

【MISCshow misc30-misc5总结】

原创

Http9999 已于 2022-03-25 09:34:27 修改 4640 收藏

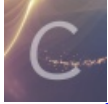
分类专栏: [CTFshow](#) 文章标签: [网络安全](#)

于 2022-03-23 22:20:37 首次发布

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/Http9999/article/details/123686692>

版权



[CTFshow 专栏收录该内容](#)

2 篇文章 0 订阅

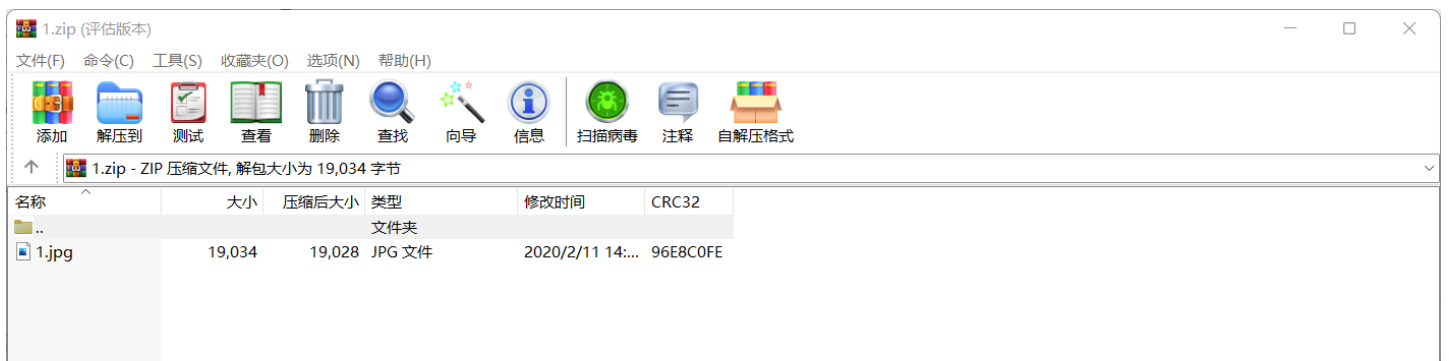
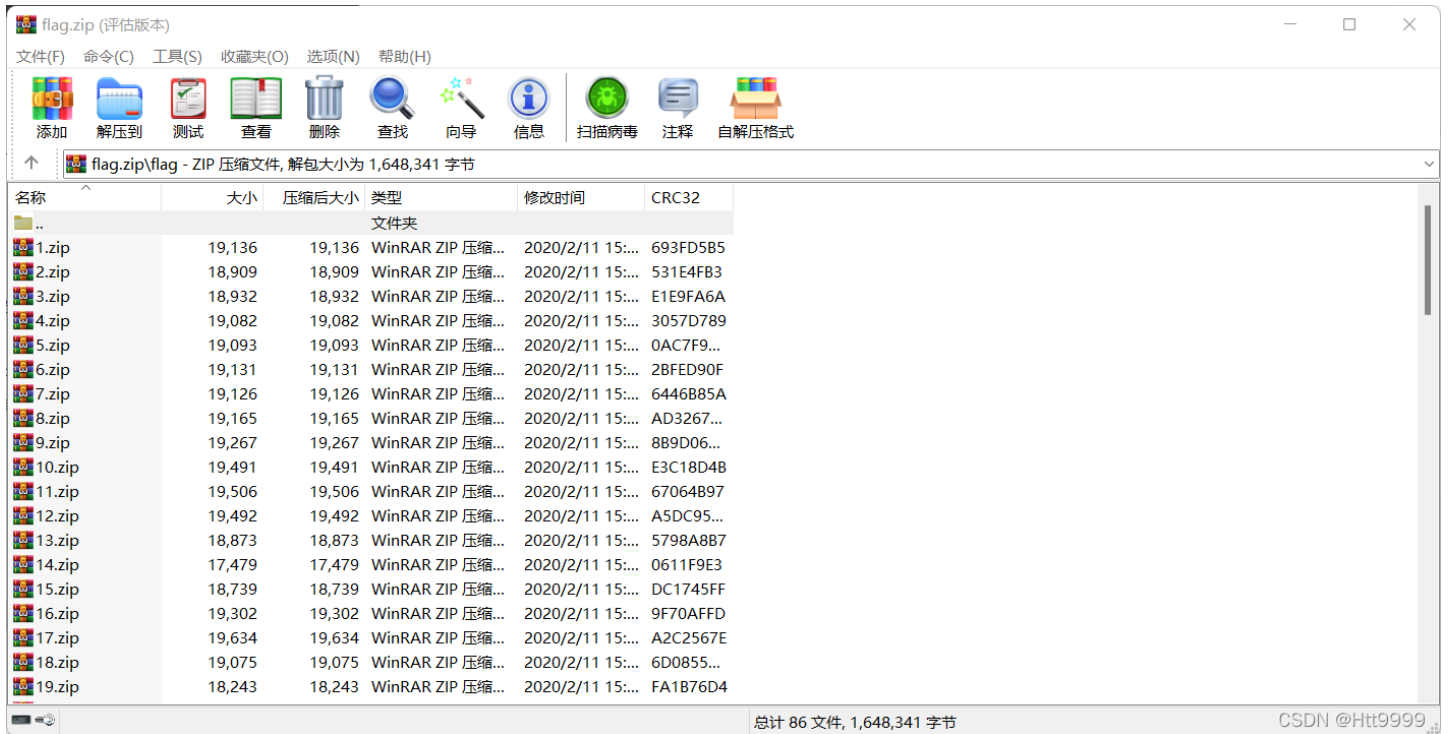
订阅专栏

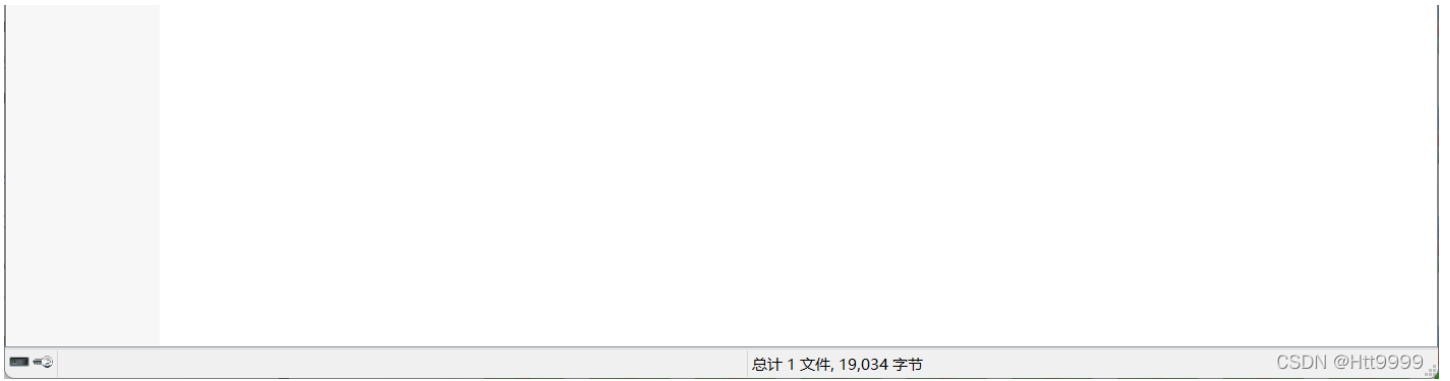
MISCshow总结

本文章均来自于CTFshow<https://ctf.show/challenges#misc2-21>

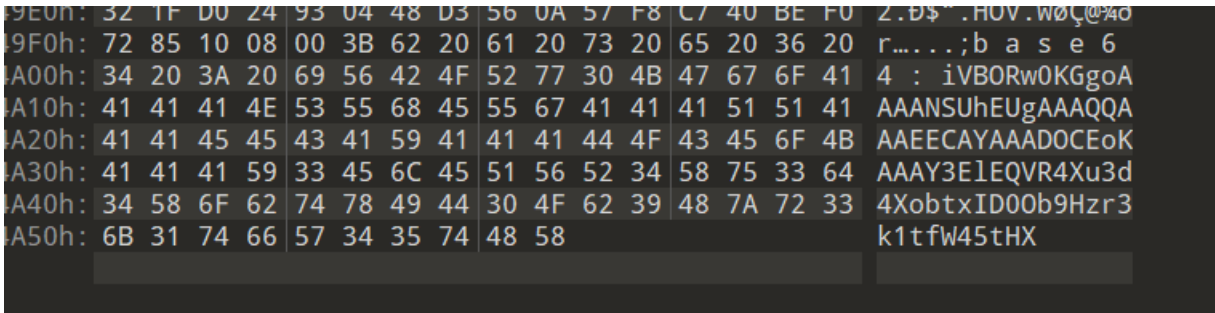
1· 红包第一弹

打开发现全是压缩包

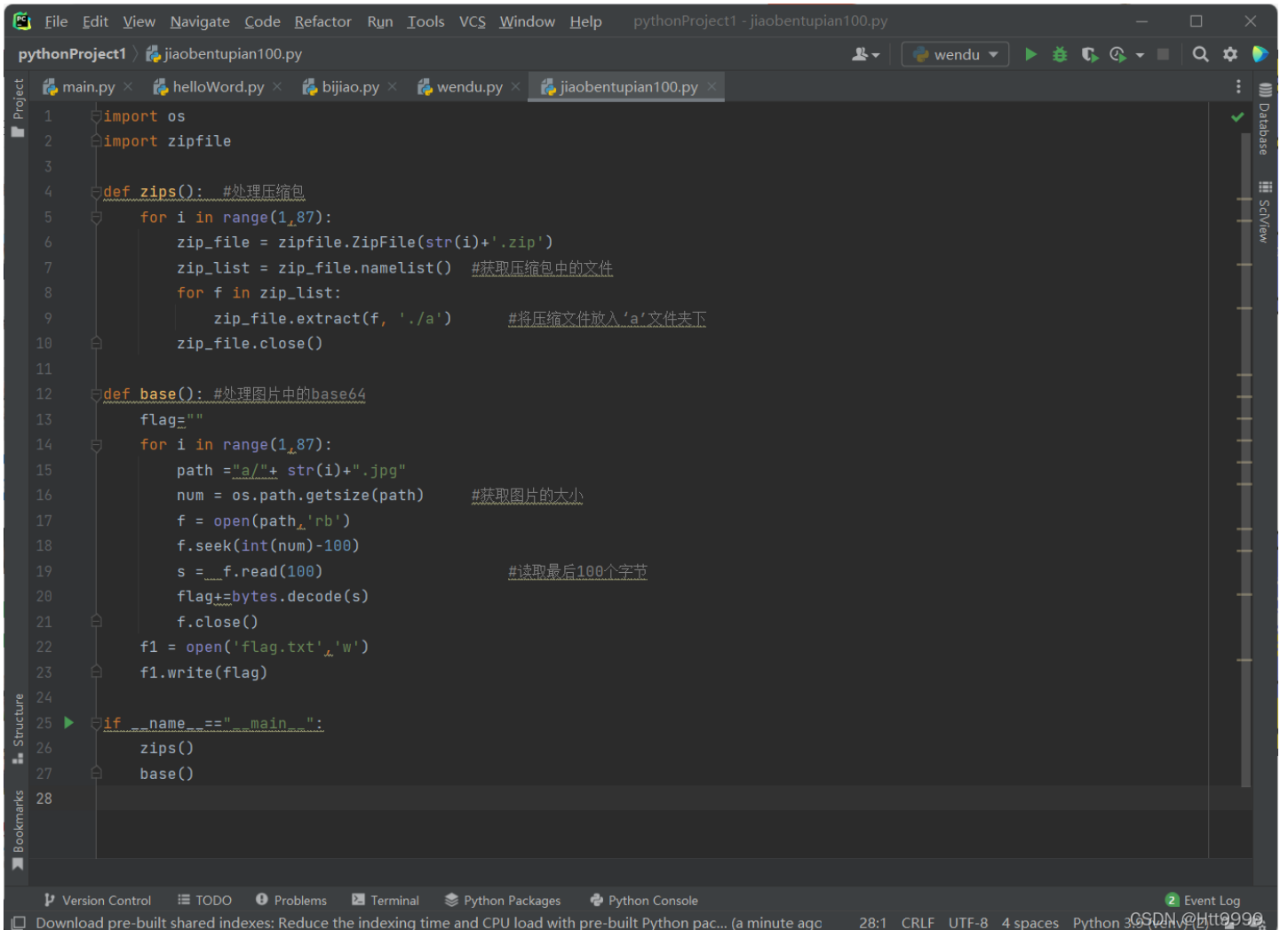




打开每个压缩包发现全是一张图片，用010editor打开第一张图片发现二进制的最后有一串base64的编码



由于图片比较多，直接脚本上手



! [在这里插入图片描述] (<https://img-blog.csdnimg.cn/1a51e214aab143d78caef0f14b6ffa1f.png?x-oss->

process=image/watermark,type_d3F5LXplbmniaQ,snadow_5U,text_Q1NE1IBASHRUU1K5UQ==,size_2U,color_FFFFFFFF,t_7U,gse,x_16

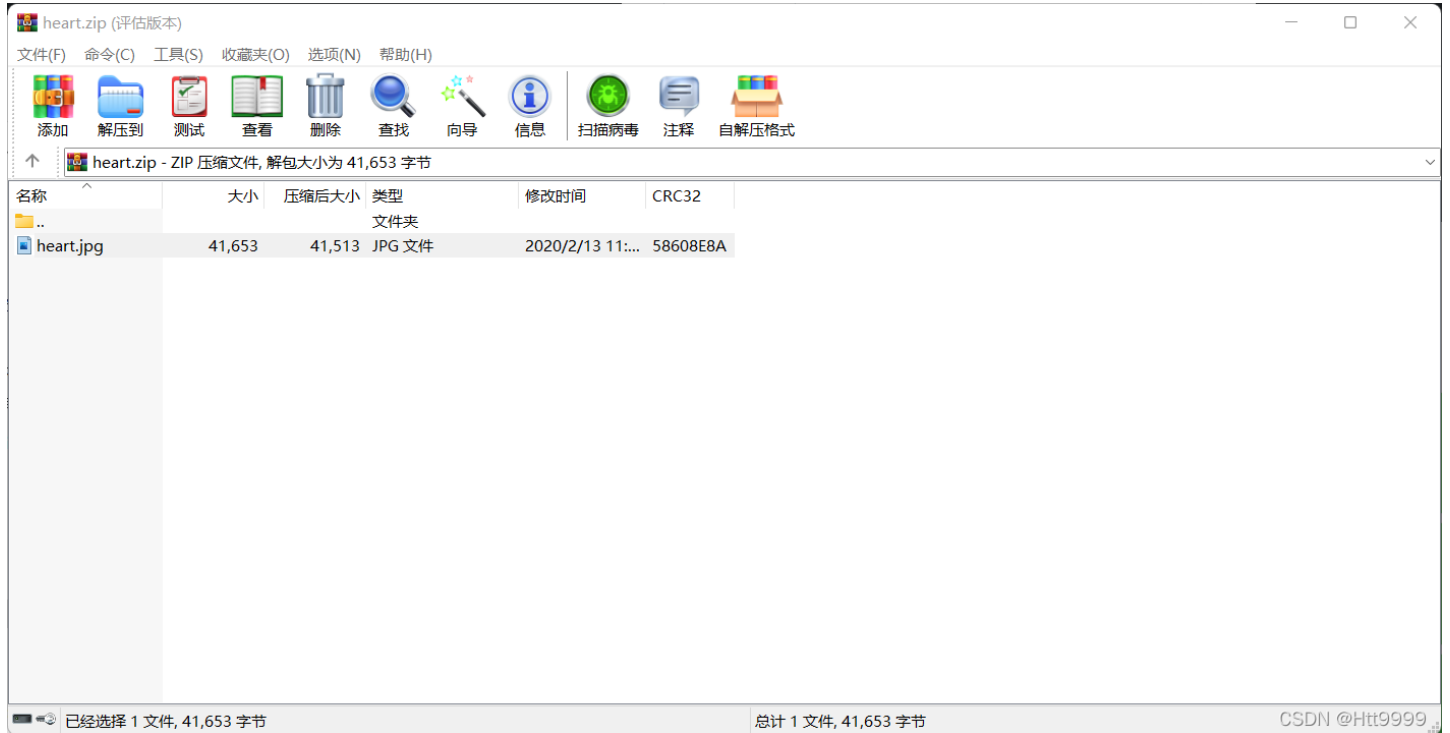
直接base64解码得到flag: flag{gif_is_so_easy}

**

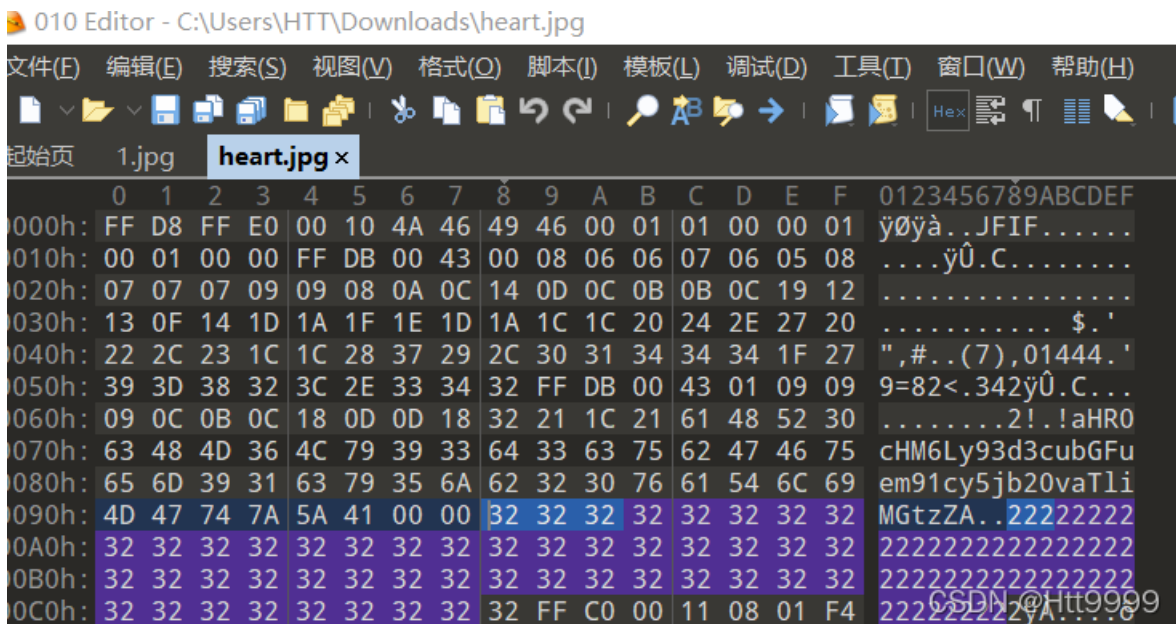
2-stega10

**

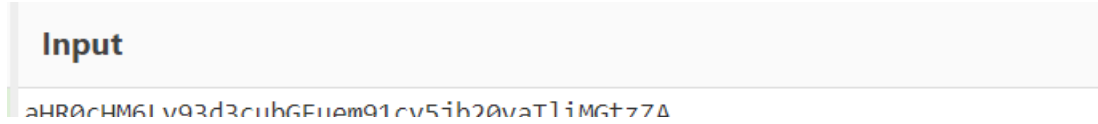
又是一个压缩包打开是一个图片



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



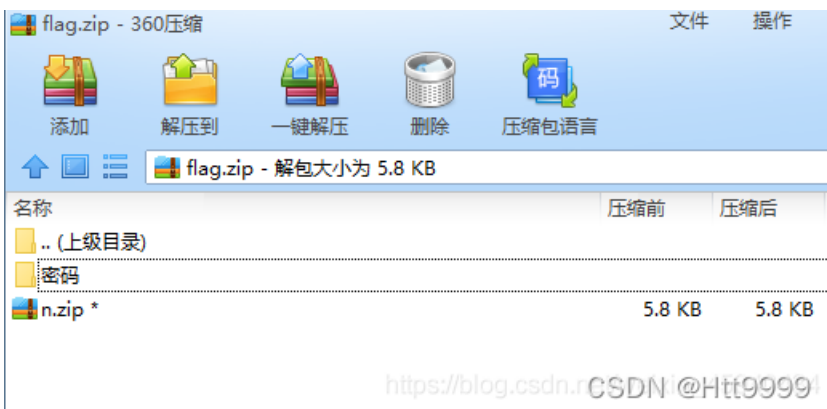
unreco... 524524001... 4cm21cy5j0z0v0111182228

Output

<https://www.lanzous.com/i9b0ksd>

CSDN @Htt9999

打开这个蓝奏云链接，我们下载到了一个加密的压缩包



<https://blog.csdn.net/Htt9999>

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

```
1 import re
2 import binascii
3
4 def read_file(filepath):
5     with open(filepath,'rb') as fp:
6         content=fp.read();
```

```

7     return content
8
9     #以二进制读取图片, 并转为16进制
10    a = read_file('n.png')
11    hexstr = str(binascii.b2a_hex(a))
12    hexstr = re.findall("b'(.*)'",hexstr)[0]
13
14    #每俩位分割成列表元素
15    result = []
16    result.append(re.findall(r'.{2}', hexstr))
17    result = result[0]
18
19    #按倒序排列, 拼接列表为文本
20    daoxu = result[::-1]
21    hex= ''
22    for i in daoxu:
23        hex +=i
24
25    print(hex)

```

CSDN @Htt9999

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_Q1NETiBASHR00Tk5OQ==,size_18,color_FFFFFFFF,t_70,gs_e,x_16)

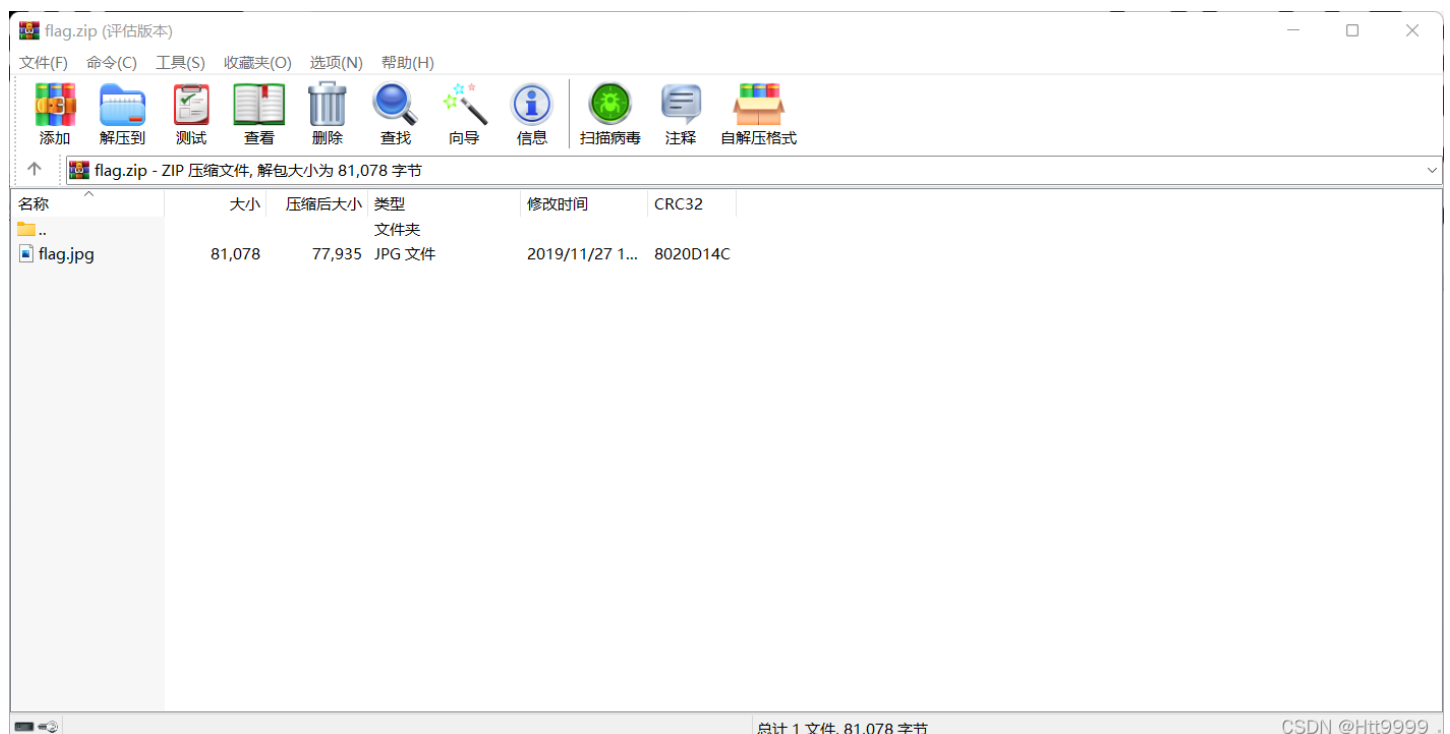
扫码得flag:flag{我好难啊}

**

3-stega11

**

打开压缩包是一个图片的格式



CSDN @Htt9999

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

1

```
ÿÛMZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJVHA4TONZYGA2DMM3FGMYH2ÿøÿà
```

Output

```
flag{6f1797d4080b29b64da5897780463e30}
```

CSDN @Htt9999

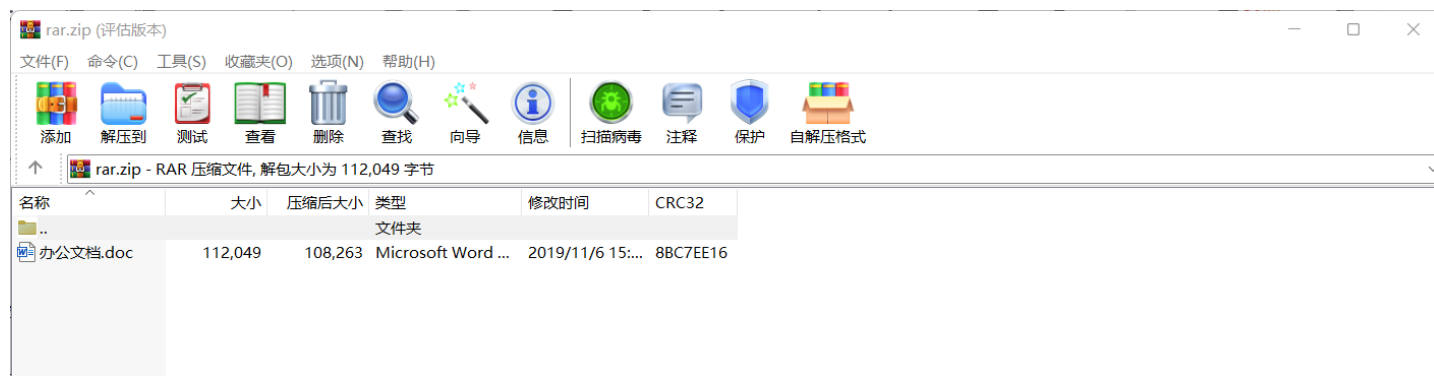
得到flag: flag{6f1797d4080b29b64da5897780463e30}

**

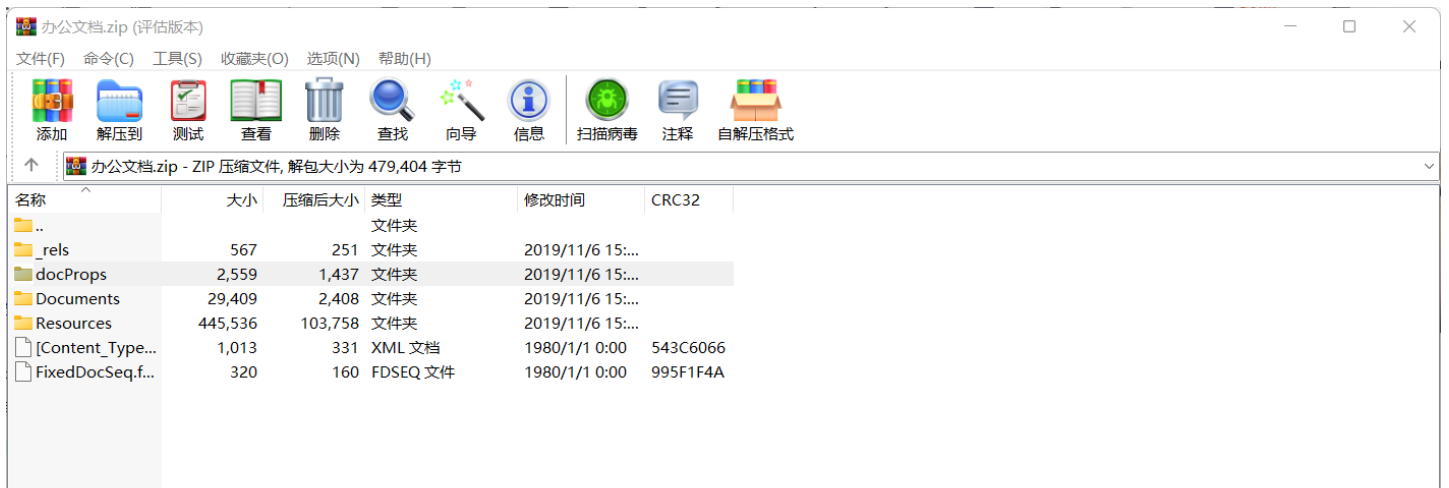
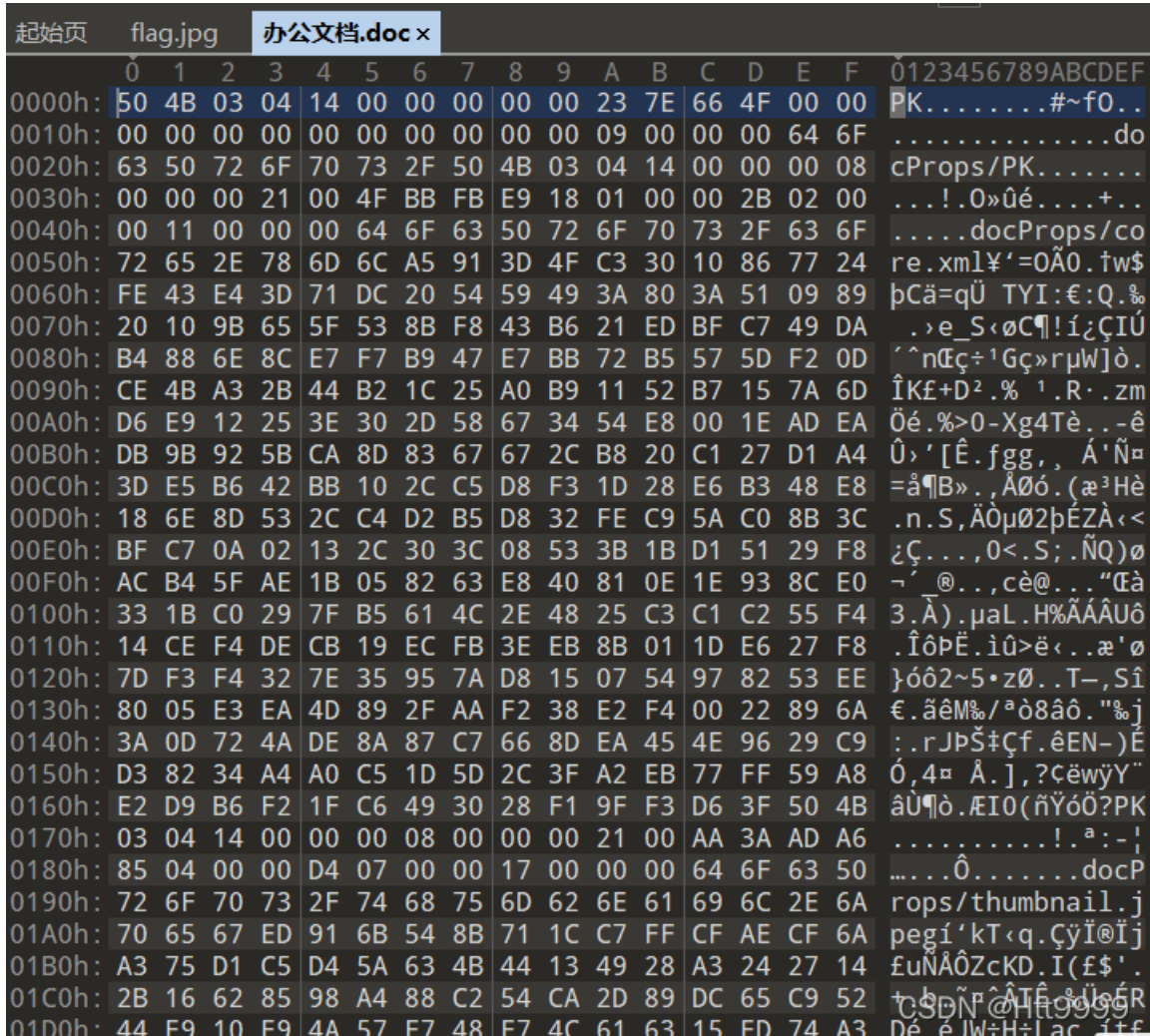
4·misc4

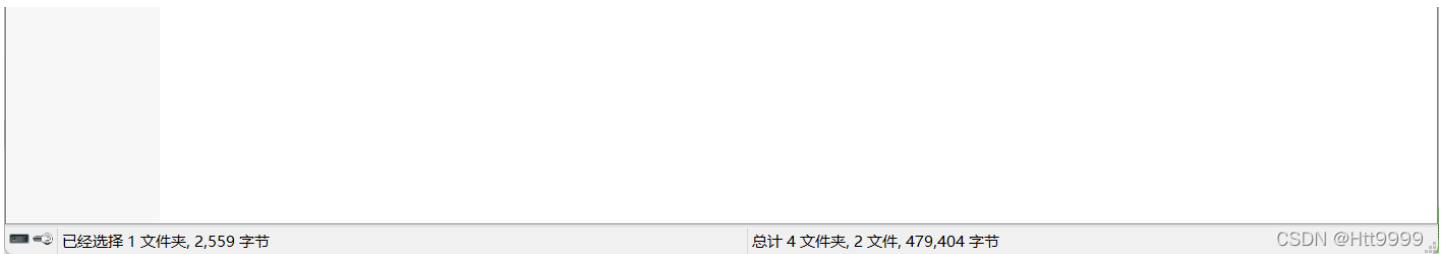
**

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

```
</Glyphs>
<Glyphs Name="a3" BidiLevel="0" Fill="#FF000000"
FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="214.13'
OriginY="83.664" UnicodeString=" " Indices="" xml:lang="en-US">
</Glyphs>
<Glyphs Name="a4" BidiLevel="0" Fill="#FF000000"
FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="90.024'
OriginY="99.024" UnicodeString="f" Indices="" xml:lang="en-US">
</Glyphs>
<Glyphs Name="a5" BidiLevel="0" Fill="#FF000000"
FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="93.264'
OriginY="99.024" UnicodeString=" " Indices="" xml:lang="en-US">
</Glyphs>
<Glyphs Name="a6" BidiLevel="0" Fill="#FF000000"
FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="90.024'
OriginY="114.62" UnicodeString="l" Indices="" xml:lang="en-US">
</Glyphs>
<Glyphs Name="a7" BidiLevel="0" Fill="#FF000000"
FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="92.424'
OriginY="114.62" UnicodeString=" " Indices="" xml:lang="en-US">
</Glyphs>
<Glyphs Name="a8" BidiLevel="0" Fill="#FF000000"
FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="90.024'
OriginY="130.22" UnicodeString="a" Indices="" xml:lang="en-US">
```

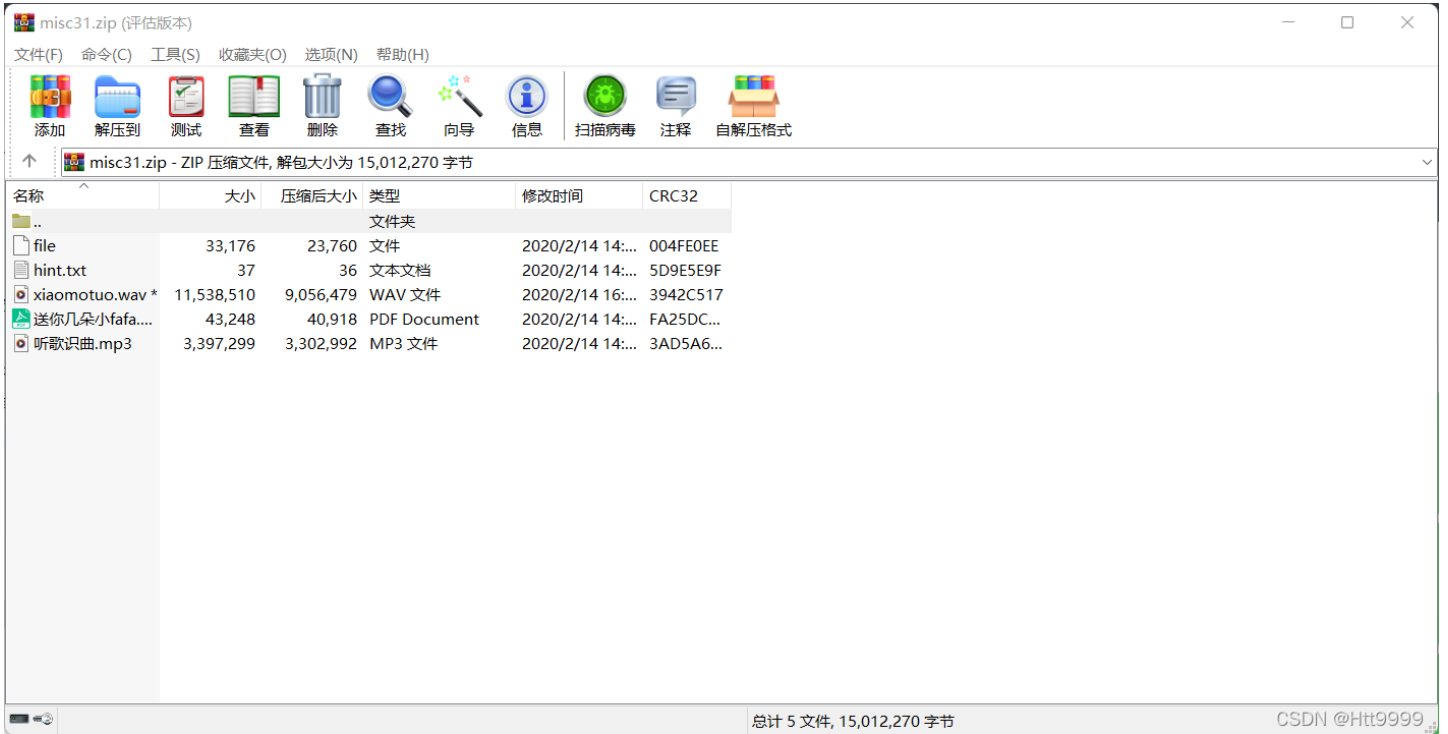
最后得到flag:flag{xps?Oh,Go0d!}

**

5-misc31

**

解压压缩包得到好多文件，一个一个试试会怎么样



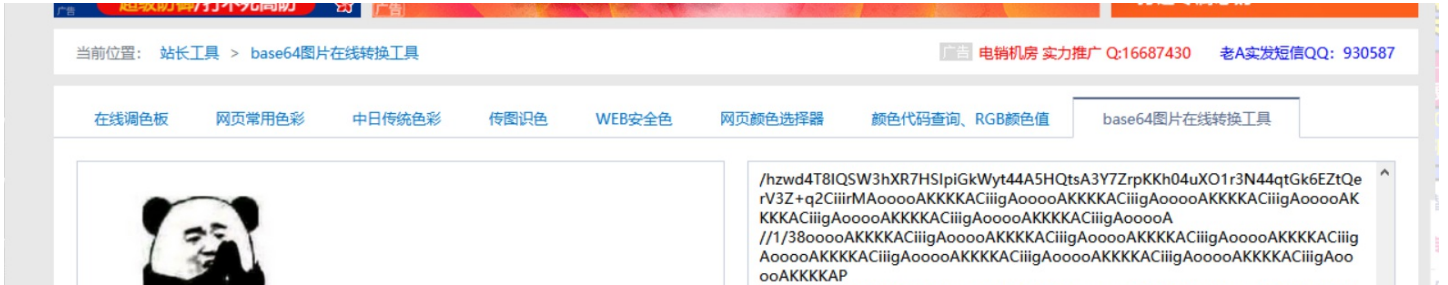
两个不加密，三个加密肯定就要对不加密的进行分析

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.jsuapi.com/base642pic.html>) 在线网址

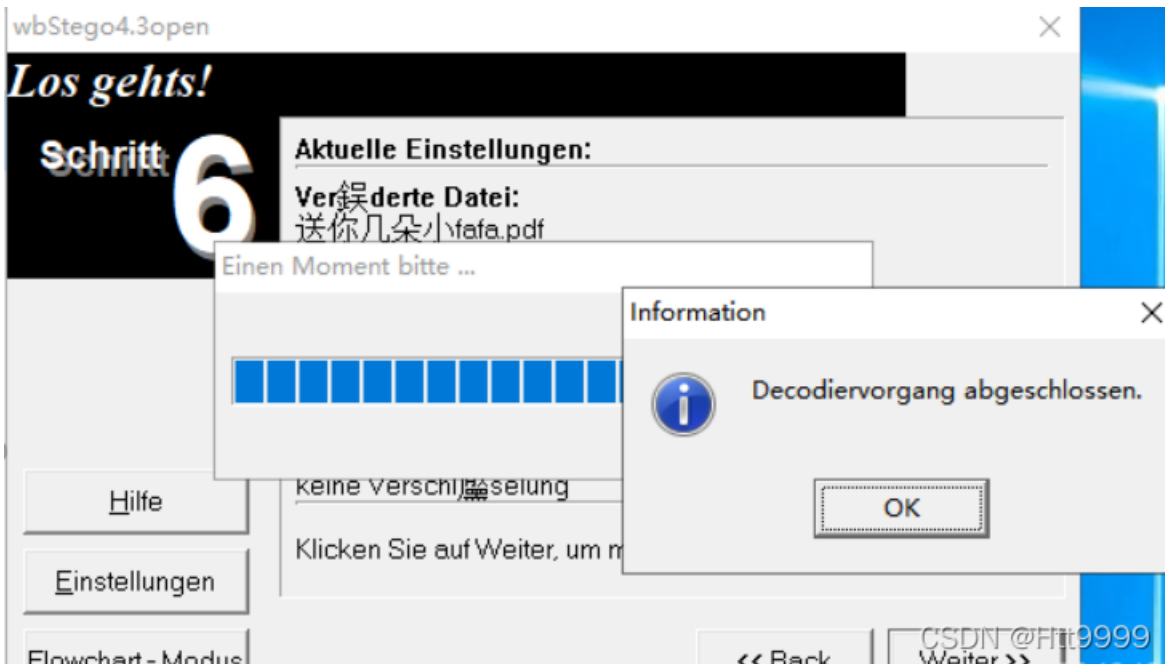


打开图片是一个dllddddhm





使用工具 wbStego4.3open 进行pdf 解密，密钥设置为空。



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

ENTYNSTLWNRNTKYWJ13287484

qwertyuiop

加密

解密

CVEFWWETBVDVESFB13287484

CSDN @Htt9999

用CVEFWWETBVDVESFB13287484进行war的解密

解出的密码，成功解出了xiaomotuo.wav 文件。

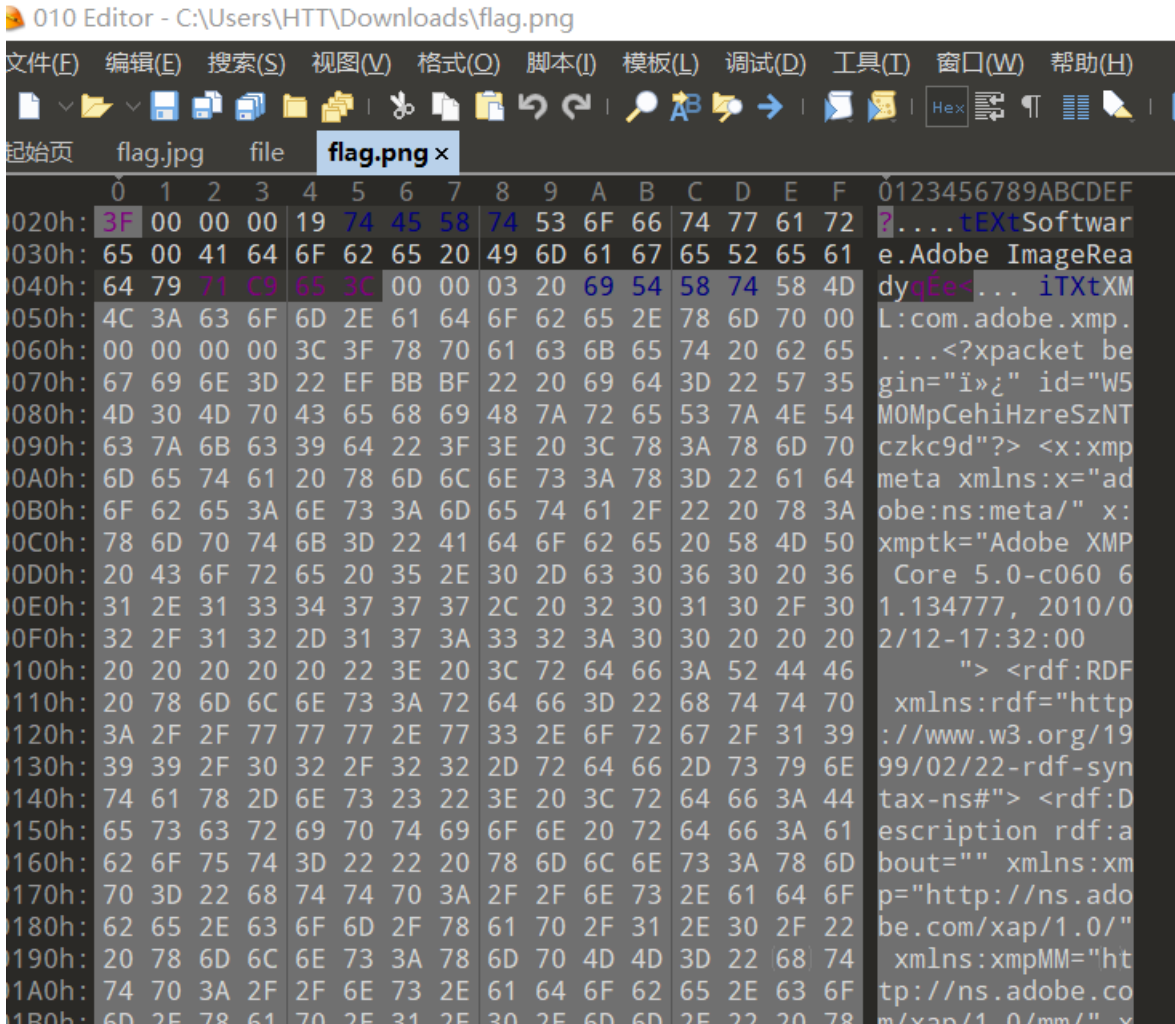
使用steghide 工具进行解密，密码是xiaomotuo，解出flag: flag{du_du_du_du}

**

6-misc5

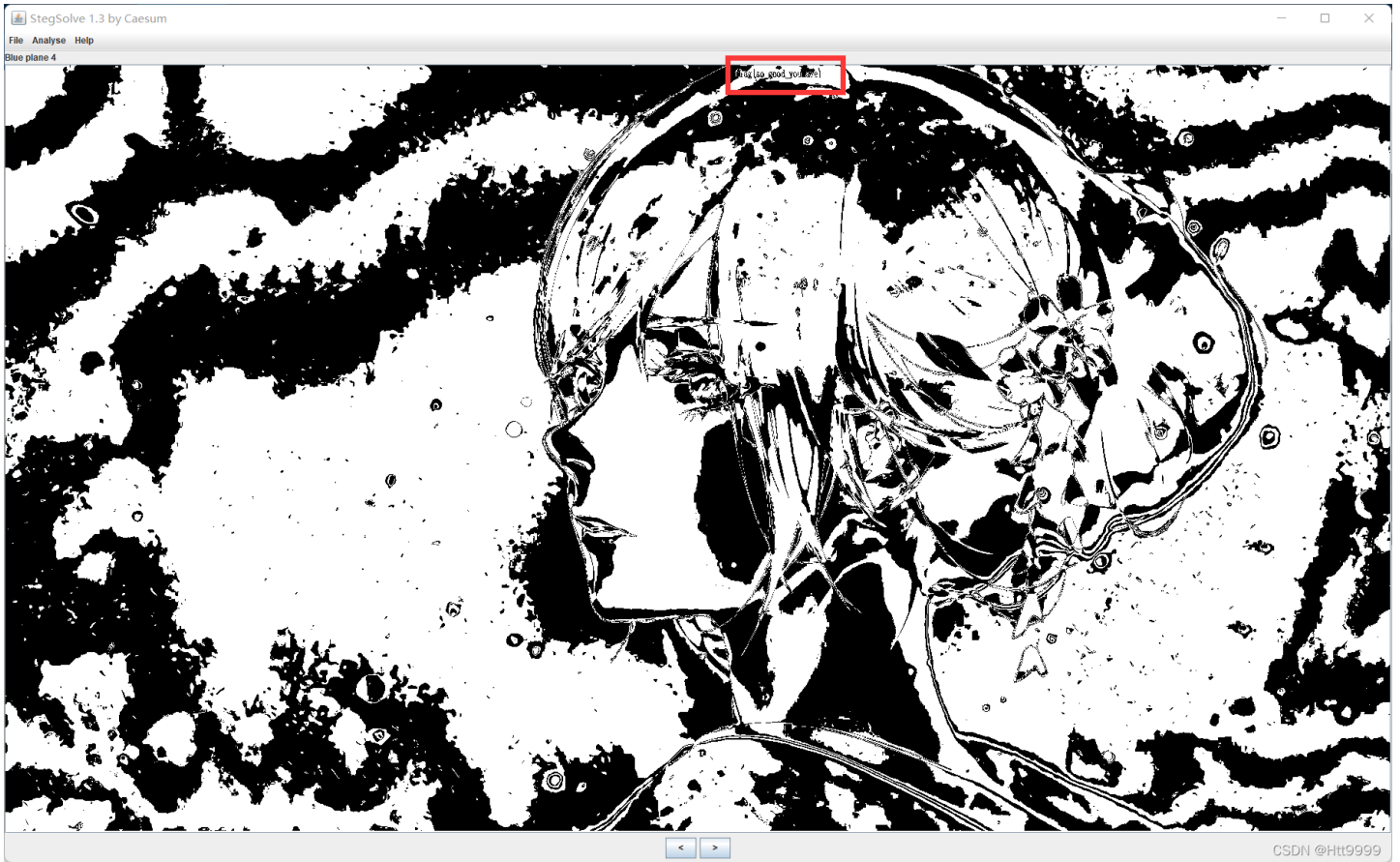
**

解压过后的文件用010editor打开



```
1C0h: 6D 6C 6E 73 3A 73 74 52 65 66 3D 22 68 74 74 70 m/ xap:/1.0/mm/ x
1D0h: 3A 2F 2F 6E 73 2E 61 64 6F 62 65 2E 63 6F 6D 2F ://ns.adobe.com/
1E0h: 78 61 70 2F 31 2E 30 2F 73 54 79 70 65 2F 52 65 xap/1.0/sType/Re
1F0h: 73 6F 75 72 63 65 52 65 66 23 22 20 78 6D 70 3A sourceRef#" xmp:
200h: 43 72 65 61 74 6F 72 54 6F 6F 6C 3D 22 41 64 6F CreatorTool="Ado
210h: 62 65 20 50 68 6F 74 6F 73 68 6F 70 20 43 53 35 be Photoshop CS5
220h: 20 57 69 6E 64 6F 77 73 22 20 78 6D 70 4D 4D 3A Windows" xmpMM:
230h: 49 6E 73 74 61 6E 63 65 49 44 3D 22 78 6D 70 2E InstanceID="xmp.
240h: 69 69 64 3A 34 37 44 32 42 38 30 37 34 46 38 42 iid:47D2B8074F8B
250h: 31 31 45 41 38 43 33 44 44 41 31 45 38 42 33 34 11EA8C3DDA1E8B34
260h: 41 35 32 38 22 20 78 6D 70 4D 4D 3A 44 6F 63 75 A528" xmpMM:Docu
270h: 6D 65 6E 74 49 44 3D 22 78 6D 70 2E 64 69 64 3A mentID="xmp.did:
280h: 34 37 44 32 42 38 30 38 34 46 38 42 31 31 45 41 47D2B8084F8B11EA
290h: 38 43 33 44 44 41 31 45 38 42 33 34 41 35 32 38 8C3DDA1E8B34A528
2A0h: 22 3E 20 3C 78 6D 70 4D 4D 3A 44 65 72 69 76 65 "> <xmpMM:Derive
2B0h: 64 46 72 6F 6D 20 73 74 52 65 66 3A 69 6E 73 74 dFrom stRef:inst
2C0h: 61 6E 63 65 49 44 3D 22 78 6D 70 2E 69 69 64 3A anceID="xmp.iid:
2D0h: 34 37 44 32 42 38 30 35 34 46 38 42 31 31 45 41 47D2B8054F8B11EA
2E0h: 38 43 33 44 44 41 31 45 38 42 33 34 41 35 32 38 8C3DDA1E8B34A528
2F0h: 22 20 73 74 52 65 66 3A 64 6F 63 75 6D 65 6E 74 " stRef:document
300h: 49 44 3D 22 78 6D 70 2E 64 69 64 3A 34 37 44 32 ID="xmp.did:47D2
310h: 42 38 30 36 34 46 38 42 31 31 45 41 38 43 33 44 B8064F8B11EA8C3D
320h: 44 41 31 45 38 42 33 34 41 35 32 38 22 2F 3E 20 DA1E8B34A528"/>
330h: 3C 2F 72 64 66 3A 44 65 73 63 72 69 70 74 69 6F </rdf:Descriptio
340h: 6E 3E 20 3C 2F 72 64 66 3A 52 44 46 3E 20 3C 2F n> </rdf:RDF> </
350h: 78 3A 78 6D 70 6D 65 74 61 3E 20 3C 3F 78 70 61 x:xmp:meta> ?>
360h: 63 6B 65 74 20 65 6E 64 3D 22 72 22 3E 3E F6 59 cket_end="r"?>?>
```

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



flag: flag:{so_good_you_are}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)