CTF题记——再战GK、BUU

原创

m0re 于 2020-06-25 23:24:08 发布 1292 收藏 3

分类专栏： CTF 文章标签： CTF BUUCTF

m0re

前言

没事做一些杂项和密码学的题，记下没见过的，总结思路。扩大脑洞。

本文目录

Crypto□

[GKCTF2020]汉字的秘密

这道题当时没做出来，做了一半。
下载下来的word文档，打不开，然后就010Editor看一下，发现是压缩包，改后缀解压。
出来一堆文件

当时做的时候，查到一篇博客(现在找不到了)，上面说这种题，信息一般都在document.xml中。然后就找
果然发现了信息，

```
王壮 夫工 王中 王夫 由由井 井人 夫中 夫夫 井王 土土 夫由
土夫 井中 士夫 王工 王人 土由 由口夫
```

是当铺密码，然后进行转换是

```
69 74 62 67  118  83  72  77   86  55  71
57
82  57
64  63   51  107
EJ>CvSHMV7G9R9@?3k
```

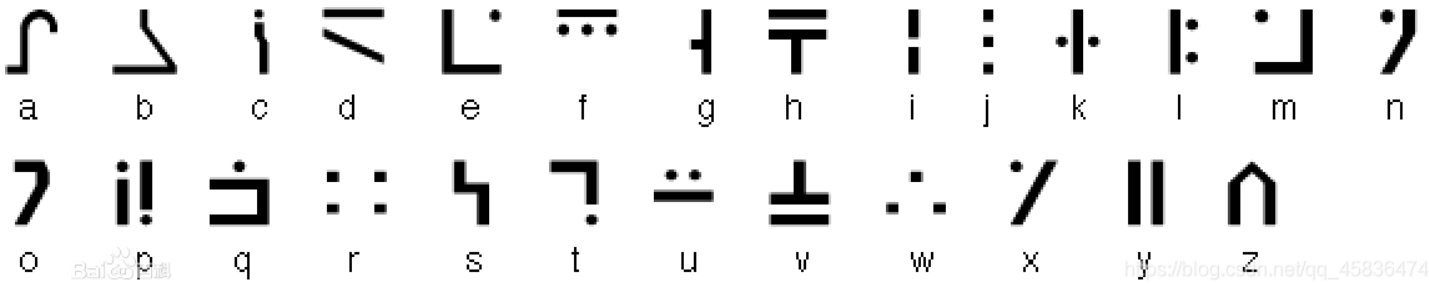
这串字符串确实不是flag，到这里我的思路就没有了，古典密码试了，看过wp后才明白是变异凯撒，之前还做过这种题，没想到害。
下面是简单脚本，

```
m0re="EJ>CvSHMV7G9R9@?3k"
flag=''

i=0
for a in miwen:
    i+=1
    flag+=chr(ord(a)+i)

print(flag)
```

跑出来flag，转换成小写提交。

[MRCTF2020]古典密码知多少

没见过的标准银河字母，其他的两种很容易看出来是猪圈密码和圣堂武士密码。然后对照百度找到的标准银河字母对照表进行解码



解出得到`FGCPFLIrtuASyoN`

ithink you can know what imean.

emmm.... maybe you can buy some fence~

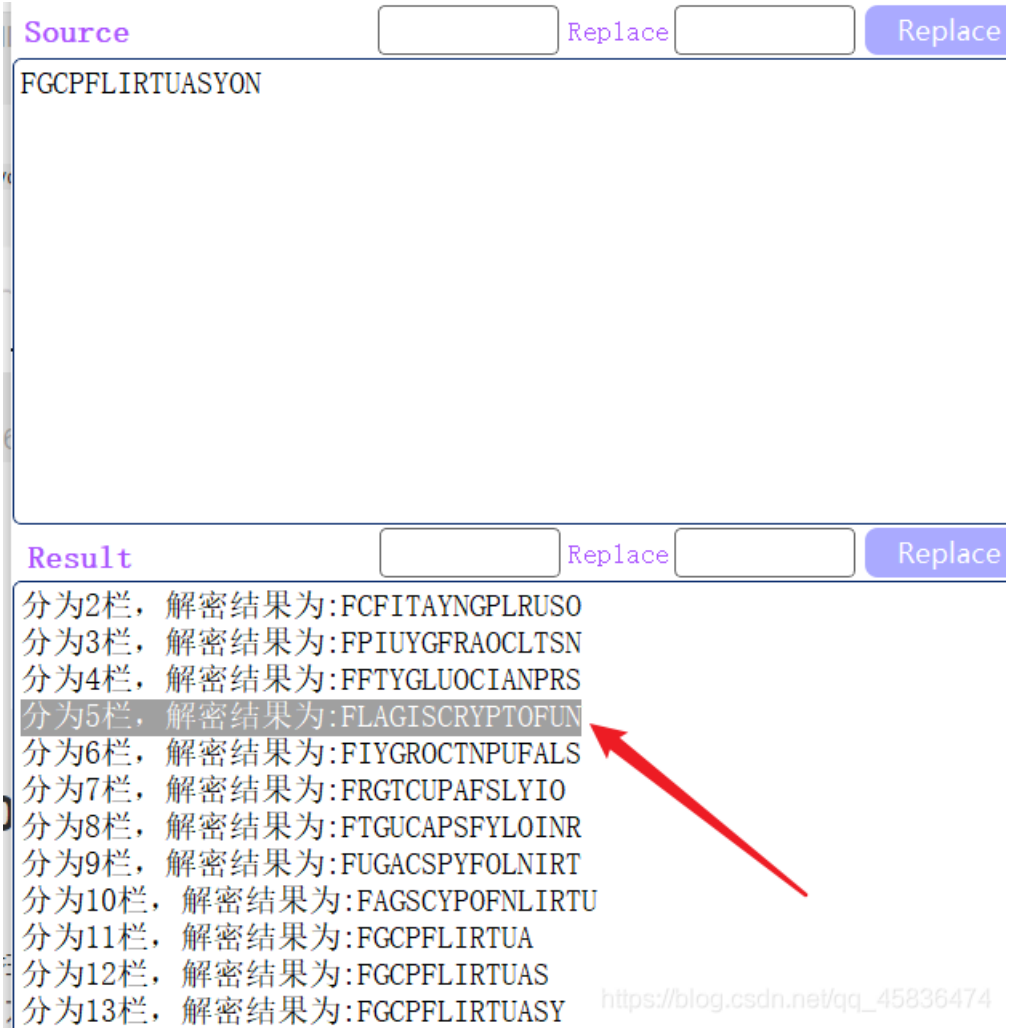
all are uppercase letters!!!

想想你知道什么意思。

嗯。。。也许你可以买一些围栏~

都是大写字母！！！

所以进行栅栏解密



得到flag

[MRCTF2020]keyboard

```
得到的flag用
MRCTF{xxxxxx}形式上叫
都为小写字母

6
666
22
444
555
33
7
44
666
66
3

```


看着键盘，也不是26键的，就是9键的，而且数字的位数不超过三。
数字是按键，个数是第几个字母。
得到flag是mobilephond
但是提交不对，改成mobilephone就对了。

[WUSTCTF2020]佛说：只能四天

题目是与佛论禅，这个新的老的都试了一遍，新约佛论禅是可以解出来的。
在线解密网站□新约佛论禅

然后是社会主义核心价值观编码
在线网站□传送门

社会主义核心价值观：富强、民主、文明、和谐；自由、平等、公正、法治；爱国、敬业、诚信、友善

RLJDQTOVPTQ606duws5CD6IB5B52CC57okCaUUC3SO4OSOWG3LynarAVGRZSJRAEYEZ_ooe_doyouknowfence

编 码　　解 码

平等文明自由友善公正自由诚信富强自由自由平等民主平等自由自由友善敬业平等公正平等富强平等自由平等民主和谐公正自由诚信平等和谐公正公正自由法治平等法治和谐和谐平等自由和谐自由自由和谐公正自由敬业自由文明和谐平等自由文明和谐平等和谐文明自由和谐自由和谐和谐平等和谐法治公正诚信平等公正诚信民主自由和民主平等平等平等平等自由和谐和谐和谐平等和谐自由诚信平等和谐自由自由友善敬业平等和谐自由友善敬业平等法治自由法治和谐和谐自由友善公正法治敬业公正友善正民主法治文明自由民主平等公正自由法治平等文明平等友善自由平等和谐自由友善自由平等文明自由民主自由平等平等敬业自由平等平等诚信富强平等友善敬业公正公正友善敬业公正平等平等诚信平等公正自由公正诚信平等法治敬业公正诚信平等法治平等公正友善平等公正诚信自由公正友善敬业法治法治公正公正公正平等公正诚信正和谐公正平等

最后doyouknowfence提示栅栏密码

Source　　Replace　　Replace　Clear　Copy　Pa

RLJDQTOVPTQ606duws5CD6IB5B52CC57okCaUUC3SO4OSOWG3LynarAVGRZSJRAEYEZ_ooe_

Result　　Replace　　Replace　Clear　Copy　Pa

分为15栏，解密结果
为:Ru5OJLw7WRJsoGAD5k3EQCCLYTDayEO6UnZVIUa_PBCroT53AoQBSVe65OG_O24R6COZdCSS
分为16栏，解密结果
为:Rwo3YLskLEJ5CyZDCan_QDUaoT6UroOICAeVB3V_P5SGTBORQ54Z62OSOCSJ6CORd5WAu7GE
分为17栏，解密结果
为:RsCnL5aaJCUrDDUAQ6CVTI3GOBSRV5OZPB4ST5OJQ2SR6COAOCWE65GYd73EuoLZwky_
分为18栏，解密结果
为:R5UALCUVJDCGD63RQISZTBOSO54JVBORP5SAT2OEQCWY6CGEO53Z67L_doyouknowCaesar_
分为19栏，解密结果
为:RCCRLD3ZJ6SSDIOJQB4RT5OAOBSEV5OYP2WETCGZQC3 65Lo07yo6onedka uCrwaAsUV5UG

最后凯撒密码，然后hint中是有提示的。

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

1. 虽然有点不环保，但hint好像是一次性的，得到后就没有利用价值了。
2. 凯撒不是最后一步，by the way，凯撒为什么叫做凯撒?

凯撒最初是移三位的。所以直接偏移3位即可。
得到后查看符合base32编码，进行base32解密

Misc

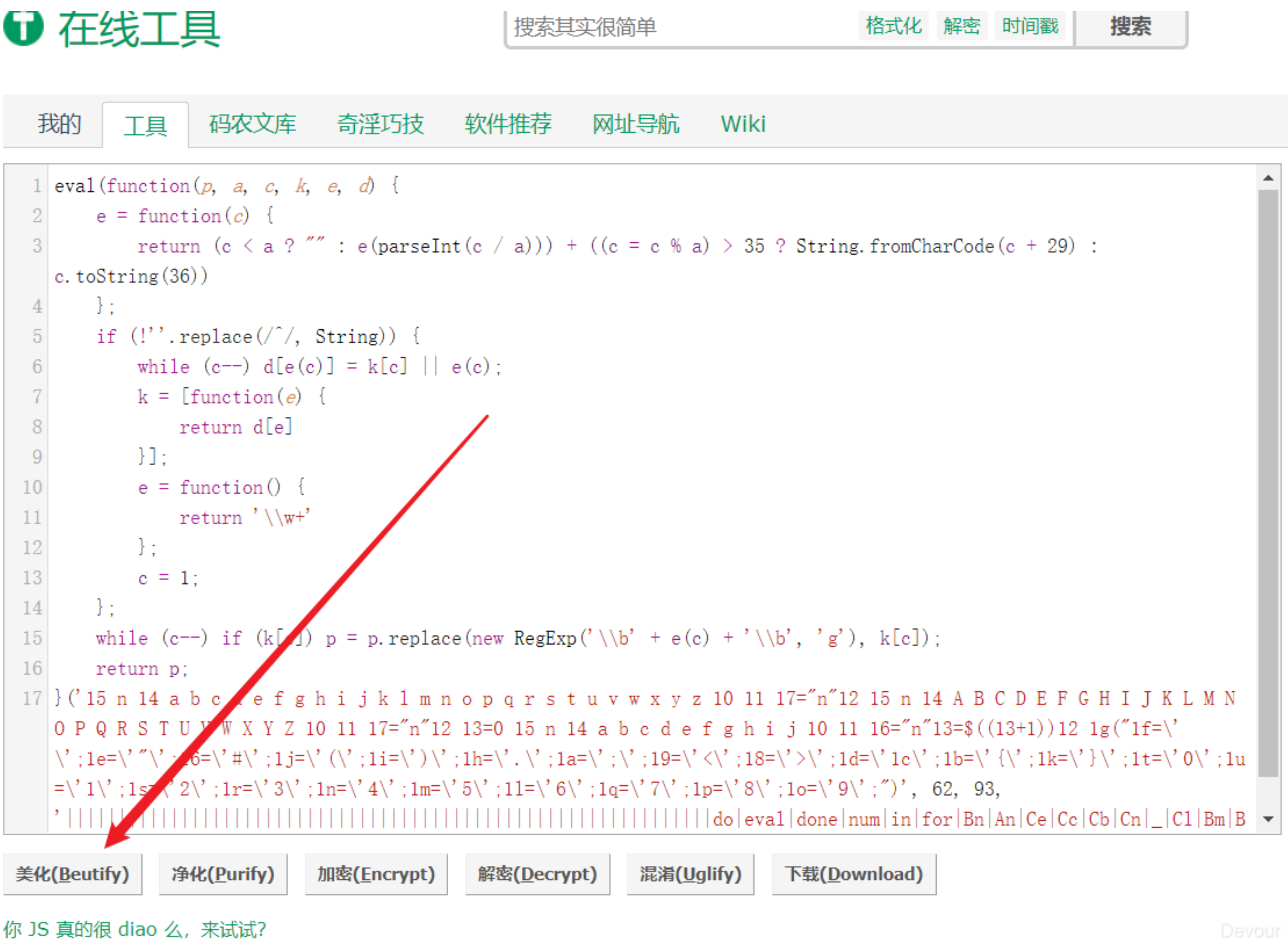
[GKCTF2020]code obfuscation

这个二维码是扭曲的，扫描是扫不出来的，看别人的wp，都是用ps了，各种方法都有，不过，QR research可以扫描，但是直接扫描也是扫描不出来的，下面一个比较有意思的方法，就是打开这个图片，截图粘贴到一块大的白屏上，然后尽可能让图片看起来小，再用工具扫描，就可以扫出来了。

然后进行文件分离，在图片中分离出来一个压缩包，有密码的，然后gkctf应该是解压密码，不过要进行base编码，只能挨个尝试，最后base58加密出来是对的。解压结果，一张图片和一个文件

```
$Bn$Ai$An$Ac$Al$Au$Ad$Ae$Bk$Cc$As$At$Ad$Ai$Ao$By$Ah$Ce
$Ai$An$At$Bk$Am$Aa$Ai$An$Bs$Bt$Cn
$Ap$Ar$Ai$An$At$Bs$Bm$Aw$Dd$Al$Ac$Da$Am$Ae$Cl$De$Ao$Cl$Dj$Ak$Ac$At$Df$Bm$Bt$Cb
$Ar$Ae$At$Au$Ar$An$Bk$Da$Cb
$Cp
```

在线工具js美化——传送门，直接将1文件拖进去，点击美化。

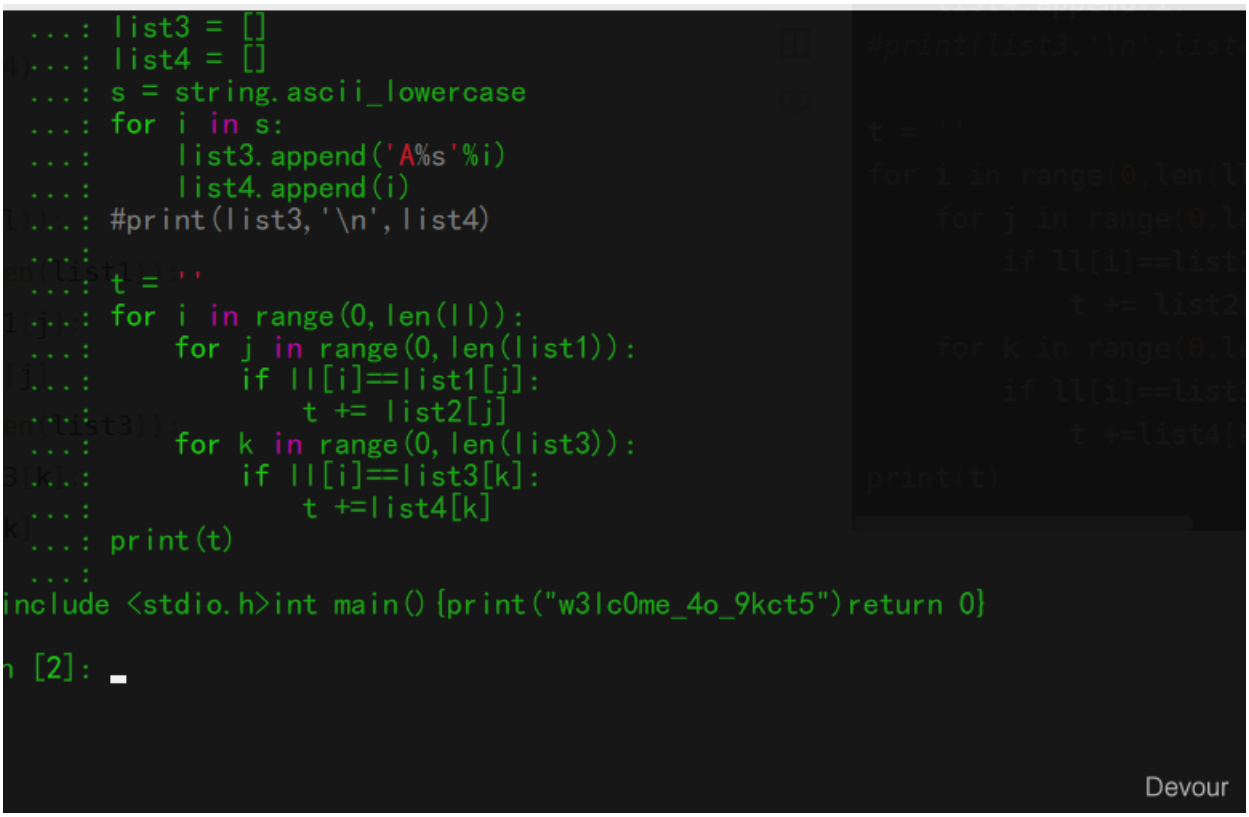


看了大佬的博客，emmm，多少还是有点不理解的地方。
整理得到

```
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';")
```

再用下大师傅的脚本跑一下。

```
import string
s = "$Bn$Ai$An$Ac$Al$Au$Ad$Ae$Bk$Cc$As$At$Ad$Ai$Ao$By$Ah$Ce$Ai$An$At$Bk$Am$Aa$Ai$An$Bs$Bt$Cn$Ap$Ar$Ai$An$At$Bs$B
m$Aw$Dd$Al$Ac$Da$Am$Ae$Cl$De$Ao$Cl$Dj$Ak$Ac$At$Df$Bm$Bt$Cb$Ar$Ae$At$Au$Ar$An$Bk$Da$Cb$Cp"
ll = s.split('$')
list1 = ['Bk','Bm','Bn','Bs','Bt','By','Cb','Cc','Ce','Cl','Cn','Cp',
'Da','Db','Dc','Dd','De','Df','Dg','Dh','Di','Dj']
list2 = [' ','"','#','(',')','.','','<','>','_','{','}','0','1','2','3','4','5','6','7','8','9']
list3 = []
list4 = []
s = string.ascii_lowercase
for i in s:
 list3.append('A%s'%i)
 list4.append(i)
#print(list3,'\n',list4)

t = ''
for i in range(0,len(ll)):
 for j in range(0,len(list1)):
  if ll[i]==list1[j]:
   t += list2[j]
 for k in range(0,len(list3)):
  if ll[i]==list3[k]:
   t +=list4[k]
print(t)
```



[GKCTF2020]Harley Quinn

下载得到音频文件和一张图片，听音频，听到最后面发现异常，也不知道是什么，也不是摩斯密码什么的，后来看hint是电话音，

Hint

HQ

hint:电话音&九宫格

Got it!

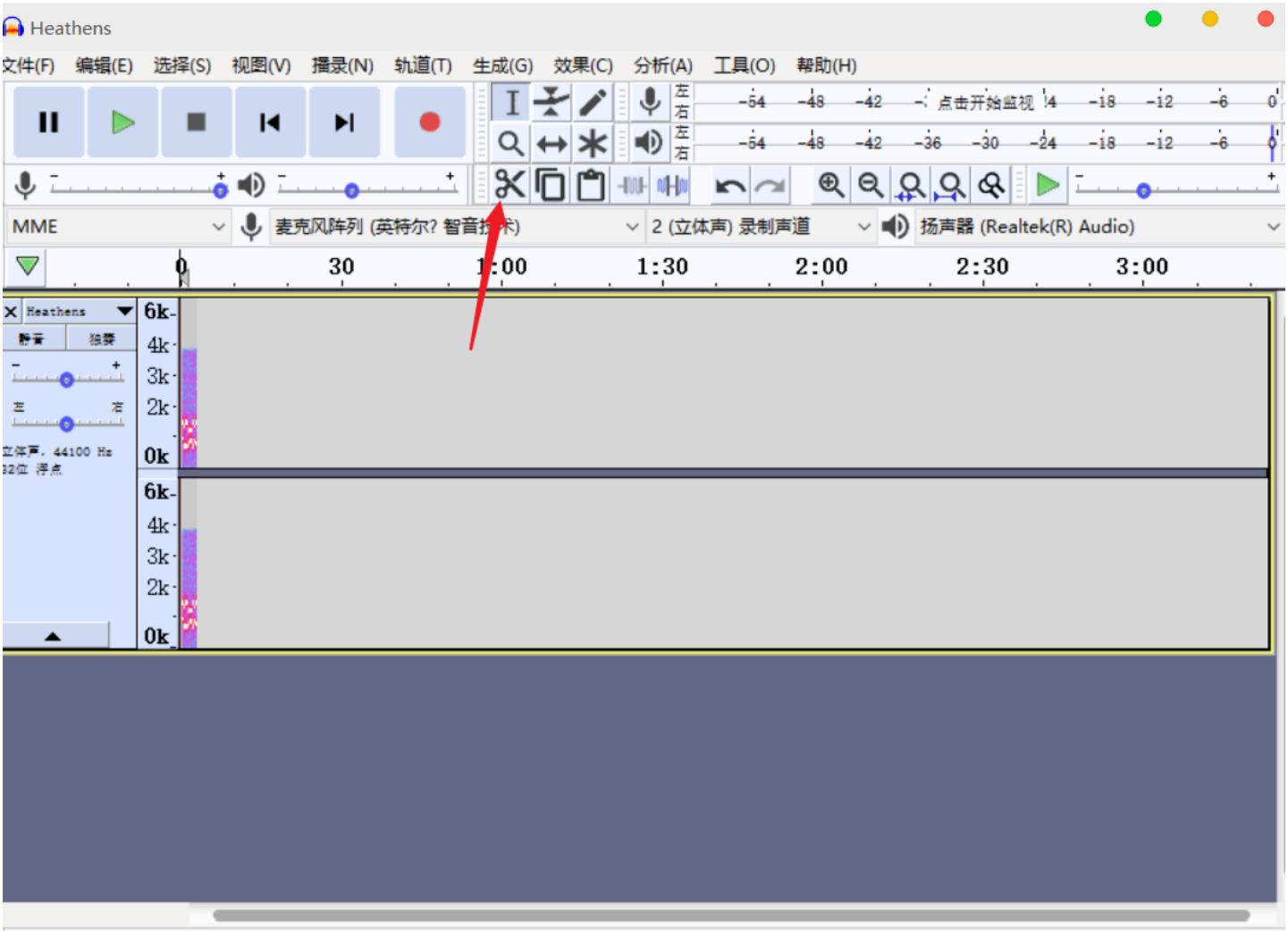
看了大佬的wp(这个比赛的时候我是没有做出来的，没有思路)

需要用到一个工具，`dtmf2num.exe`

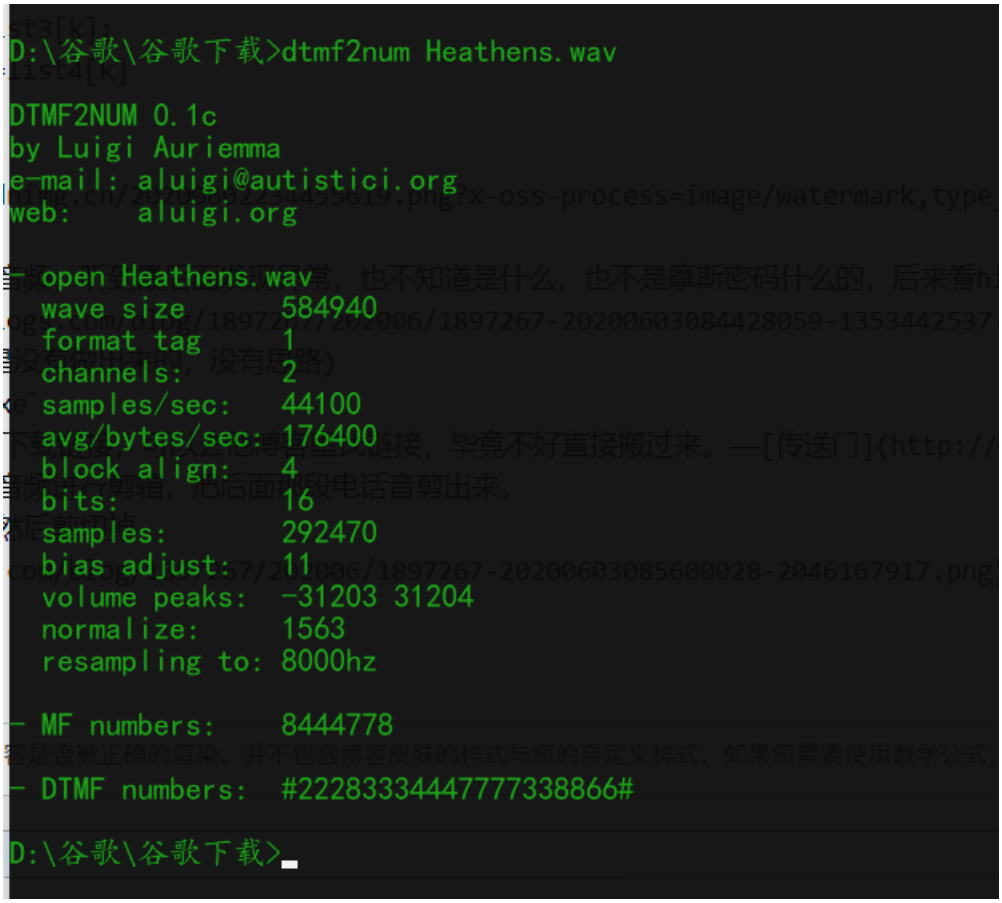
下载地址呢，emmm这个大佬他给了下载链接，可以去他博客里找链接，毕竟不好直接搬过来。——传送门

然后下载好啦之后，需要先将那个音频进行剪辑，把后面那段电话音剪出来，

可以选中电话音前面的所有部分，然后剪切掉



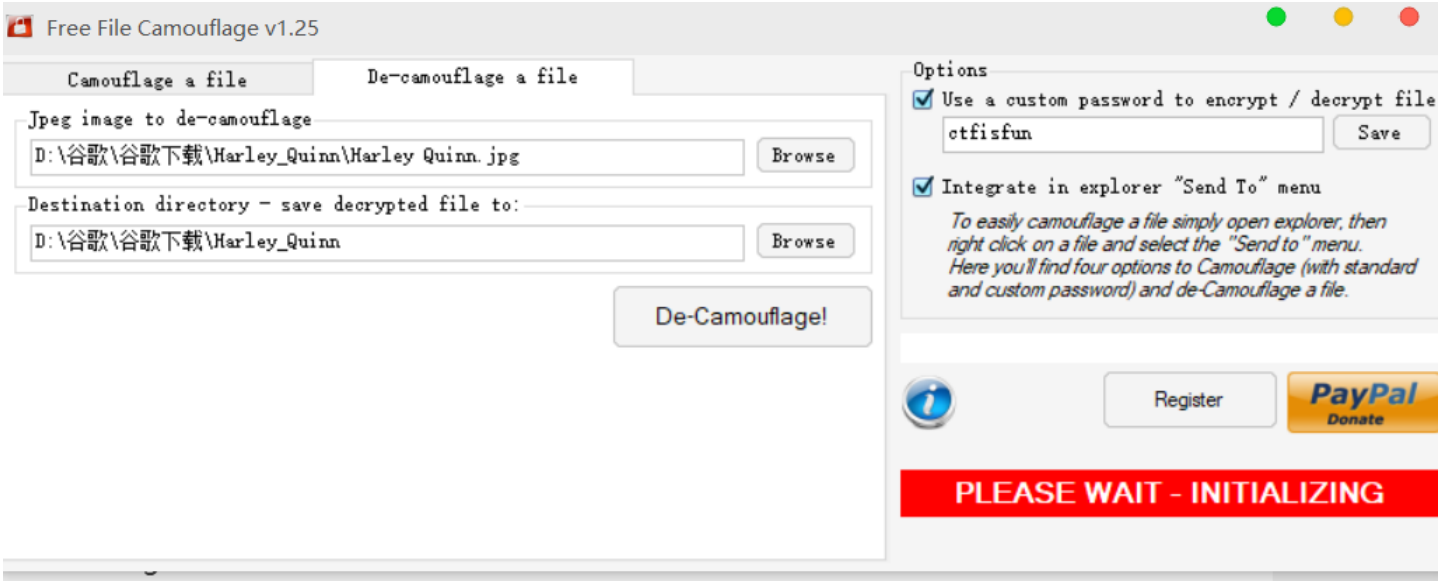
再导出文件就行了。
然后使用dtmf解题



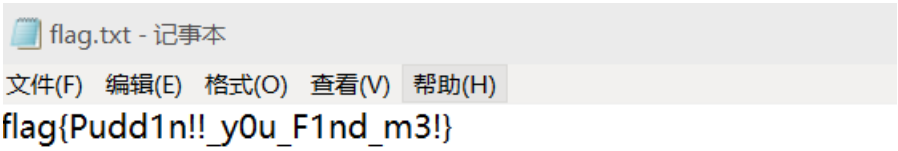
`#22283334447777338866#`
九键

是`ctfisfun`
然后第二个hint是

工具吧，百度搜索就行。
然后打开使用，可能需要将原来的JPEG为后缀的图片改成jpg格式，



输入密码，`ctfisfun`
得到一个flag.txt



flag{Pudd1n!!_y0u_F1nd_m3!}

[GXYCTF2019]gakki

foremost分离图片得到压缩包，然后是弱口令，8864（都是傻瓜式操作就不截图了）

解压出来flag.txt是

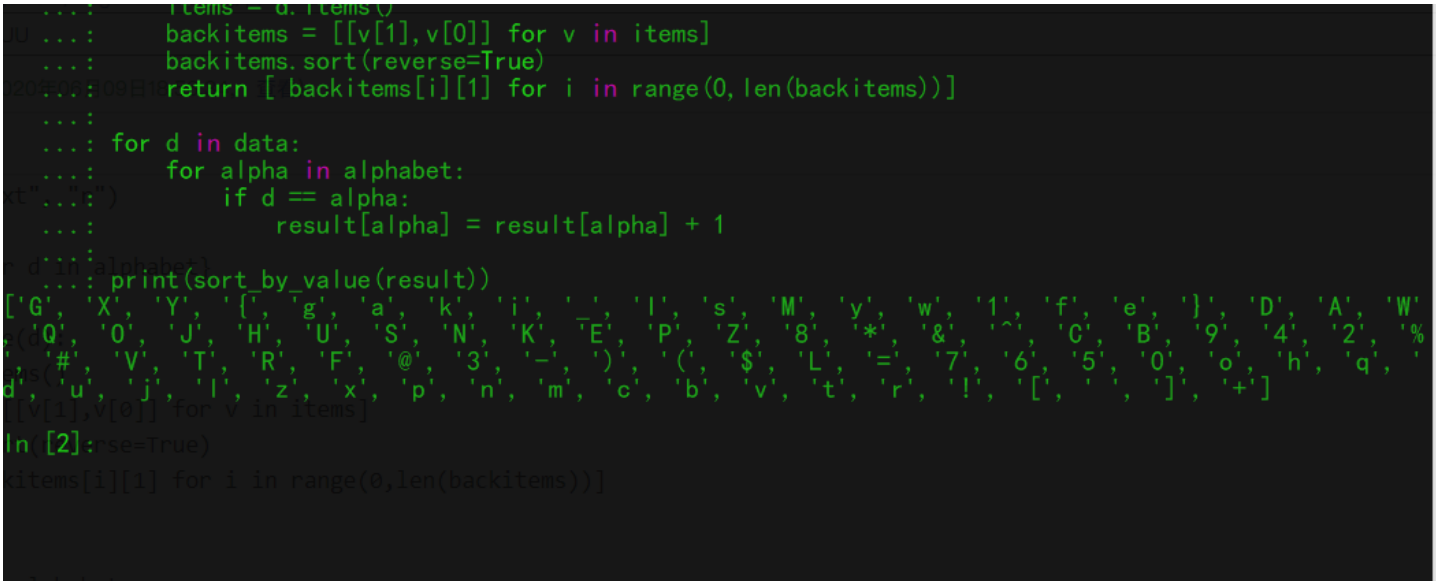
```
I&&GgJld(uPVDrp!Xkc$xE_dgFP#%0hCE8O&$=nbv@#!!Smxd3CpJt9Kw55o%6Msd3&uphGz#5%pxa0QUPk3=Qkh36)u3ZKAsXiZBj4%=nfk
VJ_(qV0-akZEcTGnvCSI=agQ_p^-1=PDmTcNPT08R&mY(LqO{0gW*xE25IBIg_XTezJogPERRM79YwM3K84Q9O}xX1wD7JwDGgVjea0JS9pV
NSw=_C3h407fxMv-4#{0ZMj*gRUxcL7T(RRKi-v9@HB^-DBHkRlvyiH8wJbFqgGiD%NQZJ{{j!nWuEs}DFYk7KiiFE%J112JNPCnXklc-h-1}!vuty}y
/l!J&z5qYdb(-nzJFIrbnBnl(6W6j60pZs8Om&=uoaUjqj(qgP0k2^OUONaggfb-sC4Cuas!Smij7H3ZU$R&99YiV3qm2#1TDQBCKiOLT)sey{()6Lx
ZULj#NK$Y=p1#4#irNjDu(g0MqB-H-}fqu*cA{*gg7q)wtBEzc0olkq7t2B3%@HFS7MqgV{UYr4F)GCNcBx)Mc-#BiR})vvEq}g5HH&l#t#3i2DGC
)G@pDTo#hbCYN0UJ&g)LPgN5g_pyMoO&T#g)SHvWltDQD4%nfJN2{*aY5-ZZ)$-Y0coF@f{NZ2zSsryV&n}B%{$*3e#xG3Jx*r$4YQZYtLjTdzll
2d!2g{m}t0DU%w!Q9JV$xpW}^^viRSrLA#KQI0AXU)EcmXl!xykUFq=dirrf4Z=mM%wi{PdPuaBJ0^JID&2bDk2ytWv5pb;6N_$9(xhpJulL=-bDI
HPgOnu9!gsU=DqQgER-=0!6Z7G^XNeJ2cr-or{z9X-F^Br4I=5(eXIYA33hkeh8FK3j$AF%=5Yuhy&S!TaaCqmL&pgSFvR%Od(GO@{N-Mfs&!p
14qjF8RaLeF{d1s*CO)Xvf#UV6I!3AIu9zL%W0@{u$llqH!UOZ8iZ9rXoE$ibe81otYb7v%g8BeQj-@&SvhgKAqZ1}S4*UuOG1nE)Mxp7GdeXti_fn
UF7AcYEoBeMPWllm4Cq!X%V{WixcJlegzNEMer8wln6*Ya01y5Cg=JZd9ZCeX7ULx#%%acpy_2-^W$(!HWO82wO5NsjeYchQUINmXpMJ@%
SIkjh!zN9G)q7-pg-$$Ke0g(V1iEE$trp-6HhP=aTsvOuyDR!L{(M5=n$clJ&XR4nRN0#g6$%rMq15Xd}O%#6FioRkQ4rlsBPkBV5g!JIf7D*2VF8E
8L2}#pM1-Ehc%)$WgFugQgtzkH^I7SQmQYyB2aZ4W&t0EwLO}GK79FuS&&MYrE-qS&YxeSzzOvKoL5uBm=euy-z1N#dK_@k-=v#MtbfVg
-XwNkU@&1X$kvv-f@S)8z{k))vL$Y1$Co$bR_5nfTu8^@wZ{MYZDtE8B2qwU%CK51z*eG3DEB#YY-u*E=2PFnXwk)YucL*%-2qa(NCOxJbB}rJ
W1oHpXvLE$h@66M$8H491W#{i3gNA0fh*Nl6=hVsfh4YM*U0ViNkI*nTXlL5GfuT5KrKUIKW$w@P@!AYx7A6lkbot&FL1WLSzmOFQi}v5nB2
11AE%o{zX)PMz5^IjEQTEogNmf6j3UBU*VN380FtZ=NO!H$WPAyp{xZ348#uzGhoX@mnI_bFny$Jn$UzoB2y=yN=pcW1feBPhULGYZ@op8!)
PN7)a(*B3xi5_EfL8BzGAM(l_UkpCASoU()xea_^B0}vKZWzt7)NXALB#0u)y94crVcQkHiDB4Mz$VP6x(O*_jJLS$7KfVf%}_#oA1LfR(l!k{#l4TwZ3%
k_d2bMy%Hj^pt8!OrMt$VM*h0@D#8MCAo-{20Ve6NnfCtjXj3ea37dpjWeG3bo(E-9Ks2P5O*2jp4=l(9wnHV$dvOce5{UQD{#X-GNC{Cvl2Ku
70v9HaGKb7cv1!5{s%768#WxP4OaKYMam0go1^#N54*V9nX&t)N=rMXchp5O)pk89Ux2t5jV%!!a{52VOuFY)QP!UY6py@G)KndWWiN*HB&
=0GEdwJTcxYyp4iq#y=Ggd&-H2ANp^DhUA*YG@YBdRm(P9OM4JDrwKTX#_*L9JTb2YG3jX32MCXuk4}ZOWcPwDYnV-88SCnOCrKKF5Ylmk
Z5vjqsi9!Aa2EwoT2kWc@AbtYwZqi-LA%pLSDlrT#}olJ#WJ&-BiRJHV5x6}xdh%7&O}Vxn8hWUmr1SWHeCUKu6E8mqEtwkFhmH$kS!KLo=6b
)=WuRG6K1B0#=B_iT5KYUti@)8C*FN({q$JnjgPKTL&j=tEi#aW%OJaE!Sunb_v0uotlg%eq)Z99DPa$BgbziXR@VT2WSF1EXx5(Lp!={-hQ4jFC38
Tk7!W8hpv*$T(4h=QocmhmJG#TTtB$WxKdCt!vGKU=_%j29WMYDUeH3)LAIrgusP^GDv5j#Q*-dAgtEl!}vYRi^wG7)Tv&31bj2LIclkfz2Egxg-$)
0N{XNXp}nDvjmTTENFaVGmSYGEAVAQ0)yICCL=9rK$a_lYbSR{ZdKf(3xs$XiTJPbjw@tNu8=X4yGyjLcQ&@8!O*WCxOqkykUx%sW0hG5c1fDu
```

进行词频分析（这个应该就是考点）

官方给的脚本，这个在线网址有点力不从心。

```
# 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))
```

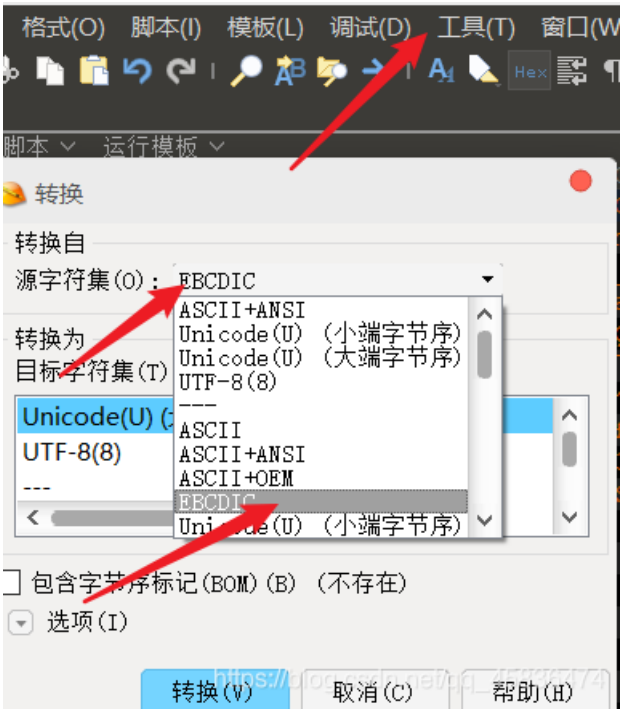
跑一遍得结果



flag{gaki_lsMyw1fe}

[SWPU2019]伟大的侦探

解压得到密码文件，misc文件夹是空的，编码没见过，所以就百度了一下，然后发现这种编码可以使用010editor转换



转换就得到密码，再次解压得到图片

是跳舞的小人，百度寻找对照表
得到flag{iloveholmesandwllm}

john-in-the-middle

这个流量分析，追踪流没得到有用的信息，尝试导出http，然后看到了六张png图片。
使用stegsolve查看，在logo.png 中得到flag

flag{J0hn_th3_Sn1ff3r}
也有直接进行foremost分离得到图片的，两种方法均可。

[GXYCTF2019]SXMgdGhpcyBiYXNlPw==

先解密这个题目，是base64，得到`Is this base?`
然后打开压缩包后得到的flag.txt看到

虽然很多，但是还是进行了解码查看了一下，但是没找到有用的信息

```
Cette nuit,
Intenable insomnie,
La folie me guette,
Je suis ce que je fuis
Je subis,
Cette cacophonie,
Qui me scie la t锚te,
Assommante harmonie,
Elle me dit,
Tu paieras tes delits,
Quoi qu'il advienne,
On tra卯ne ses cha卯nes,
Ses peines,
Je voue mes nuits,
A l'assasymphonie,
Aux requiems,
Tuant par depit,
Ce que je seme,
Je voue mes nuits,
A l'assasymphonie,
Et aux blasphemes,
J'avoue je maudis,
Tous ceux qui s'aiment,
L'ennemi,
```

```
Tapi dans mon esprit,
F锚te mes defaites,
Sans repit me defie,
Je renie,
La fatale heresie,
Qui ronge mon 锚tre,
Je veux rena卯tre,
Rena卯tre,
Je voue mes nuits,
A l'assasymphonie,
Aux requiems,
Tuant par depit,
Ce que je seme,
Je voue mes nuits,
A l'assasymphonie,
Et aux blasphemes,
J'avoue je maudis,
Tous ceux qui s'aiment,
Pleurent les violons de ma vie,
La violence de mes envies,
Siphonnee symphonie,
Deconcertant concerto,
Je joue sans toucher le Do,
Mon talent sonne faux,
Je noie mon ennui,
Dans la melomanie,
Je tue mes phobies,
Dans la desharmonie,
Je voue mes nuits,
A l'assasymphonie,
Aux requiems,
Tuant par depit,
Ce que je seme,
Je voue mes nuits,
A l'assasymphonie,
Et aux blasphemes,
J'avoue je maudis,
Tous ceux qui s'aiment,
Je voue mes nuits,
A l'assasymphonie (l'assasymphonie),
J'avoue je maudis,
Tous ceux qui s'aiment
```

还有乱码，又想到这个题是杂项里面的，应该不是只让解密的吧，反正还是没有其他的思路。

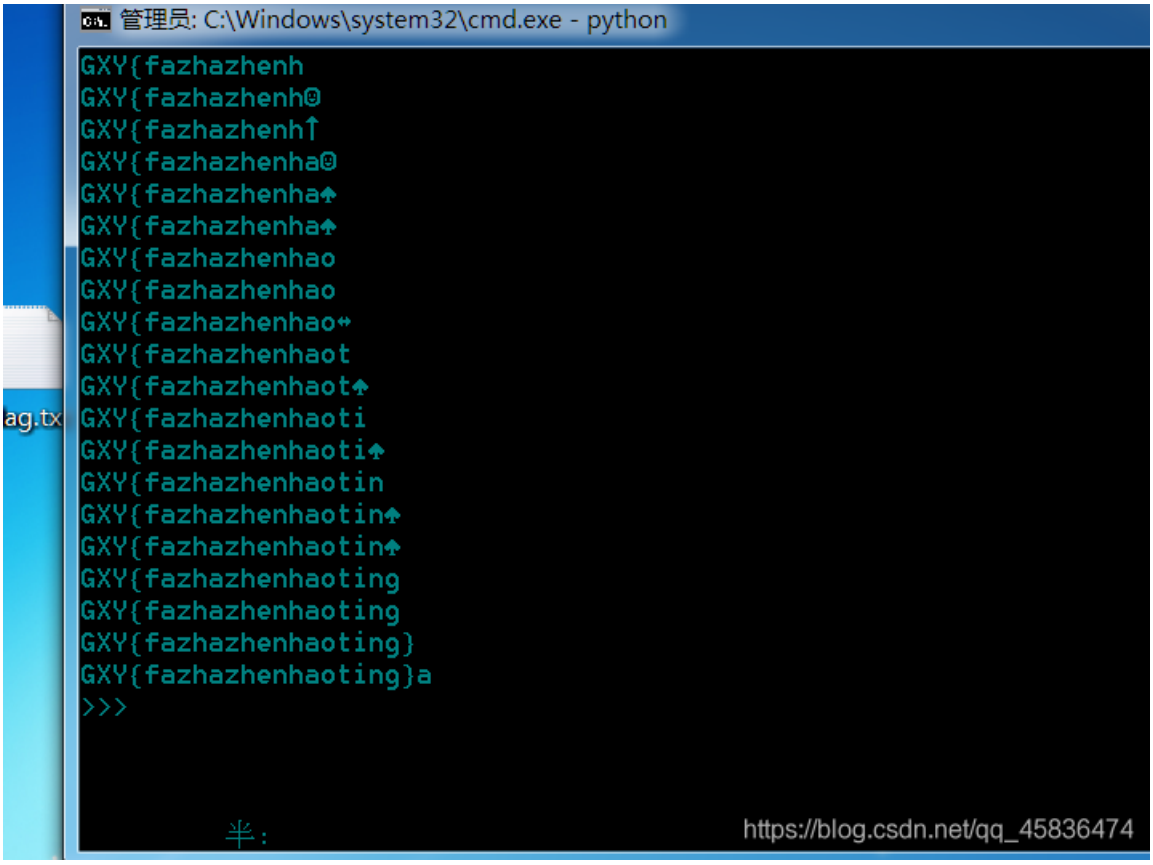
这个emmm没有什么思路了，就找wp学习学习

发现是base64隐写

学习看这里□神奇的base64

然后跑下脚本就出来了吧。

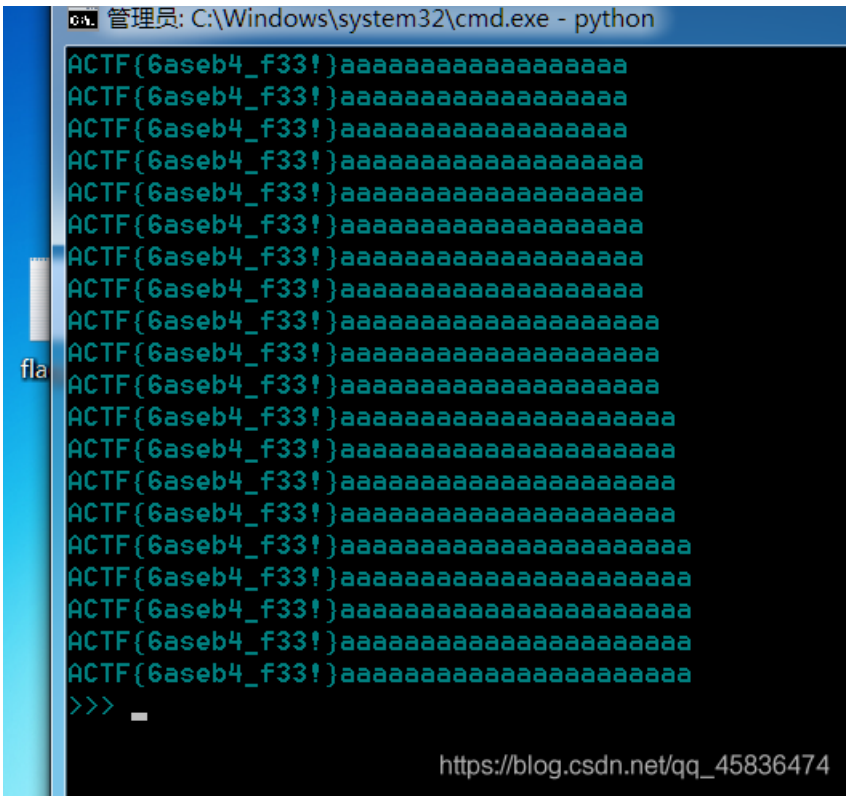
```python
# -*- coding: cp936 -*-
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('flag.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = ''.join(line.split())
        rowb64 =  ''.join(stegb64.decode('base64').encode('base64').split())
        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
```



注意是python2写的脚本，需要使用2.7的版本去运行。

flag{fazhazhenhaoting}

这道题与 （[ACTF新生赛2020]base64隐写）相似，可以一块了解。

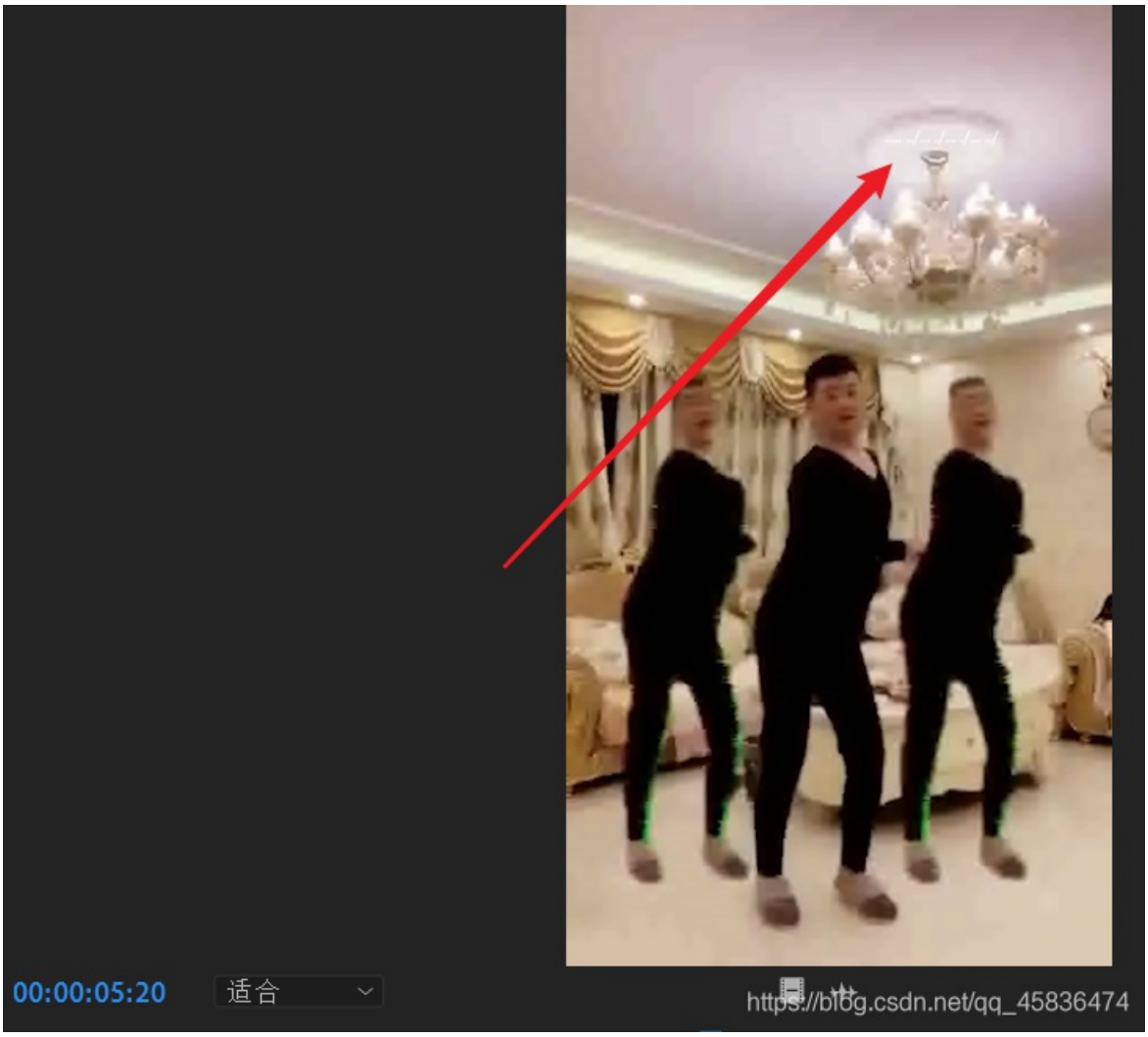


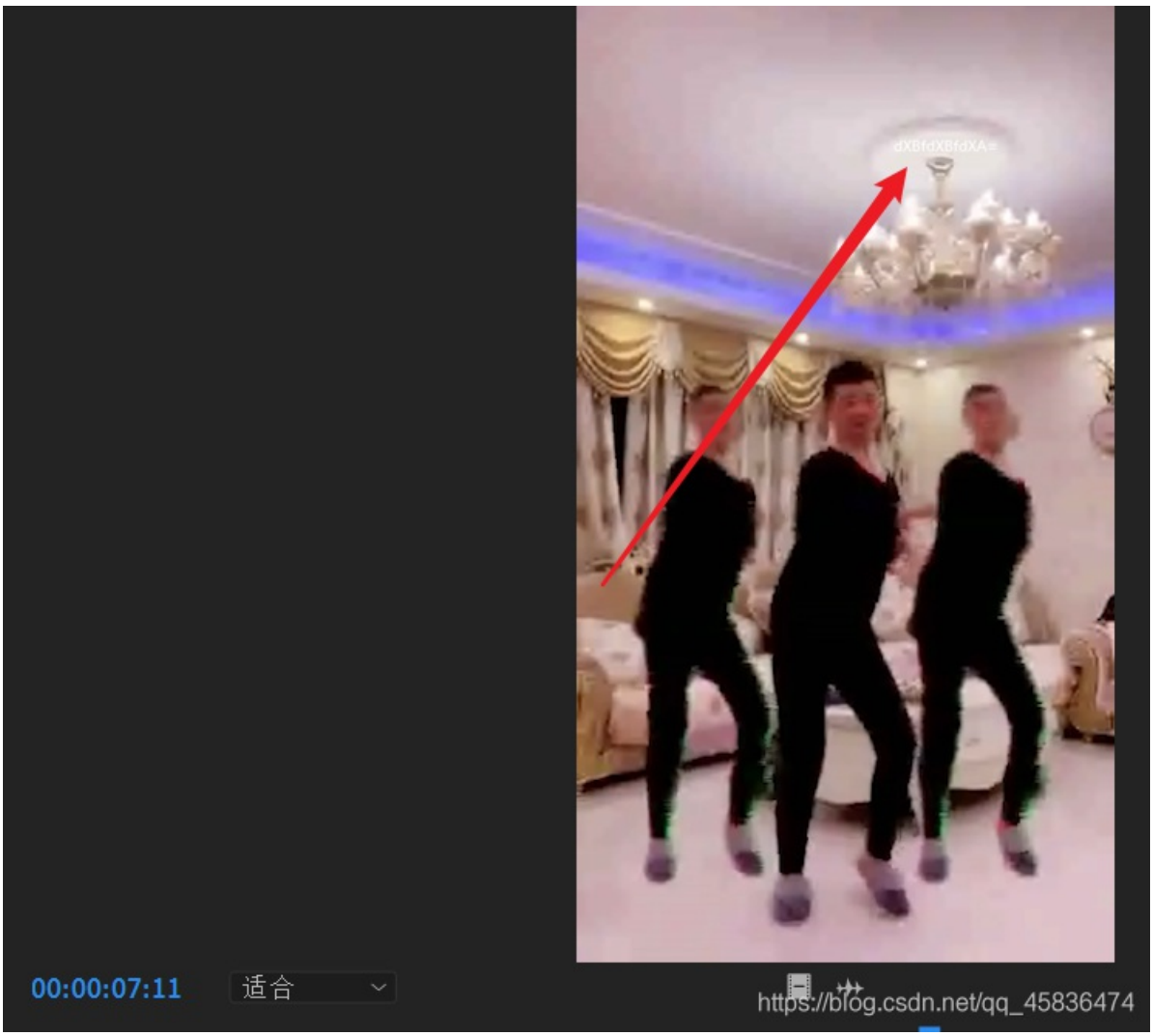
[SWPU2019]你有没有好好看网课？

两个压缩包都有密码，每个查过一遍，看到flag3.zip上有备注，是一个六位数字的密码。暴力破解就行。

然后解码得到一个word文档和影流之主的mp4文件

然后两个不寻常的数字，分别查看视频中相应的帧数所在的画面





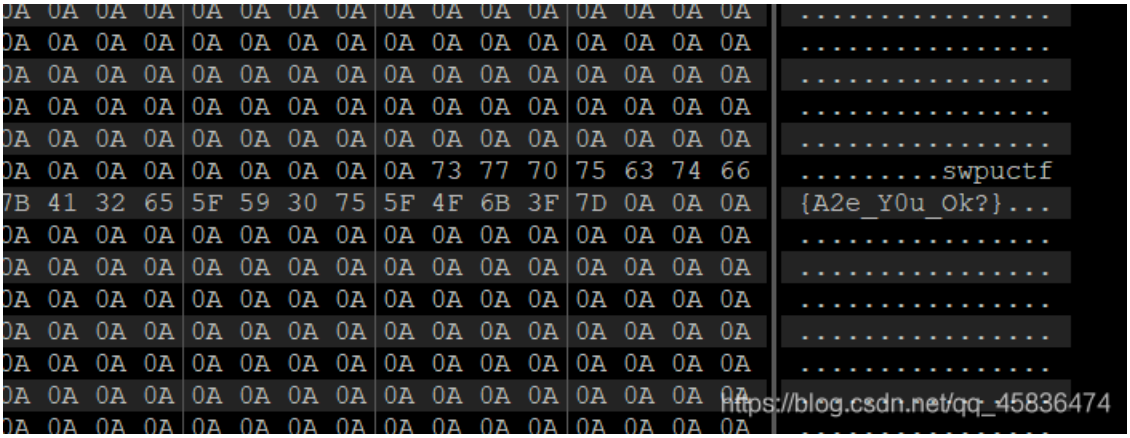
在灯上，两条信息得到

```
..... ../... ./... ./... ../
dXBfdXBfdXA=
```

第一个是敲击码

```
  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
```


解码得到WLLM，与base64解出的拼接到一起是wllmup_up_up，也就是flag2.zip的密码
得到图片用010editor打开



[BJDCTF 2nd]TARGZ-y1ng

不用爆破，tar zxvf不管用，那么密码就可能没有或者伪加密，或者在备注当中再有就是文件名就是密码。的确是文件名，但是解压好多次都没有得到结果。
看了wp，发现要解压300次，应该是不行的。
还有就是脚本，这里直接使用脚本可以。

```python
#来源官方wp#
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()
```

注意，运行自行建立一个新文件夹，然后就是傻瓜式操作。
找到flag文件用记事本打开就可以了。

黑客帝国

打开后是一个文本文件，emmm脑洞太小，想不到。看wp学习
emmm□是十六进制，用HxD编辑保存一下

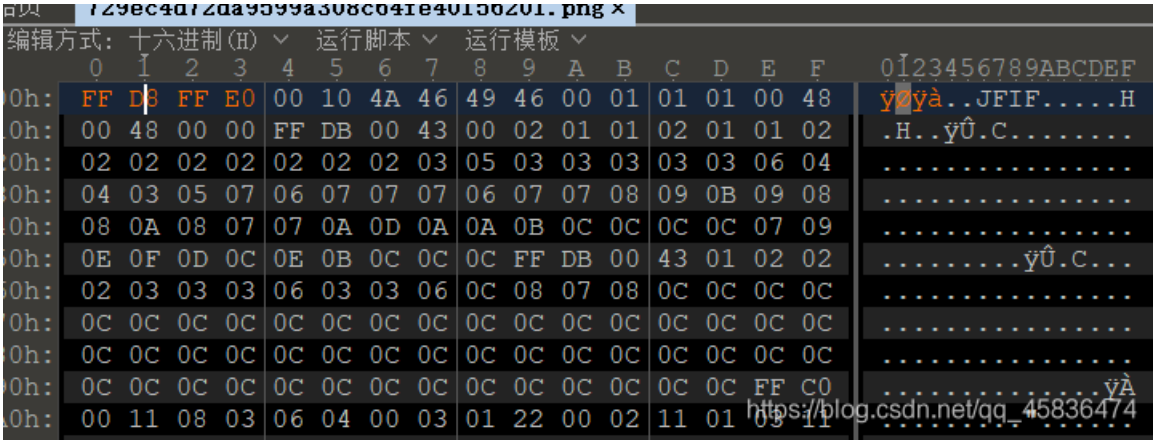
Untitled1.rar

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   52 61 72 21 1A 07 00 CE 99 73 80 00 0D 00 00 00   Rar!...Î™s€.....
00000010   00 00 00 00 E4 A0 1A B6 69 1F 9A 85 9B BC E5 56   ....ä .¶i.š…›¼åV
00000020   D5 09 28 F8 E8 66 E5 60 49 AF 8D 42 9F FF 71 0D   Õ.(øèfå`I¯.BŸÿq.
00000030   FE 75 9E 23 7B AD BF 2E C9 9D 89 1B 1B EA 8C 7B   þuž#{.¿.É.‰..êŒ{
00000040   6E FA 6C EF 6E 39 96 D9 38 FB 8F FA C5 2F 47 1B   núlïn9–Ù8û.úÅ/G.
00000050   F4 1B 64 AA C8 65 88 8B 62 65 4C BB 30 DB 8B C3   ô.dªÈeˆ‹beL»0Û‹Ã
00000060   DA 15 7A 99 7B A8 A4 E6 61 90 AE E8 80 D6 82 58   Ú.z™{¨¤æa.®è€Ö‚X
00000070   8E A2 FE 8E 7C E1 11 FE D6 D1 F7 45 A2 53 F7 38   Ž¢þŽ|á.þÖÑ÷E¢S÷8
00000080   F7 A4 4A E8 B5 D5 CE D4 5D 78 26 88 00 36 8D 69   ÷¤JèµÕÎÔ]x&ˆ.6.i
00000090   BD C8 0D 5E 92 AB 24 24 CF 56 E5 BC 31 ED 0C 02   ½È.^'«$$ÏVå¼1í..
000000A0   A8 EE 7A 49 94 C9 CD 1E 02 A8 7C AD B9 21 31 4B   ¨îzI"ÉÍ..¨|.¹!1K
000000B0   F6 17 70 40 E4 3D 19 39 8C E4 A9 BD 90 D1 3D C6   ö.p@ä=.9Œä©½.Ñ=Æ
000000C0   93 BE F8 E3 09 F8 80 CB FA 3A 04 2F AD F8 C6 39   "¾øã.ø€Ëú:./.øÆ9
000000D0   54 FC 51 71 17 A6 22 F2 03 31 5D E8 96 BB C5 16   TüQq.¦"ò.1]è–»Å.
000000E0   9A 30 C3 5A 3F 9E A6 1A 92 2B C7 12 94 AD 51 1D   š0ÃZ?ž¦.'+Ç.".Q.
000000F0   F4 BD 0E CF 88 DC 40 4C 4A ED 46 00 00 46 39 FF   ô½.Ïˆ Ü@LJíF..F9ÿ
00000100   E1 25 F6 8E 7D B7 5A DF A0 FF 99 D0 AE 09 C2 86   á%öŽ}·Zß ÿ™Ð®.Â†
00000110   38 3C 24 45 AD EF 7D F0 A7 3D EB E2 66 B6 2F 8B   8<$E.ï}ð§=ëâf¶/‹
00000120   DD 8E 9D 86 50 4D 91 8E 79 D0 F2 D5 10 5C EF 46   ÝŽ.†PM'ŽyÐòÕ.\ïF
00000130   9F CF BF 47 30 86 DE 8A 6A 61 5F DD 5C 58 85 80   ŸÏ¿G0†ÞŠja_Ý\X…€
00000140   42 85 62 1E FC 9B 6D E7 68 E9 3D 29 80 B6 D9 D9   B…b.ü›mçhé=)€¶ÙÙ
00000150   BF C8 36 A0 68 A7 F8 62 BD B0 80 E1 FC 38 74 DB   ¿È6 h§øb½°€áü8tÛ
```


是压缩包，而且压缩包有密码，emmm，也不是伪加密。那就暴力破解试试。

然后打开是个图片，但是图片无法打开。

010editor查看，发现图片类型是JFIF,应该是jpg图片格式，所以将文件头修改成jpg格式的。

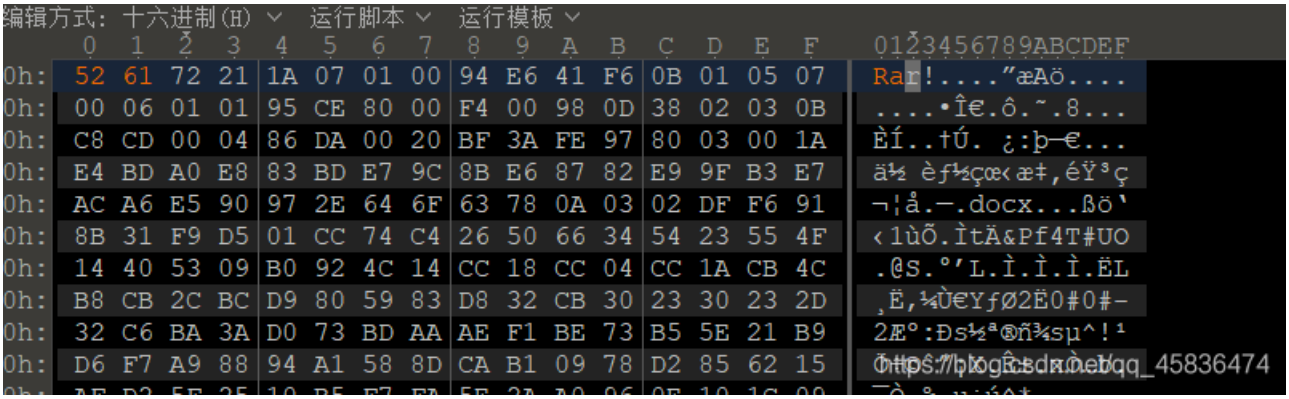


然后看到图片

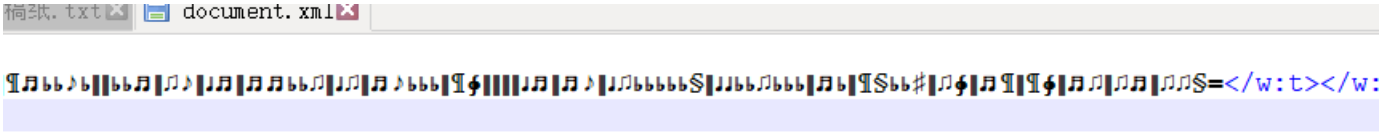

```
flag{57cd4cfd4e07505b98048ca106132125}
```

[MRCTF2020]你能看懂音符吗

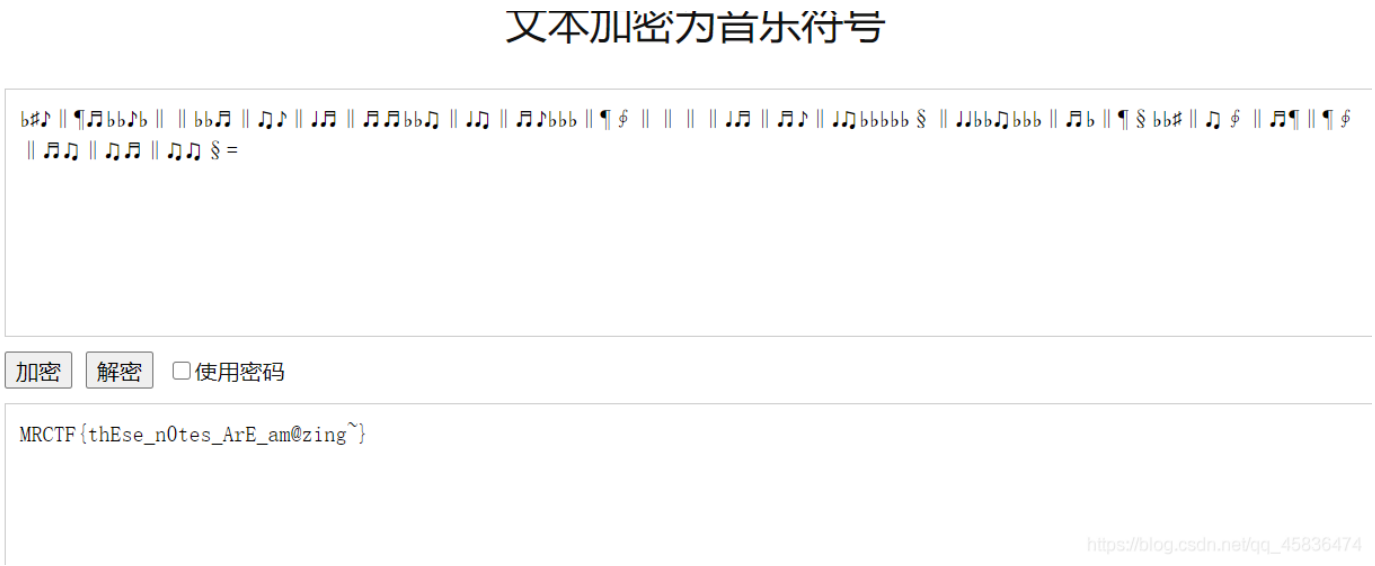
压缩包损坏，010editor看到前两组数据换了位置，改回来就行



然后解压得出一个word文档，打不开，010editor看出是zip压缩包。改后缀。
解压得到一堆文件，根据经验，信息一定藏在document里，果然找到了音符



然后使用在线网站解码就行了



百里挑一

解压文件得到的是pcap数据包，题目提示好多图片，wireshark打开导出http对象，保存到一个文件夹中。然后在kali中使用一条命令找到一半的flag

```
exiftool *|grep flag
```

意思是在当前文件夹中匹配flag字段
关于exiftool看这里□exiftool的说明使用

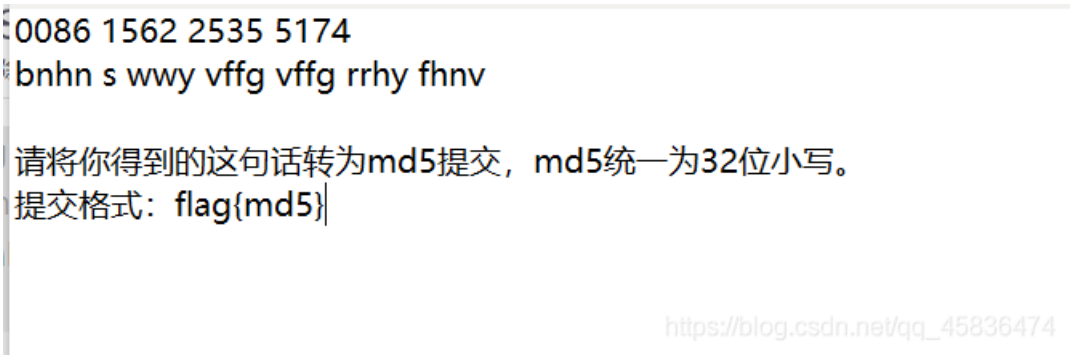
另一半需要在wireshark中找
但是我找了半天也没找到，烦躁□
看了wp发现是114……郁闷□

这……我真是□□8□

```
flag{ae58d0408e26e8f26a3c0589d23edeec}
```

从娃娃抓起

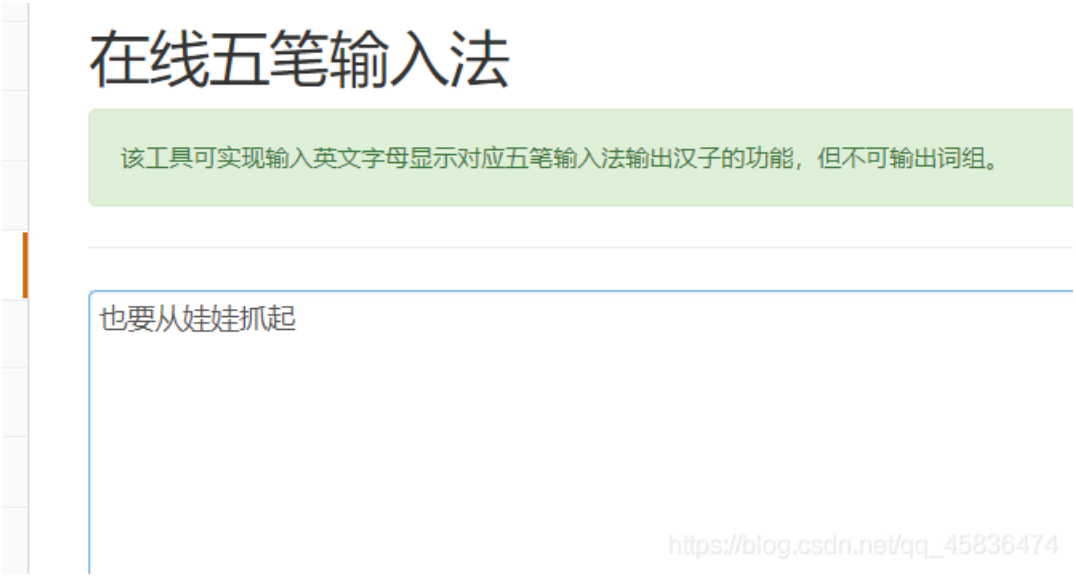
两种编码，



查询后了解到分别是中文电码和五笔编码

0086	1562	2535	5174
人	工	智	能

第一行——人工智能



第二行——也要从娃娃抓起

字符串	人工智能也要从娃娃抓起
16位 小写	d2c008fe7e2664bd
16位 大写	D2C008FE7E2664BD
32位 小写	3b4b5dccd2c008fe7e2664bd1bc19292
32位 大写	3B4B5DCCD2C008FE7E2664BD1BC19292

32位小写

[DDCTF2018](ノ°□°)ノ ┻━┻

打开文件发现一串字符串。

```
1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e3e6b4b3e2b5b0b6b1b0e6e1e5e1b5fd
```

十六进制的数字，先转换成10进制的。需要先将这么多数字中两个两个分开。
脚本：

```
s="d4e8e1f4a0f7e1f3a0e6e1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e3e6b4b
3e2b5b0b6b1b0e6e1e5e1b5fd"
a = ""
for i in range(0,len(s),2):
    a = a+"0x"
    a += s[i:i+2]
    a += ","
print(a)
```

```
0xd4,0xe8,0xe1,0xf4,0xa0,0xf7,0xe1,0xf3,0xa0,0xe6,0xe1,0xf3,0xf4,0xa1,0xa0,0xd4,0xe8,0xe5,0xa0,0xe6,0xec,0xe1,0x
e7,0xa0,0xe9,0xf3,0xba,0xa0,0xc4,0xc4,0xc3,0xd4,0xc6,0xfb,0xb9,0xb2,0xb2,0xe1,0xe2,0xb9,0xb9,0xb7,0xb4,0xe1,0xb4
,0xb7,0xe3,0xe4,0xb3,0xb2,0xb2,0xe3,0xe6,0xb4,0xb3,0xe2,0xb5,0xb0,0xb6,0xb1,0xb0,0xe6,0xe1,0xe5,0xe1,0xb5,0xfd,
```

然后转换成ascii码， 但是转换成10进制时，发现数值都大于128，所以减去128进行尝试，`(128=0x80)`

```
a=[0xd4,0xe8,0xe1,0xf4,0xa0,0xf7,0xe1,0xf3,0xa0,0xe6,0xe1,0xf3,0xf4,0xa1,0xa0,0xd4,0xe8,0xe5,0xa0,0xe6,0xec,0xe1
,0xe7,0xa0,0xe9,0xf3,0xba,0xa0,0xc4,0xc4,0xc3,0xd4,0xc6,0xfb,0xb9,0xb2,0xb2,0xe1,0xe2,0xb9,0xb9,0xb7,0xb4,0xe1,0
xb4,0xb7,0xe3,0xe4,0xb3,0xb2,0xb2,0xe3,0xe6,0xb4,0xb3,0xe2,0xb5,0xb0,0xb6,0xb1,0xb0,0xe6,0xe1,0xe5,0xe1,0xb5,0xf
d]
for i in a:
    print(chr(i-0x80), end="")
```

```
n [2]: a=[0xd4, 0xe8, 0xe1, 0xf4, 0xa0, 0xf7, 0xe1, 0xf3, 0xa0, 0xe6, 0xe1, 0xf3, 0xf4, 0xa1, 0xa0, 0xd4, 0xe8, 0xe5, 0xa0, 0xe6, 0xec, 0x
  ...: 1, 0xe7, 0xa0, 0xe9, 0xf3, 0xba, 0xa0, 0xc4, 0xc4, 0xc3, 0xd4, 0xc6, 0xfb, 0xb9, 0xb2, 0xb2, 0xe1, 0xe2, 0xb9, 0xb9, 0xb7, 0xb4, 0xe
  ...: , 0xb4, 0xb7, 0xe3, 0xe4, 0xb3, 0xb2, 0xb2, 0xe3, 0xe6, 0xb4, 0xb3, 0xe2, 0xb5, 0xb0, 0xb6, 0xb1, 0xb0, 0xe6, 0xe1, 0xe5, 0xe1, 0xb5
  ...: 0xfd]
  ...: for i in a:
  ...:     print(chr(i-0x80), end="")
  ...:
hat was fast! The flag is: DDCTF{922ab9974a47cd322cf43b50610faea5}
n [3]:
```


得到flag

还找到一个一步走的脚本

```
def hex_str(str):
    hex_str_list=[]
    for i in range(0,len(str)-1,2):
        hex_str=str[i:i+2]
        hex_str_list.append(hex_str)
    print("hex列表：%s\n"%hex_str_list)
    hex_to_str(hex_str_list)


def hex_to_str(hex_str_list):
    int_list=[]
    dec_list=[]
    flag=''
    for i in range(0,len(hex_str_list)):
        int_str=int('0x%s'%hex_str_list[i],16)
        int_list.append(int_str)
        dec_list.append(int_str-128)
    for i in range(0,len(dec_list)):
        flag += chr(dec_list[i])
    print("转化为十进制int列表：%s\n"%int_list)
    print("-128得到ASCII十进制dec列表：%s\n"%dec_list)
    print('最终答案：%s'%flag)


if __name__=='__main__':
    str='d4e8e1f4a0f7e1f3a0e6e1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e
3e6b4b3e2b5b0b6b1b0e6e1e5e1b5fd'
    print("字符串长度：%s"%len(str))
    hex_str(str)
```

总结

密码学了解

标准银河字母——对照表

键盘密码

当铺密码

变异凯撒

杂项了解

JS美化

解密电话音

工具——dtmf2num.exe

工具——FreeFileCamouflage

词频分析

- 脚本

- 在线网站

新了解的编码——EBCDIC（可用010editor转码）

跳舞的小人

base64隐写

敲击码

套娃解压压缩包——脚本

音符加密

工具——exiftool

中文电码

五笔编码

抓住端午节的小尾巴，端午节快乐！
以上就是这次总结，再接再厉。加油！加个鸡腿□

文末寄语

> 欢迎来到现实世界，它糟糕得要命，但你会爱上它的。——《老友记》