BUUCTF-刷题记录-5

原创

秋风瑟瑟... 于 2020-10-03 00:46:12 发布 342 收藏

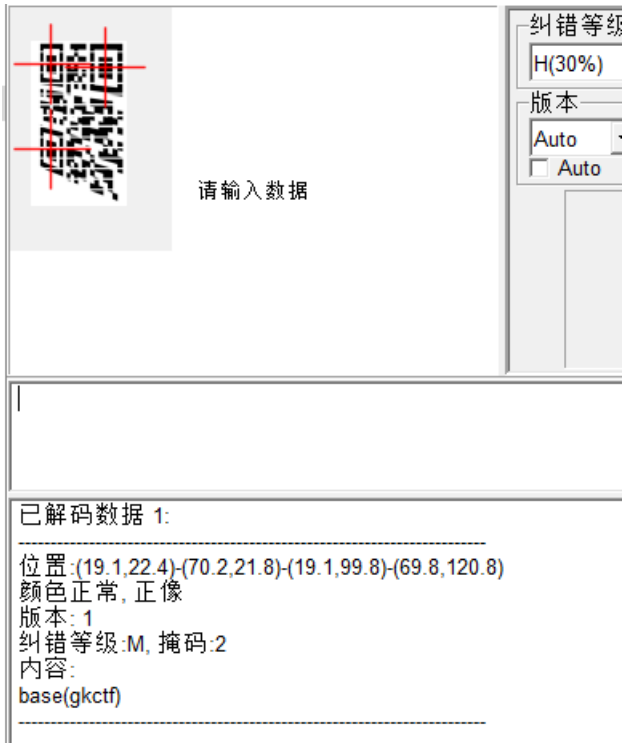
分类专栏： BUUCTF刷题记录

本文链接：https://blog.csdn.net/qq_45628145/article/details/108877156

MISC

[GKCTF2020]code obfuscation

把给的二维码缩小一下，截个图，就可以用QR扫出来了，得到一个base(gkctf)，同时binwalk分离出来一个存在密码的压缩包，猜测是某种base方法得到的结果为压缩包的密码。



最后尝试出来base58编码后的gkctf即为压缩包的密码，即 `CfjxaPF` 。

解压出来一张图片和一段JS代码，JS代码去这个在线网站解密并且整理一下，得到

```
for n in a b c d e f g h i j k l m n o p q r s t u v w x y z do eval An = "n"
done
for n in A B C D E F G H I J K L M N O P Q R S T U V W X Y Z do eval An = "n"
done num = 0
for n in a b c d e f g h i j do eval Bn = "n"
num = $((num + 1))
done alert("Bk=' ';Bm='"';Bn='#';Bs='(';Bt=')';By='.';Cb=';';Cc=' < ';Ce=' > ';Cl='_';Cn='{';Cp='}';Da='0';Db='1
';Dc='2';Dd='3';De='4';Df='5';Dg='6';Dh='7';Di='8';Dj='9';")
```

再把图片中的内容一一对换即可，最后得到`flag{w3lc0me_4o_9kct5}`。

[安洵杯 2019]easy misc

压缩包有个密码，而且有注释

```
FLAG IN ((√2524921X85÷5+2)÷15-1794)+NNULLULL,
```

计算可得前面的算式答案为7

```
>>> ((2524921**0.5)*85/5+2)/15-1794
7.0
```

也就是密码应该为7位数字+NNULLULL,，爆破一下即可得到密码`2019456NNULLULL,`，注意最后的`,`。

给的一张图片里面分离出来两张一样的图片，盲水印处理，得到提示

```
C:\Users\ieven\Desktop\CTF\misc\工具\BlindWaterMark-new>python2 bwm.py decode 1.png 2.png out.png
image<1.png> + image(encoded)<2.png> -> watermark<out.png>
```

根据解压出来的东西和这个提示，猜测是统计11.txt的字频，然后取其前16个字符，替换一下，再进行一个解码，这里把文件中的空格和制表符也放进去一起统计了，脚本如下

```
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+-    ={}[]"
f = open("11.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))
print(''.join(sort_by_value(result)))
```

得到结果

```
etaonrhisdluygw
```

替换一下，得到

```
QW8obWdIWT9pMkF5REtRQSQWjVfXiE/WSFTajBtcw=
```

但是这题网上的解是有点奇怪的。。。为什么网上都是得到

```
QW8obWdIWT9pMkFSQWtRQjVfXiE/WSFTajBtcw==
```

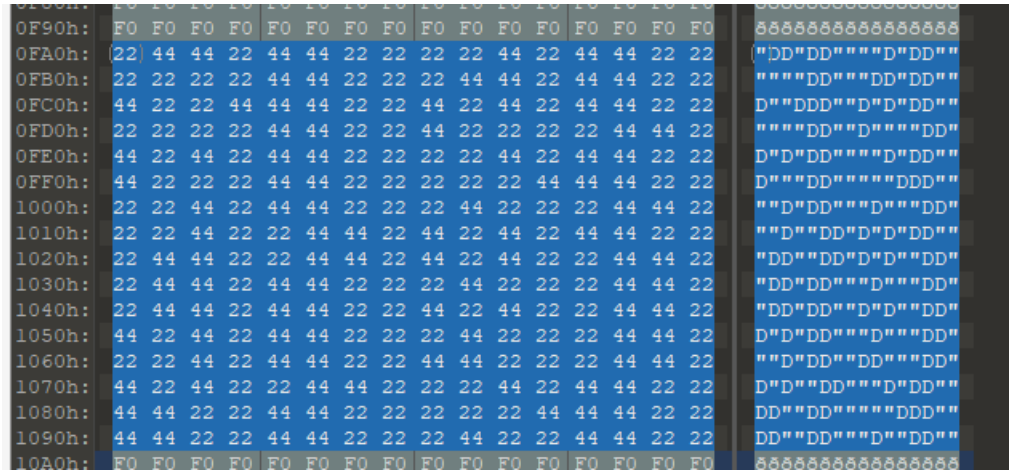
无缘无故的去掉了两个字符，然后还更换了i和s的顺序，可能是题目出了点问题，根据这个，base64解码得到

```
Ao(mgHY?i2ARAkQB5_^!?Y!Sj0ms
```

再进行base85解码得到`flag{have_a_good_day1}`

派大星的烦恼

根据题目的提示，在图片中发现了一段0x22和0x44，提取出来



把 `"` 换成0， `D` 换成1，刚好一共是256个字符
直接按照顺序每8个二进制数，转换成字符的话，是乱码的

```
l,
  l¬
    ¬,,F&¬f¦lFl¦¬F,Æ¦,ÌÌL
```

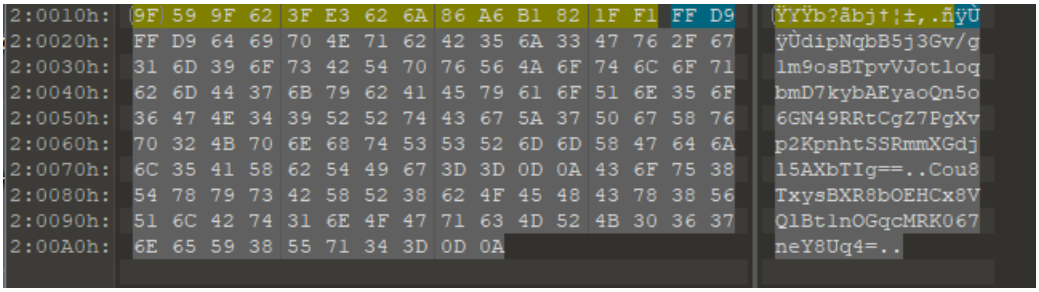
然后尝试反向输出，取每8位二进制数，反向输出字符，得到了flag

```python
s = "01101100001011000000110001101100100111001010110000000110010000110101011000010110010001100000111000010110001000110101011000110011010100110011011000100011001101100101001101010110001000110001011001100011010100110001100110000011100110011000110001001100"
flag= ""

for i in range(0,len(s),8):
    flag += chr(int(s[i:i+8][::-1],2))
    # flag += chr(int(s[i:i+8],2))

print(flag)
# 6406950a54184bd5fe6b6e5b4ce43832
```

[GKCTF2020]Harley Quinn



在图片的末端发现两段字符，像是base64，但是解码出来都是乱码
在音频的最后一段听见一段电话音，题目里面的提示也说了电话音，将电话音给剪出来，用`dtmf2num`工具识别一下，得到

```
C:\Users\ieven\Desktop\CTF\misc\工具\dtmf2num>dtmf2num 1.wav

DTMF2NUM 0.1c
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- open 1.wav
  wave size      648384
  format tag     1
  channels:      2
  samples/sec:   44100
  avg/bytes/sec: 176400
  block align:   4
  bits:          16
  samples:       324192
  bias adjust:   14
  volume peaks:  -31204 31204
  normalize:     1563
  resampling to: 8000hz

- MF numbers:    44477

- DTMF numbers:  #222833344477777338866#
```

也就是

```
22283334447777338866
```

对比频谱图发现，少了一位，加上去之后就是

```
222833344477773338866
```

然后根据提示九宫格，得到

```
ctfisfun
```

根据提示`Free_File_Camouflage`，发现这是一个可以把信息写进文件的软件，下载这个软件，解密信息，得到flag.txt

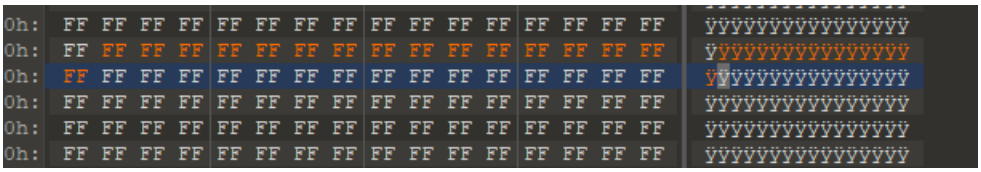
粽子的来历

一共有四个doc，每一个打开都是乱码，而且都有一句类似于这样的话

IComeFromQihooDP

敬?* € **餜?****** ***** **?**

丢进010，发现是doc文件损坏了，要把每一个`Icomefromxxxx`这一段话全部改成`ff`即可修复



发现四个文件的内容全部一样，不过行高不同，把行高大的记作1，小的记作0，按照顺序来得到这个

```
100111100010
111110010011
100100100001
111100100001
```

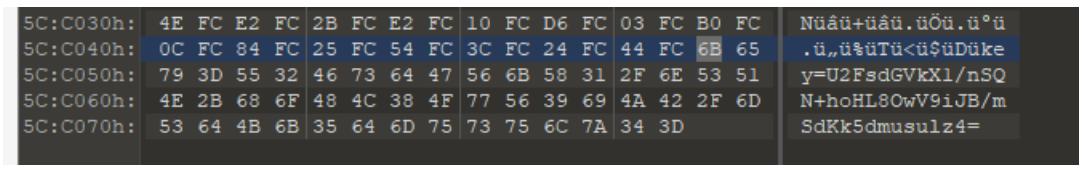
然后按照提示，对其都进行md5加密，最后发现第三个的md5为flag

[MRCTF2020]Unravel!!

图片分离出来一张图片，叫做aes.png

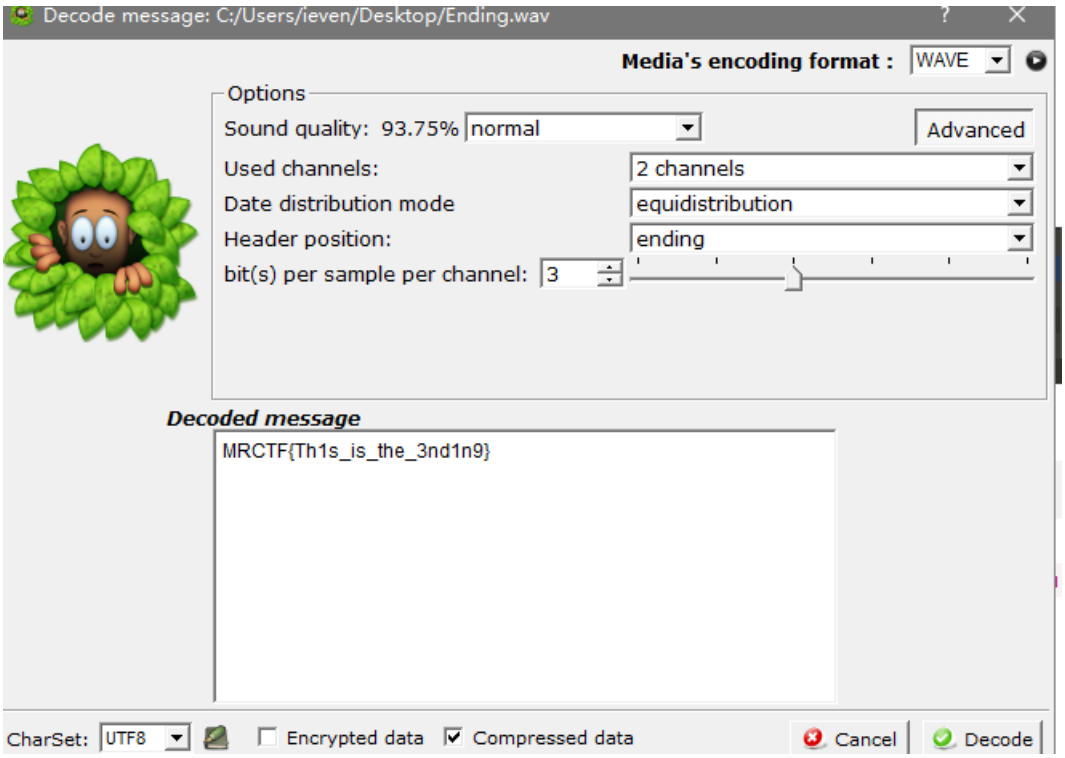
Tokyo

然后在音频的末端发现了一段key



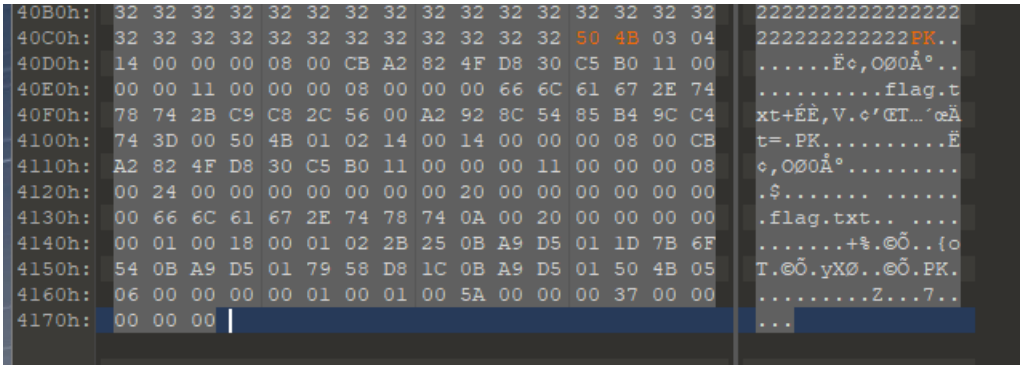
```
key=U2FsdGVkX1/nSQN+hoHL8OwV9iJB/mSdKk5dmusulz4=
```

根据图片的名称，去进行aes解密得到`CCGandGulu`，将得到的压缩包使用`slienteye`工具进行打开，解码，得到flag



[ACTF新生赛2020]明文攻击

在图片的文件末尾发现了一个文件头损坏的zip，修复之后得到flag.txt，然后进行明文攻击



然后就是明文攻击了，不过这个攻击要等很久很久

```
flag{3te9_nbb_ahh8}
```

真的很杂

分离出来一大堆图片和一个压缩包，压缩包解压后似乎是一个安卓应用

然后就是熟悉的安卓的操作了，这里记一下，因为这个总是记不太清，毕竟不是安卓逆向手:(

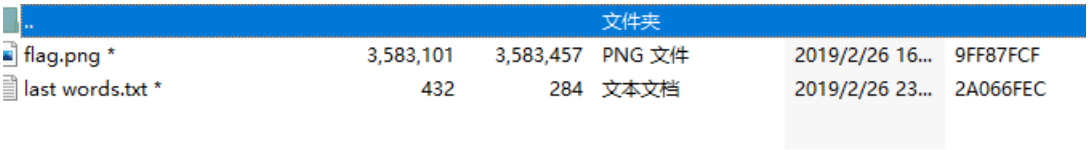
```
d2j-dex2jar.bat classes.dex
```

然后jd-gui打开即可
这里可以看得到flag是需要我们的一个爆破

最后尝试出来flag为`flag{25f991b27fcdc2f7a82a2b34386e81c4}`

[*CTF2019]otaku

一个doc和一个伪加密的压缩包，使用`ZipCenOp`工具修复，得到的加密的压缩包里面的文件内容是这样的

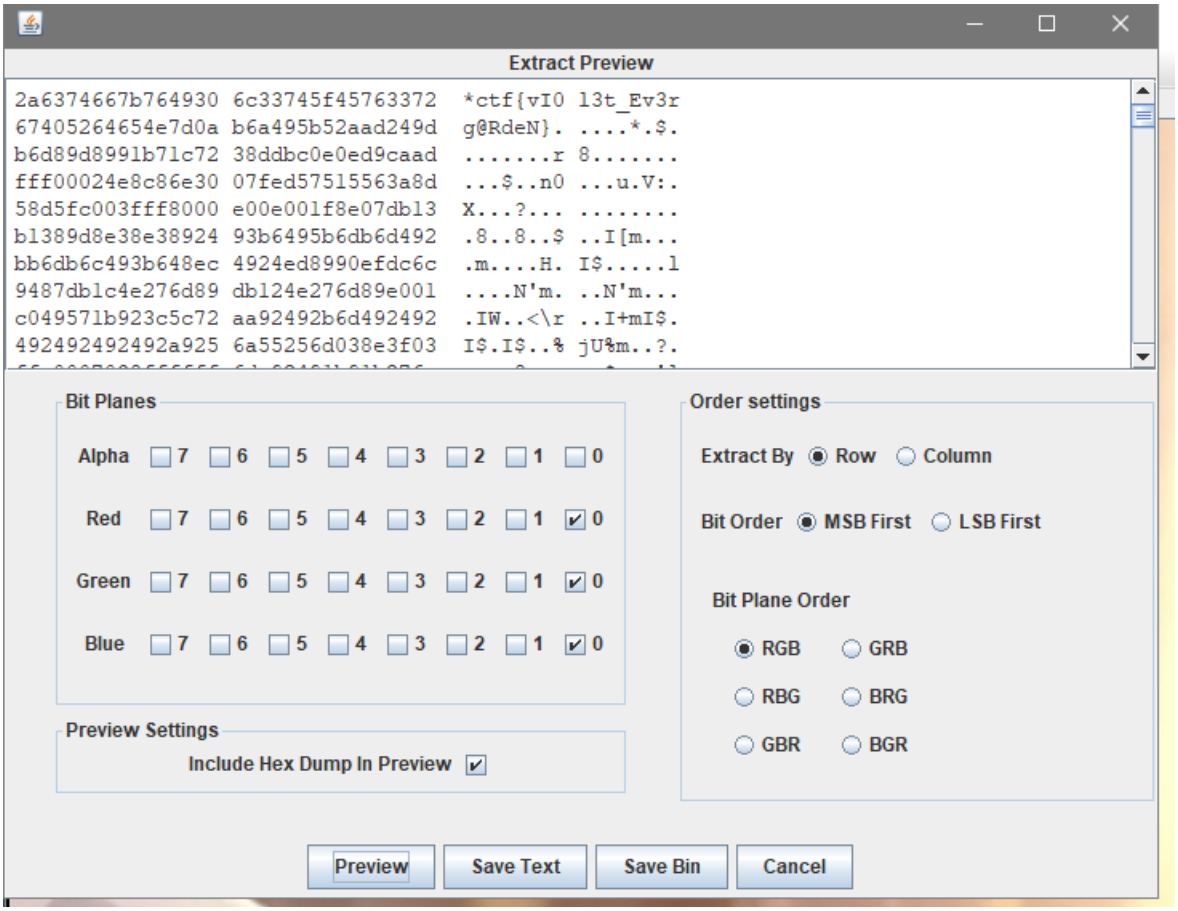


doc里面有一段隐藏文字，猜测这一段就是压缩包里面`last words.txt`的内容，不过把doc转换成txt的时候要注意编码，这题原题是有提示`GBK`的，还有注意不要把隐藏文字也给复制进去了，使用py即可对txt写入内容进行GBK编码

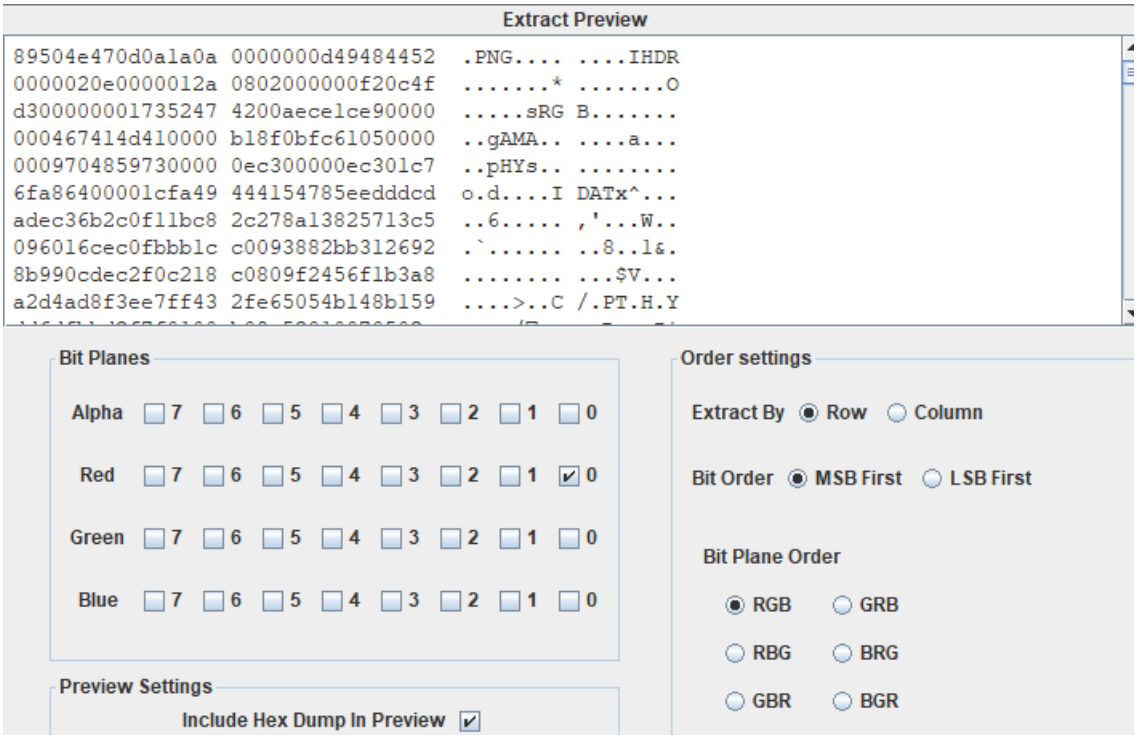
```
#encoding=GBK

f = open("last words.txt", "w")
s = "Hello everyone, I am Gilbert. Everyone thought that I was killed, but actually I survived. Now that I have
no cash with me and I’m trapped in another country. I can't contact Violet now. She must be desperate to see me
and I don't want her to cry for me. I need to pay 300 for the train, and 88 for the meal. Cash or battlenet poin
t are both accepted. I don't play the Hearthstone, and I don't even know what is Rastakhan's Rumble."
f.write(s)
f.close()
```

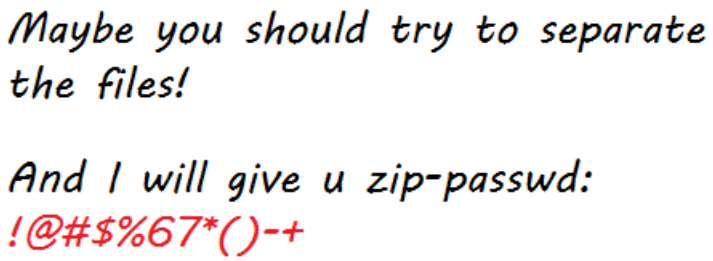
本来应该是进行明文攻击的，不过压缩的一直有问题，明文攻击这种题目真的应该少出现，压缩问题太多了，最后这个密码是`My_waifu`，LSB发现flag



[MRCTF2020]Hello_ misc



LSB发现了一点东西，保存下来，得到压缩包的密码



并且这张图片分离出来一个压缩包，解密得到一个out.txt，一大堆的数字，然后我就没思路了，看到别人是说先把每个数字转换成二进制数字，然后把前面2位取出来重组，最后转换车字符串，脚本如下

```
with open('out.txt') as a_file:
    content = [x.strip() for x in a_file.readlines()]
bins = []
for i in content:
    bins.append(bin(int(i))[2:].zfill(8)[:2])
stringBins = ''.join(bins)
num = 0
flag = ''
for i in range(int(len(stringBins)/8)):
    flag+=chr(int(stringBins[num:num+8],2))
    num+=8

print(flag)
# rar-passwd:0ac1fe6b77be5dbe
```

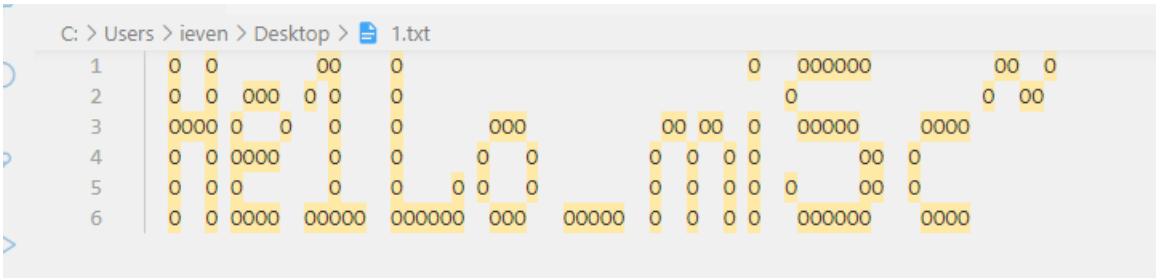
刚好得到的是rar的密码，然后解密得到一个doc，最下面有一些白色的字体

```
MTEwMTEwMTExMTExMTEwMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTA
xMTEwMDAwMDAxMTExMTExMTExMDAxMTAx
MTEwMTEwMTEwMDAxMTAxMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTE
xMTAxMTExMTExMTExMTExMTEwMTEwMDEx
MTEwMDAwMTAxMTEwMTExMDExMTEwMTExMTExMTAwMDExMTExMTExMTExMDAxMDAxM
TAxMTEwMDAwMDExMTExMDAwMDExMTExMTEx
MTEwMTEwMTAwMDAxMTExMDExMTEwMTExMTExMDExMTAxMTExMTExMTEwMTEwMTEwM
TAxMTExMTExMTAwMTEwMTExMTExMTExMTEx
MTEwMTEwMTAxMTExMTExMDExMTEwMTExMTAxMDExMTAxMTExMTExMTEwMTEwMTEwMT
AxMTAxMTExMTAwMTEwMTExMTExMTExMTEx
MTEwMTEwMTAwMDAxMTAwMDAwMTEwMDAwMDAxMTAwMDExMTAwMDAwMTEwMTEwMTEwM
TEwMTAxMTEwMDAwMDAxMTExMDAwMDExMTExMTEx
```

base64解密得到的是一大串的10，也就是

```
11011011111111001111011111111111111111111111111111011100000011111111111001101
11011011000110101111011111111111111111111111111111111011111111111111110110011
11000010111011101110111111110001111111111100100110111000001111100001111111
11011010000111101110111111011101111111111011011010111111110011011111111111
11011010111111110111101111010111011111111110110110101101111100110111111111111
11011010000110000011000000110001110000011011011010111000000111100001111111
```

简单进行一个替换，发现flag`He1Lo_mi5c~`



[BSidesSF2019]zippy

foremost分离出来一个带着密码的压缩包，里面有着flag.txt，追踪tcp流发现密码

```
nc -l -p 4445 > flag.zip
unzip -P supercomplexpassword flag.zip
Archive:  flag.zip
  inflating: flag.txt
```

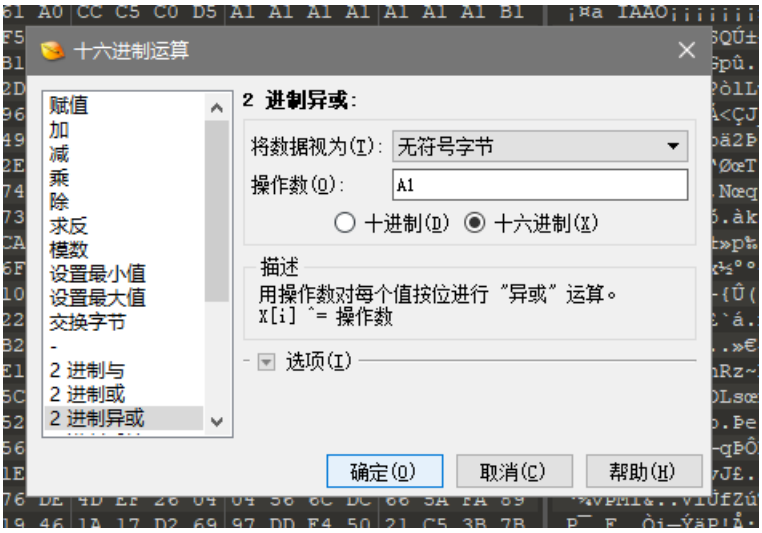
解压得到`{this_flag_is_your_flag}`

[ACTF新生赛2020]music

文件异常，并且有很多的`A1`，正常情况下m4a的文件头为

```
00 00 00 20 66 74 79 70 4D 34 41 20 00 00 00 00
```

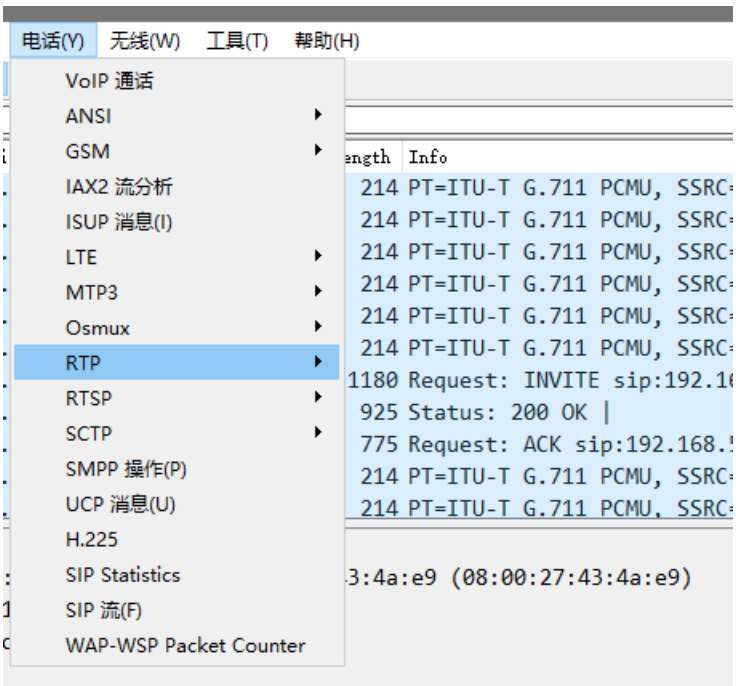
这里再次将数据异或一个A1恢复原样，然后直接听出来flag



也就是`abcdfghijk`

voip

打开流量包，发现都是RTP协议，那就听一下



然后听flag即可`flag{9001IVR}`