

MISC

Tools

隐写题，拿到题目，解压，得2个文件，一个是压缩包，名叫F5，搜索是F5隐写，并且密码在图片的备

| | | | | | |
|----|-----------------------|--|--|--|--|
| 说明 | | | | | |
| 标题 | | | | | |
| 主题 | | | | | |
| 注中 | 于是github上下载F5隐写的工具，解密 | | | | |
| 分级 | ☆☆☆☆☆ | | | | |
| 标记 | | | | | |
| 备注 | !LyJJ9bi&M7E72*JyD | | | | |

```
└─$ java Extract Matryoshka.jpg -p '!LyJJ9bi&M7E72*JyD'
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext
Huffman decoding starts
Permutation starts
577536 indices shuffled
Extraction starts
Length of embedded file: 18 bytes
(1, 127, 7) code used
```

文件(F) 编辑(E) 视图(V) 窗口(W) 帮助(H)
e@317S*p1A4bIYIs1M

到压缩包密码。解压F5.7z，发现又有两个文件，一个名叫Steghide.7z，应该是Steghide隐写，密码仍然在备注中。继续解密

```
└─$ steghide extract -sf 01.jpg
Enter passphrase:
wrote extracted data to "pwd.txt".
```

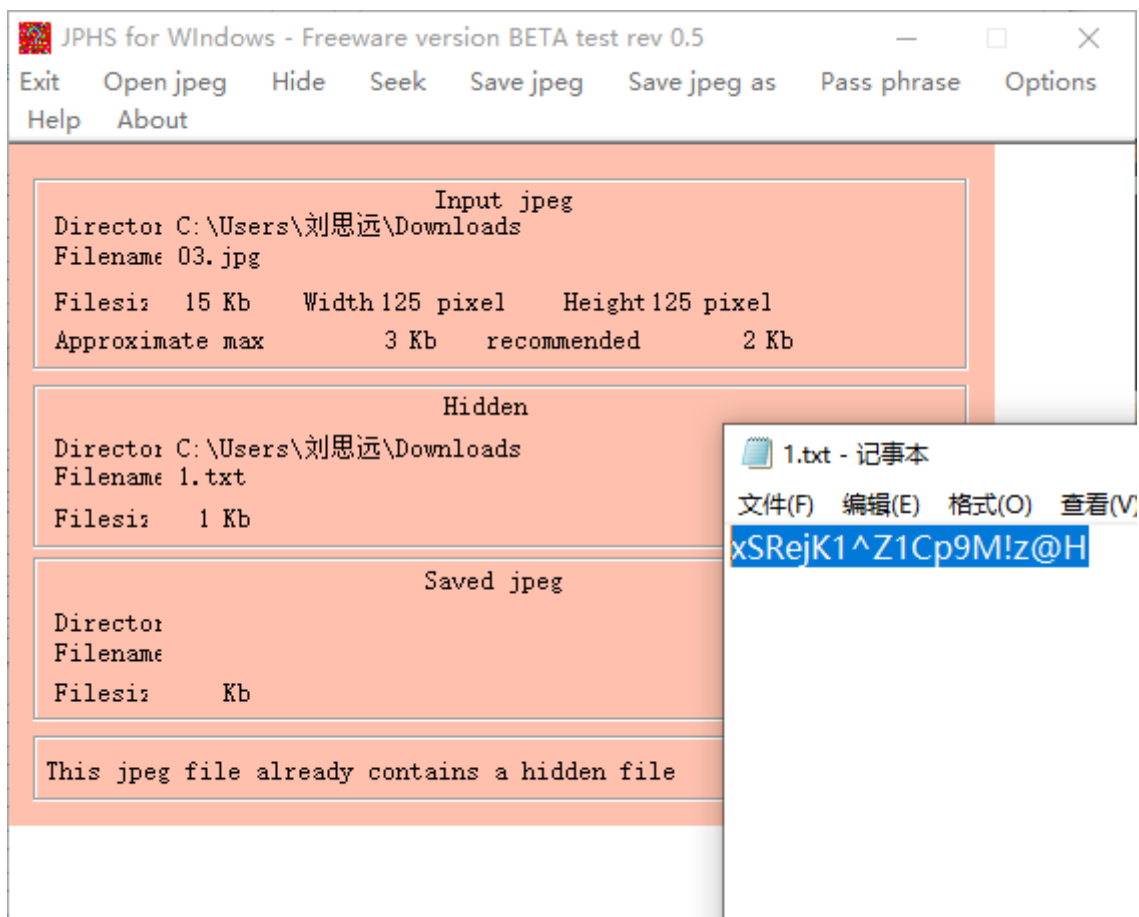
文件(F) 编辑(E) 视图(V) 窗口(W) 帮助(H)
U0!F04JUhl5!L55%\$&

，又得到一个7z和一个图片，已经2个四分之一二维码了，看7z的文件名，是Outguess加密，密码还是在备注中，于是继续找工具解密

```
└─$ outguess -r 02.jpg -k 'z0GFieYAee%gdf0%lF' -t 1.txt
Reading 02.jpg...
Extracting usable bits: 4930 bits
Steg retrieve: seed: 184, len: 18
```

文件(F) 编辑(E) 视图(V) 窗口(W) 帮助(H)
@UjXL93044V5zl2ZKI

解压文件，又得到一个四分之一二维码和一个7z，看文件名是JPHS，那么是JPHS隐写，找资料



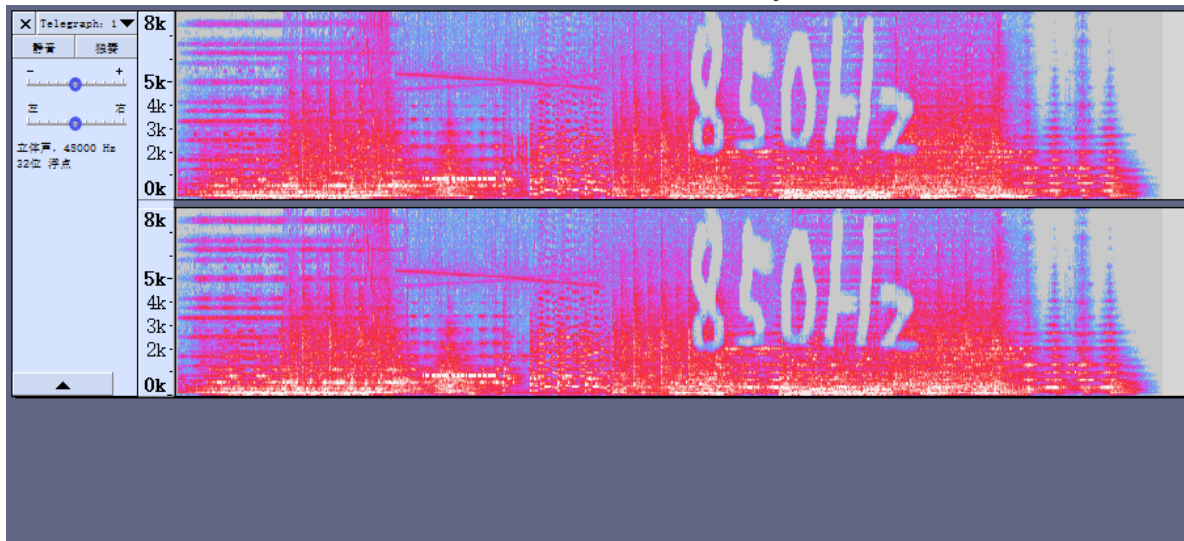
4个四分之一二维码终于集齐了，Photoshop合成一下



扫描得flag。

Telegraph: 1601 6639 3459 3134 0892

下载文件，得到一个MP3文件，应该是要频谱分析。于是用audacity打开，选择频谱



有850Hz字样，不知道要干啥。看文件名，telegraph，是电报的意思，那么后面的数字应该是电报码？

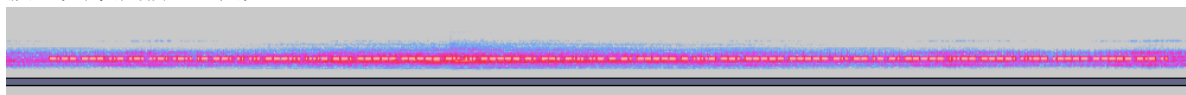
1601 6639 3459 3134 0892

找个网站翻译一下

编码 解码 中文电报 ☒ 数字代码

带通滤波器

带通滤波器？允许特定频段的波通过，同时屏蔽其他频段。audacity的效果里只有高通滤波器和低通滤波器，那就都用一次，



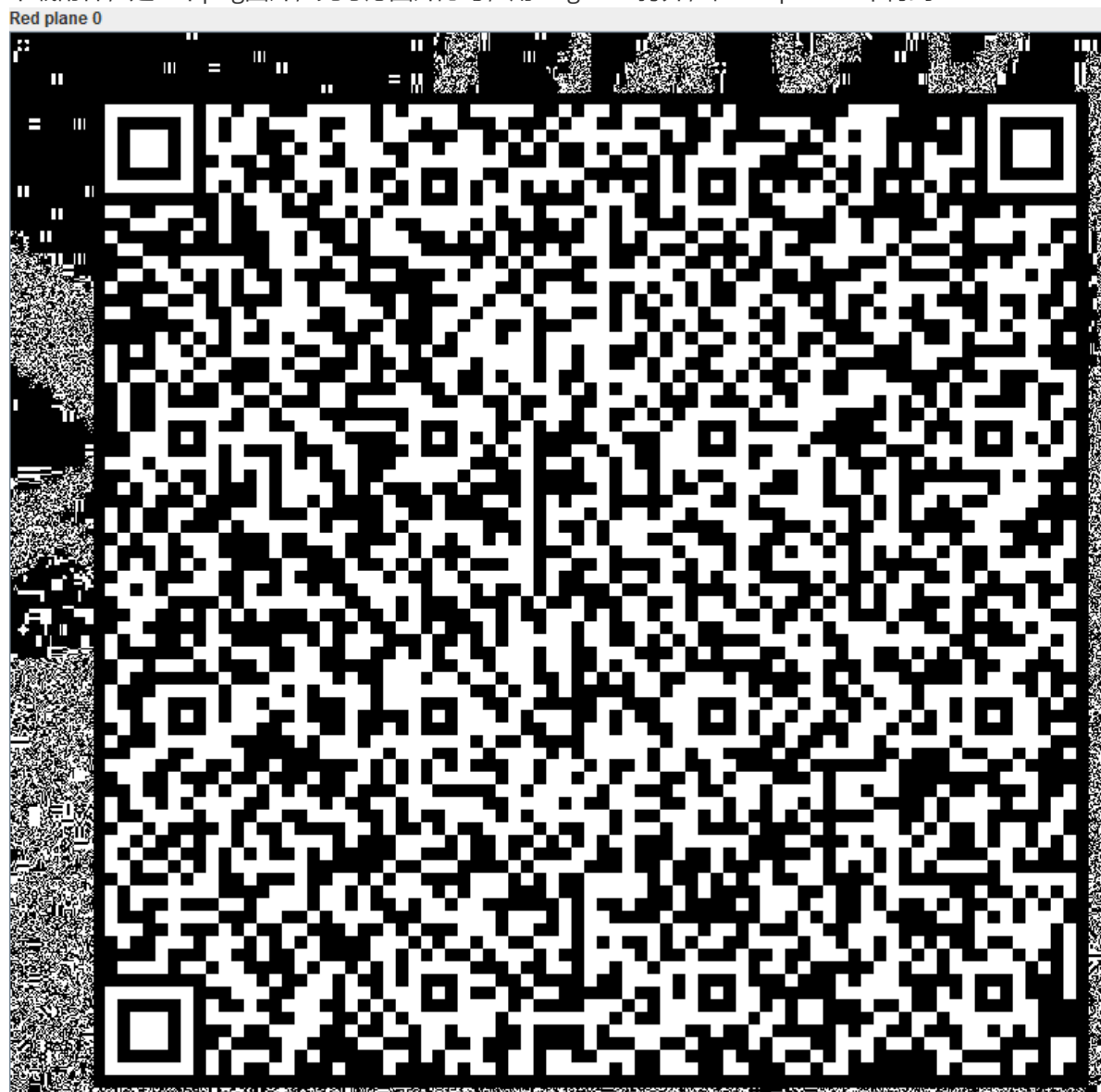
然后得到这个东西，看起来像是摩斯电码，在线翻译：

密文框：

yourflagis:4g00ds0ngbutn0t4g00dman039310ki

Hallucigenia

下载附件，是一个png图片，先考虑图片隐写，用stegsolve打开，在red plane 0中得到



二维码，扫描，得到一串base64字符，解一下，

```
.`B°DNEI...ú:à±fEj...x-ÊB...!.B).53.6JSJ.bi.õ% u0.8i.K.pÃûm`.t.Ö °i.Ädgð.$/@.õEn.«...m#æo|Ö.û .~% .ä09Â6[*£.xõZScùØ.  
¥íjI1.vëxîÄ@s.".Á..b  
ñ.i.â±èRVE  
R#..(qôÿ`ó`õIßt.)..M.BæJ.5²Ü.Ö..Äaí.±$st@.)ôI%É²+éP.±±Æð.8.mäæð7.Fiyü.Ý_  
Ö..z.í~è9x.5iZ...îç.õfÉ´...±Èõ1UzUâÆ.ù|y±.B++-. .@. |.....úe.j.-fs!.Oç.ê:úð.Ñõ...!.B.!".I.b..²ð´P.<.¥|tËÿÿ§jD.  
..Ë.í.hTADI=.....³«.....´...RDHI  
...  
.  
GNP.
```

是乱码。发现最后面有个GNP，反过来就是PNG？于是将base64粘贴到010editor里，果然是倒着的png编码，于是写个简单的倒序，将它转为正常的png

Photoshop里垂直翻转

一下得flag

```
hgame{tenchi_souzou_dezain_bu}
```

Crypto

WhitegiveRSA

直接使用工具:

```
Unciphered data :  
HEX : 0x006867616d657b7730777e794f555f6b4e6f572b523540217d  
INT (big endian) : 2559974471936861332250695601896749831380  
INT (little endian) : 7854530245008205343830713347027281383  
STR : b'\x00hgame{w0w~y0U_kNoW+R5@!}'
```

得flag