

BUUCTF misc 解题记录 二（超级详细）

原创

Vayn3 于 2021-04-14 23:40:02 发布 1441 收藏 10

分类专栏: [笔记](#) 文章标签: [安全](#) [python](#)

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/qq_51090016/article/details/115712647

版权



[笔记 专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

这里是从第四页开始的题目

[SUCTF2018]followme (kali下搜索整个文件夹)

蜘蛛侠呀 (tshark提取数据)

[RCTF2019]draw (logo解释器)

[MRCTF2020]不眠之夜 (montage和gaps)

[安淘杯 2019]easy misc (盲水印)

[MRCTF2020>Hello_misc

[BSidesSF2019]zippy (密码解压)

[ACTF新生赛2020]明文攻击(隐藏文件内容在010)

粽子的来历 (脑洞太大 ff修复 行间距问题)

派大星的烦恼 (倒过来的二进制)

[ACTF新生赛2020]music (对原文件进行异或)

[SCTF2019]电单车

hashcat(爆破ppt文件)

[UTCTF2020]zero (零宽度字符隐写)

[湖南省赛2019]Findme

真的很杂

voip (Wireshark抓取RTP包)

[MRCTF2020]pyFlag(拼接出来一个文件)

Business Planning Group (010搜索iend bpg图像格式)

[GWCTF2019]huyao (频域盲水印隐写)

[UTCTF2020]File Carving

[GUET-CTF2019]soul sipse (音频隐写)

[UTCTF2020]spectrogram (奇怪的操作)

[UTCTF2020]sstv(qsstv)

我爱Linux(Python Pickle序列化内容)

[SUCTF2018]followme (kali下搜索整个文件夹)

先导出http

再放到kali

kali下输入grep -r 'CTF' ./文件名/

```
aiji@kali2020:~/桌面$ grep -r 'CTF' ./文件夹名/...
./buu/login%3f%3d6975b9a9f7a359d322e06c0e28db112b(123):name=admin&password=S
CTF{password_is_not_weak}&referrer=http%3A%2F%2F192.168.128.145%2Fbuild%2Fad
min%2F
匹配到二进制文件 ./buu/attachment.pcapng
```

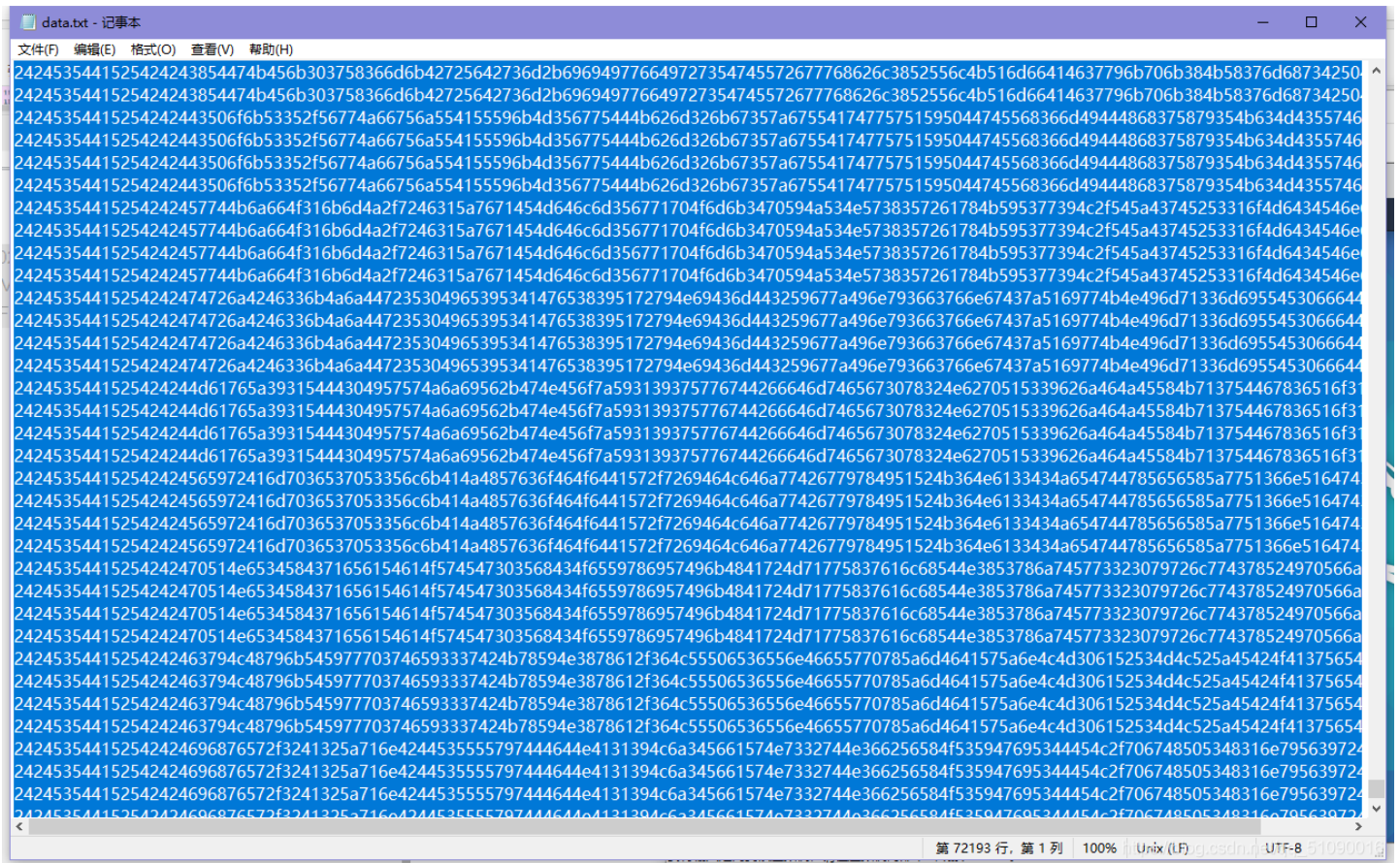
蜘蛛侠呀 (tshark提取数据)

所有的icmp包后面都跟了一串数据, 使用tshark把这些全部提取出来

The screenshot shows a Wireshark capture of ICMP traffic. The packet list pane shows several ICMP Echo (ping) requests and replies between 192.168.190.1 and 192.168.190.128. Packet 29 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The hex dump pane shows the raw data of the selected packet, with a red arrow pointing to the payload: 'T\$\$UEsDB BQAAAAIA KmQTEwls C84WTUNA K5GDQAIA AAAZmxhZy5naWZkvc FdUEQzbb Zp0.' The URL 'https://blog.csdn.net/qq_51665046' is visible in the bottom right corner.

```
tshark -r out.pcap -T fields -e data > data.txt
```

得到data.txt, 发现有重复, 用脚本去重



```
with open('data.txt', 'r') as file:
    res_list = []
    lines = file.readlines()
    print('[+]去重之前一共{0}行'.format(len(lines)))
    print('[+]开始去重, 请稍等.....')
    for i in lines:
        if i not in res_list:
            res_list.append(i)
    print('[+]去重后一共{0}行'.format(len(res_list)))
    print(res_list)

with open('data1.txt', 'w') as new_file:
    for j in res_list:
        new_file.write(j)
```

再将十六进制数据转为字符

```
import binascii

with open('data1.txt', 'r') as file:
    with open('data2.txt', 'wb') as data:
        for i in file.readlines():
            data.write(binascii.unhexlify(i[:-1]))
```

```
$$START$$-----BEGIN CERTIFICATE-----
$$START$$UEsDBBQAAAAIAKMQTEwLsC84WTUNAK5GDQAIAAAAMxhZy5naWZkVdUE0zbBZp0
$$START$$Qk3o3dBDNFsUcB0besfQxqgQKYKaRi8GBAUEDU2KiEEBUQFD70oTAVEDAqKigoJi
$$START$$eznff87LWwsuZs3FzFp75nlm7ynb1t7GyDh4AWgGyD4EiPHLSogpKEiryYkoiaMU
$$START$$5I8dV5HHYLrMDNSNjbTNjPSsrQ@trUydHU86EWx0+VtZ+9s6+jq6RzsQAgheMfb2
$$START$$MZaMMW6+MR6usQGB/q6nY05HnotISi8KT48/d/nc+YxIUgoxLNoj10GELZwuba2
$$START$$tb6x16Who5WWqZ/hSRUNa2kFEwkZrKa0mo2Crq2Ikr+iu1a2UZA2l9YIVY0c0EC
$$START$$ky+vU2nhwNQ80XISx8I5s1z9BmzcR4mhl6NIX8iZc6mpIx5Blc6+deEh9VFna10i
$$START$$a9JS6j0TC009L57yuEhvwHzCId8UL2+kX6mo42vl5ucR7ut5JoaYEBEZRiOhX75Y
$$START$$eJFcvZ/6yazq7HtaUvP67JrenFT8+Wdxefn/1dLdBSkVLzTQkICLVQmbRhdTj
$$START$$+s7+GkbYY1q6wkqxQopx8jrZWW59qTEX3YghxKTQCHJYbG4Bo7Xp4eLw/KfVd/v8
$$START$$AopYRWzFRbq9yYkMBd2sIOWMO+AQNK5hNyE8yVXKju6Hw7dH1zTudG21tK11Tep
$$START$$yMqytvRrCsYXRIUWRsbfrb+np65rp2fghz9ZeJaEFymwyeRFhwoLKZlpaqHP3FK
$$START$$Fx+INfK0UdR4EnF29dV2XWEuqzj/euGV20PG2vJqaeFIhbT8y3m3G66VtN285UA4
$$START$$Y2sf5hCcc/Pes1dr3x5U7L7CZN90CPCZS7TvSMt9sHbRlZRwlNknAGd9oGDE56ecR
$$START$$f/NGSS277o5vcgsxo9XB4/xYdpKdJSGM9iDpUrfLMMjICmWemf5UuYMo0BbRsXZ
$$START$$McCFEP6NUawtpZChp7fRlPspqvR5c8LINCpJNBkjopRhivt28+Z+R+uf8f7FmVKF
$$START$$1LE/r3om0+8crMy96uv72/tkb31NkVdClFvsy8evyx0Do71Peb1lfv7+1lc1yM0L
$$START$$+JjVlnH1aWjCND8Q8rf6xh9jBQeHf2PMTbZu+bz7+6Pj0682e5WPX3592v37Yefn
$$START$$zu6vvf2/u99/E8KLEnPu36puPPz9X83DVxX3FgrrpsiVI0mMp3F5TwAAGNwRj4u1
$$START$$h7slnmCto4UFA/+v6RcEKgw4Amj8rw74vzABwI8AQAgSiWaTqRC4cMAYi9NPgUCR
$$START$$GmgmDgjmQioSWOR3IBifhUkqAGgBQgpnXiasIzuYwJXXGP3KhQhBjJr5wLNEjn
$$START$$lcAchl4WhaftEnqLrNjKaUJ1qMzGHIWYzB5VrJ0DRr4shAoxIzGW1CogLH0TYFP
$$START$$cJ+pd1WcmD53uuig+6oe268nU77miWj4dIivDljni2khn5CAodoFA/kKT3Lwy5m8
$$START$$kzo6sde0Q2GfKvpxq+xiy1F+WfMLh4drLp2fFs3Ig0Xi0gN+KTWvtKh26HkbchC
$$START$$cvIb8BJfKVLm6fsbI4LShomrWZfewa5K0d98NYMaggkq2TGMjhIE5QeFMK71dhU6
$$START$$mQ4i6t6ssNn7mTzXtX4+Sv0w8PTY0d9DqDiafMSXc+s110ojh8qrPIamAmyi0PSf
$$START$$CJ+lzL/2TTWXPZ0317L/8QORLLhVF2YsINDdzByUa1gXkEhuR3mfzQWUgPlKw0og
$$START$$Jt80cVCBvzKWTsgeK7wzZi+1H+Lowtk4hc90XYA5pKGzxEOJqiNux0hMoIOQEVoC
$$START$$NspjvQAhmMvFPopowjVQWDkTEBje5NmIOP/s/EBA7LK1BXfawYuX3GrIGDIgohy/
$$START$$FKw5Blg0yZPYGpC46uxVEV4e/sMiIqp+z5dvuvjaID+0uVgpcKJpzS/6fIejFL0P
$$START$$PaoZj09BtY+ctVl1GEKNKNAoBPL6J2oThF1v/MvlgL+/Pe3RmBScj6A0rRTVrNZ
$$START$$wvF0e1nppCGxbNHEOLlsqggb8n3pj0h08KUG3CGHJnTBZ43yXrC7jSj4k2e972+y
$$START$$tu3lo9882MsI0atai6TyVHLL1F00yLpEhsAlDo8SFrWNYMOWCCL/8BGECjDR0tx4
$$START$$KMQG2HYR0g+VuaGHH7j4oRtgnhHR2eKGr7RHnsmQWJRTKIjzbbC8cDVbhptkXecT
$$START$$UZHphUgab1gMyHgjcd0v4p/q9mK6b+k2MUtEtDks39VkWak0wXw5PC52S4IvdYHc
$$START$$2tRw+9rH5tYtuVf8rDdHI9WyT/girdr6+UY/ofqUUFt1V6r+0+9m1nCV/A2IGn8k
$$START$$2oznbsemeXt259LjfttjX39Rho8LACzeiv7X/io488MPsfRP+1s/2z4fbvWt9fxL
$$START$$HEv/+vSnVsZLRRg0NwCcCc7I5ZHsm+Fwd9jftSZC3NptqKmduFL5JisBLJedwcX9
$$START$$7sqVAbT8LWLFiGLz14QZM2fCApfsThyX30H7e9/FZZPGgTDT6JKraFyHqTgJmJI6
$$START$$Ceqb02vCn4LRJLlAJglwYttCjLcu5RY/ET2rW4JnQ/csbpRwAg51090e16
```

去除首尾两行，将base64解码以字节流形式写成zip

```
import base64

with open('data3.txt', 'rb') as file:
    with open('res.zip', 'wb') as new_file:
        new_file.write(base64.b64decode(file.read()))
```



终于得到gif:

这一系列操作实在看的我头疼

然后是时间隐写?? Ubuntu下使用identify

```
root@kali: ~/zuoti
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/zuoti# identify -format "%T" flag.gif
20505020505020502050202050202020202050502050205020502050202050
20505050205020206666root@kali:~/zuoti# a
面
```

20替换为0

50替换为1

011011010100010000110101010111110011000101110100

```
>>>int('011011010100010000110101010111110011000101110100',2)
120139720634740
```

```
>>> hex(120139720634740)
'0x6d44355f3174'
```

```
>>> binascii.unhexlify('6d44355f3174')
b'mD5_1t'
```

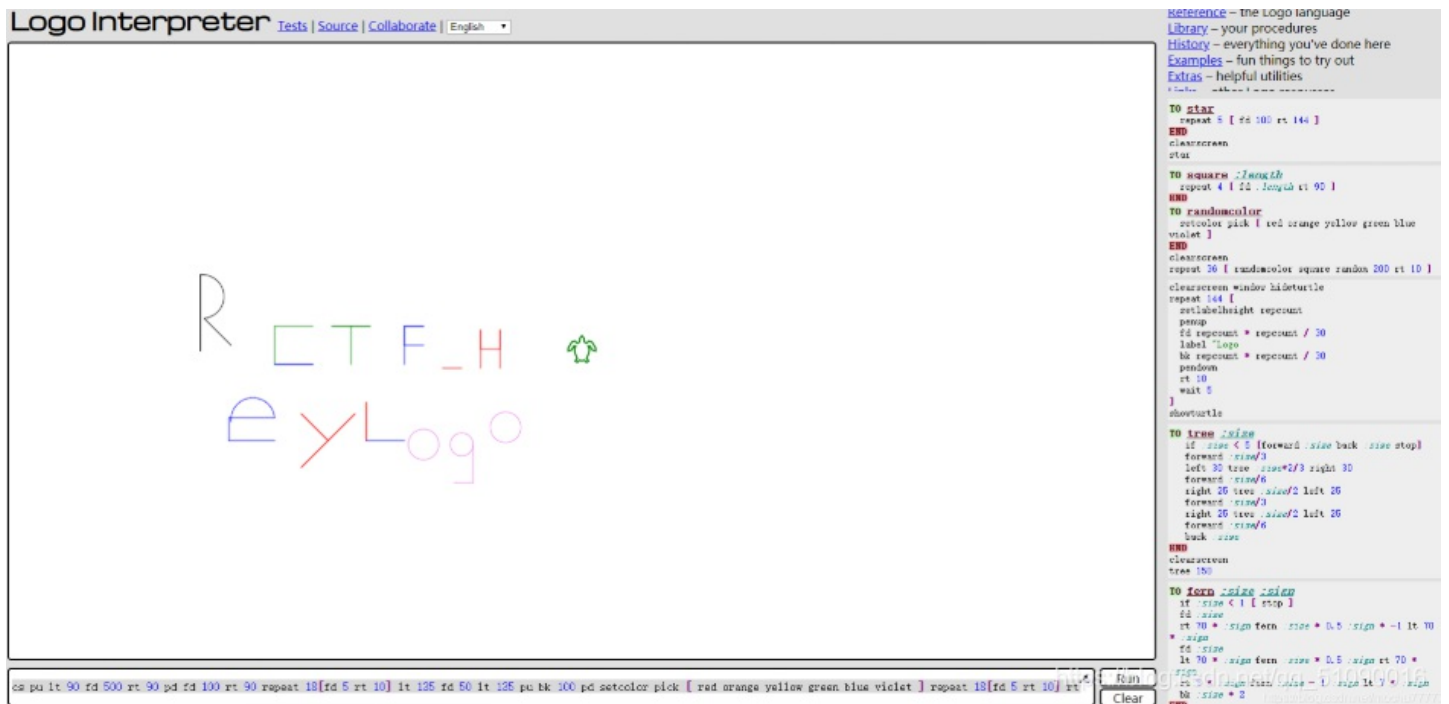
```
>>> hashlib.md5('mD5_1t'.encode('utf-8')).hexdigest()
'f0f1003afe4ae8ce4aa8e8487a8ab3b6'
```

flag{f0f1003afe4ae8ce4aa8e8487a8ab3b6}

[RCTF2019]draw (logo解释器)

将那些字符复制到这个网站: <https://www.calormen.com/jslogo/>

如图：



[MRCTF2020]不眠之夜（montage和gaps）

拼图，把最开始的文件和中间显示不了的文件去掉，120个，每张都是200 x 100，应该长：10张图片，宽：12张图片，那么拼起来的总图就应该是长：2000 x 宽：1200

放到kali里，先用montage：`montage *.jpg -tile 10x12 -geometry 200x100+0+0 flag.jpg`



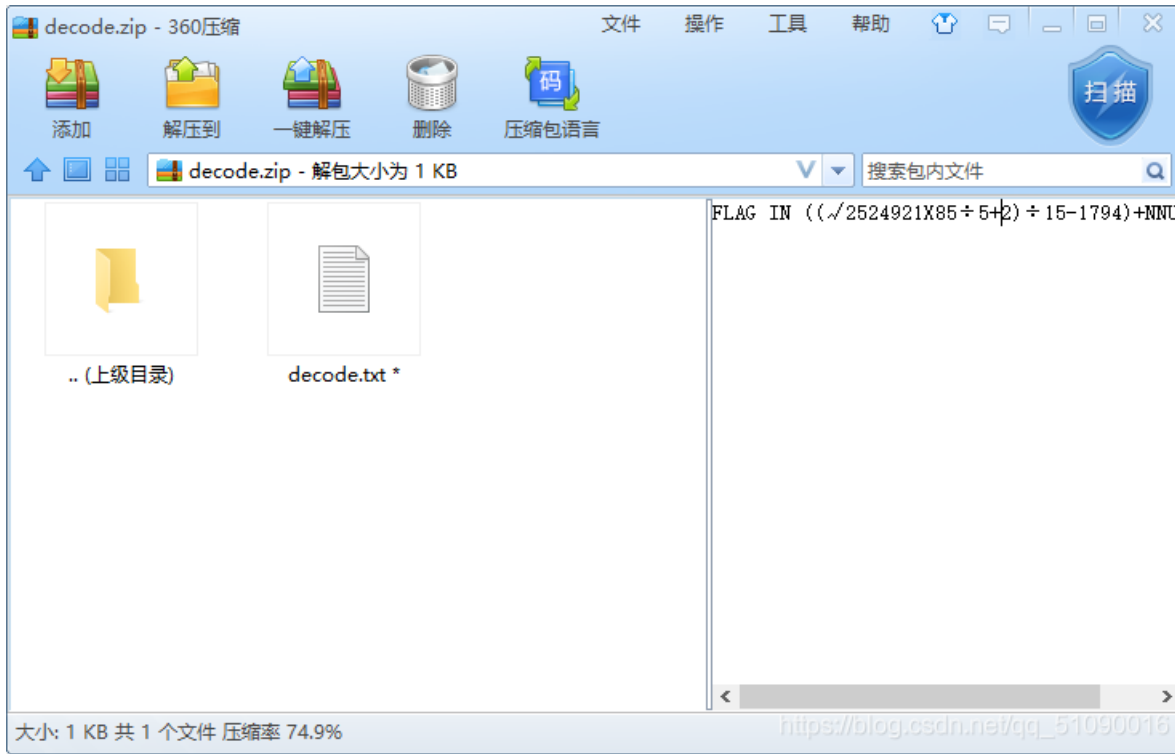
再用gaps：

```
gaps --image=flag.jpg --generations=40 --population=120 --size=100
```

为什么我费劲九牛二虎之力安装完还出错了？？真的给我弄吐了，还百度不到原因

[安淘杯 2019]easy misc（盲水印）

看压缩包：

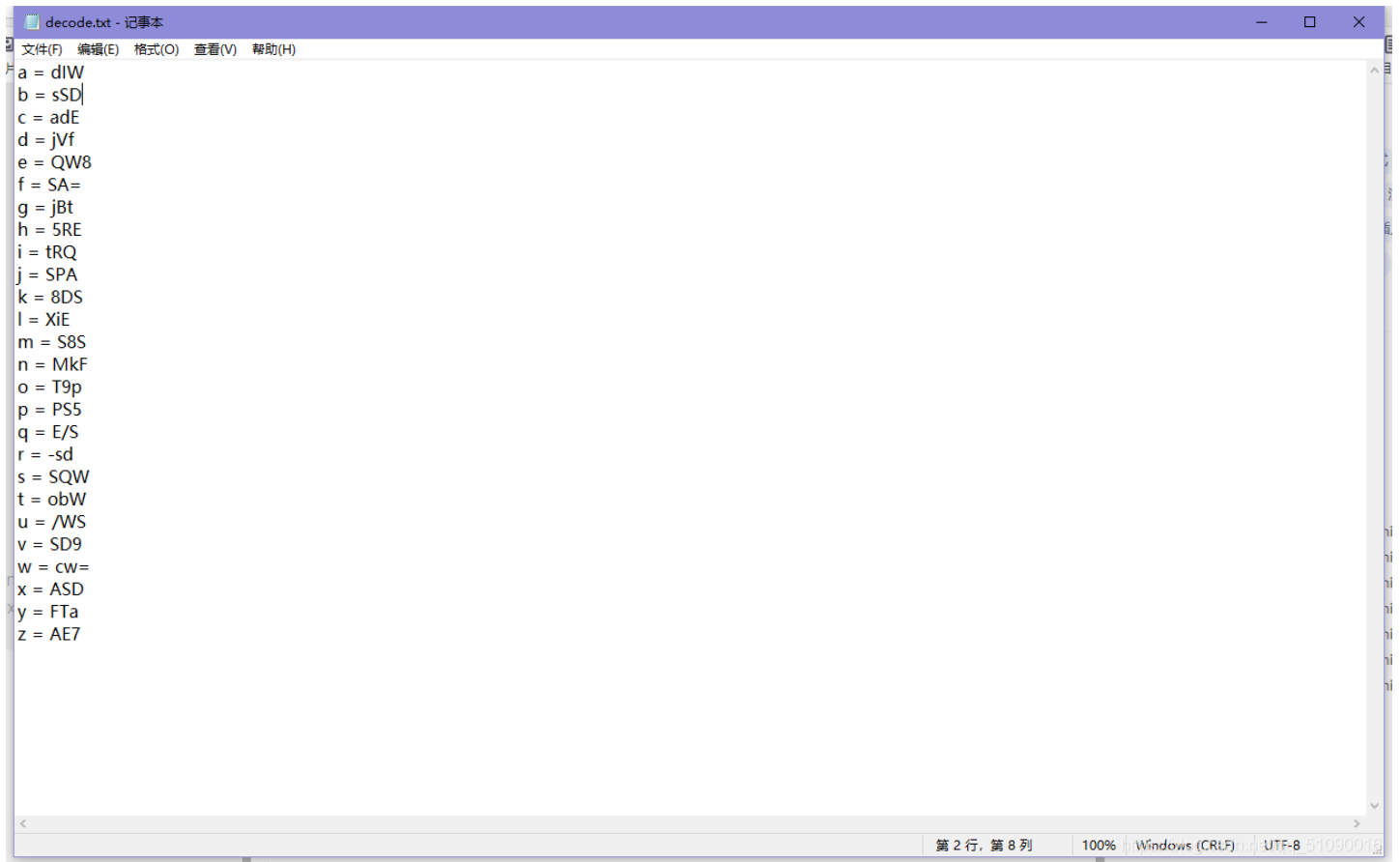


FLAG IN ((\2524921X85÷5+2)÷15-1794)+NNULLULL

前面计算得7，后面猜测是掩码



得到密码，打开解压



这又是啥。。果然做题全靠百度，原来是字频隐写
按照wp的做，先看png

binwalkt一下

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 626 x 626, 8-bit grayscale, non-interlaced
134	0x86	Zlib compressed data, best compression
118959	0x1D0AF	PNG image, 626 x 626, 8-bit/color RGB, non-interlaced

还有个png，foremost一下

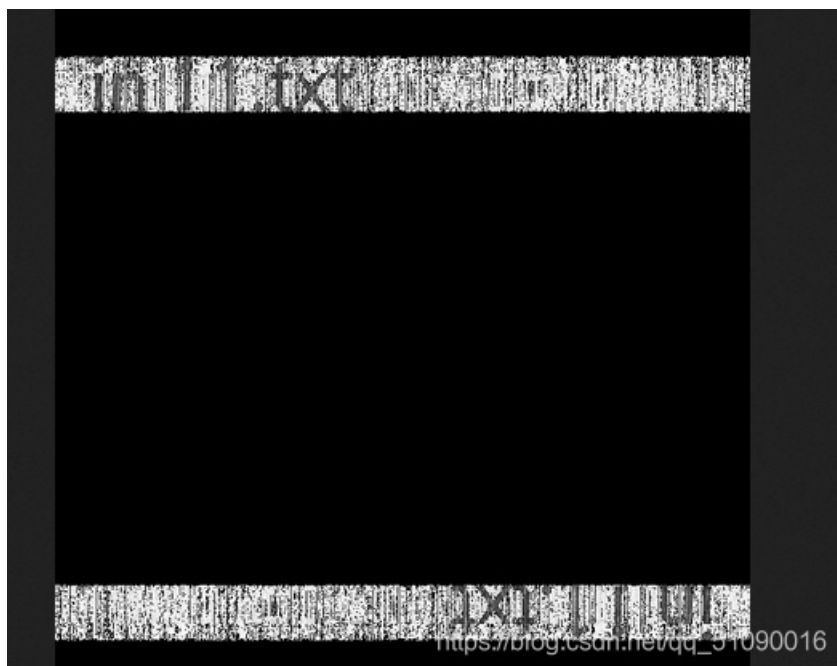


想到盲水印，安装脚本地址：
<https://github.com/chishaxie/BlindWaterMark>

输入：

```
python2 bwm.py decode 00000000.png 00000232.png output.png
```


得到



提示in 11.txt（所以费了这么大力气就这）

hint中提示取前16位，利用python脚本获取11.txt中前16高频字母

```
import re

file = open('C:/Users/Fiona/Desktop/11.txt')
line = file.readlines()
file.seek(0,0)
file.close()

result = {}
for i in range(97,123):
    count = 0
    for j in line:
        find_line = re.findall(chr(i),j)
        count += len(find_line)
    result[chr(i)] = count
res = sorted(result.items(),key=lambda item:item[1],reverse=True)

num = 1
for x in res:
    print('频数第{0}: '.format(num),x)
    num += 1
```

即：etaonrhisdluygw

对照decode.txt里面的数得到一串base64的编码：

QW8obWdIWt9pMkFSQWtRQjVfXiE/WSFTajBtcw==

解密后

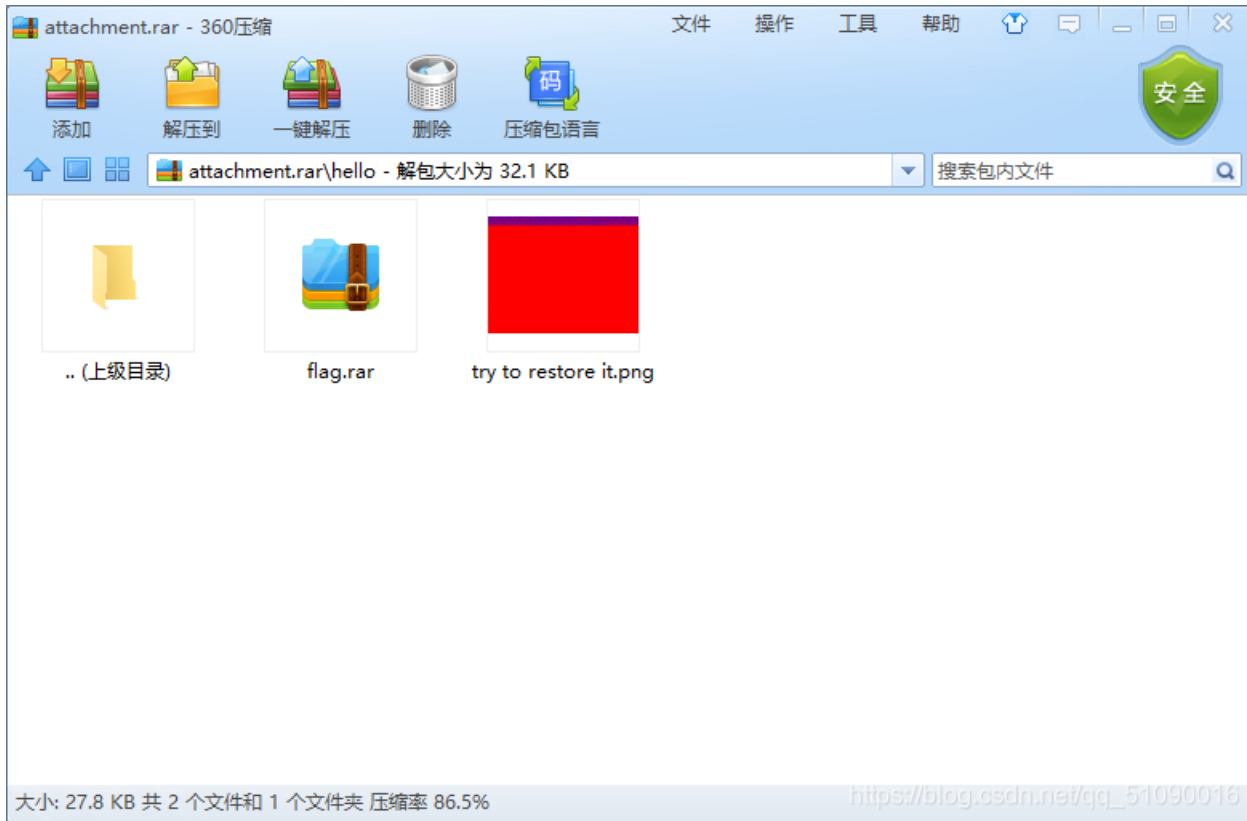
Ao(mgHY?i2ARAKQB5_?!?Y!Sj0ms

这是base85

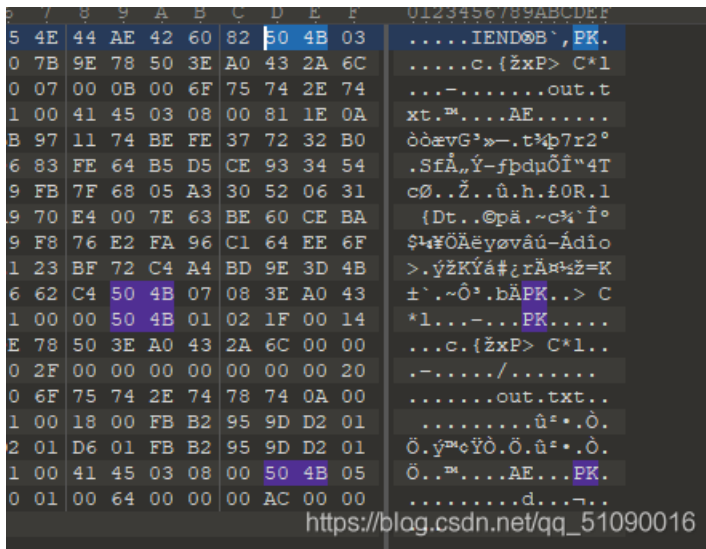
得到

flag{have_a_good_day1}

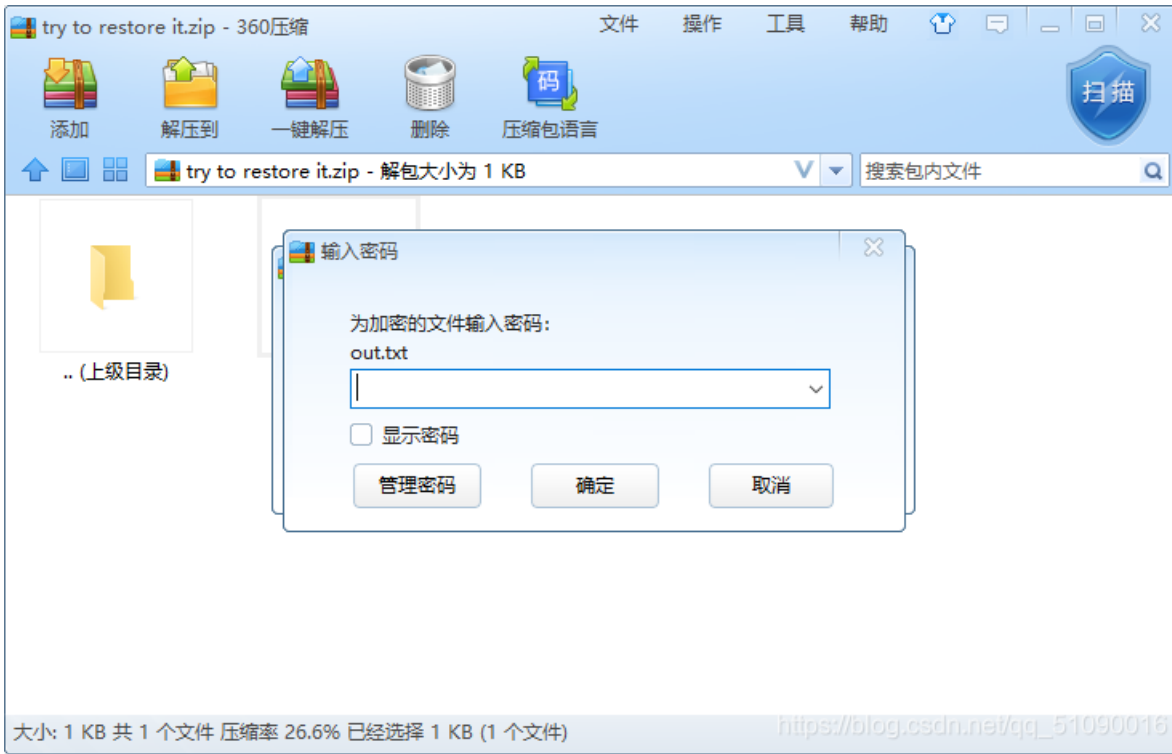
[MRCTF2020]Hello_misc



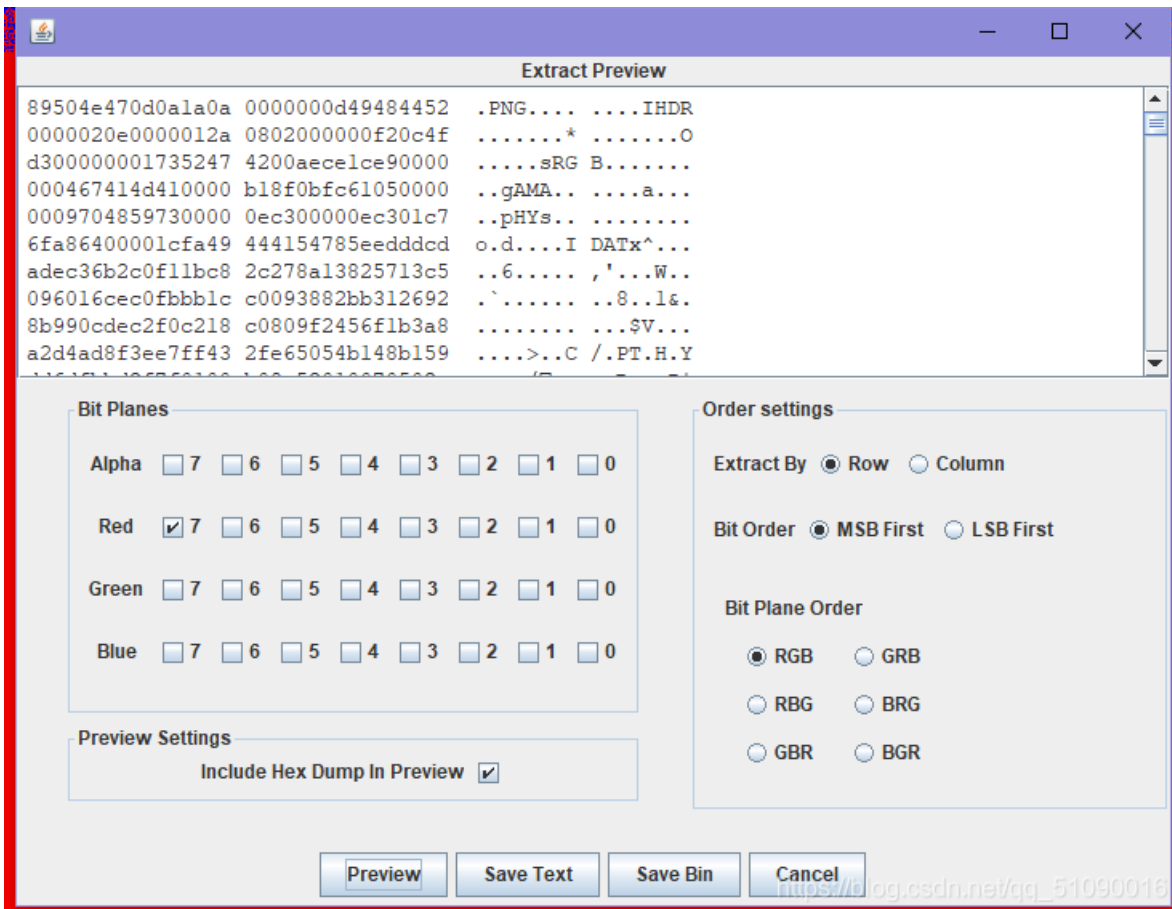
正常先把图片用010打开看看:



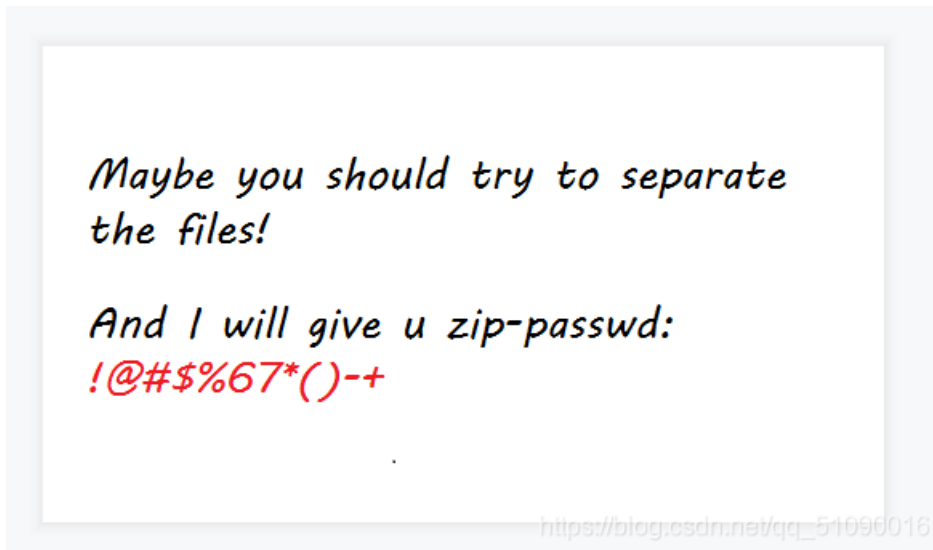
发现有压缩包的痕迹，改成zip看看



需要密码，从哪弄？应该是原本那张图片，那个颜色就让我怀疑是lsb隐写
这题和之前的不一样，在red通道发现图片（难怪图片是红色）



另存



得到解压密码，解压

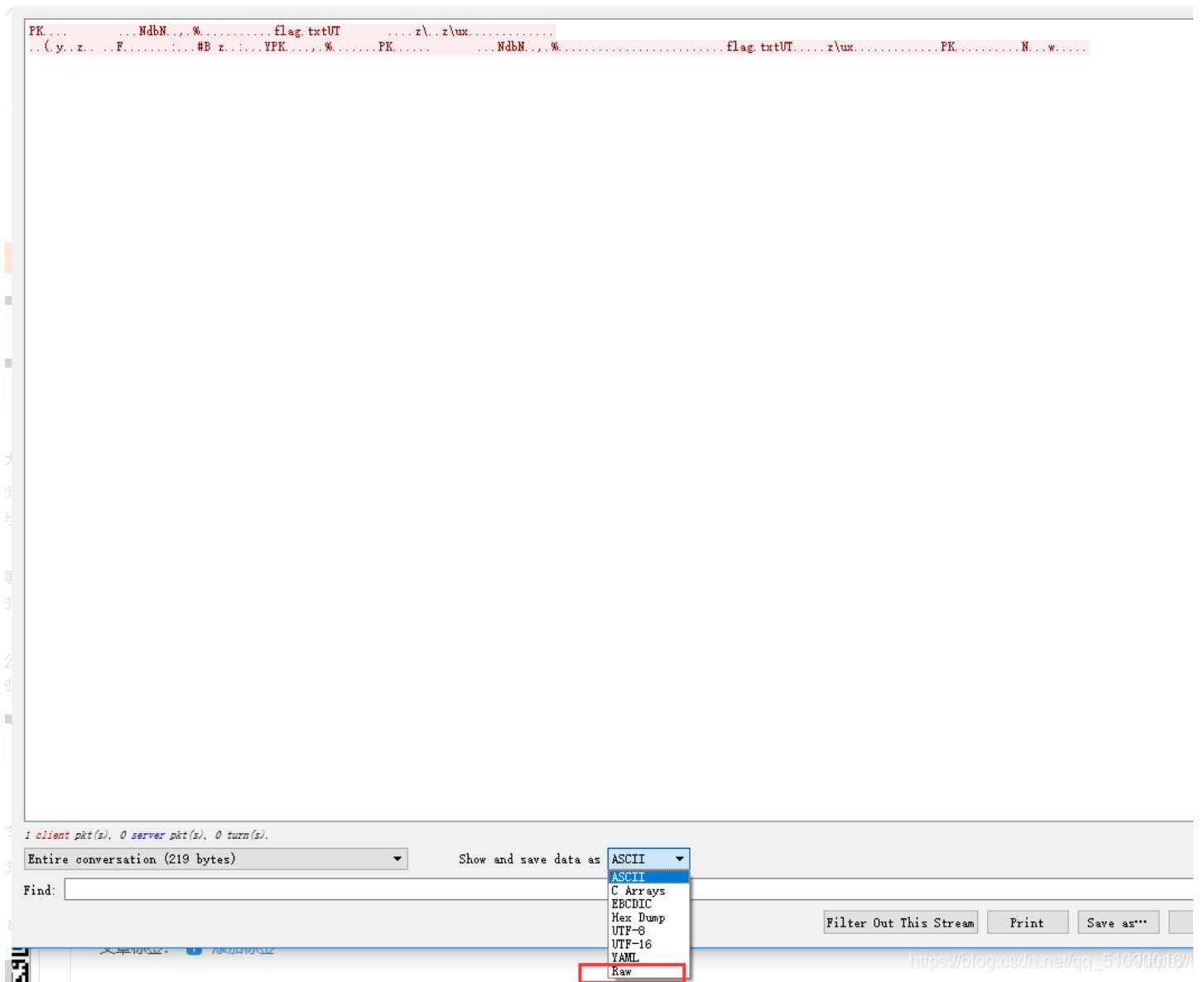
```
out.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助
127
255
63
191
127
191
63
127
127
255
63
191|
63
191
255
127
127
255
63
63
127
191
63
127
127
255
63
```

几个重复的数字，之前好像碰到过，又有点忘了，刚好复习一下

用脚本转换二进制提取前两字节，转为ASCII

得到提示rar-passwd:0ac1fe6b77be5dbe

以原始数据保存为zip文件



使用密码解压

```
root@kali:~/桌面# unzip -P supercomplexpassword flag.zip
Archive:  flag.zip
  inflating: flag.txt
```

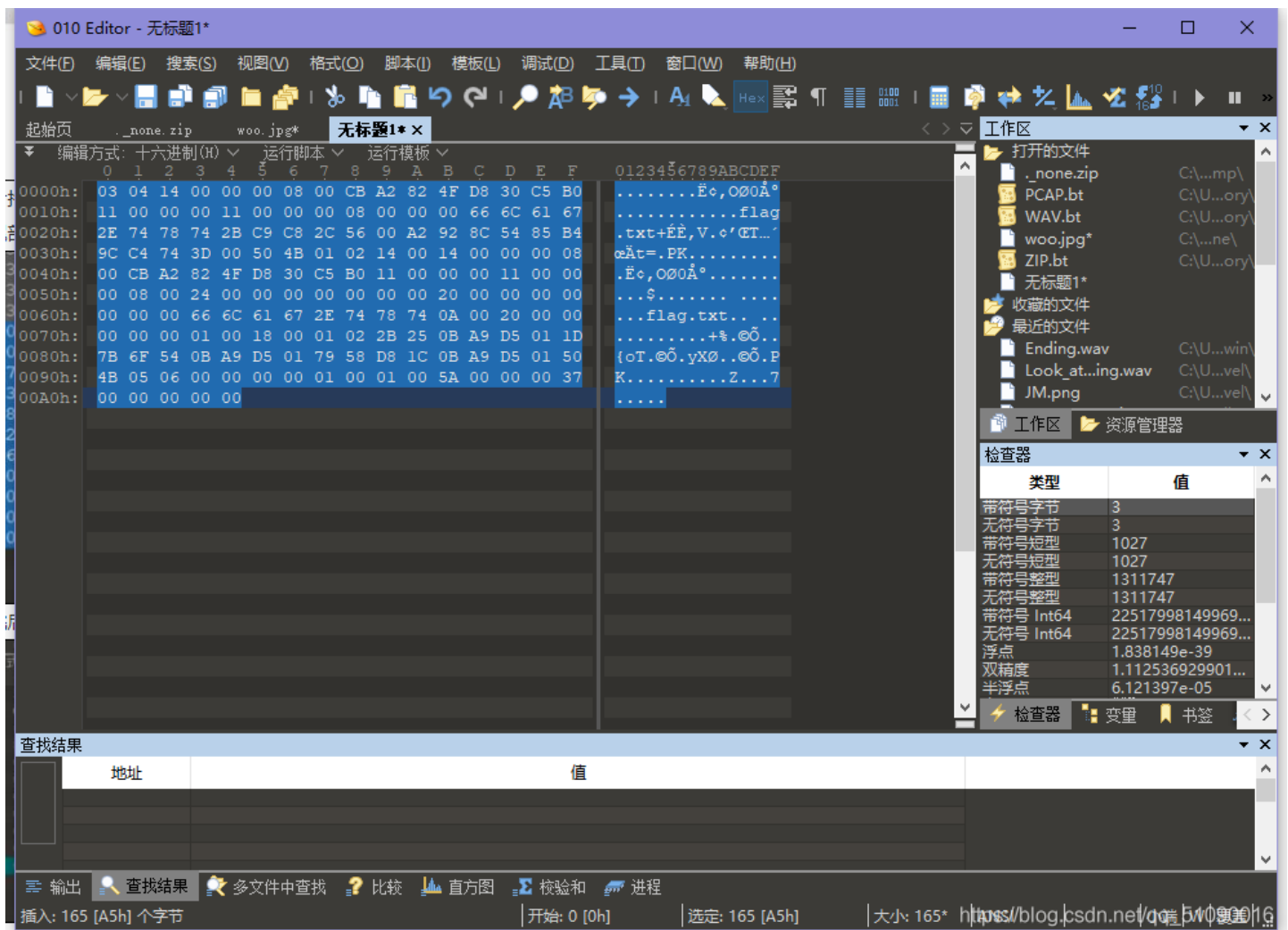
[ACTF新生赛2020]明文攻击(隐藏文件内容在010)

文件里有个压缩包和图片，压缩包里只有txt文件，根据提示明文攻击，估计是要在图片里找到一个txt文件。

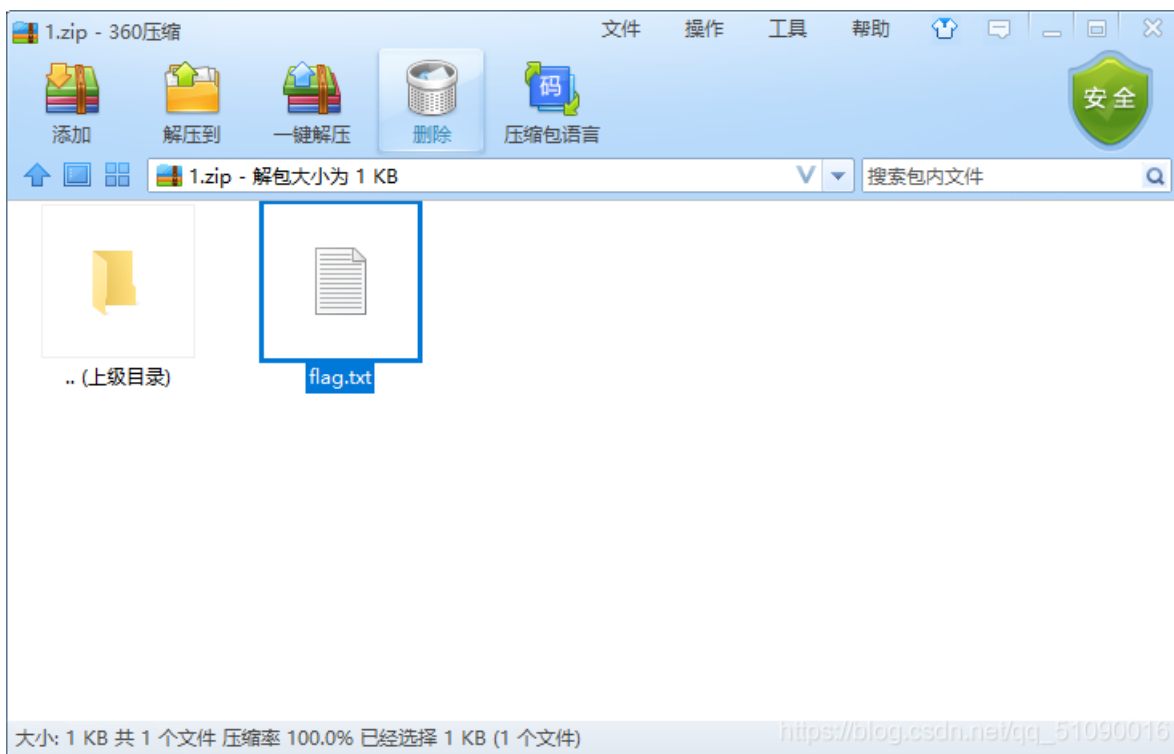
图片放到010发现有txt

C0h:	32 32 32 32	32 32 32 32	32 32 32 32	32 32 03 04	22222222222222..
D0h:	14 00 00 00	08 00 CB A2	82 4F D8 30	C5 B0 11 00Ëç,000Ã°..
E0h:	00 00 11 00	00 00 08 00	00 00 66 6C	61 67 2E 74flag.t
F0h:	78 74 B B C9	C8 2C 56 00	A2 92 8C 54	85 B4 9C C4	xt+ËË,V.ç'@T...œÃ
00h:	74 3D 00 50	4B 01 02 14	00 14 00 00	00 08 00 CB	t=.PK.....Ë
10h:	A2 82 4F D8	30 C5 B0 11	00 00 00 11	00 00 00 08	ç,000Ã°.....
20h:	00 24 00 00	00 00 00 00	00 20 00 00	00 00 00 00	.\$.....
30h:	00 66 6C 61	67 2E 74 78	74 0A 00 20	00 00 00 00	.flag.txt.. .
40h:	00 01 00 18	00 01 02 2B	25 0B A9 D5	01 1D 7B 6F+\$.@Û...{o

改成zip后缀失败。。那该咋办，看这后面的样子，像是一个压缩包，但是没有文件头，试一下复制下来加个文件头504b:



果然得到了



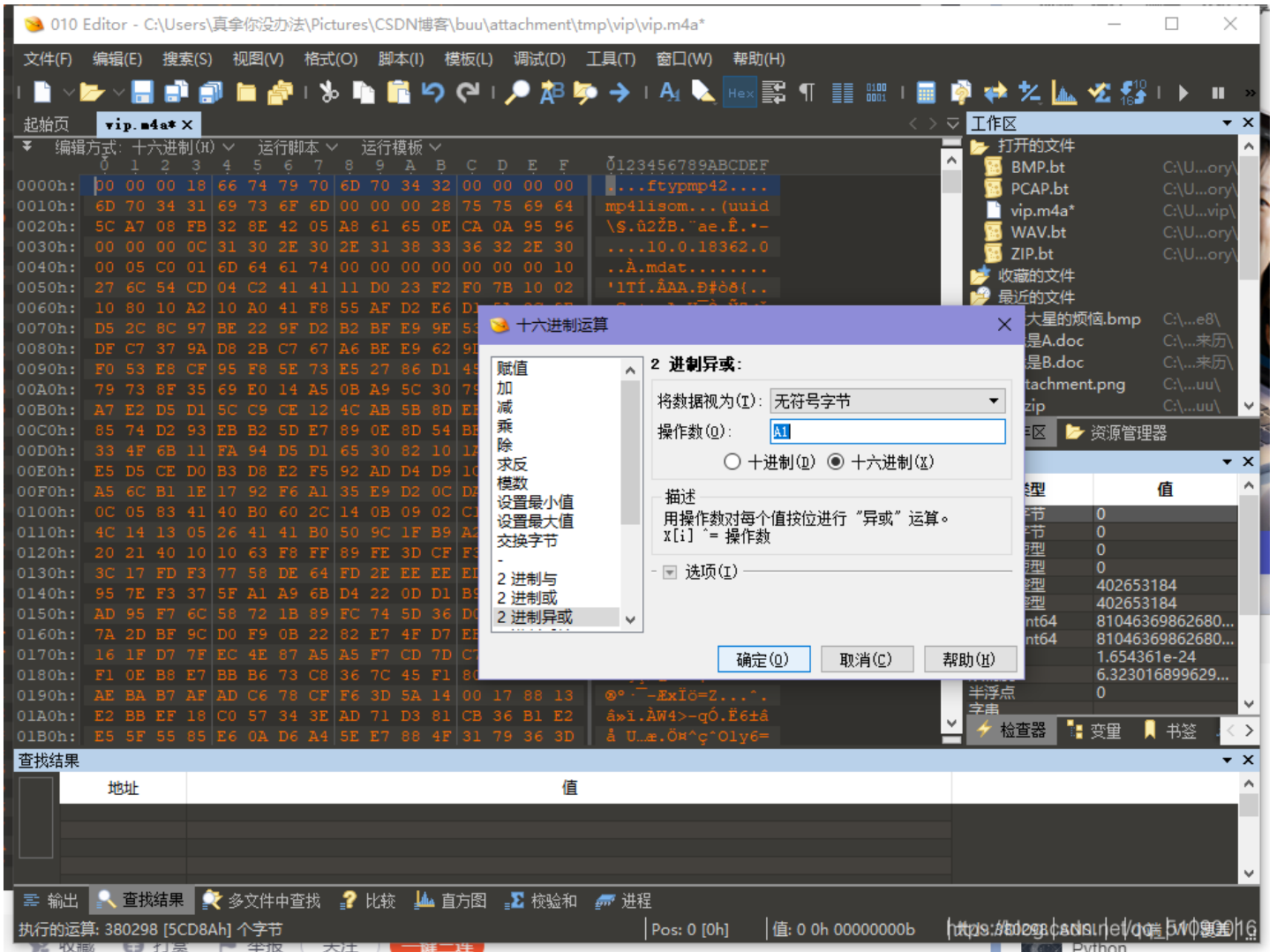
明文攻击

然后就能打开了

—
帝高阳之苗裔兮，朕皇考曰伯庸。←
摄提贞于孟陬兮，惟庚寅吾以降。←
皇览揆余初度兮，肇锡余以嘉名：←
名余曰正则兮，字余曰灵均。←
纷吾既有此内美兮，又重之以修能。←
扈江离与辟芷兮，纫秋兰以为佩。←
汨余若将不及兮，恐年岁之不吾与。←
朝搴阰之木兰兮，夕揽洲之宿莽。←
日月忽其不淹兮，春与秋其代序。←
唯草木之零落兮，恐美人之迟暮。←
不抚壮而弃秽兮，何不改乎此度？←
乘骐骥以驰骋兮，来吾道夫先路！←

仔细看，发现四个文档间距不同，想到MD5加密，设1.5倍为1,1倍为0，将每行的值连在一起，进行MD5解密（这也行？）
最后发现c是对的

帝高阳之苗裔兮，朕皇考曰伯庸。←
摄提贞于孟陬兮，惟庚寅吾以降。←
皇览揆余初度兮，肇锡余以嘉名：←
名余曰正则兮，字余曰灵均。|←
纷吾既有此内美兮，又重之以修能。←
扈江离与辟芷兮，纫秋兰以为佩。←
汨余若将不及兮，恐年岁之不吾与。←
朝搴阰之木兰兮，夕揽洲之宿莽。←
日月忽其不淹兮，春与秋其代序。←
唯草木之零落兮，恐美人之迟暮。←
不抚壮而弃秽兮，何不改乎此度？←
乘骐骥以驰骋兮，来吾道夫先路！←



保存后仔细听就得到了

[SCTF2019]电单车

放到audacity里面看看



细的为0宽的为1

0 0111010010101010011000100 011101001010101001100010

根据wp

钥匙信号(PT224X) = 同步引导码(8bit) + 地址位(20bit) + 数据位(4bit) + 停止码(1bit)

地址位长度为20bit, 后4位为数据位即01110100101010100110就是flag (咱也不懂, 咱也不敢问)

hashcat(爆破ppt文件)

010没看出啥, 改成zip也没思路, binwalk一下

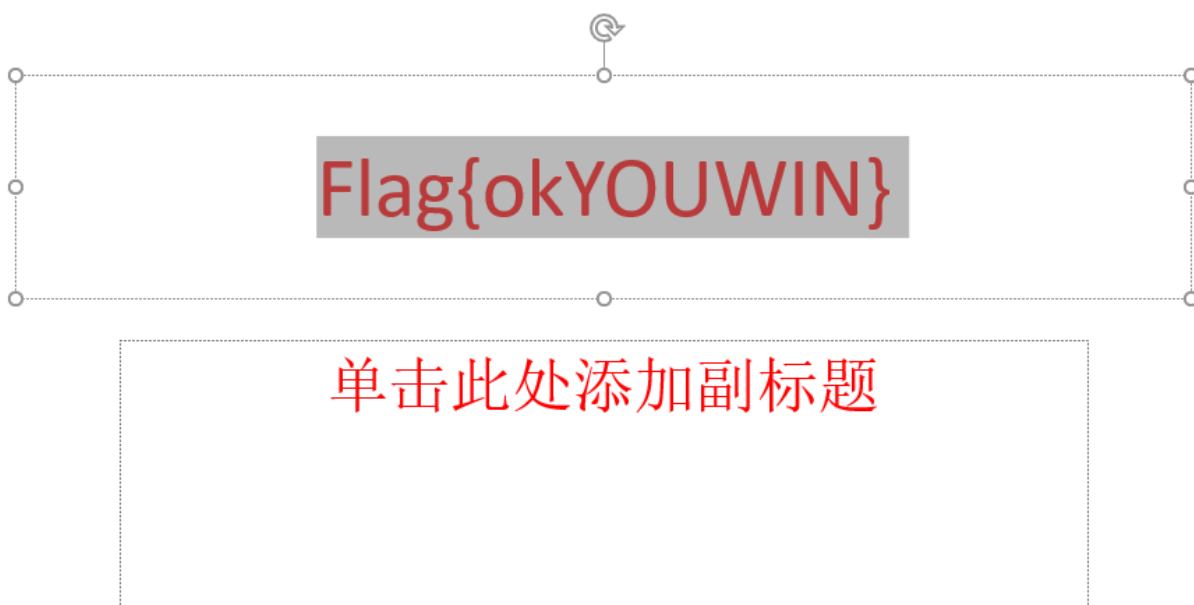
DECIMAL	HEXADECIMAL	DESCRIPTION
3656	0xE48	XML document, version: "1.0"

XML文件, 添加文件后缀为ppt, 有加密

使用Accent OFFICE Password Recovery对其爆破密码, 老样子还是猜测密码为四位纯数字

得到密码9919

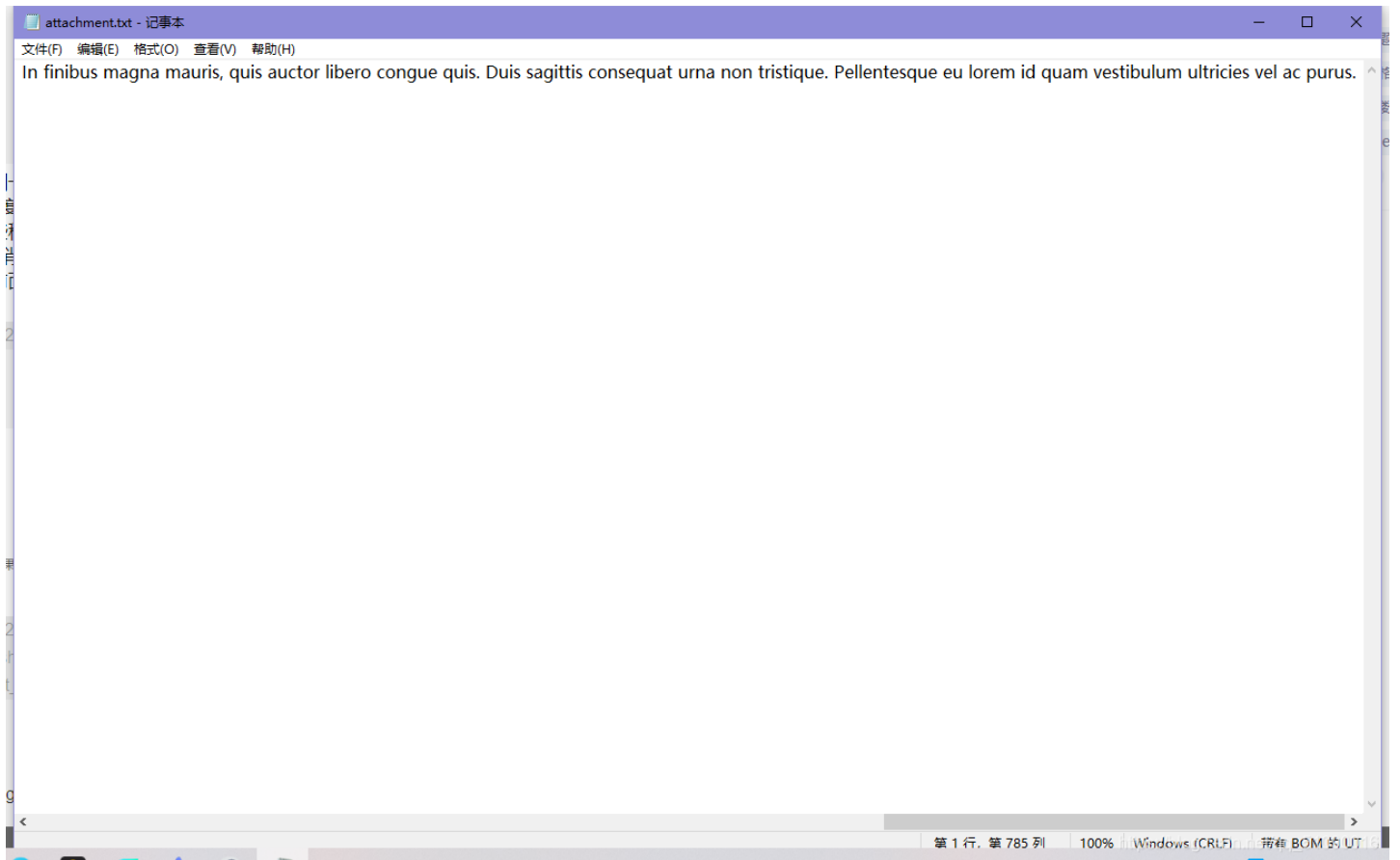
使用密码解开ppt文档, 在倒数第二页有全选中标红即可 (这个真想不到)



https://blog.csdn.net/qq_51090016

[UTCTF2020]zero (零宽度字符隐写)

又是没遇见过的类型。。。



打开看了看没思路，只好看wp

先看看什么是零宽度字符隐写

大意是，可以通过零宽度字符来隐藏一些信息，达到一些目的，比如隐写，或者水印。某种程度上来说，我们这里所说的零宽度字符可作为识别某些用户身份的“指纹”数据，也可非常方便地追溯到某些秘密数据的泄露源。然后分别插到载体消息中的每一个字符后面。若载体消息短于隐藏信息的二进制，那就把多余的都塞到载体消息的最后一个字符前面，这样在复制的时候不至于掉少一些隐藏字符。

那该怎么分辨呢。。

比如在下面这个例子中

```
"大佬早上好呀".length  
34
```

我们能看到的只有六个字，但是显示的length有34，零宽度字符就会产生这个效果，他不影响阅读，但是真实存在，也会占长度。

虽然我们看到的样子上面这个样子，但是实际上他是下面这个样子~

https://blog.csdn.net/qq_51090016

解密网址：https://330k.github.io/misc_tools/unicode_steganography.html

Original Text: (length: 709)

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus quis tempus ante, nec vehicula mi. Aliquam nec nisi ut neque interdum auctor. Aliquam felis orci, vestibulum sit amet ante at, consectetur lobortis eros. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus auctor. In finibus magna mauris, quis auctor libero congue quis. Duis sagittis consequat urna non tristique. Pellentesque eu lorem id quam vestibulum ultricies vel ac purus.

Hidden Text: (length: 32)

utflag{whyNOTesc11_4927aajbak14}

Steganography Text: (length: 965)

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus quis tempus ante, nec vehicula mi. Aliquam nec nisi ut neque interdum auctor. Aliquam felis orci, vestibulum sit amet ante at, consectetur lobortis eros. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus auctor. In finibus magna mauris, quis auctor libero congue quis. Duis sagittis consequat urna non tristique. Pellentesque eu lorem id quam vestibulum ultricies vel ac purus.

https://blog.csdn.net/qg_51990016

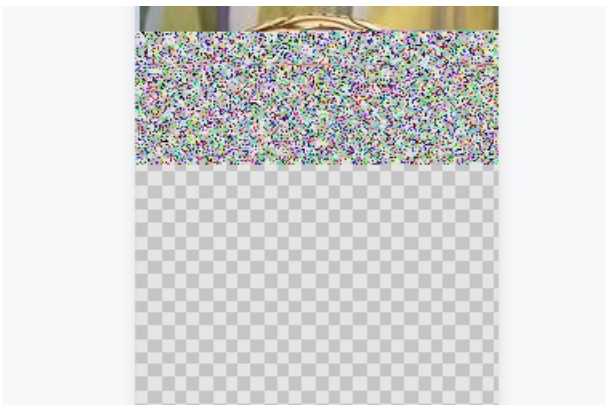
[湖南省赛2019]Findme

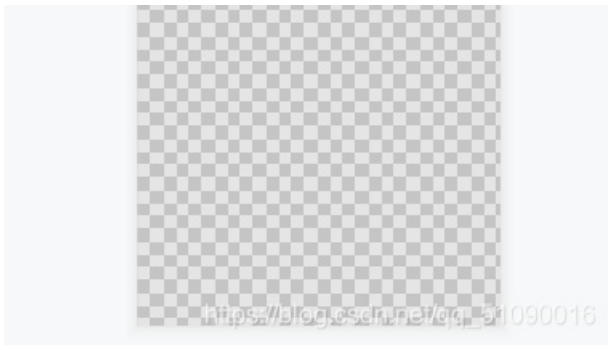
五张图片，一个个看

第一张应该是宽高不对

```
import zlib
import struct
file = '1.png'
fr = open(file, 'rb').read()
data = bytearray(fr[12:29])
#crc32key = eval(str(fr[29:33]).replace('\x', '').replace("b'", '0x').replace("'", ''))
crc32key = 0xC4ED3
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xf4\x00\x00\x01\xf1\x08\x06\x00\x00\x00')
n = 4095
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width, height)
            print(data)
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png', 'wb')
            fw.write(newpic)
            fw.close
```

改完怎么是这样





用010打开，发现错误

起始页 1.png.png X

编辑方式: 十六进制(H) 运行脚本: 运行模板: PNG.bt

地址	值
0000h	B9 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
0010h	00 00 00 E3 00 00 01 C5 08 06 00 00 00 00 0C 4E ...ä...Ä.....
0020h	D3 00 00 20 00 49 44 41 54 78 5E AC BD 79 98 1D 0.. IDATx^~sy
0030h	77 75 2D BA AA EA D4 A9 33 F4 99 7A 1E A4 1E 34 wu-°*ê0@3ó"z.κ
0040h	0F 96 35 D9 96 67 1B 4C E2 21 06 1B 1B 6C 0C 01 ,-5Û-g.Lá!...l
0050h	03 49 5E 92 4B 02 84 97 00 19 1E 24 79 EF DE 84 .I^'K.,,..\$.yif
0060h	3C 12 87 10 08 10 20 97 F0 25 D8 CC 06 6C 8C 31 <.#+...-8%0I.10
0070h	B6 6C E3 41 F2 20 D9 92 35 5A 6A 75 4B 3D F7 99 QlãAò Û'5ZjuK=-
0080h	A7 (1A) 4E 55 DD 6F ED DF 39 1A 02 37 2F 7F BC CE §.NUYoiß9..7/.4
0090h	C7 D7 B1 D4 3A 7D 4E D5 6F ED BD F6 DA 6B EF D2 Ç×±0;}NÖoi%óÜkã
00A0h	9E DB 3F 13 9A 51 0D 61 D0 C4 DF DE F7 97 D0 0D žÛ?.šQ.aÐÃAB+~#
00B0h	1F D0 1C F8 2D 17 1A 2C C4 CD 34 D6 AE D9 80 5C .Ð.ø-.,Ãí40@Ûé
00C0h	76 10 AD 96 0B 2B 92 86 15 D3 D0 6A 01 08 CB 30 v.--.+^t.ÓDj..E
00D0h	4D 07 41 D0 84 DF 2A C0 F3 2B 08 02 1B D0 1D 98 M.ÅÐ„ß*Åó+...Ð.
00E0h	5A 08 4D D3 10 09 03 20 8C 41 0F 34 20 D4 60 00 Z.MÓ...ÇA.4 Ó
00F0h	D0 F8 77 7A 08 E8 21 7C DF 81 DB 0A 61 E8 9A FC Ðøwz.è! ß.Û.aèš
0100h	BC 6D 03 41 10 A0 5A B7 B1 B0 B0 00 D7 0B 11 86 km.A. Z-±°.*.
0110h	1E FC 30 0A 7E E9 9A 0E 5D 8F CA CF 86 7C C9 20 .ú0.~éš.].ËI+ E
0120h	40 10 C6 E1 DA 21 EC 86 8E B0 95 45 D4 8C 23 62 @.EáÛ!i+ž°*EÓE
0130h	64 10 86 21 74 1D 6C 34 ÇB C8 E6 62 D8 72 F1 06 d.+!t.h4ËËab0rř
0140h	8C 8F 8F 23 12 E1 6B E9 B0 4C A0 E5 35 A1 43 83 Ç..#.áké°L å5;Q
0150h	7A 7B 01 34 CD 83 66 C4 10 CA FB B7 A0 C9 EF 0B z{.4ÍfřÄ.Èû-Éš
0160h	61 EA 0E 34 A3 01 04 15 D4 1A F3 28 2E CF A1 58 aè.4š...Ó.ó(.Í
0170h	5C 40 2C 6A 22 F0 6C F8 BE D6 FE 7D FC 79 17 A1 \@.j"ðlø%Öp)üy
0180h	CE 4F CA CF 6A 41 D7 03 84 D0 E0 79 21 5C D7 95 ÍOËÍjA×„.Ðày!\
0190h	CF 17 89 00 91 88 01 23 04 E2 09 8B 1F 04 B6 6D ĩ.%.^#.š.<..š
01A0h	43 D7 75 24 93 19 79 7F CD 66 13 61 C8 EB E2 CB C×u\$".y.Íf.aÈèš
01B0h	9F F3 F3 B4 3C BE 4E 53 5E DB 30 2C 44 F4 24 12 Ýóó<³NS^ÛO,Dóš

ERROR: CRC Mismatch @ chunk[29]; in data: 00000000; expected: 5308f045 Pos: 0 [0h]

IDAT十六进制标识为: 49 44 41 54, 将两个chunk的IDAT在union CTYPE type的位置补上即可得到完整的图片

010 Editor - C:\Users\真拿你没办法\Pictures\CSDN博客\脚本\1.png.png

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

起始页 1.png.png X

编辑方式: 十六进制(H) 运行脚本: 运行模板: PNG.bt

地址	值
1F00h	CF F8 BF 6B 6D D0 F8 42 D3 00 CF 2E 1D 45 D2 53 Īø;kmÐøBÓ.Ī..EÖš
1F10h	6C D9 72 5F C4 BC 62 37 E4 7D D3 17 CB CC 28 EE lÛx_Ã¡b7ã)Ó.ËĪ(i
1F20h	20 D6 8C B5 06 0A 65 1B 15 37 8E 48 2C 37 98 95 ÓÇu..e..7ZH,+*.
1F30h	81 F6 FC AB 27 43 35 5F 65 4B CD D8 D5 95 91 48 .òü«'C5_eKIÖÖ.'H
1F40h	DC D7 93 43 26 DD 27 8E 12 29 6A A8 70 D1 4D 81 Ū×"C&Y'ž.)j"pñM.
1F50h	9A 12 69 E8 B4 D1 CB B0 1B 2C 72 DB 45 34 68 FB š.iè'ÑÈ°.xÛE4hú
1F60h	92 CB A1 64 E6 B6 51 5A 35 CF D9 6B 64 B6 E1 1B 'È;daē1QZ5ĪÜkdŹÁ.
1F70h	D2 11 FA 74 F9 8B 9E D9 76 AB 28 45 4D 39 53 A8 Ó.úttûç žÛv«(EM9S"
1F80h	4A AA 91 A9 72 B9 84 72 A9 89 02 C7 59 1A 6A DC J*^øx^.,x@%.ÇY.jÛ
1F90h	C9 88 24 A0 D3 D2 C6 0C C0 2C 1D 58 F0 BD 38 7C È°š ÓÖE.À.,Xš%8
1FA0h	97 0D EF 8C 00 D1 8C AA FE 10 1D 38 0D A7 81 91 -.iÇ.ÑÇ*p..8.š.'
1FB0h	95 34 8A 6F 46 AE 37 AB E6 D1 E2 51 58 86 81 CA *4š0F07«ãÑãQXt+.È
1FC0h	FC 0C A8 49 E4 BA 73 52 97 4D 9D 3A 82 D7 8F 1F ü."Ia°šR-M.:.,x..

ERROR: CRC Mismatch @ chunk[29]; in data: 00000000; expected: 5308f045 Pos: 0 [0h]

Hex editor view showing memory addresses and data. The selected range is 8241 [2031h] to 8244 [2034h].

Address	Hex	ASCII
1FD0h	81 65 6A 18 5B 39 0E 43 F3 91 5F 2A E2 CC A9 19	.ej.[9.C6`*ãI@.
1FE0h	9C 9E 9A 46 29 4F 57 46 15 41 8B D7 43 43 4F 5F	œžšF)OWF.A<*CCO_
1FF0h	56 D4 D7 DE 9E 1E 99 08 59 B9 62 14 BD DD 69 71	VÔ×Ĕž.™.Y'ib.ºYiq
2000h	2D 25 62 29 01 06 85 17 8B 16 30 16 99 EC 82 F3	-šb).....<.0.™i,ó
2010h	E0 50 ED A3 AD 4C 6B 22 9E 4A 88 92 EB DB 74 E1	àPif-Lk"žJ'/'eŮtá
2020h	B0 86 34 51 58 58 14 65 F5 88 1C 3F 92 00 00 20	°+4QXX.eðs.ž'..
2030h	00 00 00 41 54 B1 9F 3E 2A E2 4E BE 58 42 2A 93	...At+Y>*ãN*XB**
2040h	C2 E0 F0 10 34 9D 07 27 85 A1 A1 21 89 DA F4 AC	Ääð.4...!¡¡!šŮð-
2050h	F2 26 57 2A 65 38 6E 53 02 1B 33 3B 6D 86 0C A4	ð&W*e8nS..3;mt.H
2060h	D5 6A 1D F5 BA 87 98 C5 79 BC 04 66 67 E6 85 2A	Ōj.ð°+~Äy*fgæ...*
2070h	53 41 AD 23 40 A9 56 46 B3 D6 14 1A 3C 22 4A EB	SA-#@@VF'ð.<"Jè
2080h	7A 5C B6 73 07 36 6F 5C 87 96 ED E0 E8 91 FD 58	z\šs.6o\+-iàè'YX
2090h	98 9D C2 86 F5 1B 60 1A 21 66 CE 4C 21 0C 9B 98	".Ätð..!fîL!..>
20A0h	9E 9E 97 59 C7 E1 15 13 C8 17 0B 78 E8 A1 9F 60	žž-YÇá..È..xèjY'
20B0h	EF 8B 27 31 31 91 C3 9D 6F BF 1D D7 5E 77 1D BA	ik'11'Ä.ož.*^w.°
20C0h	59 4F D2 C1 A5 B9 A8 E7 4B 98 CF 2F 88 57 34 08	Y00ÄY'çK'î/'W4.
20D0h	E9 D0 08 D1 9B 8A C1 B5 4B B0 A2 AA FF CA EB 4B	èð.Ñ>šÄnK<*yÈèK
20E0h	96 40 76 B0 B4 5C 10 83 3B AF 53 8B FD 45 5E 71	-@v°\'.f;Š<yE^q
20F0h	01 93 27 0E A3 C0 0B A0 05 1E 22 F4 0F 73 32 C6	..'.ÄÄ..'"ó.s2E
2100h	55 AA 2A ED 66 8E 5B 93 36 53 A9 5C 42 D3 D1 E0	U*ifž[*^6S@BÓNÄ
2110h	72 AA 86 81 9F 14 57 06 73 42 11 65 D2 A4 87 D0	r*+.Y.W.sB.e0n#ð
2120h	90 4A C7 11 8B AB 40 C0 FB C5 FE 74 7E B9 0C 9B	.Jç.<«@ÄüÄbt~>.
2130h	53 2D 32 CF 98 46 C4 64 52 51 DE 54 69 6D 30 3B	S-2I~FÄdRQpTim0;

Variable window showing PNG chunk structure:

名称	值	开始
struct PNG SIGNATURE sig		0h
struct PNG CHUNK chunk[0]	IHDR (Critical, Pu...	8h
struct PNG CHUNK chunk[1]	IDAT (Critical, Pu...	21h
struct PNG CHUNK chunk[2]	(Critical, Public, ...	202Dh
uint32 length	8192	202Dh
union CTYPE type		2031h
ubyte data[8192]		2035h
uint32 crc	F4FF7854h	4035h
struct PNG CHUNK chunk[3]	(Critical, Public, ...	4039h
struct PNG CHUNK chunk[4]	IDAT (Critical, Pu...	6045h
struct PNG CHUNK chunk[5]	IDAT (Critical, Pu...	8051h
struct PNG CHUNK chunk[6]	IDAT (Critical, Pu...	A05Dh
struct PNG CHUNK chunk[7]	IDAT (Critical, Pu...	C069h
struct PNG CHUNK chunk[8]	IDAT (Critical, Pu...	E075h
struct PNG CHUNK chunk[9]	IDAT (Critical, Pu...	10081h

第二个chunk

1.png.png X

编辑方式: 十六进制(H) 运行脚本 运行模板: PNG.bt

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
F3	98	92	75	32	99	83	AE	45	C5	1A	47	2E	2F	A5	23	6"tu2"foEA.G./Y#
1F	17	C0	07	E6	C0	C5	F8	8A	71	39	F0	A6	11	C3	F3	..A.aAAoSq98 .A6
CF	EC	45	2A	91	F4	FF	78	54	00	00	20	00	49	44	41	IiE*\9xT,..IDA
54	BD	07	3F	FB	E9	E3	48	24	D5	D2	A9	52	81	0E	93	T%.?uEeAHG00ER.."
2C	AE	BD	FE	6A	9C	3C	31	8D	3D	CF	EF	C7	3	D7	5D	,@*8jce<1.=IiC5*]
8B	8D	5B	56	41	33	E9	E1	74	F0	DC	B3	2F	E3	A7	8F	<.[VA3eAt8U'/a\$.
ED	86	A6	5B	C8	76	77	63	71	89	D6	3F	1F	D9	EE	01	it+;[E'vwccq%0?.Ui.
C9	22	(5C)	8A	E5	05	3E	BA	7B	7A	D0	DB	D7	2F	A2	10	E'\8a.>{z8U*/c.
27	F7	1B	35	2E	FE	25	53	08	90	4E	77	A3	3B	DB	25	'+.5.p%S..NwL;U%
4A	33	23	34	87	73	E5	41	2F	66	1C	4E	A3	29	4F	D6	J3#4+sAA/f.NL)O0
AA	D6	2A	A2	C6	52	15	9D	58	3D	8E	E9	E9	53	12	F1	*0*cER..X=Z'eEs.n
49	DF	7E	FD	DD	EF	44	36	9D	C1	B7	BE	F5	4D	69	A1	IB~yYiD6.A.*8Mi;
FC	CD	A7	EF	93	CC	F9	9D	EF	7E	17	F7	DF	7F	3F	AA	uI8i"iù.i~.÷B.?*
F5	92	1A	81	D1	35	24	E3	69	AC	1F	1F	C7	15	97	5E	8'..N59ai~.C.^
89	4B	2E	B9	0C	F9	42	09	8F	3F	BE	1B	07	0F	BC	2A	%K.?.ùB.?.%..%*
76	2B	3E	DB	63	EB	96	F5	78	DB	DB	EE	C2	9A	B5	E3	v+>Ucè-8x00iAšpã
F8	CE	77	BE	8B	1F	FE	8E	7B	32	7D	FF	E7	7F	FE	09	øIw%<.pè{2}ÿc.p.
6C	BC	F4	72	B8	95	0A	22	11	13	3F	7F	7A	2F	3E	FE	l*4r,*. "...z./>p
D1	8F	62	E5	8A	11	6C	BB	F8	52	8C	8E	F6	63	F7	E3	N.bâS.l»8RZ8cc+ã
8F	E3	F5	63	C7	E5	7A	EF	D8	B6	45	A6	2F	38	C5	F2	.ã8cÇãzi0QE;/8A0
D4	53	4F	E1	9D	EF	BA	07	EF	FE	C3	8F	C2	9E	5E	44	0SOá.i°.ipã.ãz^D
6C	E5	18	9A	D3	A7	B1	FB	89	A7	F0	C0	B7	BE	2B	81	lã.s0S±ùw\$8À.*+
E1	3D	F7	DE	8B	35	6B	C6	F1	85	2F	7E	09	47	5F	3F	ã=÷B<5kEñ/~.G.?
2A	03	08	BD	7D	DD	F2	A8	04	66	FA	AE	74	17	DE	FD	*..%}Yò".fú@t.Éý
9E	77	E1	8A	AB	76	C1	4C	E5	80	7A	09	A5	7C	1E	D9	žwãS«vãLãEz.¥ .Û
15	23	40	B9	88	2F	7F	F1	8B	78	FA	A9	DD	88	99	51	.#è+^/.ñk xú@Y^MQ
FC	EA	8D	37	E1	FA	EB	DF	24	ED	1D	26	00	8E	A2	69	üe.7áúE89i.ã.zci
91	98	3C	60	47	AD	5D	91	E9	03	19	B7	63	9D	CB	3D	'<`G-]`é...c.È=
B4	2C	79	62	89	A8	94	15	2D	96	4F	54	FD	65	4D	A8	'yB%"/.--OTyEM"
26	01	82	9B	CD	69	E4	E0	0F	70	D4	4F	32	A3	99	80	ã.,>iãã.p002fE

工作区

- 打开的文件
 - 1.png.png C:\Users\真拿你没办法...ures\CSDN博客\脚本\
 - BMP.bt C:\Users\真拿你没办法\Do...plates\Repository\
 - PCAP.bt C:\Users\真拿你没办法\Do...plates\Repository\
 - PNG.bt C:\Users\真拿你没办法\Do...plates\Repository\
 - WAV.bt C:\Users\真拿你没办法\Do...plates\Repository\
 - ZIP.bt C:\Users\真拿你没办法\Do...plates\Repository\
 - 模板1.bt
- 收藏的文件
- 最近的文件
 - What kin...is this_ C:\Users\真拿你没办法(P...客\buu\attachment\
 - attachment.jpeg C:\Users\真拿你没办法...ures\CSDN博客\buu\
 - vip.m4a C:\Users\真拿你没办法\Pi...ttachment\tmp\vip\
 - 派大星的烦恼.bmp C:\Users\真拿你没办法(P...7df-e271b4826ce8\
 - 我是A.doc C:\Users\真拿你没办法...1ce37e66\粽子的来历\
 - 我是B.doc C:\Users\真拿你没办法...1ce37e66\粽子的来历\
 - attachment.png C:\Users\真拿你没办法...ures\CSDN博客\buu\

资源管理器

变量

名称	值	开始	
uint32 ctype	49444154h	2031h	4
> char cname[4]	IDAT	2031h	4
> ubyte data[8192]		2035h	2
uint32 crc	F4FF7854h	4039h	4
▼ struct PNG_CHUNK chunk[3]	IDAT (Critical, Pu...	4039h	2
> uint32 length	8192	4039h	4
> union CTYPE type	IDAT	403Dh	4
> ubyte data[8192]		4041h	2
uint32 crc	3000020h	6041h	4
> struct PNG_CHUNK chunk[4]	TSZ (Critical, Pr...	6045h	2
> struct PNG_CHUNK chunk[5]	TSZ (Critical, Pr...	8051h	2

https://blog.csdn.net/qq_51090016

两个改完就可以正常打开了



真的很杂

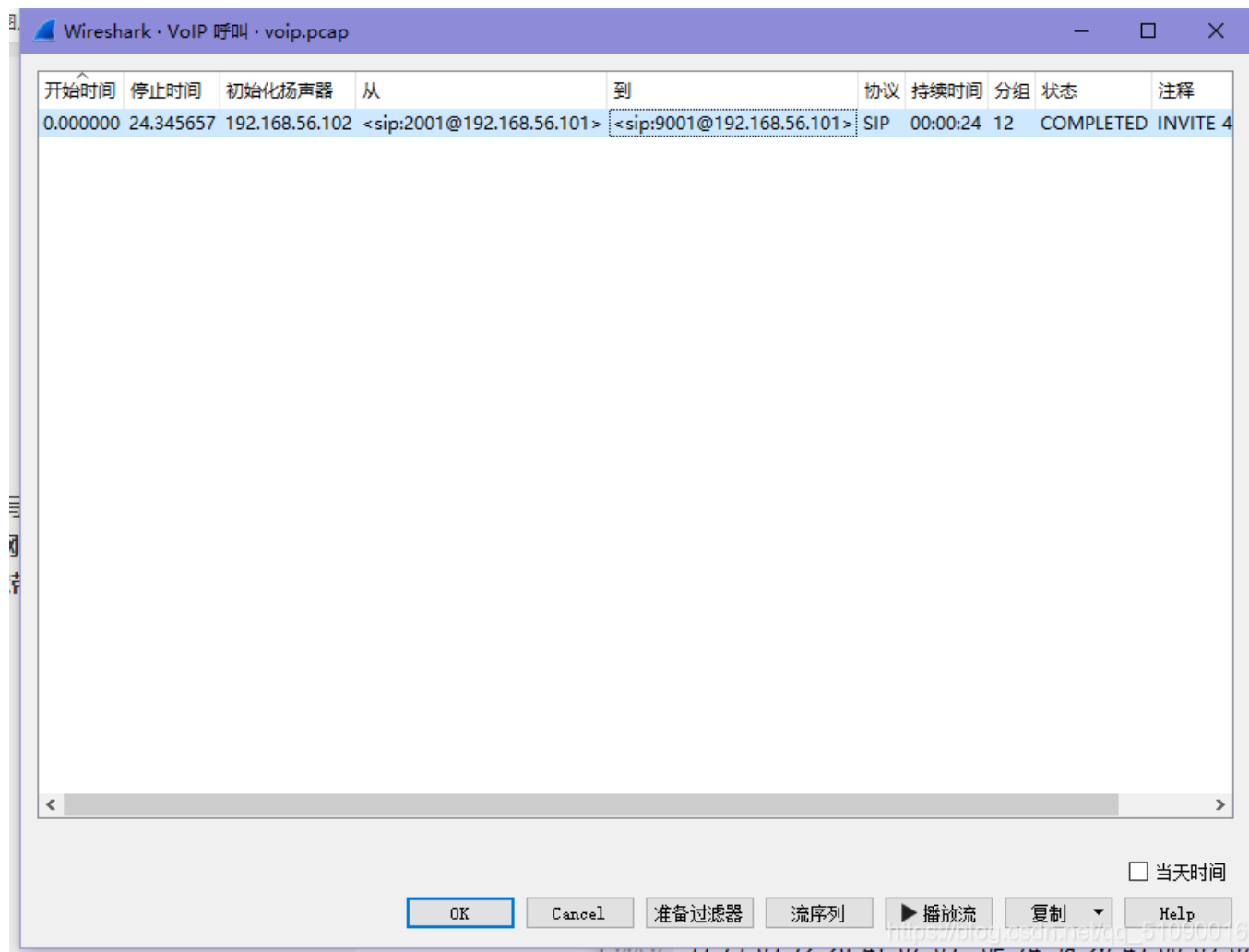
这题暂时先放着把。。

voip (Wireshark抓取RTP包)

啥是voip?

VoIP——基于IP的语音传输（英语：**Voice over Internet Protocol**，缩写为**VoIP**）是一种语音通话技术，经由网际协议（IP）来达成语音通话与多媒体会议，也就是经由互联网来进行通信。其他非正式的名称有**IP电话（IP telephony）**、**互联网电话（Internet telephony）**、**宽带电话（broadband telephony）**以及**宽带电话服务（broadband phone service）**

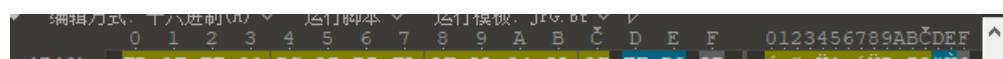
直接主菜单点击 电话——>VoIP电话 就可以听到声音



[MRCTF2020]pyFlag(拼接出来一个文件)



正常从图片入手，搜pk的时候在文件末尾发现了一个secret file，每个图片都有，提取出来组成一个zip



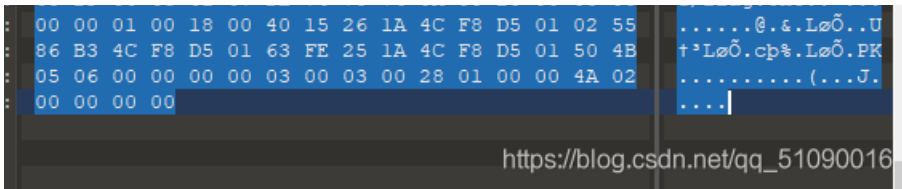
```
4750h: 53 65 63 72 65 74 20 46 69 6C 65 20 50 61 72 74 Secret File Part
4760h: 20 31 3A 5D 50 4B 03 04 14 00 00 00 00 00 54 88 1:]PK.....T^
4770h: 6C 50 00 00 00 00 00 00 00 00 00 00 00 00 0B 00 lP.....
4780h: 00 00 53 65 63 72 65 74 46 69 6C 65 2F 50 4B 03 ..SecretFile/PK.
4790h: 04 14 00 09 00 08 00 74 86 6C 50 F9 1A 23 EB DF .....t!Pù.#èß
47A0h: 00 00 00 E3 00 00 14 00 00 00 53 65 63 72 65 ...ã.....Secre
47B0h: 74 46 69 6C 65 2F 2E 68 69 6E 74 2E 74 78 74 D2 tFile/.hint.txtÖ
47C0h: D0 98 8C 59 64 4C 2A 21 4D 96 C0 5F 09 FE 93 67 ð*(YdL*!M-À .p"q
47D0h: 3A 9D 5D FE 1C C9 8E 6A 97 D9 F3 48 D5 FD 22 F0 :.]p.Éžj-ÛöHÖý"ð
47E0h: 36 F6 9F 89 C1 F9 3E A2 00 DC 69 B0 FD 3E 58 3D 6öYkÀù>ç.Ûi°ý>X=
47F0h: 20 43 6F 6B 0A 66 63 EC B8 D9 22 93 63 A4 55 35 {ok.fcì,Û""çwU5
4800h: 28 4C 51 2A A9 BD A8 86 09 B1 70 E5 52 D0 78 29 (LQ*®%:†.±pãRðx)
4810h: 3C 95 FD AB 42 97 9A DA E1 63 A9 6F FA 86 CD C9 <*ý«B-šÛácöou†iÉ
4820h: 0B 34 F2 D3 68 1E A8 0F 67 4E 77 9D C6 BC 98 03 .4òh. ".gnw.Æ* ".
4830h: 22 8D E5 24 F6 3B 3E 93 11 0B 6E 2E 2E FB 38 9A ".À$ö;>".n.û8š
4840h: 1F 40 47 A3 D8 63 FD 32 9F AE C9 6A 42 E2 60 A7 .@G£öcy2YöÉjBà`$
4850h: 5D 78 44 88 1D 21 F4 AC 20 88 2C 51 FD 99 8A 22 ]xD^.!ð~^,Qý™$"
4860h: 31 51 A5 DD A3 52 4E CD 82 FE 1D 0E 68 D7 B1 2D lQ¥Y£RNÍ,p.~h×±-
4870h: 6B 10 C5 8B 29 C4 E3 D2 5C AE 86 54 C7 44 65 23 k.Å<)Äãò\@†TÇDe#
4880h: 75 3D 42 5A FD E8 89 3D 70 B8 FB 07 A7 22 1F 1A u=BZýèk=p.ù.$"..
4890h: EC 11 91 48 D2 E0 6C FD EF 09 3D F2 A6 27 50 4B i.'Höälýi.=ð!'PK
48A0h: 03 04 14 00 09 00 00 00 0B 87 6C 50 B6 2F 9E CA .....+lPq/žË
48B0h: DF 00 00 00 68 01 00 00 13 00 00 53 65 63 72 ß...h.....Secr
48C0h: 65 74 46 69 6C 65 2F 66 6C 61 67 2E 74 78 74 19 etFile/flag.txt.
48D0h: 3A A9 27 82 33 A6 C7 54 5D 93 5F D7 80 8E DB 94 :@',3!ÇT)"_×éŽÛ"
48E0h: 73 47 BE 28 9D 22 38 6A 60 6F 28 B8 sG*(."8j`o(.
```

https://blog.csdn.net/qq_51090016

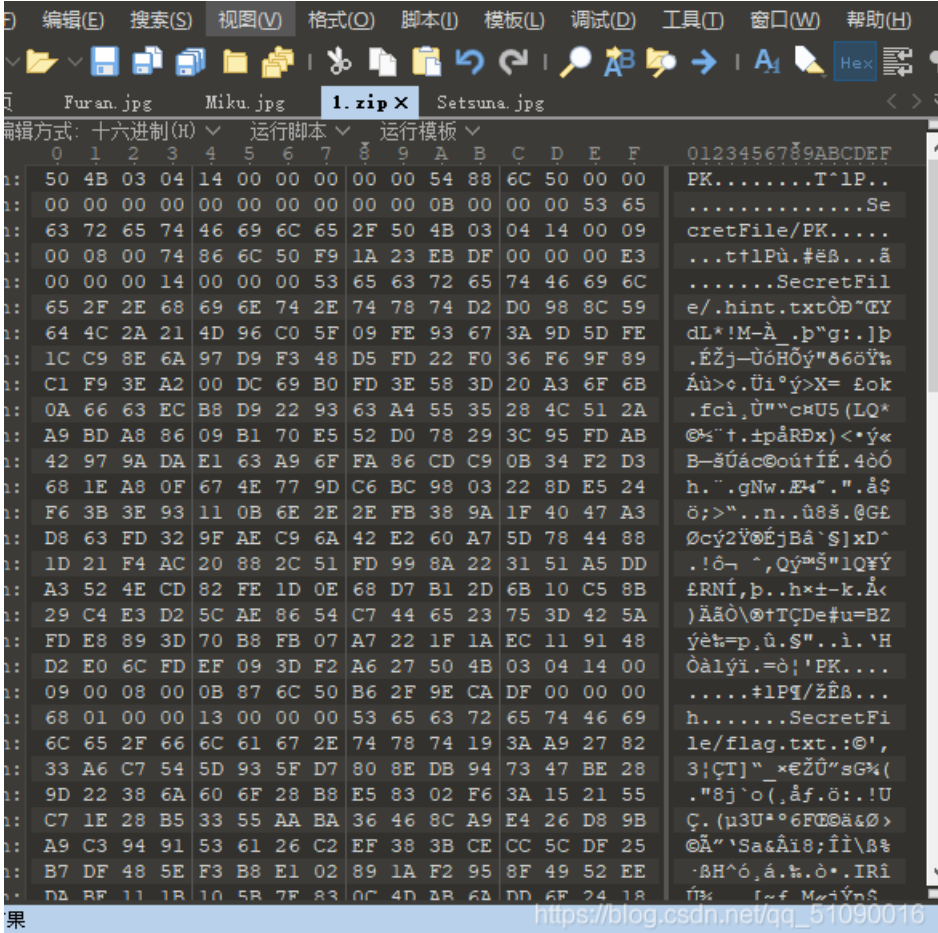
```
起始页 Furan.jpg x Miku.jpg l.zip Setsuna.jpg
编辑方式: 十六进制(H) 运行脚本 运行模板: JPG.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDE F
:6B60h: 60 6A F8 5F FE 46 3D 24 76 3A 95 B7 FE 8C 14 8A `jø_pF=$v:·pç.Š
:6B70h: 87 C4 BD 4D 5F 19 92 FE 30 D7 CB 73 FF 00 13 19 +Ä~M_.'p0*Èsý...
:6B80h: FF 00 F4 2A 45 3D 5B 38 E9 00 0E 40 F5 A6 64 F7 ý.ð*E=[8é..@ð|d÷
:6B90h: 24 80 07 95 55 B9 14 3D 87 1D CB 00 05 24 0F 53 $€.·U*. =+.È..$.S
:6BA0h: 40 CB 56 9D 5A 93 2A 24 7A 9B B0 48 90 1F 95 DB @ÉV.Z"*$z>°H..·Û
:6BB0h: E6 F7 A2 22 A8 F4 44 40 00 30 29 88 FF D9 5B 53 æ:ç""ðD(0.)^ÿÛ[S
:6BC0h: 65 63 72 65 74 20 46 69 6C 65 20 50 61 72 74 20 ecret File Part
:6BD0h: 32 3A 5D E5 83 02 F6 3A 15 21 55 C7 1E 28 B5 33 2:]Åf.ö:!.!UÇ.(µ3
:6BE0h: 55 AA BA 36 46 8C A9 E4 26 D8 9B A9 C3 94 91 53 U*°6Fç@a&ø>eÄ""\s
:6BF0h: 61 26 C2 EF 38 3B CE CC 5C DF 25 B7 DF 48 5E F3 a&Äi8;îi\Bk·BH^ó
:6C00h: B8 E1 02 89 1A F2 95 8F 49 52 EE DA BE 11 1B 10 .á.ñ.ò·IRiÜ%...
:6C10h: 5B 7E 83 0C 4D AB 6A DD 6E 24 18 D5 CE C1 E4 1B [~f.MæjYn$.öíÄä.
:6C20h: 6B 97 36 66 5E 6A 13 41 37 FC CA E0 F6 A5 A7 4A k-6f^j.A7üÈàø¥$J
:6C30h: C5 89 AD 12 B2 0A AF BD CB AC 23 04 8C E9 44 3E Äñ-. ".ÿÈ-#.ÇéD>
:6C40h: C8 FE 46 36 2F 8C 36 8C 81 F9 A6 61 9C B2 0E C1 ÈpF6/Ç6E.ù|æç.Ä
:6C50h: 9E B5 93 A6 10 F9 00 DB 24 E5 F3 30 BC 19 EB 67 žm"! .ù.Ûšãö04.ég
:6C60h: 1C C6 46 83 01 24 25 17 CC E3 84 C7 69 0D 09 04 .ÆFf.$.§.îÄ.,Çi...
:6C70h: 73 E3 A9 AC 84 57 1B B2 61 32 B0 AE 03 26 C4 A3 sã@~.W."a2°ø.ãÄÉ
:6C80h: 6F A3 4C 3F 48 87 FB F0 D1 EC E3 10 F7 35 D8 27 o&L?H+ú8Ñiä.+5ø'
:6C90h: 22 DD 56 99 90 50 4B 01 02 14 00 14 00 00 00 00 "ÝV™.PK.....
:6CA0h: 00 54 88 6C 50 00 00 00 00 00 00 00 00 00 00 .T^lP.....
:6CB0h: 00 0B 00 24 00 00 00 00 00 00 10 00 00 00 00 ...$.
:6CC0h: 00 00 00 53 65 63 72 65 74 46 69 6C 65 2F 0A ...SecretFile/.
```

https://blog.csdn.net/qq_51090016

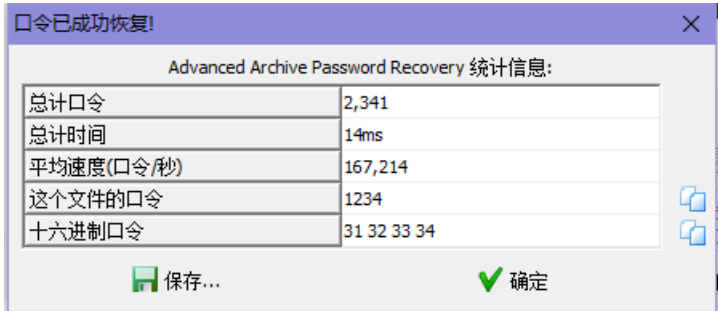
```
:09 9A 42 68 20 FA 1A 61 CF A1 A0 40 4E 69 28 C1 .šBh ú.aĩ; @Ni(Ä
F4 34 60 FA 1A 05 70 A2 8C 1F 43 46 0F A1 A0 61 ó4`ú..pç.CF.; a
45 18 3E 86 (8C) 1F 43 40 1F FF D9 5B 53 65 63 72 E.>|Ç|.ÿÛ[Secr
:65 74 20 46 69 6C 65 20 50 61 72 74 20 33 3A 5D et File Part 3:]
:00 20 00 00 00 00 01 00 18 00 81 37 39 FB 4C .....79úL
F8 D5 01 BB D9 0E FC 4C F8 D5 01 00 2E AD 19 36 øÖ.×Û.uLøÖ...-6
F8 D5 01 50 4B 01 02 14 00 14 00 09 00 08 00 74 øÖ.PK.....t
86 6C 50 F9 1A 23 EB DF 00 00 00 E3 00 00 00 14 t!Pù.#èß...ã....
:00 24 00 00 00 00 00 02 00 00 00 29 00 00 .$.
:00 53 65 63 72 65 74 46 69 6C 65 2F 2E 68 69 6E .SecretFile/.hin
74 2E 74 78 74 0A 00 20 00 00 00 00 01 00 18 t.txt.....
:00 A7 8A 4F 71 4B F8 D5 01 A8 8A 4F 71 4B F8 D5 .šŠOqKøÖ. "šOqKøÖ
:01 00 B0 20 A8 34 F8 D5 01 50 4B 01 02 14 00 14 ..° "4øÖ.PK.....
:00 09 00 08 00 0B 87 6C 50 B6 2F 9E CA DF 00 00 .....+lPq/žËß...
:00 68 01 00 00 13 00 24 00 00 00 00 00 00 80 .h.....$.
:00 00 00 3A 01 00 00 53 65 63 72 65 74 46 69 6C .....SecretFil
:65 2F 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00 e/flag.txt.....
```



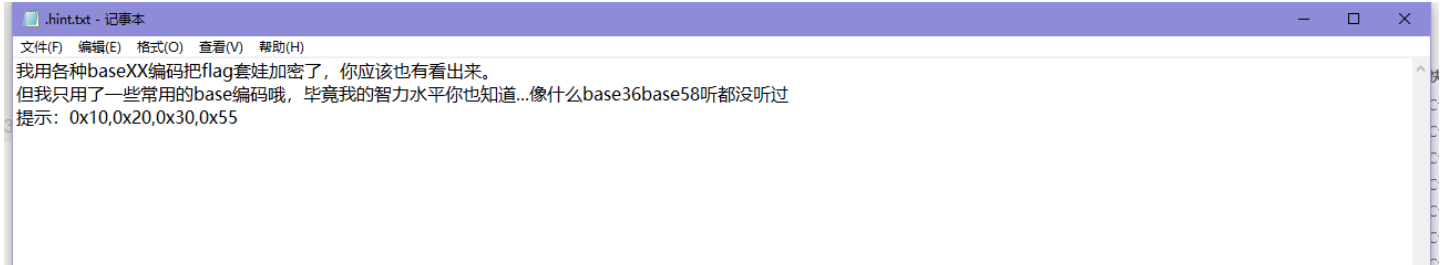
复制出来得到:



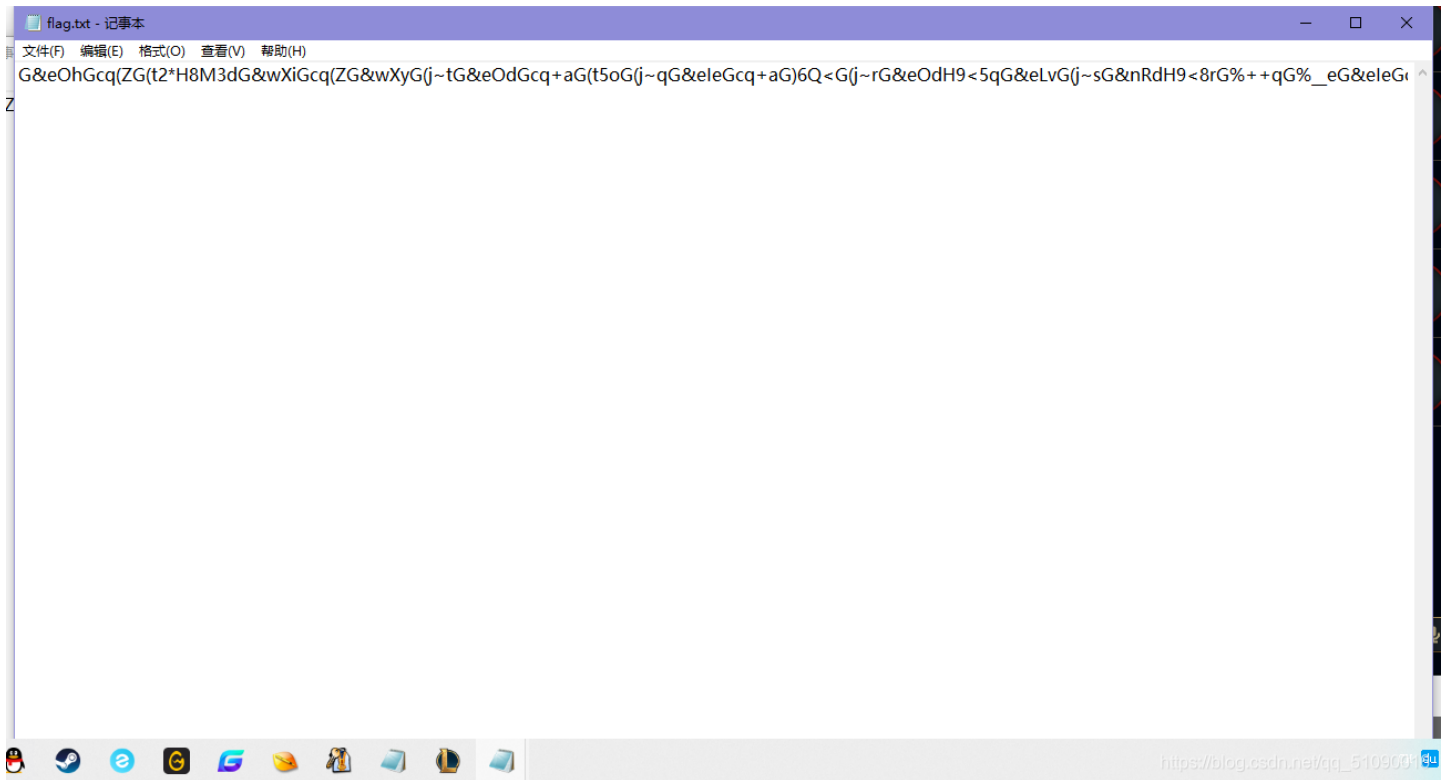
解压需要密码，爆破



得到两个txt文件，看hint



再看flag.txt



根据提示，会有的base解码：16，32，48，85（16进制转10进制）

用脚本：

```
#!/usr/bin/env python

import base64
import re

def baseDec(text,type):
    if type == 1:
        return base64.b16decode(text)
    elif type == 2:
        return base64.b32decode(text)
    elif type == 3:
        return base64.b64decode(text)
    elif type == 4:
        return base64.b85decode(text)
    else:
        pass

def detect(text):
    try:
        if re.match("[^0-9A-F=]+$",text.decode()) is not None:
            return 1
    except:
        pass

    try:
        if re.match("[^A-Z2-7=]+$",text.decode()) is not None:
            return 2
    except:
        pass

    try:
        if re.match("[^A-Za-z0-9+/=]+$",text.decode()) is not None:
            return 3
    except:
        pass

    return 4

def autoDec(text):
    while True:
        if b"MRCTF{" in text:
            print("\n"+text.decode())
            break

        code = detect(text)
        text = baseDec(text,code)

with open("flag.txt",'rb') as f:
    flag = f.read()

autoDec(flag)
```

就行了

Business Planning Group (010搜索iend bpg图像格式)

010打开后搜索iend (PNG图像的图像结束数据 (IEND))


```
0h: 72 61 74 65 64 31 6C FF 6D 00 00 00 19 74 45 58 ratedlym....tEX
0h: 74 69 63 63 3A 64 65 73 63 72 69 70 74 69 6F 6E ticc:description
0h: 00 41 70 70 6C 65 20 52 47 42 BC 75 FC FB 00 00 .Apple RGB
0h: 00 1A 74 45 58 74 69 63 63 3A 6D 61 6E 75 66 61 ..tEXticc:manufa
0h: 63 74 75 72 65 72 00 41 70 70 6C 65 20 52 47 42 cturer.Apple RGB
0h: 99 20 15 0B 00 00 00 13 74 45 58 74 69 63 63 3A ..tEXticc:
0h: 6D 6F 64 65 6C 00 41 70 70 6C 65 20 52 47 42 7C model.Apple RGB|
0h: 31 AB CA 00 00 00 00 49 45 4E 44 AE 42 60 82 42 IEND...IEND0B`B
0h: 50 47 FB 30 00 8B 47 86 3C 00 03 92 47 40 03 92 PG0...G@.'
0h: 47 40 44 09 C1 71 83 12 00 00 00 01 44 01 C1 71 G@D.Áqf....D.Áq
0h: 83 12 00 00 01 26 09 AF 8D 2E 62 F7 39 AC 62 D6 f....&...b-9-b0
0h: B5 C0 B5 ED 07 AB E1 17 B6 F2 D8 11 23 A0 00 00 µÁpi.«á.řòø.# ..
0h: 03 00 00 03 00 00 03 03 A4 8E E2 6C B8 CF 0B A4 9B 24 87 41 59 09 016
0h: 6A 74 00 00 03 00 00 03 00 03 A9 F1 18 94 9E 3A jc.....@n. zz
```

发现bpg

BPG (新的图像格式)

- 编辑
- 讨论
- 上传视频

本词条缺少概述图，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！

BPG (Better Portable Graphics, 更好的可移植图形) 是一种新的图像格式。它的目的是在质量或文件大小有问题时替换jpeg图像格式。

中文名	更好的可移植图形	编写	BPG
外文名	Better Portable Graphics	同类项	JPEG等图片格式

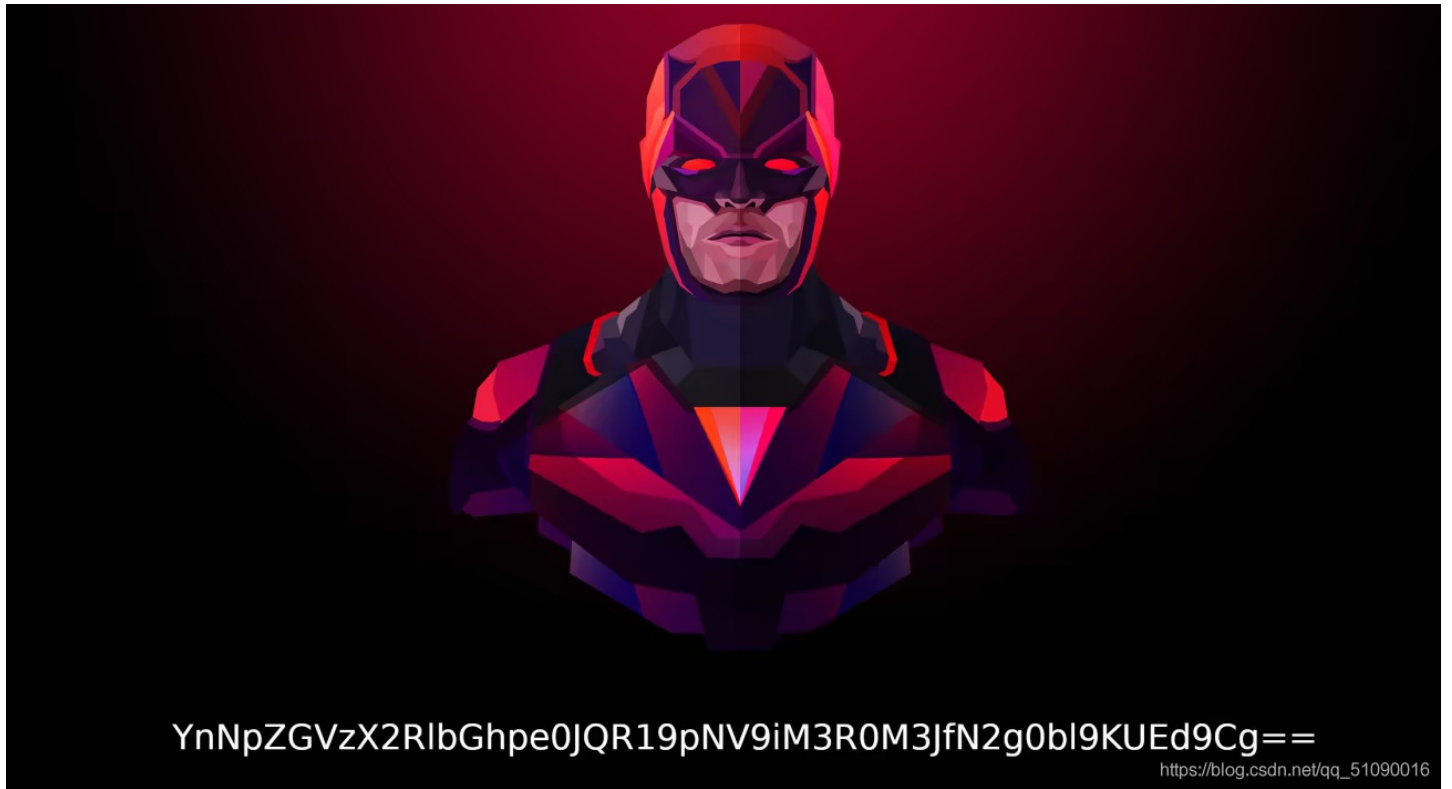
BPG (更好的可移植图形) 是一种新的图像格式。它的目的是在质量或文件大小有问题时替换jpeg图像格式。其主要优点是：

- 高压缩比。对于类似的质量，文件比jpeg小得多。
- 大多数Web浏览器都支持小型的javascript解码器 (gzipped大小: 56kb)。
- 基于HEVC开放视频压缩标准的子集。
- 支持与jpeg相同的色度格式 (灰度, ycbcr 4:2:0, 4:2:2, 4:4:4), 以减少转换过程中的损失。支持alpha通道。还支持RGB、YCGCO和CMYK颜色空间。
- 本机支持每个通道8到14位, 以获得更高的动态范围。
- 支持无损压缩。
- 可以包含各种元数据 (如exif、icc profile、xmp)。
- 动画支持。 [1]

https://blog.csdn.net/qq_51090016

将这些数据另存出来为bpg文件, 发现Windows的图像软件不能直接打开, 网上能打开的工具

<https://bellard.org/bpg/>



base64解密即可

[GWCTF2019]huyao（频域盲水印隐写）

看到两张一样的图片，想到盲水印，但这里用BlindWaterMark还不行，看wp知道是频域盲水印隐写，用脚本

```

# coding=utf-8
import cv2
import numpy as np
import random
import os
from argparse import ArgumentParser
ALPHA = 5

def build_parser():
    parser = ArgumentParser()
    parser.add_argument('--original', dest='ori', required=True)
    parser.add_argument('--image', dest='img', required=True)
    parser.add_argument('--result', dest='res', required=True)
    parser.add_argument('--alpha', dest='alpha', default=ALPHA)
    return parser

def main():
    parser = build_parser()
    options = parser.parse_args()
    ori = options.ori
    img = options.img
    res = options.res
    alpha = options.alpha
    if not os.path.isfile(ori):
        parser.error("original image %s does not exist." % ori)
    if not os.path.isfile(img):
        parser.error("image %s does not exist." % img)
    decode(ori, img, res, alpha)

def decode(ori_path, img_path, res_path, alpha):
    ori = cv2.imread(ori_path)
    img = cv2.imread(img_path)
    ori_f = np.fft.fft2(ori)
    img_f = np.fft.fft2(img)
    height, width = ori.shape[0], ori.shape[1]
    watermark = (ori_f - img_f) / alpha
    watermark = np.real(watermark)
    res = np.zeros(watermark.shape)
    random.seed(height + width)
    x = range(height / 2)
    y = range(width)
    random.shuffle(x)
    random.shuffle(y)
    for i in range(height / 2):
        for j in range(width):
            res[x[i]][y[j]] = watermark[i][j]
    cv2.imwrite(res_path, res, [int(cv2.IMWRITE_JPEG_QUALITY), 100])

if __name__ == '__main__':
    main()

```

得到



[UTCTF2020]File Carving

[GUET-CTF2019]soul sipse (音频隐写)

[UTCTF2020]spectrogram (奇怪的操作)

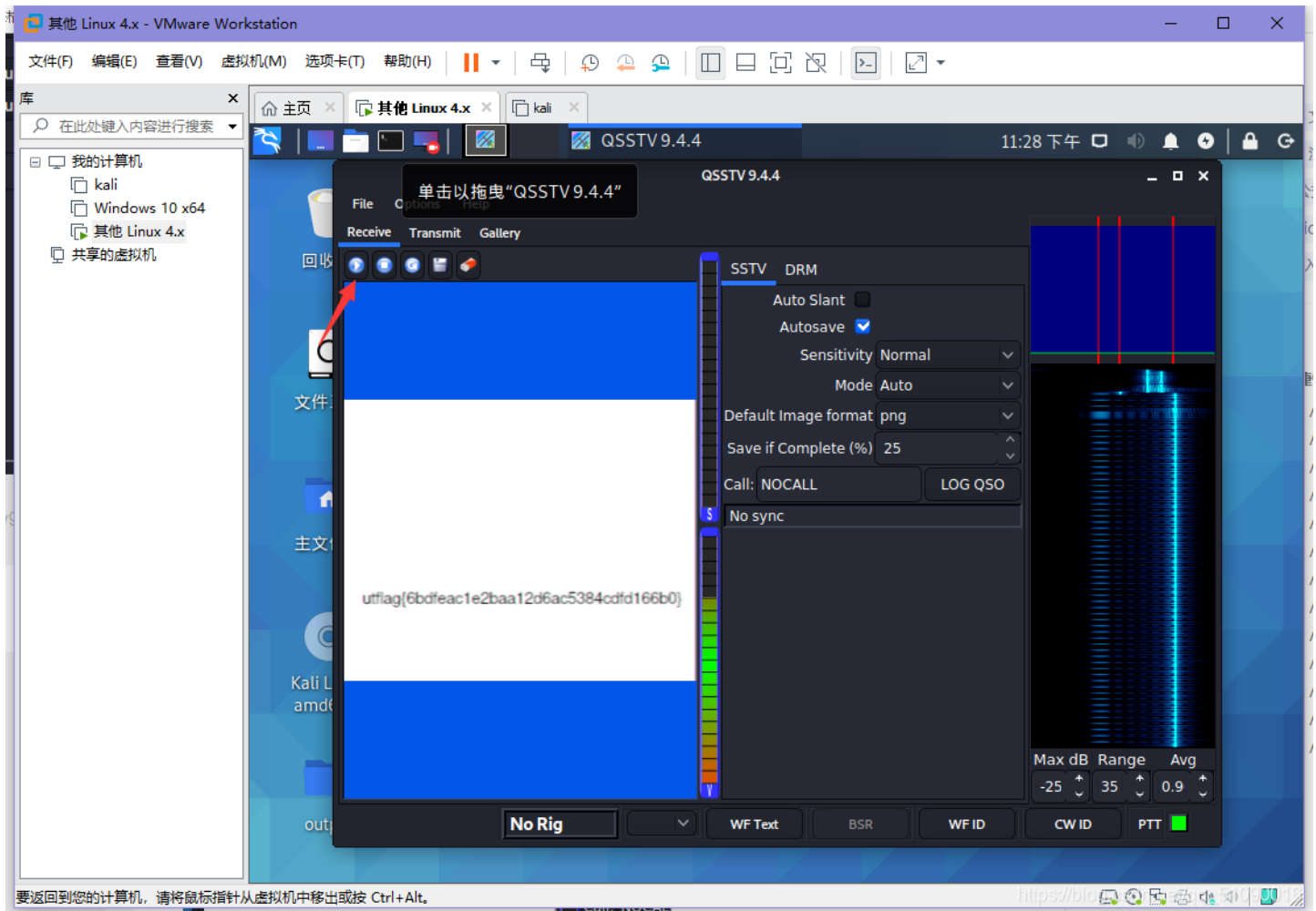
[UTCTF2020]sstv(qsstv)

kali打开qsstv

Options->Configuration->Sound勾选From file



点这个



我爱Linux(Python Pickle序列化内容)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)