

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[wp 专栏收录该内容](#)

9 篇文章 0 订阅

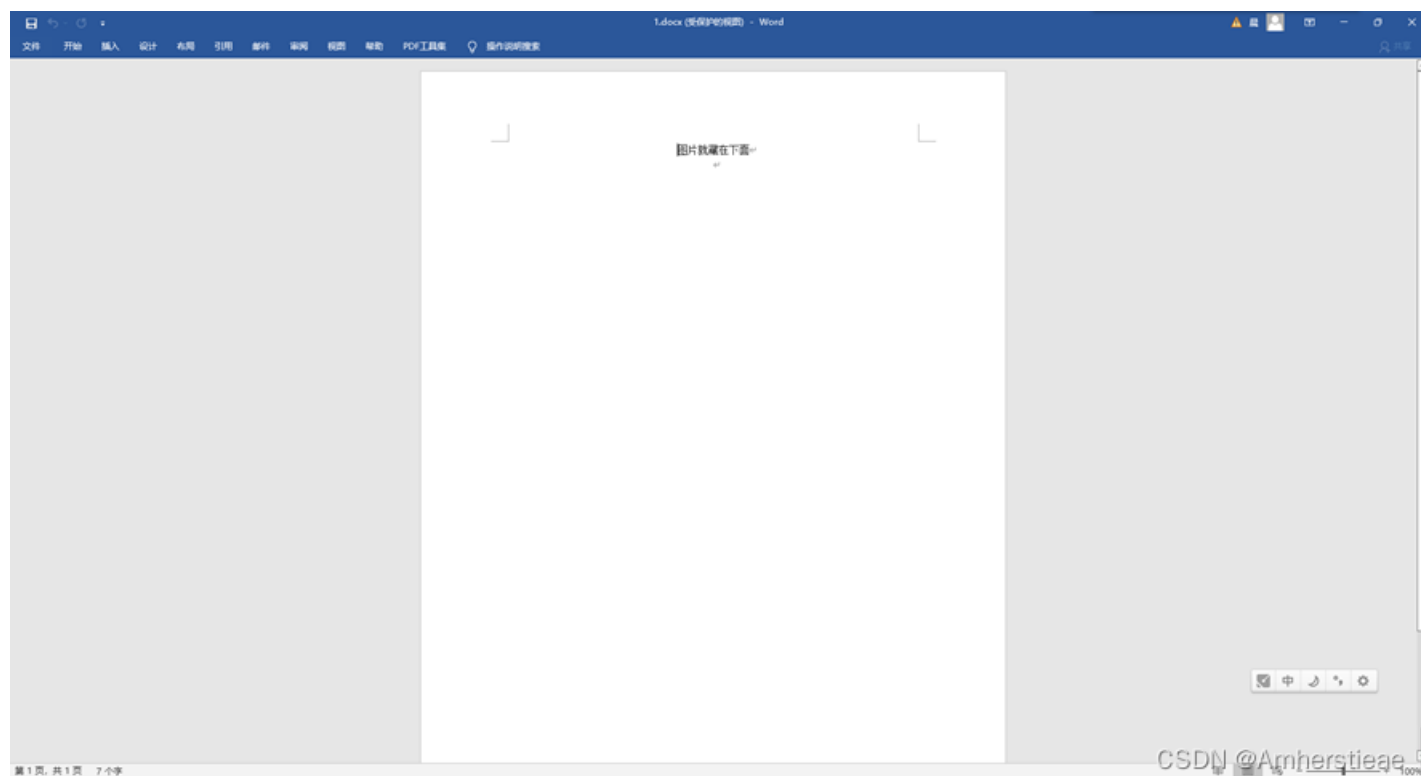
订阅专栏

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

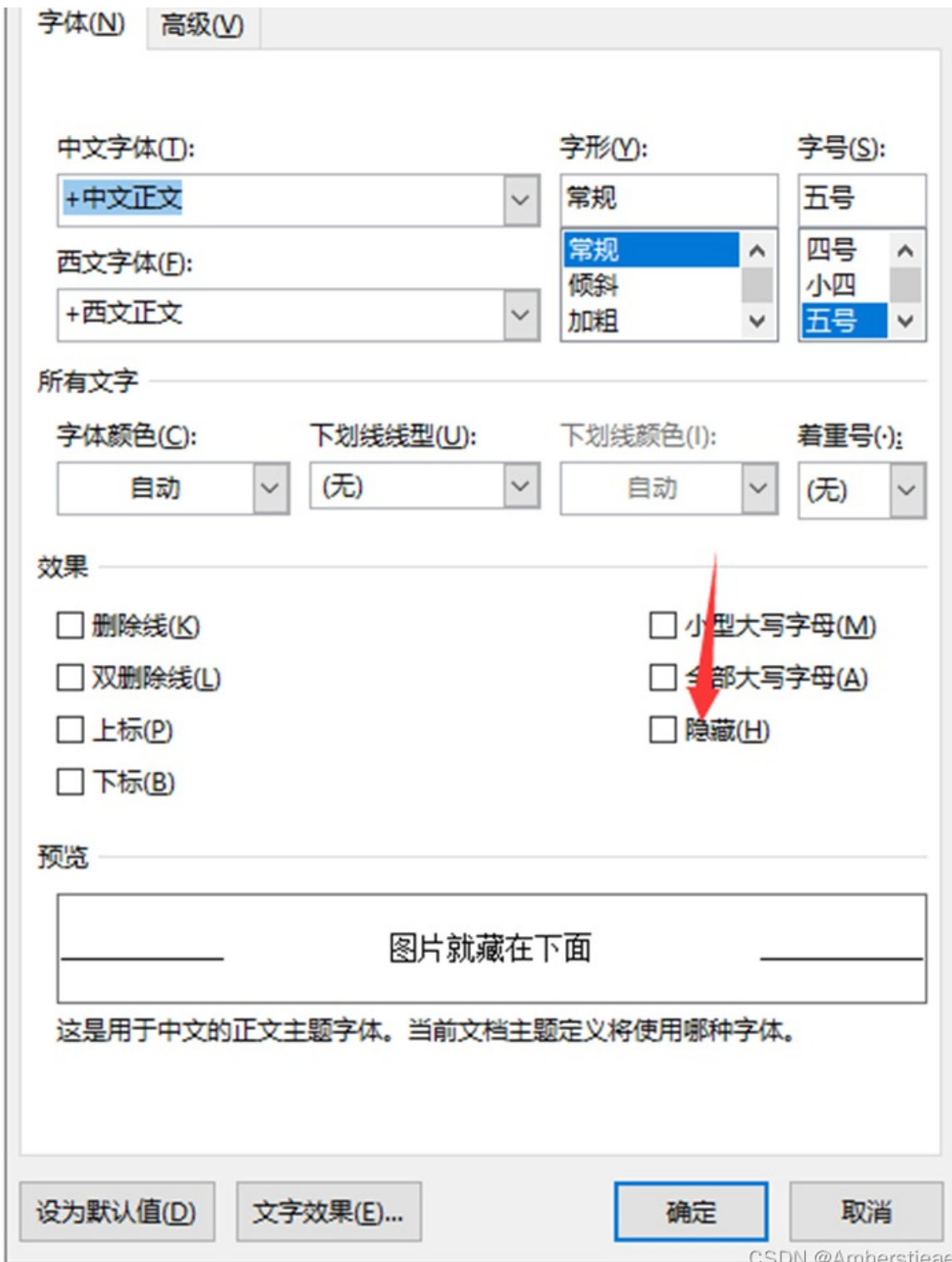
下载文件附件名称为docx, 那么一般文件就是一个文档, 修改名称为1.docx即可看见里面正文, 如下



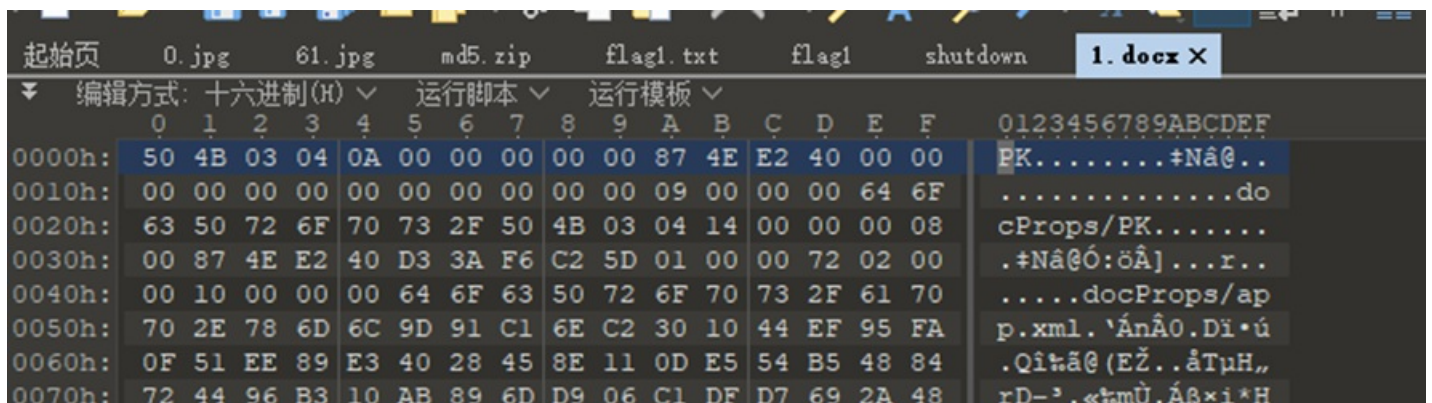
对于docx文档有一个字体隐藏, 或者是文字被改成了白色, 如果有段落起止符的话可以根据这个来看, 没有的话先大体看一下文字&隐藏文字

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



0080h:	AF BD ED CC	CA E3 A7 1D	32 BF B4 4D	70 06 63 85	~iîÊã\$.2¿`Mp.c...
0090h:	92 79 88 E3	24 0C 40 72	55 09 79 CC	C3 6D B9 8A	'y`ã\$.@rU.yîÅm²Š
00A0h:	A6 61 60 1D	93 15 6B 94	84 3C BC 82	0D E7 F4 F1	!a`."k"„<¼,.çôñ
00B0h:	81 AC 8D D2	60 9C 00 1B	F8 08 69 F3	B0 76 4E CF	.-..Ò`œ..ø.ió°vNĪ
00C0h:	10 B2 BC 86	96 D9 D8 AF	A5 DF 1C 94	69 99 F3 D2	.²¼t-ÛØ`¥B."i"óÒ
00D0h:	1C 91 3A 1C	04 87 A5 E2	A7 16 A4 43	69 92 4C 10	.':..#¥ã\$.#Ci'L.
00E0h:	5C 1C C8 0A	AA 48 DF 02	C3 3E 71 76	76 FF 0D AD	\.È.²HB.Ã>qvvÿ.-
00F0h:	14 EF F8 EC	67 79 D5 1E	98 92 12 5A	DD 30 07 F4	.iøigyÖ.~'.ZÝ0.ó
0100h:	BD C3 69 E2	4A B9 96 A0	9B 4B D6 EC	08 96 62 82	¾ÃiâJ²- >KÖi.-b,
0110h:	FA 81 EC 94	A9 2C 4D 08	EA 07 52 D4	CC 30 EE FC	ú.ì"©,M.ê.RÔİ0iü
0120h:	9D 3A 73 A0	C8 9B 90 FE	A5 37 FB C1	27 19 76 34	.:s È>.p¥7ûÁ'.v4
0130h:	4C D7 3F E6	40 91 52 39	D6 94 A2 05	8A FD 47 77	Lx?æ@`R9Ö"°c.ŠÿGw
0140h:	45 36 9C 35	50 78 5E 7A	60 8D 05 82	EE 46 17 FF	E6æ5Px^z`..,îF.ÿ
0150h:	65 B7 BA 54	CB 8E FE 77	FF D7 1C C0	ED 84 AB 37	e·°TEŽpwÿ×.Àí„«7
0160h:	9A F1 9E E8	8E 39 F0 C9	42 EB 46 70	E6 7C E1 74	šñžèŽ9ðÉBëFpæ át
0170h:	B7 DE 04 1F	3F A5 EC 31	8E 7D FB 31	C6 A3 49 B6	·P..?¥i1ž}ûlÆI¶
0180h:	5F E1 D7 51	FA F4 52 44	E9 E4 B9 88	C6 A3 AC 8A	_á×QúôRDéá²^Æ£-Š
0190h:	16 38 4B A3	24 2B B2 71	32 4D 92 B4	58 10 34 4C	.8K£\$+°q2M'`X.4L
01A0h:	22 BE D5 0D	F0 93 11 EE	DA 5D 63 28	FD 55 6F DD	"%Ö.ð".îÚ]c(ÿUoÝ
01B0h:	D2 6F 50 4B	03 04 14 00	00 00 08 00	87 4E E2 40	ÒoPK.....#Nâ@
01C0h:	A7 3B 63 BB	56 01 00 00	7F 02 00 00	11 00 00 00	\$;c»V.....
01D0h:	64 6F 63 50	72 6F 70 73	2F 63 6F 72	65 2E 78 6D	docProps/core.xml
01E0h:	6C 8D 92 4D	4E C3 30 10	85 F7 48 DC	21 F2 3E 71	l.'MNÃ0.....÷HÛ!ò>q
01F0h:	92 FE 80 AC	24 95 00 75	45 25 24 8A	40 EC 2C 7B	'p€-\$.·.uE%\$Š@ì,{
0200h:	DA 5A C4 8E	65 9B FE 5C	83 3D 0B 8E	D0 0B 70 1B	ÚZÄže>p\ f=.žĐ.p.
0210h:	16 DC 02 27	4D 43 10 2C	58 8E DF 9B	6F 9E ED C9	.Û.'MC.,XžB>ožíÉ
0220h:	26 5B 59 06	6B 30 56 54	2A 47 49 14	A3 00 14 AB	&[Y.kOVT*GI.£..«
0230h:	B8 50 CB 1C	DD CD A7 E1	39 0A AC A3	8A D3 B2 52	,PÈ.ÝÍŠá9.-£ŠÓ°R
0240h:	90 A3 1D 58	34 29 4E 4F	32 A6 09 AB	0C DC 98 4A	.£.X4)NO2! .«.Û~J
0250h:	83 71 02 6C	E0 49 CA 12	A6 73 B4 72	4E 13 8C 2D	fq.làIÈ.¡s`rN.€-
0260h:	5B 81 A4 36	F2 0E E5 C5	45 65 24 75	BE 34 4B AC	[.²6ò.ãÅEe\$u%4K~
0270h:	29 7B A2 4B	C0 69 1C 8F	B1 04 47 39	75 14 D7 C0) {cKÀi..±.G9u.×À
0280h:	50 77 44 D4	22 39 EB 90	FA D9 94 0D	80 33 0C 25	PwDÔ"9ë.úÛ" €3.š
0290h:	-- -- -- --	-- -- -- --	-- -- -- --	-- -- -- --	---â^--- CSDN @Amherstieae

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

```
0 10 20 30 40 50 60 70 80 90 100 110
1 Execute(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)&chr(2+4797))|
vbscript|
```

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

题目名字为维吉尼亚，那么应该就是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>

Input

Cipher Text:

```
lui hndkq fesnr xbb anhxy sii 13 psmc uhba. nmfxfvq
glv ydzyx jicp-vbglfzvziq hvwuemgmdwt ss e gsdlecicihigmt
gaclvk riy jbvdydnxvw wg ribr selgmjmv irfrvkm seslgy 1467
ith hwh s ziktg kotuui hafg kh neoxpl siljivg xqvlrv
rphuesxoa. gpoiixa'f wploms sapp wovxtazl gpclrfwgw ryomx
wrzvvsy afkya, grq wnmplvl rmxv vrumunxvw wg cvvxzry glv
ezbie sw xzr gfkmytbrumft ecicihig me xzr gziomxxrbk.
psgii, bi 1508, rulnreik gvzmcmsmhw, zr zvw nhms
vsymxvsczlz, dvbiavh lui ktwore eitxs, n gibogley gfqhbrvgo
wl xui mmvrrèix xqvlrv. klw gvzmcmsmhw tmhuui. aiekzrv. frdl
```

Cipher Variant:

Language:

Key Length:
(e.g. 8 or a range e.g. 6-10)

Result

Clear text [\[hide\]](#)

Clear text using key "snertvigenere":

```
letters a to z (in shifted order). although there are 26 key rows
shown, a code will use only as many keys (different alphabets) as
there are unique letters in the key string, here just 5 keys: {l,
e, m, o, n}. snert, '{' and 'welcometosnertvigenere' and '}' for
successive letters of the message, successive letters of the key
string will be taken and each message letter enciphered by using
its corresponding key row. the next letter of the key is chosen,
and that row is gone along to find the column heading that matches
the message character. the letter at the intersection of [key-row,
msg-col] is the enciphered letter.
```

Details [\[show\]](#)

CSDN @Amherstieae

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
313833667a33333634786564373567363461396d663536323470646132343231656465656471
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']  
  

```

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()
```

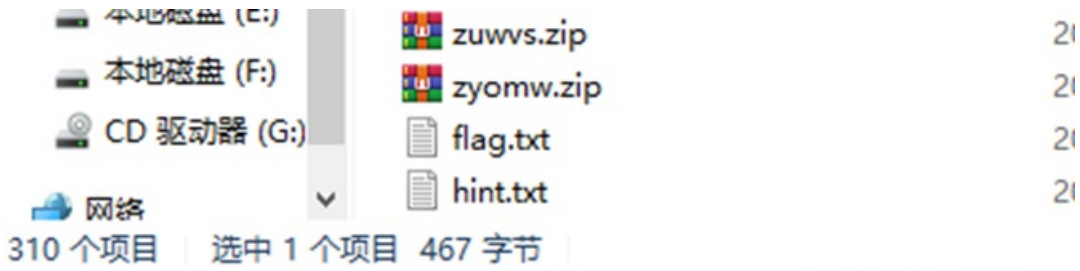
```
 except:
```

```
 break
```

```
 if(len(tag)>6):
```

```
 os.system("rm "+tag)
```

```
 orginal_zip=password+".zip"
```



CSDN @Amherstieae

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

嚟猫抡彤挺籍茂恫正舸阡恫抡虬衷茂伶抡伶皓节阡圪抡启启奴启皓启阡适伶纛舸纛皓伶谨=

就...直接千千秀字

<https://www.qqxiuzi.cn/bianma/wenbenjiami.php>

嚟猫抡彤挺籍茂恫正舸阡恫抡虬衷茂伶抡伶皓节阡圪抡启启奴启皓启阡适伶纛舸纛皓伶谨=

使用密码

snert {965b76e2890e03c7feddad3d7104b430}

CSDN @Amherstieae

高领大人



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





```

0500h: 31 68 54 00 00 53 30 64 0f 34 95 07 77 86 11 00 7e7115-d14* wt...
05c0h: 86 77 09 00 00 88 17 93 46 37 c5 c3 97 9f 00 07 7e6117-77AA-Ye+
05d0h: A1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11111111-1111h...
05e0h: 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11111111-1111A11...
05f0h: 57 58 43 00 00 0f 43 0c 10 00 00 0c 74 12 00 00 0*011c,c.110e.11
0600h: 53 61 03 00 00 9c 0a 01 4c 00 00 45 93 12 00 00 0a.11a.111k".11
0610h: 73 26 98 00 00 78 75 10 87 00 00 62 c4 12 00 00 04811e0.111bA.11
0620h: 3c 00 76 00 00 36 8a 18 53 00 00 38 08 63 00 00 00011b5.1110e11
0630h: f0 88 a0 00 00 29 c7 21 8c 00 00 58 01 81 00 00 y" 11)C10110A.11
0640h: 02 83 83 00 00 00 00 26 42 00 00 03 0d 48 00 00 0f11110110.111
0650h: 01 00 21 12 00 00 72 50 7a 00 00 87 6c 00 00 00 0.111P11111111
0660h: 9a 10 aa 10 43 6c 65 26 07 9c 98 3d c2 f0 5f 9f 0.11e1e"~Ad_
0670h: 00 a1 81 1a 00 04 c6 80 c6 92 05 61 07 a2 87 f1 0;11.11000.110110
0680h: a5 12 31 00 00 12 31 18 65 a7 40 08 00 00 62 28 0.111.1100111b1
0690h: 01 00 00 00 00 00 00 12 88 1c 12 31 00 00 64 16 11111111.1111d.
06a0h: 94 00 00 00 00 00 00 1a 75 65 23 00 00 ca 00 03 11111111.00111011
06b0h: 4c a0 a1 00 00 0f 32 04 62 12 32 00 00 00 17 a8 1a"11.2"b.211".
06c0h: a7 59 c6 00 00 06 27 65 72 13 13 00 00 87 83 24 0Y111111"0e.111f5
06d0h: 0f 11 03 00 00 70 61 56 09 13 11 00 00 c7 32 13 .11110aV0.1112.
06e0h: c0 4a 8f 00 00 08 18 46 66 31 00 00 c0 8f c0 92 1a.11.11111A.A'
06f0h: 34 49 a1 00 00 00 00 86 fa 12 00 00 32 04 06 f3 415111110.11.00
0700h: 11 a0 09 11 00 00 09 78 86 31 23 00 00 02 20 a3 1.0.1111x1111011
0710h: 01 30 36 57 61 70 c6 a1 54 50 1a 00 00 a0 6f 94 ;00010;T1.11 0"
0720h: 20 64 7a 0f 46 f9 18 9c 25 0c 30 00 00 9c 38 2c f0x170.00.11100.
0730h: 05 03 00 89 00 3a c0 a3 01 62 04 00 00 11 2a 00 0.110:11.0.11.1.
0740h: 01 90 38 84 ac 26 40 34 82 80 a0 00 00 03 a5 31 0.11.1104.1110Y1
0750h: 0c c7 2f 61 60 09 ca 93 78 2a 10 30 00 00 5c 10 0c/ak06"p.1111\
0760h: c8 46 08 04 02 70 01 84 72 10 c9 3c 00 00 10 c9 0r.11.11.0011.8
0770h: 41 47 84 04 00 08 59 49 73 8c 03 00 f1 32 48 05 00.0MY1ac00000p
0780h: 59 f6 74 a0 65 02 6c 34 41 c1 08 70 ca 30 00 24 0ot.0114AA.110000
0790h: 00 02 c8 08 09 f7 43 05 04 19 f0 9c f4 40 fa 28 1.R.0yc.11.1100001
07a0h: 02 f6 43 60 0f 00 94 00 57 90 a0 2a ca 30 55 40 f00000"00e"8;0R
07b0h: 68 00 a0 40 77 33 00 77 14 04 00 c0 c1 88 a0 c2 0f0003.w."c1A"-A
07c0h: 11 02 05 43 85 89 72 2f 84 33 00 09 0d 40 10 21 110C.11r/1.11AM.1
07d0h: 80 37 44 39 03 04 89 41 2c 0f aa 85 c7 18 c0 3a 1.7000"0A.0"0.11
07e0h: 50 c0 29 07 70 87 a8 75 41 05 78 00 4f 39 86 93 11)011"0A000911"
07f0h: 60 10 c0 30 5f 44 40 6a 01 18 04 36 06 0f 00 00 0e.11-0K11.01a.Y0
0800h: 14 03 a4 37 77 83 c0 04 58 a7 0c 65 61 f2 00 f1 1.11000"0.000Y0
0810h: 09 5c 13 68 78 00 05 01 a2 73 45 66 03 50 f9 40 0A.0x1.000K".1100
0820h: 04 04 f0 75 44 05 5f a7 14 00 00 f7 20 c6 04 48 f.0000"1100-000
0830h: 65 02 c8 95 a4 c7 90 c9 03 c0 09 1c 06 00 63 0f 00000C.0A10.0000
0840h: 83 78 0c 68 27 f4 78 04 0a 55 8f 00 43 f6 2f 45 f000"00a.0.000/0
0850h: 0c 18 00 77 00 26 31 92 43 8a a1 f6 76 35 31 c8 0.Y0011"00;0v01R
0860h: 03 00 50 18 48 07 00 56 38 f6 10 c0 20 20 40 00 11.1100V0.11 0A
0870h: 64 a2 c7 3c 84 08 28 22 17 4c 4a c3 0a 37 90 80 00000a.110A"7.0

```

模板结果 - GIF.bt

```

名称
> struct GIFHEADER GifHeader
> struct LOGICALSCREENDESRIPTOR LogicalScreenDescriptor
> struct GLOBALCOLORTABLE GlobalColorTable
> struct DATA Data
. . .

```

查找结果

地址	内容
已找到 136 个 'eeee'.	
394h	eeee
3A3h	eeee
3ABh	eeee

输出 查找结果 多文件中查找 比较 直方图 CSDN @Amherstieae

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

```

kali@kali:~/Desktop/1$ zsteg -a ctf1.png
imagedata .. text: "!\"\\\"*.0\n\r"
b2,r,lsb,xy .. text: "GC?^bF~2"
b2,rgb,lsb,xy .. text: "https://pan.baidu.com/s/1CVBQ9X9eOzHG_VX_MQfIuw6"
b4,r,lsb,xy .. text: "#DUUUUDUT3\"
b4,g,lsb,xy .. text: "uuEVTHIEfEulbdlfuufffffy"

```

根据出题人提示，去掉最后一位

[https://pan.baidu.com/s/1CVBQ9X9eOzHG\\_VX\\_MQflw](https://pan.baidu.com/s/1CVBQ9X9eOzHG_VX_MQflw)

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



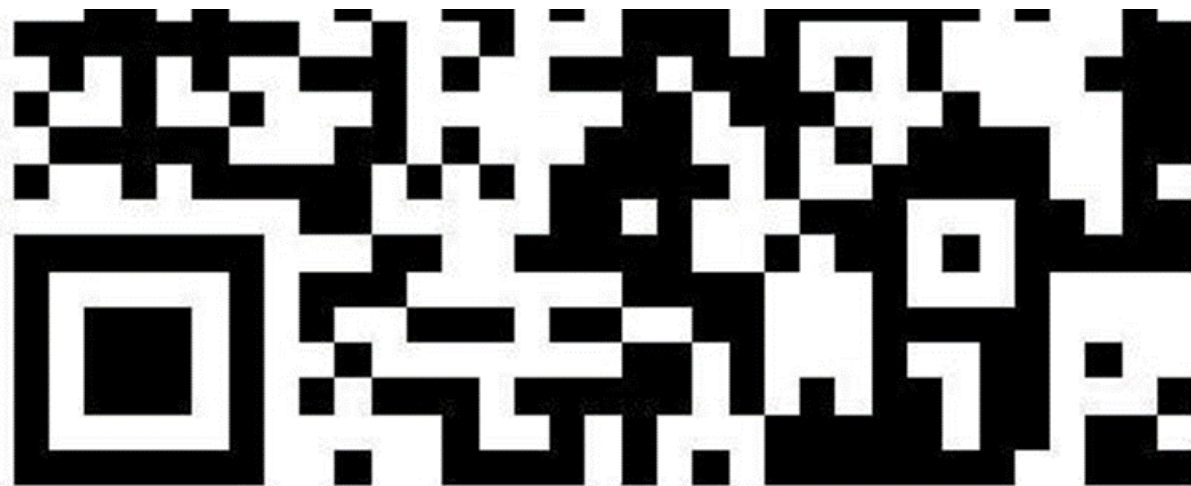
The screenshot shows the website's interface for merging images. At the top, there are navigation links for various categories like '生物科学', '乱七八糟', etc. The main area features a 'filesmerge' logo and a navigation menu with options like '合并成JPG', '合并成PDF', etc. Below this, there are input fields for '输入格式' (JPG, JPEG, PNG, GIF, BMP) and '输出格式' (JPG, PNG, GIF, BMP). A central box prompts the user to '选择本地文件' or '拖动文件到这里'. There is also a '文件URL' field and a '添加文件' button. A table lists 14 files with their names and actions (Up, Down, Delete). On the right, there is an advertisement for 'NEGOCIOS INTERNACIONALES' and a section titled '如何在线合并文件' with a 5-step guide. A 'Tags' section lists various merge options like '合并成JPG', '合并成Word', etc. A watermark 'CSDN @Amherstieae' is visible in the bottom right corner of the screenshot.

顺序	文件 ^ v	排序&操作
1	20223132212371461_1.png	Up Down Delete
2	20223132212371461_100.png	Up Down Delete
3	20223132212371461_10.png	Up Down Delete
4	20223132212371461_11.png	Up Down Delete
5	20223132212371461_12.png	Up Down Delete
6	20223132212371461_13.png	Up Down Delete
7	20223132212371461_14.png	Up Down Delete
8	20223132212371461_15.png	Up Down Delete
9	20223132212371461_16.png	Up Down Delete
10	20223132212371461_17.png	Up Down Delete
11	20223132212371461_4.png	Up Down Delete
12	20223132212371461_2.png	Up Down Delete
13	20223132212371461_18.png	Up Down Delete
14	20223132212371461_19.png	Up Down Delete

但这个网站不能拼太多，所以分两半拼出来就行了

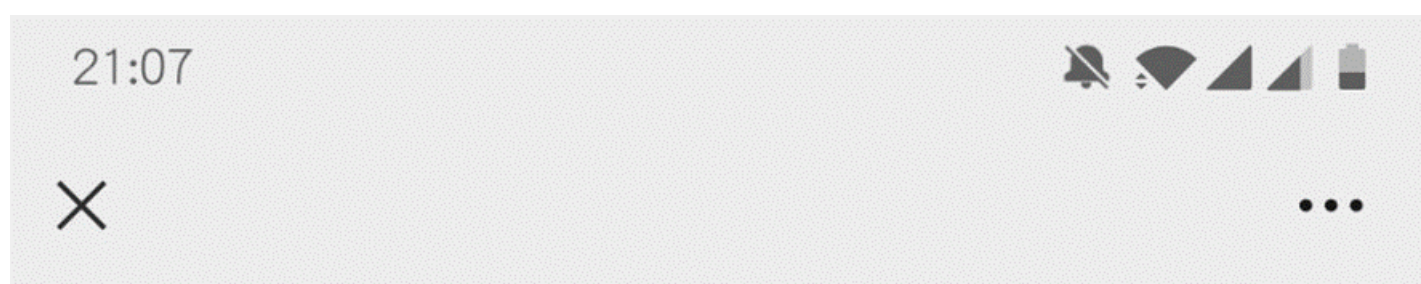






CSDN @Amherstieae

snert{jianjiandandan\_snert}



snert{jianjiandandan\_snert}

CSDN @Amherstieae

简单题





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":"", "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":"", "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>"}

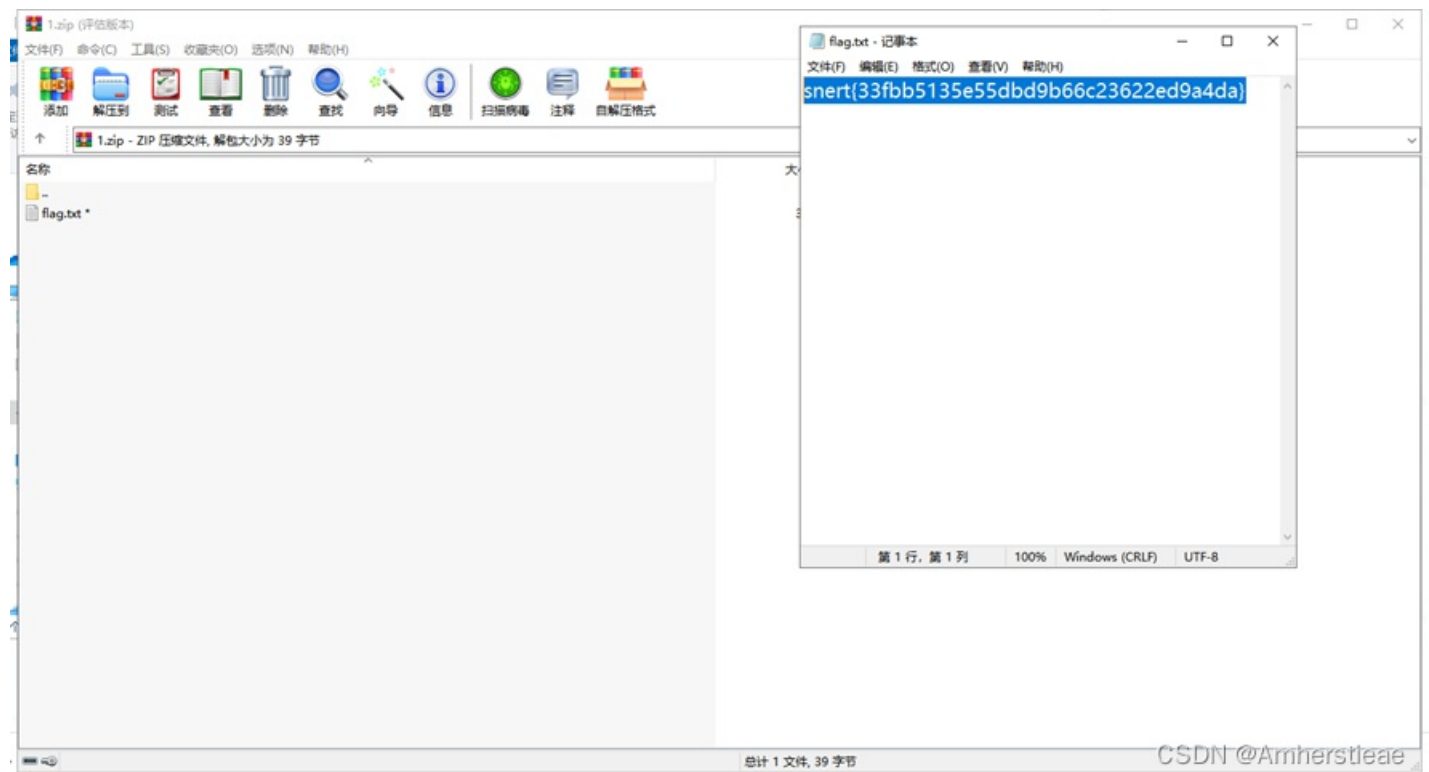
nums = []
keys = open('1.txt')
for line in keys:
 if len(line)!=17: #首先过滤掉鼠标等其他设备的USB流量
 continue
 nums.append(line[0:2]+line[4:6]) #取一、三字节
keys.close()
output = ""
for n in nums:
 if n[2:4] == "00" :
 continue

 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 ❀❀ 丶(°▽°)ノ ❀