CTFshow-Misc（部分wp）

原创

i_kei 于 2021-01-31 22:19:30 发布 2470 收藏 11

分类专栏： CTFshow 文章标签： 信息安全 加密解密 zip base64 密码学

本文链接：https://blog.csdn.net/i_kei/article/details/113465825

因为太菜了，所以更新比较慢，会慢慢边复现边写wp，flag打码是想让看我博客的小伙伴们能够自己独立复现一遍而不是照抄flag，有错误的地方还请师傅们不吝指教

目录

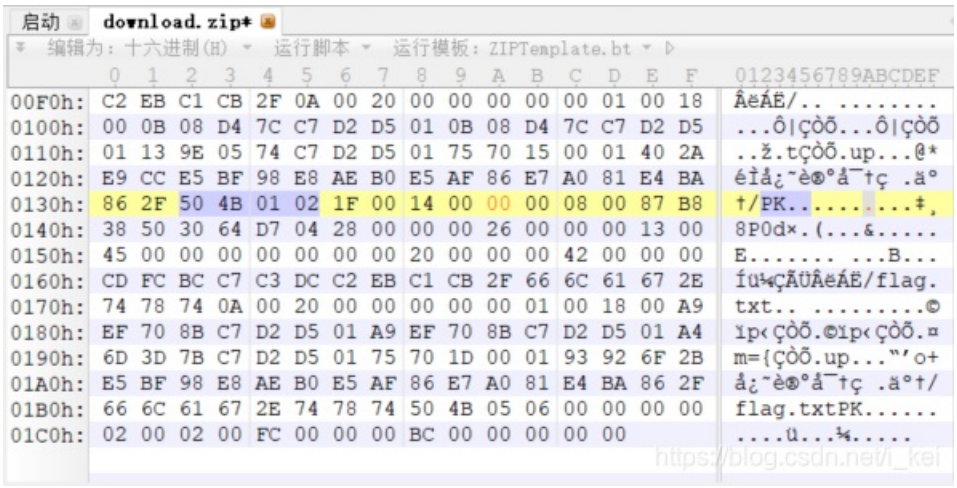
杂项签到

用ZipCenOp.jar可以解zip压缩包伪加密

```
┌──(root㉿kali)-[~/tools/misc]
└─# java -jar ZipCenOp.jar r download.zip
```

再次解压压缩包就不提示要输入密码了，打开flag.txt即可获得flag

用010将图中09改为00也可以达到同样效果



misc2

新建一个虚拟机，然后添加一个软盘，设置成如图所示

然后开启虚拟机即可看到flag

miscx

打开压缩包发现注释的提示，和没加密的misc1.zip

打开misc1.zip，解压出没加密的misc.png

打开misc.png，没发现什么，难道压缩包密码就是2020

试一下果然是，太良心了（不像牛年大吉藏在图片文件头那么狗）
打开word，发现一串音乐符号加密

```
♭ ‖ ♭ ‖ ‖♯ ♭ ♭ ♬ ‖ ♩ ♬‖♬ 𝄞 ♭ ♭ ¶ ♭ ‖♯‖¶ ♭ ♭ ‖ 𝄞 ‖‖ ♭ ‖§ ♭ ‖♬♪ ♭ ♯§‖‖♯‖‖♬ ‖‖♪‖‖♪‖¶§‖‖♬ ♭ ♯‖ ♭ ♯♪‖‖ 𝄞 ‖♬§ ♭ ‖‖‖ ♩ ♪‖‖♬ ♭ ♭ ♬‖ ♩ ♪‖ ♩ ¶‖
♩ ♪‖ ♩ ♬‖¶§‖‖ ♩ ‖¶♫♭ ♭ ♩ ‖♬♯‖♬§ ♭ ‖ ♭ ‖ ♩ ¶‖‖ 𝄞 ♭ ♭ ♬‖‖ ♭ ‖♫§‖¶♫‖ ♩ 𝄞 ♭ ♭ §‖ ♭ §‖ ♭ §§=
```

音乐符号解密

文本加密为音乐符号

♭ ‖ ♭ ‖ ‖ ♯♭♭♬ ‖ ♩♫ ‖ ♬ 𝄞 ♭♭¶♭ ‖ ♯ ‖ ¶♭♭ ‖ 𝄞 ‖ ‖ ♭ ‖ § ♭ ‖ ♬♪♭♯§ ‖ ‖ ♯ ‖ ‖ ♬ ‖ ‖ ♪ ‖ ‖ ♪ ‖ ¶§ ‖ ‖ ♬♭♯ ‖ ♭♯♪ ‖ ‖ 𝄞 ‖ ♬ § ♭ ‖ ‖ ‖ ♩♪ ‖ ‖
♬♭♭♬ ‖ ♪♪ ‖ ♩¶ ‖ ♪♪ ‖ ♩♬ ‖ ¶§ ‖ ‖ ♩ ‖ ¶♫♭♭♩ ‖ ♬♯ ‖ ♬ § ♭ ‖ ♭ ‖ ♩¶ ‖ ‖ 𝄞 ♭♭♬ ‖ ‖ ♭ ‖ ♫ § ‖ ¶♫ ‖ ♩ 𝄞 ♭♭ § ‖ ♭ § ‖ ♭ § § =

加密 解密 使用密码

U2FsdGVkX1/eK2855m8HM4cTq8Fquqtm6QDbcUu4F1yQpA==

Rabbit解密，密钥为2020，解出misc2的压缩包密码

在线Rabbit算法加密解密工具

U2FsdGVkX1/eK2855m8HM4cTq8Fquqtm6QDbcUu4F1yQpA==

2020

Rabbit加密 Rabbit解密 清空输入框 复制结果文本

welcome_to_payhelp

解出hint.txt

hint.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

VmpKMFUxTXhXWGxVV0dob1RUSjRVVll3V2t0aFJscDBZMGhLYTAxWGVIaFZiRkpUWWtaYVZWSnJXbFpOVjJoeVZYcEdZVkpzVG5KVWJHaHB
Wa1ZWZDFkV1ZtRmtNRFZYVjJ4c2FWSlVWbFJVVnpWdVRXeFZlV1ZHVGxSaVZrWTBXVlJPYzFWR1pFZFRiVGxYWW01Q1dGcEdXbE5UUjBZMlV
XMTBWMWRGU2xkV1ZtUXdVekpGZUZOWWJHaFRSVFZWV1d0YVMxTXhjRVZUYTFwc1ZteHdlRlp0ZERCV01VcFlaRE53V0Zac2NIWldSekZMV
W1zeFdWSnNTbWxXUjNodlZtMXdUMkl5Vm5OaVNGWnBVbXh3YzFac1VrZFNiRlY0WVVkMFZXSlZXbmxWYlRWUFZsWlplbEZyWkZSaVJrcFFW
V3hGYkUwd1VXeE5NRkVsTTBRJTNE

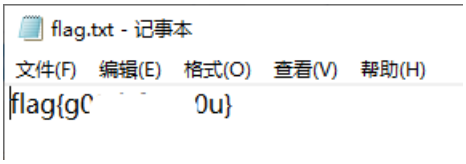
连续进行base64解码

```
welcome_to_2020%0Aflag%20is%20coming...%0Athe%20key%20is%20hello%202020%217
```

url解码会好看一些

压缩包密码时hello 2020!

解压得到flag.txt



misc50

将图片foremost分离出压缩包和另一张图片
用zsteg一把梭得到base64编码字符串

```
┌──(root㉿kali)-[~/test/output/png]
└─# zsteg 00000000.png
meta Software       .. text: "gnome-screenshot"
meta Comment        .. text: "Sk5DVlM2Mk1NRjVIU1gyTk1GWEgyQ1E9Cg=="

┌──(root㉿kali)-[~/test/output/png]
└─# echo Sk5DVlM2Mk1NRjVIU1gyTk1GWEgyQ1E9Cg== | base64 -d                    1
 ㉿
JNCVS62MMF5HSX2NMFXH2CQ=


┌──(root㉿kali)-[~/test/output/png]
└─# echo JNCVS62MMF5HSX2NMFXH2CQ= | base32 -d
KEY{Lazy_Man}
```

解码得KEY{Lazy_Man}，提交不对，可能是后面需要用到得密钥

解压分离出来的压缩包，再打开fbi.rar得到flag.zip和注释中的提示

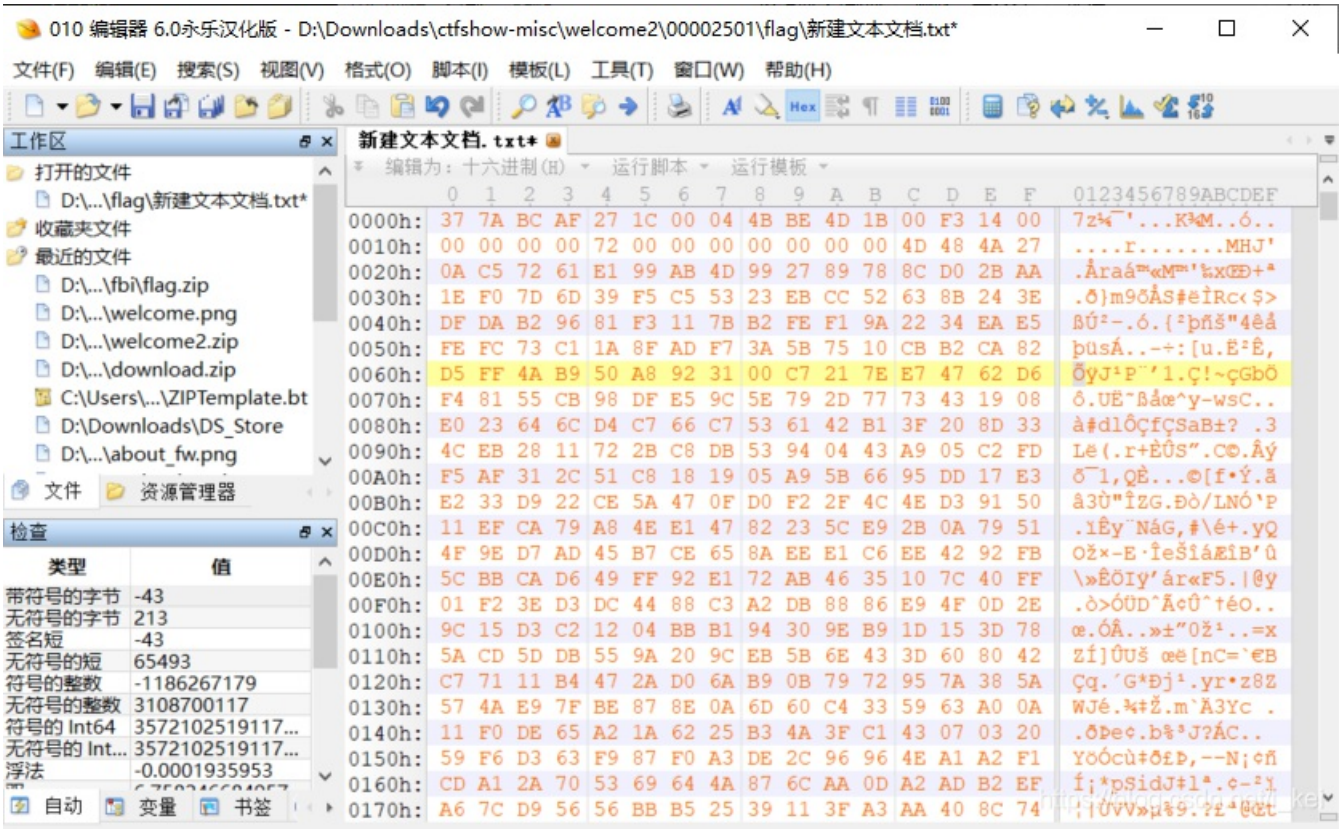

```
GEZDGNBVGYFA====
```

base32解密得到flag.zip压缩包密码为123456

得到thienc.txt，将其转换成16进制文本
附上大佬脚本：
https://blog.csdn.net/weixin_45940434/article/details/104292369

```
import re

def read_file(filepath):
    with open(filepath) as fp:
        content=fp.read();
    return content

number = read_file('thienc.txt')
result = []
result.append(re.findall(r'.{2}', number))
result = result[0]

strings =''
for i in result:
    y = bytearray.fromhex(i)
    z = str(y)
    z= re.findall("b'(.*?)'",z)[0]
    strings += z

b= strings.split('0x')

strings=''
for i in b:
    if len(i) ==1:
        i= '0' + i
    strings +=i

with open('result.txt', 'w') as f:
    f.write(strings)
    print("complete! ")
```

将得到的16进制文本填充的文件，后缀名改为.7z

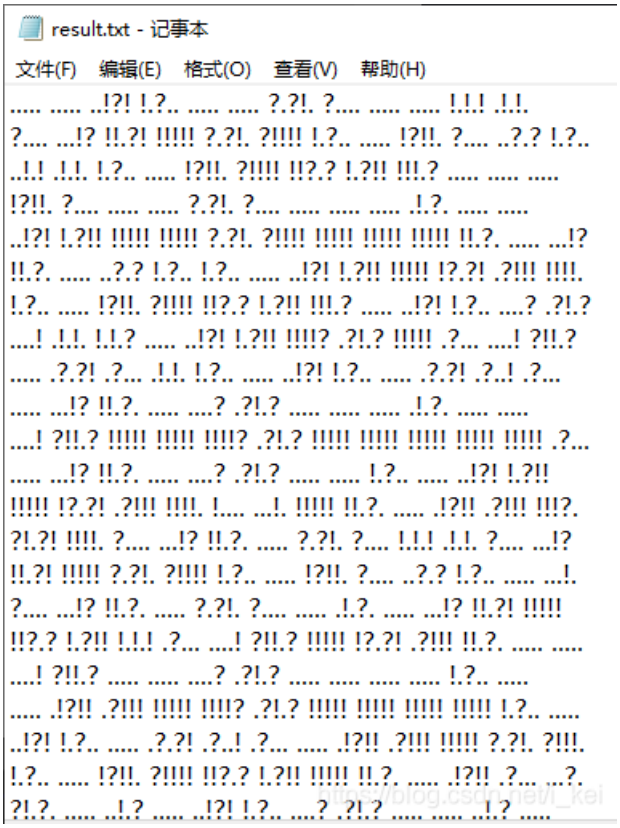


解压密码是刚刚的KEY{Lazy_Man}，得到secenc.txt

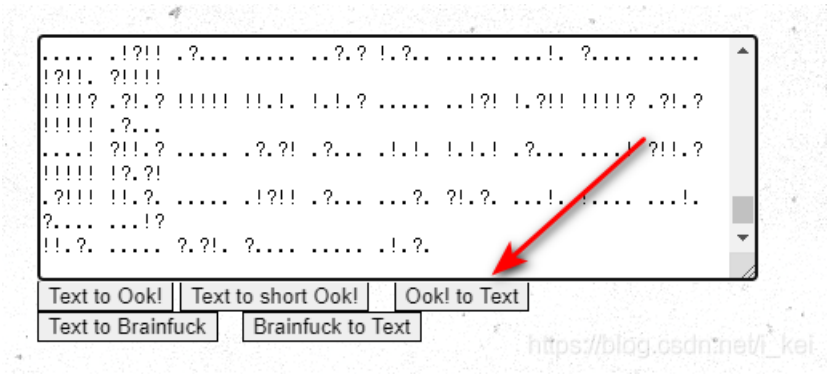
文本是base64和base32循环加密
附上Cheyenne大佬的代码，我自己改了一丢丢

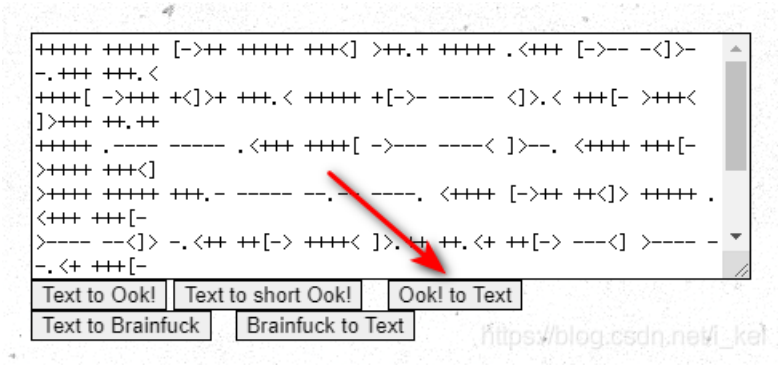
```python
# @Author: Cheyenne
import base64
import re

f = open('secenc.txt').read().encode('utf-8')

while True:
    if re.match('^[2-7A-Z=]+$', f.decode('utf-8')):
        f = base64.b32decode(f)
    elif re.match('^[0-9a-zA-Z+/=]+$', f.decode('utf-8')):
        f = base64.b64decode(f)
    else:
        print(f.decode('utf-8'))
        break

with open('result.txt', 'w', encoding='utf-8') as file:
    file.write(str(f,encoding='utf-8'))
print("Decryption complete!")
```

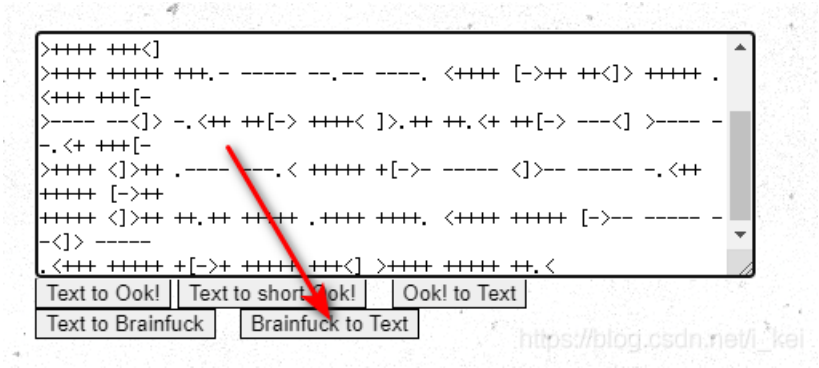
解出后进行Brainfuck解密



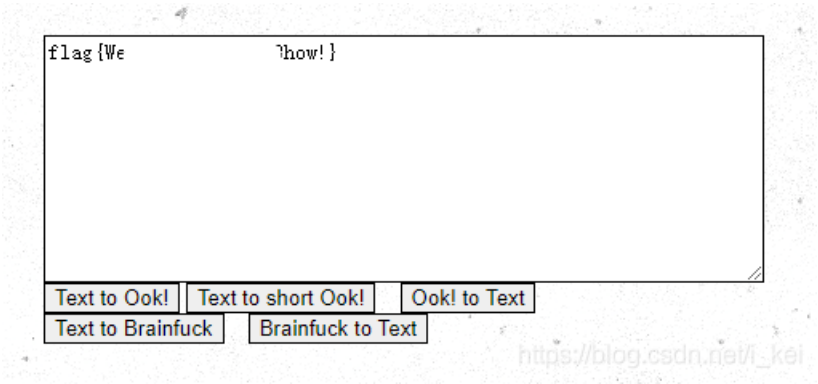
一步步解就好







得到flag



misc30

解压出一张图片，在备注中发现小星星

再次解压，密码为little stars，解压出一个doc文档
此地无银三百两，全选后将文字颜色设置为黑，发现另一个压缩包密码Hello friend!

这里什么都没有
里什么都没有
什么都没有
么都没有
都没有
没有
有

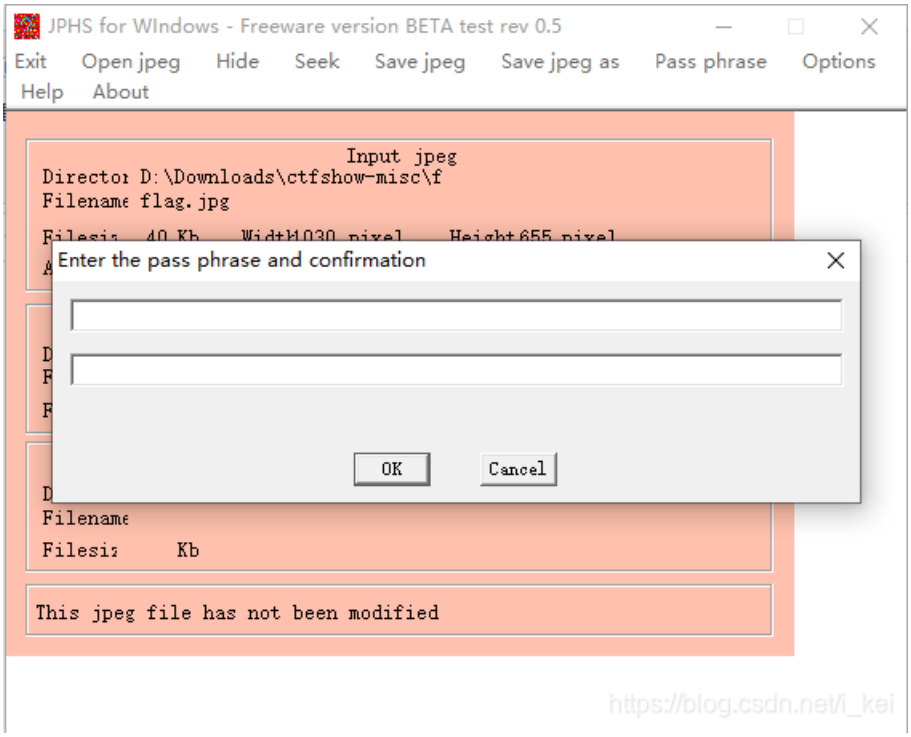
你知道梵高的星空吗？
Hello friend!

解压出一张二维码，扫描得flag

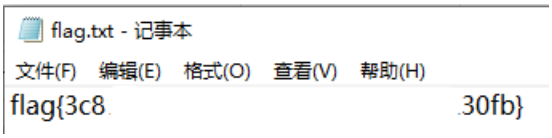

QR Research
文件(F) 工具(T) 帮助(H)
纠错等级
H(30%)
掩码
Auto
版本
Auto
Auto
尺寸
4
已解码数据 1:
位置:(58.0,29.8)-(280.4,29.8)-(57.8,252.4)-(280.5,252.7)
颜色正常,正像
版本:2
纠错等级:L,掩码:4
内容:
flag{v. w}
https://blog.csdn.net/i_kei

stega1

使用JPHS工具打开，点Seek，密码为空。



保存为flag.txt，打开即为flag



misc3

misc3

1

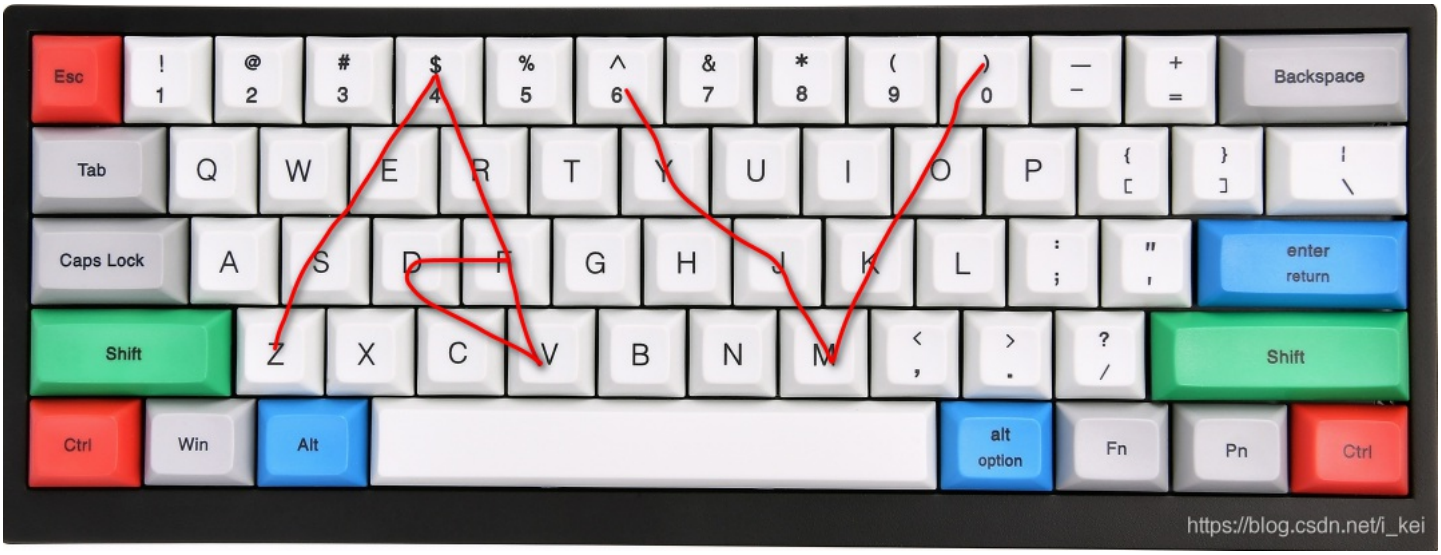
密文：zse4rfvsdf 6yjmko0

提示1：解密后两个字符,小写 提示2：看看自己下面

提交flag{明文}

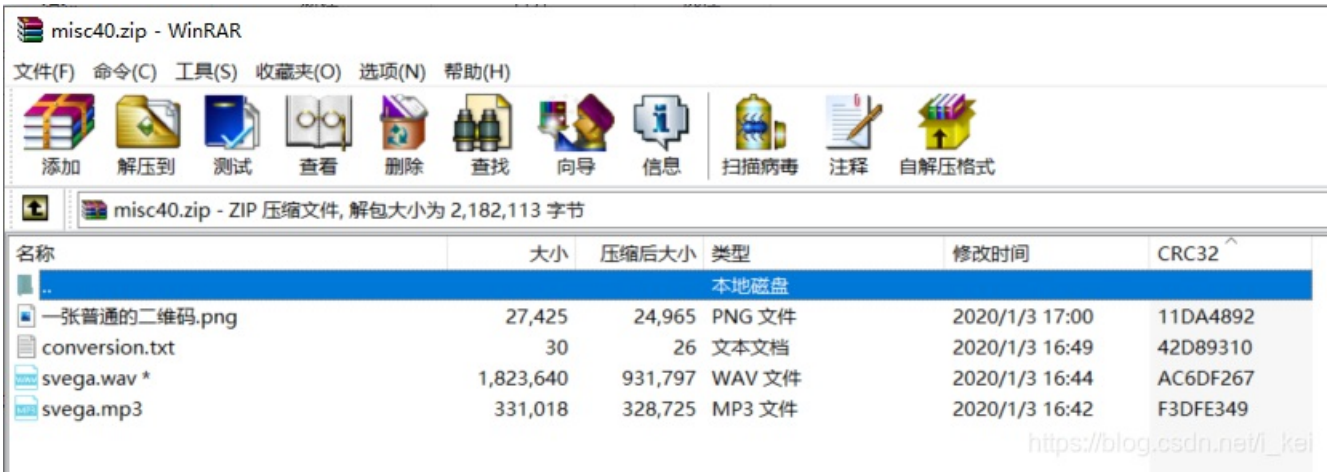
~~看自己下面可还行~~

按照提示依次连接键盘字母数字即可

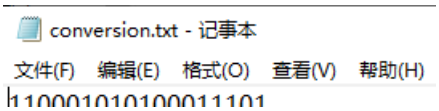


misc40

有三个文件未加密，依次查看



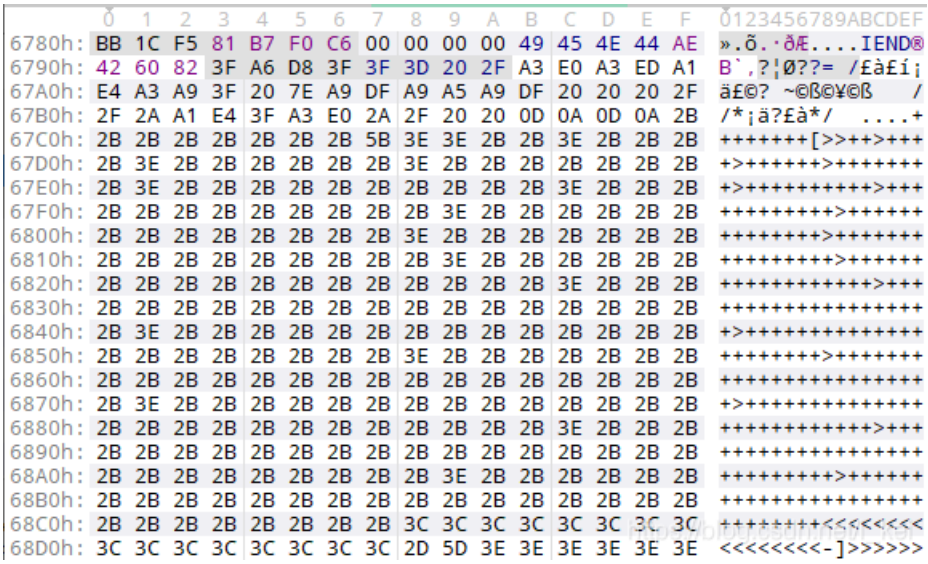
首先打开txt文件



2>4>8>10

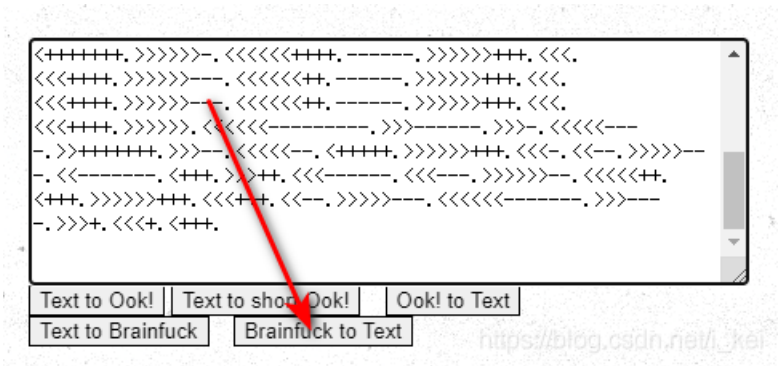
根据提示将字符串由二进制依次转到10进制，这里我们直接转，得到202013

用010打开图片，发现一段brainfuck，复制出来



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
6780h:	BB	1C	F5	81	B7	F0	C6	00	00	00	00	49	45	4E	44	AE	».õ.·ðÆ....IEND®
6790h:	42	60	82	3F	A6	D8	3F	3F	3D	20	2F	A3	E0	A3	ED	A1	B`‚?¦Ø?‡= /£à£í¡
67A0h:	E4	A3	A9	3F	20	7E	A9	DF	A9	A5	A9	DF	20	20	20	2F	ä£©? ~©ß©¥©ß /
67B0h:	2F	2A	A1	E4	3F	A3	E0	2A	2F	20	20	0D	0A	0D	0A	2B	/*¡ä?£à*/ ....+
67C0h:	2B	2B	2B	2B	2B	2B	2B	5B	3E	3E	2B	2B	3E	2B	2B	2B	+++++++[>>++>+++
67D0h:	2B	3E	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	+>++++++>+++++++
67E0h:	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	+>++++++++++>+++
67F0h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	+++++++++>++++++
6800h:	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	2B	++++++++>+++++++
6810h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	+++++++++>++++++
6820h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	++++++++++++>+++
6830h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	++++++++++++++++
6840h:	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	+>++++++++++++++
6850h:	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	2B	++++++++>+++++++
6860h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	++++++++++++++++
6870h:	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	+>++++++++++++++
6880h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	++++++++++++>+++
6890h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	++++++++++++++++
68A0h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	+++++++++>++++++
68B0h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	++++++++++++++++
68C0h:	2B	2B	2B	2B	2B	2B	2B	2B	3C	3C	3C	3C	3C	3C	3C	3C	++++++++<<<<<<<<
68D0h:	3C	3C	3C	3C	3C	3C	3C	3C	2D	5D	3E	3E	3E	3E	3E	3E	<<<<<<<<-]>>>>>>

brainfuck解密

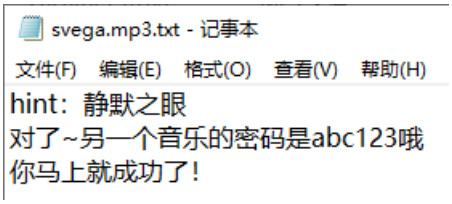


解出来一段核心价值观编码，解码得123456

使用MP3Stego解密

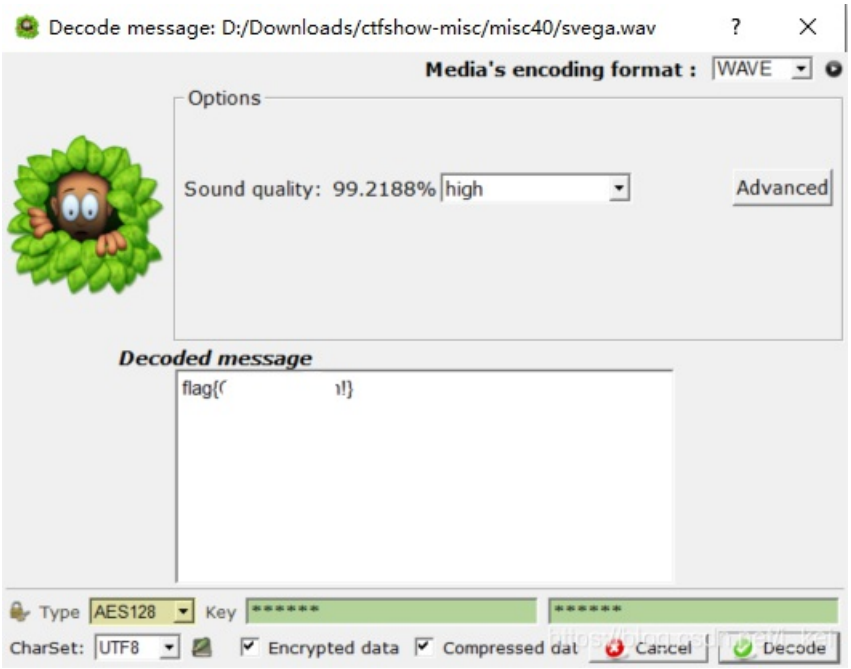
```
D:\Tools\Misc\MP3Stego_1_1_18\MP3Stego>Decode.exe -X -P 123456 svega.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'svega.mp3'  output file = 'svega.mp3.pcm'
Will attempt to extract hidden information. Output: svega.mp3.txt
the bit stream file svega.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame  791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega.mp3" is finished
The decoded PCM output file name is "svega.mp3.pcm"
```


得到svega.mp3.txt，打开得到hint



得到压缩包密码abc123，解压得svega.wav

根据提示静默之眼，就是使用SilentEye解密，Sound quality为high，type为AES128，Key为202013
点decode得到flag

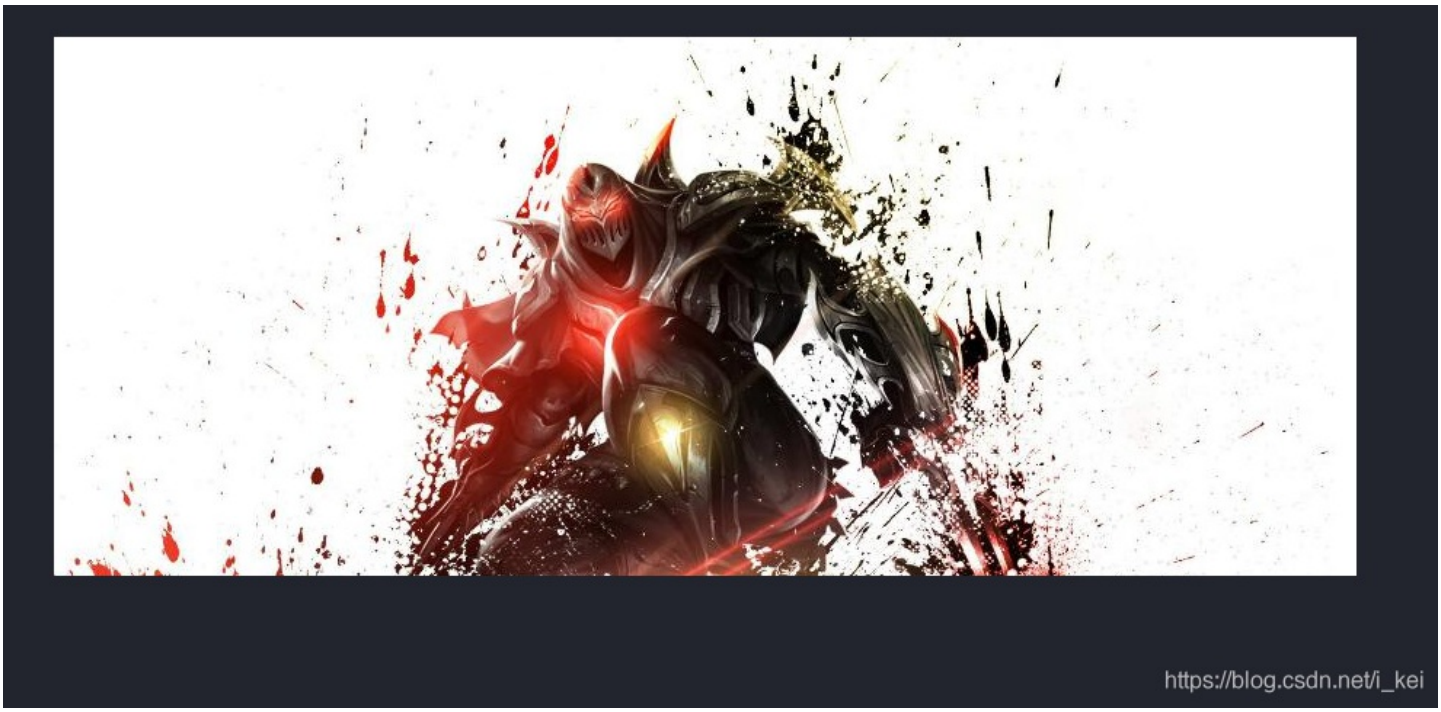


misc30

使用zipcenop解开zip伪加密

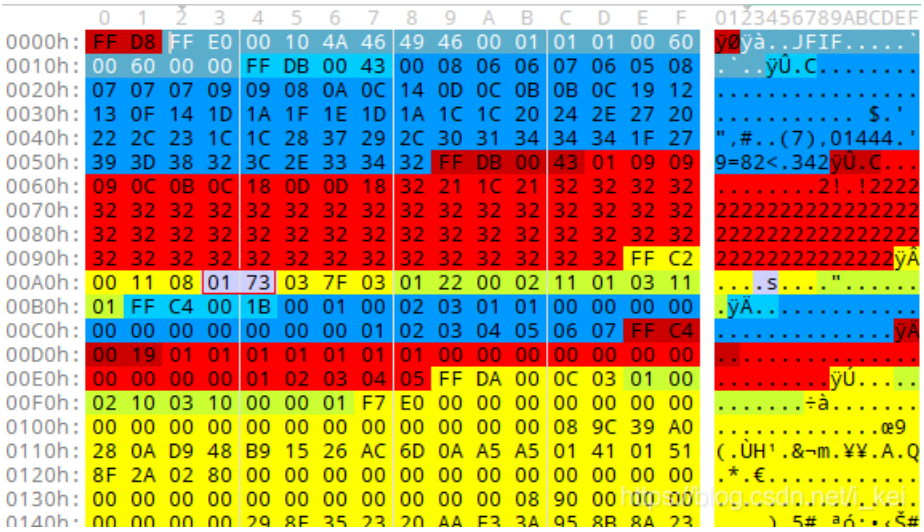
```
┌──(root㉿kali)-[~/tools/misc]
└─# java -jar zipcenop.jar r aihe.zip
```

解压得aihe.mp3
使用foremost分离出一张图片



很明显劫脚下肯定还隐藏着东西，需要恢复正确得宽高
查看图片属性，看到高度为371，宽度为895，分别将其由10进制转为16进制：0173、037f

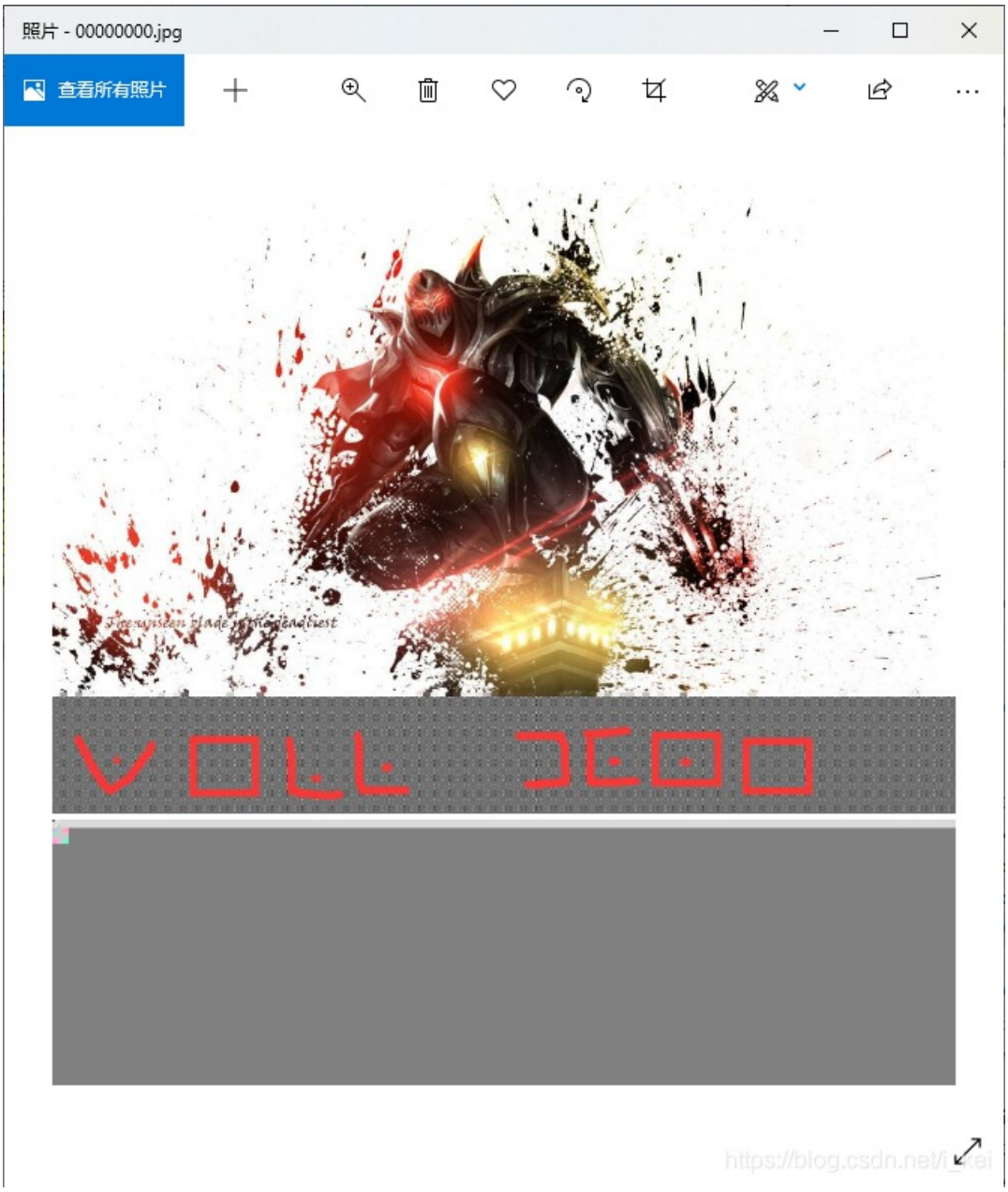
用010打开图片，ctrl+f搜索0173



将高度数值调高，例如和宽一样大

```
00C0h: 00 00 00 00 00 00 00 01 02 03 04 05 06 07 FF C4  ................ÿÄ
00D0h: 00 19 01 01 01 01 01 01 01 00 00 00 00 00 00 00  ................
00E0h: 00 00 00 00 01 02 03 04 05 FF DA 00 0C 03 01 00  .........ÿÚ.....
00F0h: 02 10 03 10 00 00 01 F7 E0 00 00 00 00 00 00 00  .......÷à.......
0100h: 00 00 00 00 00 00 00 00 00 00 00 00 08 9C 39 A0  ..............œ9
0110h: 28 0A D9 48 B9 15 26 AC 6D 0A A5 A5 01 41 01 51  (.ÙH¹.&¬m.¥¥.A.Q
0120h: 8F 2A 02 80 00 00 00 00 00 00 00 00 00 00 00 00  .*.€............
0130h: 00 00 00 00 00 00 00 00 00 00 00 00 08 90 00 00  ................
0140h: 00 00 00 00 29 8F 35 23 20 AA F3 3A 95 8B 8A 23  ....) 5# ªó:•‹Š#
```

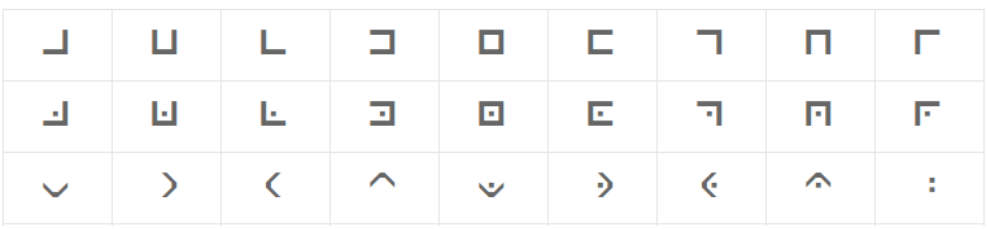
保存后打开图片，得到隐藏的猪圈密码

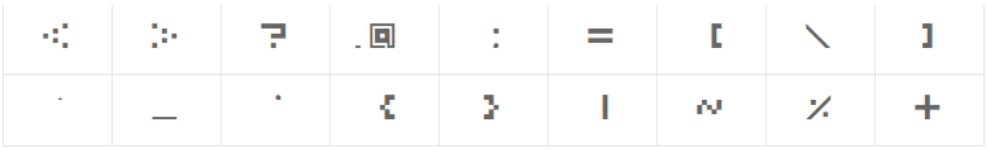


猪圈密码解密

猪圈密码

Pigpen Cipher





明文: welldone

解出来well done（有空格）

红包题第一弹