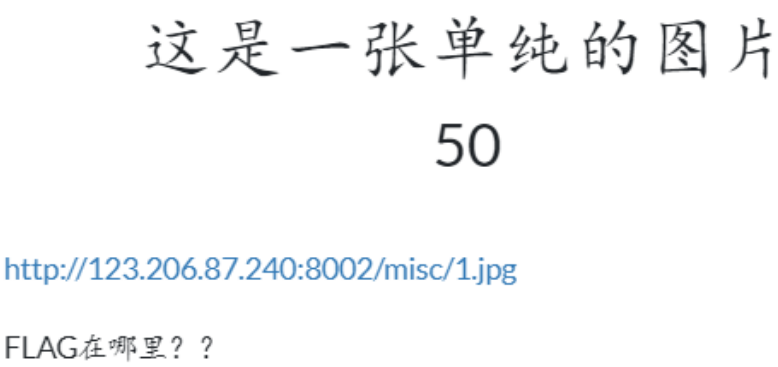
Author: Qftm

1、签到

get flag:

```
Qftm{You should sign in}
```

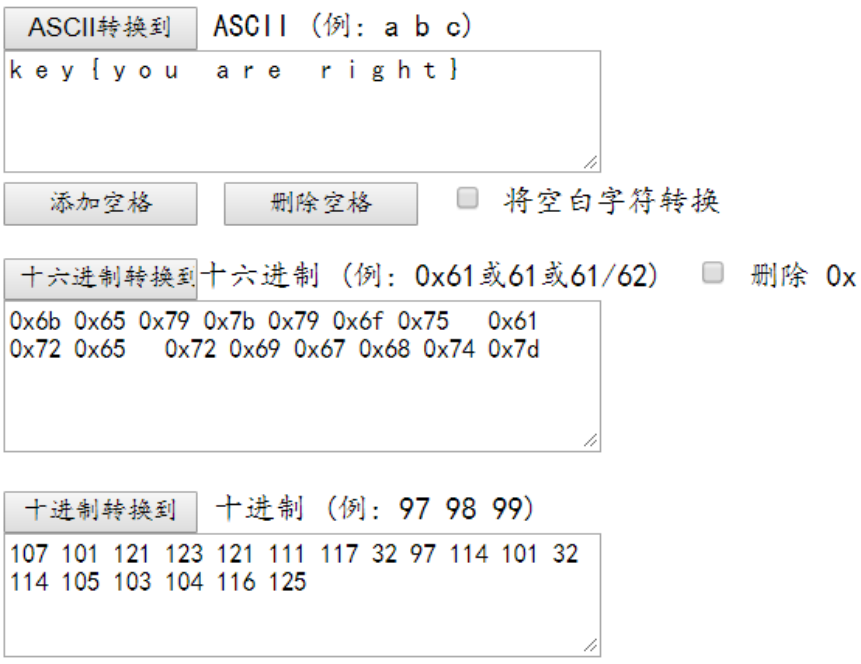
2、这是一张单纯的图片



查看图片十六进制

```
DA 78 3A 2D 0F E2 C3 EB FA 54 0D 0D BE AF 03 A5   Úx:-.âÃëúT..¾¯.¥
E7 95 1E E5 33 0F 98 97 FE EE ED AA 43 72 01 57   ç•.å3.˜—þîíªCr.W
1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28   .d.Š(.Ð¨¢Š.(¢Š.(
A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B   ¢Š.ÿ&#107;&#101;
26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32   &#121;&#123;&#12
31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23   1;&#111;&#117;&#
33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23   32;&#97;&#114;&#
31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26   101;&#32;&#114;&
23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34   #105;&#103;&#104
3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9      ;&#116;&#125;ÙÙ
```

提去特殊字符串进行解码



get flag:

```
key{you are right}
```

3、隐写

隐写

50

2.rar

解压压缩包得到一张图片

打开图片发现只有一个“Bu“可能缺少了什么东西，尝试更改其宽高，得到 flag

2. png

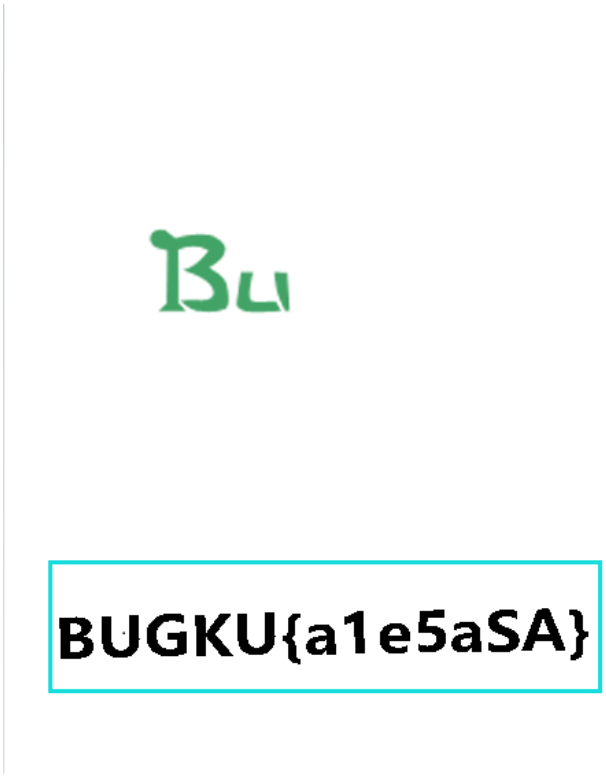
Edit As: Hex Run Script Run Template

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG........IHDR
0010h:	00	00	01	F4	00	00	11	A4	08	06	00	00	00	CB	D6	DF	...ô...¤.....ËÖß
0020h:	8A	08	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š....pHYs...t...
0030h:	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t.Þf.x...MiCCPPh
0040h:	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
0050h:	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile..xÚ.SwX"÷.>ß
0060h:	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08	÷e.VBØð±—l.."#¬.
0070h:	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È.Y¢.'.a„..@Å…ˆ.
0080h:	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	V...œHUÄ‚Õ.H.ˆâ
0090h:	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(¸gAŠˆZ‹U\8î.Ü§µ
00A0h:	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF	}zïííû×û¼çœçüÎyÏ
00B0h:	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8	.€..&'æ¢j.9R…<:Ø
00C0h:	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	..OHÄÉ½€..Hà. .æ
00D0h:	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC	ËÂg.Å..ð.yx~t°?ü
00E0h:	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	.¯o...pÕ.$.Çáÿƒº

宽

高

PS：从第二行开始，前四位是宽，后四位是高。

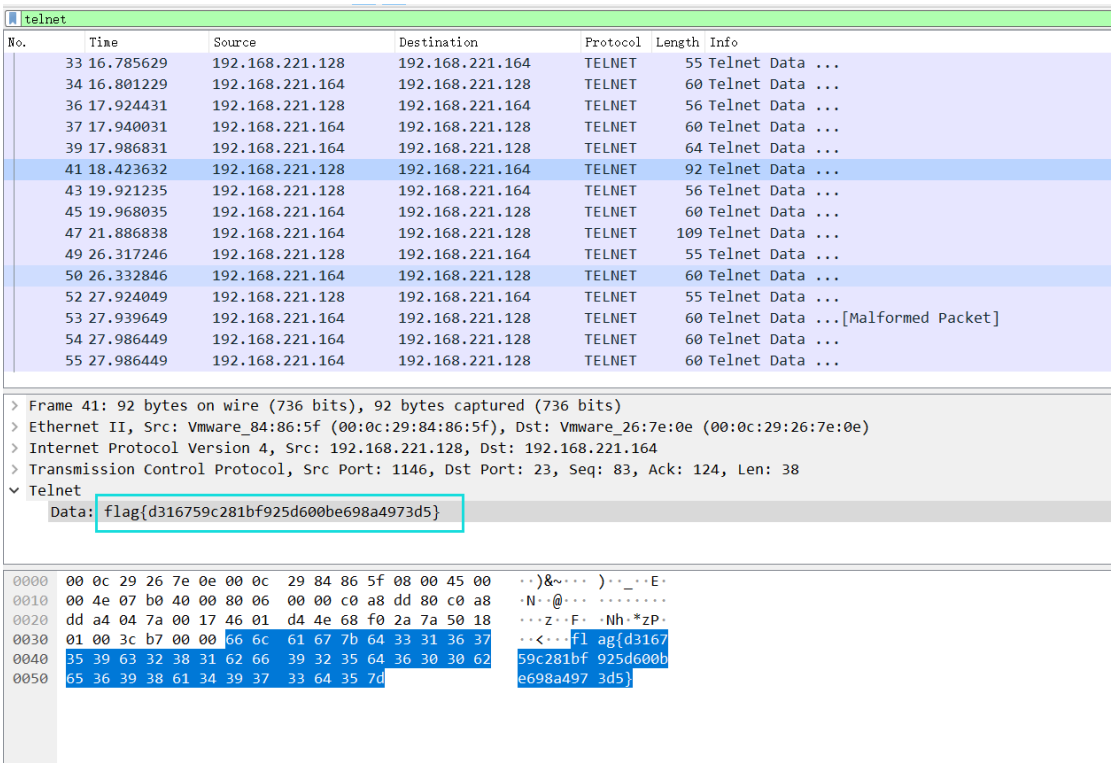


get flag:

```
BUGKU{a1e5aSA}
```

4、telnet

wires hark 打开数据包进行分析，根据提示对 telnet 进行过滤，get flag。

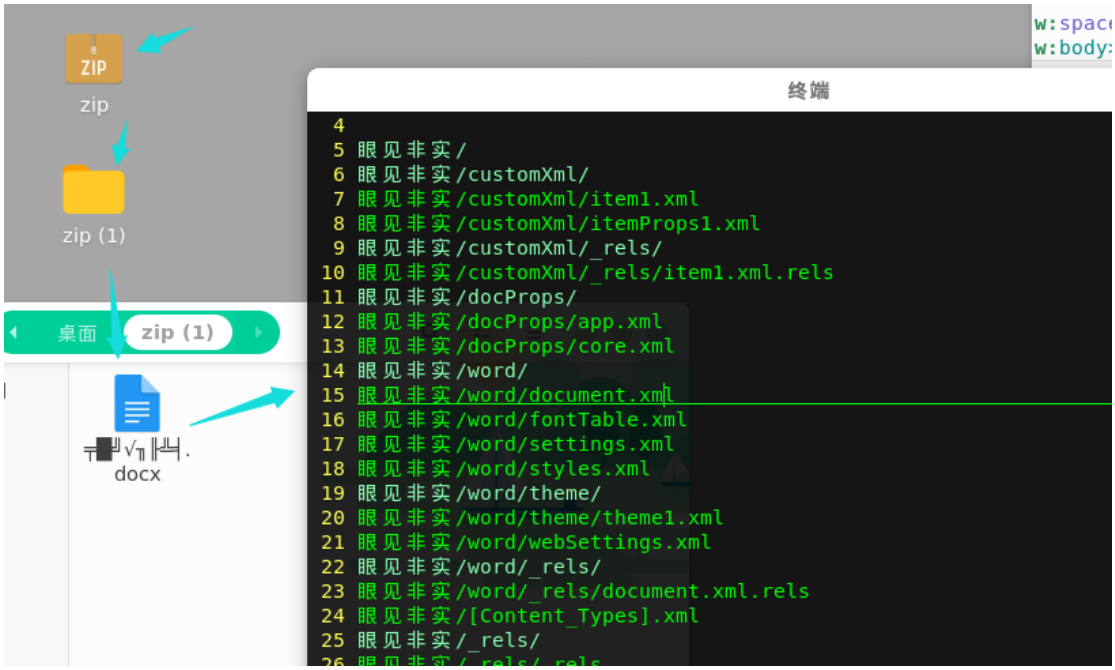


get flag:

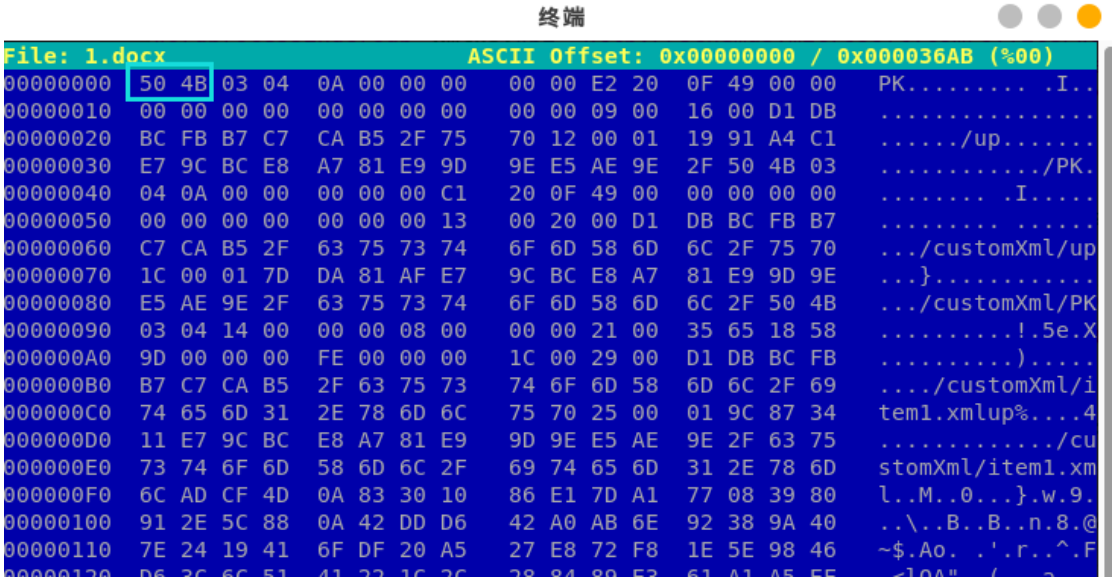
```
flag{d316759c281bf925d600be698a4973d5}
```

5、眼见非实(ISCCCTF)

解压得到一个 word，vi 查看文件内容，可以看到有许多目录，猜测 word 是一个压缩包



word---->zip



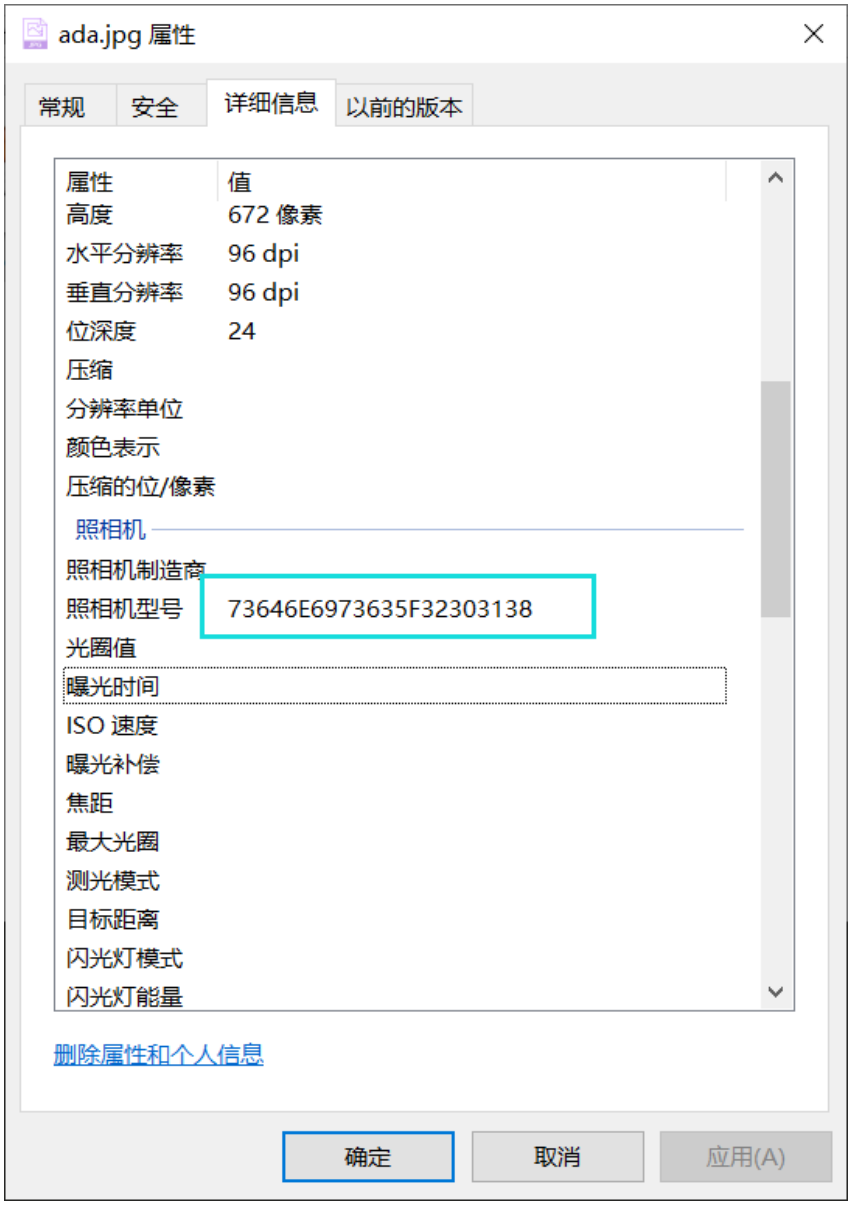
解压 word 压缩包，得到许多 xml 文件，遍历内容得到 flag

get flag:

```
flag{F1@g}
```

6、啊哒

查看图片属性，得到特殊数据



解码十六进制得到一个字符串

ASCII转换到 ASCII （例： a b c）

sdnisc_2018

添加空格 删除空格 将空白字符转换

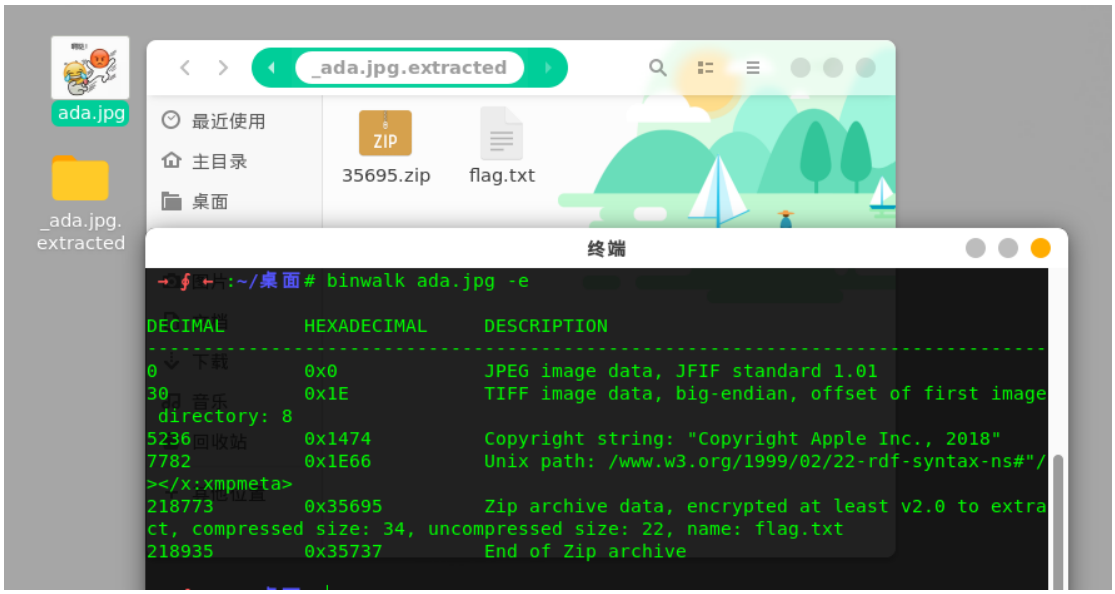
十六进制转换到 十六进制 （例： 0x61或61或61/62） 删除 0x

0x730x640x6e0x690x730x630x5f0x320x300x310x38

十进制转换到 十进制 （例： 97 98 99）

1151001101051159995504849 56

提交，发现并不是 flag，binwalk 分析得到压缩包里面有一个 flag.txt 被加密，使用上面解出的字符串作为密码得到 flag

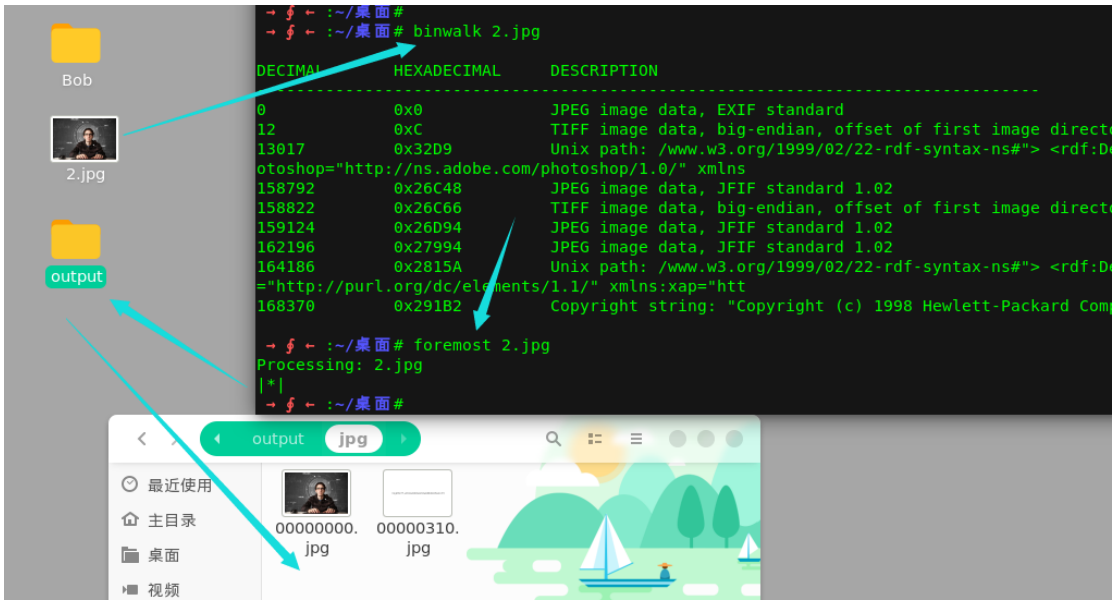


get flag:

```
flag{3XiF_iNf0rM@ti0n}
```

7、又一张图片，还单纯吗

binwalk 分析可知里面存在其它图片，利用 foremost 快速得到其中的图片



get flag:

```
falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}
```

8、猜

猜

60

http://123.206.87.240:8002/misc/cai/QQ20170221-132626.png

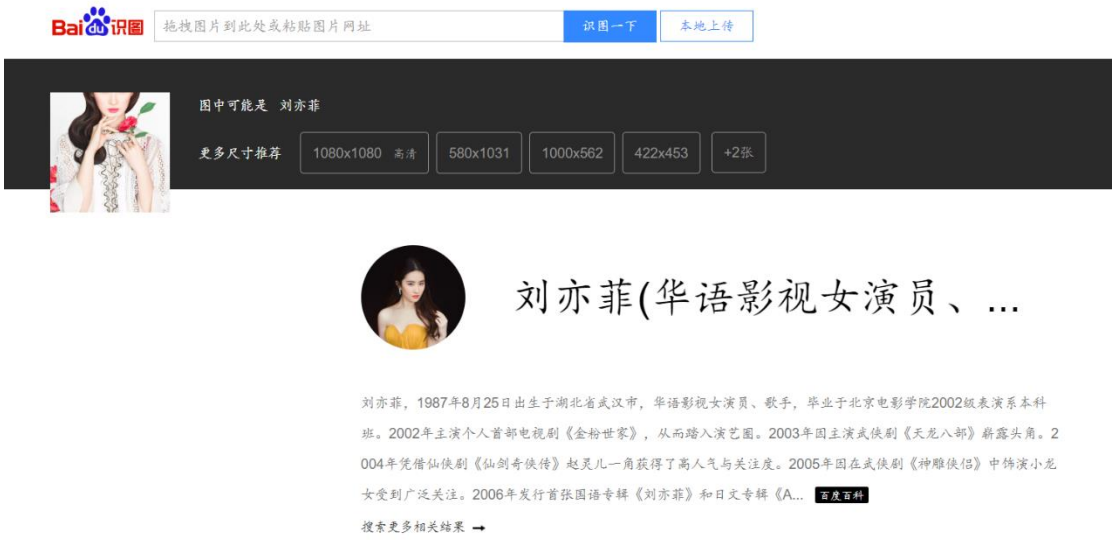
flag格式key{某人名字全拼}

Flag

Submit

根据提示，尝试进行图片识别

识图得到：刘亦菲

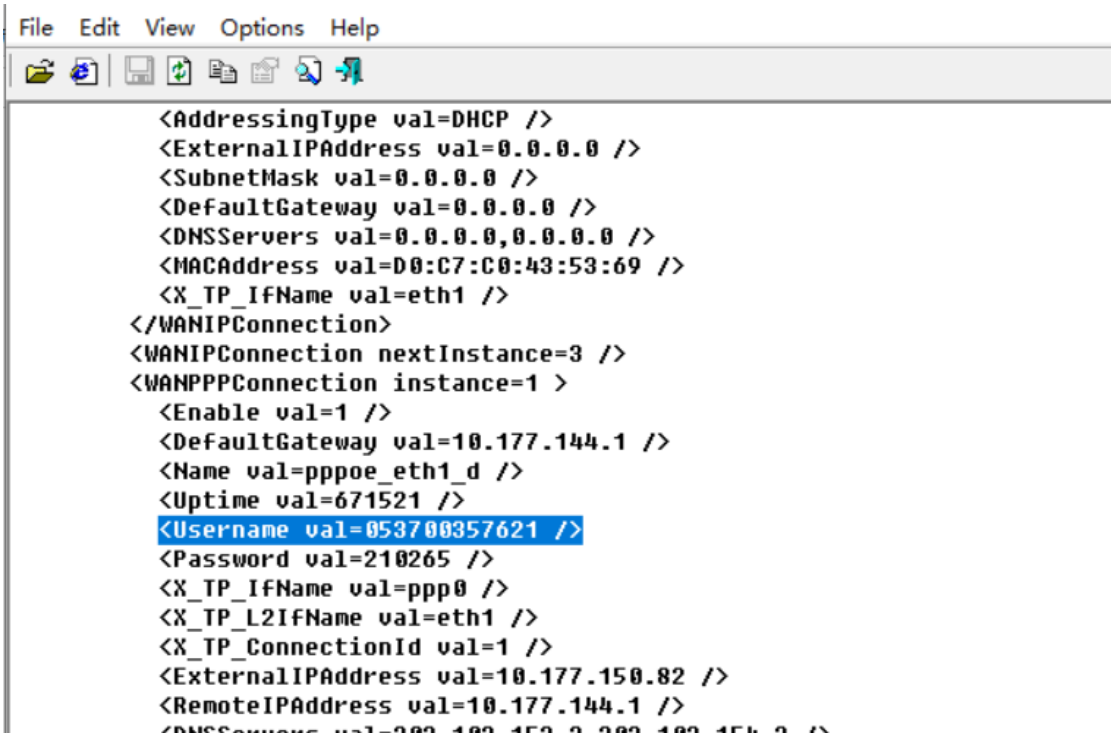


get flag:

```
key{liuyifei}
```

9、宽带信息泄露

根据提示，则需要找到某个用户，下载的文件是一个配置文件，可能是路由器的配置文件，使用工具 RouterPassView 打开查看宽带用户



PS：RouterPassView 可以帮助你从你的路由器恢复您丢失密码的文件。

get flag；

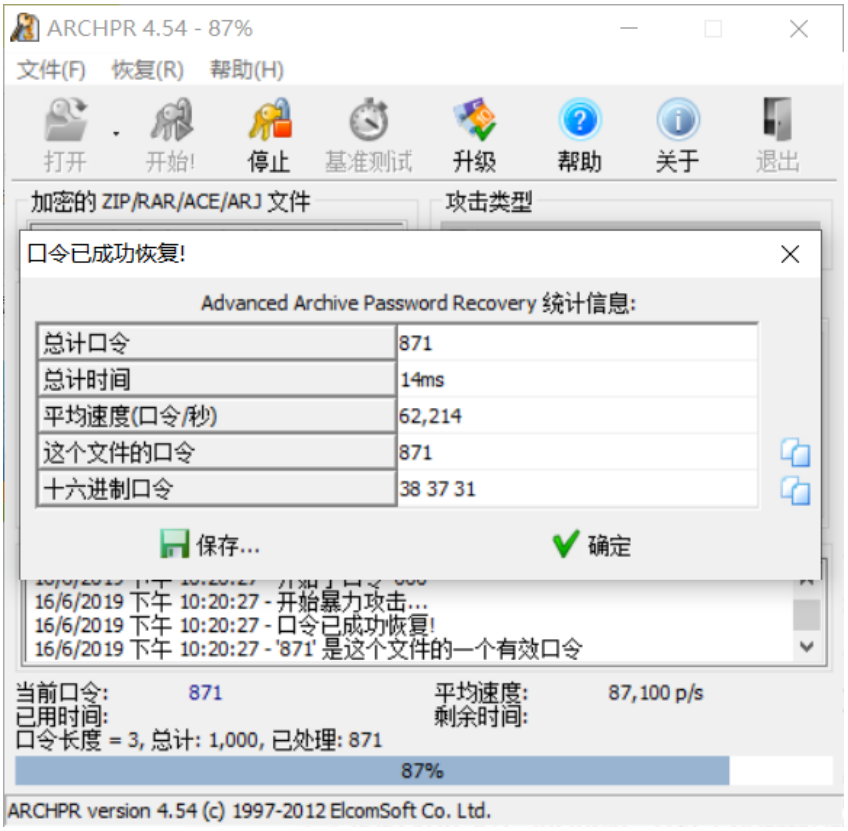
```
flag{053700357621}
```

10、隐写 2

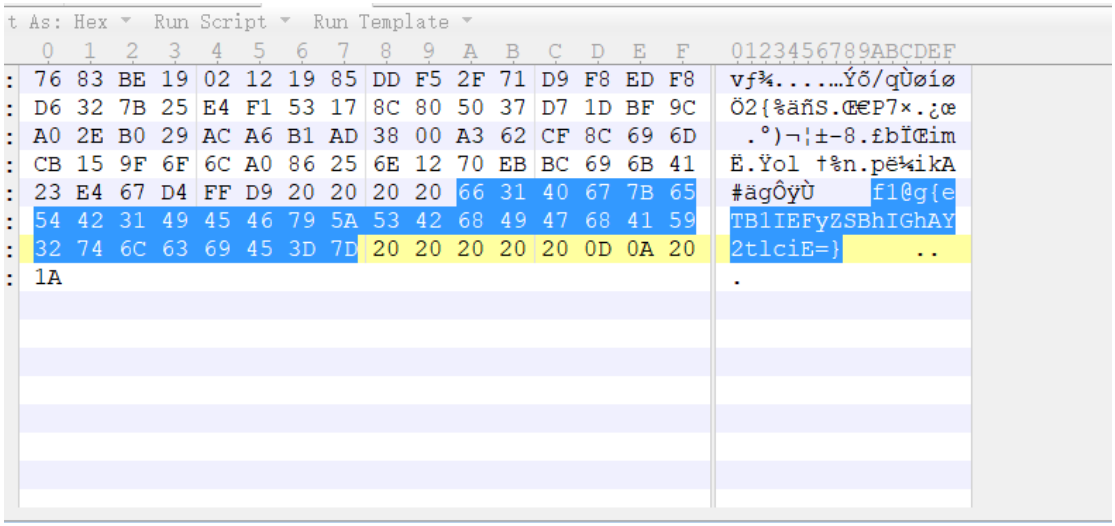
foremost 分离图片中存在文件，根据提示进行压缩包爆破

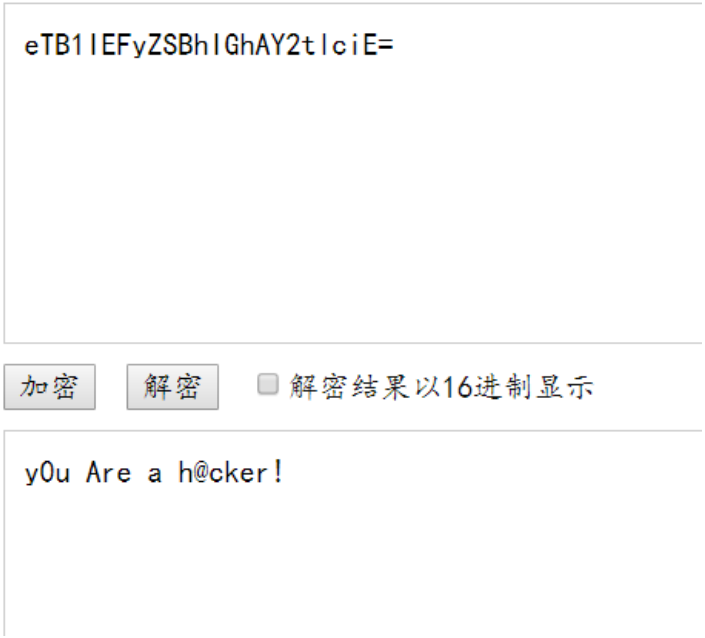
告诉你们一个秘密，密码是3个数哦。

查理曼：
查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。
雅典娜：
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
兰斯洛特，
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。
Hint:
其实斗地主挺好玩的。



取出图片查看其十六进制得到 flag





get flag:

```
flag{y0u Are a h@cker!}
```

11、多种方法解决

多种方法解决

60

在做题过程中你会得到一个二维码图片

http://123.206.87.240:8002/misc/3.zip

查看 key.exe 十六进制得到二维码，扫描 get flag

Startup | KEY.exe

Edit As: Text /wrap | Run Script | Run Template

```
1  
-  ARnQU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1Uouic
-  Kg19hwPCDcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rXO3P4lLvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78z
-  hU+5i9yxv4T3T2O0/7eud68OT2H3LCft0l/ae9ZlTo+23pPvX7/rwJHbfcsI+3aW9Z33m1Gj7Len+9bs+PIndt5
-  ywT3dp71mfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S7l+/68MJc5O0OSWpcyexnFjfcsI+JW1ukpRfv+vDC
-  XOTtDklqXMnsZxY33LCPiVtbpKUX7/rwwlzk7Q5JalzJ7GcWN9ywj4lbW6SlF+/68MJc5O0OSWpcyexnFjfcsI+
-  JW1ukpRfv+vDCXOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73
-  PctL2DbvH3CQpv37XhxPmJrGctP1d7H2Wk7Zv2D3mJkn59bs+nDA3ieWEfdNImylJnelp7H6bmyTl1+/6cMLcJJ
-  YT9k0jbaYkdaansfttbpKUX7/rwwlzk1hO2DeNtJmS1Jmexu63uUlSfv2uDyfMTWI5Yd800mZKUmd6Grvf5iZJ+
-  fW7PjzJ7v12b33LSdtvsfuW75LuX7/rw5Ps3m/31rectP0Wu2/5Lun+9bs+PMnu/XZvfctJ22+x+5bvku5fv+vD
-  k+zeb/fWt5y0/Ra7b/ku6f71+++HT0v+5l3+tK935vApyd+8y5/29c4cPiX5m3f5077emcOnJH/zLn/ar3d+/fl
-  BpI+cMDeNtJkSywn79BP5uK+yfzTmppE2U2I5YZ9+Ih/3VfaPxtw00mZKLCfs00/k477K/tGYm0baTInlhH36iS
-  xflT78TpI605bdPbF7lhvct54mvWOaWJ6m4Z0kdaYtu3ti9yw3uG89TXrHNLE8TcM7SepMW3b3xO5ZbnDfepr0j
-  mlieZqGd5LUmbbs7onds9zgvvU06R3TxPXcSxPrW07YpyR1pqTNKUmdKUmdk5LUaXzdWB/eYX3LCfuUpM6UtDkl
-  qTMlqXNSkjqNrxvrwzusbzlhn5LUmZI2pyR1piR1TkpSp/F1Y314h/UtJ+xTkjpT0uaUpM6UpM5JSeo0ft34+vO
```

点击这里选择选择要转换成Base64的图片

复制 清空

```
n7FPD+paTtk9O71sTT3MV7WD3LSfsU8P6IpOZ1U7VWxPXcy/tYPcD+xTW/qWk7ZPTu9bE9dzL+Tg9y0n7FPD+paTtk9O
71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Syw3uTZI6U6PtE+4/3dc3rw8nzE1iucG9SVJnarR9wv2n+/rm9eGE
uUksN7g3SepMjbZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmnzXQ3r7+bE+pafhu+jr876cMLcJG2+q2
H93ZxY3/LT8H301VkfTpibpM13Nay/mxPrW34avo++OuvDCXOT7OZGu7e+5YT9XYnlhH36DlfvfsTcJLu50e6tbzlhf1di
OWGfvsPVux8xN8lubrR761tO2N+VWE7Yp+9w9e5HzE2ymxvt3vqWE/Z3JZYT9uk7XL1+1GD3LX8avt8klhu2t5yc6F+/6
8OT2H3Ln4bvN4nlhu0tJyf61+/68CR23/Kn4ftNYrlhe8vJif71uz48id23/Gn4fpNYbtjecnKif/3+++HTnub0fd4zieUtvLfrO1
y9PH7K05y+z3smsbyF93Z9h6uXx095mtP3ec8klrfw3q7vcPXy+ClPc/o+75nE8hbe2/Udzv9X+sv/OP/881/SqtvcdpBh+
wAAAABJRU5ErkJggg==
```

还原生成的Base64编码为图片：

get flag:

```
KEY{dca57f966e4e4e31fd5b15417da63269}
```

12、闪的好快

打开图片发现是动图，并且每一帧的动画都是一个二维码，尝试分离每一帧，使用工具 GifSplitter 进行分离，但是分离出来的二维码不完整

此时可以利用工具 Stegsolve 进行每一帧的浏览

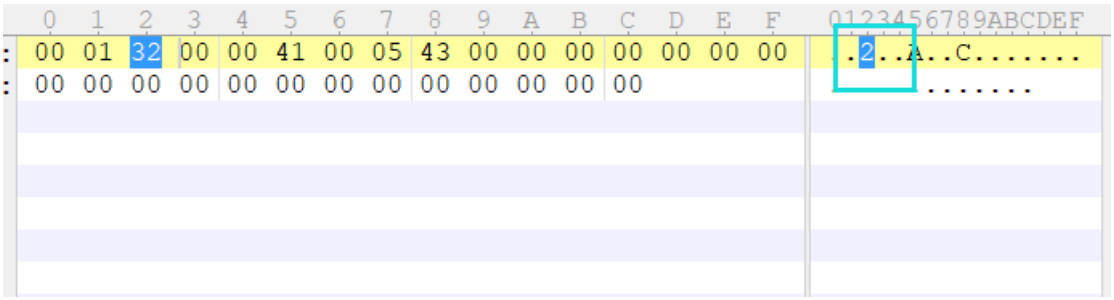
通过扫码发现每一帧都存在一个字符，将这 18 个字符进行拼接得到 flag

get flag:

```
SYC{F1aSh_so_f4sT}
```

13、come_game

通过玩游戏(当游戏玩到第二关的时候)可以得到游戏配置文件 save1，十六进制查看 save1，猜测字符 2 为通关的数字



尝试将其修改为 33 34 35，当到了第 5 关的时候可以得到 flag，游戏通关

get flag:

```
SYC{6E23F259D98DF153} #flag 格式有问题
```

14、白哥的鸽子

白哥的鸽子

60

咕咕咕

jpg

将文件放入十六进制编辑器中，在后面得到一串特殊字符串

```
8D 47 DA 3E D1 EE CF 94 1A E6 2A C5 8E 3C F8 00   .GÚ>ÑîÏ”.æ*ÅŽ<ø.
EA 03 A8 35 12 39 F0 8E 6C A2 9E 1D 66 E2 BB 87   ê.¨5.9ðŽl¢ž.fâ»‡
74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49   t÷Ke°X/.:’¿.s*ÇI
E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20   æ.§....yÐ.(.¥.@
78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC   xÜYiÚ.dnæ{£W1î.Ü
CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67   ËbEb‰î[Ü¶s.ãÿÙfg
32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77   2ivyo}l{2s3_o@aw
5F 5F 72 63 6C 40                                  __rcl@
```

将字符串进行栅栏解密得到 flag

栅栏密码

在下面的文本框输入明文或密文，点加密或解密，文本框中即可出现所得结果

加密 解密 列举加密 列举解密 栏数: 2 只列举完整匹配的

密文框:

```
fg2ivyo}l{2s3_o@aw__rcl@

2栏:
f3g_2oi@vaywo_}_lr{c2ls@

3栏:
flag{w22_is_v3ry_cool}@@

4栏:
fo3_g}__2lori{@cv2alysw@

6栏:
fvl3argy{_wc2o2o_li}s@_@

8栏:
fio{3@_cgv}2_a_l2ylsowr@

12栏:
f2vol23oa_rlgiy}{s_@w_c@
```

get flag:

```
flag{w22_is_v3ry_cool}
```

15、linux

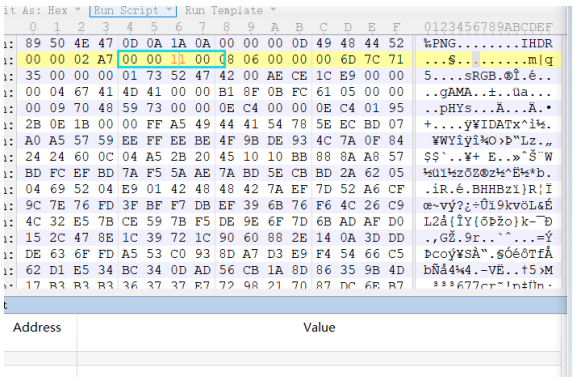
终端下 cat flag 得到 flag

get flag:

```
key{feb81d3834e2423c9903f4755464060b}
```

16、隐写 3

下载图片发现图片高度不正常，尝试更改，得到 flag



get flag:

```
flag{He1l0_d4_ba1}
```

17、做个游戏(08067CTF)

懂点 Android 逆向的人都会很快做出来，使用 jd-gui 查看 Java 代码，在 PlaneGameFrame.class 文件中得到 flag

get flag:

```
flag{DajiDali_JinwanChiji}
```

18、想蹭网先解开密码

想蹭网先解开密码

100

flag格式：flag{你破解的WiFi密码}

tips：密码为手机号，为了不为难你，大佬特地让我悄悄地把前七位告诉你
1391040**
Goodluck!!

作者@NewBee

wifi.cap

根据 tips 密码为手机号，现在知道密码前 7 位，后四位可通过爆破得到，利用 Linux 下的 crunch 工具辅助爆破。

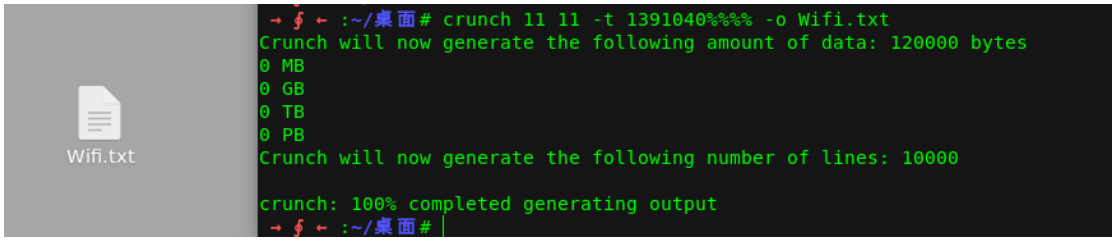
PS：Crunch 是一种创建密码字典工具，该字典通常用于暴力破解。使用 Crunch 工具生成的密码可以发送到终端、文件或另一个程序。

```
crunch [minimum length] [maximum length] [character set] [options]
```

crunch 命令常用的选项如下所示。

-o：用于指定输出字典文件的位置。 -b：指定写入文件最大的字节数。该大小可以指定 KB、MB 或 GB，但是必须与-o START 选项一起使用。 -t：设置使用的特殊格式。 -l：该选项用于当-t 选项指定@、%或^时，用来识别占位符的一些字符。

生成 Wifi.txt 字典



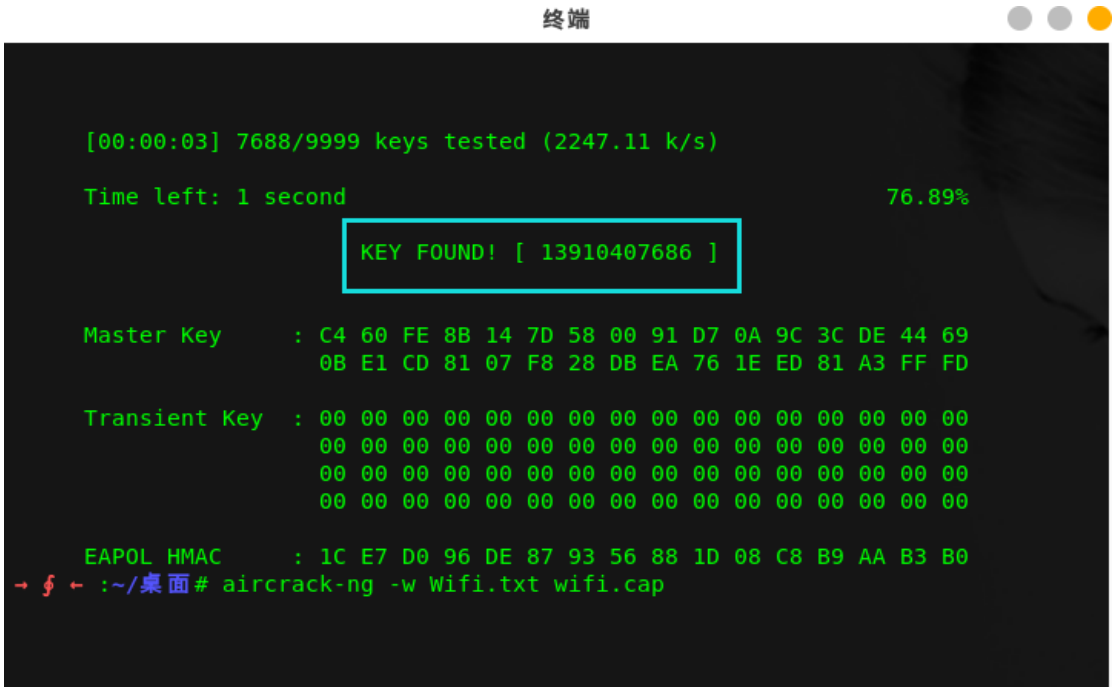
PS：命令解析

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

最小 11　　最大 11

```
-t          指定模式
  @         插入小写字母
  ,         插入大写字母
  %         插入数字
  ^         插入特殊符号
```

利用 Linux 下 Wifi 破解工具 aircrack-ng 破解 wifi.cap 密码



get flag:

```
flag{13910407686}
```

19、Linux2

根据提示，使用 Linux 下 grep 搜索关键字 KEY 得到 flag

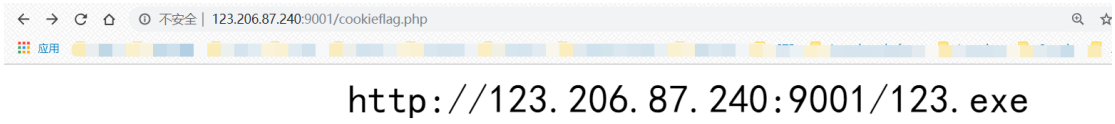
```
→ ∮ ← :~/桌面# grep "KEY" -an brave


PS：a 代表二进制问价、n 代表字符串出现的位置
```

get flag:

```
KEY{24f3627a86fc740a7f36ee2c7a1c124a}
```

20、账号被盗了

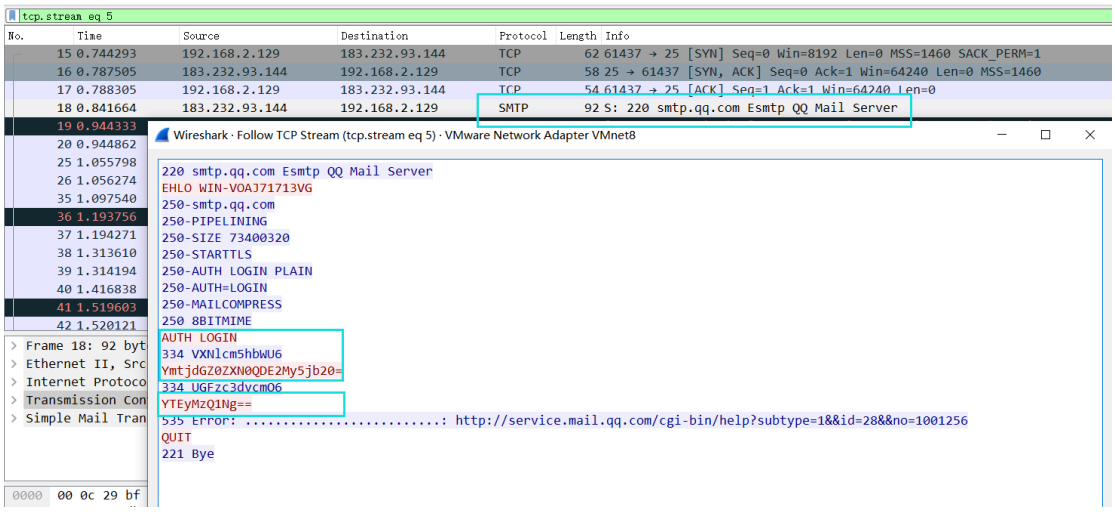
修改 cookie 得到新的 Url



Login 游戏界面

填写信息进行抓包，真的可以刷枪，你信不 233333

过滤 TCP 可以看到特殊流量



可以看到，上面 base64 编码内容是某账号账户和密码

利用账号登陆 163 邮箱得到 flag

get flag:

```
flag{182100518+725593795416}
```

21、细心的大象

细心的大象

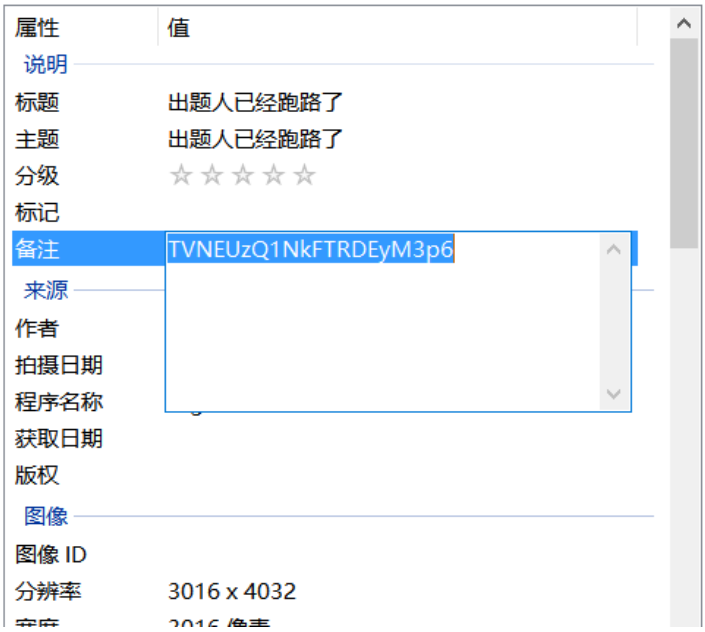
100

https://share.weiyun.com/9287be0a629971ac53d97f39727eee18

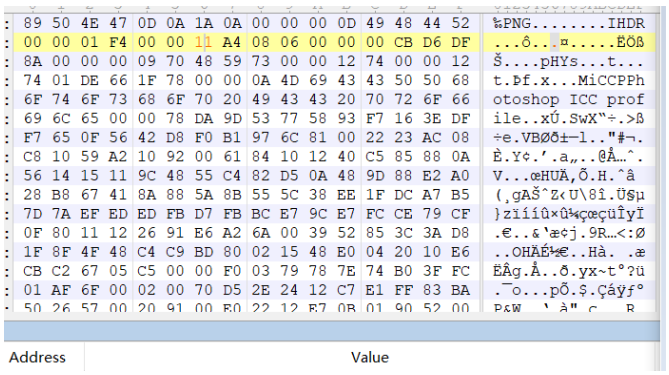
Flag

Submit

查看图片属性



foremost 分离处压缩包，利用图片备注信息 base64 解码进行解密得到图片，修改图片高度得到 flag



BUGKU{a1e5aSA}

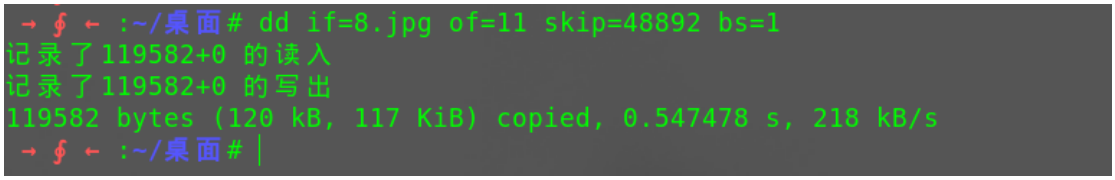
get flag:

```
BUGKU{a1e5aSA}
```

22、爆照(08067CTF)

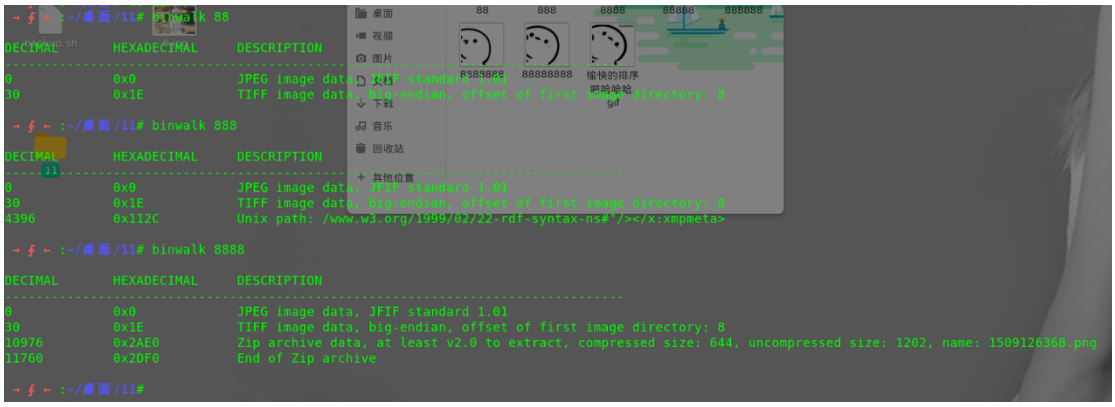
binwalk 分析图片发现隐藏文件，利用 binwalk 和 foremost 分离隐藏文件，只能得到 88 文件其他的不到，此时利用 dd 命令进行分离


```
dd if=8.jpg of=11 skip=48892 bs=1
```



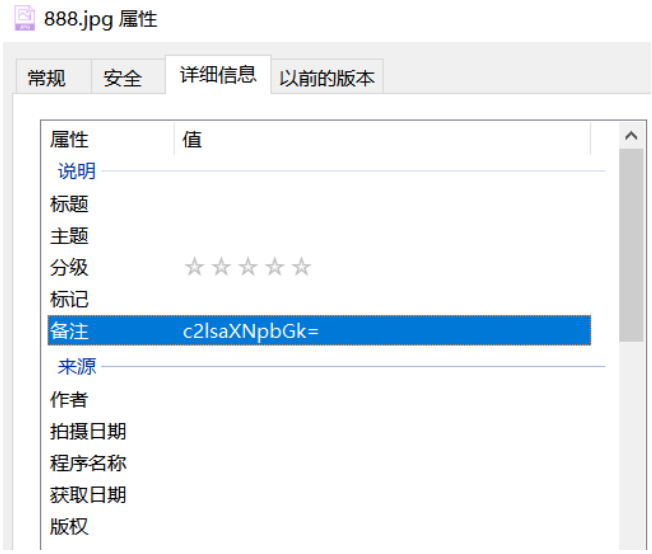
得到几张图片

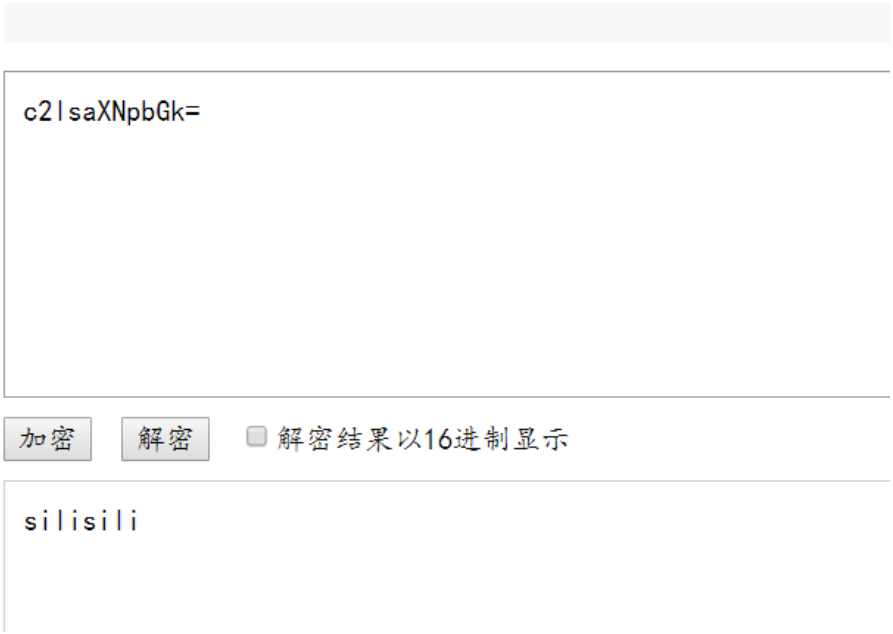
binwalk 分析这几张图片，发现前三张存在被修改的记录



第一张包含二维码直接扫描得到：bilibili

第二张图片属性中存在特殊字符串，对其进行解码





第三张图片 binwalk 分析，分离出压缩包，得到一张二维码，扫描得到：panama

根据题目 flag 提示，将上述得到的三个字符串组合成最终的 flag

get flag:

```
flag{bilibili_silisili_panama}
```

23、猫片(安恒)

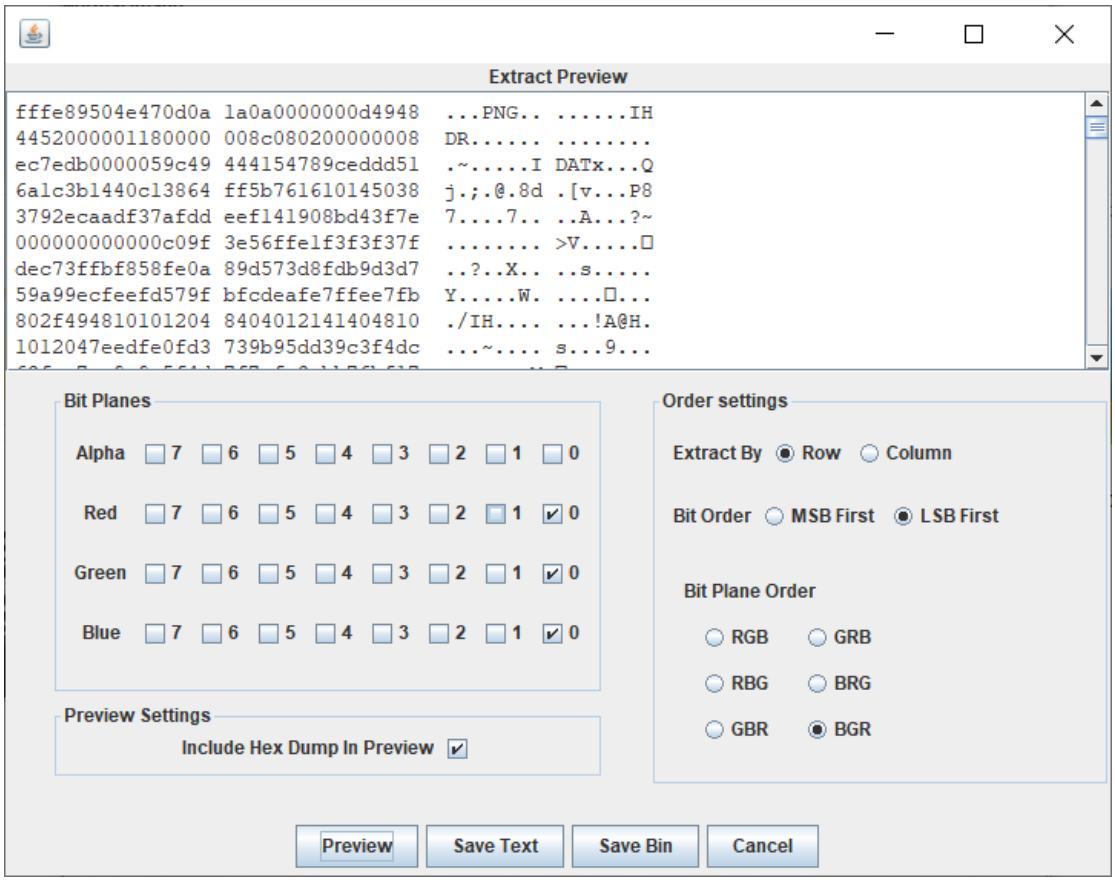
猫片(安恒)

100

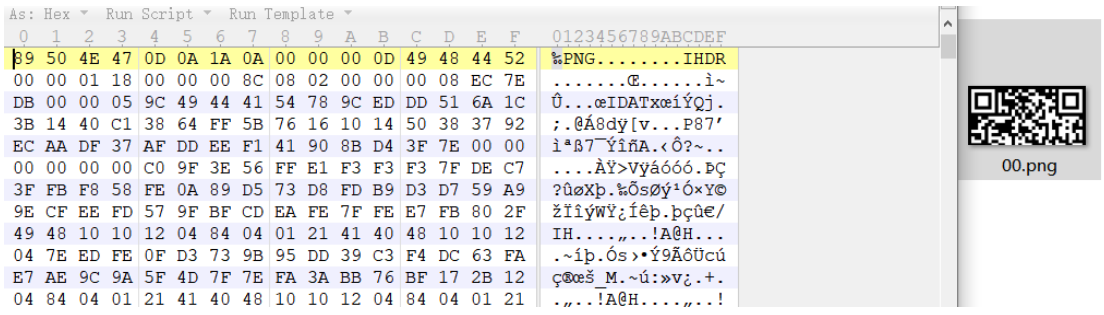
hint:LSB BGR NTFS

png

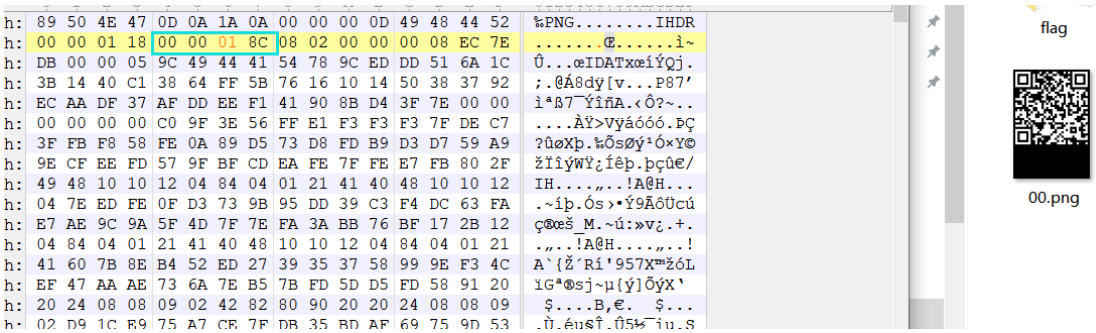
根据提示 LSB 隐写得到新的二维码



修改图片头部得到二维码

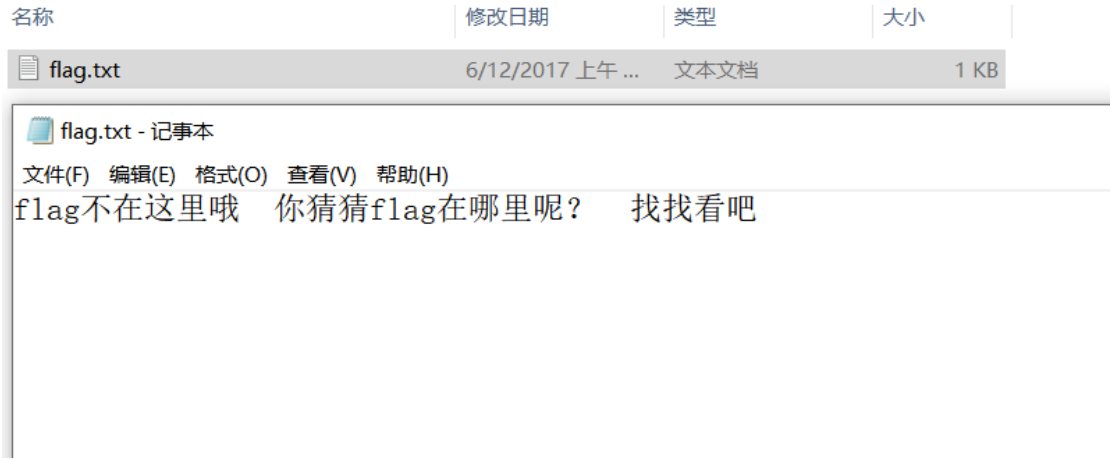


下意识修改图片高度，得到完整二维码

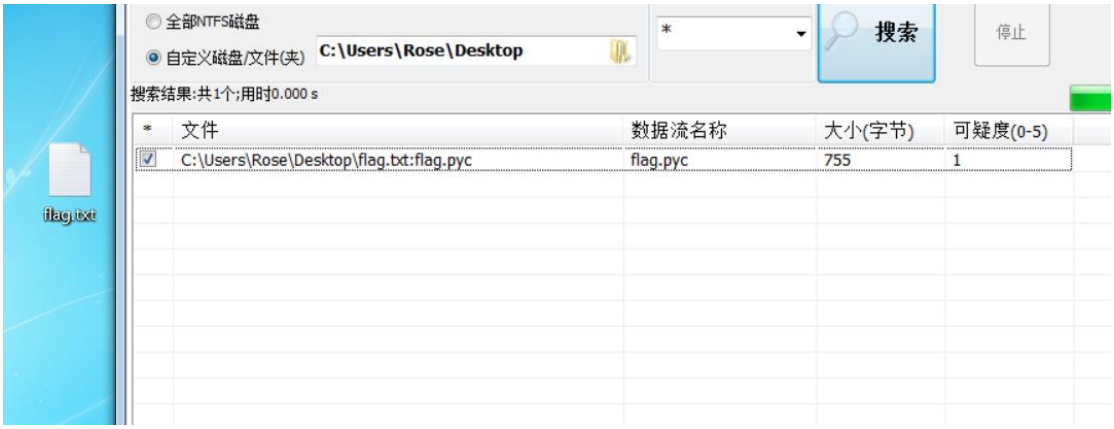


扫描二维码得到云盘连接：https://pan.baidu.com/s/1pLT2J4f

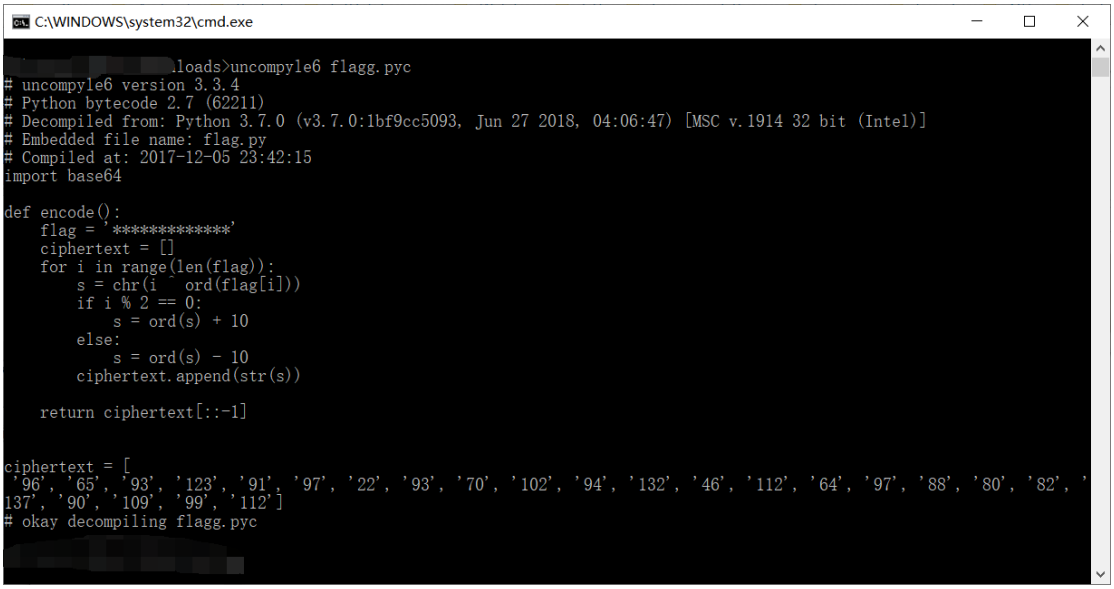
链接下载得到 flag.rar 压缩包，使用 WinRAR 解压，得到 flag.txt，发现并不是 flag，依据题目提示还有一个提示 NTFS 没有用到，于是利用工具 ntfsstreamseditor 进行提取，得到一个 pyc 文件，将 pyc 反编译回去，得到一个 python 的 flag 加密函数。



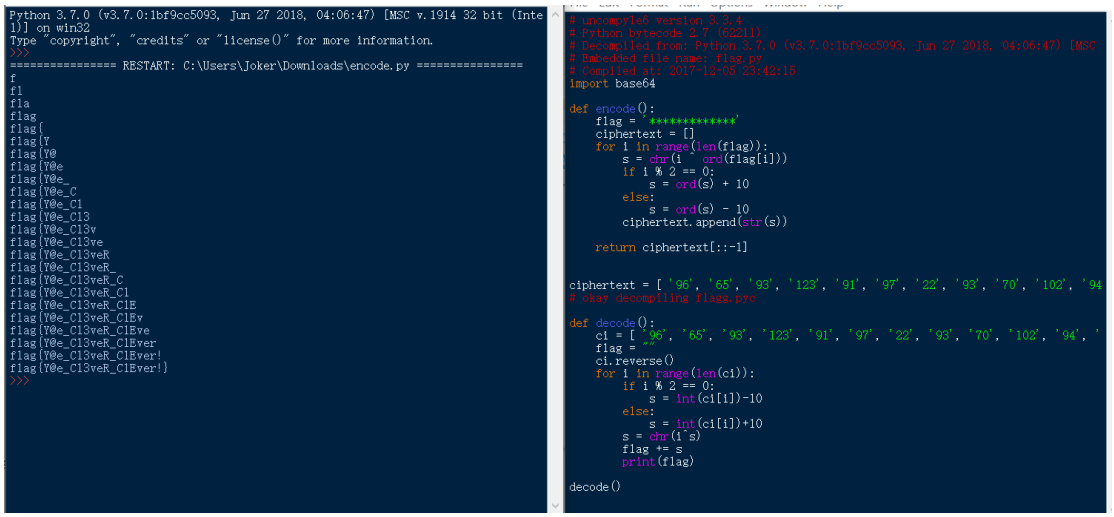
NTFS 数据提取



pyc 反编译



编写相应的解密函数得到解密的 flag



get flag:

```
flag{Y@e_C13veR_C1Ever!}
```

24、多彩

该题脑洞很大！！！！

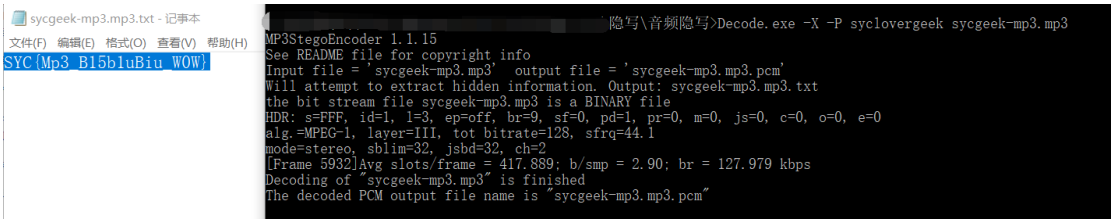
附上安全脉搏一篇详细的 writeup

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

25、旋转跳跃

利用音频分析工具 MP3Steno，结合 key 直接进行解码得到 sycgeek-mp3.mp3.txt

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

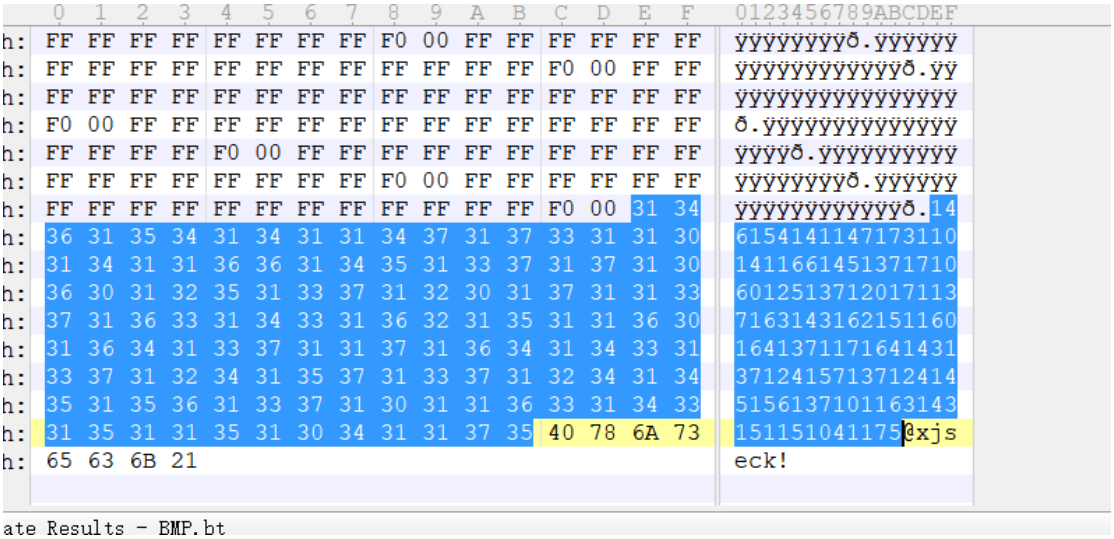


get flag:

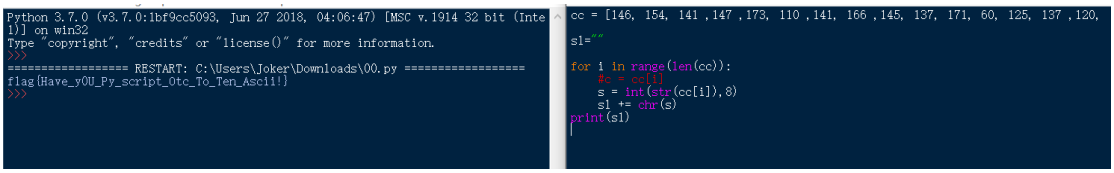
```
SYC{Mp3_B15b1uBiu_W0W}
```

26、普通的二维码

查看图片十六进制得到特殊字符串



分析这一串数字，每三个数的前面大部分都是 1，可能是 8 进制对应的 Ascii 值，将其转码

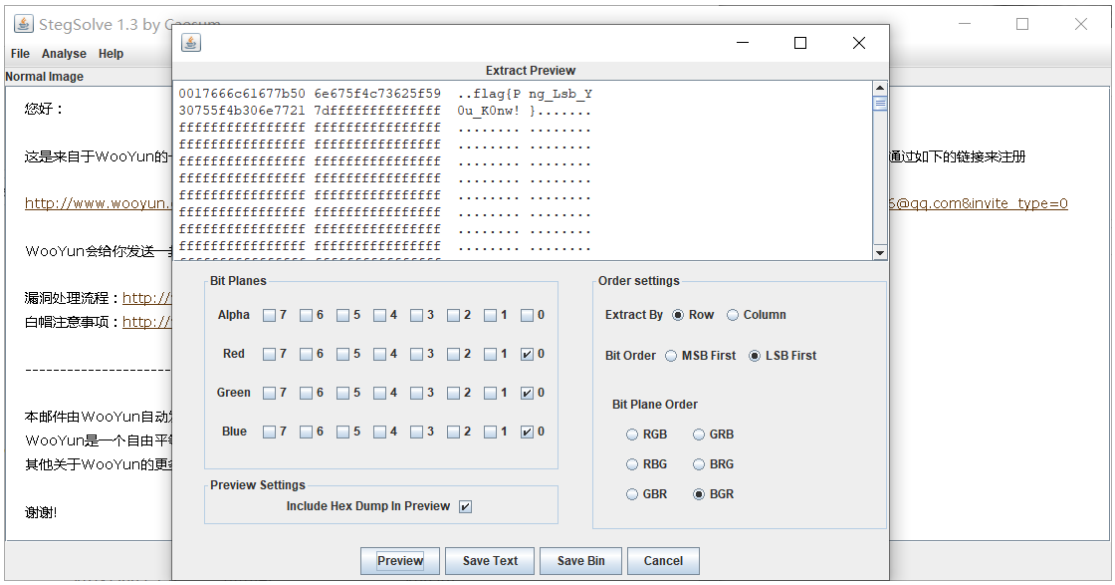


get flag:

```
flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}
```

27、乌云邀请码

LSB 隐写

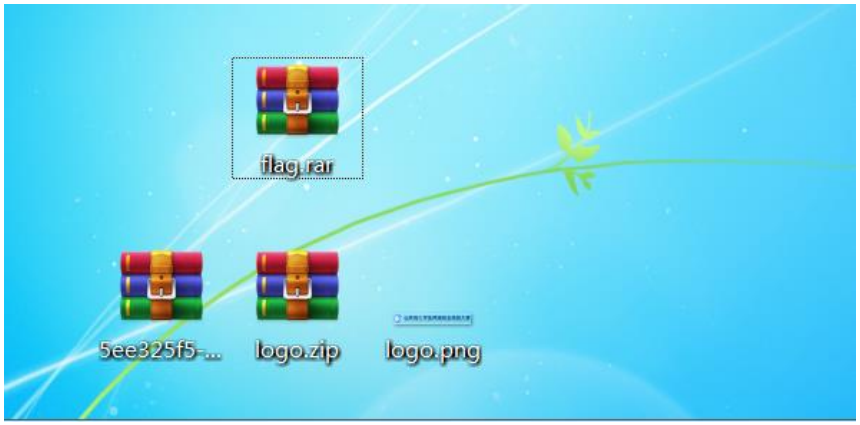


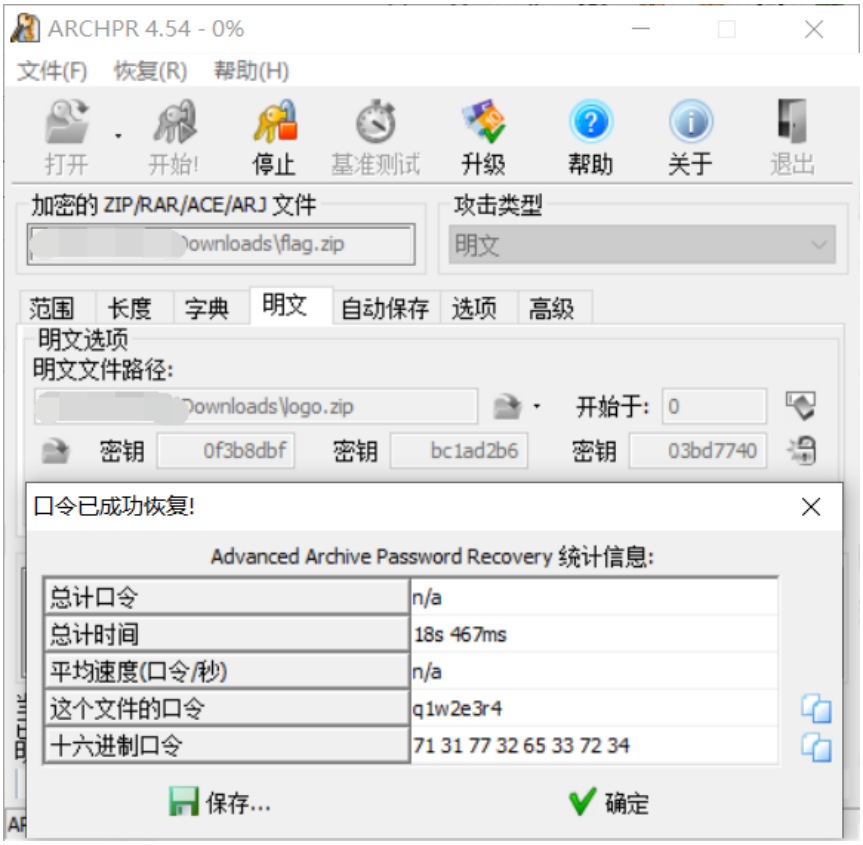
get flag:

```
flag{Png_Lsb_Y0u_K0nw!}
```

28、神秘的文件

分析压缩包，可知明文攻击，利用 WinRAR 解压，并且压缩图片 logo.png 作为明文攻击





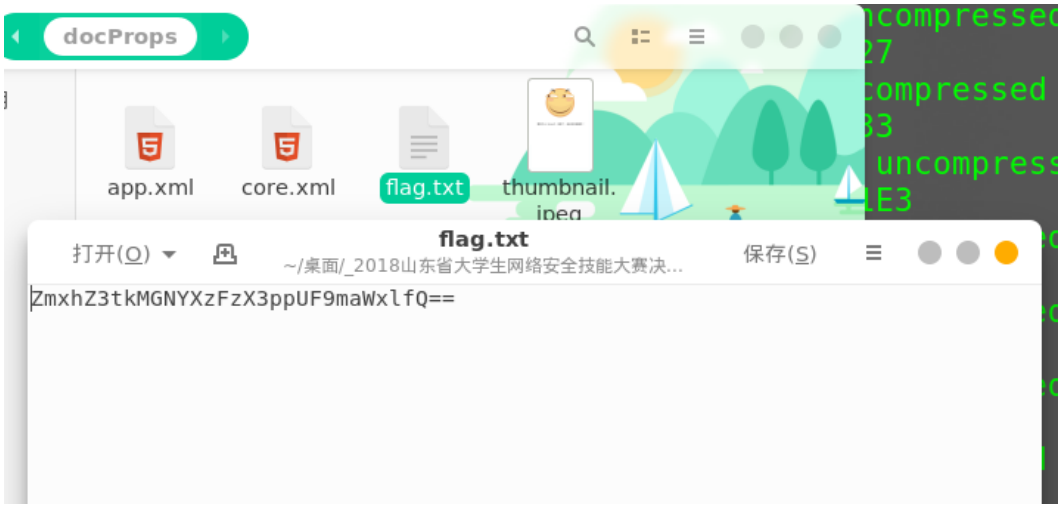
得到口令：q1w2e3r4，解压得到 word 文档发现并没有什么

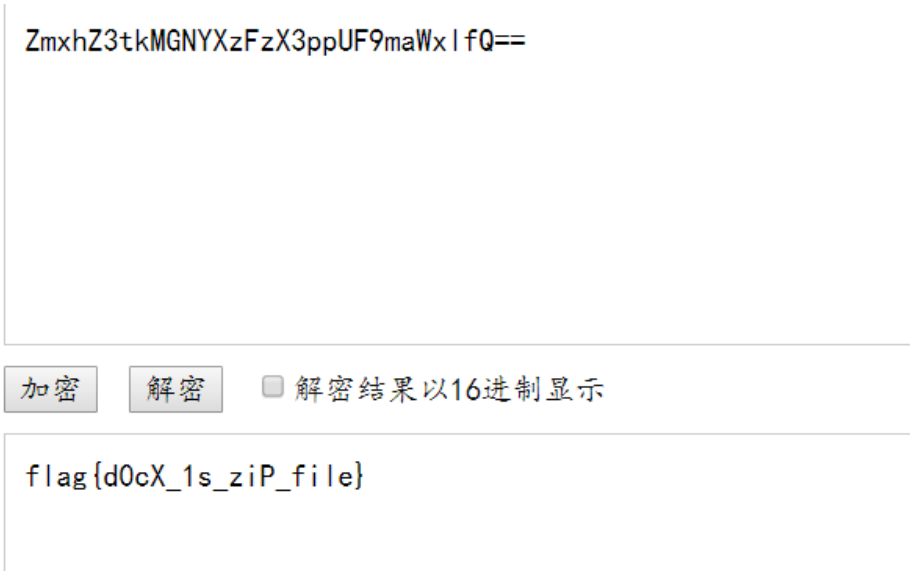
哪有什么 WriteUP，别想了，老老实实做题吧！

利用 binwalk 分析 word 文档得到发现存在隐藏文件

```
→ ~ :~/桌面# binwalk 2018山东省大学生网络安全技能大赛决赛writeup.docx

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size:
672           0x2A0           Zip archive data, at least v2.0 to extract, compressed size:
1370          0x55A           Zip archive data, at least v1.0 to extract, compressed size:
il.jpeg
37875         0x93F3          Zip archive data, at least v2.0 to extract, compressed size:
39207         0x9927          Zip archive data, at least v2.0 to extract, compressed size:
39731         0x9B33          Zip archive data, at least v1.0 to extract, compressed size:
ge1.png
262627        0x401E3         Zip archive data, at least v2.0 to extract, compressed size:
263791        0x4066F         Zip archive data, at least v2.0 to extract, compressed size:
266756        0x41204         Zip archive data, at least v2.0 to extract, compressed size:
xml
268319        0x4181F         Zip archive data, at least v2.0 to extract, compressed size:
268656        0x41970         Zip archive data, at least v2.0 to extract, compressed size:
xml.rels
269244        0x41BBC         Zip archive data, at least v2.0 to extract, compressed size:
270175        0x41F5F         Zip archive data, at least v2.0 to extract, compressed size:
270991        0x4228F         Zip archive data, at least v2.0 to extract, compressed size:
272048        0x426B0         End of Zip archive
```

分离文件找到 flag.txt 解码得到 flag





get flag:

```
flag{dOcX_1s_ziP_file}
```

update+ing