【MISCshow misc30-misc5总结】

原创

Htt9999 已于 2022-03-25 09:34:27 修改 4640 收藏

分类专栏： CTFshow 文章标签： 网络安全

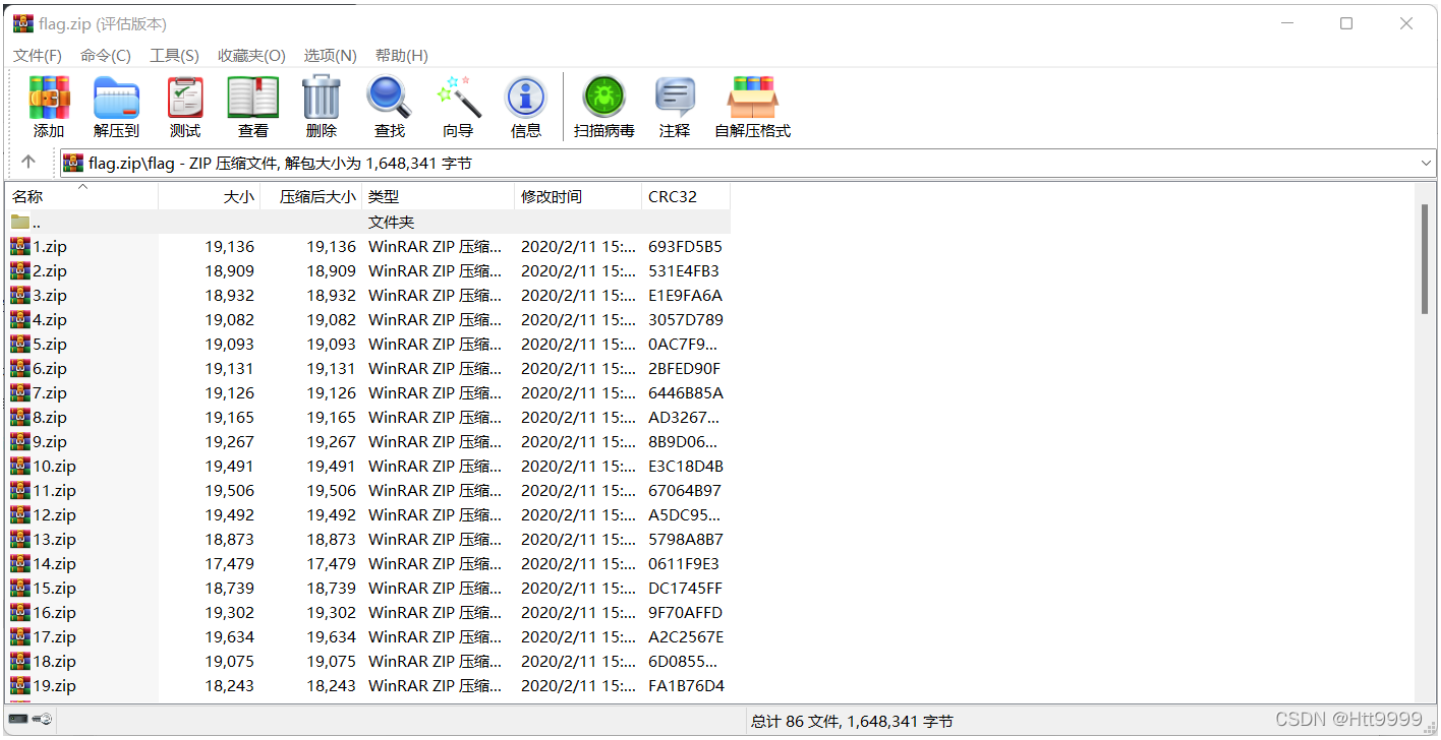
于 2022-03-23 22:20:37 首次发布

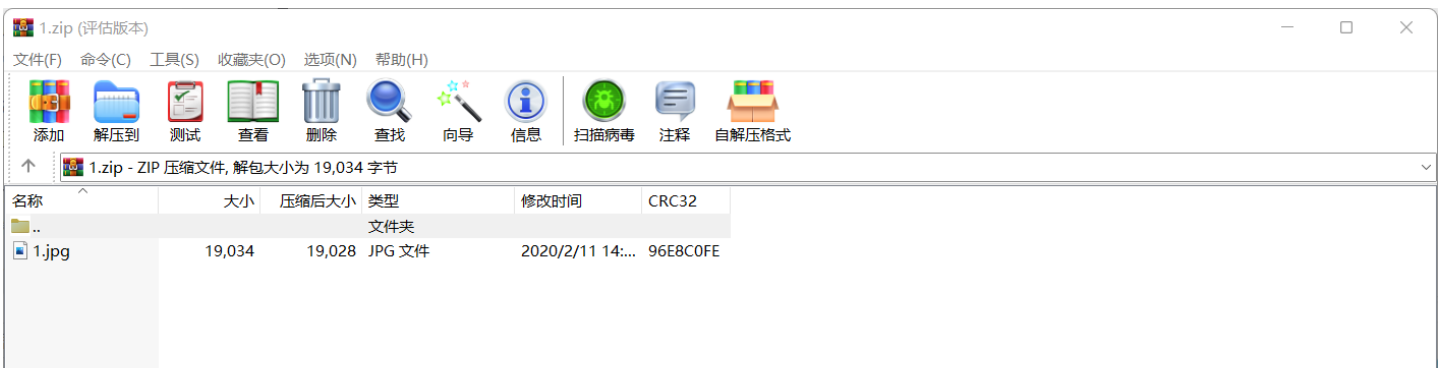
MISCshow总结

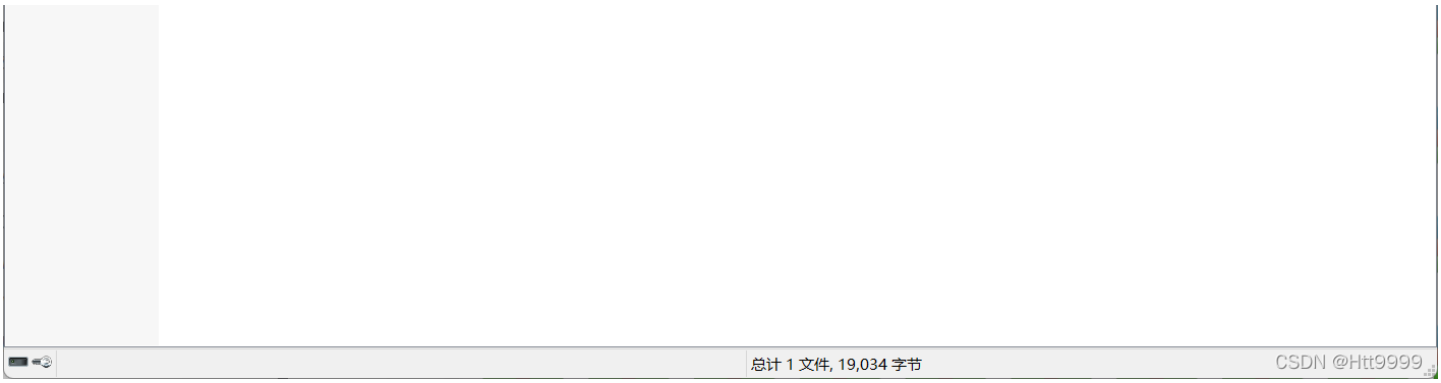
本文章均来自于CTFshowhttps://ctf.show/challenges#misc2-21

1· 红包第一弹

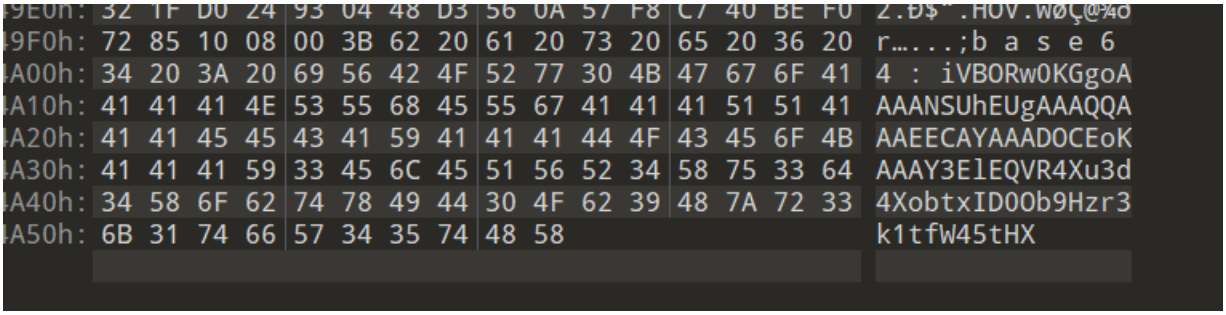
打开发现全是压缩包



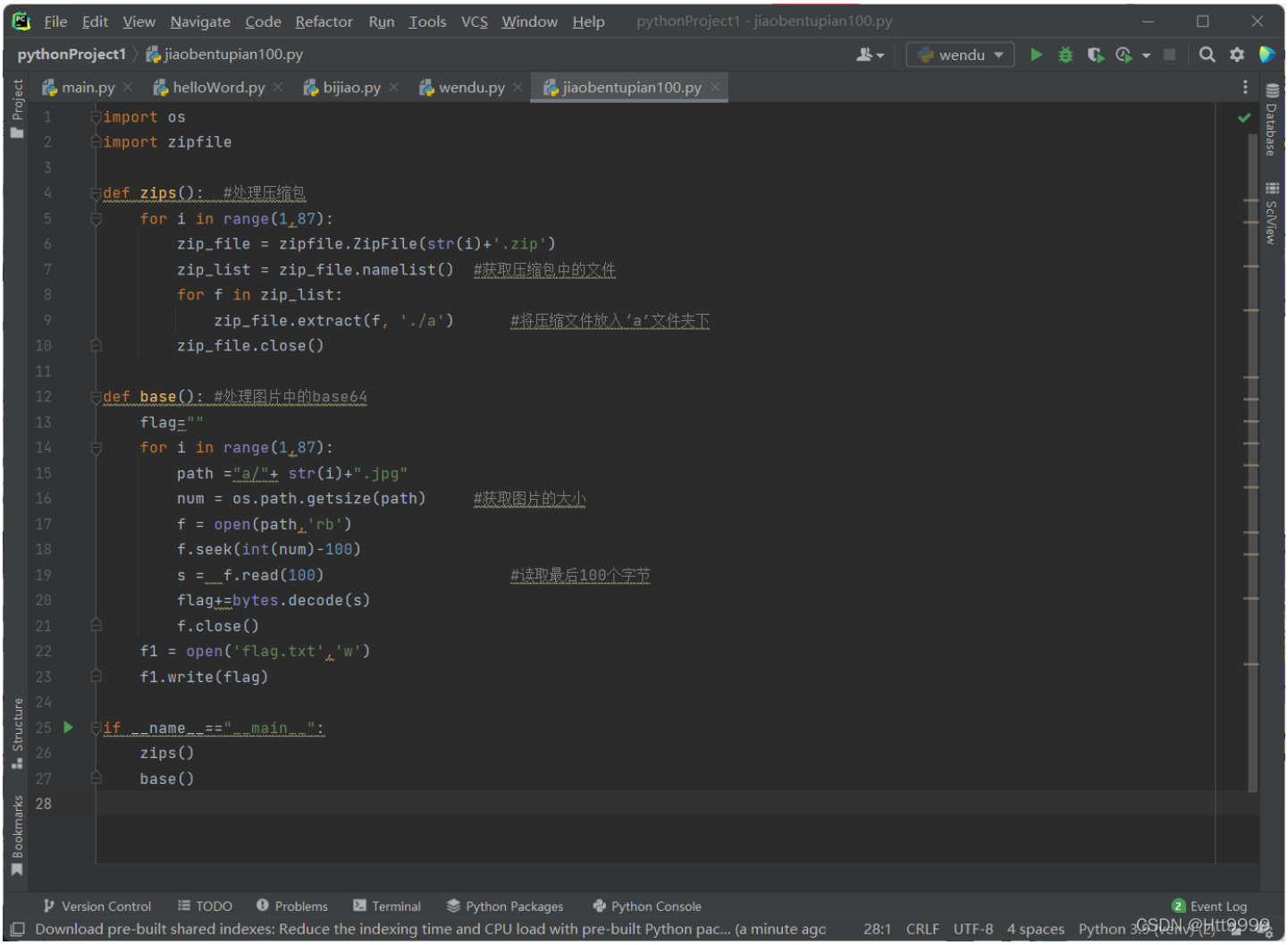




打开每个压缩包发现全是一张图片，用010editor打开第一张图片发现二进制的最后有一串base64的编码



由于图片比较多，直接脚本上手



process=image/watermark,type_d3F5LXplbmhlaQ,shadow_50,text_Q1NETiBASHR0dk5OQ==,size_20,color_FFFFFF,t_70,g_se,x_16

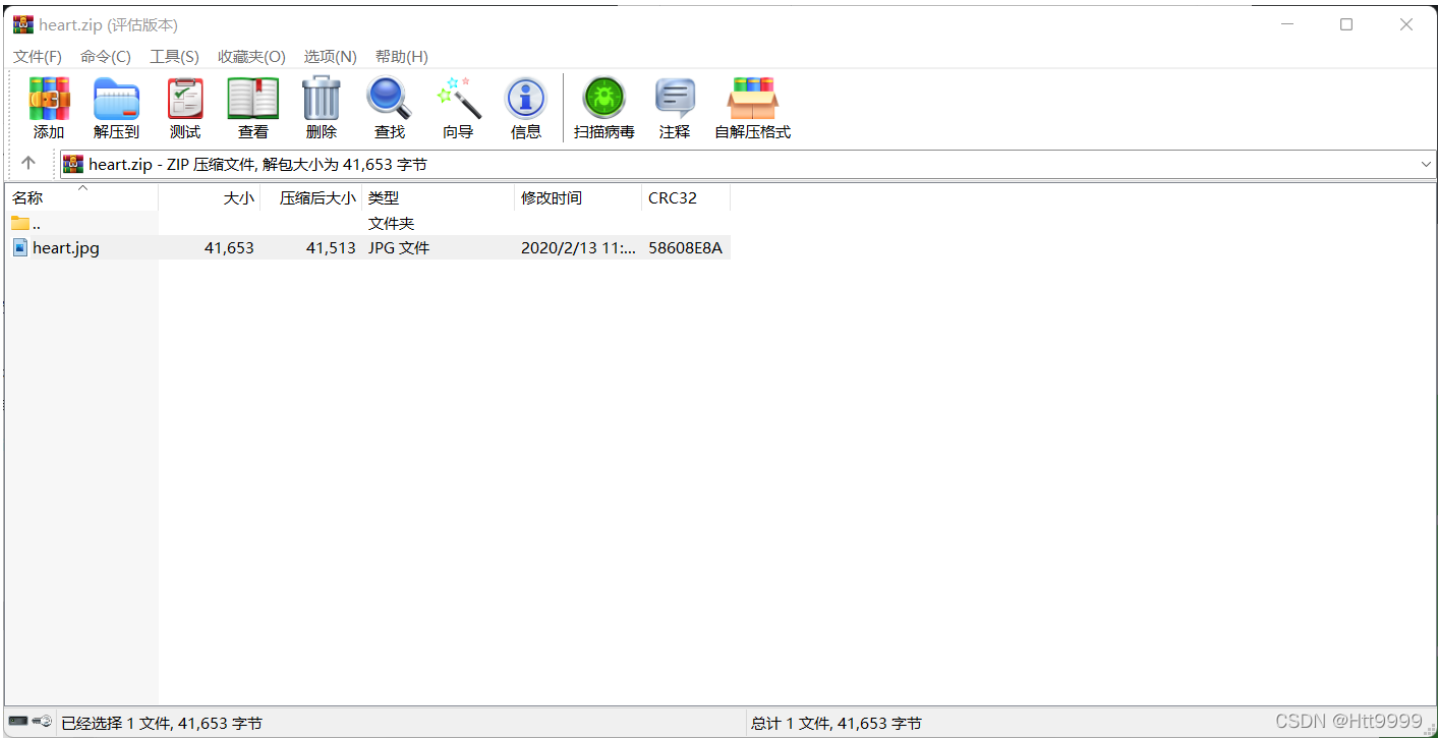
直接base64解码得到flag：flag{gif_is_so_easy}

**

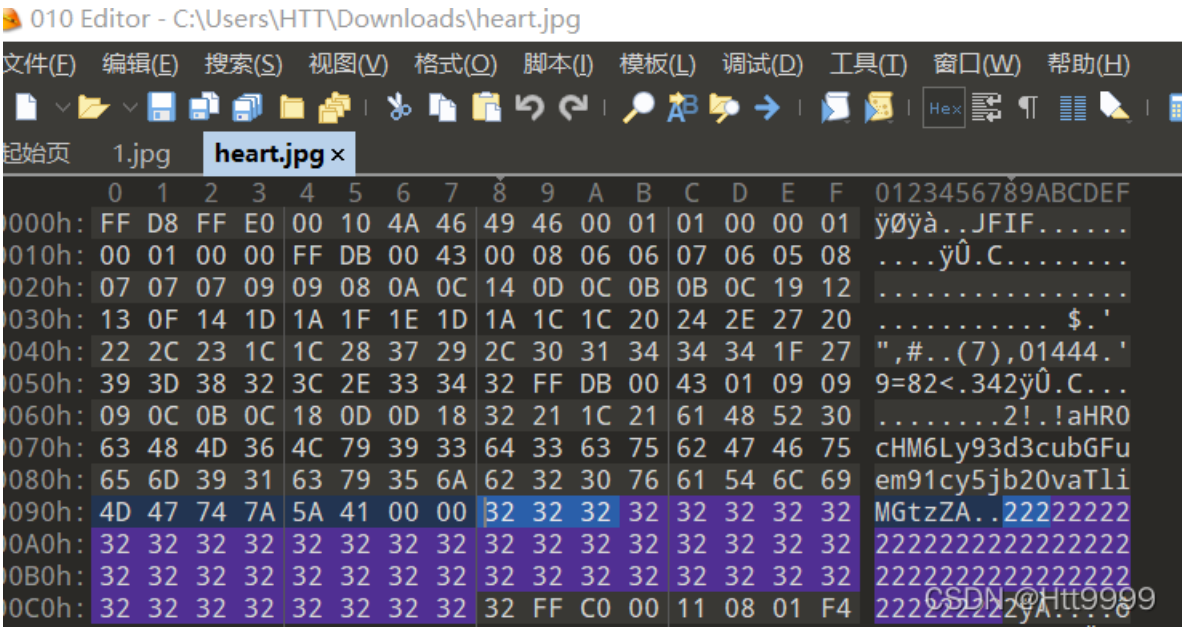
2·stega10

**

又是一个压缩包打开是一个图片



不用想直接010editor打开看看里面到底有啥

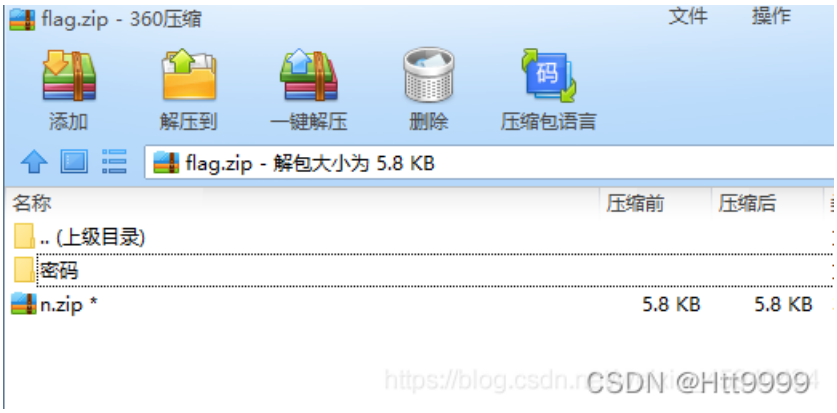


竟然发现了一串类似于base64的编码，解码之后是个网站

Output

```
https://www.lanzous.com/i9b0ksd
```


打开这个蓝奏云链接，我们下载到了一个加密的压缩包



直接爆破得到密码，成功解压出来n.png,但却无法打开
用010editor发现是个倒序的，Python脚本走起

```python
import re
import binascii

def read_file(filepath):
    with open(filepath,'rb') as fp:
        content=fp.read();
```

```python
    return content

#以二进制读取图片，并转为16进制
a = read_file('n.png')
hexstr = str(binascii.b2a_hex(a))
hexstr = re.findall("b'(.*?)'",hexstr)[0]

#每俩位分割成列表元素
result = []
result.append(re.findall(r'.{2}', hexstr))
result = result[0]

#按倒序排列，拼接列表为文本
daoxu = result[::-1]
hex= ''
for i in daoxu:
    hex +=i

print(hex)
```


得到一个二维码![在这里插入图片描述](https://img-blog.csdnimg.cn/d4870b31ccd445739b12defd287cd759.png?x-oss-process=image/watermark,type_d3F5LXplbmhlaQ,shadow_50,text_Q1NETiBASHR0OTk5OQ==,size_18,color_FFFFFF,t_70,g_se,x_16

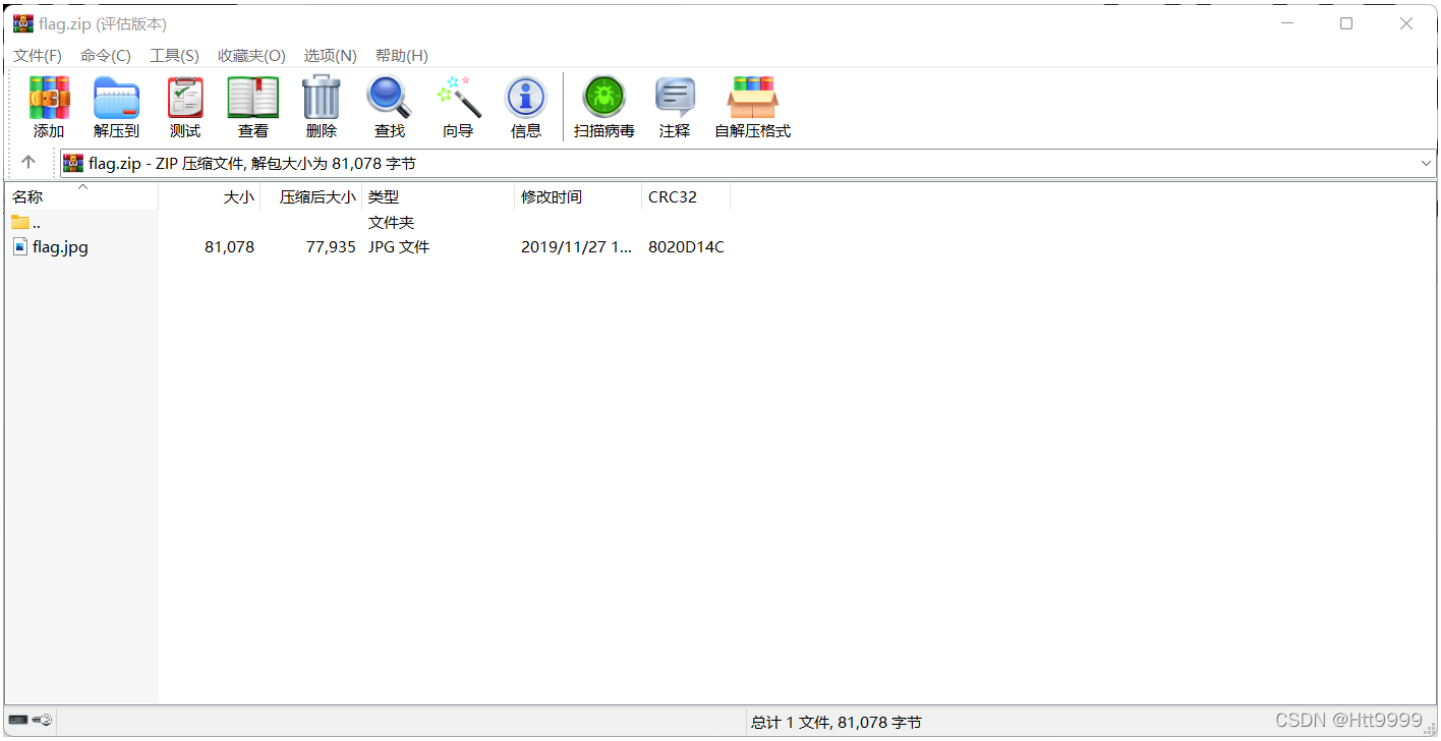
扫码得flag:flag{我好难啊}

**

3·stega11

**

打开压缩包是一个图片的格式



打开一看啥东西也没有直接010editor分析一波，发现了一串base64的一串代码，直接base起手，一个一个试，结果是base32

Input

```
ÿÙMZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJVHA4TONZYGA2DMM3FGMYH2ÿØÿà
```

Output

```
flag{6f1797d4080b29b64da5897780463e30}
```

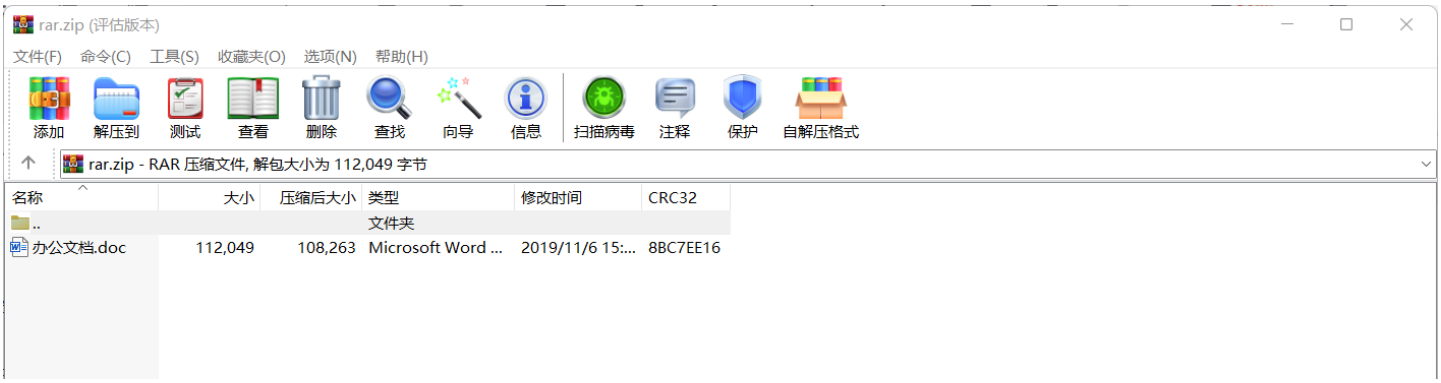

得到flag：flag{6f1797d4080b29b64da5897780463e30}

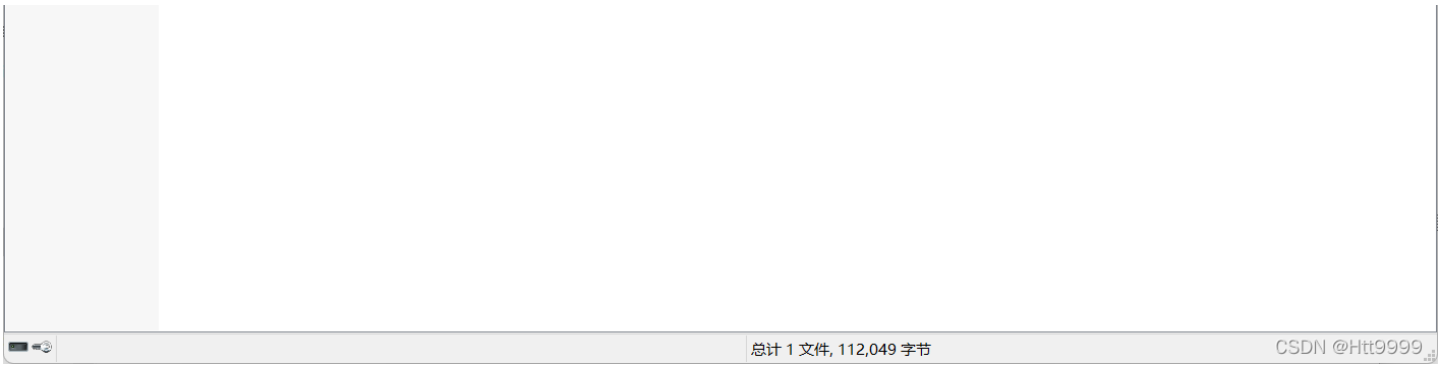
**

4·misc4

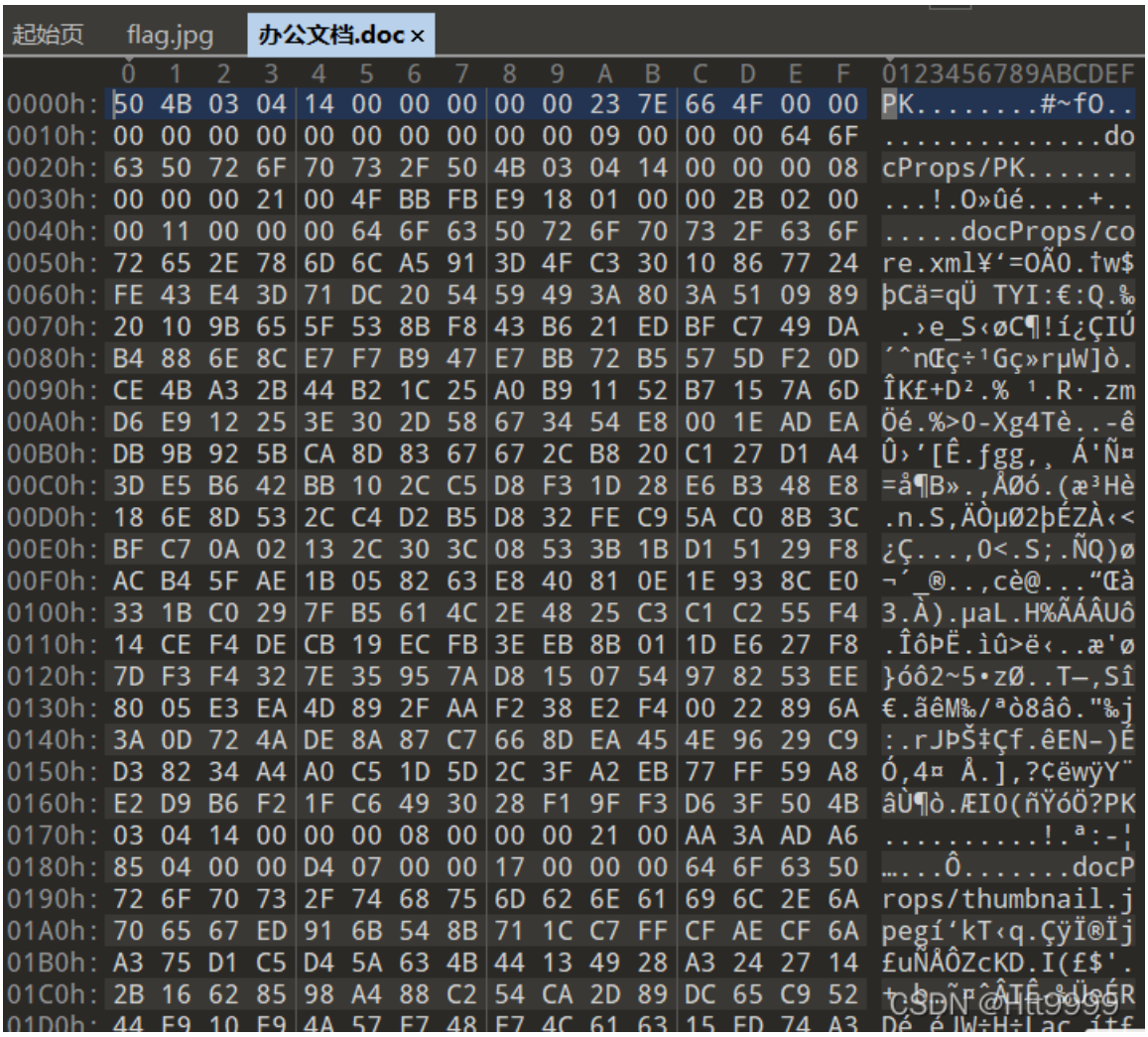
**

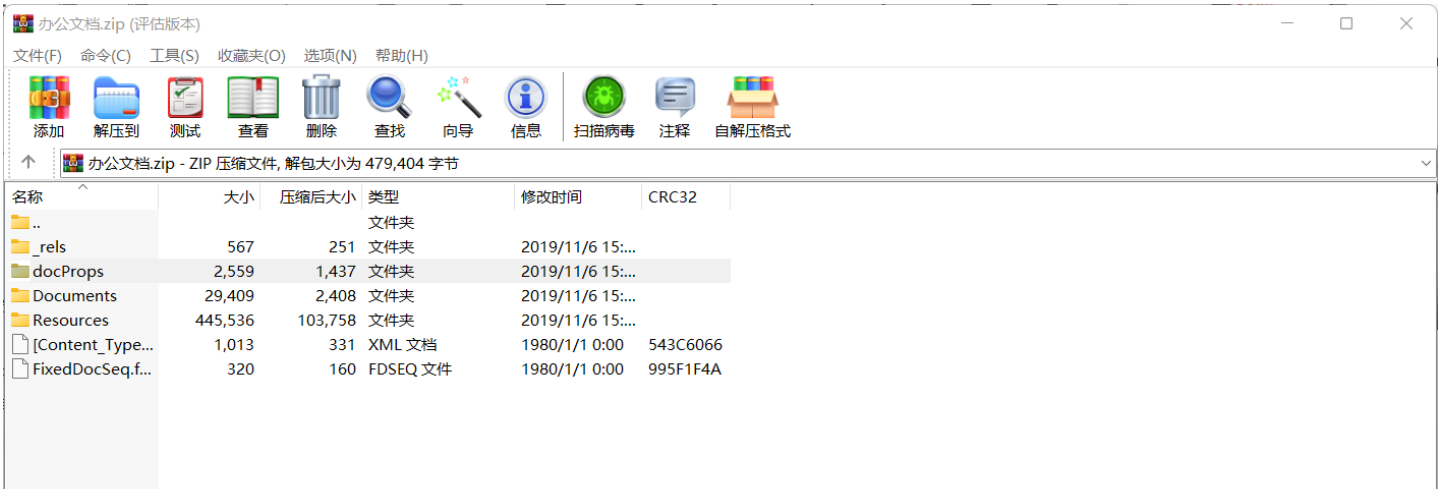
下载是一个没有后缀的东西，但是看到名称明白了，应该是的rar的压缩包，直接改后缀

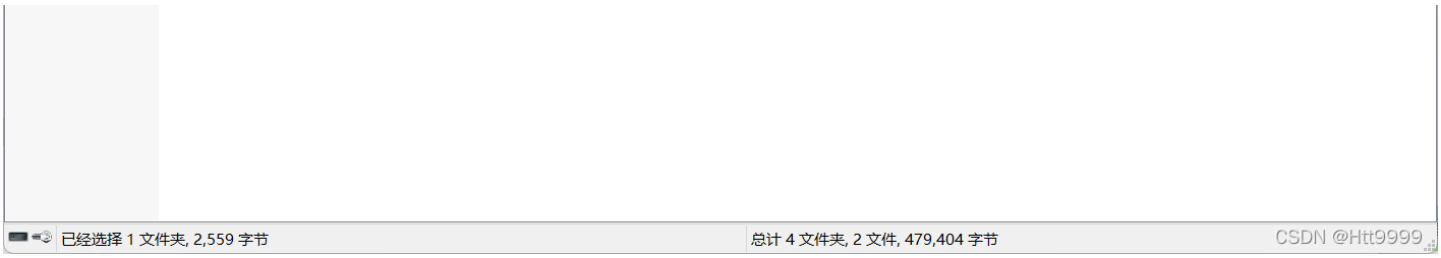




结果解压后的文档打不开，结果010editor分析得到还是一个压缩包还是改后缀







解压之后发现这么多文件，一个一个打开看看能不能发现什么，一个个翻，在Documents\1\Pages\1.fpage中发现不同

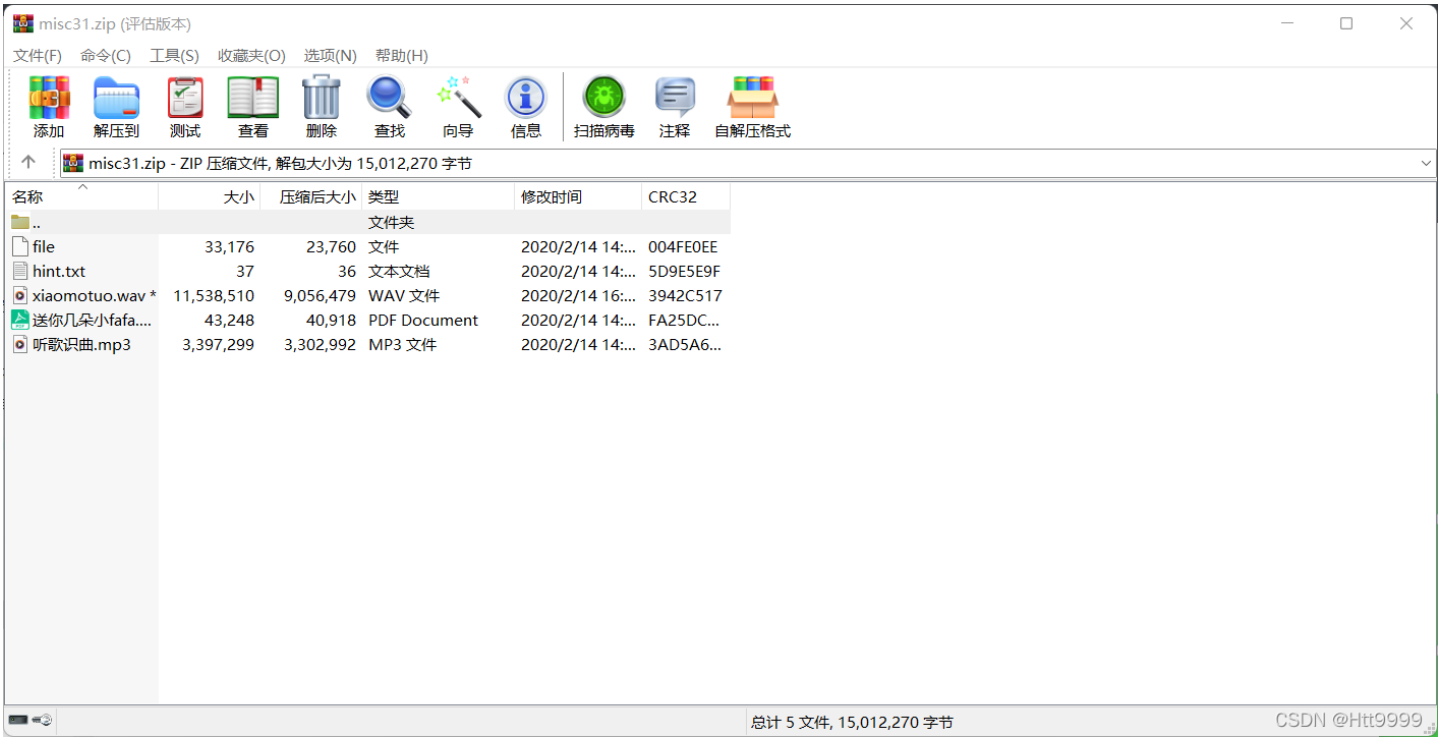
最后得到flag:flag{xps?Oh,Go0d!}

**

5·misc31

**

解压压缩包得到好多文件，一个一个试试会怎么样

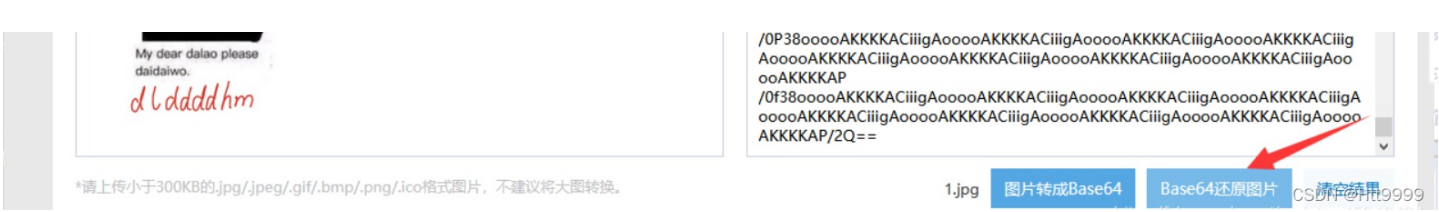


两个不加密，三个加密肯定就要对不加密的进行分析

打开file结果发现一串base64的代码，用base64解密没结果，想一下可能是base64的图片类型

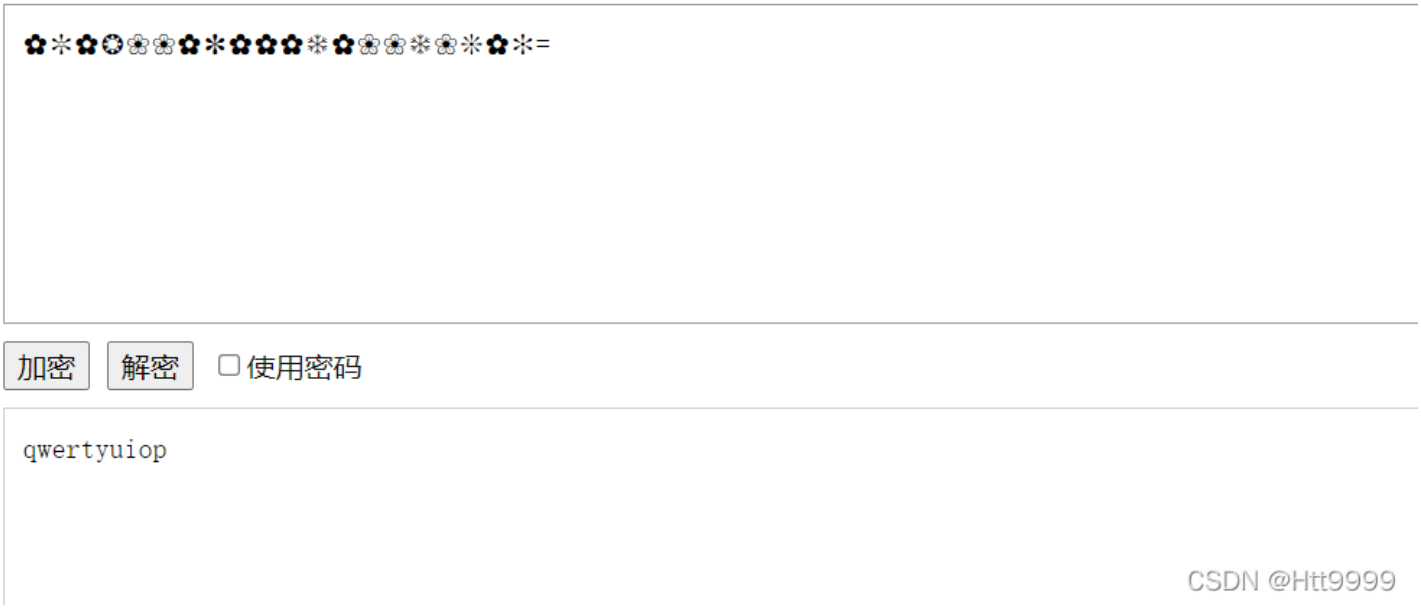
（https://tool.jisuapi.com/base642pic.html）在线网址

打开图片是一个dlddddhm



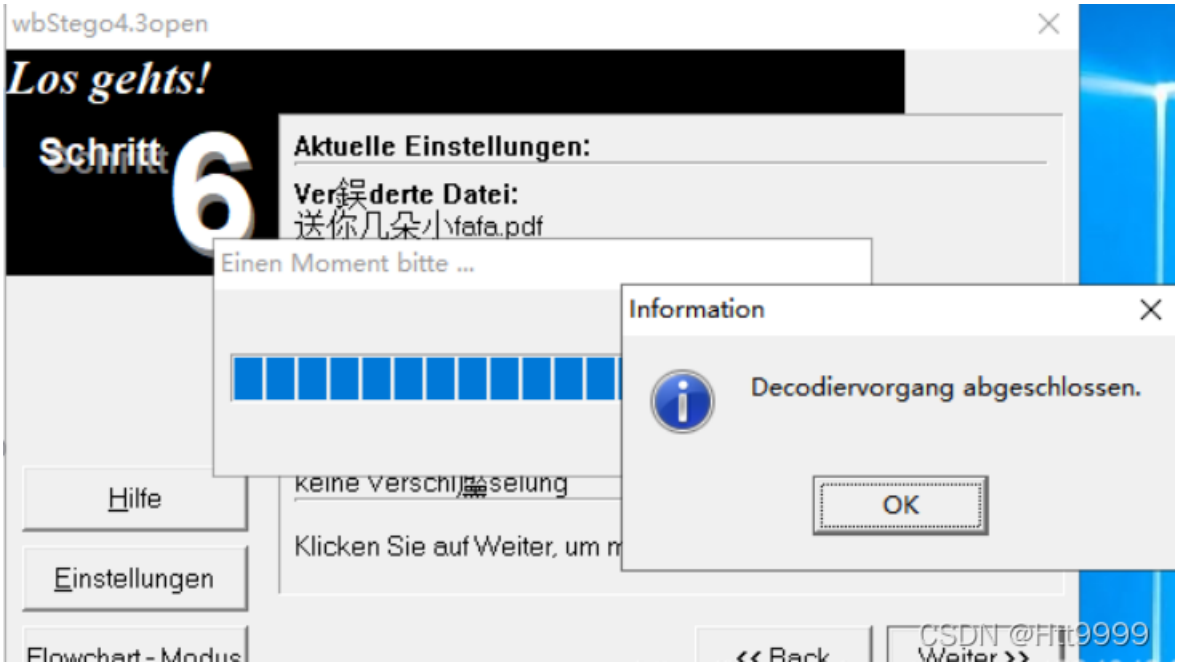
这个密码可以用在PDF中打开看看发现一段花瓣

直接在线解密（https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=huaduo）在线网址



但是我们用010editor进行对PDF查看时发现PDF有隐写

使用工具 wbStego4.3open 进行pdf 解密，秘钥设置为空。



得到一串数字ENTYNSTLWNRNTKYW13287484
目前pdf中解出了：
qwertyuiop
ENTYNSTLWNRNTKYW13287484
我们用关键字解密（http://www.hiencode.com/keyword.html）

关键字密码
Keyword Cipher

ENTYNSTLWNRNTKYW13287484

qwertyuiop

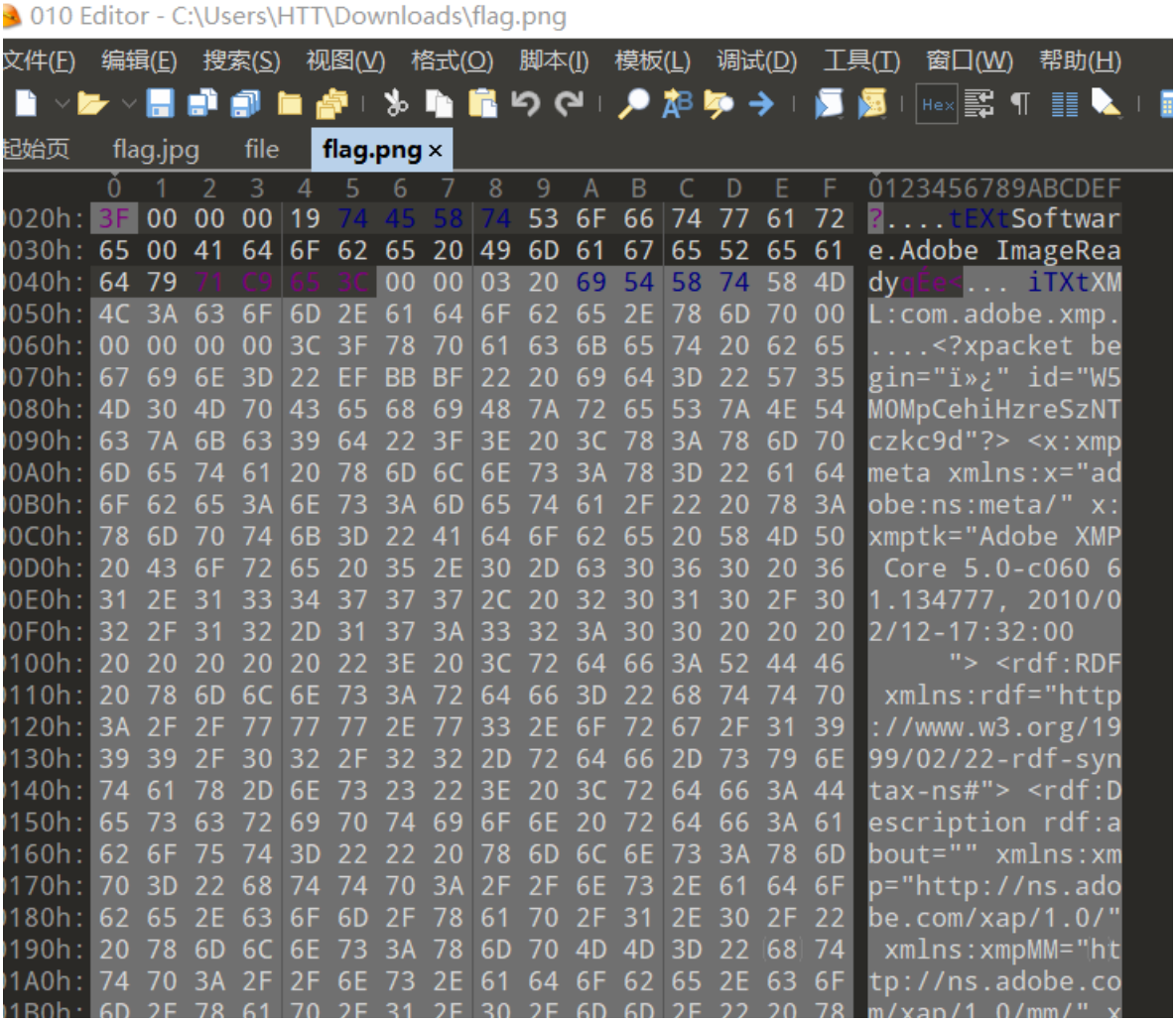
加 密　　解 密

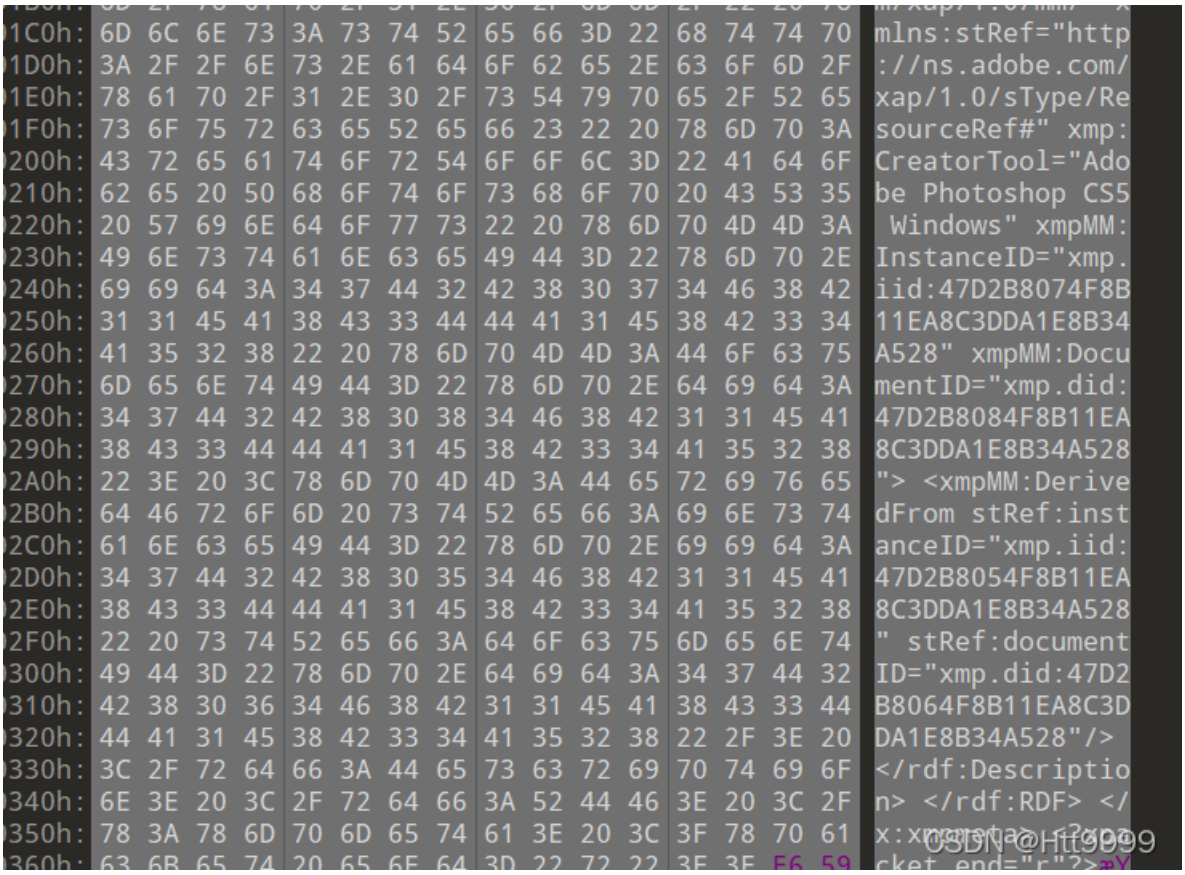
CVEFVWETBVDVESFB13287484

用CVEFVWETBVDVESFB13287484进行war的解密
解出的密码，成功解出了xiaomotuo.wav 文件。
使用steghide 工具进行解密，密码是xiaomotuo，解出flag：flag{du_du_du_du}
**

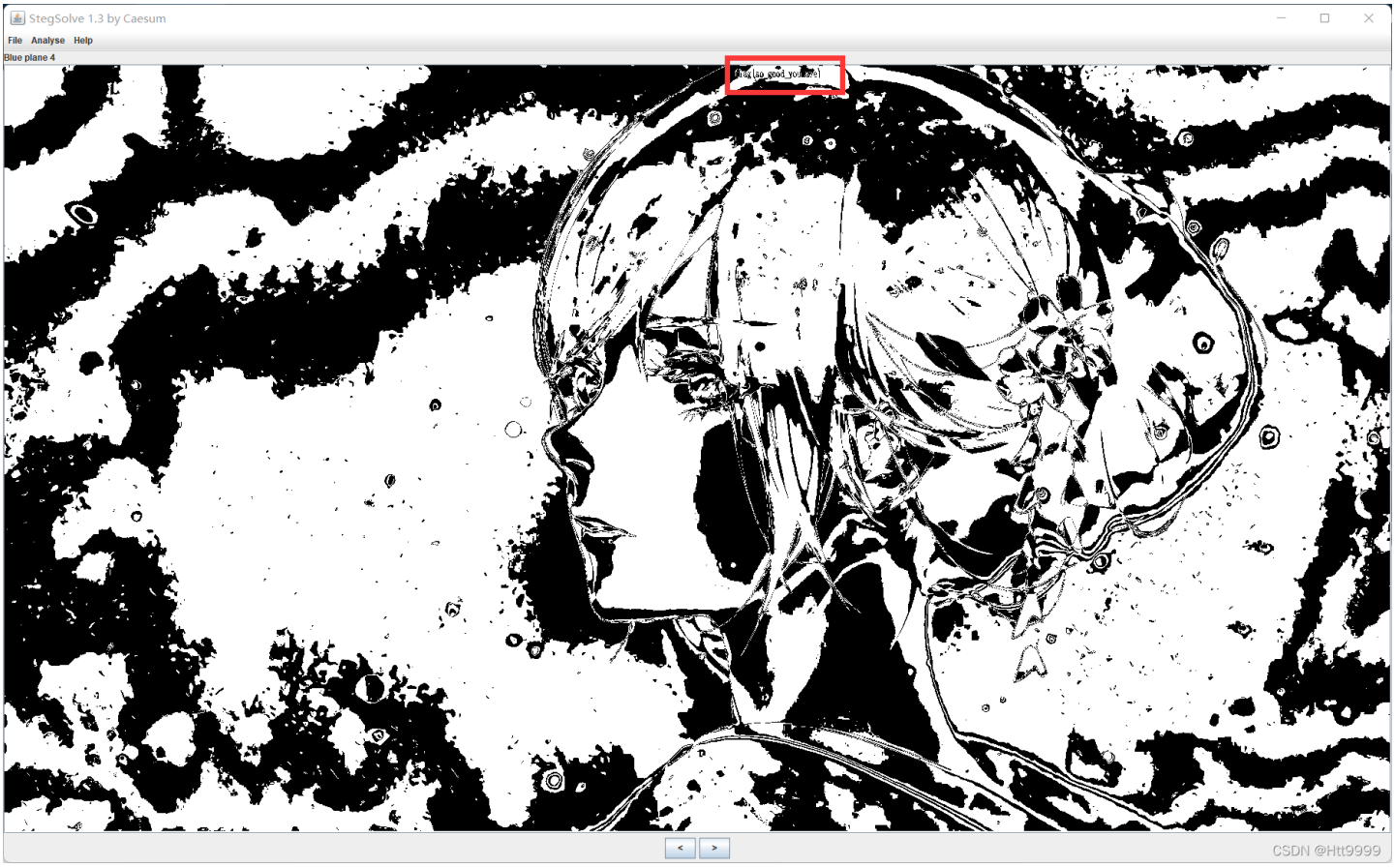
6·misc5

**
解压过后的文件用010editor打开





发现图片中有东西，使用stegsolve，在blue plane 4 发现flag



flag：flag:{so_good_you_are}