BUUCTF——MISC

原创

皮皮要开心每一天 于 2020-04-14 19:55:38 发布 2895 收藏 12

文章标签： 安全

本文链接：https://blog.csdn.net/bdm1121/article/details/105477137

1 签到

flag：flag{buu_ctf}

2 金仨胖

gif文件，用2345看图王打开，可以看到得到三段信息图片，组合后得到flag：

flag{he11ohongke}

3 二维码

扫描二维码提示secret is here，binwalk图片得到一个压缩包，提示4位数，爆破得到密码7639，解压得到flag：

flag{vjpw_wnoei}

4 N种解决方法

得到exe文件，用notepad打开发现图片base64密码，使用在线图片编码得到一张二维码图片：

flag{dca57f966e4e4e31fd5b15417da63269}

5 大白

一张不完整png，拖入010editor，提示crc错误，使用脚本跑出图片宽高为679*479，修改高度之后得到flag：

flag{He1l0_d4_ba1}

6 基础破解

解压得到一个rar包，4位纯数字爆破得到密码2563，解压得到

ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=，base64解密得到flag：

flag{70354300a5100ba78068805661b93a5c}

7 你竟然赶我走

解压文件后得到一张jpg图片，用winhex打开，拉到最后发现flag：

flag{stego_is_s0_bor1ing}

8 LSB

考察lsb隐写，拖入stegsolve，打开Data Extract，save bin，得到一张二维码，扫描得到flag：

flag{1sb_i4_s0_Ea4y}

9 乌镇峰会种图

用winhex打开，拉到最后发现flag：

flag{97314e7864a8f62627b26f3f998c37f1}

10 rar

4位纯数字爆破得到密码8795，解压得到flag：flag{1773c5da790bd3caff38e3decd180eb7}

11 qr

用QR Research扫描二维码，得到flag：

flag{878865ce73370a4ce607d21ca01b5e59}

12 文件中的秘密

解压得到一张图片，用winhex打开，发现flag：flag{870c5a72806115cb5439345d8b014396}

13 ningen

用binwalk分离图片，得到一个压缩包，根据提示4位数，爆破得到密码8368，解压得到flag：
flag{b025fc9ca797a67d2103bfbc407a6d5f}

14 wireshark

打开流量文件，筛选http协议，追踪tcp流，得到password：
email=flag&password=ffb7567a1d4f4abdffdb54e022f8facd

15、你有没有好好看网课

得到两个压缩包，其中一个注释提示6位数密码，暴力破解得到密码183792，解压后得到一个word文档和视频文件，根据内容提示，520/711，在视频5秒20、7秒11里可以看到

找到视频里的隐藏信息，

… …/… ./… ./… …/

dXBfdXBfdXA= base64解压为up_up_up

第一部分百度发现是敲击码：

敲击码

敲击码(Tap code)是一种以非常简单的方式对文本信息进行编码的方法。因该编码对信息通过使用一系列的点击声音来编码而命名，敲击码是基于5×5方格波利比奥斯方阵来实现的，不同点是是用K字母被整合到C中。

敲击码表：

#!shell

1 2 3 4 5

1 A B C/K D E

2 F G H I J

3 L M N O P

4 Q R S T U

5 V W X Y Z

比如：F是（2,1… .）、O是（3,4 … …）

… …/… ./… ./… …/ 得到wllm

用wllmup_up_up解压flag2压缩包，把图片拖进winhex

swpuctf{A2e_Y0u_Ok?}

16、吹着贝斯扫二维码

打开压缩包，看到有注释：

GNATOMJVIQZUKNJXGRCTGNRTGI3EMNZTGNBTKRJWGI2UIMRRGNBDEQZWGI3DKMSFGNCDMRJTII3TMNBQGM4TERRTGEZTOMRXGQYDGOBWGI2DCNBY

用winhex查看其他文件发现是jpg文件，修改后缀得到36张局部二维码图片，手动拼二维码。

扫描二维码得到：BASE Family Bucket ???

85->64->85->13->16->32

将之前得到的

base32：

3A715D3E574E36326F733C5E625D213B2C62652E3D6E3B7640392F3137274038624148

base16：

:q]>WN62os<^b]!;,be.=n;v@9/17’@8bAH

base13/rot13:

:d]>JA62bf<^o]!;,or.=a;i@9/17’@8oNU

base85：

PCtvdWU4VFJnQUByYy4mK1lraTA=

base64：

<+oue8TRgA@rc.&+Yki0

base85：

ThisIsSecret!233

解压压缩包得到flag

flag{Qr_Is_MeAn1nGfuL}

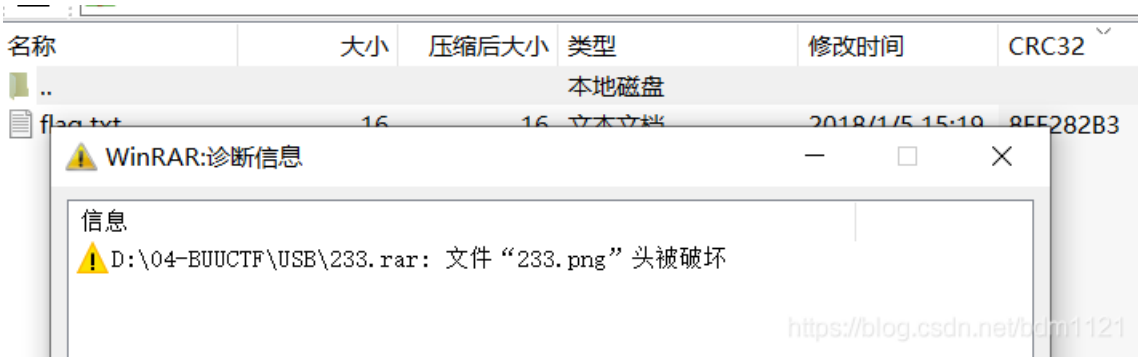
17、SXMgdGhpcyBiYXNlPw==

根据题目标题解码得到“Is this base?”，打开txt可以发现是base64隐写，使用工具得到GXY{fazhazhenhaoting}?

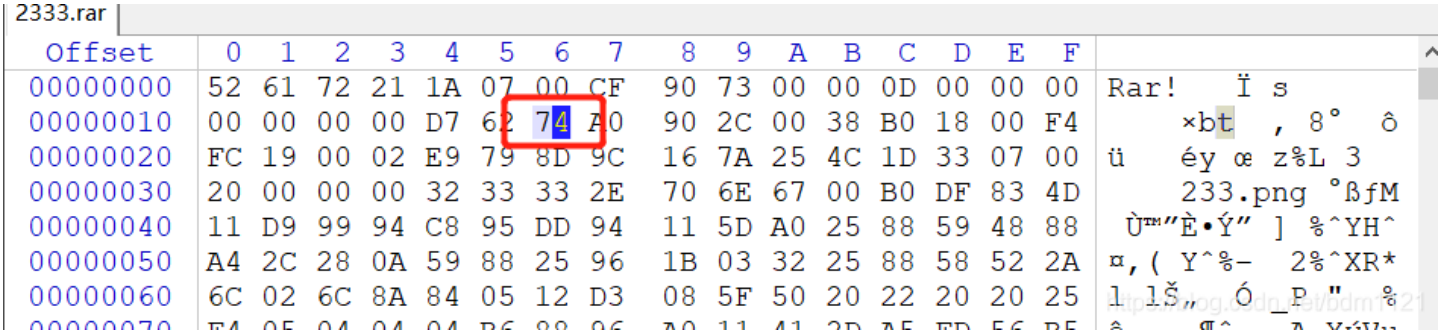
提交flag：flag{fazhazhenhaoting}

18、USB

用WinRAR打开提示



需要修复此压缩包，用winhex打开，RAR文件头的头类型必须是0x74
将233.png前面的7A改为74。



解压文件得到一张png图片，用stegsolve打开查看可以看到一张二维码，*扫描得到ci{v3erf_0tygidv2_fc0}*

再分析另外一个文件，binwalk key.ftm文件可以得要一个流量包文件key.pcap
根据题目提示可知此题是USB流量分析

先在kali下通过命令得到pcap包中的数据部分，命令如下：

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

再通过usb脚本解码，得到

```
    0x2C: " ",
    0x2D: "-",
    0x2E: "=",
    0x2F: "[",
    0x30: "]"
}
nums = []
keys=open('data.txt')
for line in keys:
    if line[0]!='0'or line[1]!='0'or line[3]!='0'or line[4]!
        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
```

```
output:nKEYXINAN
[Finished in 0.2s]
```

https://blog.csdn.net/bdm1121

得到key：XINAN

维基利亚解密得到：fa{i3eei_0llgvgn2_sc0}

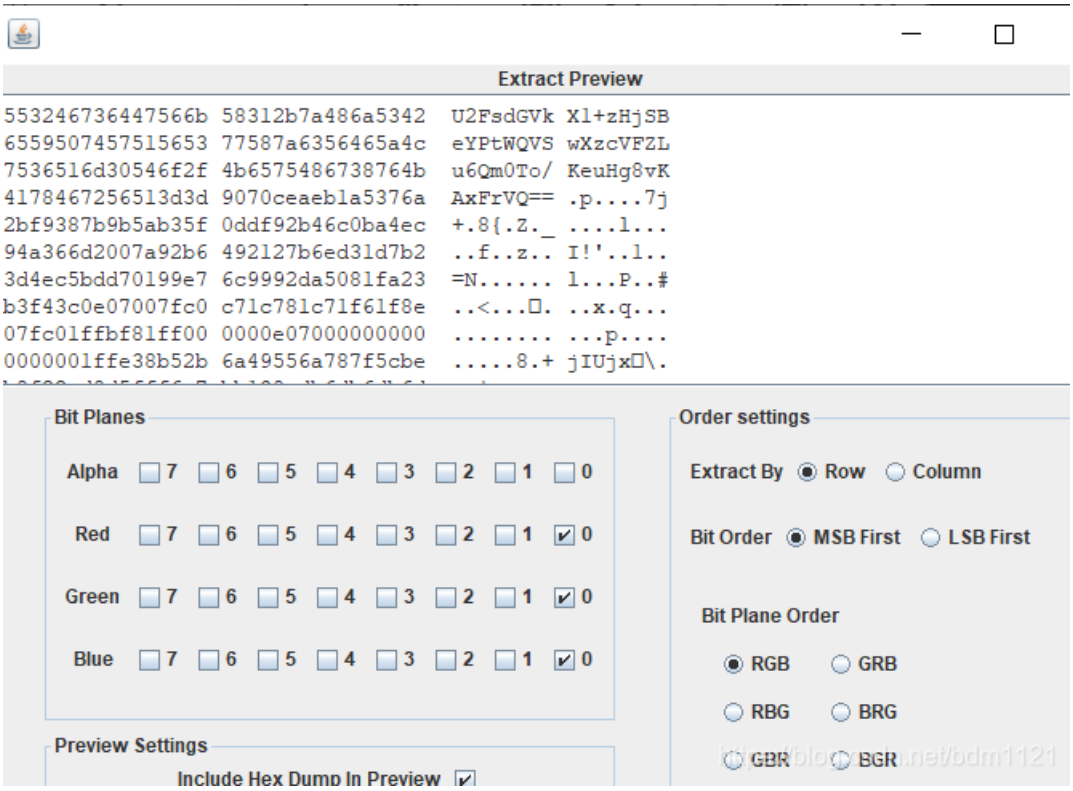
明显的栅栏分组：flag{vig3ne2e_is_c00l}

19、game

解压文件，有个index.html，用notepad++打开看到flag：ON2WG5DGPNUECSDBNBQV6RTBNMZV6RRRMFTX2===

base32解码得到：suctf{hAHaha_Fak3_F1ag}

再分析图片，lsb



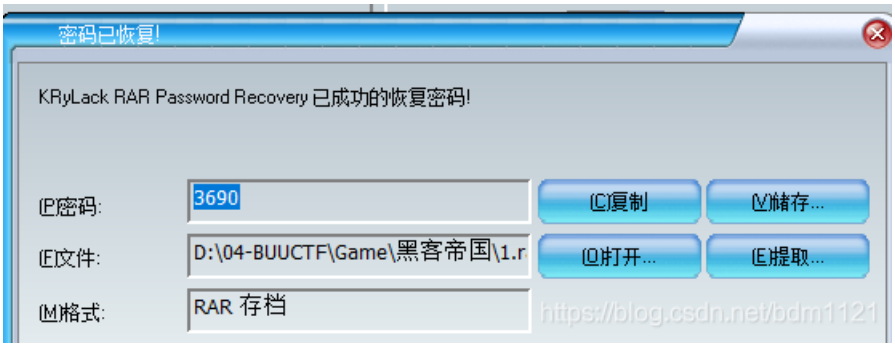
得到：

U2FsdGVkX1+zHjSBeYPtWQVSwXzcVFZLu6Qm0To/ KeuHg8vKAxFrVQ==

用上面得到的字符串当key，TripleDES解密：

20、黑客帝国

打开文件看到52617221，猜到是rar文件，用winhex打开得到一个加密的rar文件，直接用破解软件爆破，得到密码



解压之后得到一张png图片，拖进010editor提示不是png图片，文件头看到JFJF，想到是jpg图片，修改文件头，打开看到flag。

21、KO

使用ook在线解码。得到welcome to CTF

22、network

打开文本看有四个数字

63 00111111

127 01111111

191 10111111

255 11111111

可以看到8位二进制的前两位是不一样的，写一个脚本所有数字的最高两位提取出来，并且4个一组转换位ASCII。发现写出来的16进制数开头是504B。

```python
fp = open('Network.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.zip','wb')
wp.write(flag)
wp.close()
```


使用伪加密得到解密的压缩包。

```
(c) 2019 Microsoft Corporation。保留所有权利。

D:\Zip伪加密>java -jar ZipCenOp.jar r D:\04-BUUCTF\Game\flag.zip
success 3 flag(s) found
```

得到一个TXT文件，base64加密，多次base64次解密得到flag

![在这里插入图片描述](https://img-blog.csdnimg.cn/20200417224601358.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L2JkbTExMjE=,size_16,color_FFFFFF,t_70

23、丢失的MD5

根据题目给的信息写python脚本，运行即可。

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'.encode('utf-8')+chr(i).encode('utf-8')+'O3RJMV'.encode('utf-8')+chr(j).encode('utf-8
')+'WDJKX'.encode('utf-8')+chr(k).encode('utf-8')+'ZM'.encode('utf-8'))
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print (des)
```

24、篱笆墙的影子

栅栏分组，flag{wethinkwehavetheflag}

25、[BJDCTF 2nd]最简单的misc-y1ng

伪加密，解压文件得到一个文件，发现确实png图片头部，补齐得到一张png图片，得到一串16进制，转化得到flag：
BJD{y1ngzuishuai}

26、[BJDCTF 2nd]A_Beautiful_Picture

用010winhex打开提示错误，使用脚本跑出该图片的宽高为1000*1000，修改之后看到flag。
BJD{PnG_He1ghT_1s_WR0ng}

27、[BJDCTF 2nd]小姐姐-y1ng

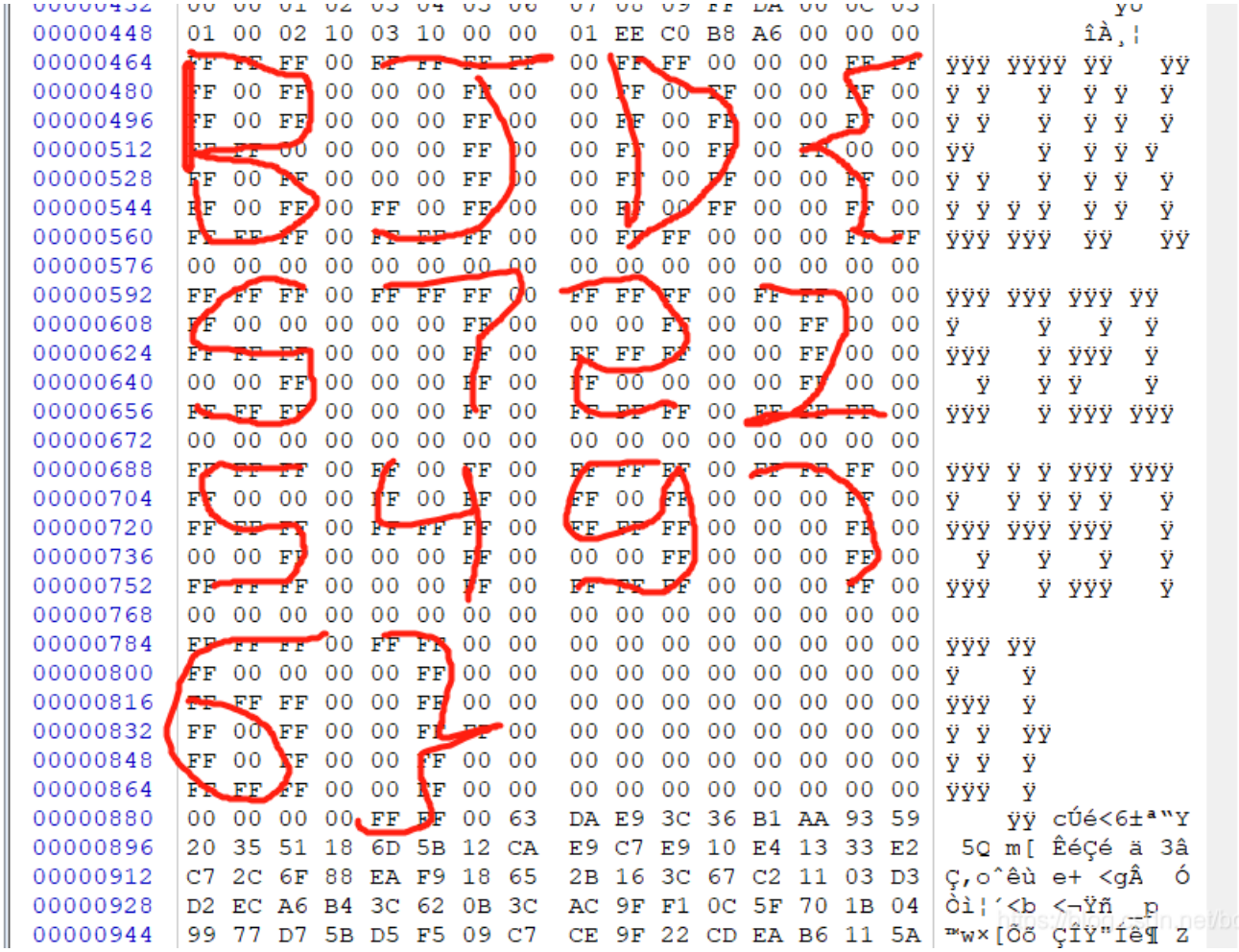
在kali下strings，得到一串字符串。
BJD{haokanma_xjj}

28、[BJDCTF 2nd]EasyBaBa

用winhex打开图片，查找FFD9，可以看到后面接了一个zip文件。手动分解出来，解压得到一张jpg图片，但是打不开，看到里面有primer字眼，在kali下分析文件属性，发现是avi文件，用pr打开，逐帧分解，可以看到有4张二维码图片，第四张要调整一下亮度才能扫错出来，得到一串16进制：
6167696E5F6C6F76655F59424A447B696D316E677D，hex转text，得到agin_love_YBJD{im1ng}
调整一下。
BJD{imagin_love_Y1ng}

29、[BJDCTF 2nd]Real_EasyBaBa

用winhex打开



```
00000432  00 00 01 02 03 04 05 06  07 08 09 FF DA 00 0C 03  ÿÚ
00000448  01 00 02 10 03 10 00 00  01 EE C0 B8 A6 00 00 00  îÀ¸¦
00000464  FF FF FF 00 FF FF FF FF  00 FF FF 00 00 00 FF FF  ÿÿÿ ÿÿÿÿ ÿÿ   ÿÿ
00000480  FF 00 FF 00 00 00 FF 00  00 FF 00 FF 00 00 FF 00  ÿ ÿ   ÿ  ÿ ÿ  ÿ
00000496  FF 00 FF 00 00 00 FF 00  00 FF 00 FF 00 00 FF 00  ÿ ÿ   ÿ  ÿ ÿ  ÿ
00000512  FF FF 00 00 00 00 FF 00  00 FF 00 FF 00 FF 00 00  ÿÿ    ÿ  ÿ ÿ ÿ
00000528  FF 00 FF 00 00 00 FF 00  00 FF 00 FF 00 00 FF 00  ÿ ÿ   ÿ  ÿ ÿ  ÿ
00000544  FF 00 FF 00 FF 00 FF 00  00 FF 00 FF 00 00 FF 00  ÿ ÿ ÿ ÿ  ÿ ÿ  ÿ
00000560  FF FF FF 00 FF FF FF 00  00 FF FF 00 00 00 FF FF  ÿÿÿ ÿÿÿ  ÿÿ   ÿÿ
00000576  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000592  FF FF FF 00 FF FF FF 00  FF FF FF 00 FF FF 00 00  ÿÿÿ ÿÿÿ ÿÿÿ ÿÿ
00000608  FF 00 00 00 00 00 FF 00  00 00 FF 00 00 FF 00 00  ÿ     ÿ   ÿ  ÿ
00000624  FF FF FF 00 00 00 FF 00  FF FF FF 00 00 FF 00 00  ÿÿÿ   ÿ ÿÿÿ  ÿ
00000640  00 00 FF 00 00 00 FF 00  FF 00 00 00 00 FF 00 00    ÿ   ÿ ÿ    ÿ
00000656  FF FF FF 00 00 00 FF 00  FF FF FF 00 FF FF FF 00  ÿÿÿ   ÿ ÿÿÿ ÿÿÿ
00000672  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000688  FF FF FF 00 FF 00 FF 00  FF FF FF 00 FF FF FF 00  ÿÿÿ ÿ ÿ ÿÿÿ ÿÿÿ
00000704  FF 00 00 00 FF 00 FF 00  FF 00 FF 00 00 00 FF 00  ÿ   ÿ ÿ ÿ ÿ   ÿ
00000720  FF FF FF 00 FF FF FF 00  FF FF FF 00 00 00 FF 00  ÿÿÿ ÿÿÿ ÿÿÿ   ÿ
00000736  00 00 FF 00 00 00 FF 00  00 00 FF 00 00 00 FF 00    ÿ   ÿ   ÿ   ÿ
00000752  FF FF FF 00 00 00 FF 00  FF FF FF 00 00 00 FF 00  ÿÿÿ   ÿ ÿÿÿ   ÿ
00000768  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000784  FF FF FF 00 FF FF 00 00  00 00 00 00 00 00 00 00  ÿÿÿ ÿÿ
00000800  FF 00 00 00 00 FF 00 00  00 00 00 00 00 00 00 00  ÿ    ÿ
00000816  FF FF FF 00 00 FF 00 00  00 00 00 00 00 00 00 00  ÿÿÿ  ÿ
00000832  FF 00 FF 00 00 FF FF 00  00 00 00 00 00 00 00 00  ÿ ÿ  ÿÿ
00000848  FF 00 FF 00 00 FF 00 00  00 00 00 00 00 00 00 00  ÿ ÿ  ÿ
00000864  FF FF FF 00 00 FF 00 00  00 00 00 00 00 00 00 00  ÿÿÿ  ÿ
00000880  00 00 00 00 FF FF 00 63  DA E9 3C 36 B1 AA 93 59      ÿÿ cÚé<6±ª"Y
00000896  20 35 51 18 6D 5B 12 CA  E9 C7 E9 10 E4 13 33 E2   5Q m[ ÊéÇé ä 3â
00000912  C7 2C 6F 88 EA F9 18 65  2B 16 3C 67 C2 11 03 D3  Ç,oˆêù e+ <gÂ  Ó
00000928  D2 EC A6 B4 3C 62 0B 3C  AC 9F F1 0C 5F 70 1B 04  Òì¦´<b <¬Ÿñ _p
00000944  99 77 D7 5B D5 F5 09 C7  CE 9F 22 CD EA B6 11 5A  ™w×[ÕõÇÎŸ"ÍêÂ¶ Z
```

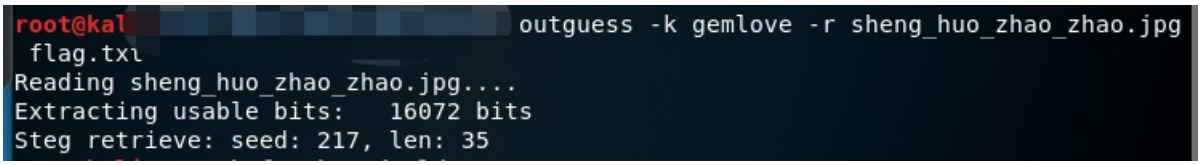

BJD{572154976}

30、[BJDCTF 2nd]圣火昭昭-y1ng

查看图片属性，新佛曰：諸壽隸僧壽降吽壽諸壽陀壽摩隸僧缽薩願心壽咤壽囉寂壽闍諸壽哆壽慧壽聞壽色吽愍壽所壽蜜如

题目提示：开局一张图，flag全靠猜

因为出题人失误搞错了，解出来的key去掉后3位的com，得到flag。



31、[BJDCTF 2nd]TARGZ-y1ng

压缩包的名字是解压密码，写脚本逐个解压，最后得到一个flag文件

```
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()
```

BJD{wow_you_can_rea11y_dance}

*32、开场曲**

玩mikutap，根据键盘键位打出相似的拍子，然后移位得到密码

hint：大写、mikutap、开场曲重复了两遍、flag交一遍的就行、格式BJD{字母+数字}、数字范围0-5

（横，圈点，实心方块）x 2+（叉，空心方块，实心散布圆，空心散布圆，实心方块，空心多边形，实心多边形）x 2+（中心出发圆，中心出发圆，空心多边形，中心出发圆）x 2

最后得到flag：BJD{MIKUTAP3313313}