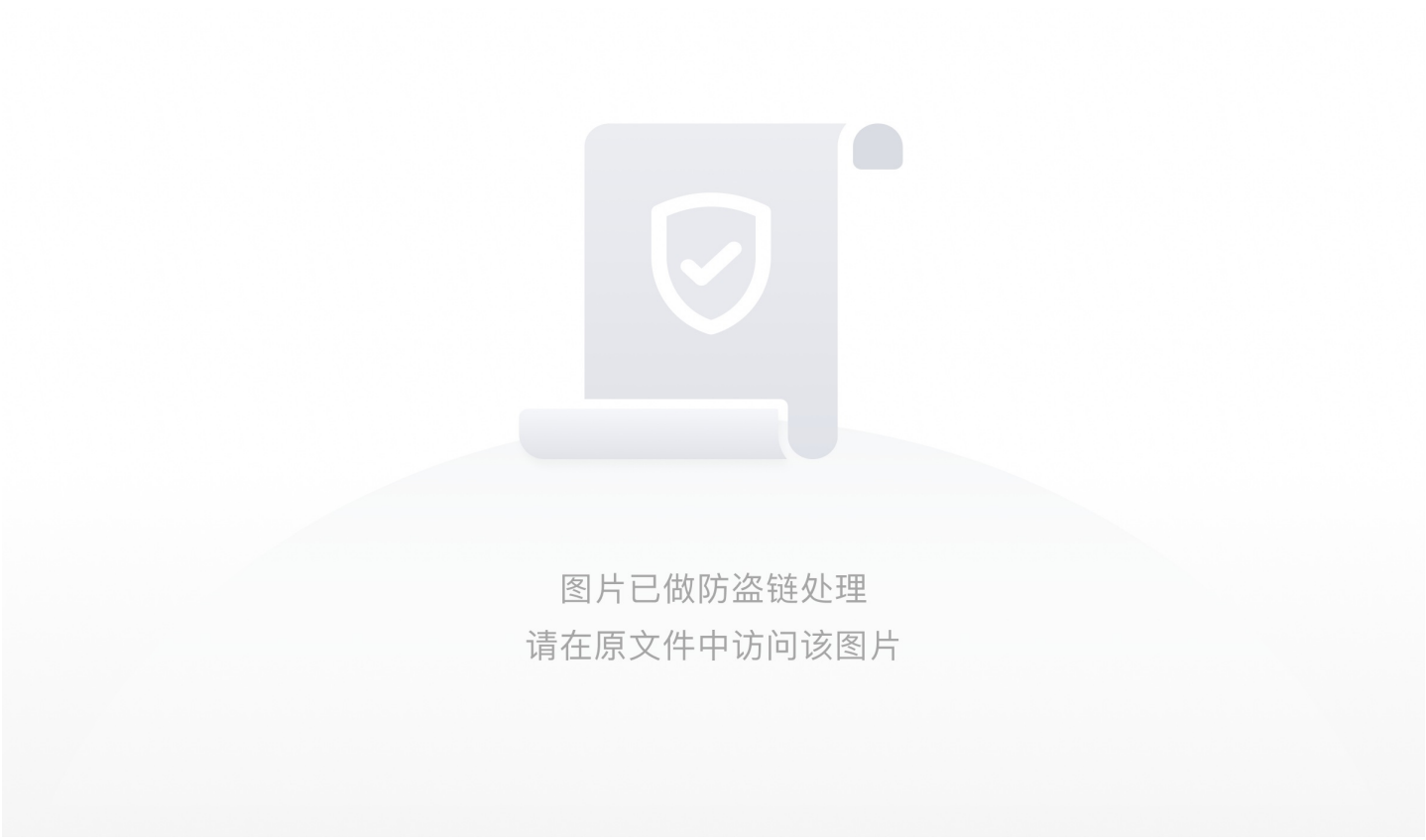
很大脑洞的题目由于有些账号被封禁

```
flag{3101041992083148136354202112 7}
```

间谍启示录 | SOLVED |

ios 使用fore分离

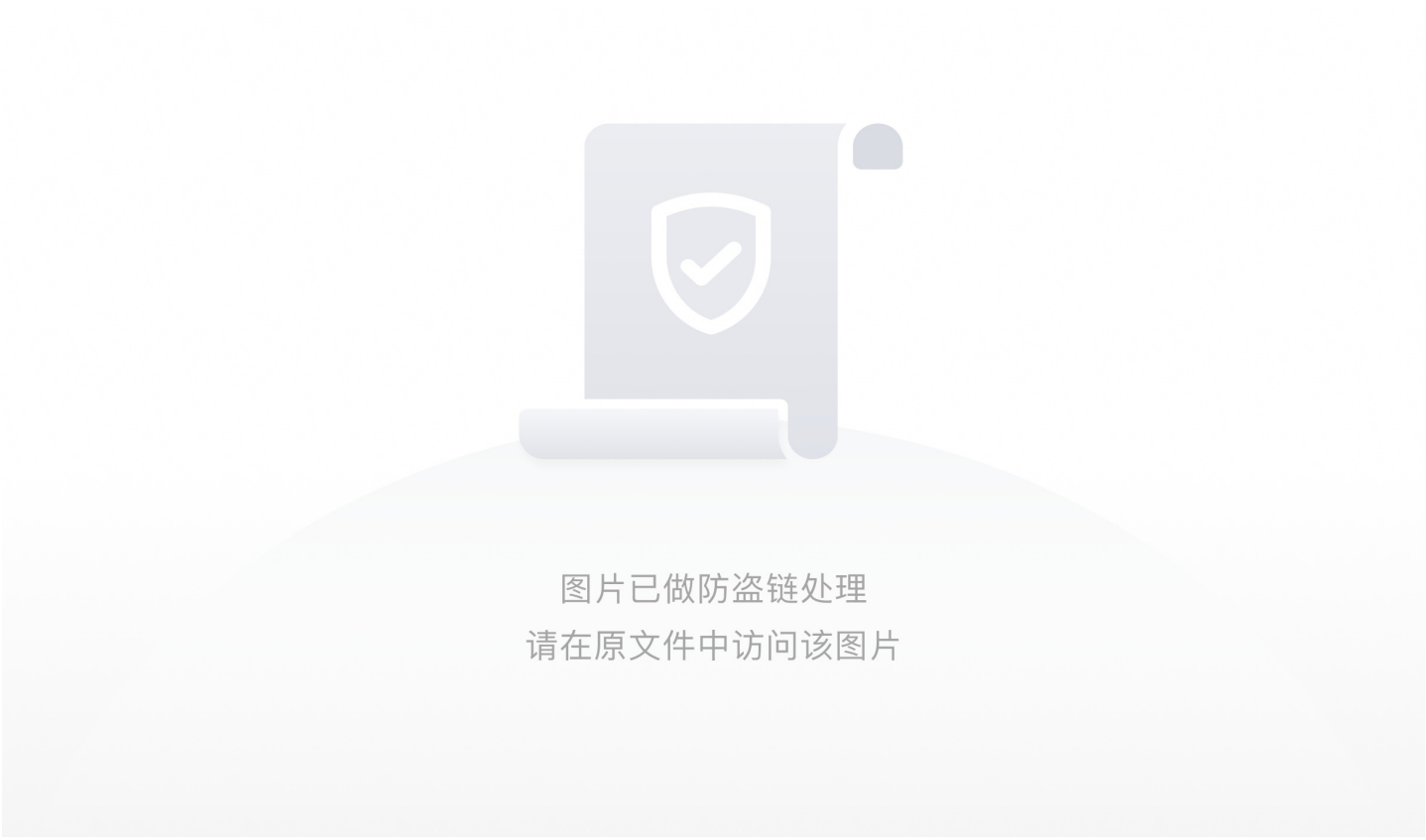
得到4个东西 进入rar，打开压缩包运行flag.exe就生成了一个flag




```
Flag{379:7b758:g7dfe7f19:9464f:4g9231}
```

[GXYCTF2019]gakki | SOLVED |

首先解压文件，发现是图片，使用fore分离得到了rar



用破解密码软件跑

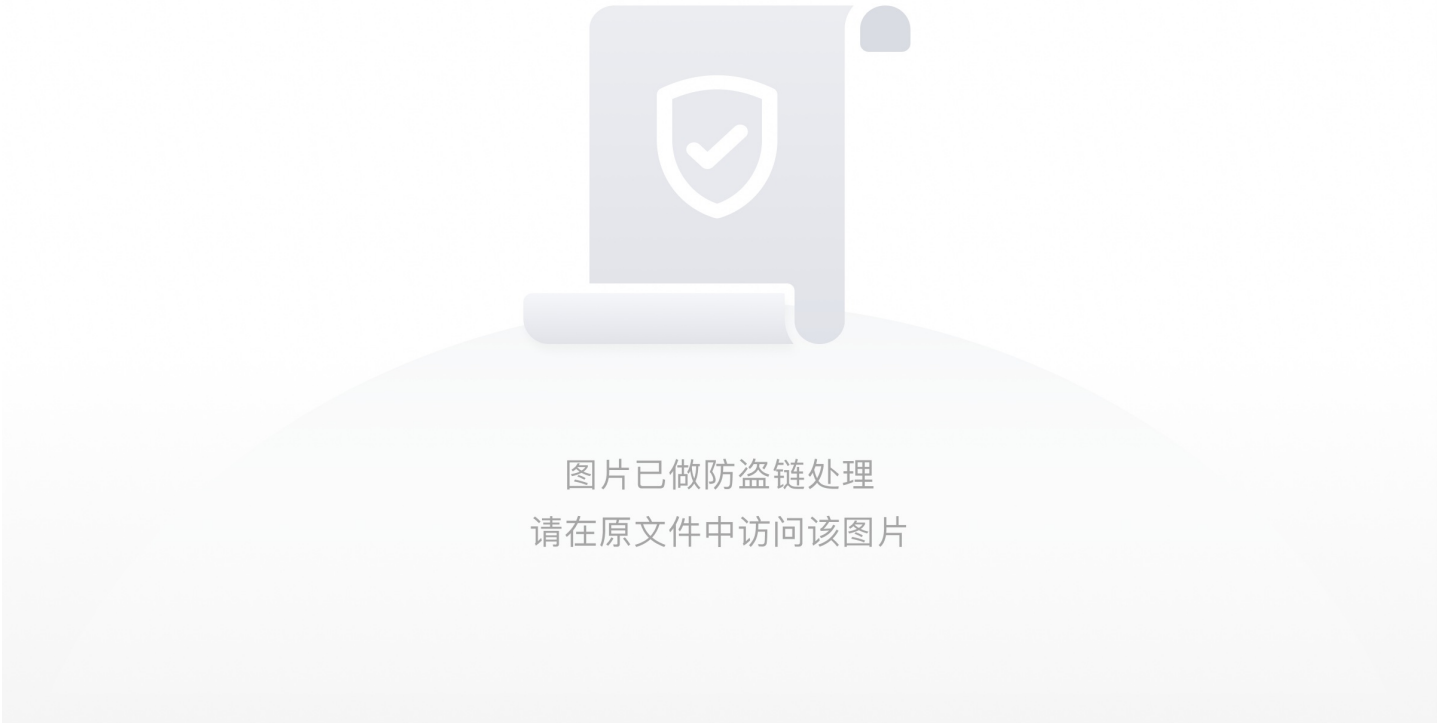
然后打开txt发现是杂乱的字符，就使用查重复字码以下脚本

```
# gakki_exp.py
# Author : imagin
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- ={}[]"
f = open("flag.txt", "r")
data = f.read()
result = {d:0 for d in alphabet}

def sort_by_value(d):
    items = d.items()
    backitems = [[v[1],v[0]] for v in items]
    backitems.sort(reverse=True)
    return [ backitems[i][1] for i in range(0,len(backitems))]

for d in data:
    for alpha in alphabet:
        if d == alpha:
            result[alpha] = result[alpha] + 1

print(sort_by_value(result))
```




```
flag{gaki_IsMyw1fe}
```

黑客帝国 | **SOLVED** |

解压文件，然后用notepad，用插件转换成ascii，发现是rar文件

爆破一下

获得一个文件，然后放进winhex里面发现文件头错误

修改一下


```
flag{57cd4cfd4e07505b98048ca106132125}
```

[安洵杯 2019]吹着贝斯扫二维码 | SOLVED |

解压文件绕后给没有后缀名的文件加上.jpg就是漫长的拼图了


```
BASE Family Bucket ??? 85->64->85->13->16->32
```

然后看样子base85不可能,所以换一下反过来是base32->base16->rot13->base85->base64->base85的顺序解密得到压缩包密码

```
ThisIsSecret!233
flag{Qr_Is_MeAn1nGfuL}
```

[GXYCTF2019]SXMgdGhpcyBiYXNlPw== | SOLVED |

以为是base64，用note转码发现是乱码，看起来不是，然后百度一下发现有一种base64隐写术

```
# -*- coding: cp936 -*-
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('flag.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = ''.join(line.split())
        rowb64 =  ''.join(stegb64.decode('base64').encode('base64').split())
        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1]))
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
        print ''.join([chr(int(bin_str[i:i + 8], 2)) for i in xrange(0, len(bin_str), 8)]) #8 位一组
```


```
GXY{fazhazhenhaoting}
```

[SUCTF 2019]Game | SOLVED |

解压发现他的index里面有base32

可惜不是flag

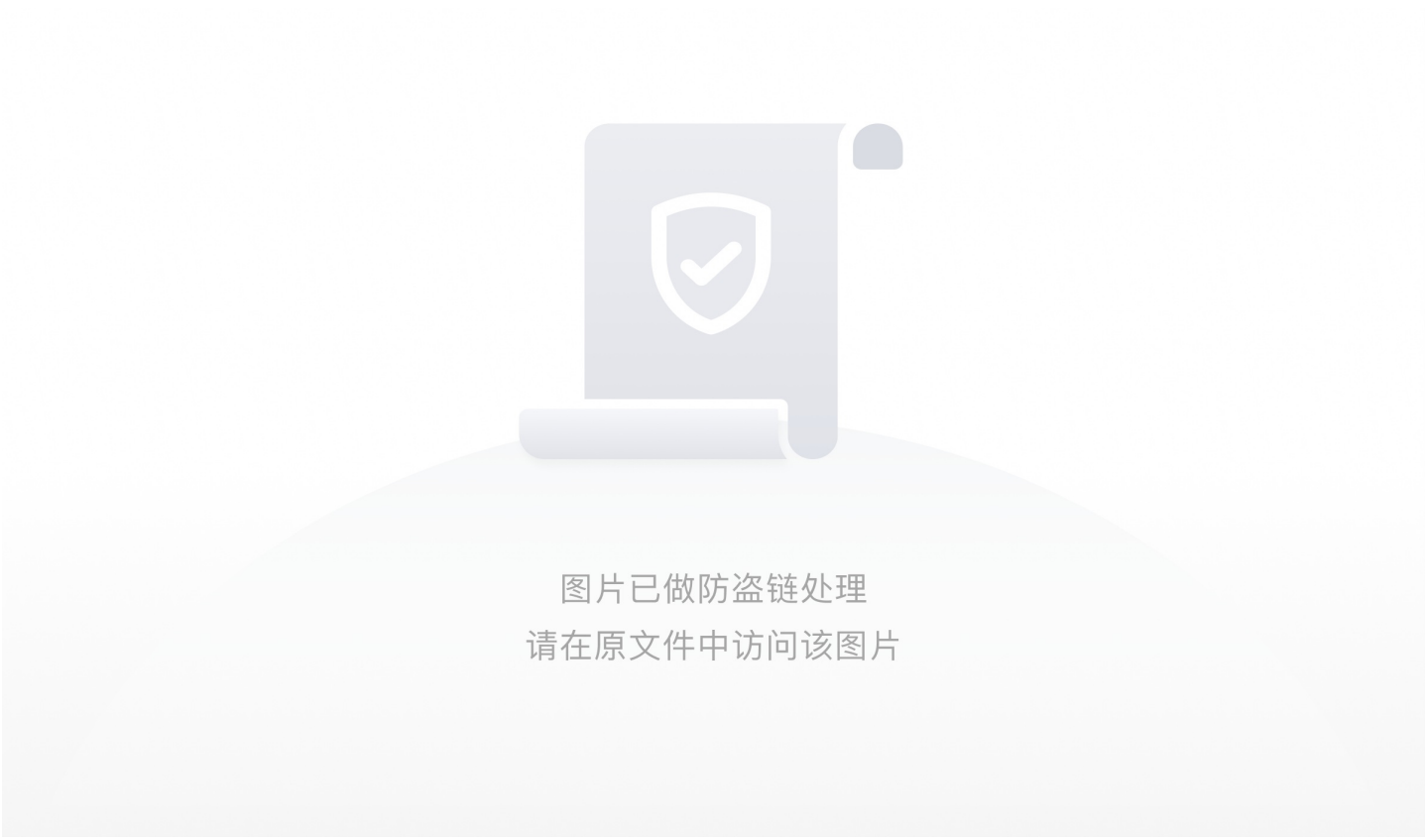
在图片中看到了密码，没有密钥，就猜测是之前的假flag

试了N此成功了

```
suctf{U_F0und_1t}
```

小易的U盘 | SOLVED |

这个研究的我心态爆炸，先说iso文件解压，然后找不到flag，然后用发开压缩包看见了一堆



可是解压了没有，后面发现，没打开显示隐藏文件，如果不知道怎么打开隐藏文件看这个文章

```
https://jingyan.baidu.com/article/574c5219cf48e86c8d9dc11a.html
```

起初以为，启动一个就生成flag，然后发现没有用，只生成都是ffff的文件
然后发现有个时间不一样

然后打开文件，搜索flag，就找到了


```
flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}
```

[GUET-CTF2019]KO | SOLVED |

一看就是ook加密https://www.splitbrain.org/services/ook，破解一下

```
flag{welcome to CTF}
```

[HBNIS2018]caesar | SOLVED |

百度一下caesar是凯撒，就凯撒密码破解一下


```
flag{flagiscaesar}
```

[ACTF新生赛2020]base64隐写 | SOLVED |

名字既然如此，看到了文件

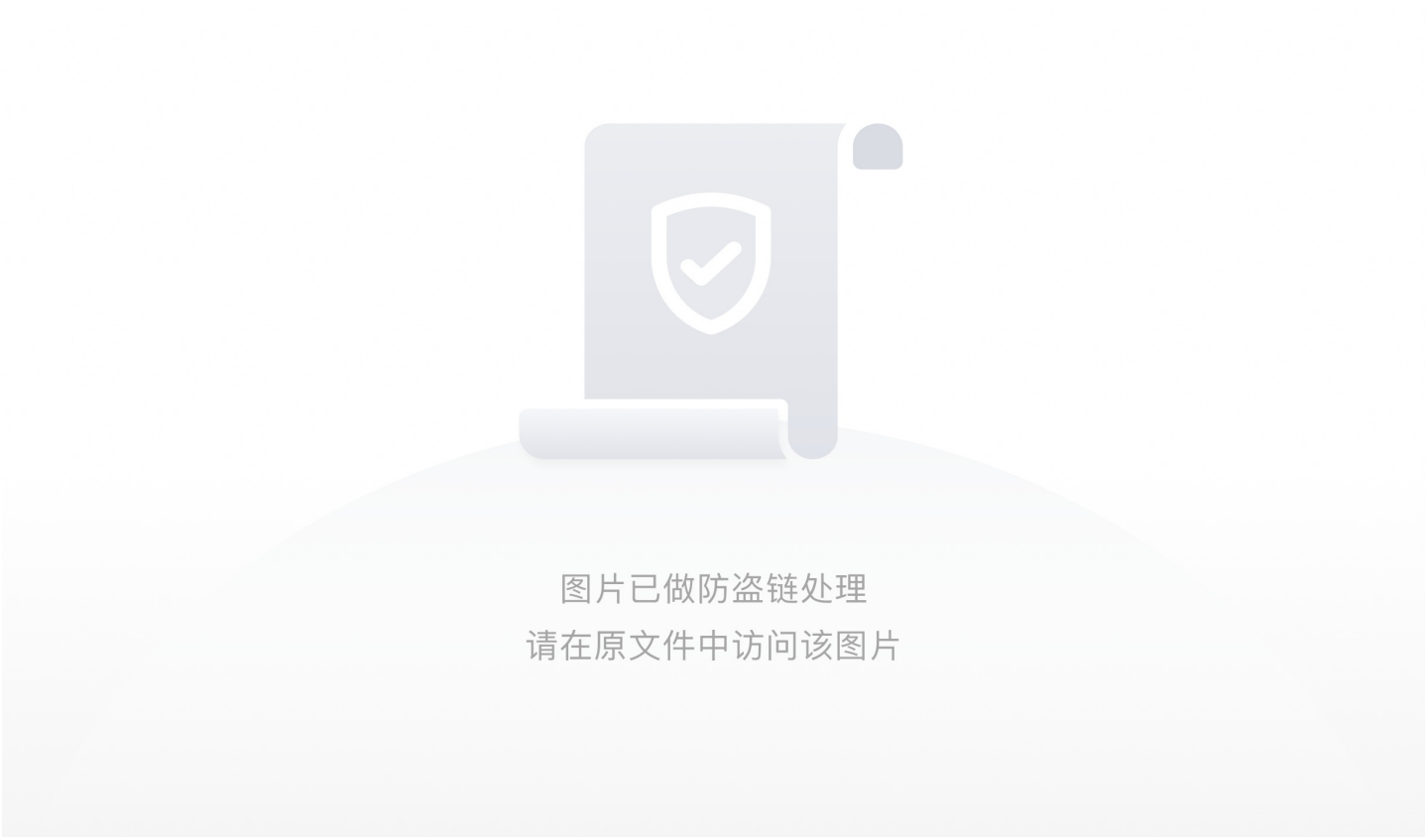
脚本跑一下

```
# -*- coding: cp936 -*-
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('flag.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = ''.join(line.split())
        rowb64 =  ''.join(stegb64.decode('base64').encode('base64').split())
        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1]))
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
        print ''.join([chr(int(bin_str[i:i + 8], 2)) for i in xrange(0, len(bin_str), 8)]) #8 位一组
```


```
ACTF{6aseb4_f33!}
```

[SWPU2019]Network | SOLVED |

打开文本



始终找不到思路，看到大佬的提示

然后明白还有这种操作！！

```
fp = open('attachment.txt','r')
a = fp.readlines()
p = []
for i in a:
    p.append(int(i))
s = ''
for i in p:
    if i == 63:
        a = '00'
    elif i == 127:
        a = '01'
    elif i == 191:
        a = '10'
    elif i == 255:
        a = '11'
    s += a

import binascii
flag = ''
for i in range(0,len(s),8):
    flag += chr(int(s[i:i+8],2))
flag = binascii.unhexlify(flag)
wp = open('flag.txt','wb')
wp.write(flag)
wp.close()
```

转换之后打开txt

发现是zip，给你改个扩展名，发现有密码，然后检查一下发现是伪加密

修改为00，打开文件知道看到最后知道是base64，然后N次，解码成功拿到flag

```
flag{189ff9e5b743ae95f940a6ccc6dbd9ab}
```

[GUET-CTF2019]zips | SOLVED |

解压zip，然后看到还有加密的zip，用软件破解

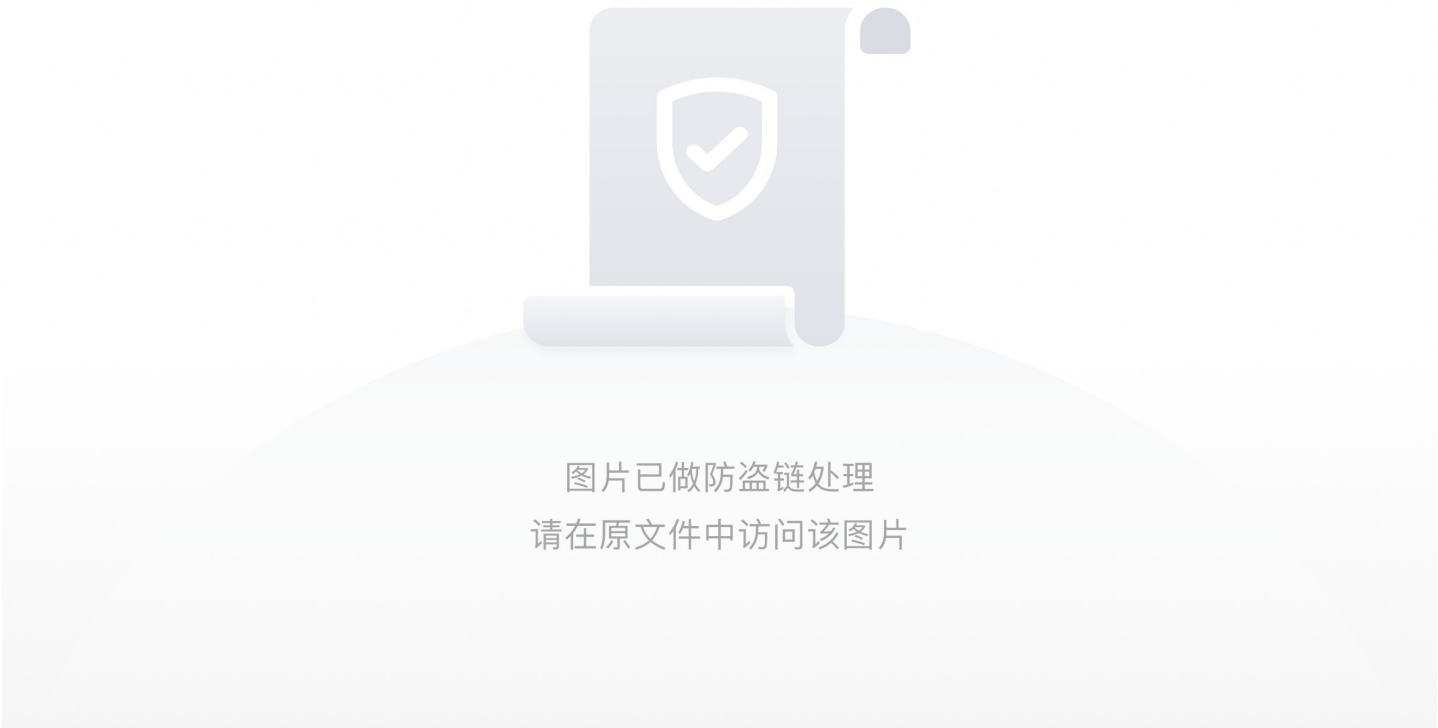
得到密码解压，发现还是加密，是伪加密

修改一下09变成00之后，解压

打开setup 打开一看发现是py，然后运行一下

看不懂，完后百度了一下知道了这是掩码破解 格式是???.??

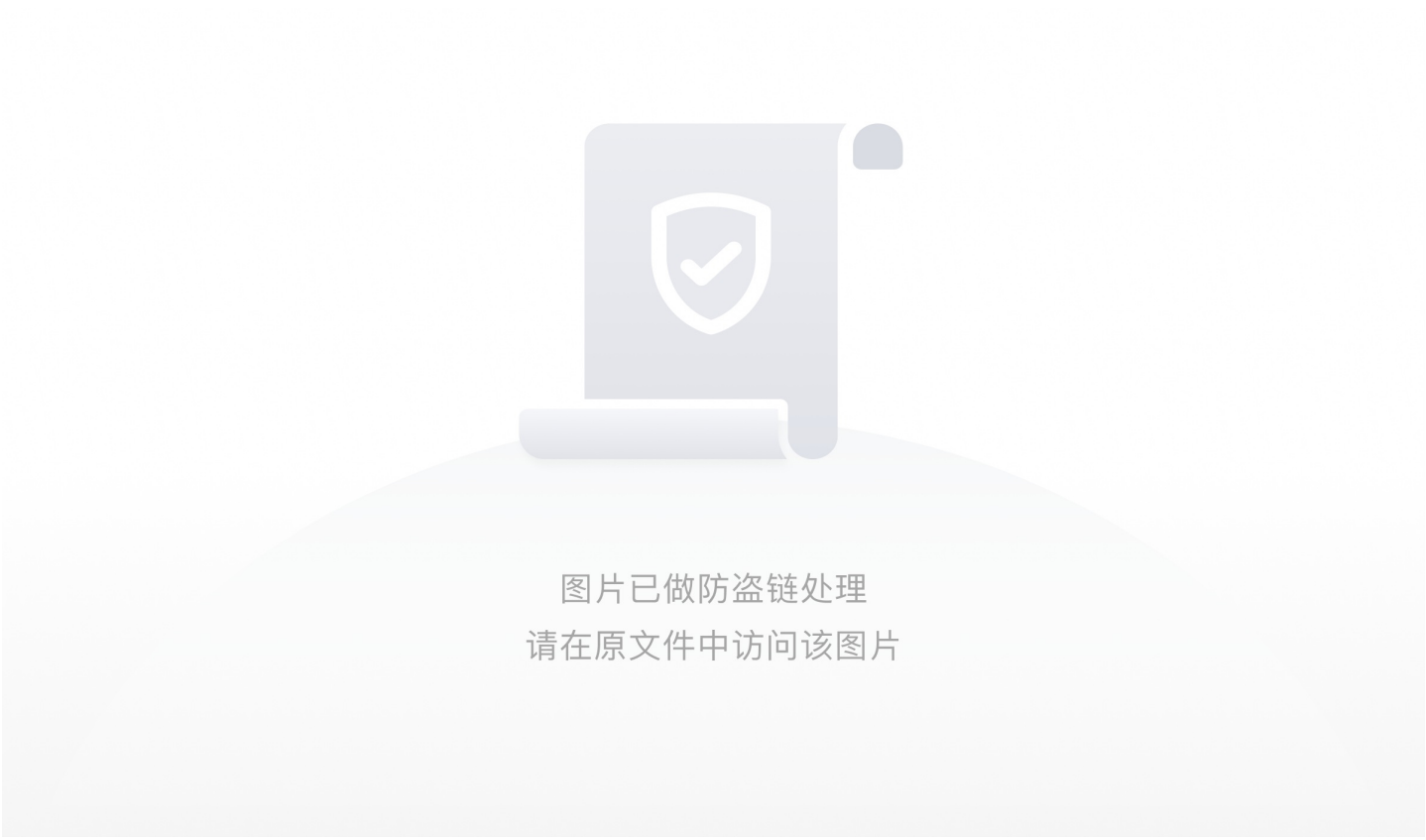
然后用软件破解




```
flag{fkjabPqnLawhvuikfhgzyffj}
```

[HBNIS2018]低个头 | SOLVED |

他说低头，我低头看着键盘，看见这些能组成3个字就是CTF




```
flag{CTF}
```

百里挑一 | SOLVED |

解压打开，导出http，

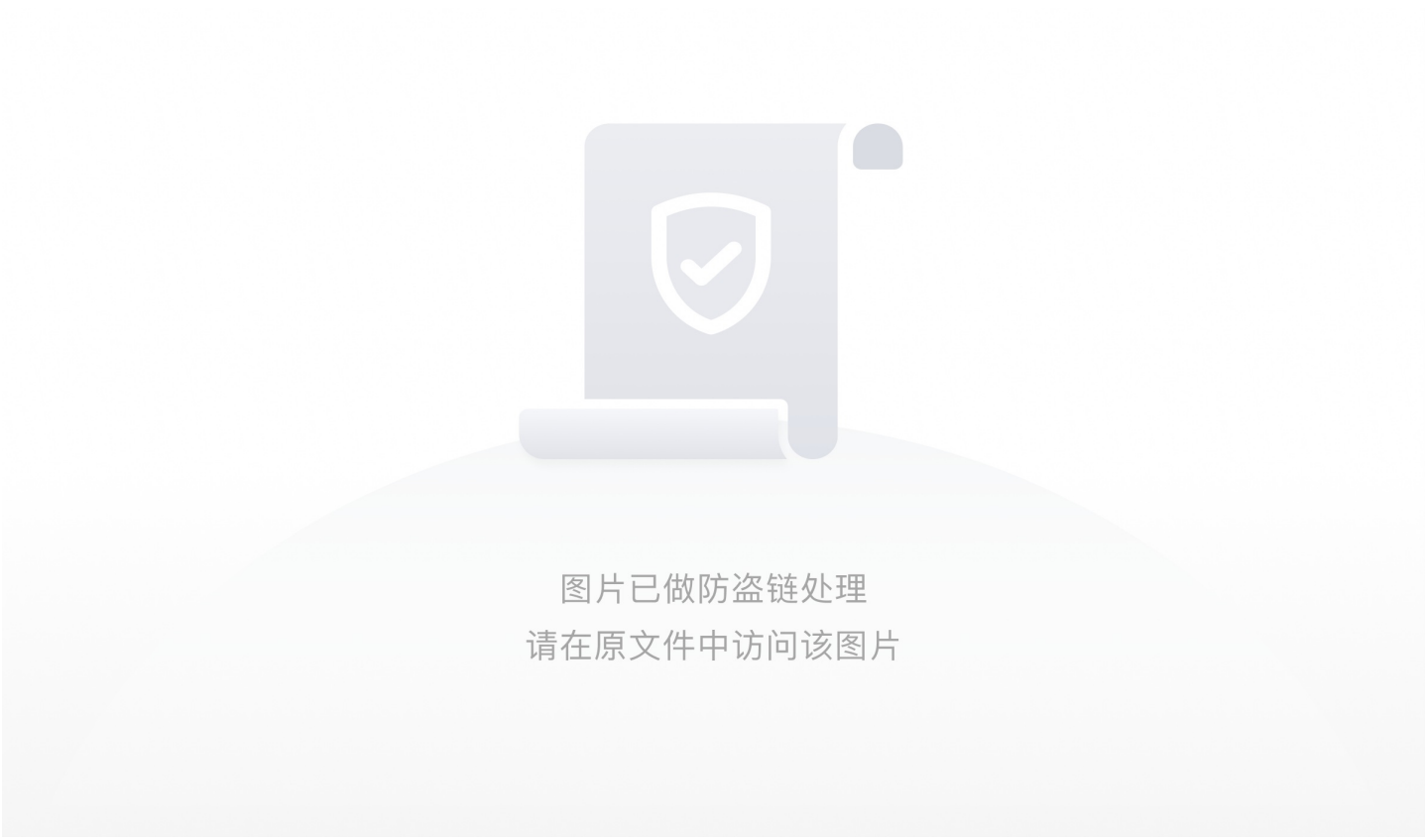
，发现都是图片，百度才知道有这个exiftool找flag的办法

```
summer@summer:~/桌面/cc/flag$ exiftool *|grep flag
XP Comment                      : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f
```

这样代码找到一般，另外一半，找了半天才知道

```
tcp.stream eq 114
```

这里



真的的人脑洞大无止境啊！！！

```
flag{ae58d0408e26e8f26a3c0589d23edeec}
```

[RCTF2019]draw | SOLVED |

打卡文件，刚开始以为是字频，发现太少了，然后放进百度，发现是画logo的密文？？？？

https://www.calormen.com/jslogo/


```
flag{RCTF_HeyLogo}
```

[WUSTCTF2020]find_me | SOLVED |

属性面板看到了盲文解密一下

https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen

```
wctf2020{y$0$u_f$1$n$d$_M$e$e$e$e$e}
```

我吃三明治 | SOLVED |

分离一下发现没有任何问题，属性也没有，然后打开winhex，在2张图片的连接处找到了

base32解码


```
flag{6f1797d4080b29b64da5897780463e30}
```

sqltest | SOLVED |

打开文件，文件–>导出文件–>http

看到这个我研究了半天，找到大佬才知道这是一个注入，先复制出来然后用

知道，就是取flag字段一个进行判断从第一个开始判断，从第一个框知道102>flag1>101

所以就是102，慢慢测试出来

102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57 101 99 100 101 102 55 125

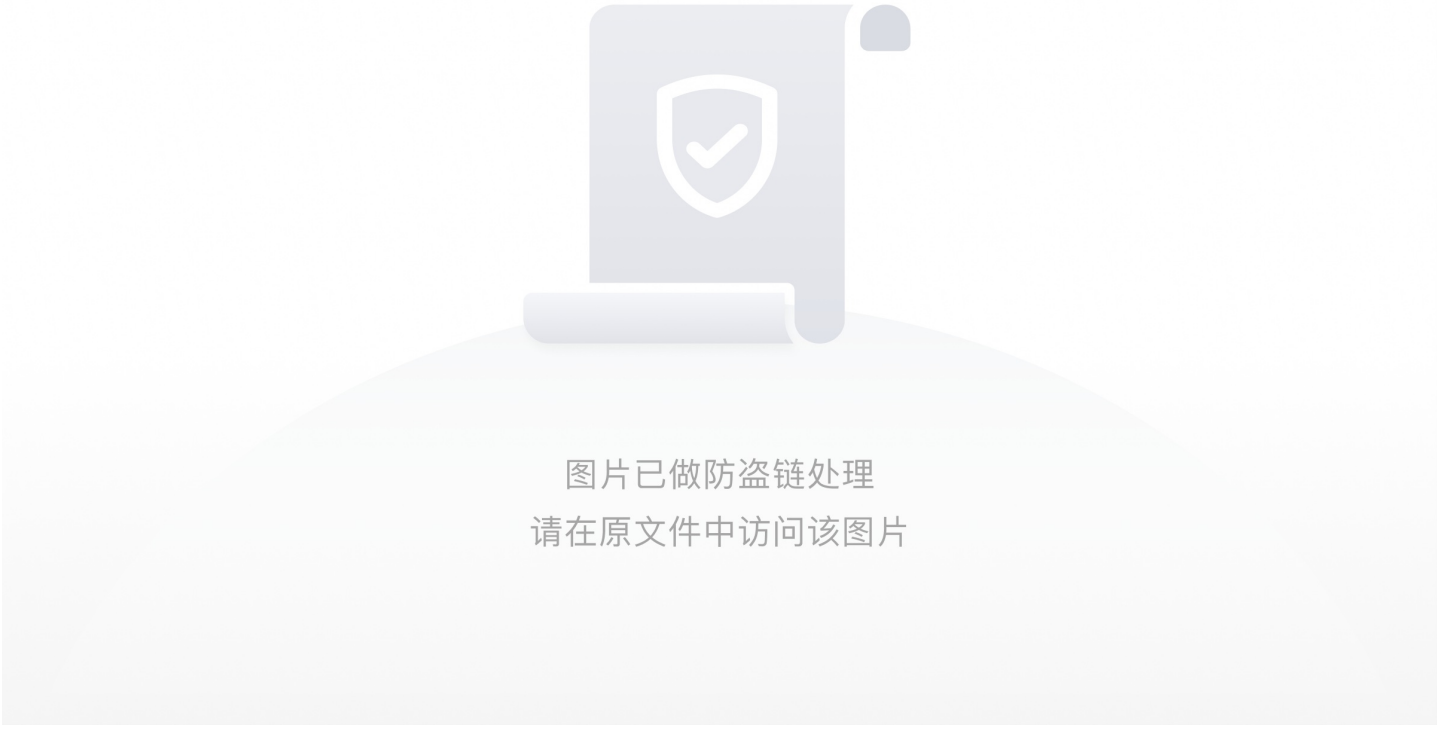
转为字符串得flag

flag{47edb8300ed5f9b28fc54b0d09ecdef7}

弱口令 | SOLVED |

似乎有东西

sublime打开，发现了是莫斯



用binw和fore

都没结果，最后在lsb，隐写上面，下载脚本

```
#网上脚本#
太长了就省略
#用法#
$ python lsb.py
LSB steganogprahy. Hide files within least significant bits of images.

Usage:
  lsb.py hide <img_file> <payload_file> <password>
  lsb.py extract <stego_file> <out_file> <password>
  lsb.py analyse <stego_file>
```

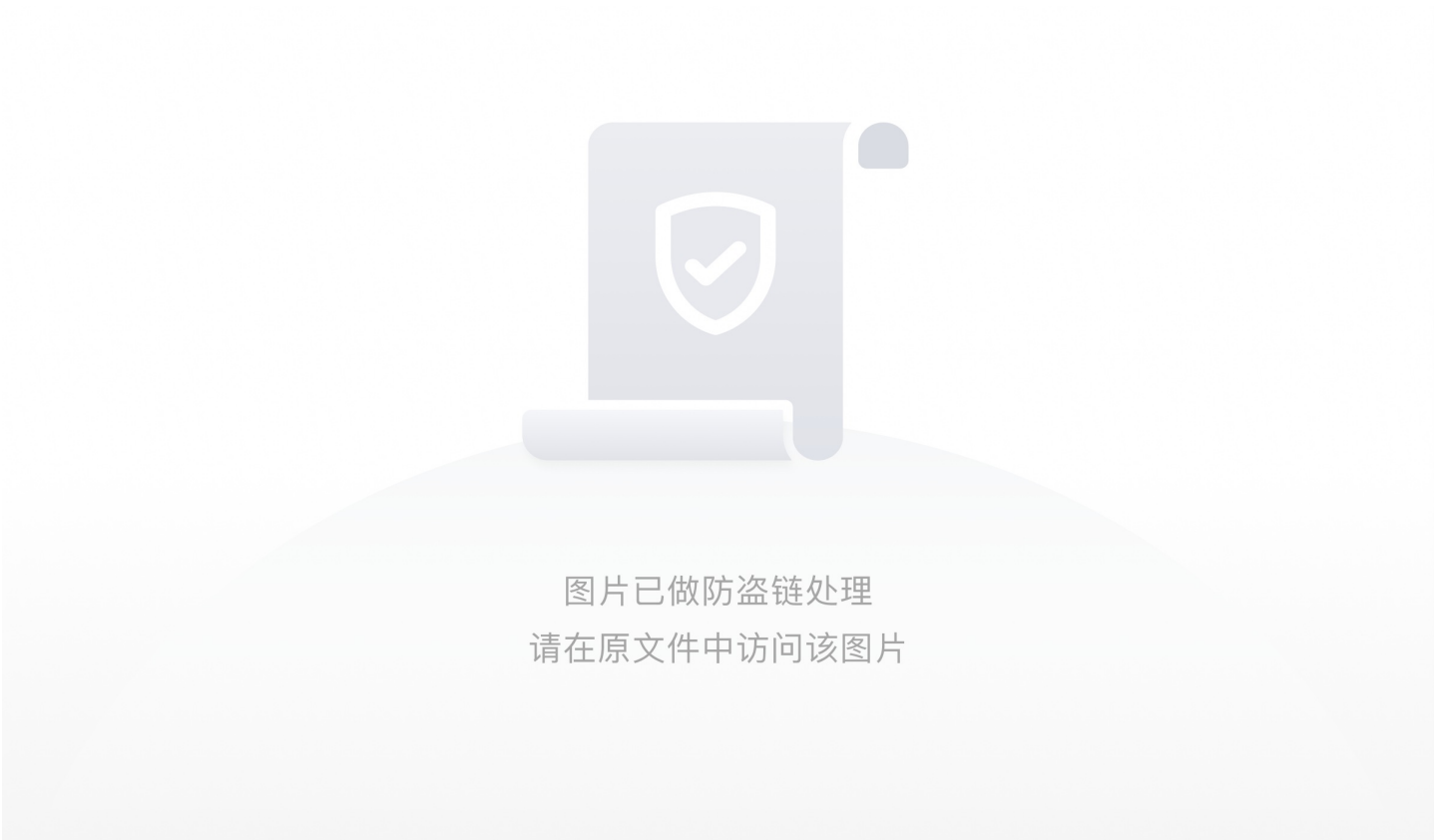
搞这个安装了超级多的库比如

```
pip install pycryptodome
pip install Crypto
pip install Pillow
pip install matplotlib
pip install numpy
```

最后用py2，输入

```
E:\桌面\脚本库>py lsb.py extract 1.png 1.txt 123456
[+] Image size: 500x500 pixels.
[+] Written extracted data to 1.txt.
```

因为是弱口令就密码是123456




```
flag{jsy09-wytg5-wius8}
```

真的很杂 | SOLVED |

下载，解压，使用fore分离，发现了000001.zip其实是apk，更换该后缀名.apk，安卓文件，apktool先通过这个编译

```
apktool d 00001.apk
```

然后在zip方式打开，看到

复制到dex2jar-2.0


```
d2j-dex2jar.bat classes.dex
```

jd-gui使用这个打开，就能看到flag

```
flag{25f991b27fcdc2f7a82a2b34386e81c4}
```

[V&N2020 公开赛]拉胯的三条命令 | SOLVED |

首先，下载，百度如何抓包，查端口，然后知道了可以用tcpdump

```
tcpdump -n -r nmapll.pcapng 'tcp[13] = 18' | awk '{print $3}'| sort -u
```

```
-n  不把 [网络地址转换](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%9C%B0%E5%9D%80%E8%BD%AC%E6%8D%A2) 成名字;
-r  从指定的文件中读取包(这些包一般通过-w选项产生);
```

awk ‘{print $3}’

取第三为字符串

sort -u 拒绝重复


```
flag{21226318013306}
```

USB | SOLVED |

下载文件，然后解压，发现文件有个png文件头损坏。然后去看数据结构

修改7A到74，解压图片，在blue通道中看到二维码


```
ci{v3erf_0tygidv2_fc0} 发现不是凯撒也不是栅栏~
接下来看看binwalk -e key.ftm
看到了有key.pcap
```

使用读取usb数据

```
tshark -r key.pcap -T fields -e usb.capdata > usbdata.txt
```

得到一个txt用脚本跑

```
mappings = { 0x04:"A",  0x05:"B",  0x06:"C", 0x07:"D", 0x08:"E", 0x09:"F", 0x0A:"G",  0x0B:"H", 0x0C:"I",  0x0D:
"J", 0x0E:"K", 0x0F:"L", 0x10:"M", 0x11:"N",0x12:"O",  0x13:"P", 0x14:"Q", 0x15:"R", 0x16:"S", 0x17:"T", 0x18:"U
",0x19:"V", 0x1A:"W", 0x1B:"X", 0x1C:"Y", 0x1D:"Z", 0x1E:"1", 0x1F:"2", 0x20:"3", 0x21:"4", 0x22:"5",  0x23:"6",
 0x24:"7", 0x25:"8", 0x26:"9", 0x27:"0", 0x28:"\n", 0x2a:"[DEL]",  0X2B:"    ", 0x2C:" ",  0x2D:"-", 0x2E:=", 0
x2F:"[",  0x30:"]",  0x31:"\\", 0x32:"~", 0x33:";",  0x34:"'", 0x36:",",  0x37:"." }
nums = []
keys = open('usbdata.txt')
for line in keys:
    if line[0]!='0' or line[1]!='0' or line[3]!='0' or line[4]!='0' or line[9]!='0' or line[10]!='0' or line[12]
!='0' or line[13]!='0' or line[15]!='0' or line[16]!='0' or line[18]!='0' or line[19]!='0' or line[21]!='0' or l
ine[22]!='0':
        continue
    nums.append(int(line[6:8],16))
keys.close()
output = ""
for n in nums:
    if n == 0 :
        continue
    if n in mappings:
        output += mappings[n]
    else:
        output += '[unknown]'
print 'output :\n' + output
```

得到key

```
output :
KEYXINAN
```

维吉尼亚密码破解一下，在栅栏一下

```
ci{v3erf_0tygidv2_fc0}
key=XINAN
fa{i3eei_0llgvgn2_sc0}
栅栏
flag{vig3ne2e_is_c00l}
```

蜘蛛侠呀 | SOLVED |

分离也出不来，fore和binw都失败了，然后知道了可以用

```
tshark -r out.pcap -T fields -e data >out.txt
```

提取隐写

一堆看不懂，然后百度一下原来要删除筛选一些，这是脚本

```
lines = open("out.txt",'rb').readlines()
files = open("out1.txt","wb")
for line in lines:
 files.write(line.strip().decode('hex'))
files.close()
```

得到的结果还要往下面解base64这边使用notepad++，插件转换发现很多都重复了，使用脚本删除重复的

```
a = open("out1.txt",'rb').readlines()
file1 = open("out2.txt",'wb')
for i in range(len(a)):
 bb = a[i].strip()
 if bb == a[i-1].strip():
  continue
 file1.write(bb+'\n')
```

然后转换还有问题，多了一些没用的东西

删除

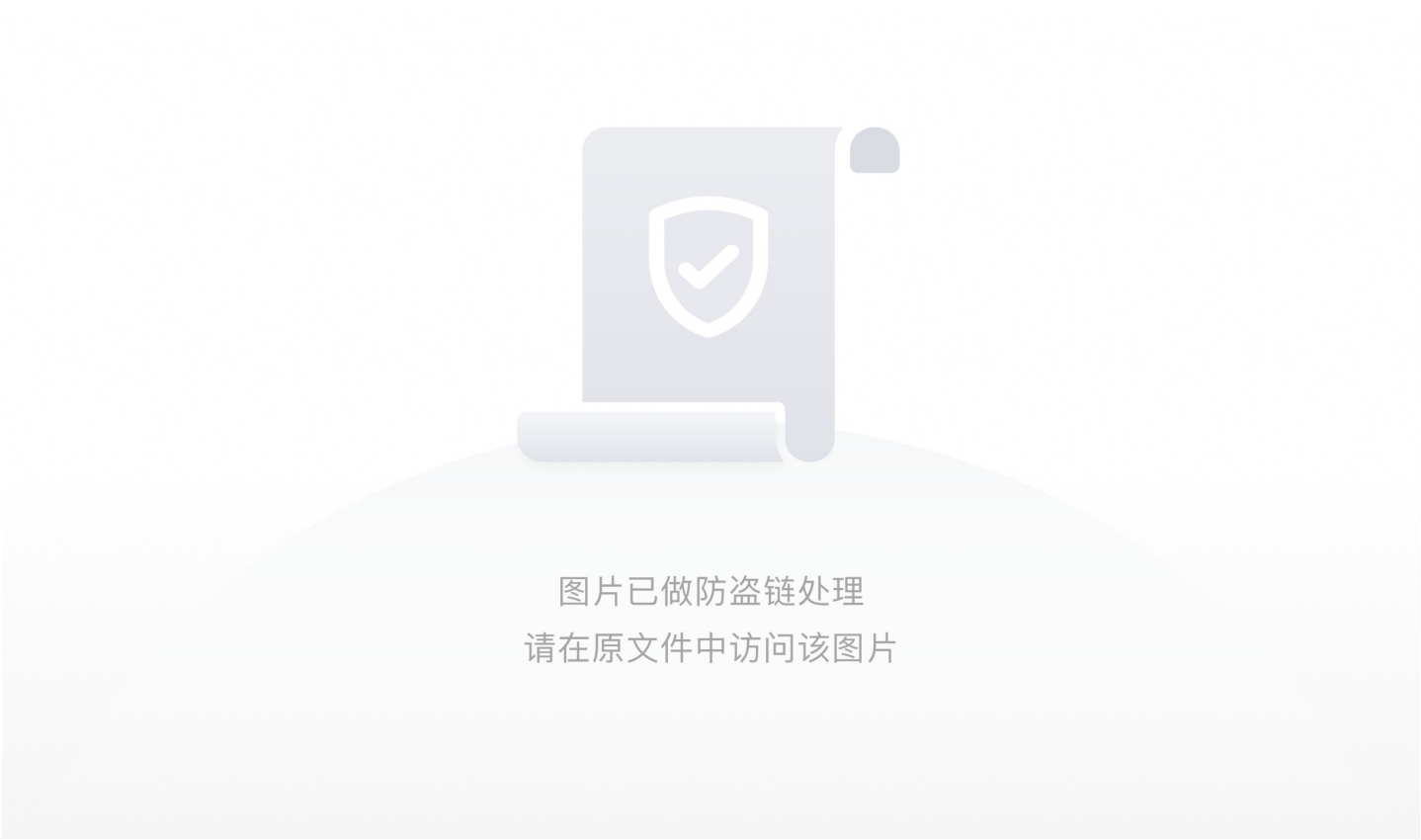
然后用notepad++插件转换成base64解码

，然后转换zip就成功了拿到了gif然后搜索一下有什么隐写，知道了一个这个**identify**

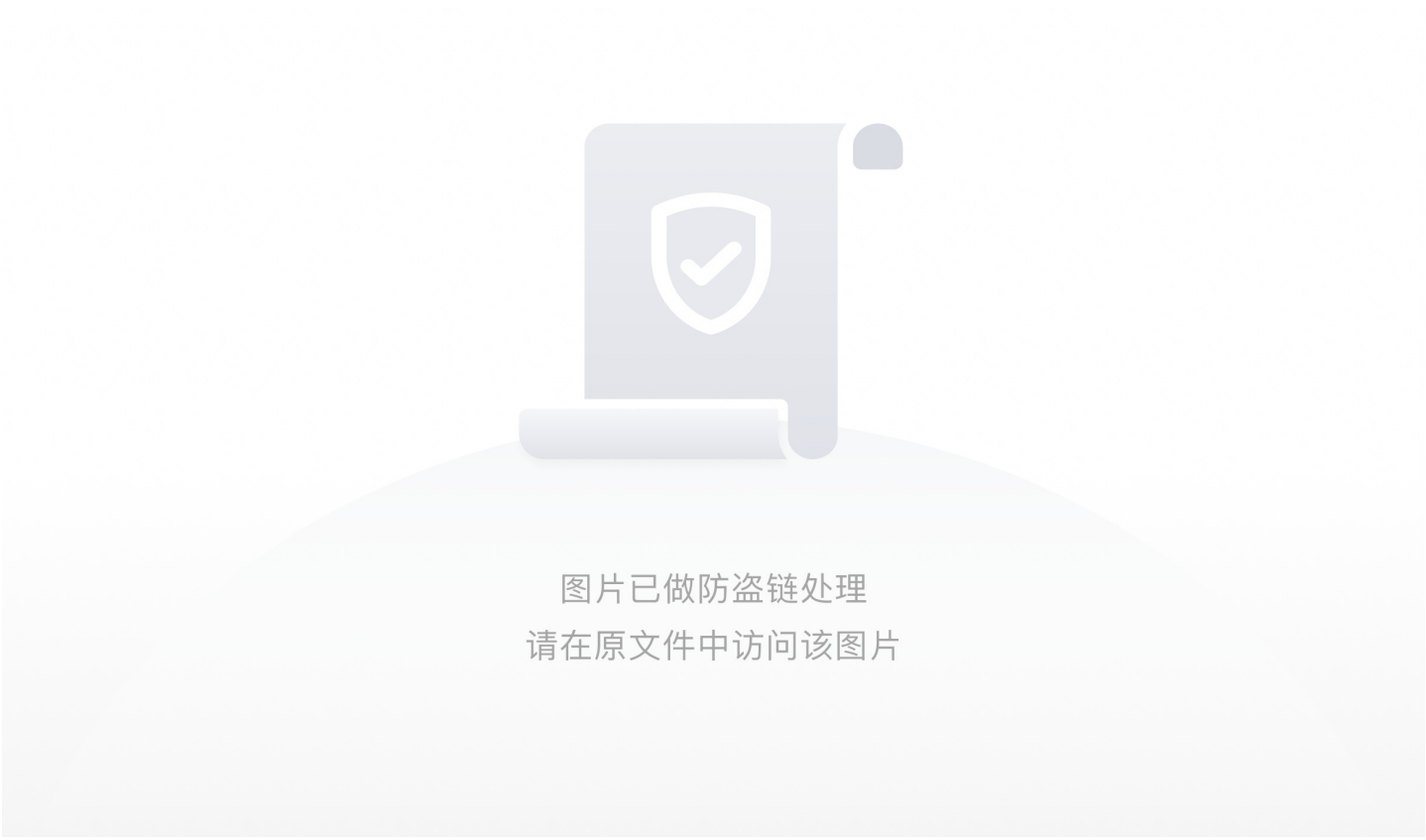
```
#identify -format “%T” flag.gif
“20”“50”“50”“20”“50”“50”“20”“50”“20”“50”“20”“20”“20”“50”“20”“20”“20”“20”“50”“50”“20”“50”“20”“50”“20”“50”“20”“50”
“50”“50”“50”“50”“20”“20”“50”“50”“20”“20”“20”“50”“20”“50”“50”“50”“20”“50”“20”“20”“66”“66”
起初以为是二进制可是看到有66，打消，以为是莫斯，还是不对，最后又绕回了二级制
01101101 01000100 00110101 01011111 00110001 01110100
翻一下
m           D          5        _        1         t
mD5_1t
md5加密一下
flag{f0f1003afe4ae8ce4aa8e8487a8ab3b6}
```

[安洵杯 2019]Attack | SOLVED |

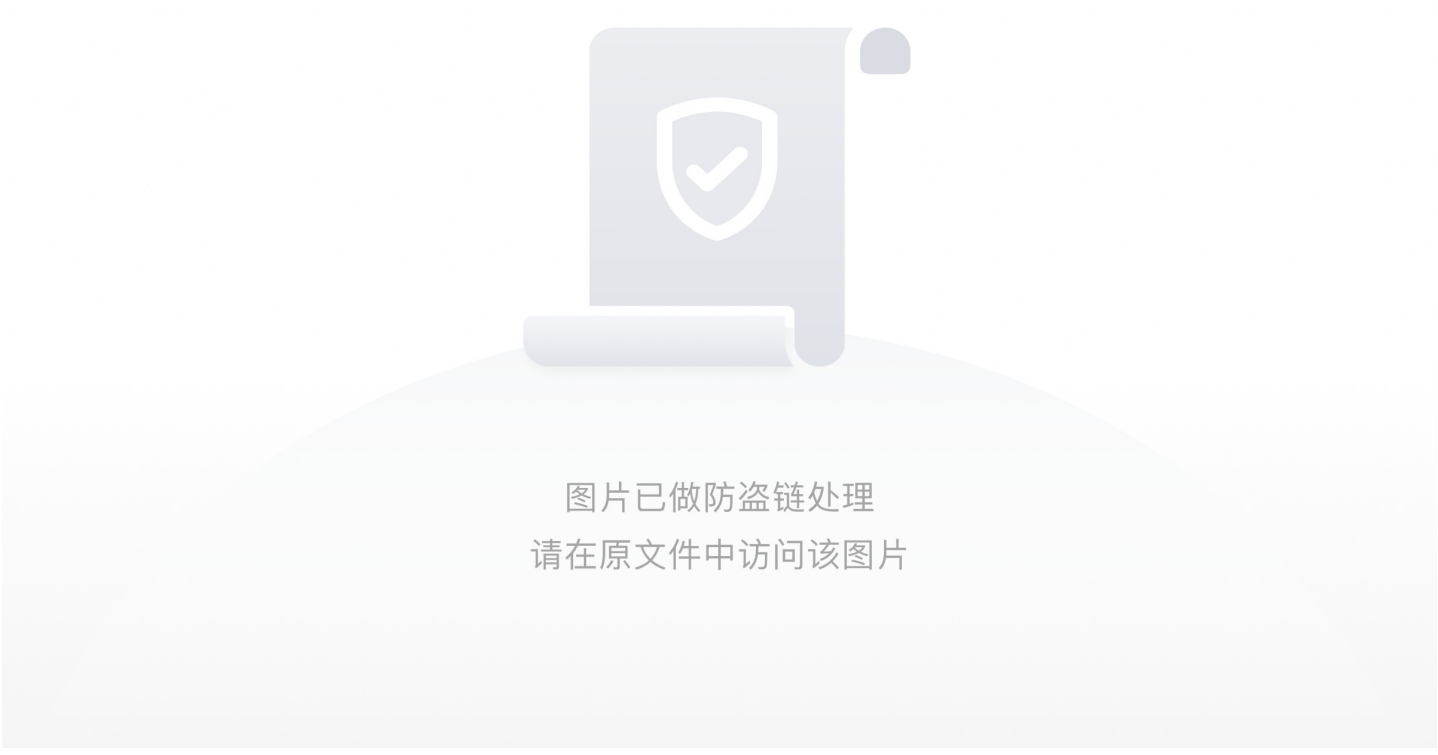
下载文件，使用fore分离发现了又flag的zip



然后在wir到处对象-》html -》看到一个蓝屏数据



然后百度一下



似乎用这个办法不行找到一个mimikatz，这个来找win密码

```
privilege::debug
sekurlsa::minidump lsass.dmp
sekurlsa::logonpasswords full
进入模式
选择文件
找密码
```


```
        * Username : Administrator
        * Domain   : WIN7
        * Password : W3lc0meToD0g3
```

解压

```
D0g3{3466b11de8894198af3636c5bd1efce2}
```

[ACTF新生赛2020]NTFS数据流 | SOLVED |

下载，然后一看这么多文件都是一样大小，百度一下知道是ntfs隐写流


```
ACTF{AAAds_nntfs_ffunn?}
```

[ACTF新生赛2020]swp | SOLVED |

下载导出文件-》html-》发现了zip。保存

，然后，解压，发现失败，一看就发现是伪加密

，解压，swp恢复一下，

在liunx中

```
pjy@admin:~/桌面/bb$ vim -r flag
pjy@admin:~/桌面/bb$ cat flag
```


```
flag{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
```

[安洵杯 2019]easy misc | SOLVED |

下载打开zip

然后前面算式解出来是7


```
7+NNULLULL,和 7NNULLULL,都不是
```

试了很久


```
2019456NNULLULL,
```

解压

看起来是什么密码百度一下，发现是原来分离出来2张一样的图片是有用的，盲水印

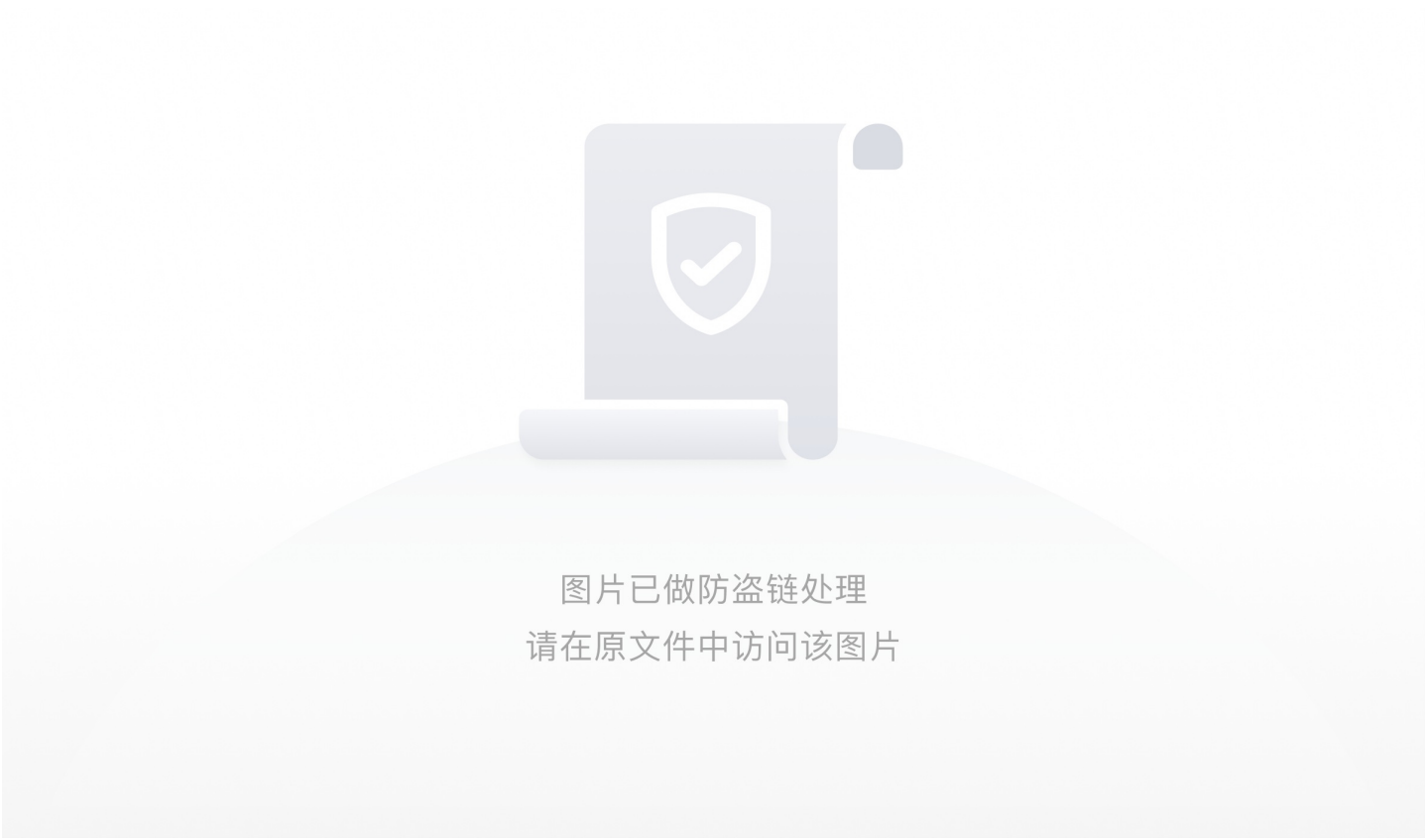
在11里面，字屏爆破看看

也就只有11可以运行把

```
etaonrhisdluygwm
base64: QW8obWdIWT9pMkFSQWtRQjVfXiE/WSFTajBtcw==
base85: Ao(mgHY?i2ARAkQB5_^!?Y!Sj0ms    这一步还以为的栅栏
flag{have_a_good_day1}
```

[XMAN2018排位赛]通行证 | SOLVED |

```
base64：a2FuYmJyZ2doamx7emJfX19ffXZ0bGFsbg==
得到这个：kanbbrgghjl{zb____}vtlaln
这个迷住了，最后师傅提醒，就是栅栏和凯撒，然后尽然解密不行，那我就加密吧，
```



看到一个很想flag的


```
xman{oyay_now_you_get_it}
```

hashcat | SOLVED |

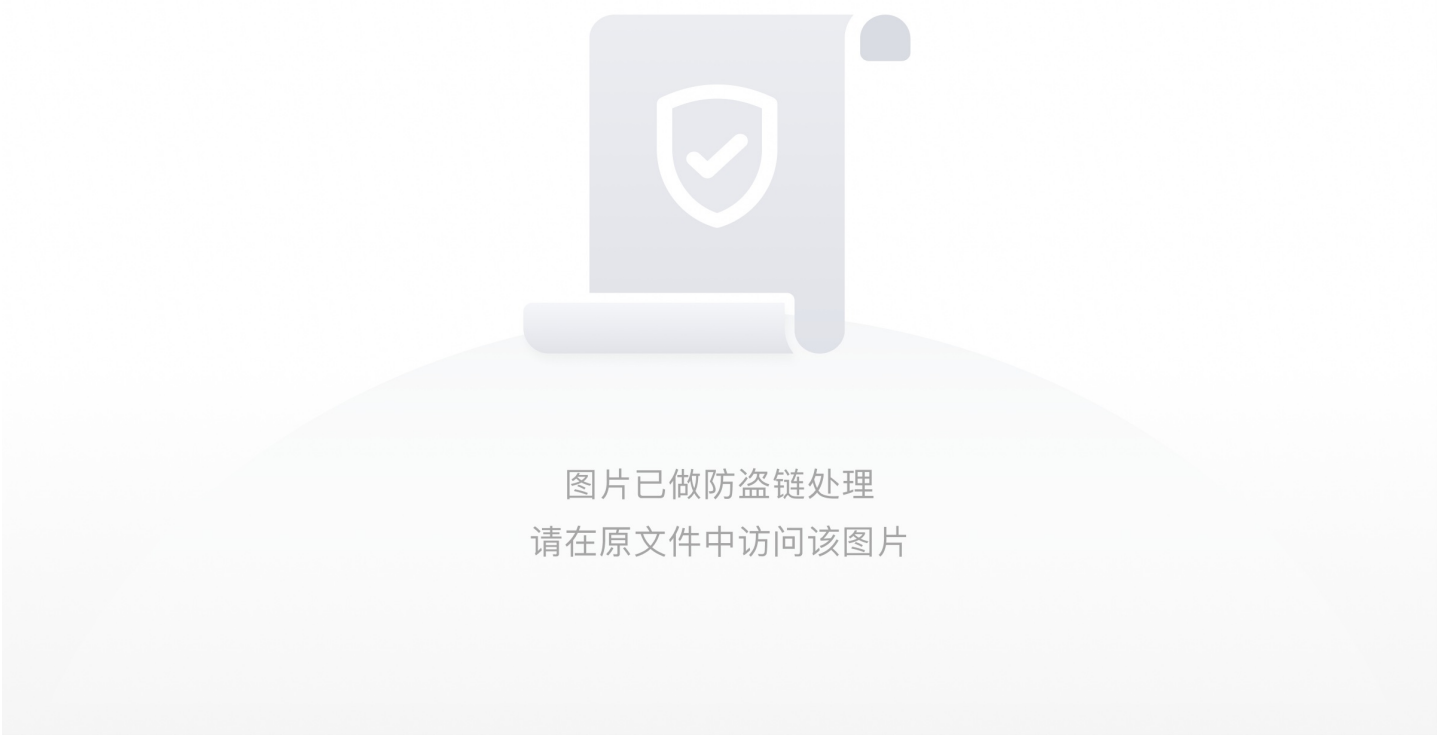
放入winhex，发现有xml的信息，就改成doc，没想到有密码，使用软件破解一下

```
Accent OFFICE Password Recovery v5.1 CracKed By Hmily[LCG]
```

知道了密码9919

都提交一下不对，然后

看着这些白色的东西



其他没东西

似乎有东西


```
Flag{okYOUWIN}
```

Business Planning Group | SOLVED |

放入winhex，分离都没有，最后放入010，发现了bpg，搜索了一下

看一啦是一个图片，分离出来


```
YnNpZGVzX2RlbGhpe0JQR19pNV9iM3R0M3JfN2g0bl9KUEd9Cg= =
bsides_delhi{BPG_i5_b3tt3r_7h4n_JPG}
```