SWCTF2022Writeup

原创

Amherstieae 于 2022-04-28 17:45:59 发布 309 收藏

分类专栏： wp 文章标签： wp

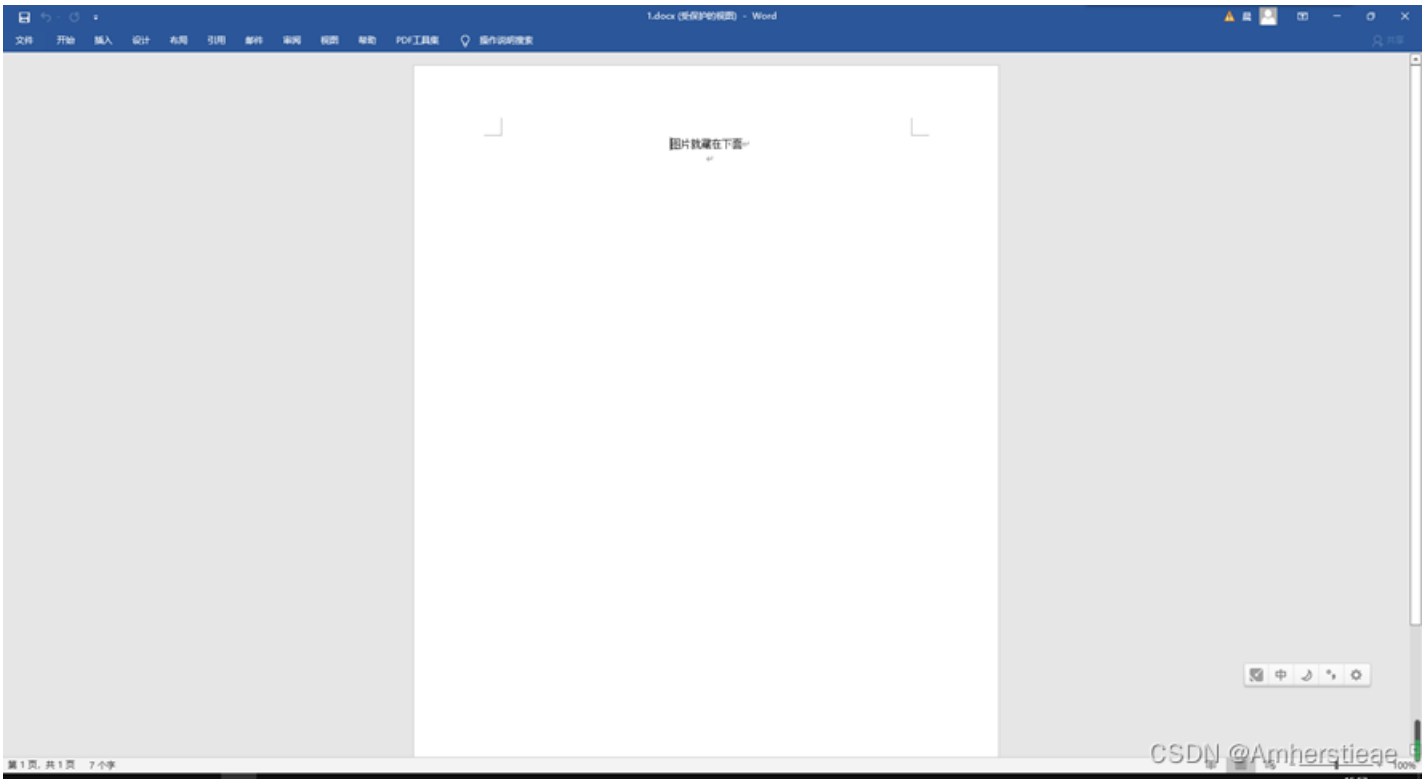
本文链接：https://blog.csdn.net/Amherstieae/article/details/124479260

写在前面：啊很久没有打一场完整的比赛并且复盘了，刚才得知有师傅读了我的博客学到一些新的东西啦，感觉写博客也是超有意义的一件事情，希望自己能继续坚持不懈的走下去，也算是对自己的一个勉励吧。

Game

图片在下面

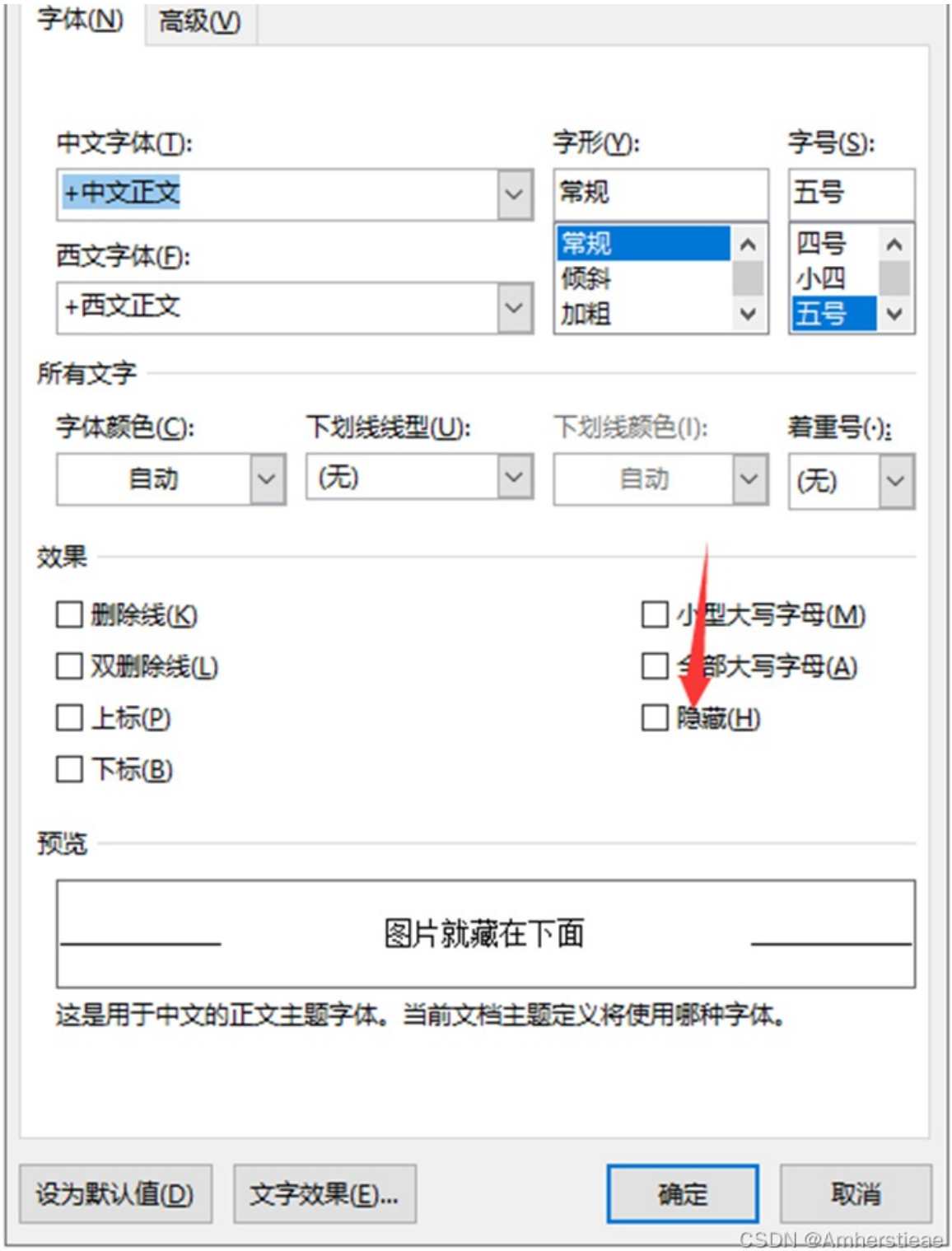
下载文件附件名称为docx，那么一般文件就是一个文档，修改名称为1.docx即可看见里面正文，如下



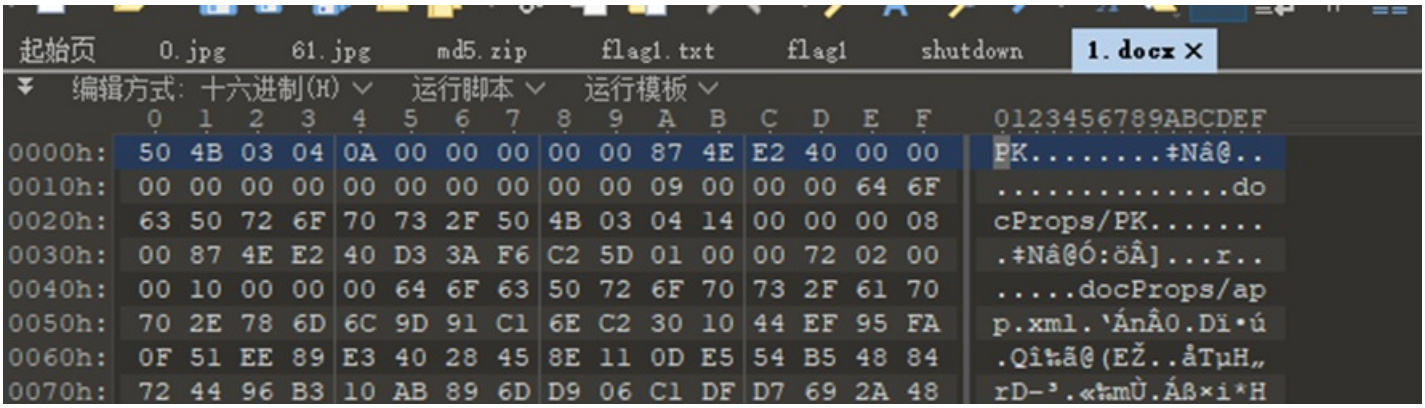
对于docx文档有一个字体隐藏，或者是文字被改成了白色，如果有段落起止符的话可以根据这个来看，没有的话先大体看一下

文字&隐藏文字

隐藏文字：选中所有文字，右击有个字体，



看这个样子就是没有了，那我们可以直接用010打开这个文件，一般来说doc都是一个zip的文件，但也是有的不是，这是因为office的版本不一样

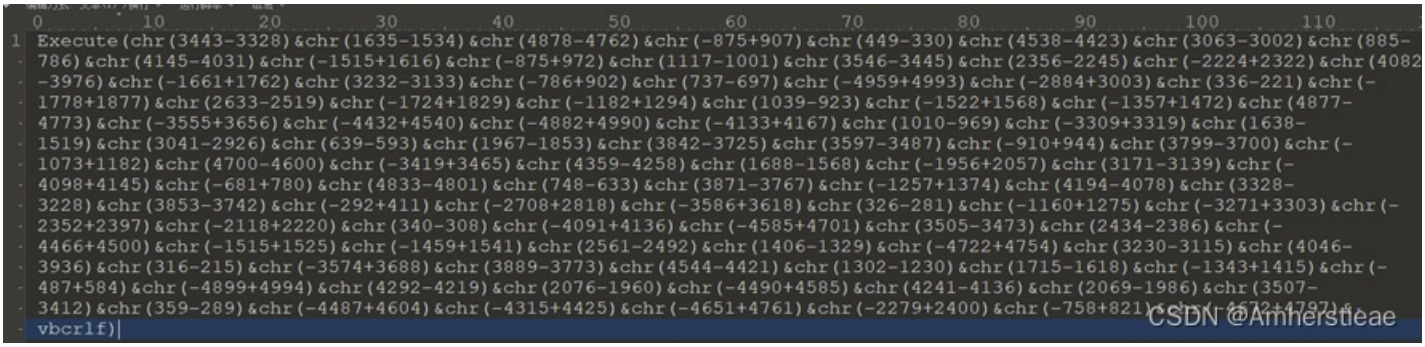


直接修改后缀名为1.zip，解压后一般这个地方会有图片，还有其他地方会显示文字

flag即为图片上

经典花活

这个题目是一个后缀为vbs的文件，下载后直接360报毒2333（出题人这可真狠呐
直接无视不打开，修改后缀让他不能识别用010打开，看到以下的东西



浅算一下昂，第一个是s，直接手撕（可行√

```
from operator import le
from re import S

s = 'chr(3443-3328)&chr(1635-1534)&chr(4878-4762)&chr(-875+907)&chr(449-330)&chr(4538-4423)&chr(3063-3002)&chr(885-786)&chr(4145-4031)&chr(-1515+1616)&chr(-875+972)&chr(1117-1001)&chr(3546-3445)&chr(2356-2245)&chr(-2224+2322)&chr(4082-3976)&chr(-1661+1762)&chr(3232-3133)&chr(-786+902)&chr(737-697)&chr(-4959+4993)&chr(-2884+3003)&chr(336-221)&chr(-1778+1877)&chr(2633-2519)&chr(-1724+1829)&chr(-1182+1294)&chr(1039-923)&chr(-1522+1568)&chr(-1357+1472)&chr(4877-4773)&chr(-3555+3656)&chr(-4432+4540)&chr(-4882+4990)&chr(-4133+4167)&chr(1010-969)&chr(-3309+3319)&chr(1638-1519)&chr(3041-2926)&chr(639-593)&chr(1967-1853)&chr(3842-3725)&chr(3597-3487)&chr(-910+944)&chr(3799-3700)&chr(-1073+1182)&chr(4700-4600)&chr(-3419+3465)&chr(4359-4258)&chr(1688-1568)&chr(-1956+2057)&chr(3171-3139)&chr(-4098+4145)&chr(-681+780)&chr(4833-4801)&chr(748-633)&chr(3871-3767)&chr(-1257+1374)&chr(4194-4078)&chr(3328-3228)&chr(3853-3742)&chr(-292+411)&chr(-2708+2818)&chr(-3586+3618)&chr(326-281)&chr(-1160+1275)&chr(-3271+3303)&chr(-2352+2397)&chr(-2118+2220)&chr(340-308)&chr(-4091+4136)&chr(-4585+4701)&chr(3505-3473)&chr(2434-2386)&chr(-4466+4500)&chr(-1515+1525)&chr(-1459+1541)&chr(2561-2492)&chr(1406-1329)&chr(-4722+4754)&chr(3230-3115)&chr(4046-3936)&chr(316-215)&chr(-3574+3688)&chr(3889-3773)&chr(4544-4421)&chr(1302-1230)&chr(1715-1618)&chr(-1343+1415)&chr(-487+584)&chr(-4899+4994)&chr(4292-4219)&chr(2076-1960)&chr(-4490+4585)&chr(4241-4136)&chr(2069-1986)&chr(3507-3412)&chr(359-289)&chr(-4487+4604)&chr(-4315+4425)&chr(-4651+4761)&chr(-2279+2400)&chr(-758+821)&chr(-4672+4797)'
s = s.replace('chr(','').replace(')','')
s = s.split('&')
```

```
flag = ''
for i in s:
    length = len(i)
    print(length)
    if length == 9:
        num1 = i[:4]
        print(num1)
        num2 = i[5:]
        print(num2)
        symbol = i[4:5]
        print(symbol)
        if symbol=='-':
            flag += chr(int(num1)-int(num2))
        else:
            flag += chr(int(num1)+int(num2))
    elif length == 8:
        num1 = i[:4]
        num2 = i[5:]
        symbol = i[4:5]
        if symbol=='-':

            flag += chr(int(num1)-int(num2))
        else:
            flag += chr(int(num1)+int(num2))
    elif length == 7:
        num1 = i[:3]
        num2 = i[4:]
        symbol = i[3:4]
        if symbol=='-':

            flag += chr(int(num1)-int(num2))
        else:
            flag += chr(int(num1)+int(num2))
    else:
        num1 = i[:5]
        num2 = i[6:]
        symbol = i[5:6]
        if symbol=='-':

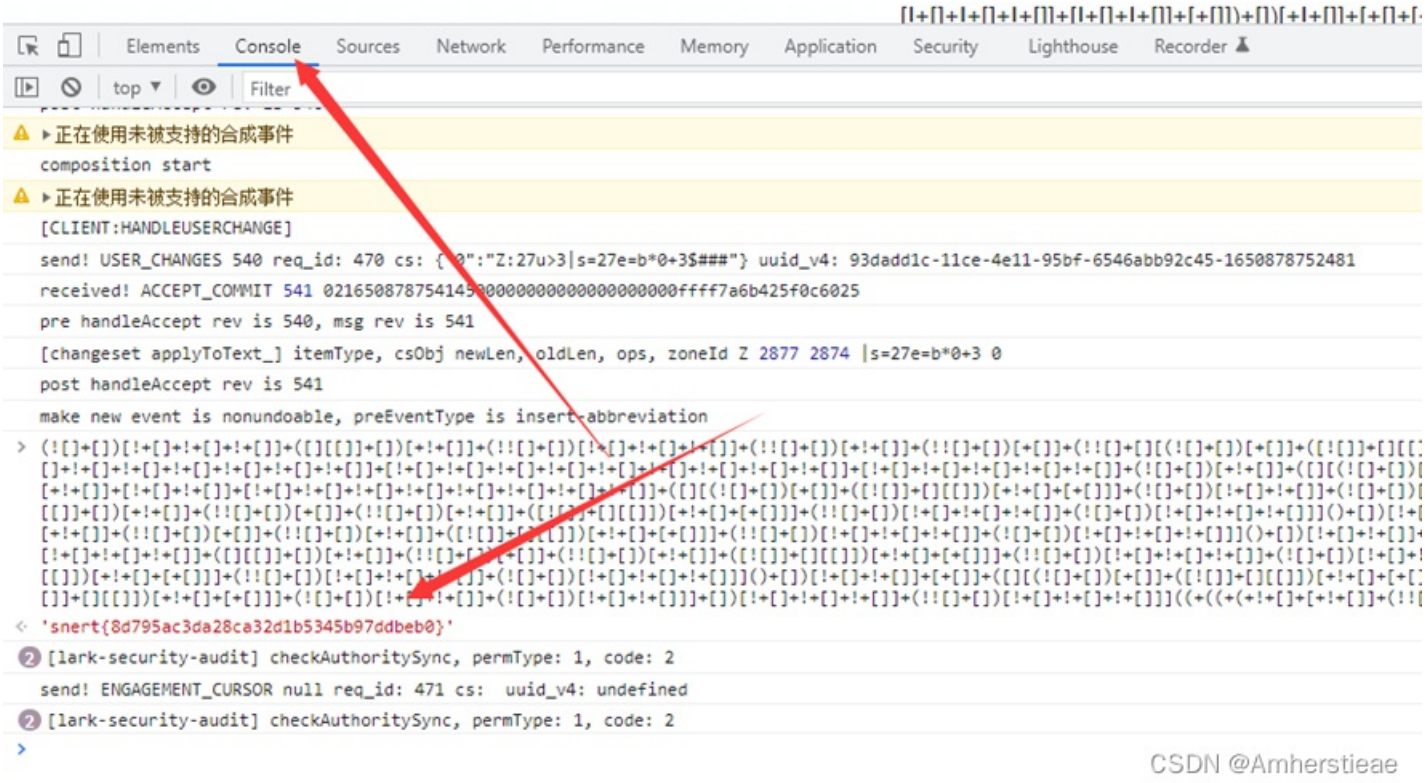
            flag += chr(int(num1)-int(num2))
        else:
            flag += chr(int(num1)+int(num2))
print(flag)
```

base64

昂c25lcnR7Y2U2OTAxNmJiZmQ1ZTQ4OWI1YWViMTc2NGRkMTY0MmF9很简单昂
解一下base64就好了
snert{ce69016bbfd5e489b5aeb1764dd1642a}

F**K

浅浅的；浏览器控制台跑一下f12，点第二个，贴进去，回车

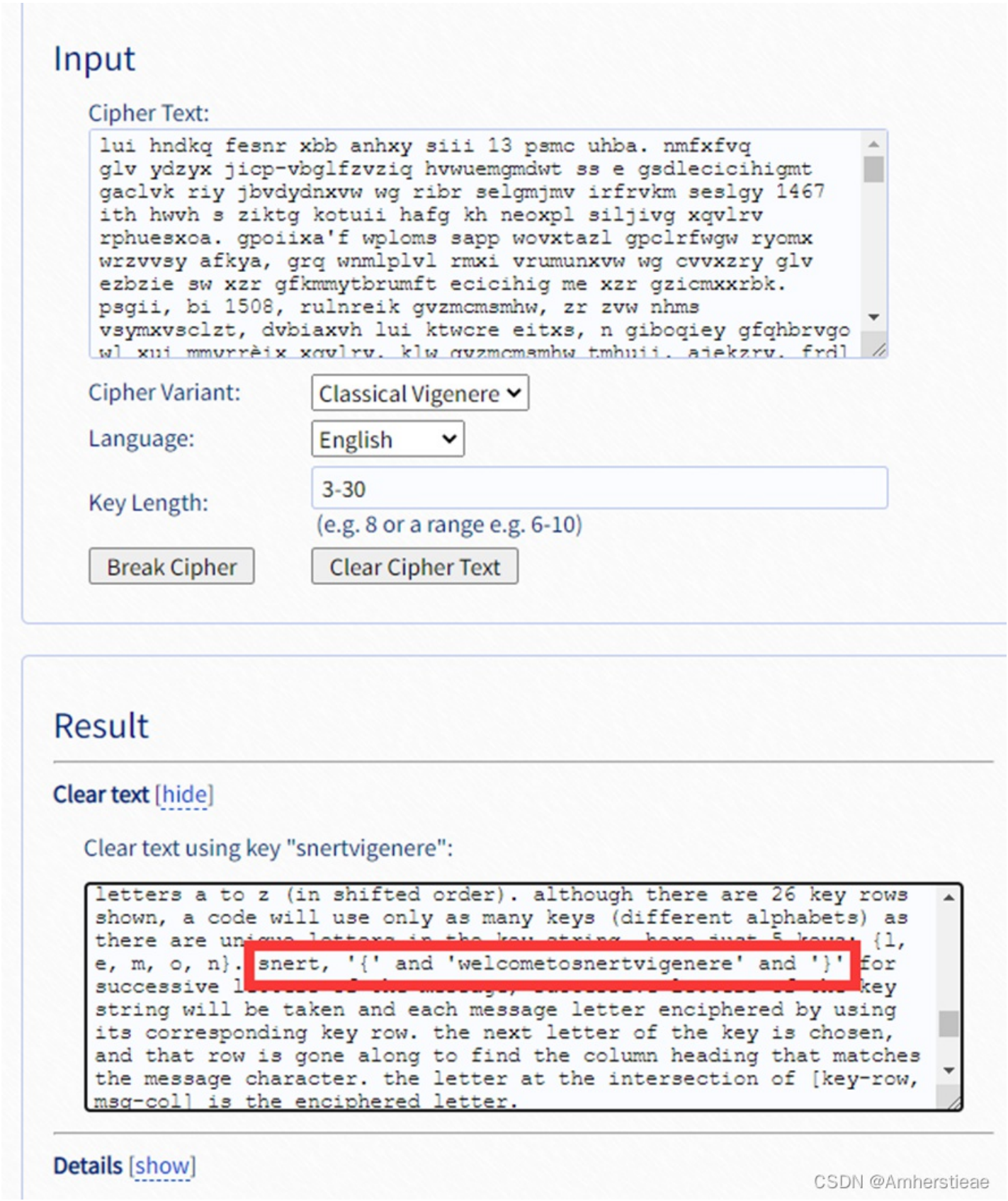


Crypto

easy_vigenere

题目名字为维吉尼亚，那么应该就是我们印象中的维吉尼亚了，但是并没有给密钥，那么应该。。。。

https://www.guballa.de/vigenere-solver



md5

下载附件压缩包，已经被加密了，工具浅浅爆破一下（一般没有提示的压缩包加密可以考虑伪加密和数字4-8位爆破

密码为以上，解压后得到两个txt，一个是提示，另一个为flag，那么看上去就很像是十六进制

313833667a3333363478656437356736346139 6d6635363234706461323432316564656564 71

183fz3364xed75g64a9mf5624pda2421edeedq

此时的hint就可以上场了，md5的形式是指0-9a-f，所以将不是md5里包含的全部删掉就可以了

183f3364ed7564a9f5624da2421edeed

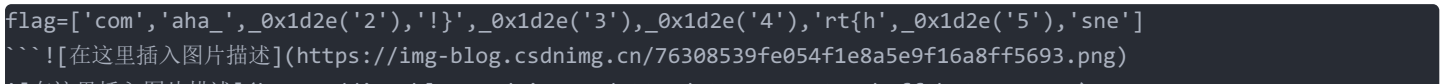
md5解密

包裹上snert{}就好啦

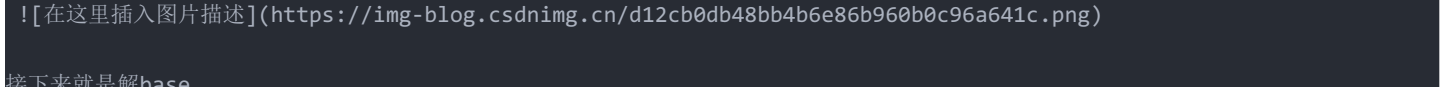
WEB

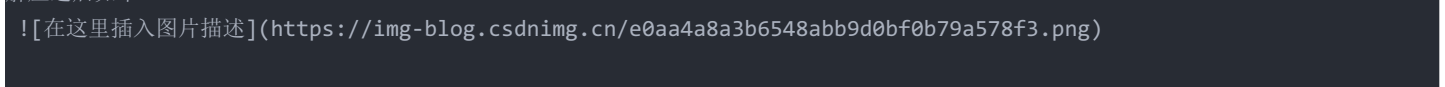
别踩白块儿

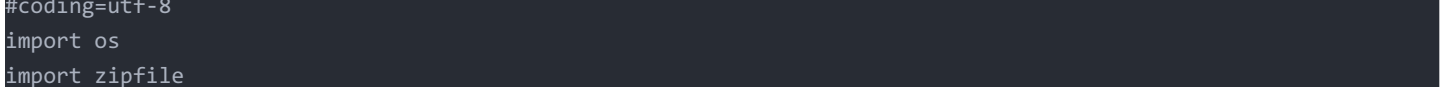
昂是个网页游戏题，浅玩一下，挺好玩的，就是不适配手机，看了一下网页源代码，有一个js昂，浅浅的格式化一下（比较好看，但下面的图是新截的
浅浅看一下逻辑，就是定义了一个flag，然后那些0x开头的都是函数，会调用这些函数生成一个字符串，且是固定的，就...复制这些函数到控制台运行一下就会出现

```
flag=['com','aha_',_0x1d2e('2'),'!}',_0x1d2e('3'),_0x1d2e('4'),'rt{h',_0x1d2e('5'),'sne']
```
```
```![在这里插入图片描述](https://img-blog.csdnimg.cn/76308539fe054f1e8a5e9f16a8ff5693.png)


然后就...拼起来就好了
 snert{haha_you_are_great_come_on!}
Misc
多看经文
下载附件压缩包可以看到一个未加密的密码和一个加密的flag，打开密码&联系题目名字猜测是与佛论禅，直接扒出收藏夹网址解密
 

看到解密之后的结果很像base但是开头又不是，猜测对称加密
尝试多次为rabbit
 

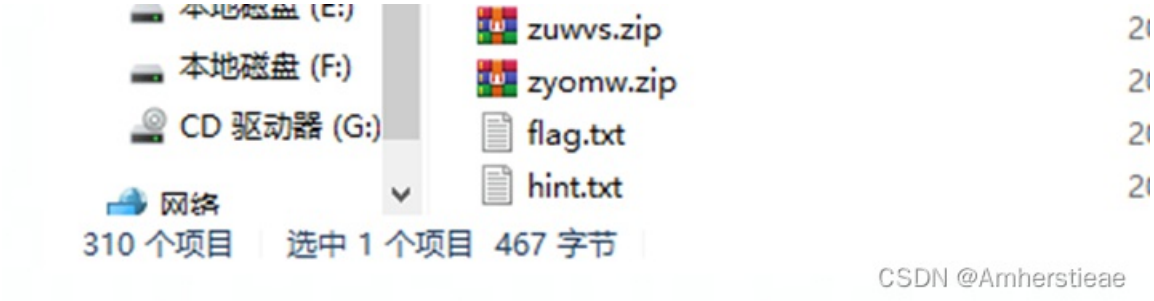
接下来就是解base
 

此时注意还有一点URL解码，但已经得到key了snert s1xs1xs1x
解压之后如下
 

套娃
一看很多个压缩包&压缩包密码都是名字，那么直接上脚本、

```python
#coding=utf-8
import os
import zipfile


orginal_zip = "4606.zip"
while True:
    tag = orginal_zip
    orginal_zip = zipfile.ZipFile(orginal_zip)
    for contents in orginal_zip.namelist():
        password = contents[0:contents.find('.')]
    print password
    orginal_zip.setpassword(tag[:-4])
    try:
        orginal_zip.extractall()
    except:
        break
    if(len(tag)>6):
        os.system("rm "+tag)
    orginal_zip=password+".zip"
```



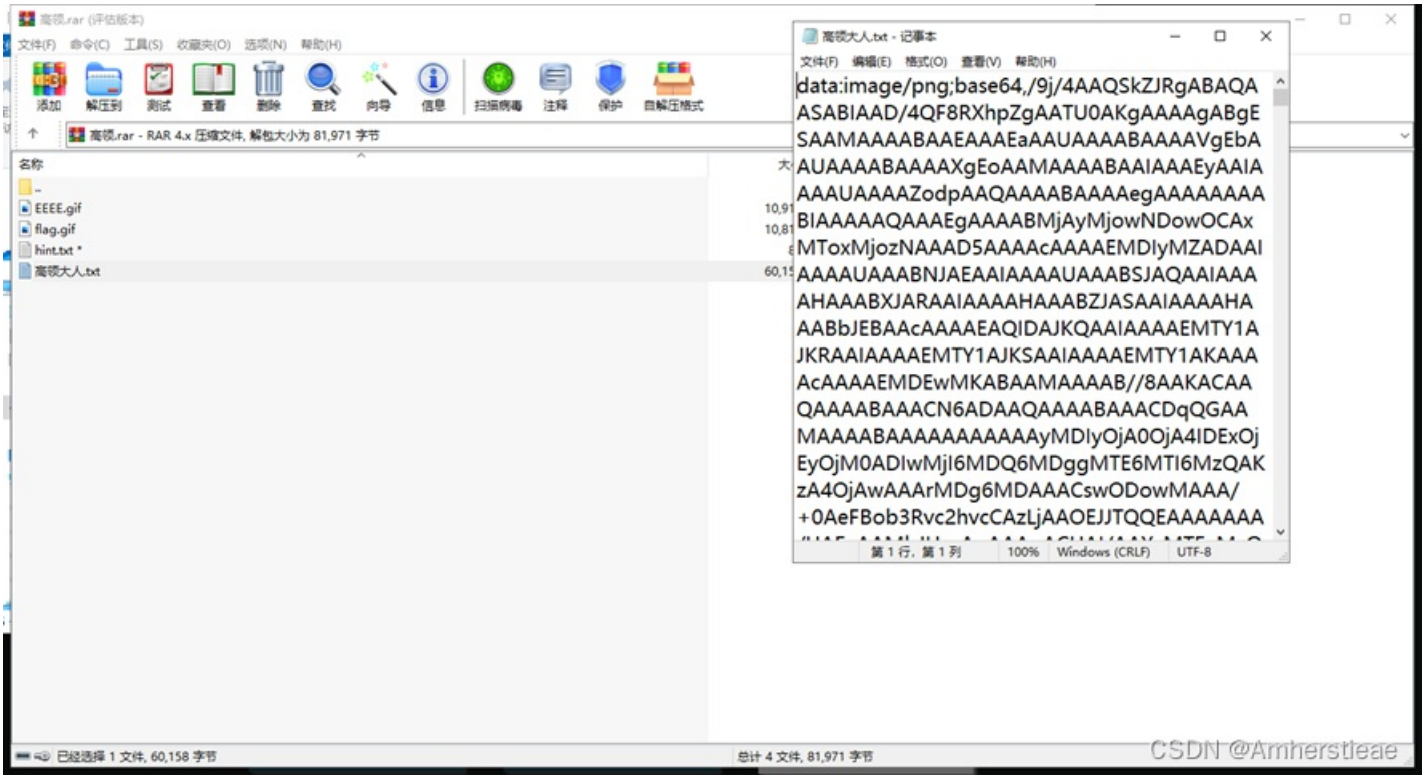
emmmm就307个？（出题人其心可诛
打开flag文件竟然还不是直接的flag，(大锤80，小锤60

```
嚼喵抡彤铤籍茂恫正舸阒恫抡虬衷茂怜抡怜皑节阒圯抡启启奴启皑启阒适怜缬舸缬皑怜馑=
```

就...直接千千秀字
https://www.qqxiuzi.cn/bianma/wenbenjiami.php

高领大人

下载压缩包之后打开入如下



非常明显的base64转图片，随便一个在线网站转图片，如下，emmmm就是压缩包密码了

解压了一个hint

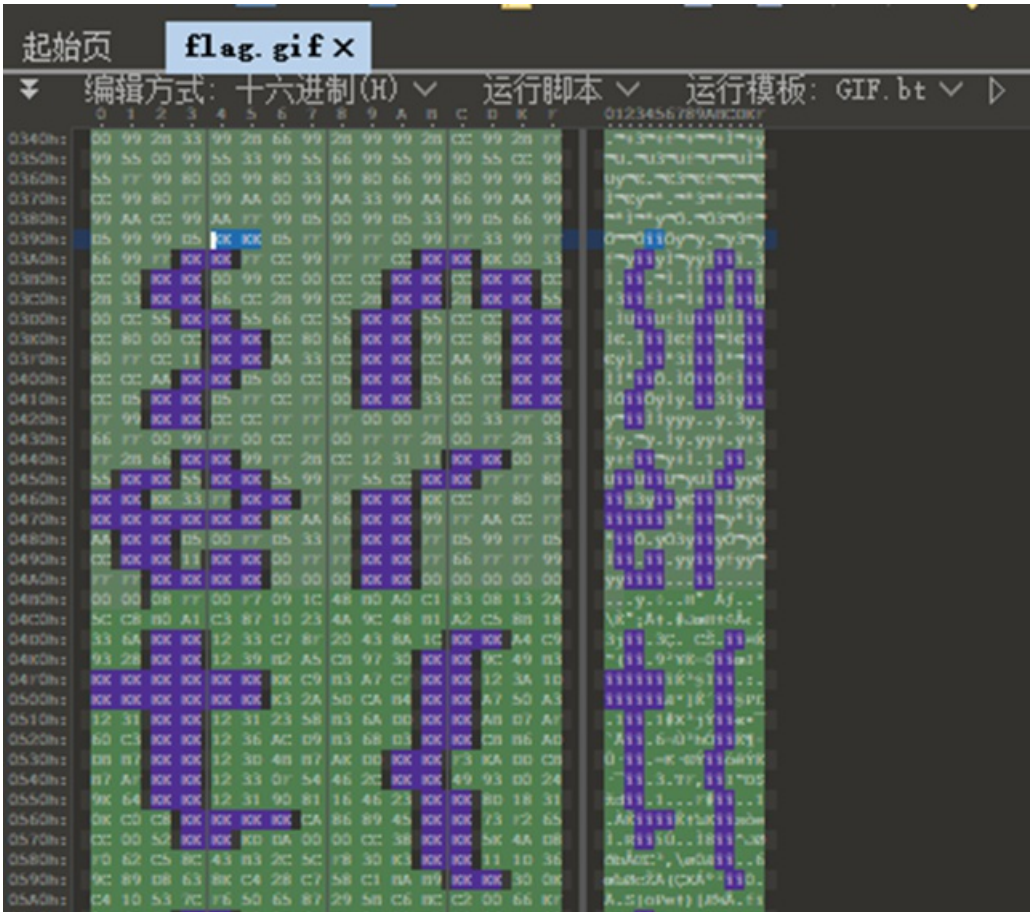
✻✻✻✻✻✻✻❁✻✳❉❉❀✻✻❁==

千千秀字一下

提示十六进制

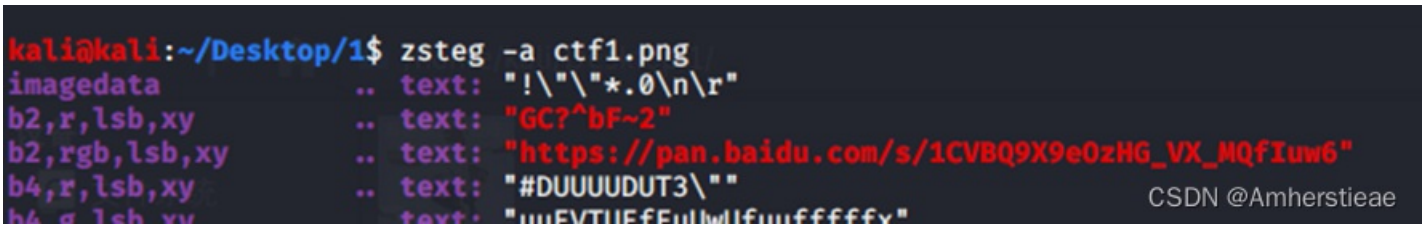
把flag那个GIF打开

联系到另一个正常GIF的eeee.gif，我以为是对比两个文件的不同，后来又搜了一下flag.GIF



简简单单的图片隐写

开局一张图，关于png的隐写一般是lsb，，直接zsteg梭一哈子
如下



根据出题人提示，去掉最后一位

https://pan.baidu.com/s/1CVBQ9X9eOzHG_VX_MQfluw

提取码就是那张图片的文件名啦ctf1（爆破什么的别想啦

下载发现是100张小图，把一张二维码切割成100小图（出题人其心可诛

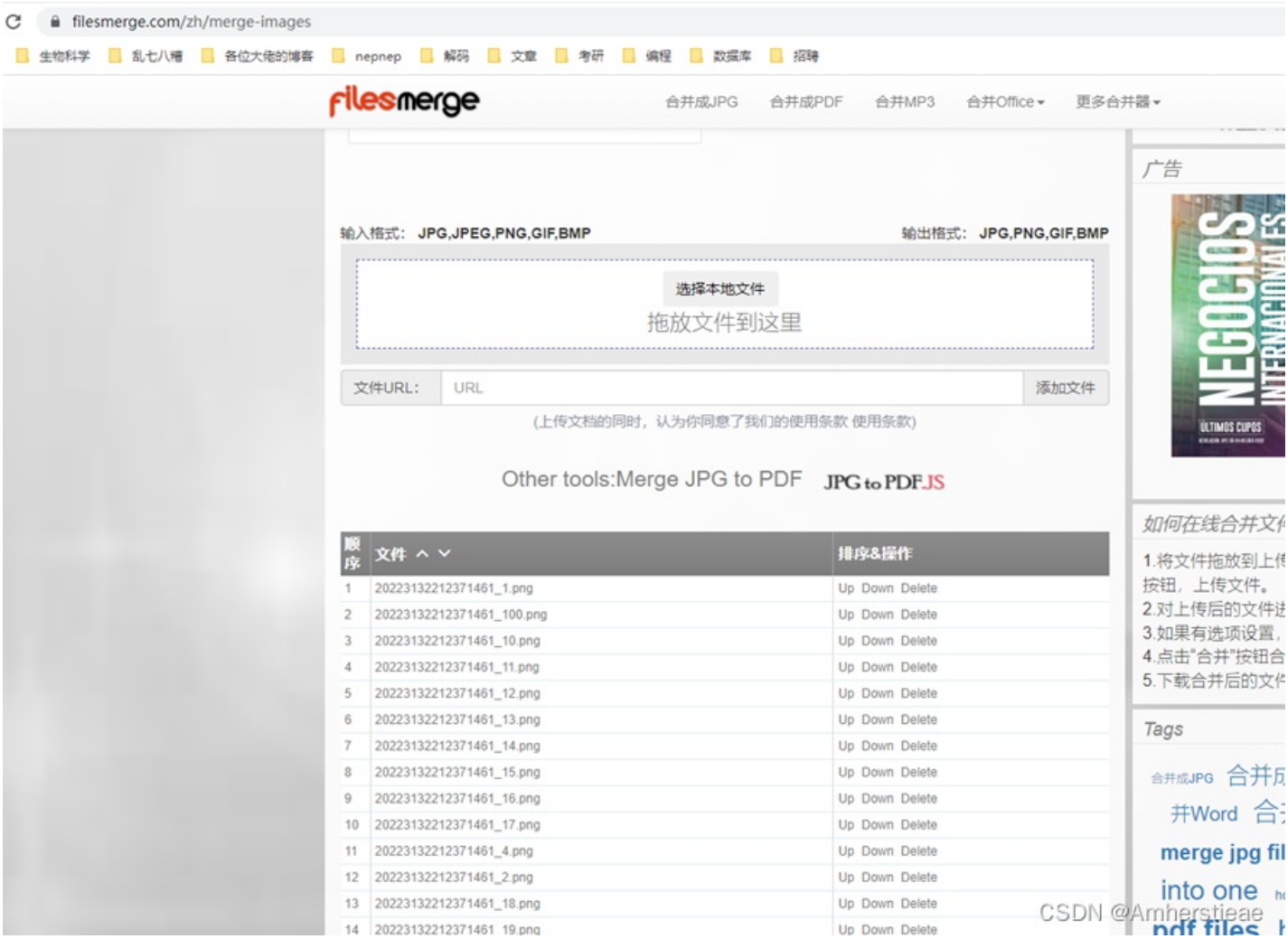
不难想象是10*10

因此，很随意的找一个在线顺序拼图的网站

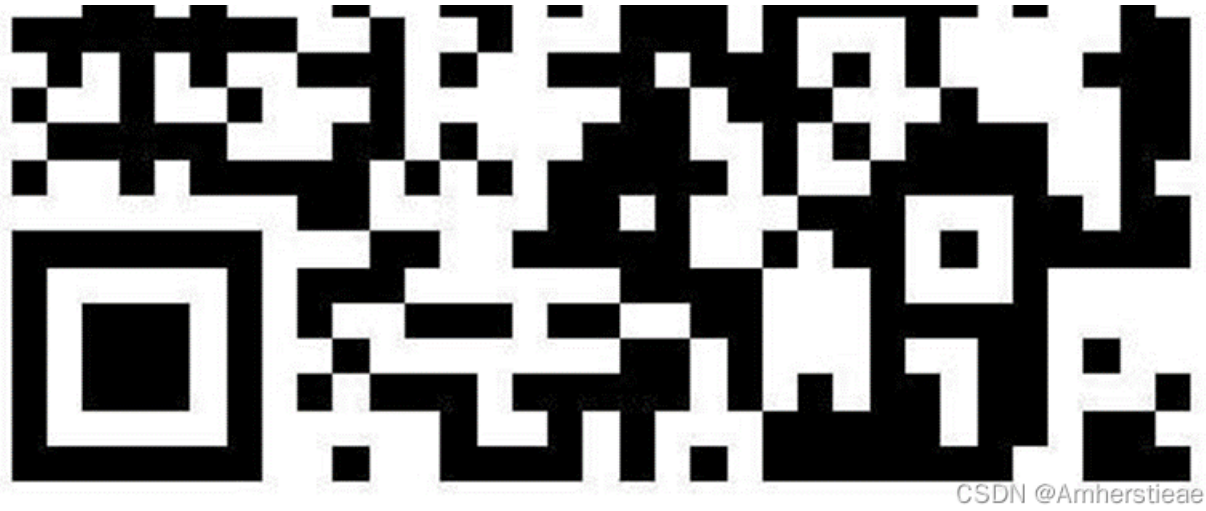
（一般来说自动拼图命令也有，但是不会按文件顺序，且会拼的稀碎，如下

）

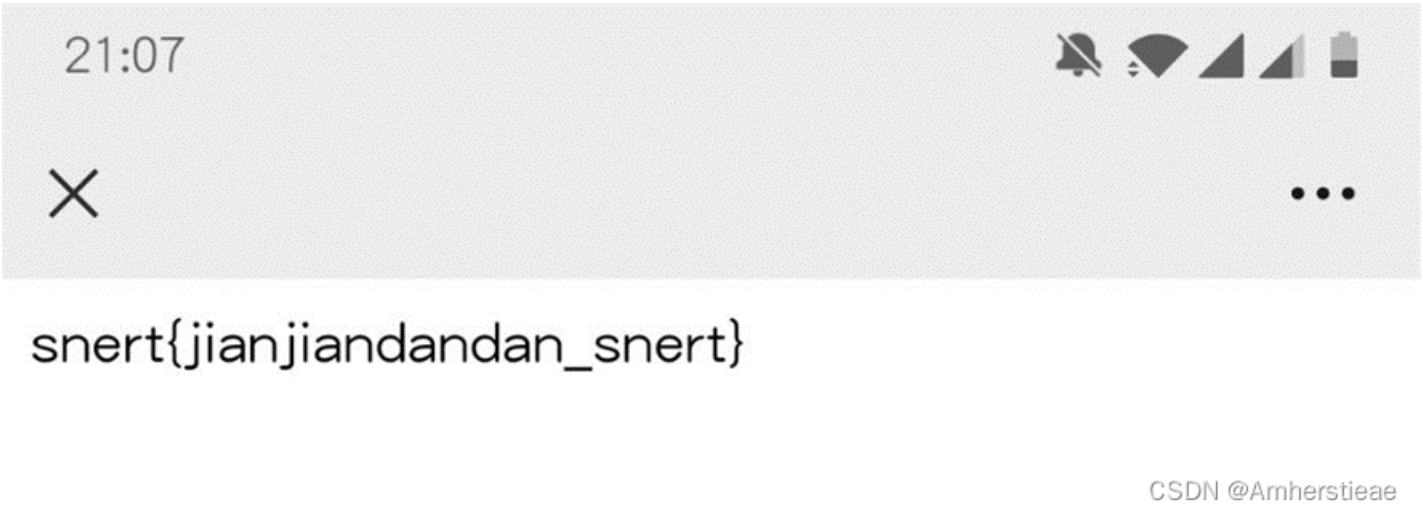
https://filesmerge.com/zh/merge-images



但这个网站不能拼太多，所以分两半拼出来就行了

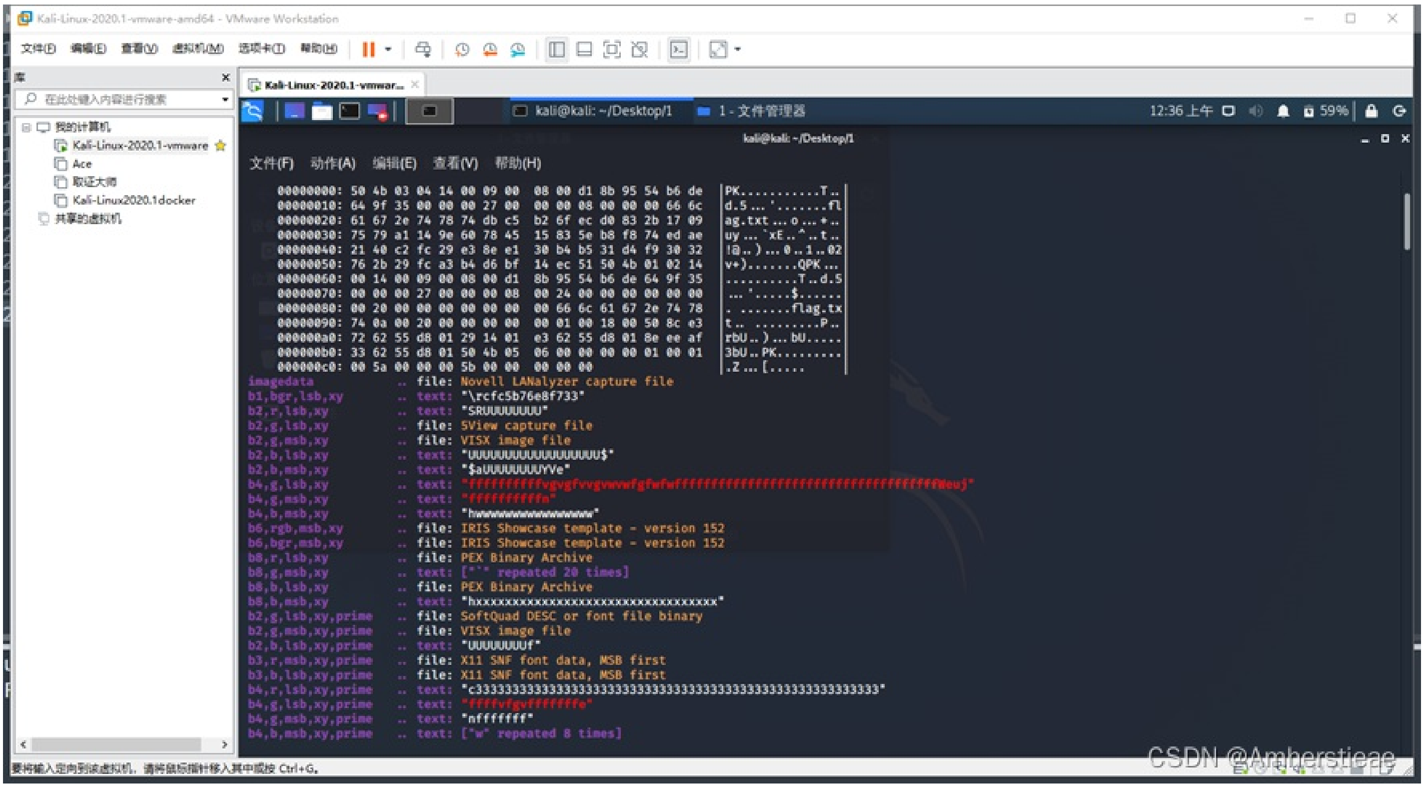


snert{jianjiandandan_ snert}

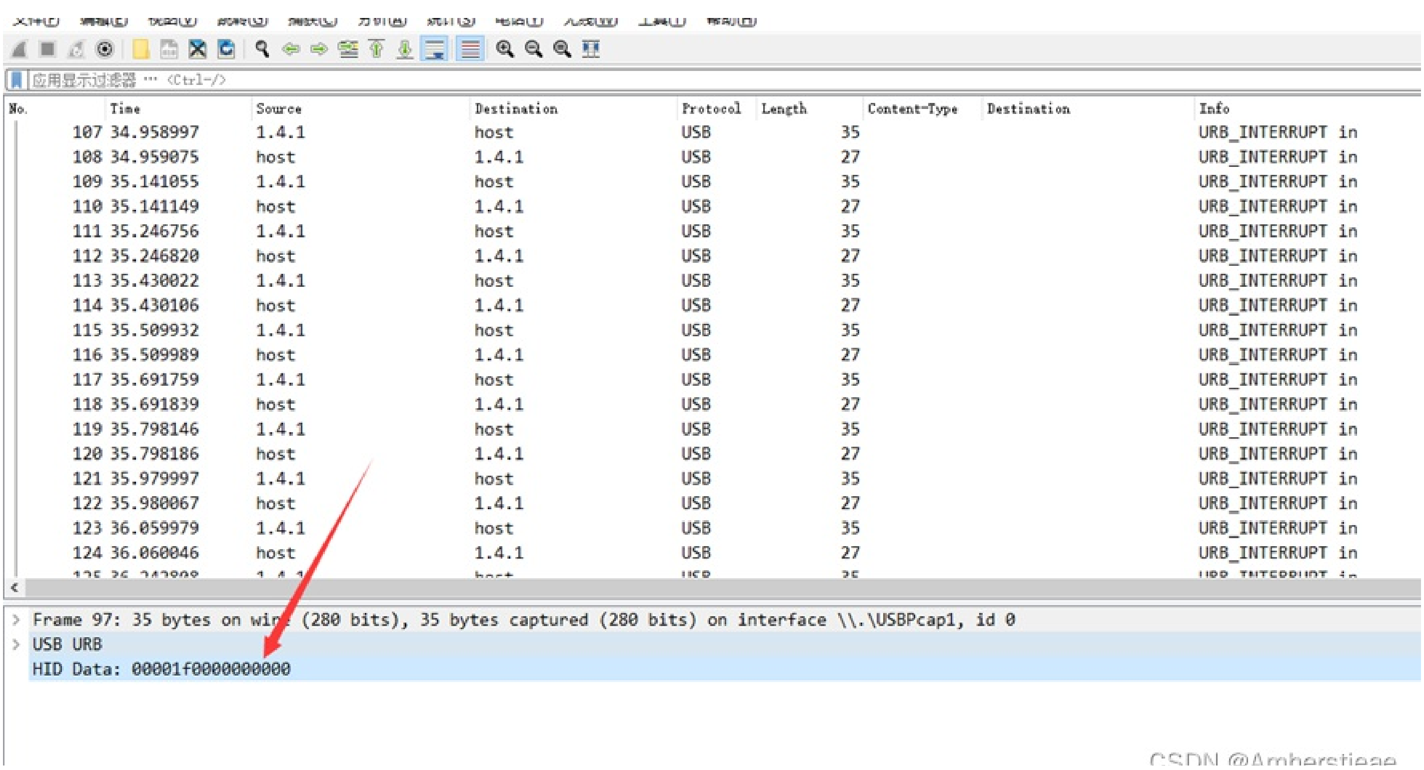


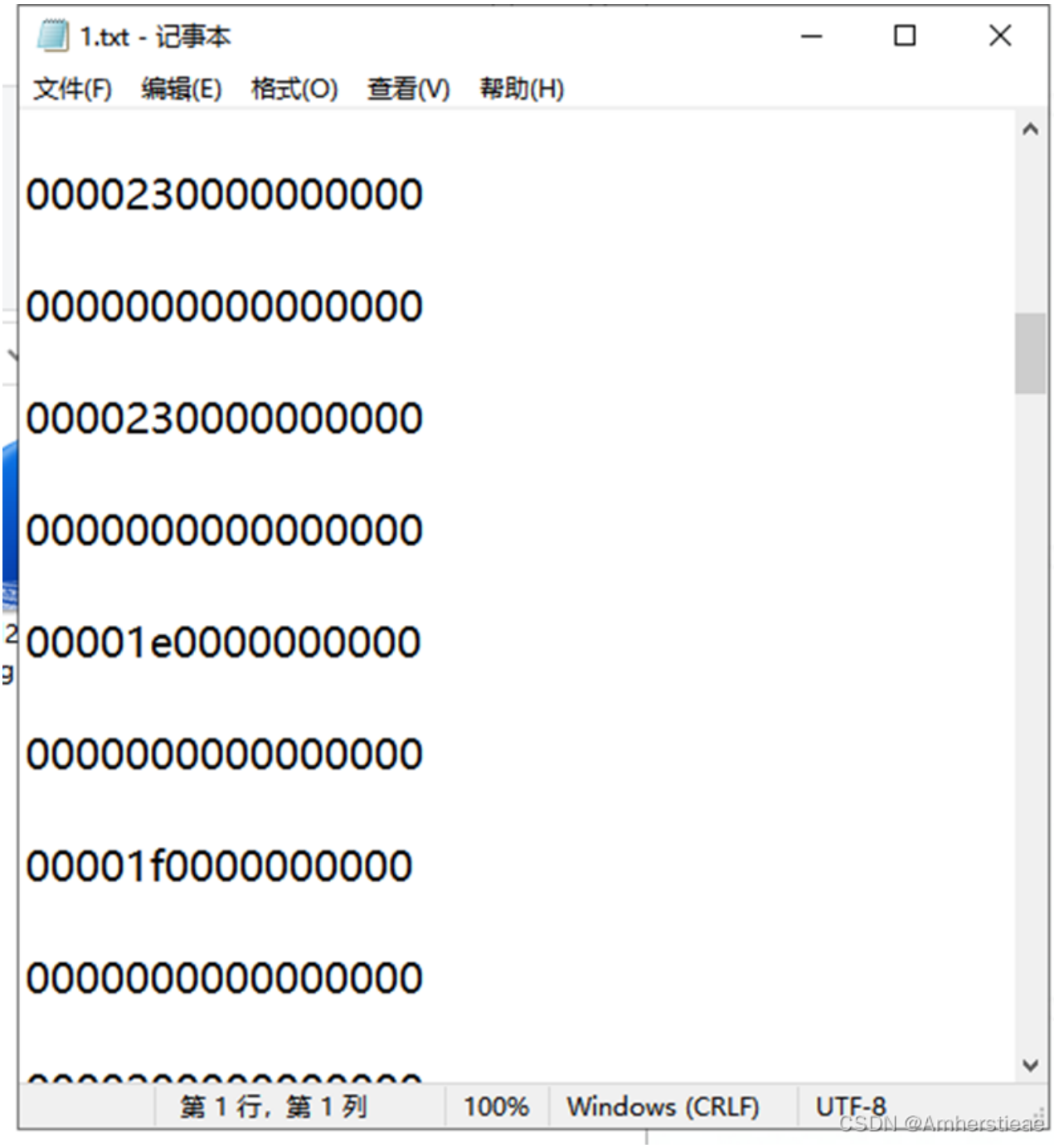
简单题

很明显，这个题图片这么大，出题人想搞的不是我，是我的电脑
直接010先看图片，最后面有个zip的压缩包，直接复制出来生成一个新的文件，打开之后发现密码，先放一边，根据hint说了两个不简单的图片，说明除了这个压缩包还有别的东西
直接虚拟机zsteg梭一下子，



嗯，就\r那个，不要\r就行了（第一部分over
看另一个流量包，名字为passwd2，也就是说压缩包密码有两部分，所以才想着去那张图片在找密码的第一部分
打开发现是USB的流量，看样子应该是键盘流量（出题人上错附件了，还没有发现，而且新的流量还是现抓的，快出来女装（狗头）
浏览几个流发现下面的部分有改变，直接用tshark提取出来
thark -r passwd2.pcapng -T fields -e usbhid.data>1.txt





然后脚本处理一下数据

Apache

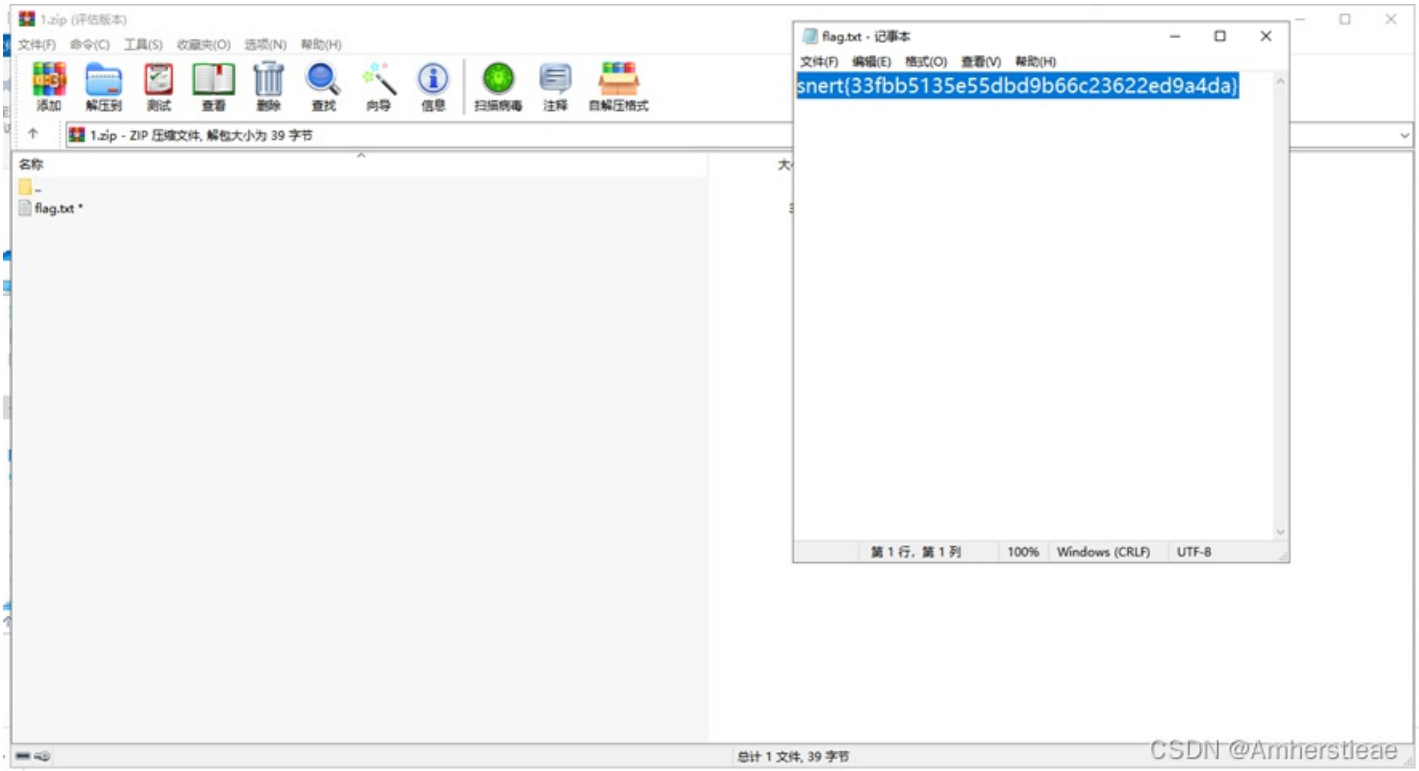
```
#tshark -r hack.pcapng -T fields -e usb.capdata > usb1data.txt
normalKeys = {"04":"a", "05":"b", "06":"c", "07":"d", "08":"e", "09":"f", "0a":"g", "0b":"h", "0c":"i", "0d":"j"
, "0e":"k", "0f":"l", "10":"m", "11":"n", "12":"o", "13":"p", "14":"q", "15":"r", "16":"s", "17":"t", "18":"u",
"19":"v", "1a":"w", "1b":"x", "1c":"y", "1d":"z","1e":"1", "1f":"2", "20":"3", "21":"4", "22":"5", "23":"6","24"
:"7","25":"8","26":"9","27":"0","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"-","2e":"
=","2f":"[","30":"]","31":"\\","32":"<NON>","33":";","34":"'","35":"<GA>","36":",","37":".","38":"/","39":"<CAP>
","3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F4>","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>","
43":"<F10>","44":"<F11>","45":"<F12>"}

shiftKeys = {"04":"A", "05":"B", "06":"C", "07":"D", "08":"E", "09":"F", "0a":"G", "0b":"H", "0c":"I", "0d":"J",
 "0e":"K", "0f":"L", "10":"M", "11":"N", "12":"O", "13":"P", "14":"Q", "15":"R", "16":"S", "17":"T", "18":"U", "
19":"V", "1a":"W", "1b":"X", "1c":"Y", "1d":"Z","1e":"!", "1f":"@", "20":"#", "21":"$", "22":"%", "23":"^","24":
"&","25":"*","26":"(","27":")","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"_","2e":"+
","2f":"{","30":"}","31":"|","32":"<NON>","33":"\"","34":":","35":"<GA>","36":"<","37":">","38":"?","39":"<CAP>"
,"3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F4>","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>","4
3":"<F10>","44":"<F11>","45":"<F12>"}

nums = []
keys = open('1.txt')
for line in keys:
    if len(line)!=17: #首先过滤掉鼠标等其他设备的USB流量
         continue
    nums.append(line[0:2]+line[4:6]) #取一、三字节
keys.close()
output = ""
for n in nums:
    if n[2:4] == "00" :
        continue

    if n[2:4] in normalKeys:
        if n[0:2]=="02": #表示按下了shift
            output += shiftKeys [n[2:4]]
        else :
            output += normalKeys [n[2:4]]
    else:
        output += '[unknown]'
print('output :' + output)
```

65366dd1c405354
所以压缩包密码为
cfc5b76e8f73365366dd1c405354



snert{33fbb5135e55dbd9b66c23622ed9a4da}

以上，over
完结撒花✿✿ヽ(°▽°)ノ✿