Bugku杂项题目解析

原创

北岸冷若冰霜 于 2020-07-31 20:17:18 发布

分类专栏： # CTF夺旗 安全 文章标签： 信息安全 网络安全

本文链接：https://blog.csdn.net/u013469753/article/details/107720551

CTF夺旗 同时被 2 个专栏收录

7 篇文章 2 订阅

订阅专栏

安全

34 篇文章 3 订阅

订阅专栏

Bugku杂项

目录

1.签到题

2.这是一张单纯的图片

解析：
直接使用命令cat 1.jpg
最后一行的的信息，可知使用了base解密。

```
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;
```

在站长之家base解密

答案：

key{you are right}

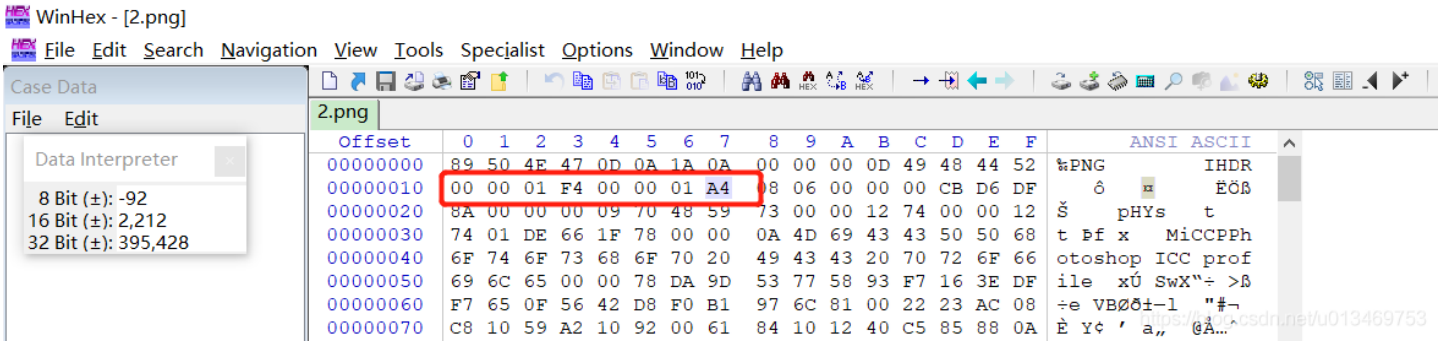
3.隐写

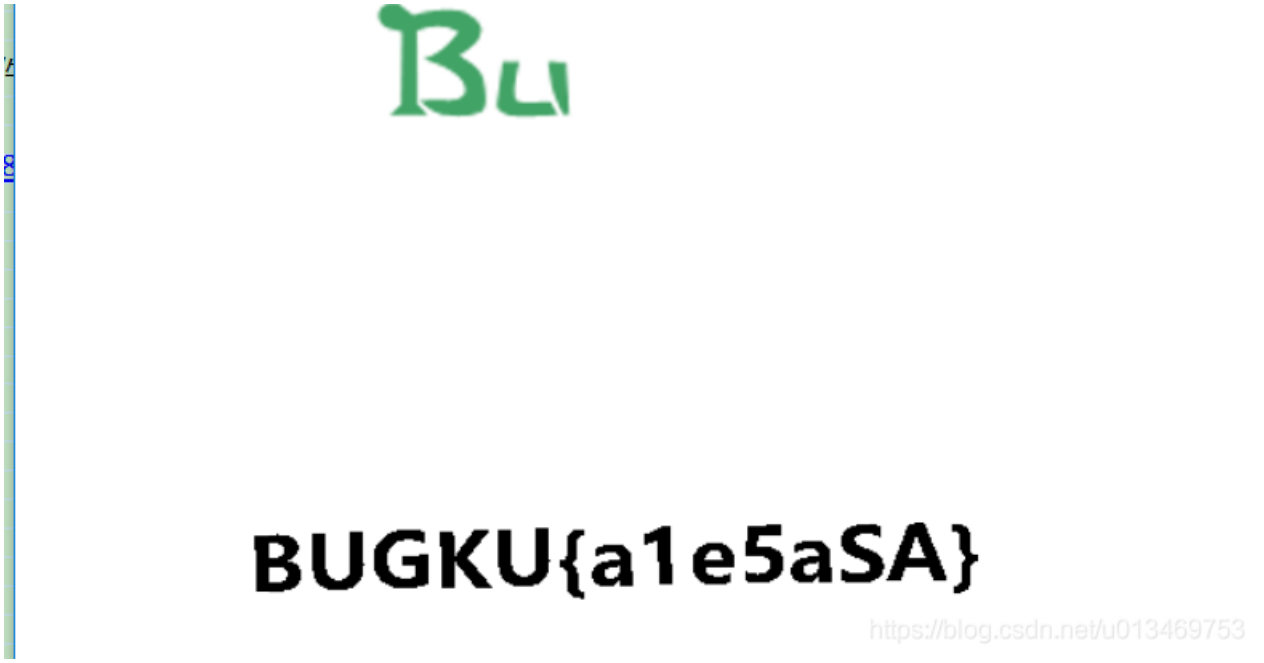
参考链接

解析：

```
urar e 2.rar
```

然后，用winhex打开2.png，将A4改成F4，则接触flag





答案：

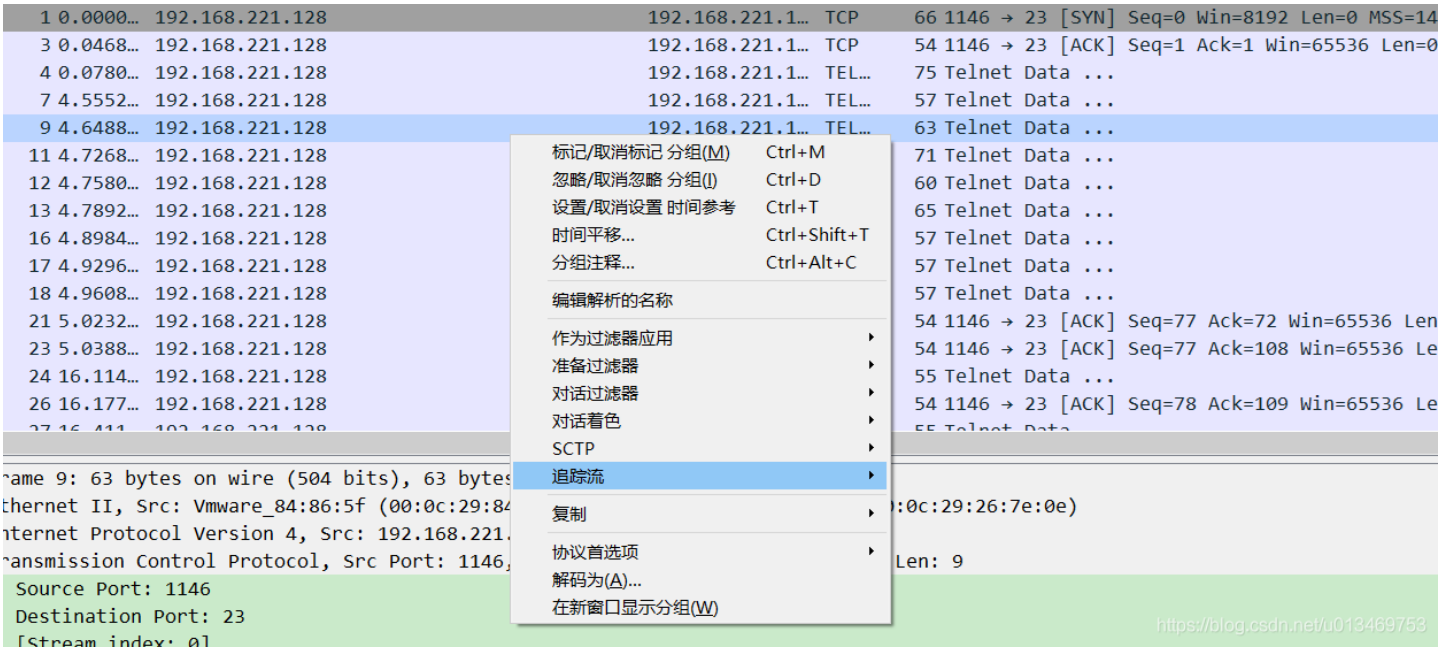
BUGKU{a1e5aSA}

4.telnet

参考链接

解析：

下载压缩包，发现里面是pcap文件格式，使用wireshark打开，右击查看TCP数据流

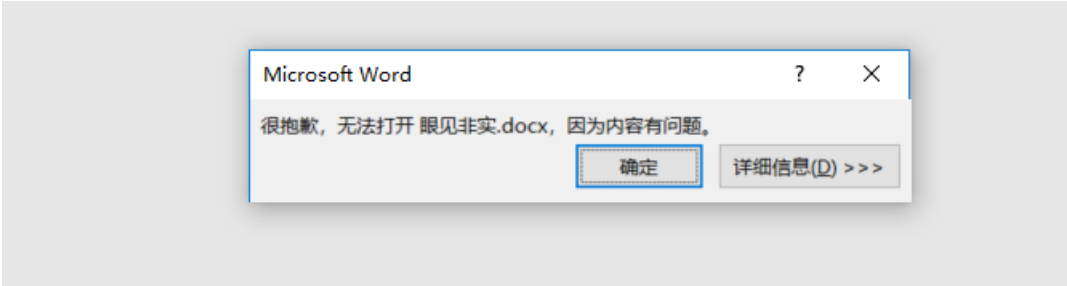


答案：

flag{d316759c281bf925d600be698a4973d5}

5.眼见非实(ISCCCTF)

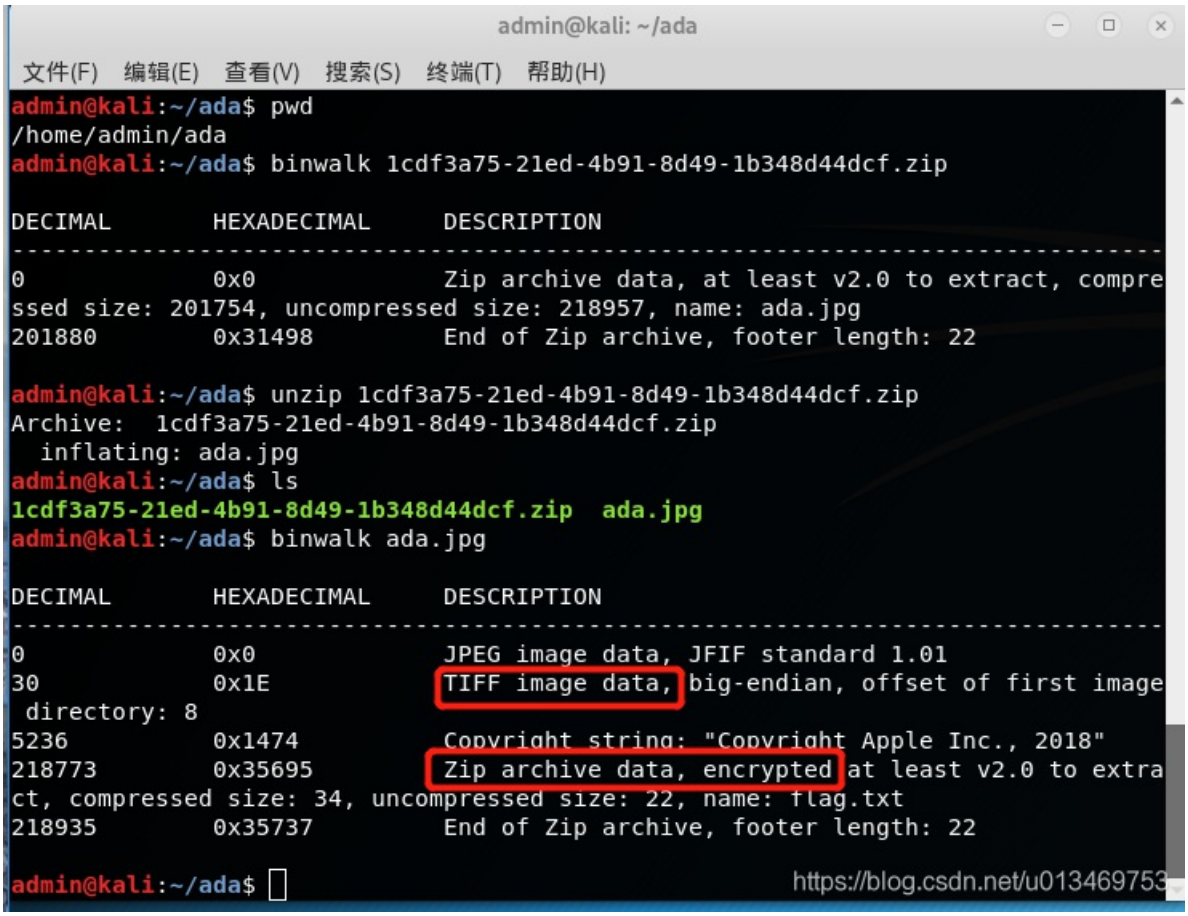
下载文件后修改文件，将zip文件名添加文件类型即zip.zip



6.啊哒

解析：

解压后得到一个图片，先使用binwalk分析图片，图片里面隐藏一段tiff信息以及一个压缩包且压缩包被加密



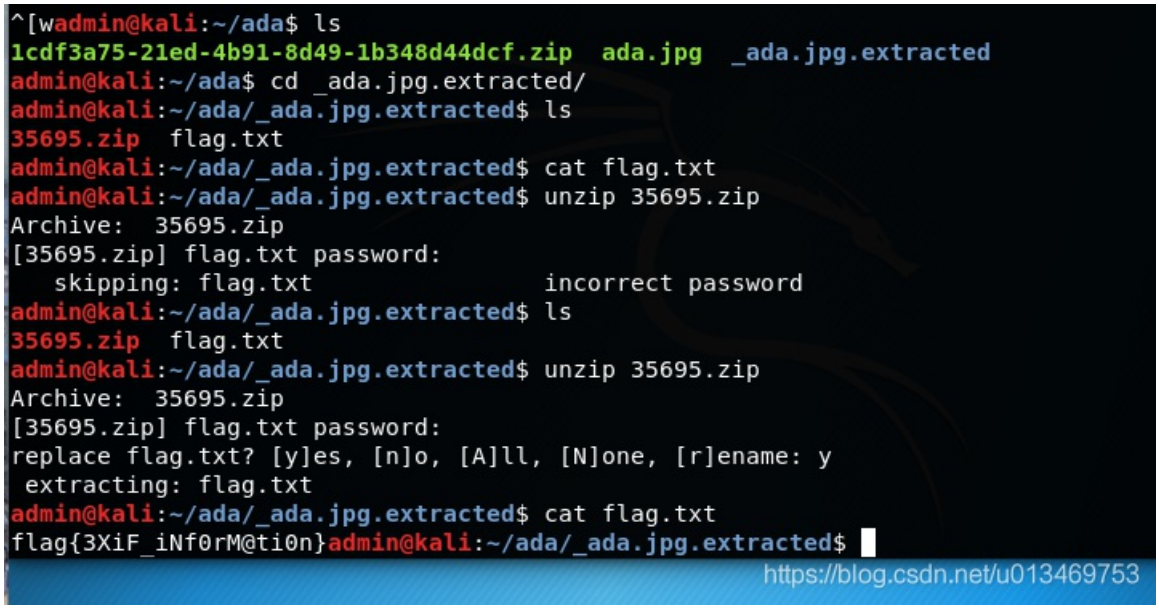
查看图片文件属性

`73646E6973635F32303138`

然后进行：十六进制转字符串

得到解压密码sdnisc_2018

解压：unzip



答案：

flag{3XiF_iNf0rM@ti0n}

7.又一张图片，还单纯吗

解析：

放进kali，binwalk查看里面竟然还有有个图片，使用foremost 分离文件 拿到flag！

```
binwalk 2.jpg
```

```
foremost 2.jpg
```

进入output文件夹，flag图片已分离

答案：

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

8.猜

解析：

直接百度识图

答案：

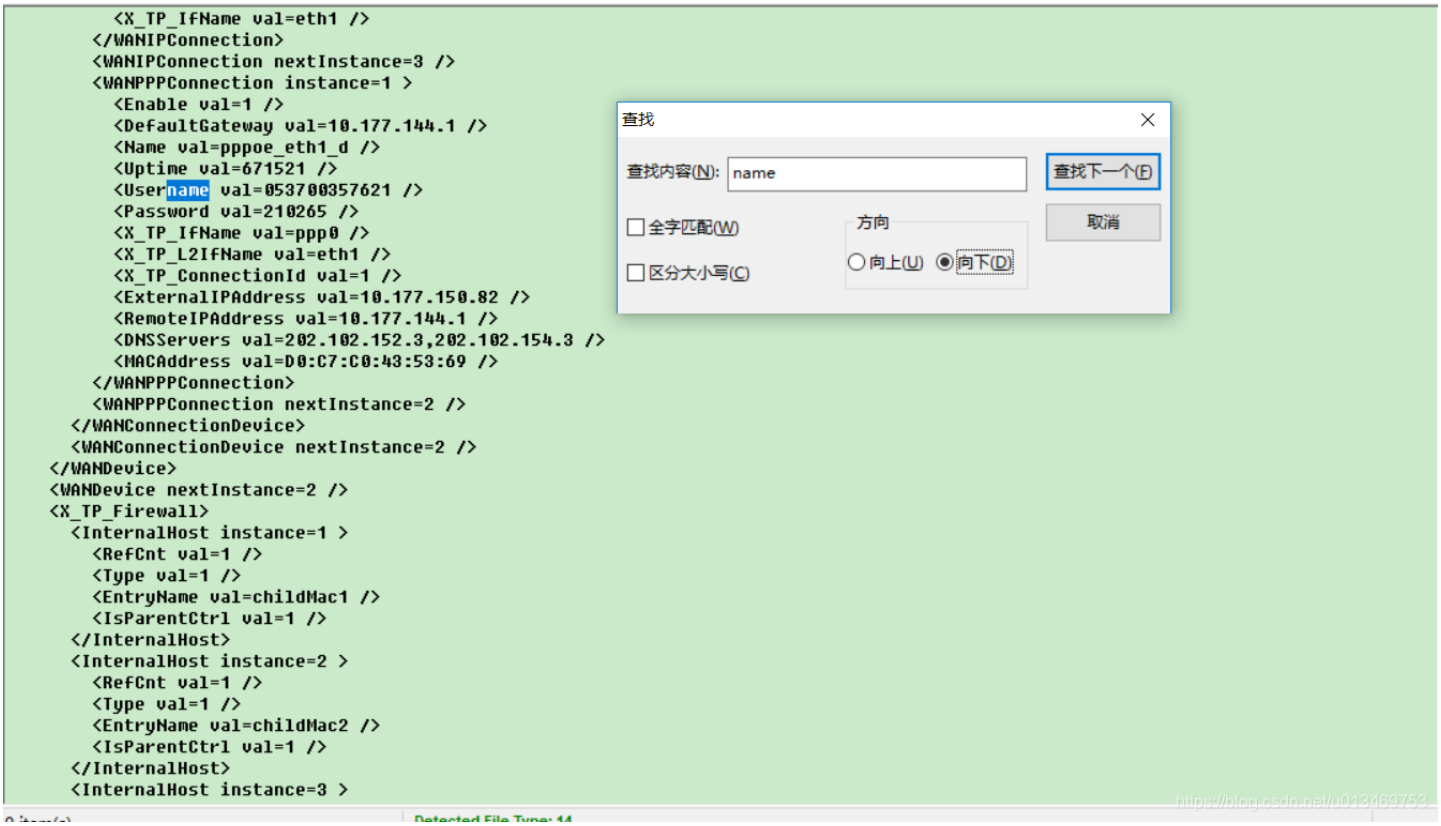
key{liuyifei}

9.宽带信息泄露

解析：

下载routerpassview工具

然后使用该工具查看，即可得到flag



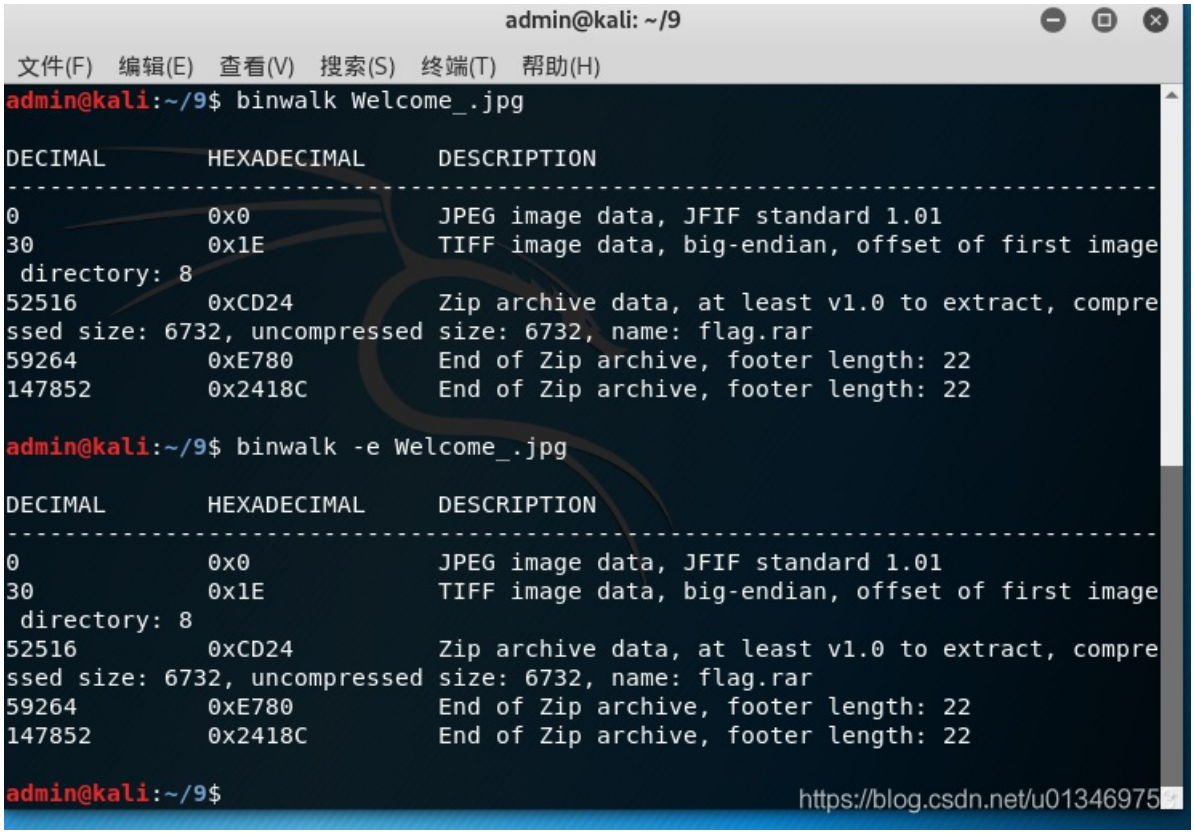
答案：

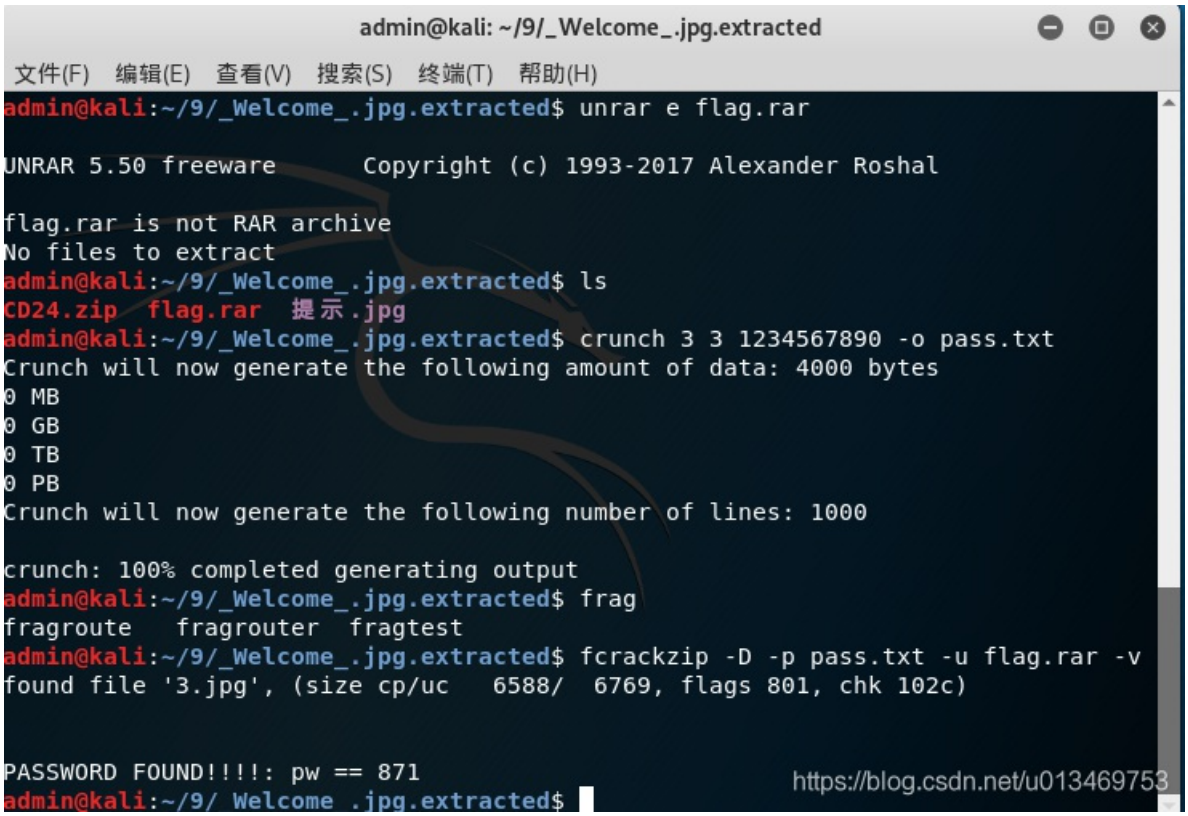
flag{053700357621}

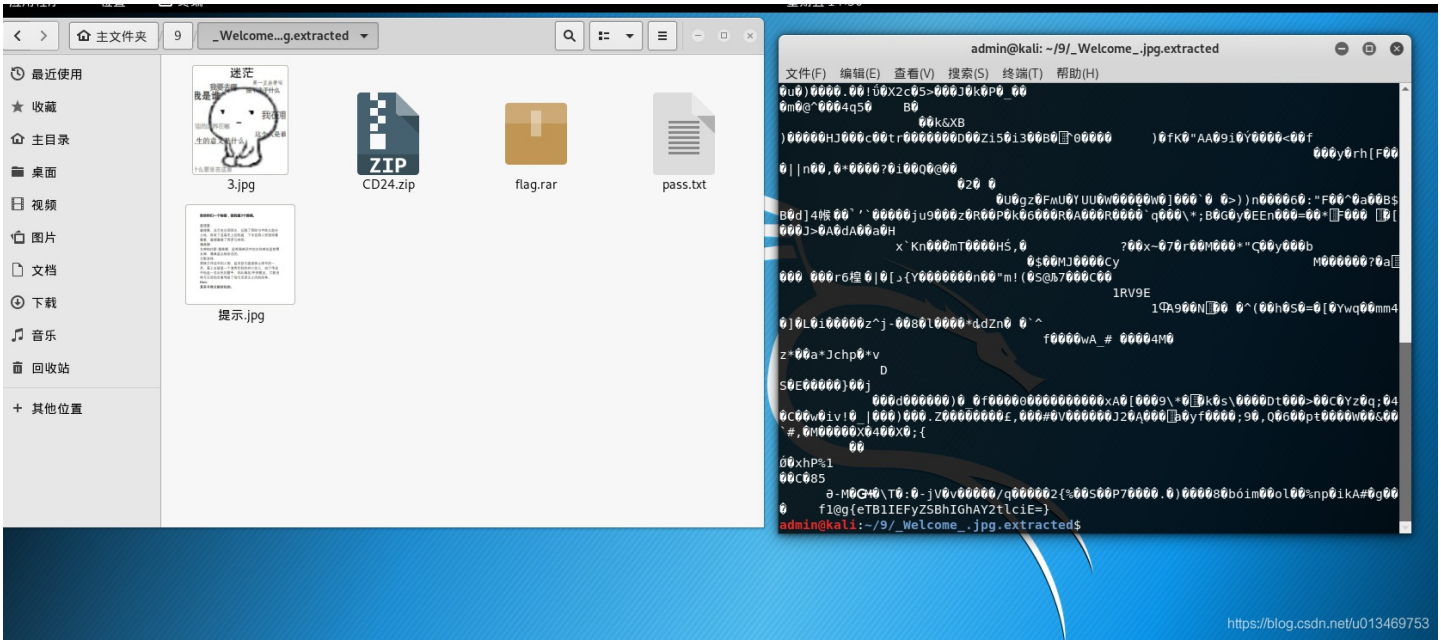
10.隐写2

解析：

```
binwalk Welcome_.jpg
binwalk -e Welcome_.jpg
ls
cd _Welcome_.jpg.extracted/
ls
unrar e flag.rar
ls
crunch 3 3 1234567890 -o pass.txt
fcrackzip -D -p pass.txt -u flag.rar -v
cat 3.jpg
```







cat 3.jpg之后，对做base解密，

base64解密：

https://base64.supfree.net/

http://tool.chinaz.com/tools/base64.aspx

`f1@g{eTB1IEFyZSBhIGhAY2tlciE=}`

输入：`eTB1IEFyZSBhIGhAY2tlciE=`

答案：

flg{y0u Are a h@cker!}

11、多种方法解决

解析：

先使用unzip 3.zip解压得到KEY.exe

cat KEY.exe

根据提示有一张二维码

cat KEY.exe，然后做base64转码

答案：

KEY{dca57f966e4e4e31fd5b15417da63269}

12.闪的好快

解析：

将git图片逐帧分解，扫描一堆二维码的到flag，

GIF分解工具：

在线分解https://tu.sioe.cn/gj/fenjie

本地分解：GifSplitter

答案：

SYC{F1aSh_so_f4sT}

13.Come_game

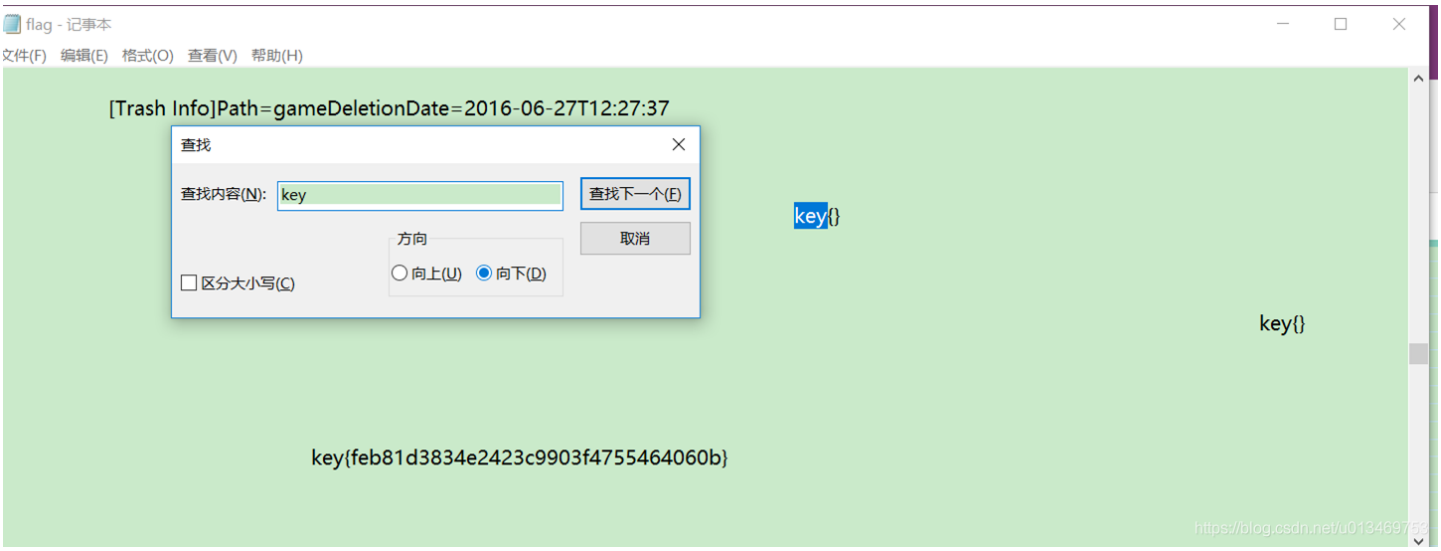
Bugku Come_game

参考链接

SYC{6E23F259D98DF153}

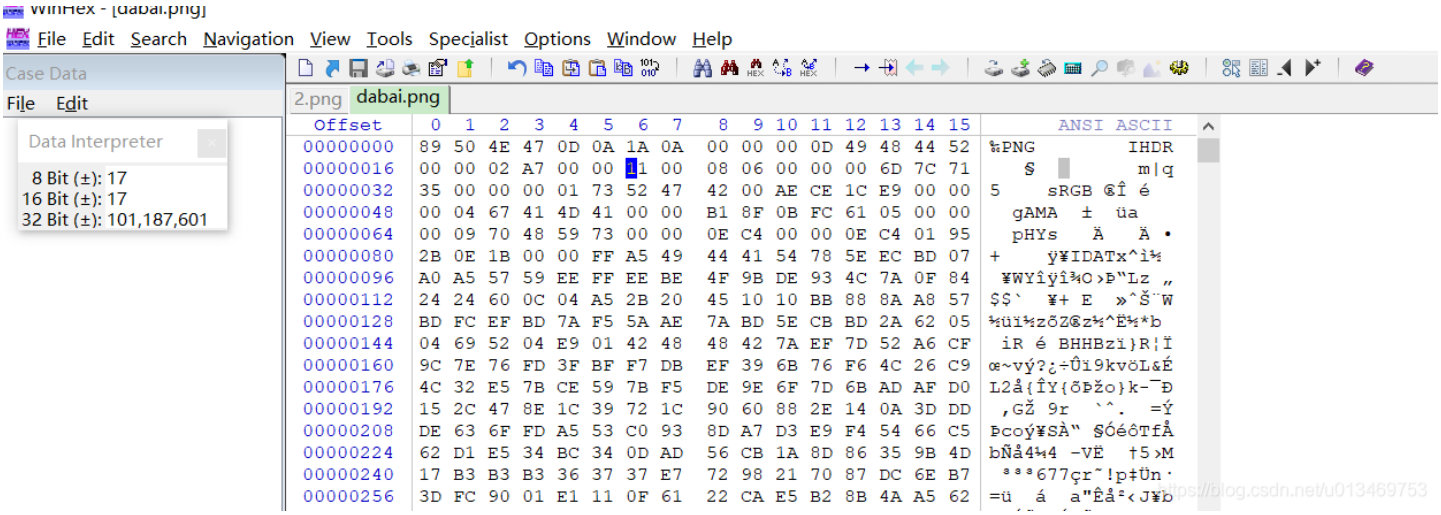
14.linux

```
tar -xvf 1.tar.gz
```

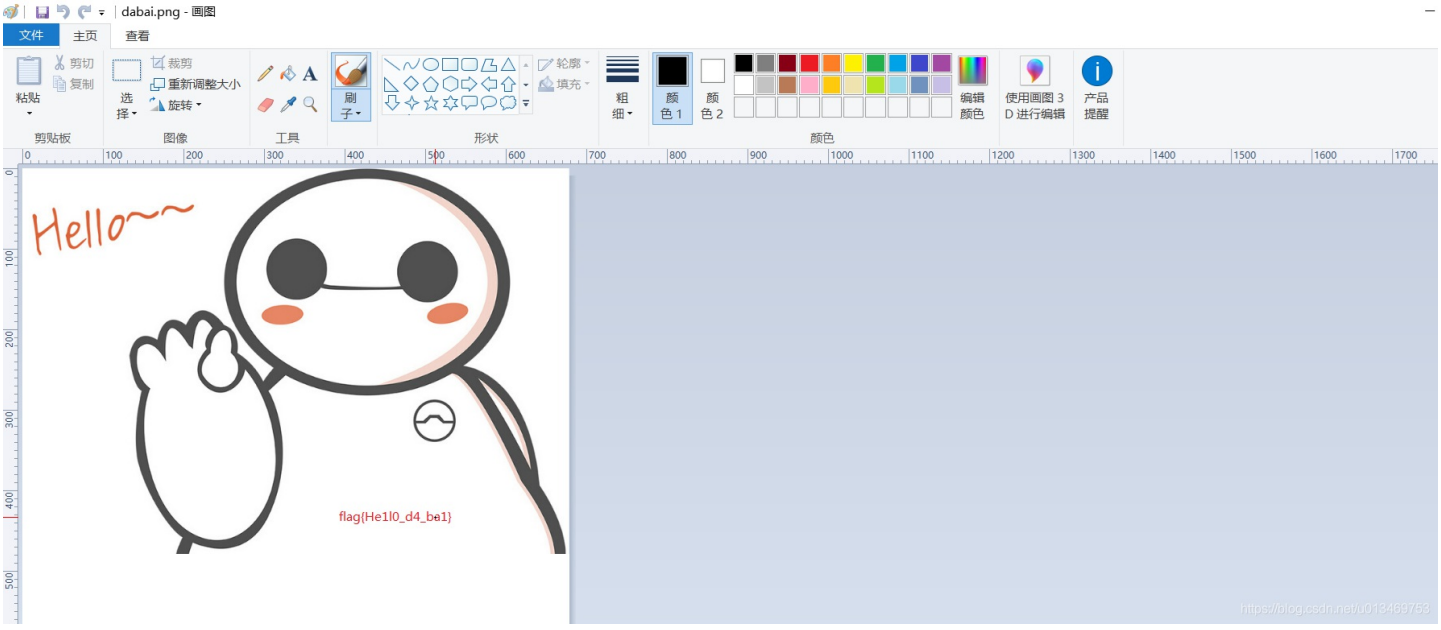


key{feb81d3834e2423c9903f4755464060b}

15、隐写3



保存，再次打开图片可知



flag{He1l0_d4_ba1}

16、做个游戏

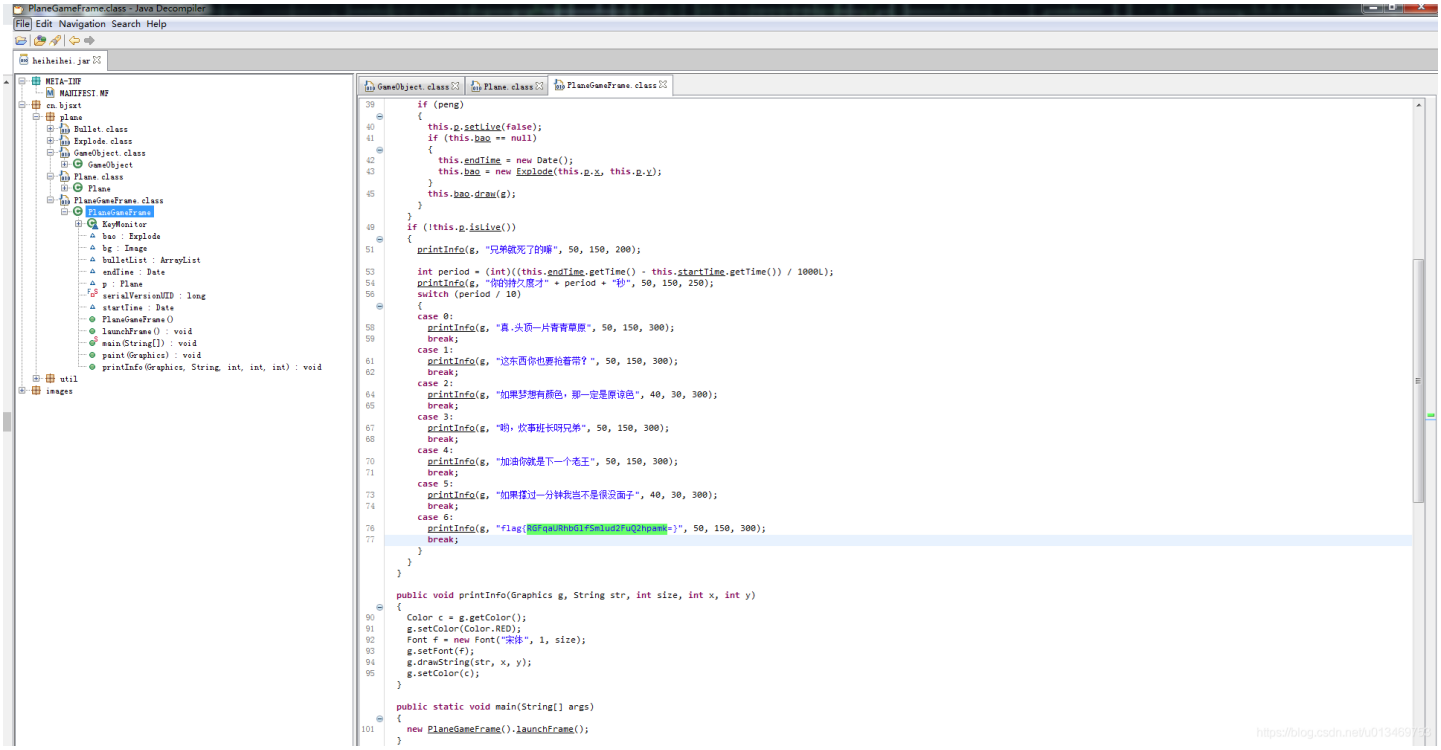
jd-gui工具

https://github.com/java-decompiler/jd-gui/releases

Java环境

https://www.java.com/zh_CN/download/windows-64bit.jsp

直接用jd-jui打开heihei.jar文件



flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

直接输入后提示错误，现对：`RGFqaURhbGlfSmlud2FuQ2hpamk=`做base64进行编码

http://tool.chinaz.com/Tools/Base64.aspx

`DajiDali_JinwanChiji`

所以flag为

flag{DajiDali_JinwanChiji}

17、想蹭网先解开密码

（1）生成长度为4位，且以“R开头+三位数字”的密码

```
crunch 4 4 -t R%%%
```

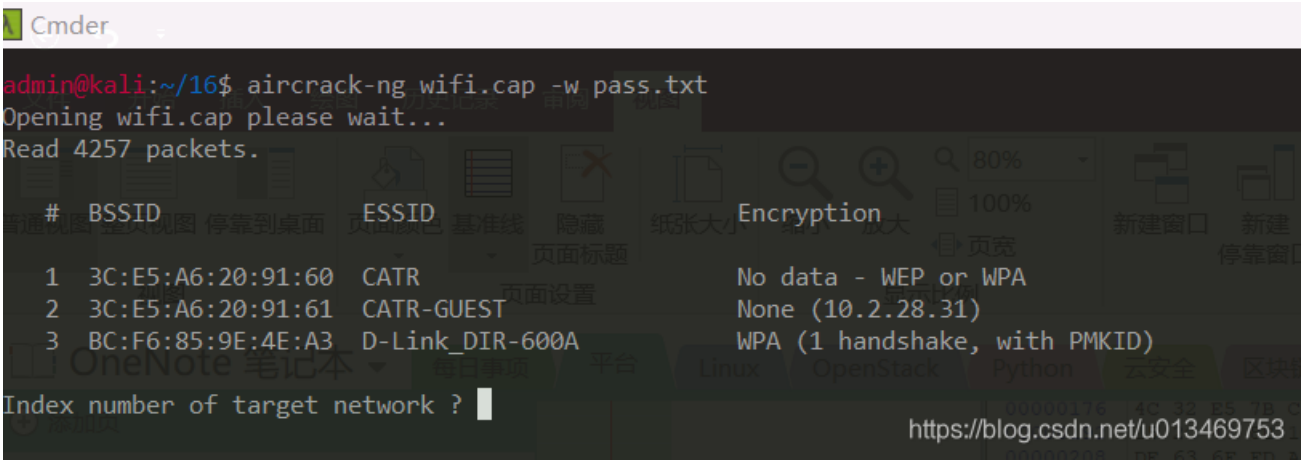
（2）生成长度为6的纯数字密码

```
crunch 6 6 -t %%%%%%
```

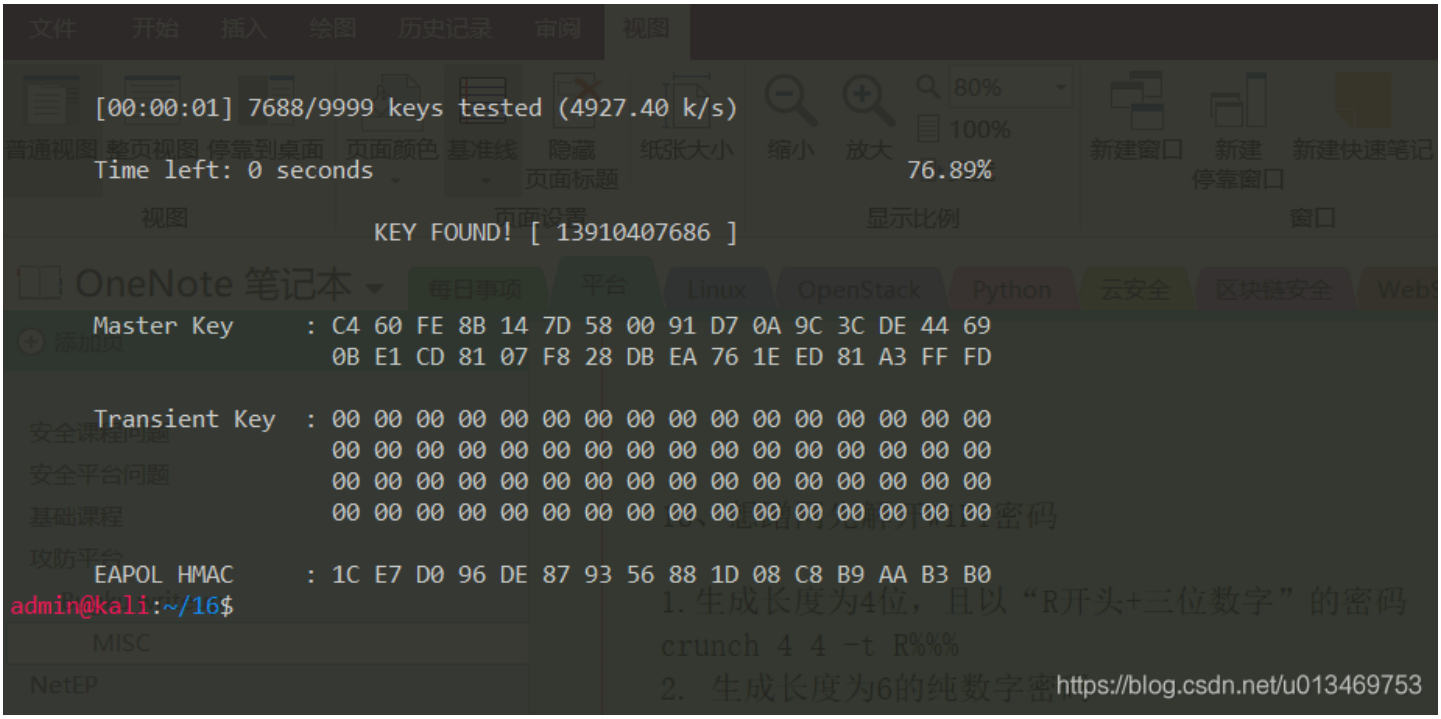
按提示生成1391040开头的手机号码并存入pass.txt

```
crunch 11 11 -t 1391040%%%% -o pass.txt
```

```
aircrack-ng wifi.cap -w pass.txt
```



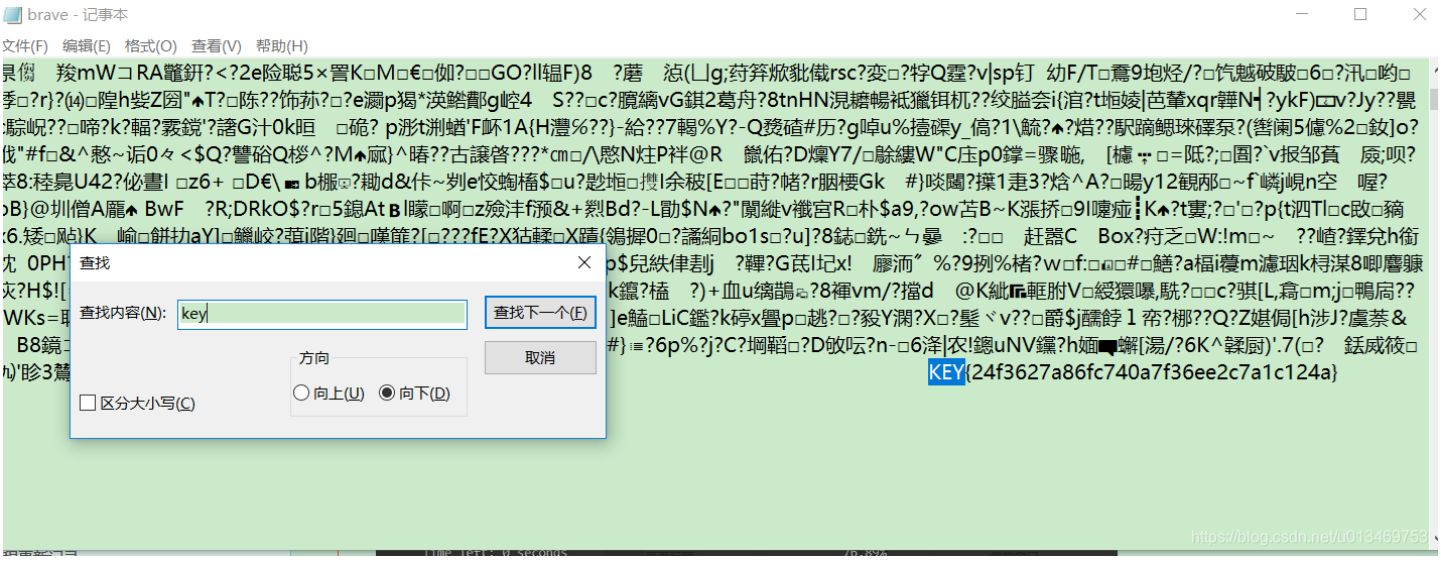
选择3，即WPA



flag{13910407686}

18、Linux2

依然是记事本打开



KEY{24f3627a86fc740a7f36ee2c7a1c124a}

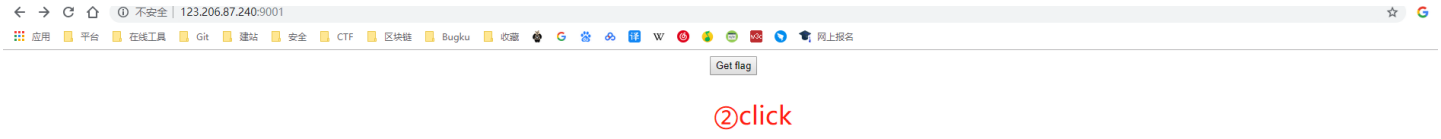
19、号被盗了

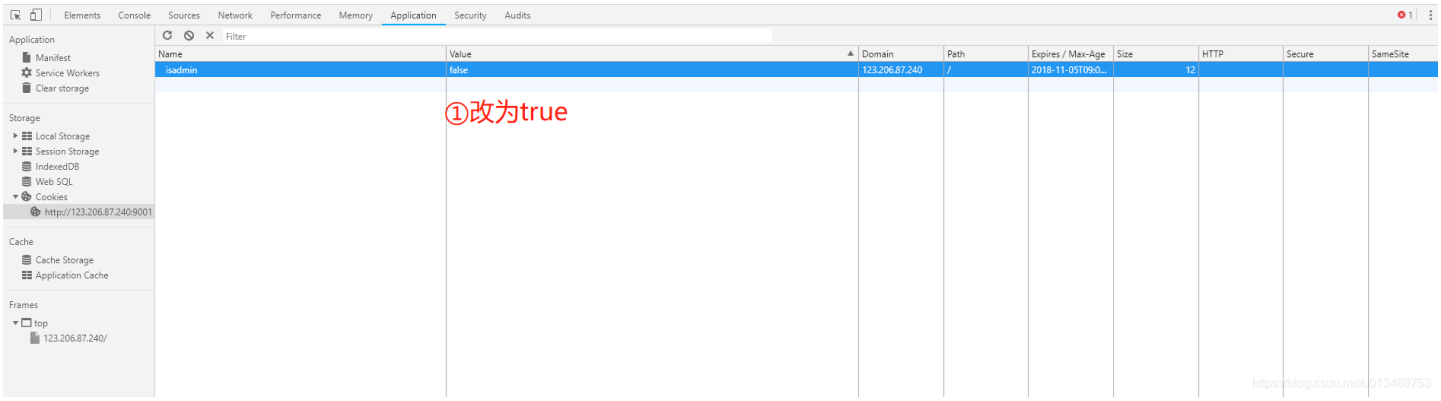
https://www.jianshu.com/p/9d8269ca2da4

http://123.206.87.240:9001/

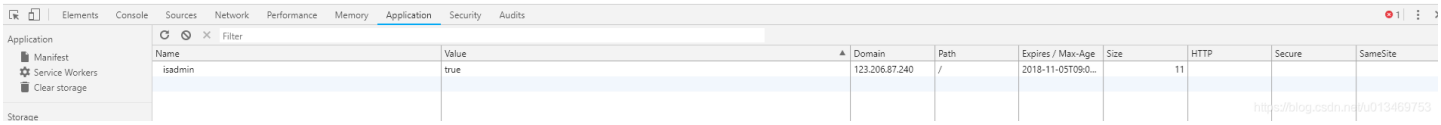
burp suite 将isadmin=false改为isadmin=true，
找到一个文件
http://123.206.87.240:9001/123.exe

或者





http://120.24.86.145:9001/123.exe



```
<html><head><style>
span {
 display: block;
          margin: auto;
          height: 25px;
          text-align: center;
          font-size: 30px;
   }
</style>

   <title>bugku</title>
   <link href="style.css" rel="stylesheet" type="text/css">
 </head>
 <body>
   <span>http://120.24.86.145:9001/123.exe</span>


</body></html>
```

下载后运行，并用wireshark抓包，

YmtjdGZ0ZXN0QDE2My5jb20=

解密：bkctftest@163.com

YTEyMzQ1Ng0KDQo=

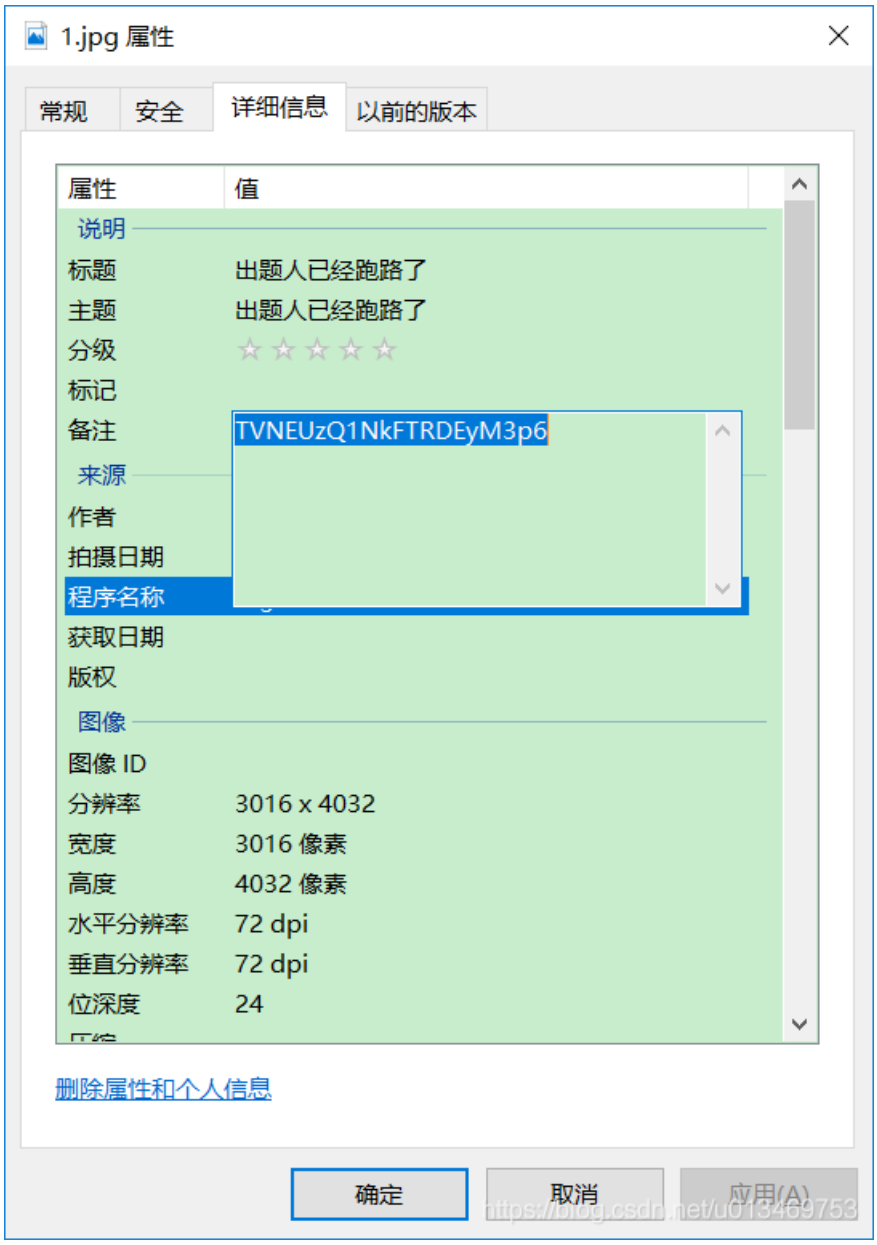
解密a123456

邮箱：红旗邮件

flag{182100518+725593795416}

20、细心的大象

解压，查看文件属性



TVNEUzQ1NkFTRDEyM3p6做base解密得到：MSDS456ASD123zz

http://tool.chinaz.com/Tools/Base64.aspx

1.jpg放到kali，

```
binwalk 1.jpg
```

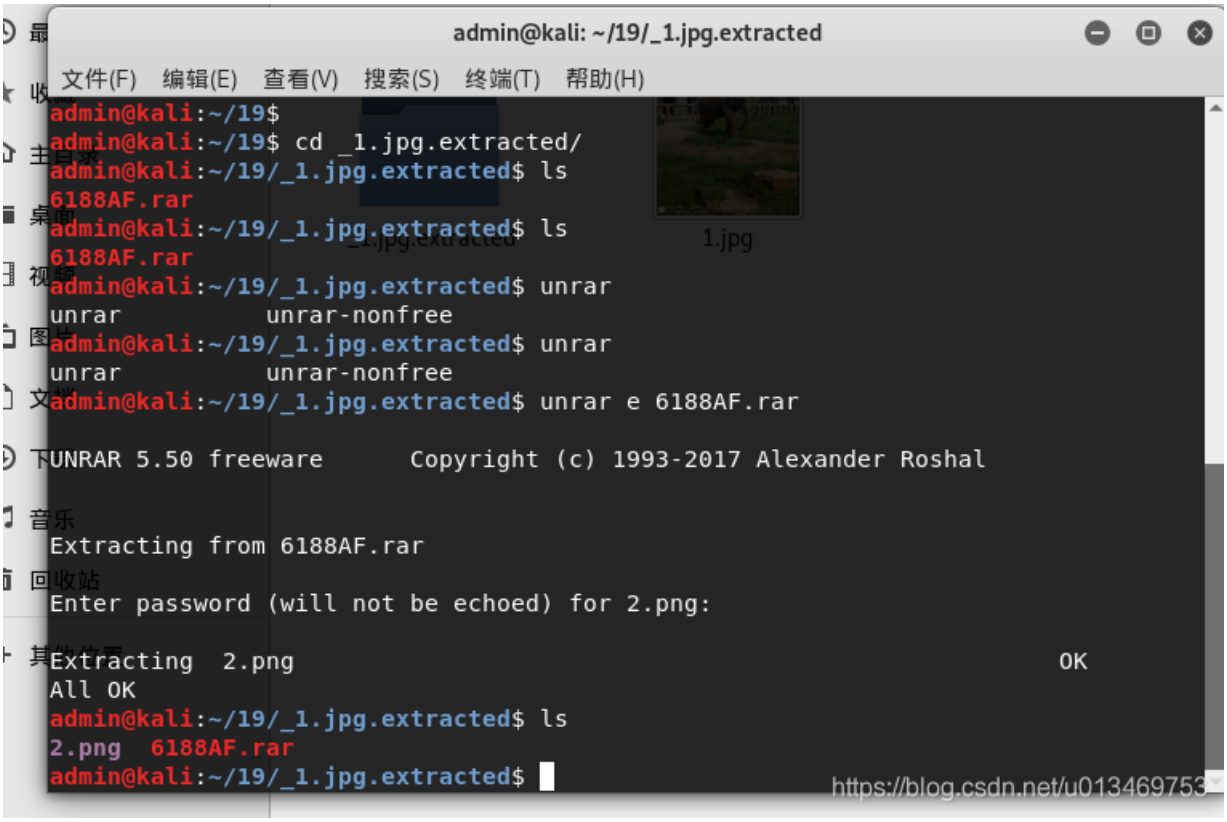
发现有压缩包，ok，执行分离：

```
binwalk -e 1.jpg
```

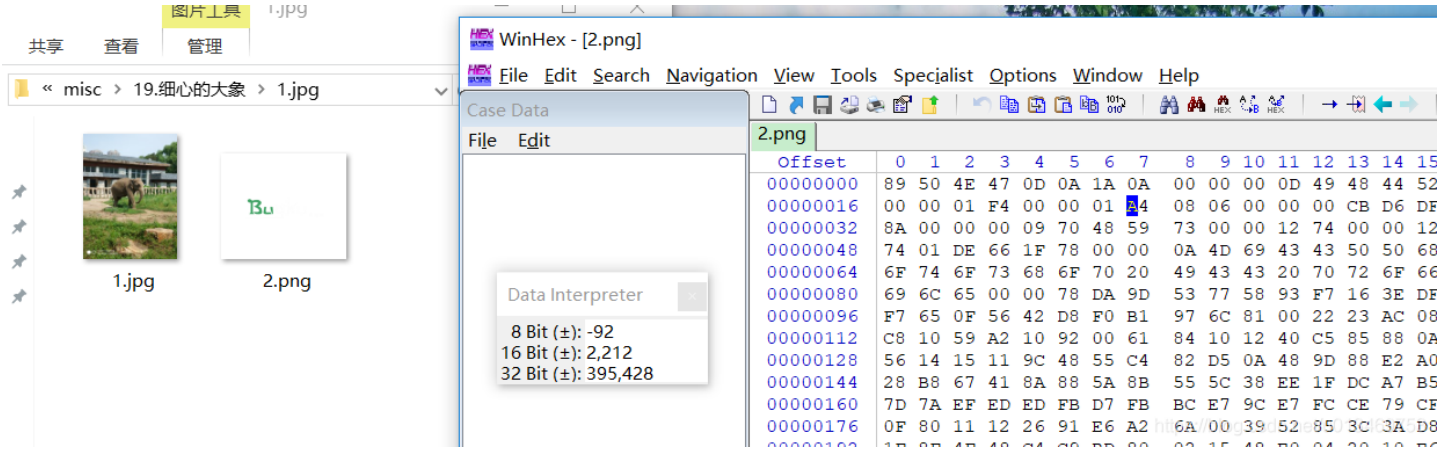
解压，

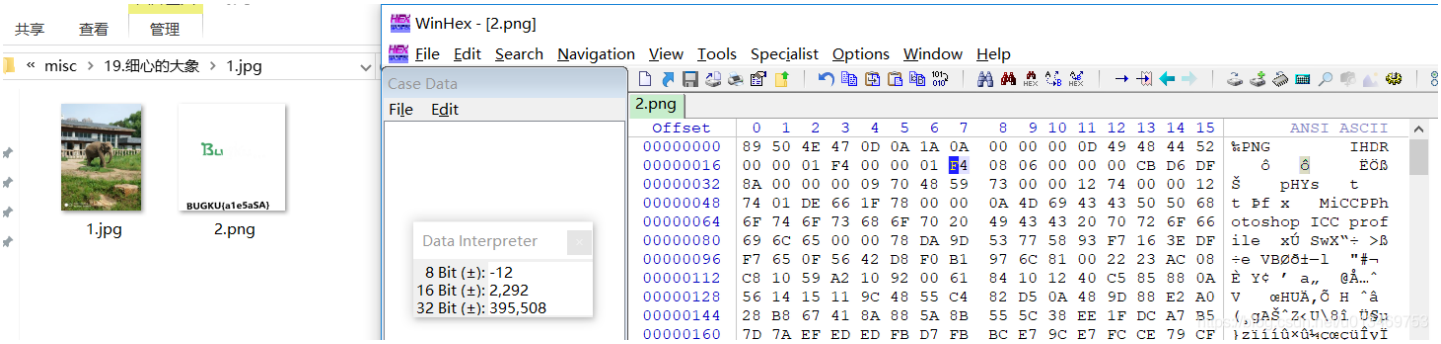
```
unrar e 6188AF.rar
```

输入密码：MSDS456ASD123zz



winhex分析，修改高度并保存，





BUGKU{a1e5aSA}

21、爆照

依然放进kali

```
binwalk 8.jpg
```

```
admin@kali:~/20$
admin@kali:~/20$ ls
8.jpg
admin@kali:~/20$ binwalk 8.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
40499         0x9E33          Zip archive data, encrypted at least v2.0 to extract, compr
essed size: 8362, uncompressed size: 92278, name: 8
48892         0xBEFC          Zip archive data, at least v2.0 to extract, compressed size
: 14906, uncompressed size: 15739, name: 88
63830         0xF956          Zip archive data, at least v2.0 to extract, compressed size
: 11129, uncompressed size: 18479, name: 888
74992         0x124F0         Zip archive data, at least v2.0 to extract, compressed size
: 10371, uncompressed size: 11782, name: 8888
85397         0x14D95         Zip archive data, at least v2.0 to extract, compressed size
: 6945, uncompressed size: 92278, name: 88888
92377         0x168D9         Zip archive data, at least v2.0 to extract, compressed size
: 6824, uncompressed size: 92278, name: 888888
99237         0x183A5         Zip archive data, at least v2.0 to extract, compressed size
: 7076, uncompressed size: 92278, name: 8888888
106350        0x19F6E         Zip archive data, at least v2.0 to extract, compressed size
: 8219, uncompressed size: 92278, name: 88888888
168452        0x29204         End of Zip archive, footer length: 22
```



```
foremost  8.jpg
```

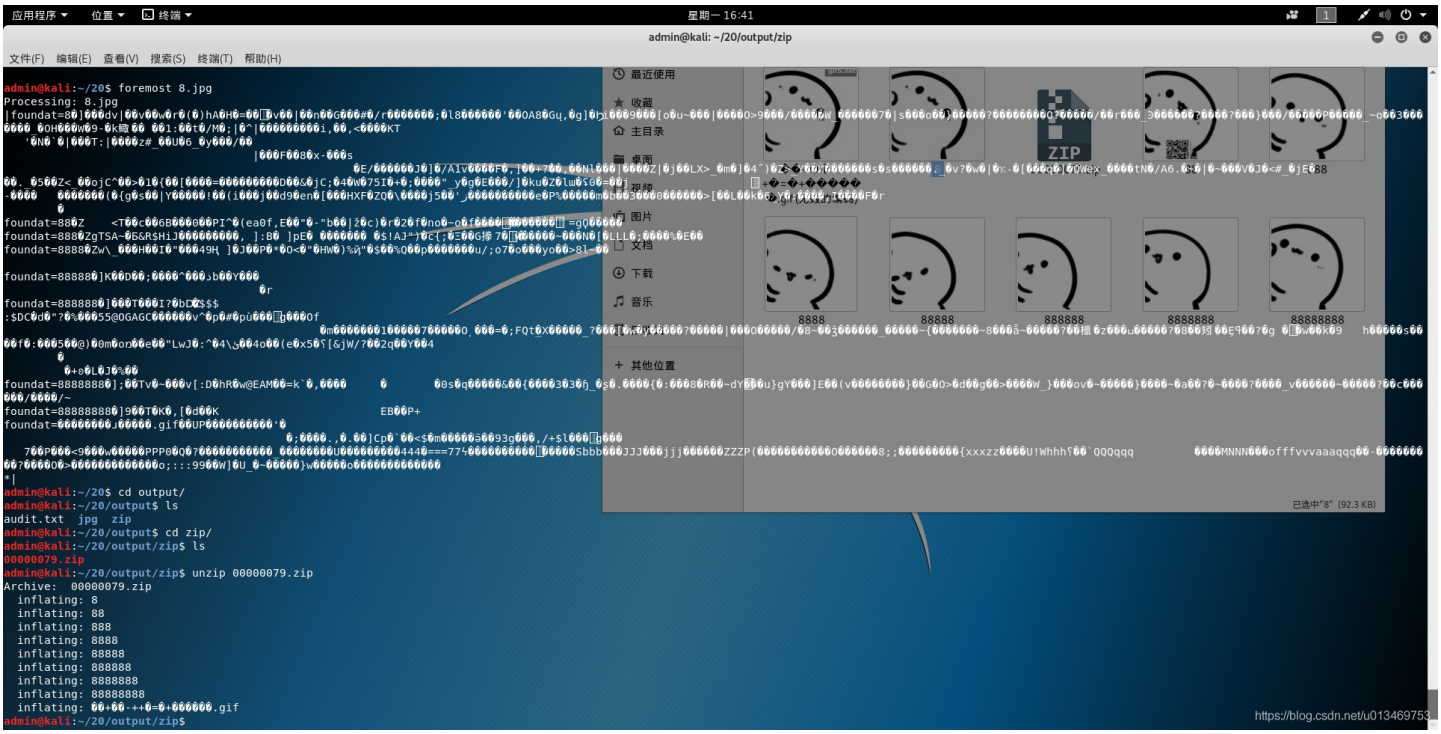
```
admin@kali:~/20$ foremost 8.jpg
Processing: 8.jpg
|foundat=8@]@@@dv|@@v@@w@r@(@)hA@H@=@@▓@v@@|@@n@@G@@@#@/r@@@@@@@;@l8@@@@@@'@@OA8@Gu,@g]@@
i@@@9@@@[o@u~@@@|@@@@O>9@@@/@@@@@W_@@@@@@7@|s@@@o@@}@@@@@?@@@@@@@O?@@@@@/@@r@@@_ↄ@@@@@@?
@@@@?@@@}@@@/@@@@@P@@@@@_~o@@3@@@@@@@_@OH@@@W@9-@k蝢@@ @@1:@@t@/M@;|@^|@@@@@@@@@i,@@,<@@@
@KT
   '@N@`@|@@@T:|@@@@z#_@@U@6_@y@@@/@@
                                    |@@@F@@8@x-@@@s
                                                  @E/@@@@@@J@]@/A1v@@@@F@,]@@+?@@,@@Nl@
@@|@@@@Z|@j@@LX>_@m@]@4˝)@Z>_Y@@И@@@@@@@s@s@@@@@@._@v?@w@|@ĸ-@[@@@q@|@QWex_@@@@tN@/A6.@~@
|@~@@@V@J@<#_@jE@
@@._@5@@Z<_@@ojC^@@>@1@{@@[@@@@=@@@@@@@@@D@@&@jC;@4@W@75I@+@;@@@@"_y@g@E@@@/]@ku@Z@lw@ʕ0@
=@@j
-@@@@   @@@@@@@(@{g@s@@▓Y@@@@@!@@(i@@@j@@d9@en@[@@@HXF@ZQ@\@@@@j5@@'ɹ@@@@@@@@@@e@P%@@@@@m
@b@@3@@@0@@@@@@>[@@L@@k@6_Y@:@@@@,I@@@@F@r
        @
foundat=88@Z    <T@@c@@6B@@@0@@PI^@(ea0f,E@@"@-"b@@|ž@c)@r@2@f@no@~o@f@@@@▓@@@@@@@▓ =gQ@@
@@@
foundat=888@ZgTSA~@Б&R$HiJ@@@@@@@@@, ]:B@ ]pE@ @@@@@@@ @$!AJ")@c{;@Ξ@@G撑 7@▓@@@@@@~@@@N@[
@LLL@;@@@@%@E@@
foundat=8888@Zw\_@@@H@@I@"@@@49Ң ]@J@@P@*@O<@"@HW@)%ӈ"@$@@%Q@@p@@@@@@@u/;o7@o@@@yo@@>8l~@
@

foundat=88888@]K@@D@@;@@@@^@@@ɔb@@Y@@@
                                  @r
foundat=888888@]@@@T@@@I?@bD@$$$
:$DC@d@"?@%@@@55@OGAGC@@@@@@v^@p@#@pù@@@▓g@@@Of
                                                 @m@@@@@@@1@@@@@7@@@@@O_@@@=@;FQt@X@@@@@_?@
@@[@w@y@@@@@?@@@@@|@@@O@@@@@/@8~@@ž@@@@@@_@@@@@~{@@@@@@@~8@@@ã~@@@@@?@@欄@z@@@ᴜ@@@@@?@8@@
矧@@Ę9@@?@g @▓w@@k@9   h@@@@@s@@@@f@:@@@5@@@)@@m@oɒ@@e@@"LwJ@:^@4\ʒ@@4o@@(e@x5@ʔ[&jW/?@@
2q@@Y@@4
        @
         @+ɵ@L@J@%@@
foundat=88888888@];@@Tv@~@@@v[:D@hR@w@EAM@@=k`@,@@@@     @       @0s@q@@@@@&@@{@@@@3@3@ƒ_@
ş@.@@@@{@:@@@8@R@@~dY▓@@u}gY@@@]E@@(v@@@@@@@}@@G@O>@d@@g@@>@@@@W_}@@@ov@~@@@@@}@@@@~@a@@
?@~@@@@?@@@@_v@@@@@@~@@@@@?@@c@@@@@@/@@@@/~
foundat=88888888@]9@@T@K@,[@d@@K                          EB@@P+
foundat=@@@@@@@@ɹ@@@@@.gif@@UP@@@@@@@@@@'@
                                        @;@@@@.,@.@@]Cp@`@@<$@m@@@@@ä@@93g@@@,/+$l@@@▓g
@@@
   7@@P@@@<9@@@w@@@@@PPP0@@Q@?@@@@@@@@@@@@ _@@@@@@@@U@@@@@@@@@444@===77ϟ@@@@@@@@@▓@@@@Sbbb
@@@JJJ@@@jjj@@@@@@ZZZP(@@@@@@@@@@@@O@@@@@@8;;@@@@@@@@@{xxxzz@@@@U!Whhhʕ@@`QQQqqq          @
@@@MNNN@@@offfvvvaaaqqq@@-@@@@@@@@@?@@@@O@>@@@@@@@@@@@@@@o;:::99@@W]@U_@~@@@@@}w@@@@@o@@@@
@@@@@@@@@@
```

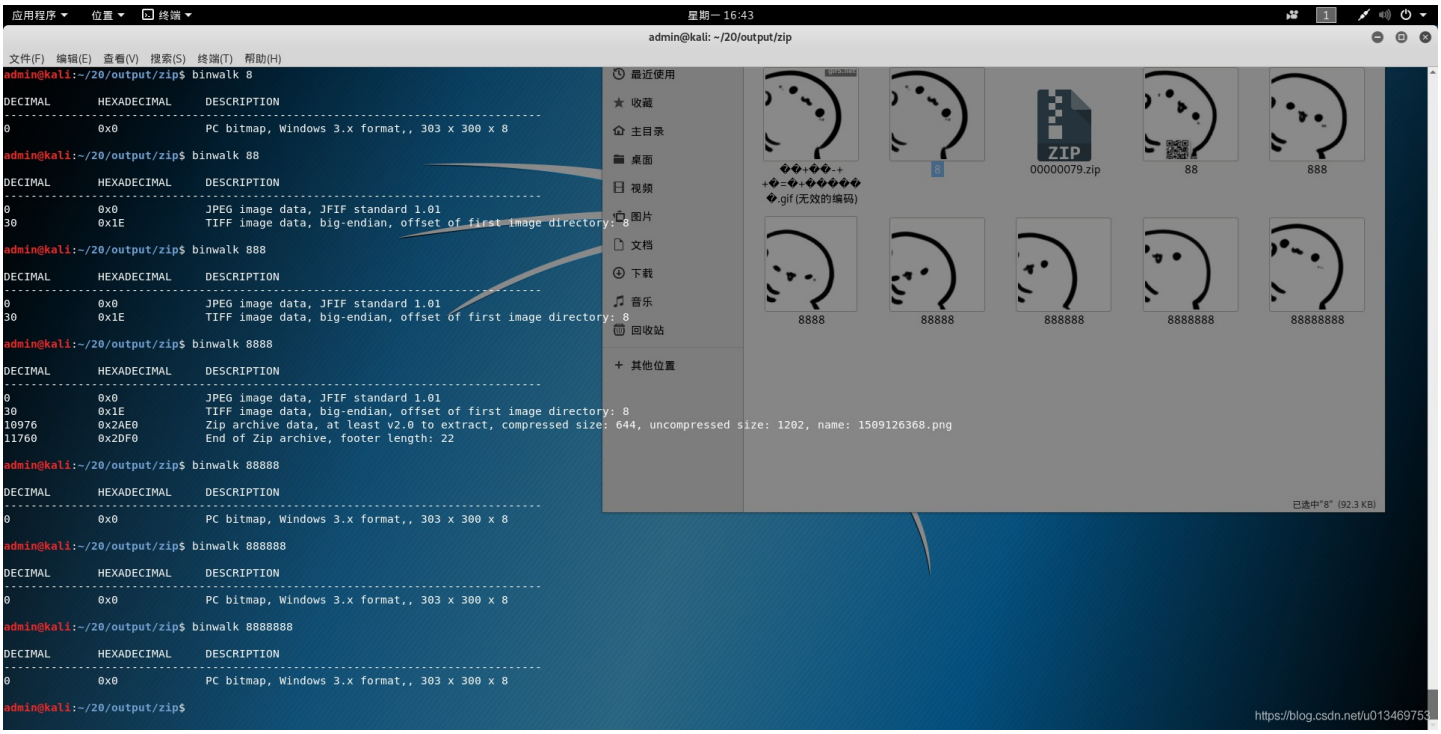
```
admin@kali:~/20$ cd output/
admin@kali:~/20/output$ ls
audit.txt  jpg  zip
```

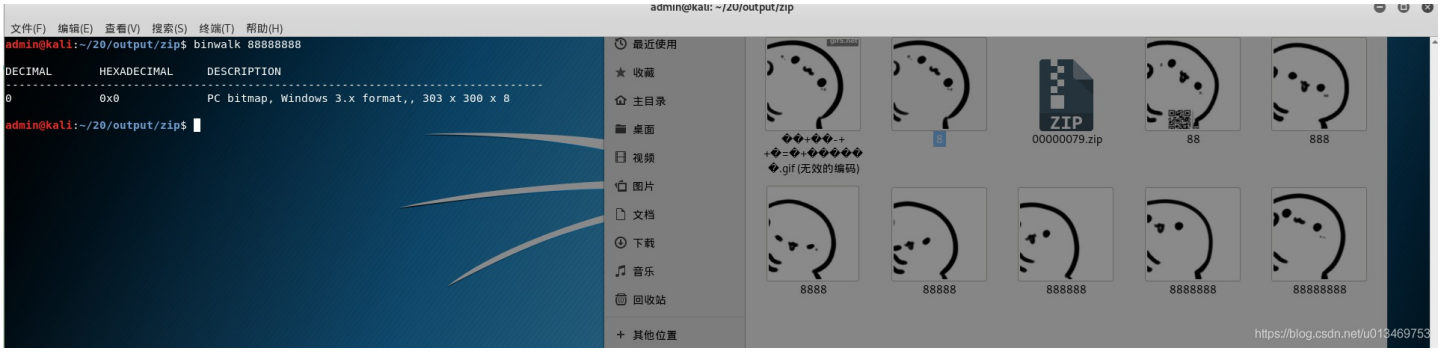


```
admin@kali:~/20/output/zip$ ls
00000079.zip
admin@kali:~/20/output/zip$ unzip 00000079.zip
Archive:  00000079.zip
  inflating: 8
  inflating: 88
  inflating: 888
  inflating: 8888
  inflating: 88888
  inflating: 888888
  inflating: 8888888
  inflating: 88888888
  inflating: ???+???-+++?=?+???????.gif
admin@kali:~/20/output/zip$
```

逐个查看文件





现在分析：

（1）8

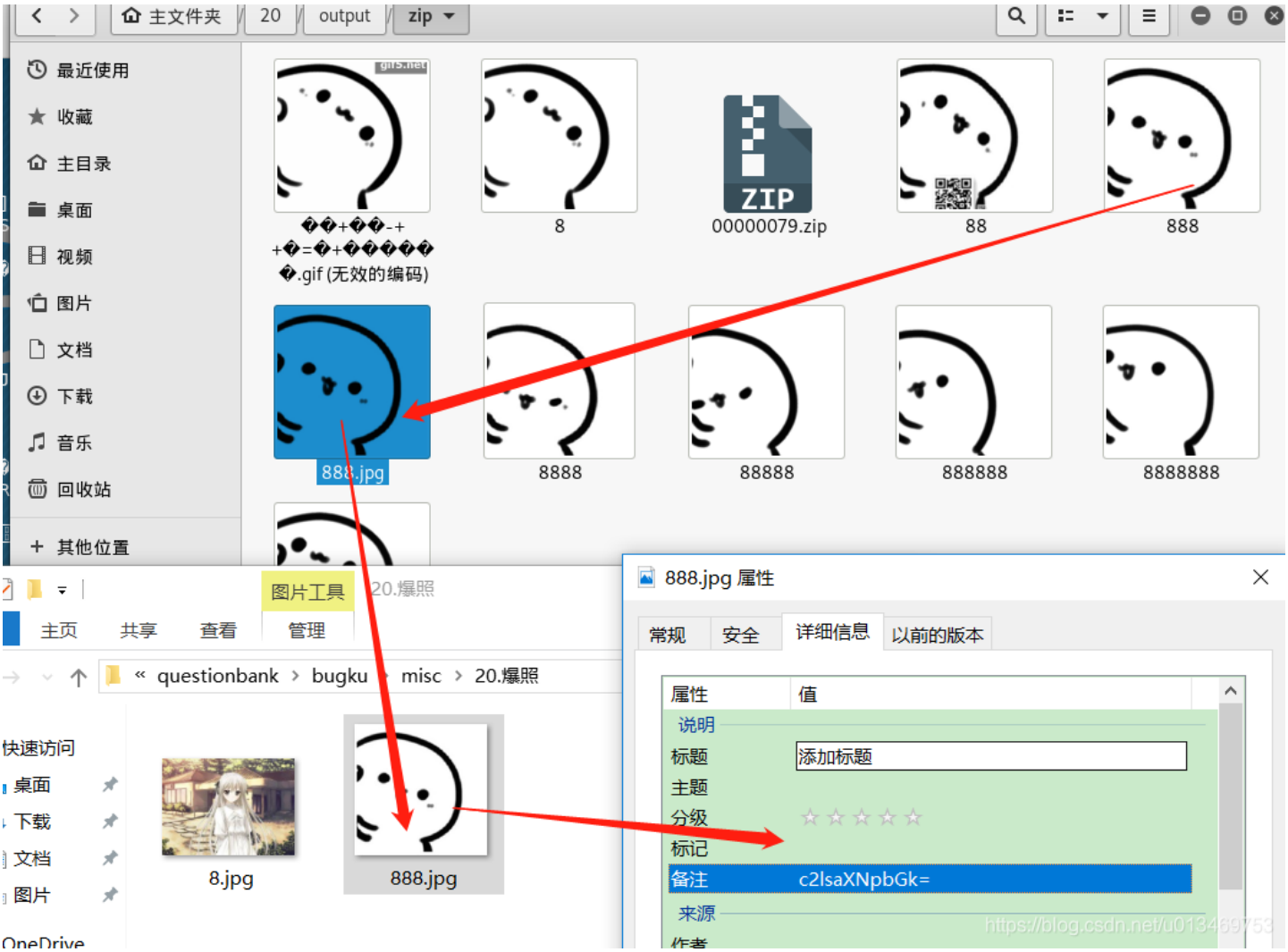
就一张图

（2）88

扫描二维码得到：

bilibili

（3）888

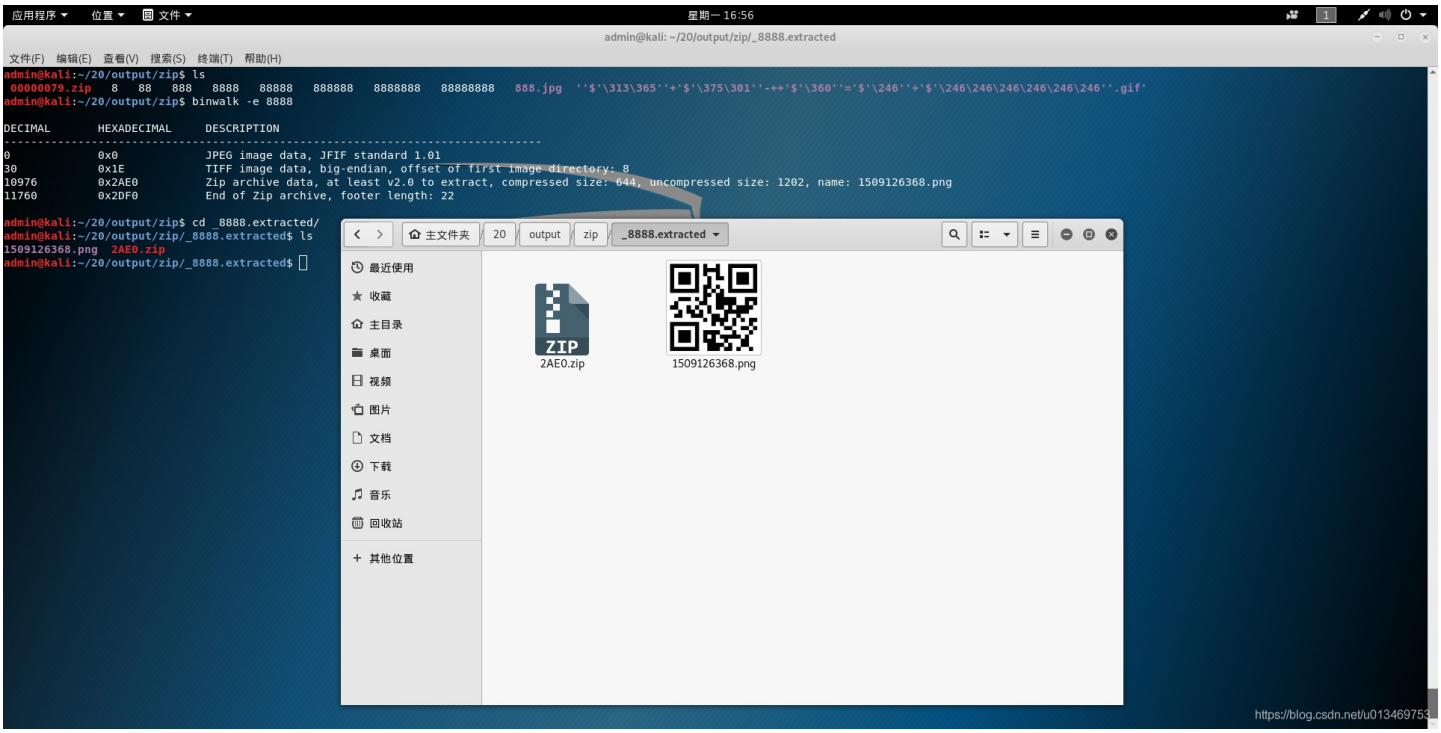


`c2lsaXNpbGk=`进行base64解密

得到：silisili

（4）8888

```
bninwalk -e 8888
```



扫描的到：panama

根据gif提示：愉快的排序吧

猜测flag为：flag{bilibili_silisili_panama}

22、猫片（安恒）

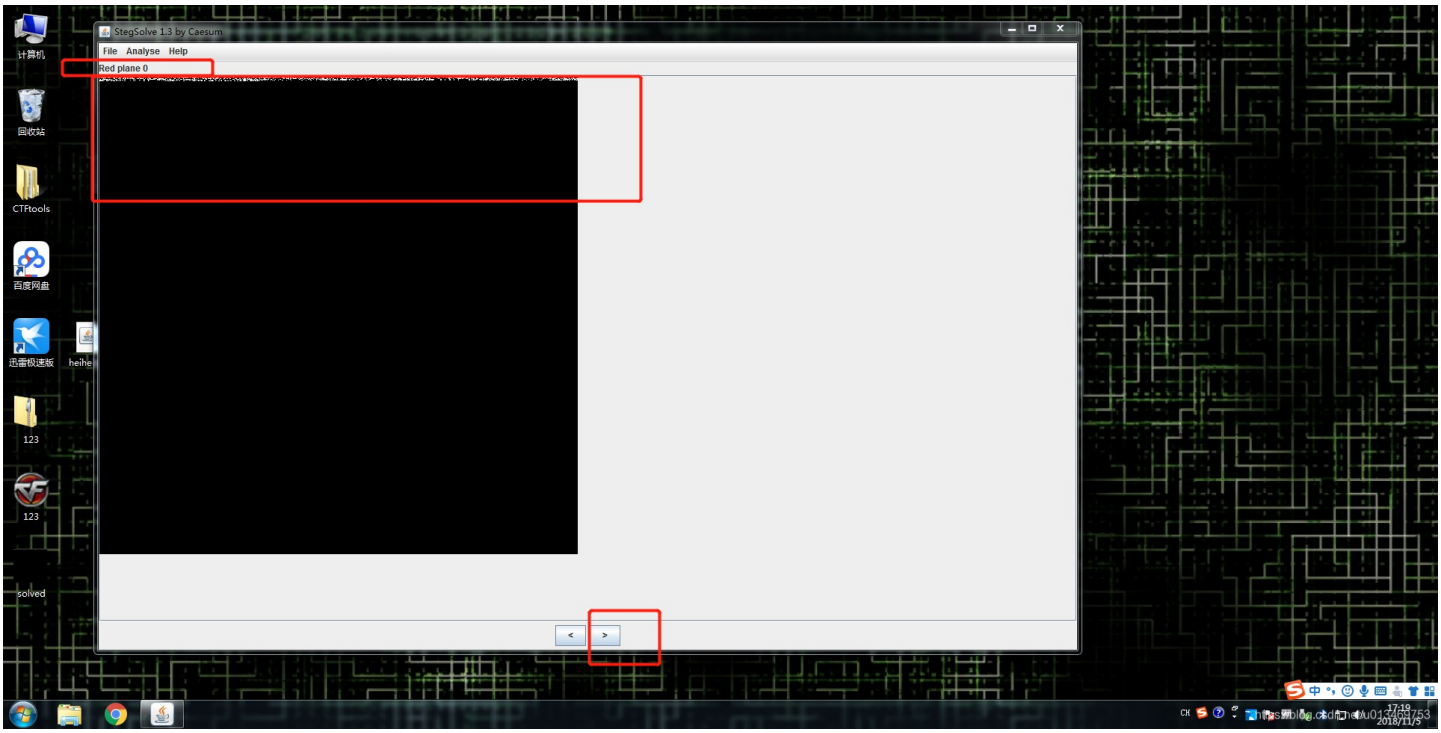
bugkuCTF——猫片(安恒)

来自 https://blog.csdn.net/x947955250/article/details/81482471

https://www.jianshu.com/p/f84b33bf04a7

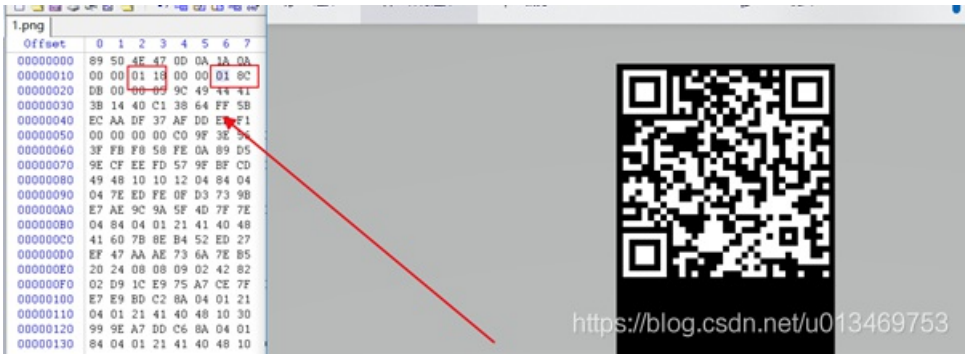
使用工具
http://www.caesum.com/handbook/Stegsolve.jar

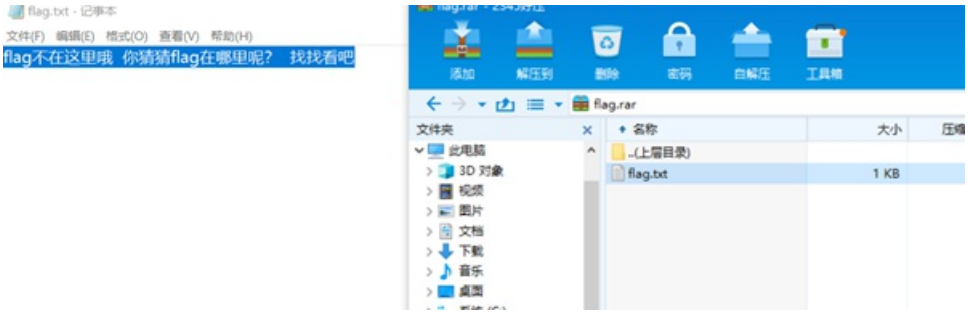
来自 https://github.com/manisashank/stegsolve/blob/master/process to install stegsolve



疑似二维码，保存当前为png
使用winhex打开，修改高度

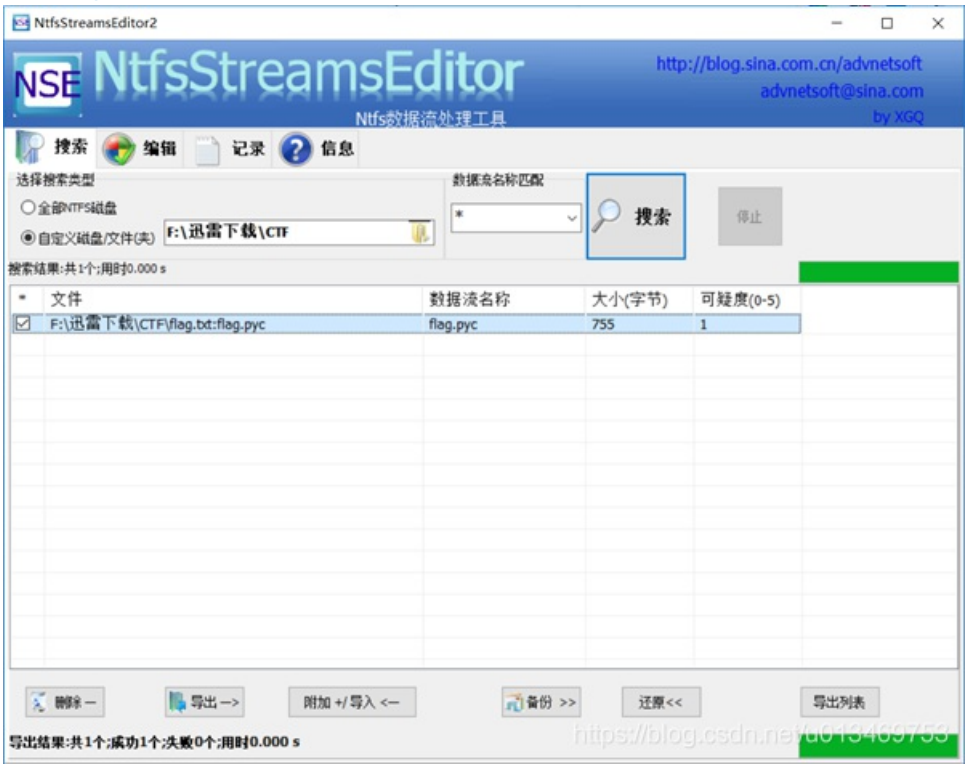
```
01 18 00 00 01 8C
```





ntfstreamseditor 查看数据流

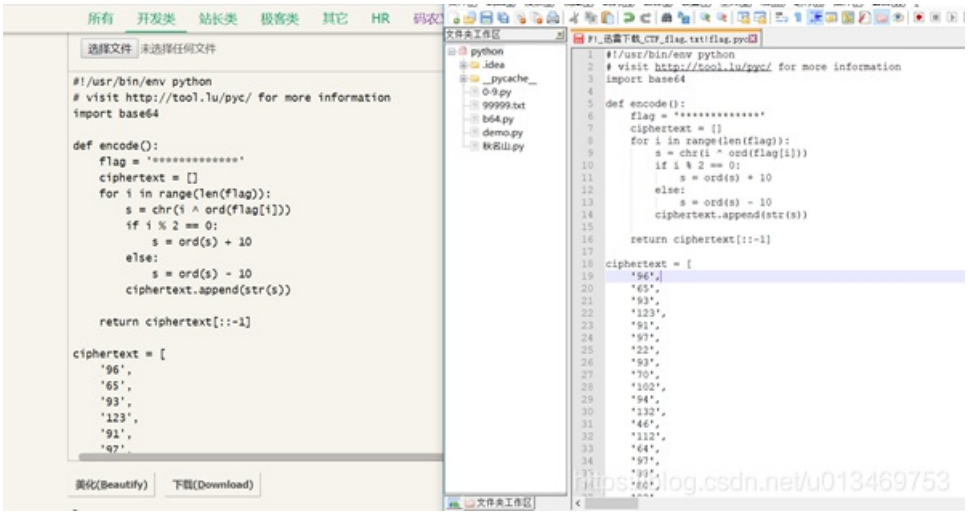
来自 https://www.jianshu.com/p/f84b33bf04a7



pyc解密

在线反编译

https://tool.lu/pyc/



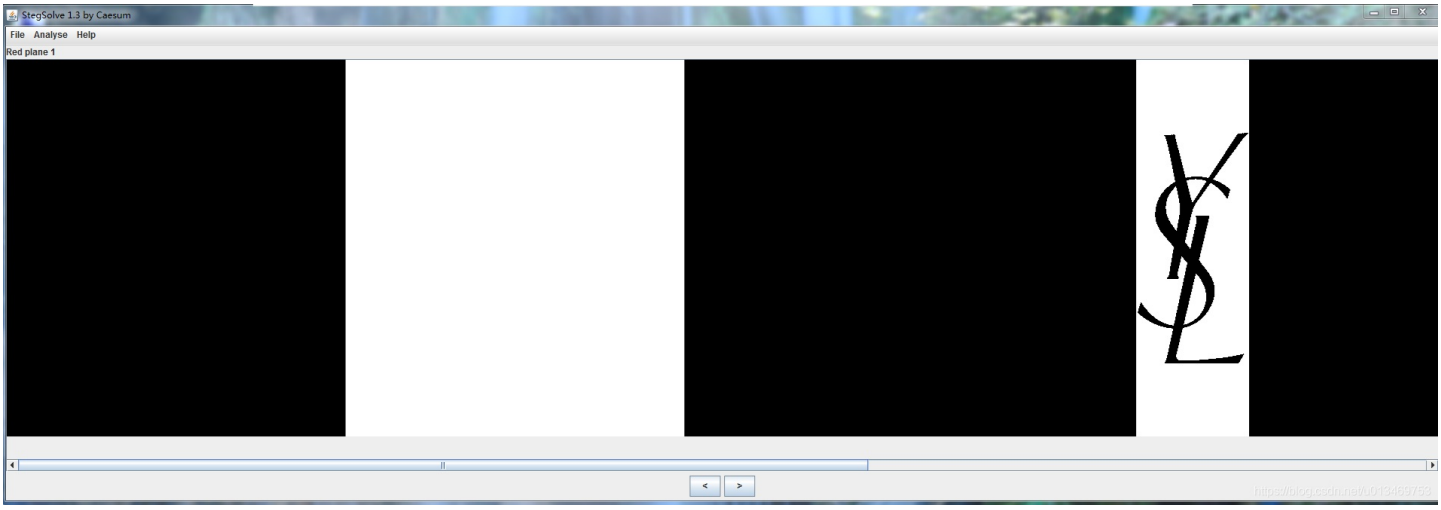
flag{Y@e_Cl3veR_C1Ever!}

23.多彩

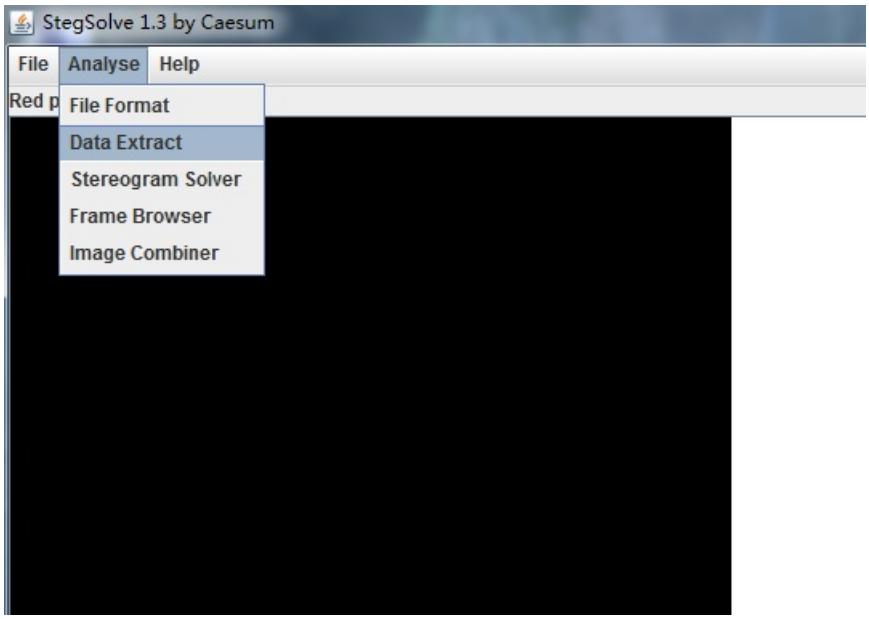
Lipstick

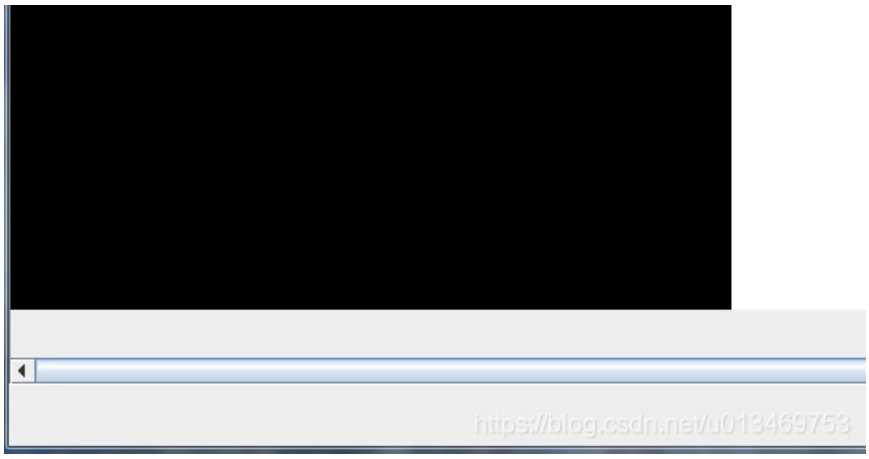
来自 https://www.secpulse.com/archives/69465.html

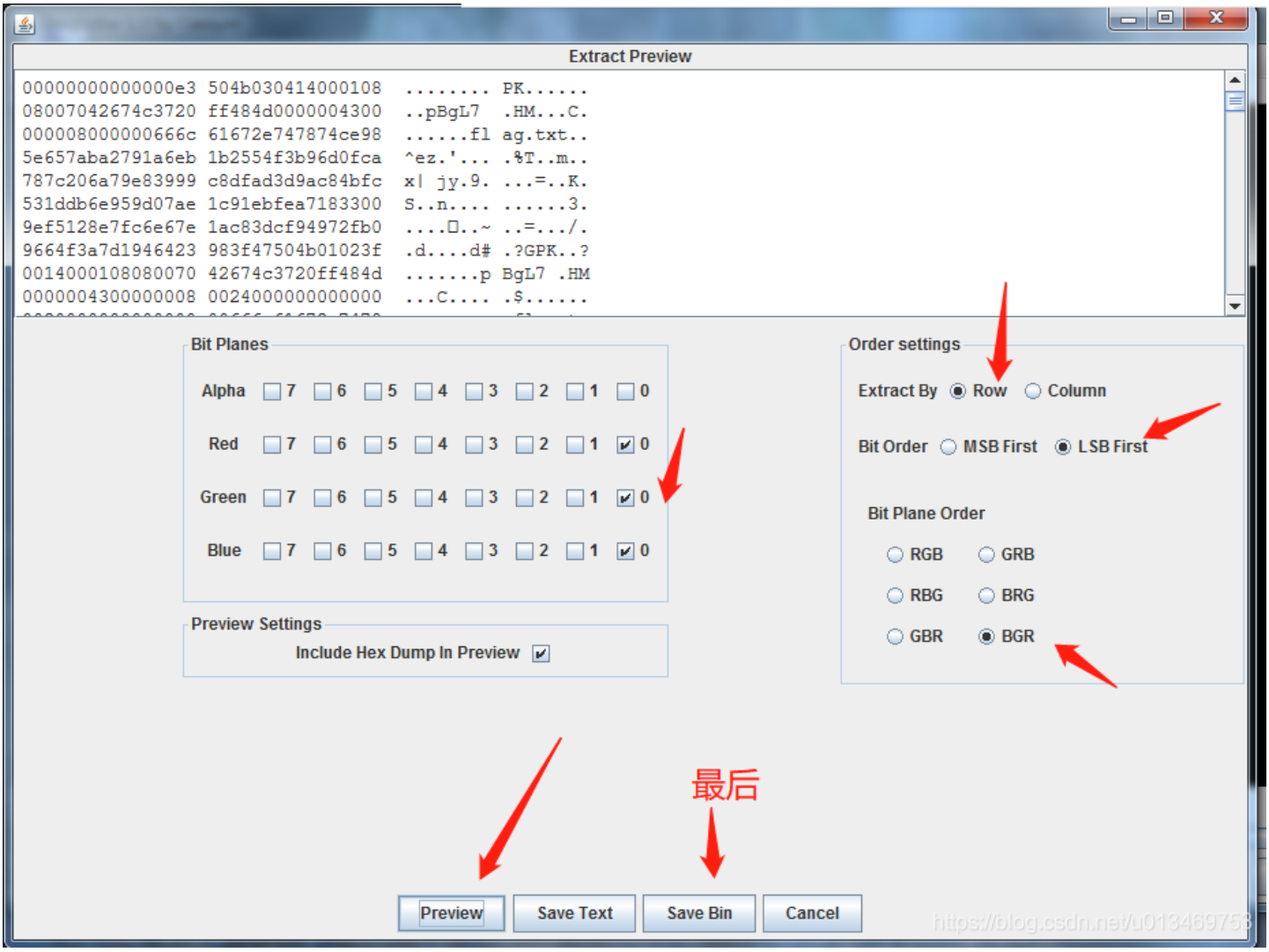
直接用Stegsolve file/open，



发现YSL口红品牌，继续深入，使用Analyse




https://blog.csdn.net/u013469753


Extract Preview
00000000000000e3 504b030414000108 .... PK.....
08007042674c3720 ff484d0000004300 ..pBgL7 .HM...C.
000008000000666c 61672e747874ce98 ......fl ag.txt..
5e657aba2791a6eb 1b2554f3b96d0fca ^ez.'... .%T..m..
787c206a79e83999 c8dfad3d9ac84bfc x| jy.9. ...=..K.
531ddb6e959d07ae 1c91ebfea7183300 S..n.... ......3.
9ef5128e7fc6e67e 1ac83dcf94972fb0 ....□..~ ..=.../.
9664f3a7d1946423 983f47504b01023f .d....d# .?GPK..?
0014000108080070 42674c3720ff484d ....p BgL7 .HM
0000004300000008 0024000000000000 ...C.... .$......
Bit Planes
Alpha 7 6 5 4 3 2 1 0
Red 7 6 5 4 3 2 1 0
Green 7 6 5 4 3 2 1 0
Blue 7 6 5 4 3 2 1 0
Preview Settings
Include Hex Dump In Preview
Order settings
Extract By Row Column
Bit Order MSB First LSB First
Bit Plane Order
RGB GRB
RBG BRG
GBR BGR
最后
Preview
Save Text
Save Bin
Cancel
https://blog.csdn.net/u013469753

SaveBin林村为一个zip压缩包

直接解压有错，放到kali

尝试伪加密，无果。于是整个过程就剩下一个密码。一般来说图片隐写的话，要么是二进制里藏了东西，要么就是图形藏了东西。这里二进制里藏了zip包，剩下的密码就只能从图形里入手。

图形里是21个颜色格，分别取色

`BC0B28 D04179 D47A6F C2696F EB8262 CF1A77 C0083E BC0B28 BC0B28 D13274 6A1319 BC0B28 BC0B28 D4121D D75B59 DD8885 CE0A4A D4121D 7E453A D75B59 DD8885`

来自 https://www.secpulse.com/archives/69465.html

YSL色号

https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL

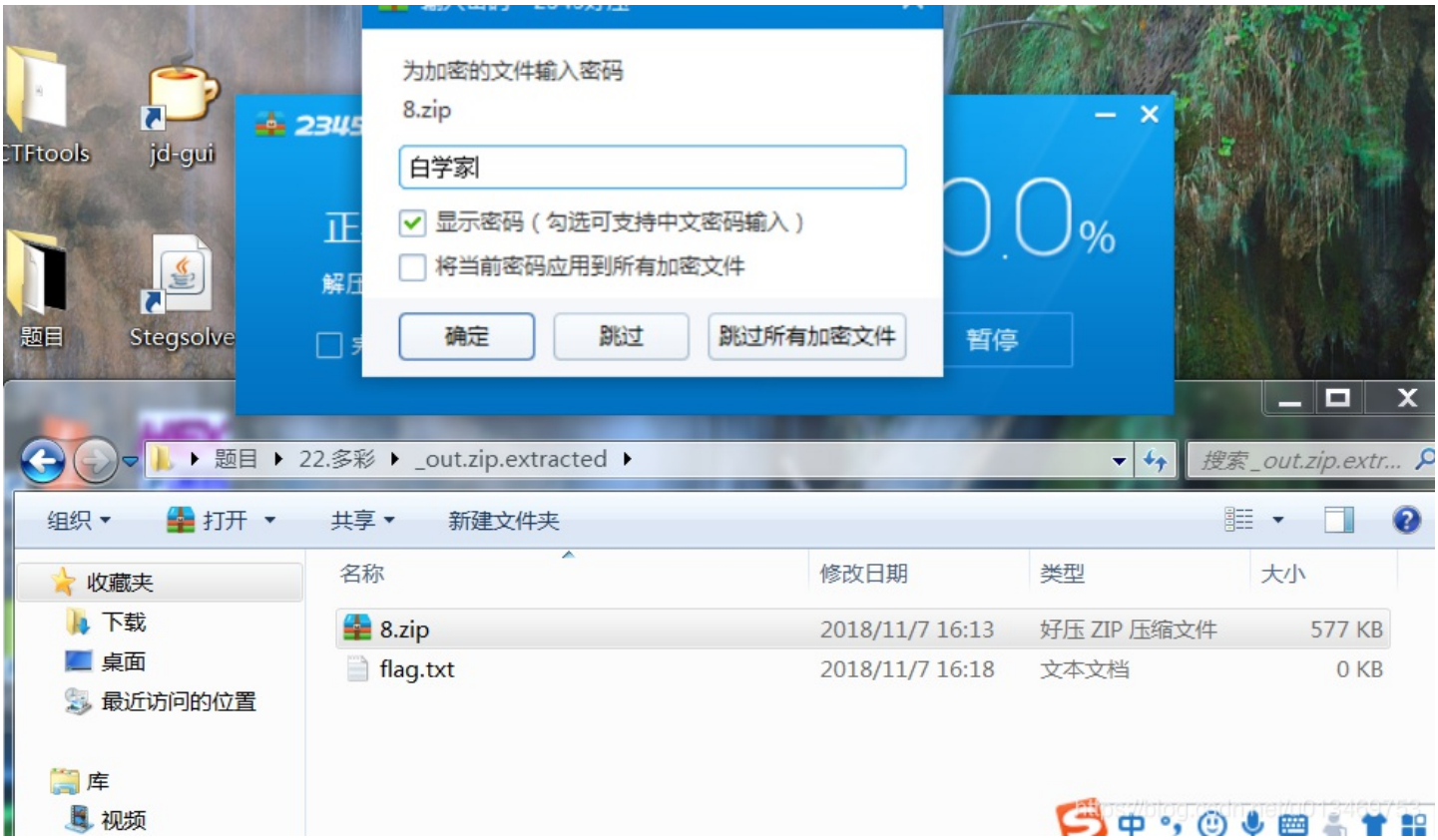
```
# -*- coding:utf8 -*-
__author__='pcat@chamd5.org'
import requestsimport re
import libnum
def foo():
url=r'https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL'
cont=requests.get(url).content
# print cont
pattern=r'YSL_color=(.*?)%20[sS]*?background-color: #(.*?)"'
rst=re.findall(pattern,cont)
dYSL={}
for num,color in rst:
dYSL[color]=int(num.lstrip('0'))
lst=['BC0B28','D04179','D47A6F','C2696F','EB8262', 'CF1A77','C0083E','BC0B28','BC0B28','D13274', '6A1319','BC0B2
8','BC0B28','D4121D','D75B59', 'DD8885','CE0A4A','D4121D','7E453A','D75B59', 'DD8885']
flag=''.join('{:b}'.format(dYSL[i]) for i in lst)
print libnum.b2s(flag)
pass
if __name__ == '__main__':
foo()
print 'ok'
```

打印出来是
白学家，即，解压密码。

```
7z x out.zip
```

使用命令解压出错可能是编码格式的问题

这里使用2345好压打开，来自 https://www.secpulse.com/archives/69465.html



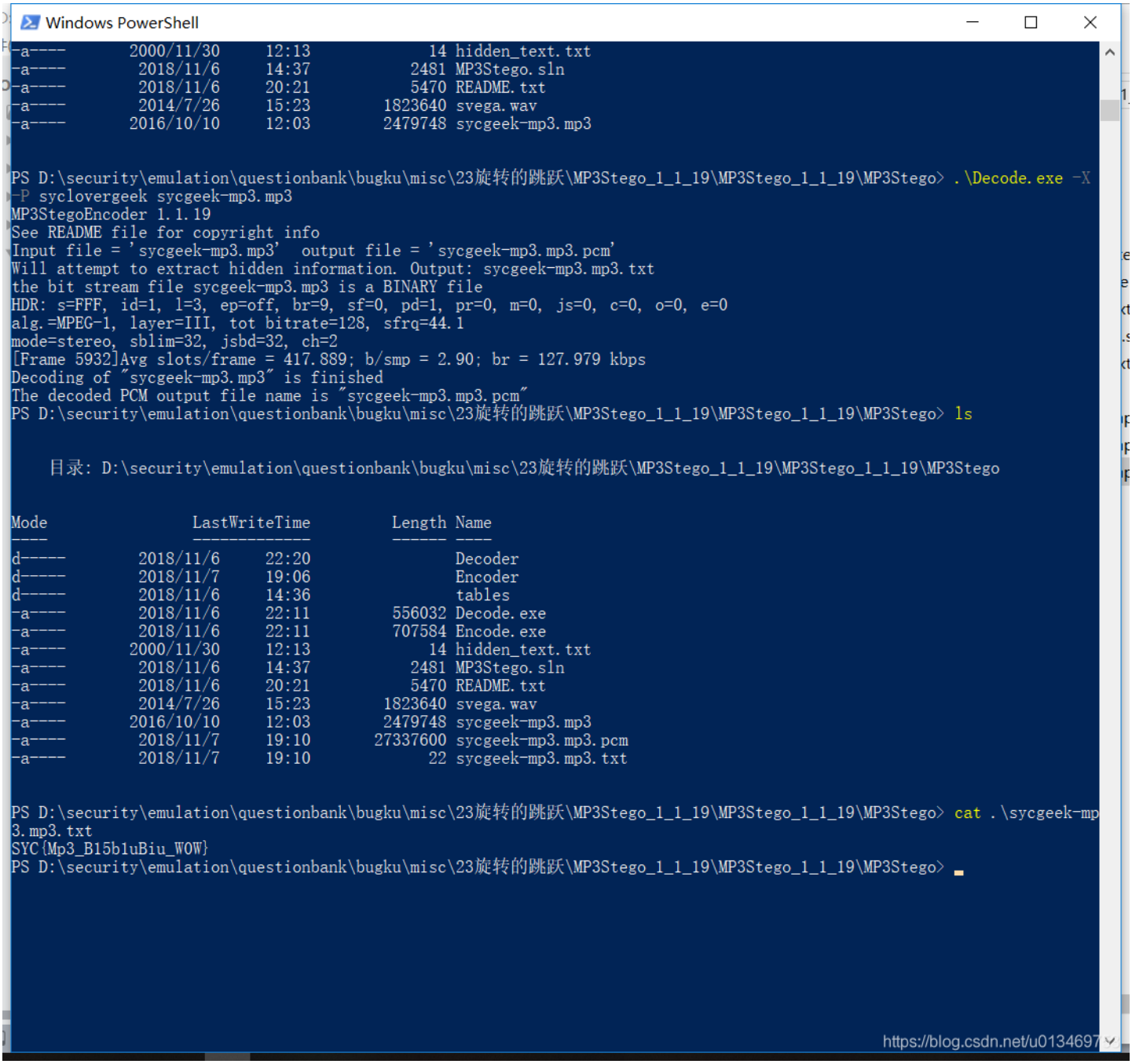
flag{White_Album_is_Really_worth_watching_on_White_Valentine's_Day}

24、旋转的跳跃

熟悉的声音中貌似又隐藏着啥，key：syclovergeek题目来源：第七季极客大挑战

```
wget https://www.petitcolas.net/fabien/software/MP3Stego_1_1_19.zip
```

```
.\Decode.exe -X -P syclovergeek sycgeek-mp3.mp3
```



SYC{Mp3_B15b1uBiu_W0W}

25.普通的二维码

直接解压，使用微信扫描得到

使用winhex打开

http://www.cnblogs.com/leixiao-/p/9825703.html

```
00002992  FF FF FF FF FF FF FF FF   F0 00 FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿð ÿÿÿÿÿÿ
00003008  FF FF FF FF FF FF FF FF   FF FF FF FF F0 00 31 34  ÿÿÿÿÿÿÿÿÿÿÿÿð 14
00003024  36 31 35 34 31 34 31 31   34 37 31 37 33 31 31 30  6154141147173110
00003040  31 34 31 31 36 36 31 34   35 31 33 37 31 37 31 30  1411661451371710
00003056  36 30 31 32 35 31 33 37   31 32 30 31 37 31 31 33  6012513712017113
00003072  37 31 36 33 31 34 33 31   36 32 31 35 31 31 36 30  7163143162151160
00003088  31 36 34 31 33 37 31 31   37 31 36 34 31 34 33 31  1641371171641431
00003104  33 37 31 32 34 31 35 37   31 33 37 31 32 34 31 34  3712415713712414
00003120  35 31 35 36 31 33 37 31   30 31 31 36 33 31 34 33  5156137101163143
00003136  31 35 31 31 35 31 30 34   31 31 37 35 40 78 6A 73  151151041175@xjs
00003152  65 63 6B 21                                       eck!
```


这段数据发现只有0-7，没有8和9，很容易想到是8进制数据，可以将其转换成10进制，然后再转成ascii字符。一开始看这个数字总长126个，2的倍数，加上以前转换16进制的惯性思维，让我以为这里也是两两一对的转换，转换出来自然不正确，一堆乱码，后来发现两位的8进制数据最大077（数字前加0表示8进制），转换成10进制63也表示不完ascii码表上的字符啊，而且126刚好也是3的倍数，所以三个一组来转换，如下脚本：

破解这串数字了，这里有两点，第一，都是小于8的数，第二，每三个数似乎是一个可以转成字符的集体，于是写脚本

https://blog.csdn.net/csdn_Pade/article/details/82779112

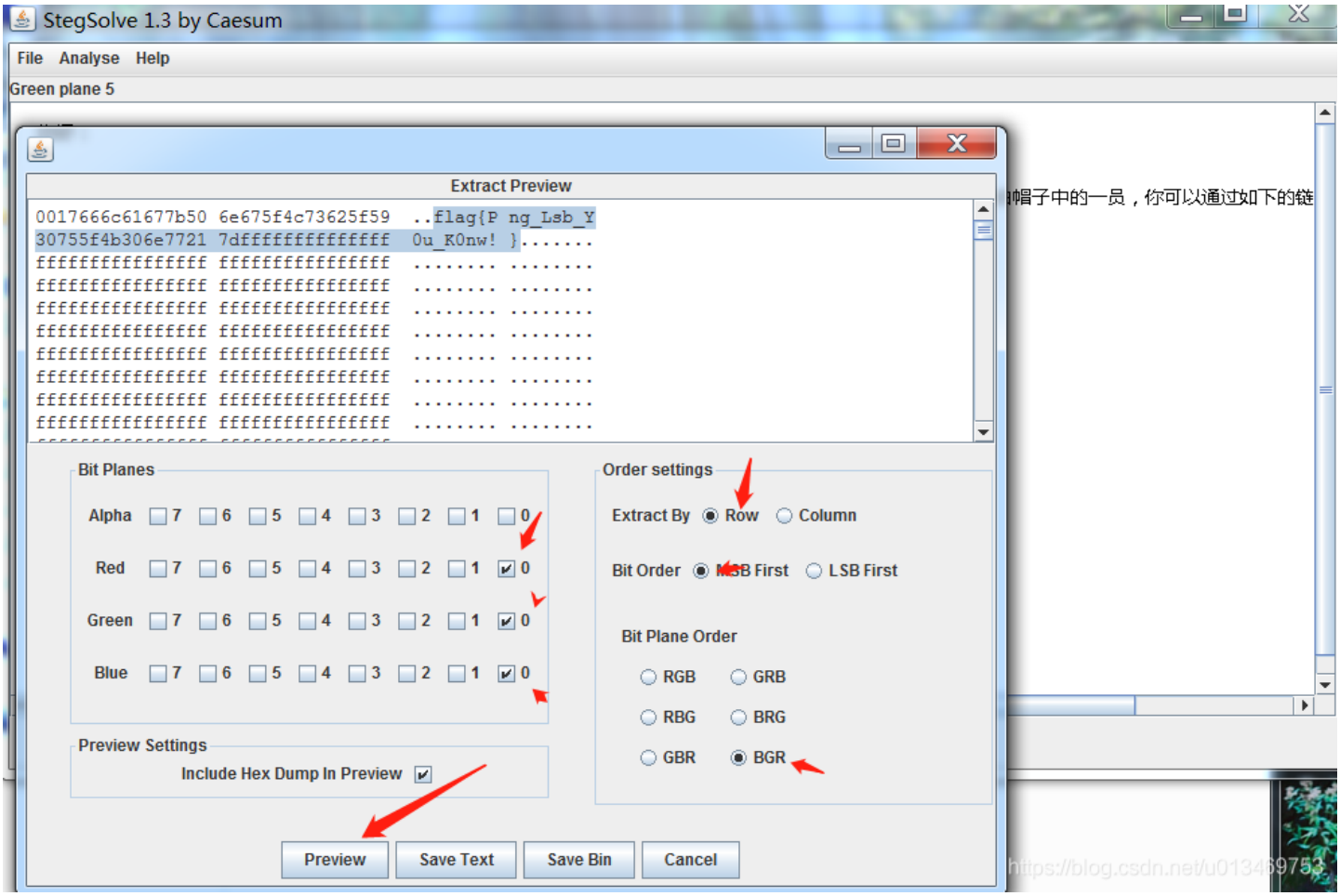
```
code = "14615414114717311014116614513717106012513712017113716314316215116016413711716414313712415713712414515613
710116314315115104175"
a = ''
for i in range(0,len(code),3):
    try:
        a += chr(int(code[i:i+3],8))
    except:
        pass
print(a)
```

```
[redacted]/security/emulation/questionbank/bugku/misc/24普的维$ pwd
lation/questionbank/bugku/misc/24普的维
/security/emulation/questionbank/bugku/misc/24普的维$ touch misc80.py
/security/emulation/questionbank/bugku/misc/24普的维$ nano misc80.py
/security/emulation/questionbank/bugku/misc/24普通的二维码$ python misc80.py
flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}
```

flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}

26.乌云邀请码

直接放到stegsolve，data extract一下



flag{Png_Lsb_Y0u_K0nw!}

27、神秘的文件

要点：

明文破解 + doc隐写

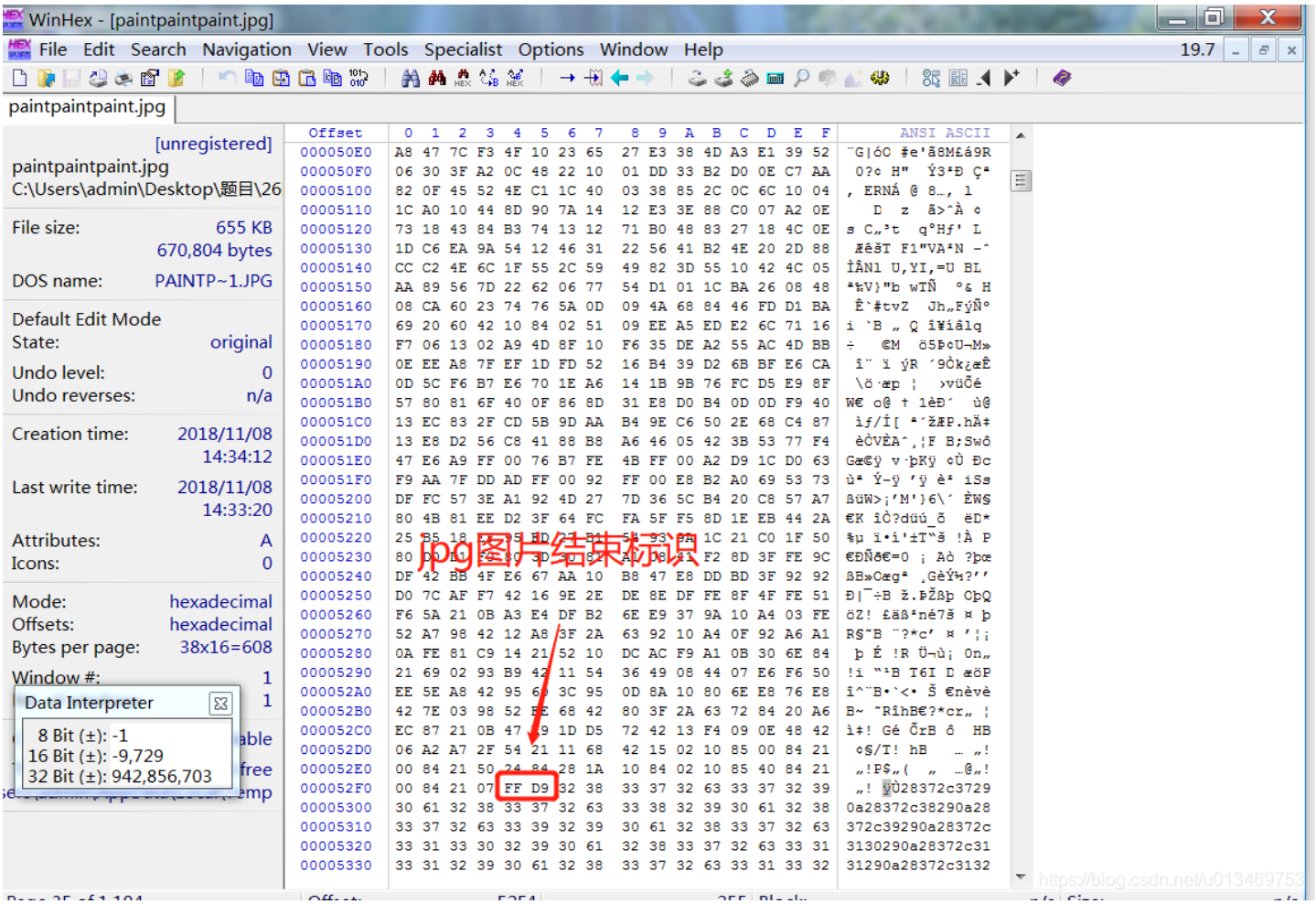
解题过程：

将题目解压出来，题目压缩包里有个logo.png和一个加密压缩包，很明显的明文破解，使用题目压缩包作为key和writeup压缩包进行明文破解(或者使用2345好压的标准压缩算法压缩logo.png)，得到密码：

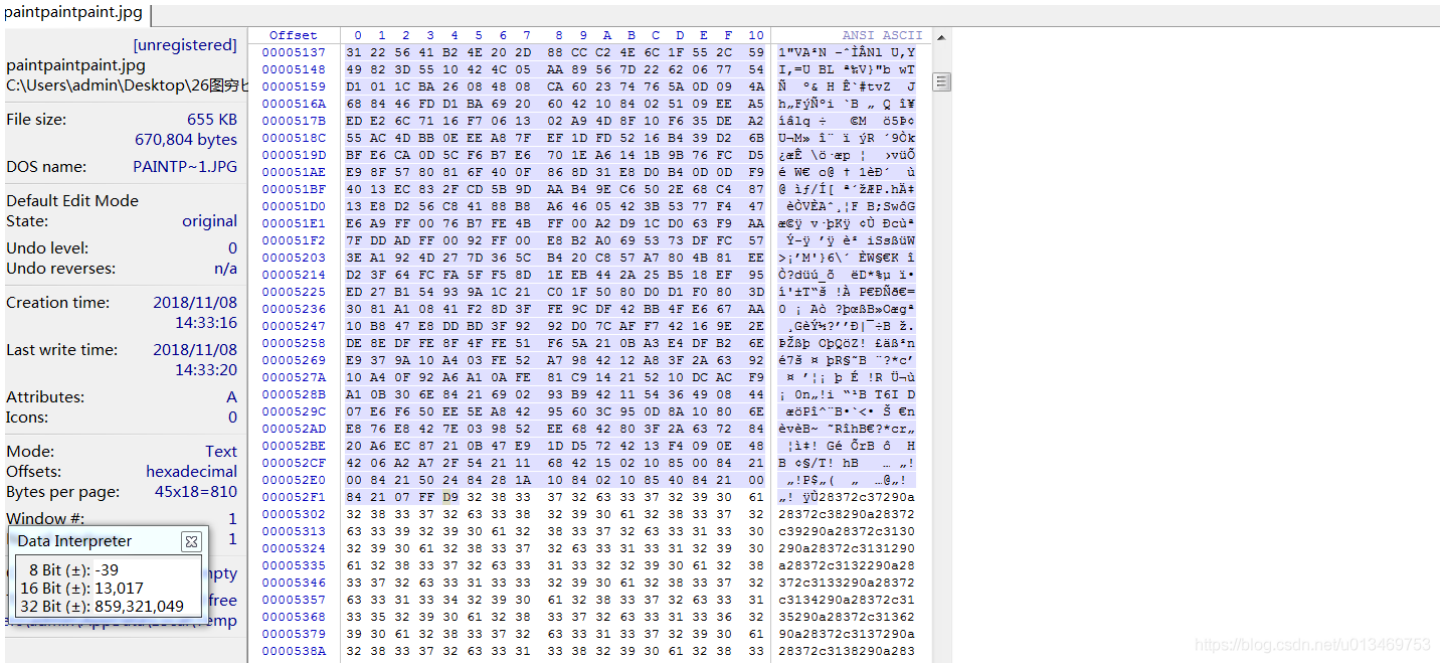
http://www.sdnisc.cn/detail_285_286_747.html

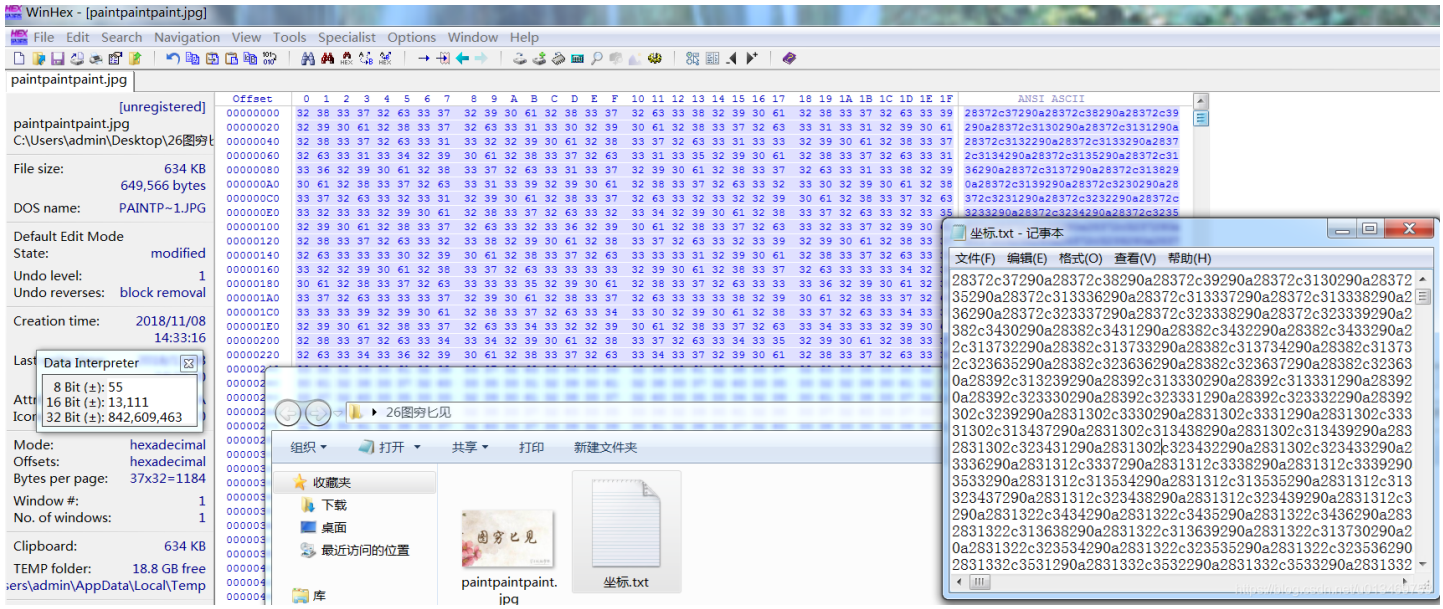
28图穷匕见

直接用winhex打开图片，找到jpg图片的结束位置



可以看到FF D9是jpg的结尾，后面明显是追加的一些值，备份原图，删掉原图的数据





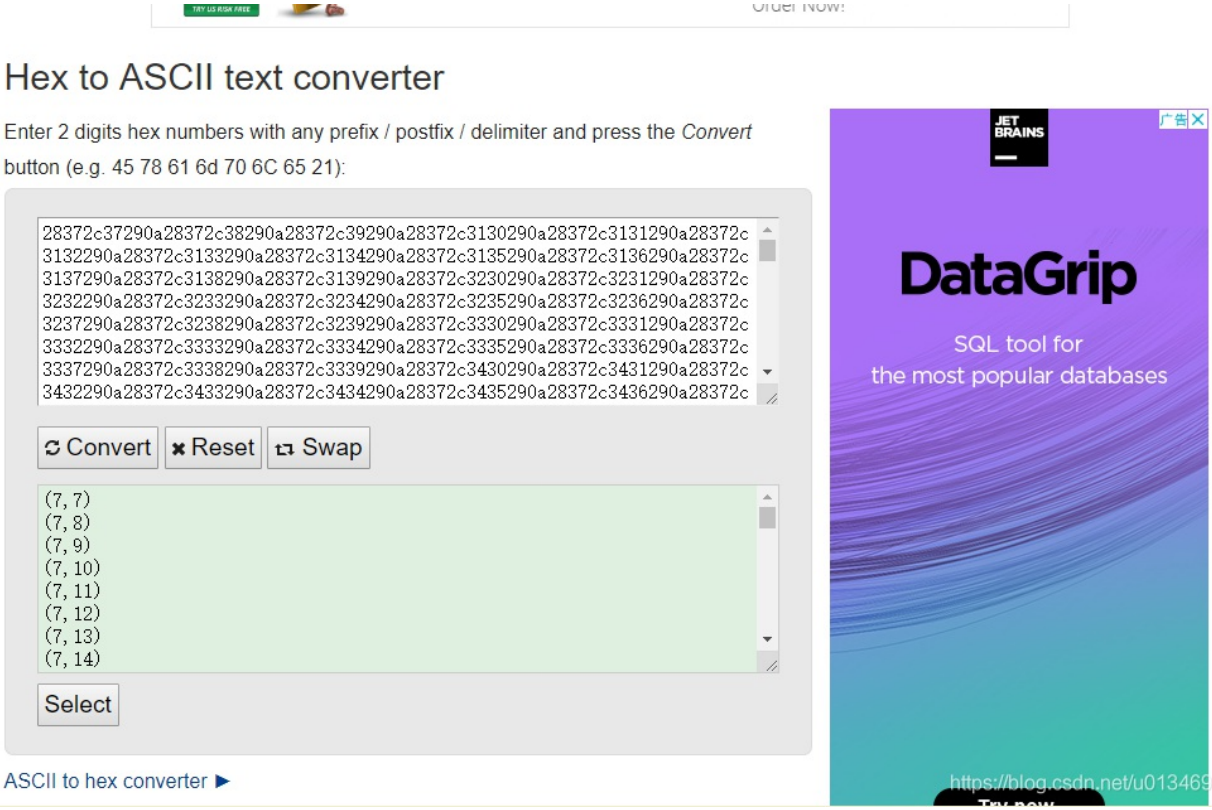
后面的值拷贝出来

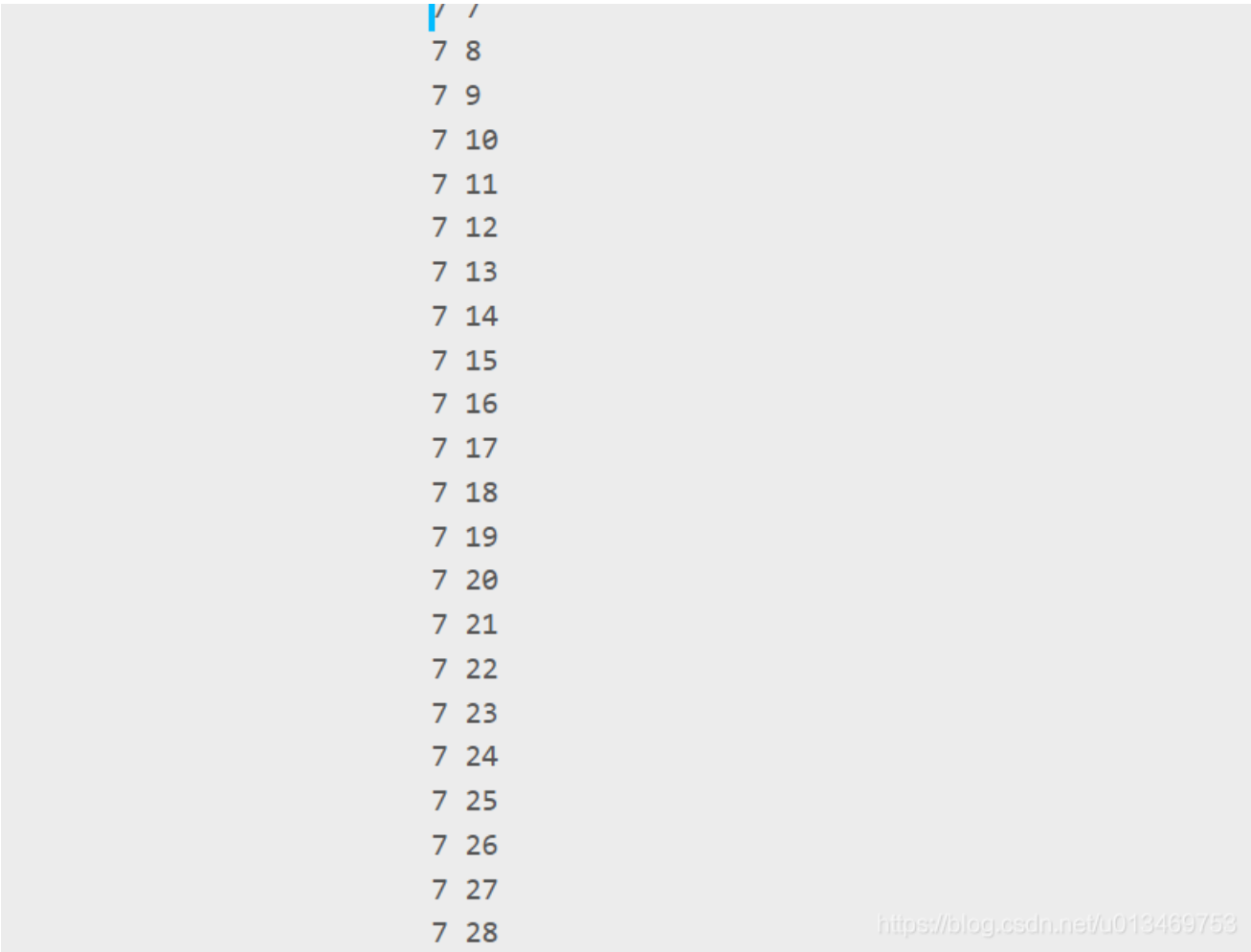
进行16进制转ASCII

我们可以看到这些都是一个个坐标值：

16进制转为ascii

https://www.rapidtables.com/convert/number/hex-to-ascii.html





去掉括号和逗号的txt放到kali中进行绘图。
gnuplot这个工具比较方便，因此将坐标转为gnuplot能识别的格式 坐标1 坐标2

来自 https://www.cnblogs.com/WangAoBo/p/6950547.html
安装gnuplot

来自 https://www.jianshu.com/p/6eef7dfe51bf

gnuplot
plot “qukongge.txt”

flag{40fc0a979f759c8892f4dc045e28b820}

29、convert

convert

来自 https://blog.csdn.net/yaofeiNO1/article/details/78459569#t3

txt文件内都是二进制01字串
将二进制转为16进制，再把16进制符写入winhex文件中，发现rar文件，
另存为rar文件解压得到一张图片，查看属性有base64编码，解码得到flag
bintohex的demo以及存入rar包的代码

来自 https://blog.csdn.net/yaofeiNO1/article/details/78459569#t3

flag{01a25ea3fd6349c6e635a1d0196e75fb}

30.听首音乐

用Audacity音频分析软件打开，猜测是摩尔斯电码，

放大

长的用“-”表示，短的用“.”表示，中间用空格隔开。

```
..... -... -.-. ----. ..--- ..... -.... ....- ----. -.-. -... ----- .---- ---.. ---.. ..-. ..... ..--- . -....
.---- --... -.. --... ----- ----. ..--- ----. .---- ----. .---- -.-.
```

http://tool.bugku.com/mosi/

space方式为空格

5BC925649CB0188F52E617D70929191C

31.好多数值

数值很多255，猜测与RGB有关，下使用RGB值转化为图片的脚本

flag{youc@n'tseeme}

32、很普通的数独

使用binwalk查看发现有25张图片

```
binwalk -e zip
```

提取

下载解压后一堆数独图片，把所有带数字的方框改成黑色

来自 https://ctf.yuanlichenai.cn/2018/05/03/Bugku/Misc-3/

应该是是一张二维码，刚好是25张，5X5组合起来。

样子好像有点不对，这里需要把第1张、第5张和第21张互换位置

扫码得到
`Vm0xd1NtUXlWa1pPVldoVFlUSlNjRlJVVGtOamJGWnlWMjFHVlUxV1ZqTldNakZIWVcxS1IxTnNhRmhoTVZweVdWUkdXbVZHWkhOWGJGcHBWa1paZWxaclpEUmhNVXBYVW14V2FHVnFRVGs9`
使用base64多次解码7次

flag{y0ud1any1s1}

33.PEN_AND_APPLE

PEN_AND_APPLE

来自 http://www.nsoad.com/Article/CTF/20161109/726.html
必须吐槽出题人的视频素材/捂脸
核心
利用NTFS交换数据流隐藏文件来自 https://www.qingsword.com/qing/812.html
原题提供的素材无法解析到文件

联想到视频隐写，搜索之，但只查到WAV格式的。提示是Windows下命令行，查阅《数据隐藏技术解密》一书的Windows相关内容，了解到是NTFS数据流隐写

34.你见过彩虹吗

要点：
考点
拉长图片，二进制转字符串。

来自 http://www.sdnisc.cn/detail_285_286_747.html
查看每张图片的最低位，发现有变化。组成之后是一句话：
可以参考：
https://blog.csdn.net/CoolD_/article/details/83793060#MiscCrack_it8pts_33

得到七串二进制

发现原来图像下部，有黑白块儿，按照黑->1，白->0转化成二进制数。

`11111111010111101111 11111011111110111111 00001100101010110001 01001010010000001101 11010011011101010111 10011011011010110110 00111001101101111101`

经过多次尝试之后发现，每一列，七个数字组成一个字符，进行二进制转化之后即可得到flag。

横着解不出来 尝试竖着解

脚本

```
c1 = '11111111010111101111'
c2 = '11110111111110111111'
c3 = '00001100101010110001'
c4 = '01001010010000001101'
c5 = '11010011011101010111'
c6 = '10011011011010110110'
c7 = '00111001101101111101'

flag = ''

for i in range(0,20):
    c = c1[i]+c2[i]+c3[i]+c4[i]+c5[i]+c6[i]+c7[i]
    flag += chr(int(c,2))
```

print flag
作者：Coo1D
来源：CSDN
原文：https://blog.csdn.net/CoolD_/article/details/83793060
版权声明：本文为博主原创文章，转载请附上博文链接！

35.好多压缩包

```
binwalk 123.zip
```

编写脚本，进行爆破

编写脚本，通过CRC32碰撞，暴力破解出值

打开out.txt，可以看出碰撞出的结果是经过base64编码的，进行base64解码
待解码

`z5BzAAANAAAAAAAAAKo+egCAIwBJAAAAVAAAAAKGNKv+a2MdSR0zAwABAAAAQ01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfG0ruGnKnygsMyj8SBaZHxsYHY84LEZ24cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0wCAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZmlsZSBhbmQgZ2V0IHRoZSBmbGFnxD17AEAHAA==`

https://www.qqxiuzi.cn/bianma/base64.htm

结果按16进制显示

```
\xcf \x90 \x73 \x00 \x00 \x0d \x00 \x00
\x00 \x00 \x00 \x00 \x00 \xaa \x3e \x7a
\x00 \x80 \x23 \x00 \x49 \x00 \x00 \x00
\x54 \x00 \x00 \x00 \x02 \x86 \x34 \xab
\xfe \x6b \x63 \x1d \x49 \x1d \x33 \x03
\x00 \x01 \x00 \x00 \x00 \x43 \x4d \x54
\x09 \x15 \x14 \xcb \xdd \x41 \x4f \x95
\x24 \x48 \xd3 \xe8 \x8f \x98 \x45 \x11
\x51 \x41 \x46 \xf7 \x9f \x1d \x20 \x42
\x7c \x6d \x2b \xb8 \x69 \xca \x9f \x28
\x2c \x33 \x28 \xfc \x48 \x16 \x99 \x1f
\x1b \x18 \x1d \x8f \x38 \x2c \x46 \x76
\xe1 \xc5 \xed \x67 \x4d \x72 \xde \x4d
\x4a \xd5 \x82 \x74 \xbe \x92 \xbd \x1f
\x0a \x94 \xcd \xbe \xae \xf7 \x3f \x22
\x80 \x4a \xf7 \x74 \x20 \x90 \x2d \x00
\x1d \x00 \x00 \x00 \x1d \x00 \x00 \x00
\x02 \x62 \xd1 \xe7 \xd5 \x4f \x63 \x1d
\x49 \x1d \x30 \x08 \x00 \x20 \x00 \x00
\x00 \x66 \x6c \x61 \x67 \x2e \x74 \x78
\x74 \x00 \xb0 \x34 \x69 \x66 \x66 \x69
\x78 \x20 \x74 \x68 \x65 \x20 \x66 \x69
\x6c \x65 \x20 \x61 \x6e \x64 \x20 \x67
\x65 \x74 \x20 \x74 \x68 \x65 \x20 \x66
\x6c \x61 \x67 \xc4 \x3d \x7b \x00 \x40
\x07 \x00
```

去掉

`\x`

```
cf 90 73 00 00 0d 00 00
00 00 00 00 00 aa 3e 7a
00 80 23 00 49 00 00 00
54 00 00 00 02 86 34 ab
fe 6b 63 1d 49 1d 33 03
00 01 00 00 00 43 4d 54
09 15 14 cb dd 41 4f 95
24 48 d3 e8 8f 98 45 11
51 41 46 f7 9f 1d 20 42
7c 6d 2b b8 69 ca 9f 28
2c 33 28 fc 48 16 99 1f
1b 18 1d 8f 38 2c 46 76
e1 c5 ed 67 4d 72 de 4d
4a d5 82 74 be 92 bd 1f
0a 94 cd be ae f7 3f 22
80 4a f7 74 20 90 2d 00
1d 00 00 00 1d 00 00 00
02 62 d1 e7 d5 4f 63 1d
49 1d 30 08 00 20 00 00
00 66 6c 61 67 2e 74 78
74 00 b0 34 69 66 66 69
78 20 74 68 65 20 66 69
6c 65 20 61 6e 64 20 67
65 74 20 74 68 65 20 66
6c 61 67 c4 3d 7b 00 40
07 00
```

winhex新建文件，将解码后结果粘贴进入

fix the file and get the flag，需要进行文件修复
根据末尾以及rar压缩包固定的结束字符串c4 3d 7b 00 40 07 00，进行以下修改
上rar的文件头526172211A0700

参考链接

flag{nev3r_enc0de_t00_sm4ll_fil3_w1th_zip}

36.一个普通胡的压缩包

检查下文件的头尾结构是否有问题，根据文件头判断这是个zip压缩的文件，改后缀名zip，直接解压得到一个目录，目录中两个文件flag.rar和flag.txt，flag.txt文件很小，二进制、属性内容各种查看确定没有隐藏信息，这样重点就是flag.rar

下载解压得到一个flag.txt打开写着flag不在里面。

用HxD打开压缩包，发现文件头PK，

修改后缀为zip解压，
得到flag.rar文件，解压依然不行

将7A改成74后保存，解压得到一张secret.png图片，用HxD打开发现其实是gif图片

使用stegsolve打开图片，发现R通道含有半个二维码，

使用gifsplitter将gif图片进行分离，得到2张图片，这2张再放进stegsolve分析
得到二维码的一半，将2张图片合并补齐，扫描二维码得到flag

手机扫描二维码得到flag
flag{yanji4n_bu_we1shi}

37.2B

```
binwalk 2B
```

```
git clone https://github.com/linyacool/blind-watermark.git
```

提取水印

```
python2.7 decode.py --original ./_2B.extracted/B2.png --image 2B --result B2extract.png
```

得到flag

NUST{I_10v3_2B_F0r3v3r}

40妹子的陌陌

```
binwalk momo.jpg,
```

有压缩包

```
binwalk -e momo.jpg
```

得到一个rar压缩包，双击发现里面一个txt文件，但是加密了，再次查看题目有没有其他的提示
只有一个，图片上的文字：喜欢我吗.

输入解压密码：喜欢我吗.

打开momo.txt文件

```
..../-/-/.--./---.../-.-./-..-././-./-.-./---/-.././.-.-.-/-.-./..../.-/..../..-/---/.-.-.-/-.-./---/--/-..-.
```

内容：http://c.bugku.com/U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0=

```
AES Key：@#@#￥%……￥￥%%……&￥
```

先解开摩斯电码

解密得到网址

HTTP://ENCODE.CHAHUO.COM/

来自 http://atool.org/morse.php

打开后发现是一个在线加解密的网站。再根据后边的AES key猜想，应该是对进行AES解密得到

momoj2j.png

这样网址就变成了

http://c.bugku.com/momoj2j.png

2018年11月19日15点23分目前该网站已经无法访问。使用已有的图片WriteUP博客

得到一章二维码的图片，但黑白进行了反转。

使用Windows自带的画图工具打开，组合键

crtl+shift+i

来自 https://www.cnblogs.com/zaqzzz/p/9480060.html

扫描得到flag

即KEY{nitmzhen6}

41.就五层你能解开吗？

链接: http://pan.baidu.com/s/1i4TQoz7 密码: w65m

提示：

第一层：CRC32 碰撞

第二层：维吉尼亚密码

第三层：sha1 碰撞

第四层：md5 相同文件不同

第五层：RSA

来自参考链接

bugku-就五层你能解开吗WP

> 来自
> https://www.cnblogs.com/Byqiyou/p/9410885.html
> https://blog.csdn.net/preserphy/article/details/79599397
> https://www.cnblogs.com/Byqiyou/p/9410885.html

直接解压需要密码

下面试试第一层碰撞

第一层：

第一层：CRC32 碰撞

```
git clone https://github.com/theonlypwner/crc32
```

```
git clone git@github.com:theonlypwner/crc32.git
```

```
python crc32.py reverse 0x7c2df918
python crc32.py reverse 0xa58a1926
python crc32.py reverse 0x4dad5967
```

可查看pw1.txt/pw2.txt文件内容
选取：
_CRC32_i5_n0t_s4f3
作为解压密码

```
7z e Challengs：Cryptography+500.7z
```

第二层：维吉尼亚密码

继续解压

```
7z e CRC32\ Collision.7z
```

```
cat tips
```

```
cat ciphertext.txt
```

我们来看一下密文。开头是三个字母的单词，常用的三个字母的单词作为开头的就是the、her、she、his、but、and等等，
试一下，假如rla对应的明文是the，那么它的密钥就是YEW

```
cat keys.txt
```

密钥：YEWCQGEWCYBNHDHPXOYUBJJPQIRAPSOUIYEOMTSV

解密：
https://www.ctftools.com/down/

the vigenere cipher is a method of encrypting alphabetic text by using a series of different caesar ciphers based on the letters of a keyword it is a simple form of polyalphabetic substitution so password is vigenere cipher funny

vigenere cipher funny

第三层：sha1 碰撞

用密码解密压缩包
vigenere cipher funny

```
import string
import hashlib
a=string.maketrans('', '')[33:127]
for key1 in a:
    for key2 in a:
        for key3 in a:
            for key4 in a:
                keys=key1+"7"+key2+"5"+"-"+key3+"4"+key4+"3"+"?"
                sha1=hashlib.sha1(keys)
                flag=sha1.hexdigest()
                if "619c20c" and "a4de755" and "9be9a8b" and "b7cbfa5"and "e8b4365"i$
                    print keys
                    break
```

```
admin@kali:~/5ceng$ python cracksha1.py
*705-q4w3?
8725-{4}3?
F7M5-i4@3?
I7~5-s4F3?
k7T5-)4l3?
p7.5-"4'3?
```

解压
试试，解压密码
`I7~5-s4F3?`

第四层：md5 相同文件不同
MD5

Hello World □
MD5校验真的安全吗？
有没有两个不同的程序MD5却相同呢？
如果有的话另一个程序输出是什么呢？
解压密码为单行输出结果。

Hello World □
MD5 check is really safe?
There are two different procedures MD5 is the same?
If so what is the output of another program?
The decompression password is a single-line output.

百度搜索这段话

```
http://www.win.tue.nl/hashclash/SoftIntCodeSign/HelloWorld-colliding.exe
```

运行

```
http://www.win.tue.nl/hashclash/SoftIntCodeSign/GoodbyeWorld-colliding.exe
```

运行
得到解压密码
Goodbye World □
来自 https://www.cnblogs.com/alexyuyu/articles/3508110.html

7z e

第五层：RSA
使用Openssl导入公钥，查看模数n和指数e
openssl rsa -inform PEM -in rsa_public_key.pem -noout -modulus -text -pubin

可以看到指数（Exponent）很大，在RSA中如果n确定，e非常大，会导致d很小，从而出现维纳攻击，使用连分式（Continued fraction）去求得d。
n=`28FFF9DD3E6FE9781649EB7FE5E9303CF696347C4110BC4BA3969F0B11669840C51D81A6842B6DF2B090F21CD76D4371A8C0E47048C965ECA5B46913AFBB8DA052072A0566D7039C618ABA9065759B059E29E485DC5061A16AC63129438D9354E65DF5747546B85DB3D699819C4B7732DF927C7084A5D52D6E6D6AAC144623425`

e= `01:f8:fb:a4:10:05:2d:f7:ed:a3:46:2f:1a:ac:d6: 9e:40:76:04:33:ca:33:57:67:cd:73:05:a3:d0:90:80:5a:5f:d4:05:dd:6e:ea:70:e9:8f:0c:a1:e1:cf: 25:47:48:67:1b:f0:c9:80:06:c2:0e:ee:1d:62:79:04:35:09:fe:7a:98:23:8b:43:91:60:a5:61:2d:a7: 1e:90:45:14:e8:12:80:61:7e:30:7c:3c:d3:31:3f:a4:c6:fc:a3:31:59:d0:44:1f:bb:18:d8:3c:af:4b: d4:6f:6b:92:97:a8:0a:14:2d:d6:9b:f1:a3:57:cc:b5:e4:c2:00:b6:d9:0f:15:a3`

去掉冒号：

e= `01f8fba410052df7eda3462f1aacd6 9e40760433ca335767cd7305a3d090 805a5fd405dd6eea70e98f0ca1e1cf254748671bf0c98006c20eee1d6279 043509fe7a98238b439160a5612da7 1e904514e81280617e307c3cd3313fa4c6fca33159d0441fbb18d83caf4b d46f6b9297a80a142dd69bf1a357cc b5e4c200b6d90f15a3`

维纳攻击工具

```
git clone https://github.com/pablocelayes/rsa-wiener-attack.git
```

修改一下RSAwienerHacker.py 中的n值和e值，添上16进制：0x

```
python RSAwienerHacker.py
```

`Hacked!`

得到私钥

d= `826466797229427501729333977237178332216882214947197683422108239340936369189 5`

知道了私钥d那么就可以生成私钥文件来破解flag，在github上面找的rsatool，根据d,n,e生成私钥rsa_private_key.pem文件。

```
git clone https://github.com/ius/rsatool.git
```

```
pip install gmpy
```

```
python rsatool.py -d 826466797229427501729333977237178332216882214947197683422108239340936369189 5 -n 0x28fff9dd3e6fe9781649eb7fe5e9303cf696347c4110bc4ba3969f0b11669840c51d81a6842b6df2b090f21cd76d4371a8c0e47048c965eca5b46913afbb8da052072a0566d7039c618aba9065759b059e29e485dc5061a16ac63129438d9354e65df5747546b85db3d699819c4b7732df927c7084a5d52d6e6d6aac144623425 -e 0x1f8fba410052df7eda3462f1aacd69e40760433ca335767cd7305a3d090805a5fd405dd6eea70e98f0ca1e1cf254748671bf0c98006c20eee1d6279043509fe7a98238b439160a5612da71e904514e81280617e307c3cd3313fa4c6fca33159d0441fbb18d83caf4bd46f6b9297a80a142dd69bf1a357ccb5e4c200b6d90f15a3 -o key.pem -f PEM
```

```
openssl rsautl -decrypt -in flag.enc -inkey key.pem -out flag.txt
```

实际命令：

```
openssl rsautl -decrypt -in ../flag.enc -inkey ./key.pem -out ../get_the_flag.txt
cat ../get_the_flag.txt
```

flag{W0rld_Of_Crypt0gr@phy}

论剑

题解参考 https://www.52pojie.cn/thread-854349-1-1.html

继续用binwalk分析，发现里面有两张图片，

Base16解密 https://www.qqxiuzi.cn/bianma/base.php?type=16

注意： 文件头，base编码，考虑往上一步分析，二进制，jpeg图片高度的修改（不要只掌握png文件的哦）
需要有常见文件头的积累哦，下面附上一部分（也可以去百度，一大把呢。） JPEG (jpg)，文件头：FFD8FFE0
PNG (png)，文件头：89504E47
GIF (gif)，文件头：474946383961
ZIP Archive (zip)，文件头：504B0304
RAR Archive (rar)，文件头：52617221
Wave (wav)，文件头：57415645
AVI (avi)，文件头：41564920
Real Audio (ram)，文件头：2E7261FD
Real Media (rm)，文件头：2E524D46
MPEG (mpg)，文件头：000001BA
MPEG (mpg)，文件头：000001B3
7z文件头：37 7A BC AF 27 1C