HGAME 2021 Week2 Writeup

MISC

Tools

jpg隐写套娃，将压缩包密码隐写进图片中，隐写密码可用exiftool指令查看备注得到，压缩包中有新的图片和压缩包对应新的隐写方法，最后通过把压缩包中的图片用ps组合成二维码扫码得到flag，注意隐写对密码的输入。

第一个，F5隐写：

隐写密码：

```
XP Comment                      : !LyJJ9bi&M7E72*JyD
```

F5解密：

```
F5-steganography(master*)$ java Extract Matryoshka.jpg -p '!LyJJ9bi&M7E72*JyD'
Huffman decoding starts
Permutation starts
577536 indices shuffled
Extraction starts
Length of embedded file: 18 bytes
(1, 127, 7) code used
```

压缩包密码：`e@317S*p1A4bIYIs1M`

第二个，Steghide隐写：

隐写密码：

```
XP Comment                      : A7SL9nHRJXLh@$EbE8
```

Steghide解密：

```
桌面$ steghide extract -sf 01.jpg -p 'A7SL9nHRJXLh@$EbE8'
wrote extracted data to "pwd.txt".
```

压缩包密码：`u0!FO4JUhl5!L55%$&`

第三个，Outguess隐写：

隐写密码：

```
XP Comment                      : z0GFieYAee%gdf0%lF
```

Outguess解密：

```
桌面$ outguess -r 02.jpg 02.txt -k 'z0GFieYAee%gdf0%lF'
Reading 02.jpg....
Extracting usable bits:   4930 bits
Steg retrieve: seed: 184, len: 18
```

压缩包密码：

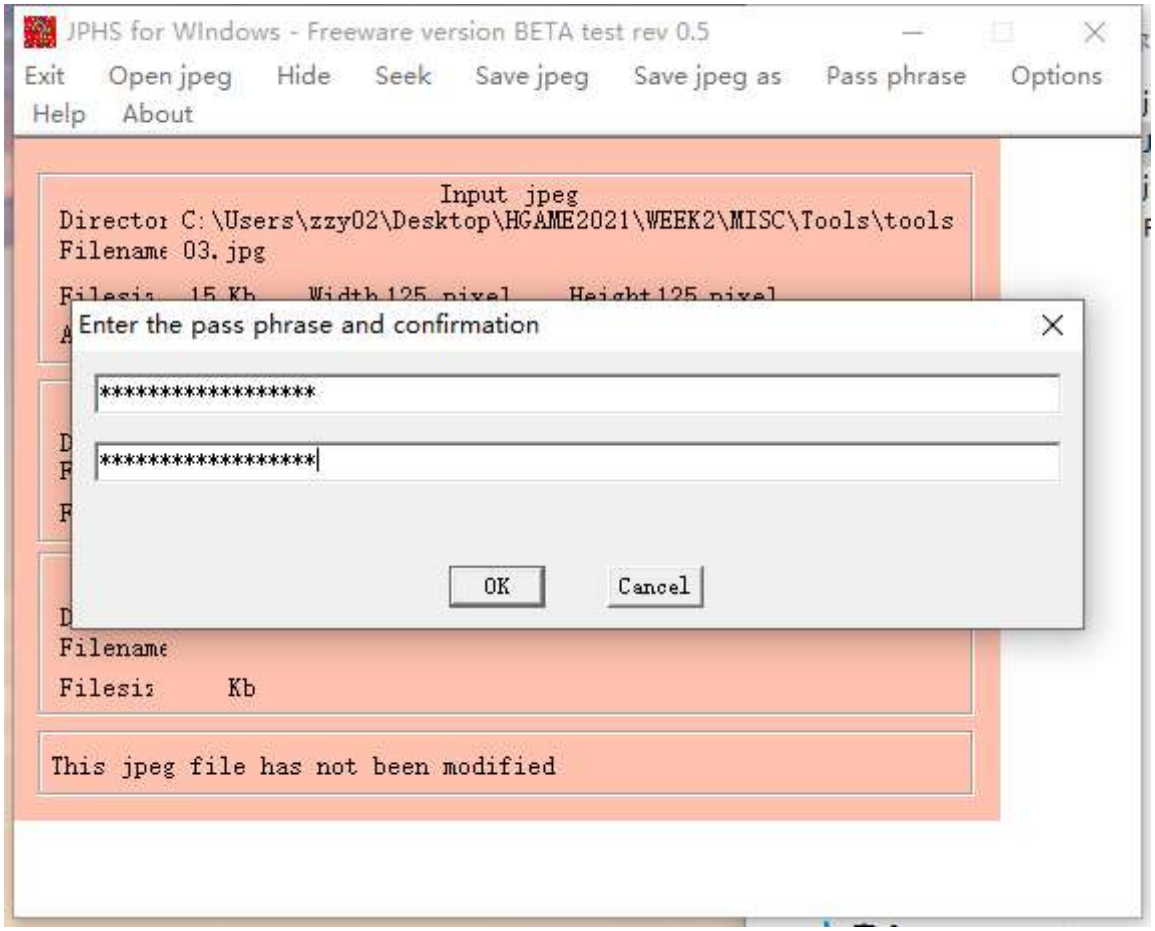
```
@UjXL93044V5zl2ZKI
```

第四个，JPHS加密：

隐写密码：

```
XP Comment                          : rFQmRoT5lze@4X4^@0
```

JPHS解密：



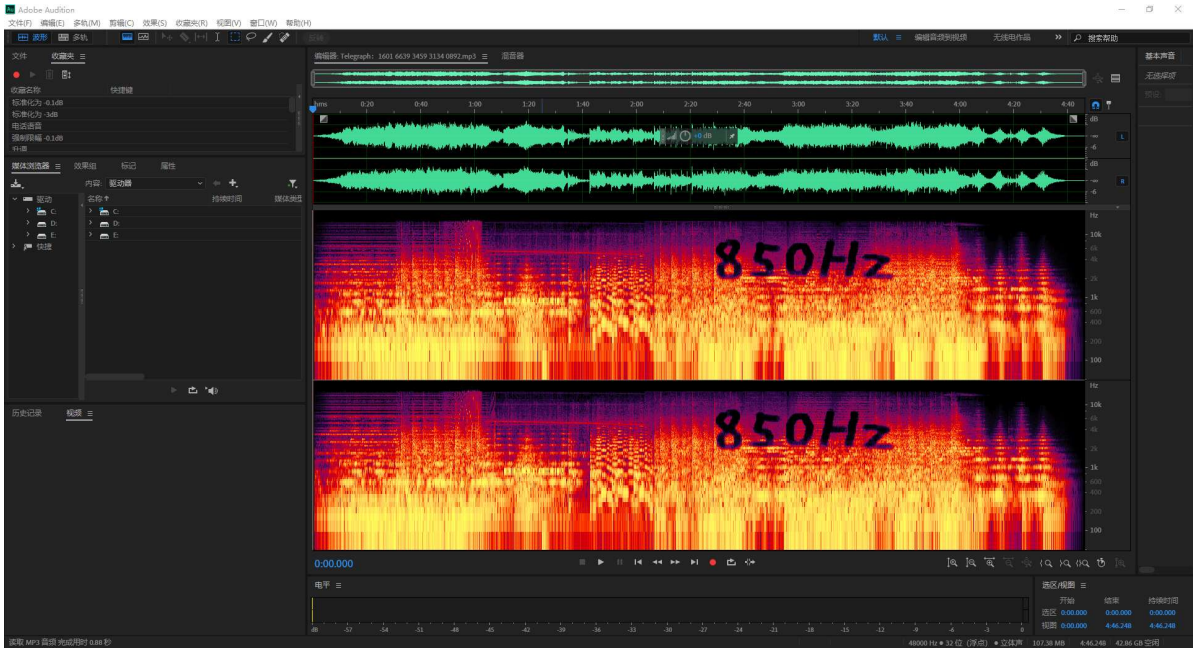
压缩包密码：xSRejK1^Z1Cp9M!z@H

拼图：

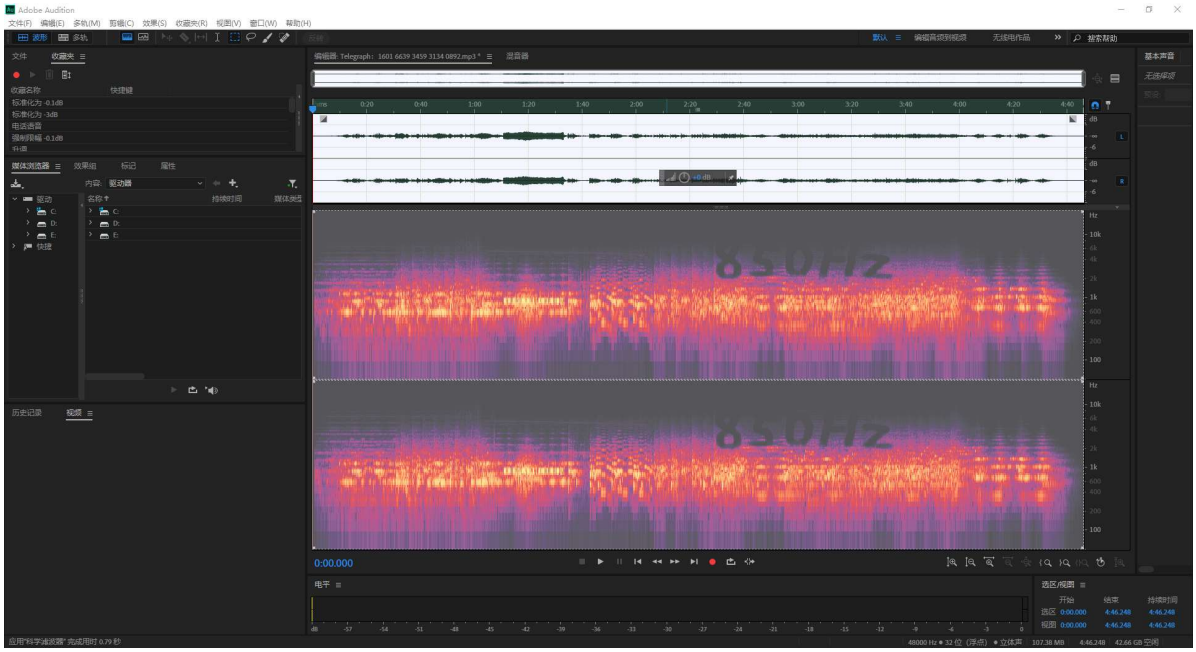
扫码得到flag：`hgame{Taowa_is_N0T_g00d_but_T001s_is_Useful}`

Telegraph：1601 6639 3459 3134 0892

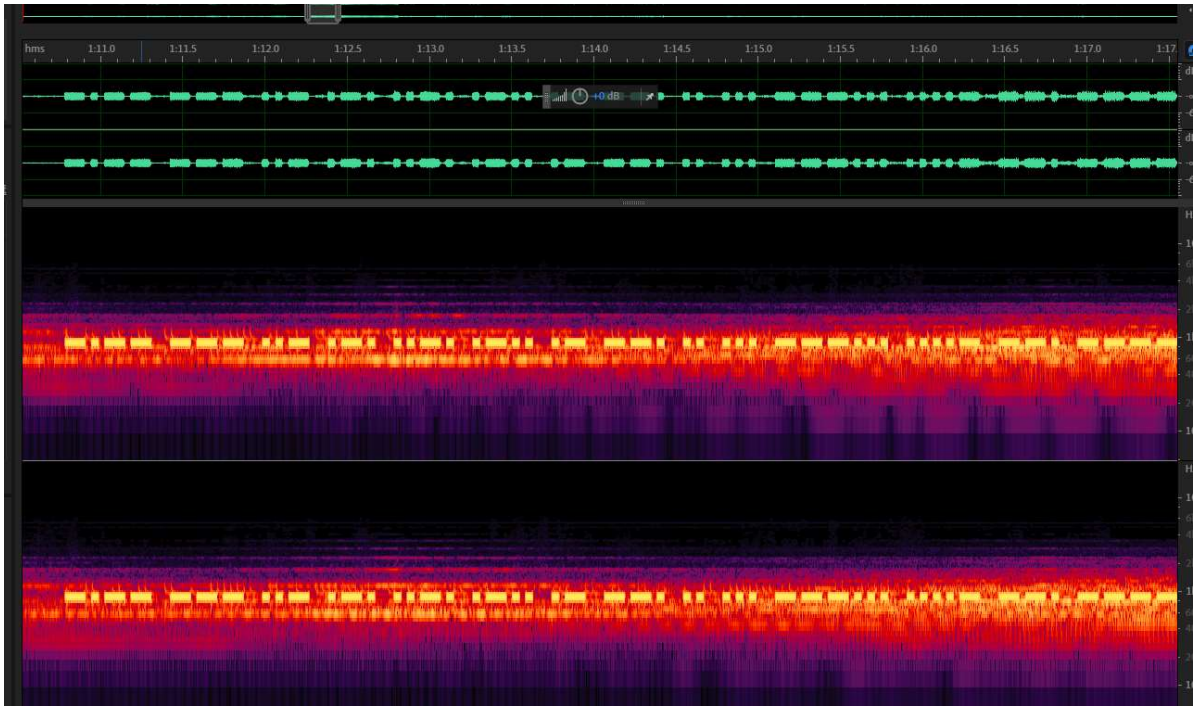
mp3文件，先用AU打开看看



提示850Hz，感觉音频限制在850Hz时出现隐藏信息，用滤波器滤波



发现某段音频不同，应该时摩斯密码，长音和短音分别标识"-"和"."，长间隔来代替/



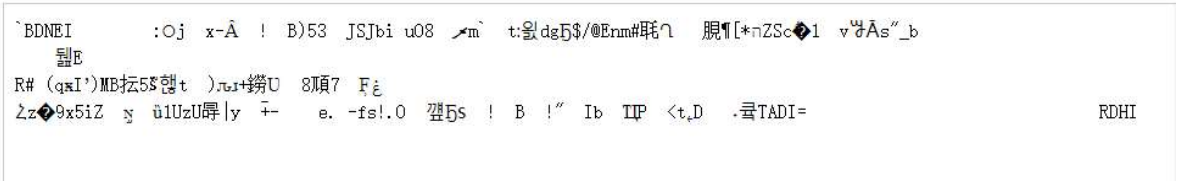
```
-.--/---/..-/.-./..-./.-../.-/--./../.../---.../....-/--./-----/-----/-../.../-----/-./--./-.../..-/-/-./-----/-/....-/--./-----/-----/-../--/.-/-./-----/....--/----./....--/.----/-----/-.-/../
```

解密得到flag：`hgame{4G00DS0NGBUTN0T4G00DMAN039310KI}`

Hallucigenia

图有点掉san值，png的LSB隐写，用stegsolve可找到二维码

扫码得到一串意义不明的字符串，应该是base64加密过了，base64解密后看到一堆乱码，但结合描述和头尾的字符"BDNEI"、“TADI"、"RDHI"是倒过来的"IENDB"、”IDAT"、"IHDR"，是png格式文件反转



用脚本跑下反转文件

```
f = open('rewrite.txt','wb')
with open('decode.txt','rb') as g:
    f.write(g.read()[::-1])
f.close()
```

修改文件后缀为png得到颠倒的flag，再颠倒得到：`hgame{tenchi_souzou_dezain_bu}`

DNS

- wireshark打开流量包导出http对象中提示flag和txt，根据题目DNS，用系统自带nslookup指令查看txt记录就能找到flag，对象为导出http对象中的主机名`flag.hgame2021.cf`，得到flag：`hgame{DOmain_N4me_5ystem}`

Crypto

WhitegiveRSA

最基础的RSA，分解N后脚本跑出

```
import gmpy2 as gp
import binascii
from pwn import *
from gmpy2 import invert
from Crypto.Util.number import long_to_bytes
p =  gp.mpz(85750408333971275248999381077 7)
q =  gp.mpz(102922494794299807508034864721 9)
e =  gp.mpz(65537)
c =  gp.mpz(74783149135389678036565451774821662479851776963726074215 5527)
n = p*q
phi = (p-1) * (q-1)
d = gp.invert(e, phi)
m = pow(c, d, n)
print(long_to_bytes(m))
```

得到flag：`hgame{w0w~y0U_kNoW+R5@!}`