Hctf Game week2 Writeup

20-啥也不会-小九

MISC

Tools

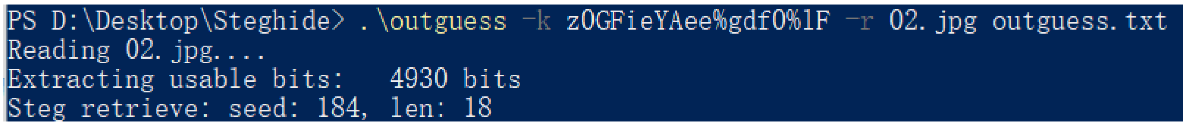
根据压缩包的名字提示 使用F5-steganography Steghide Outguess和jphs，将备注中的字符串作为秘钥逐层解压 得到隐藏的压缩包密码

e@317S*p1A4bIYIs1M

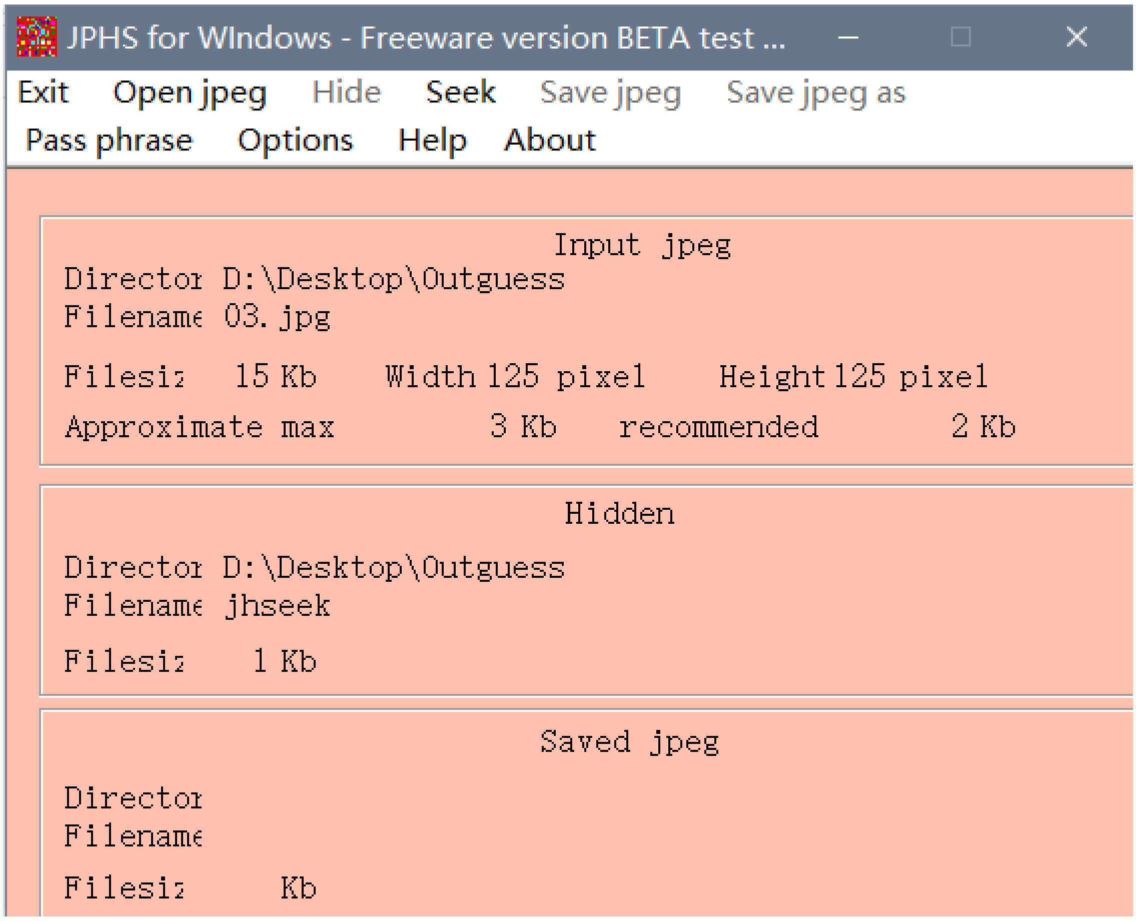
@UjXL93044V5zl2ZKI

u0!FO4JUhl5!L55%$&

还有一个找不到了懒得复现了（逃



```
PS D:\Desktop\Steghide> .\outguess -k zOGFieYAee%gdf0%1F -r 02.jpg outguess.txt
Reading 02.jpg....
Extracting usable bits:   4930 bits
Steg retrieve: seed: 184, len: 18
```



Input jpeg

Director D:\Desktop\Outguess

Filename 03.jpg

Filesiz 15 Kb Width 125 pixel Height 125 pixel

Approximate max 3 Kb recommended 2 Kb

Hidden

Director D:\Desktop\Outguess

Filename jhseek

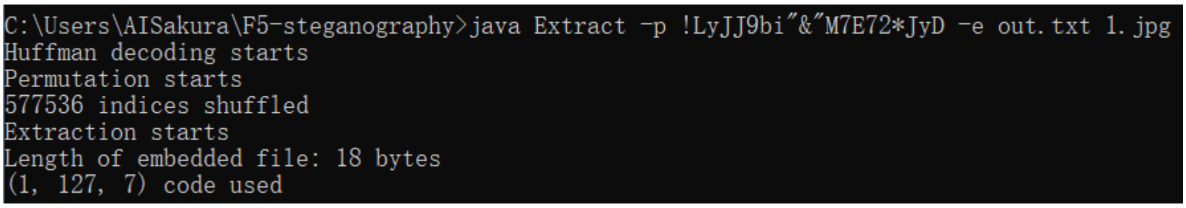
Filesiz 1 Kb

Saved jpeg

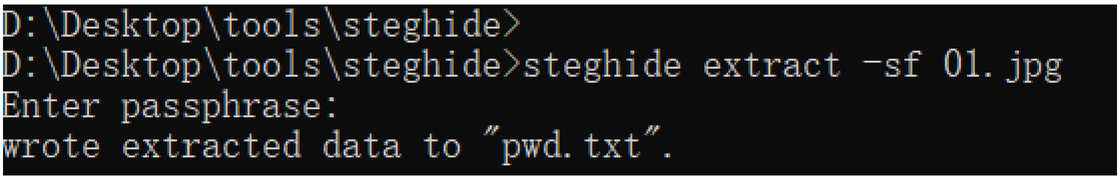
Director

Filename

Filesiz Kb

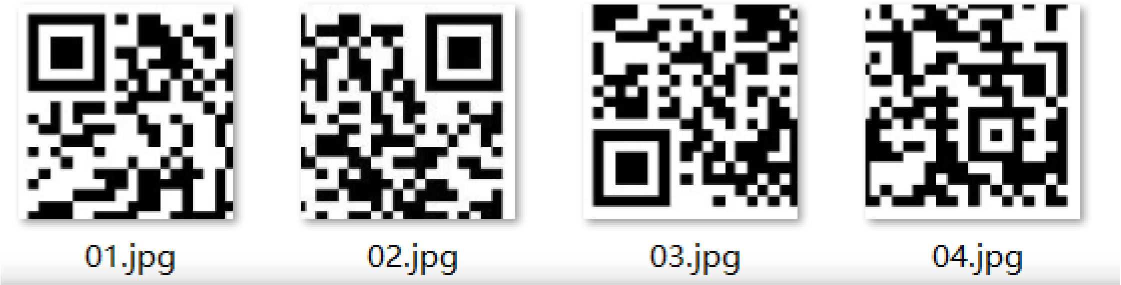


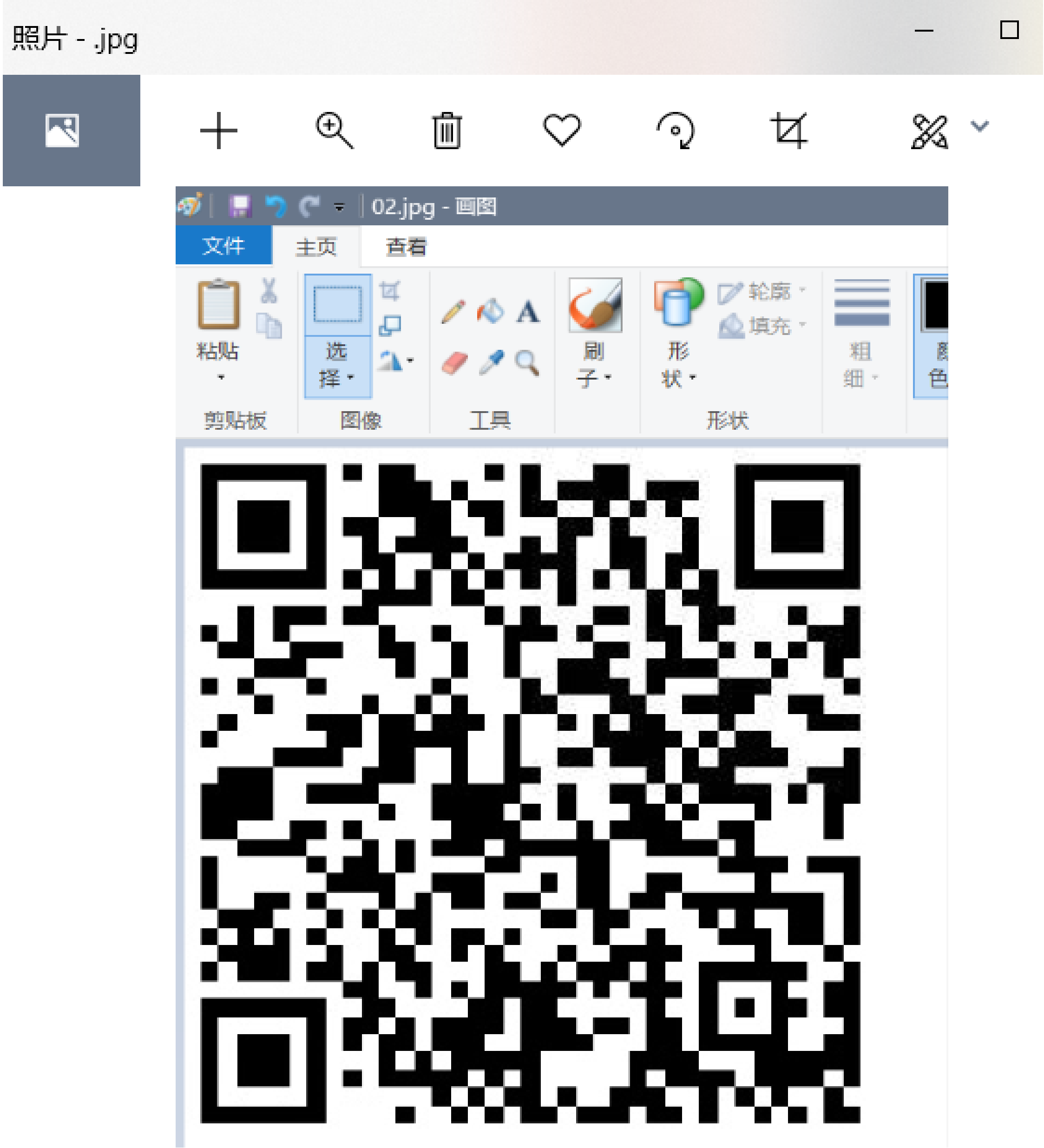
```
C:\Users\AISakura\F5-steganography>java Extract -p !LyJJ9bi"&"M7E72*JyD -e out.txt 1.jpg
Huffman decoding starts
Permutation starts
577536 indices shuffled
Extraction starts
Length of embedded file: 18 bytes
(1, 127, 7) code used
```



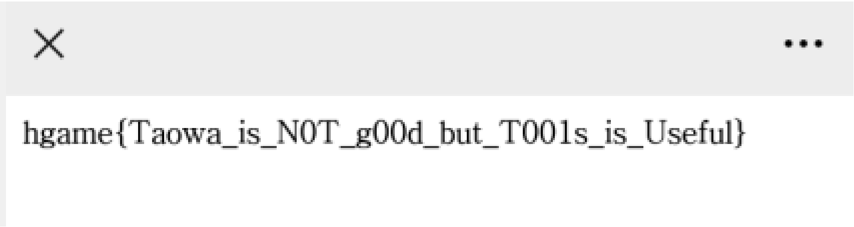
```
D:\Desktop\tools\steghide>
D:\Desktop\tools\steghide>steghide extract -sf 01.jpg
Enter passphrase:
wrote extracted data to "pwd.txt".
```

每层各有二维码的一个角 用画图拼好





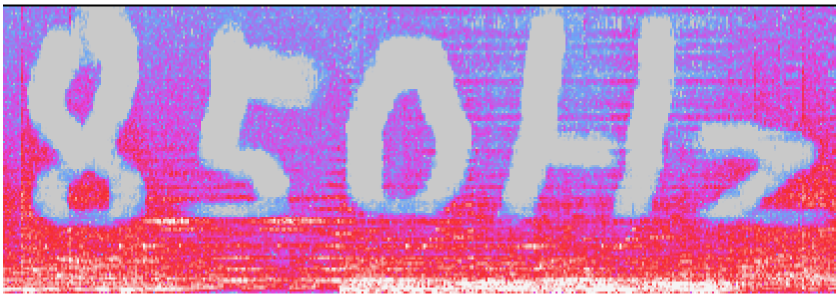
扫描得flag



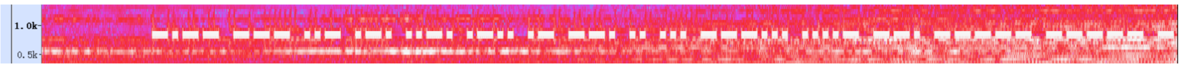
hgame{Taowa_is_N0T_g00d_but_T001s_is_Useful}

Telegraph：1601 6639 3459 3134 0892

用Audacity打开 完整听一遍发现三处不自然的电报声，1分钟出头的位置最为明显，查看频谱图发现"850Hz"字样



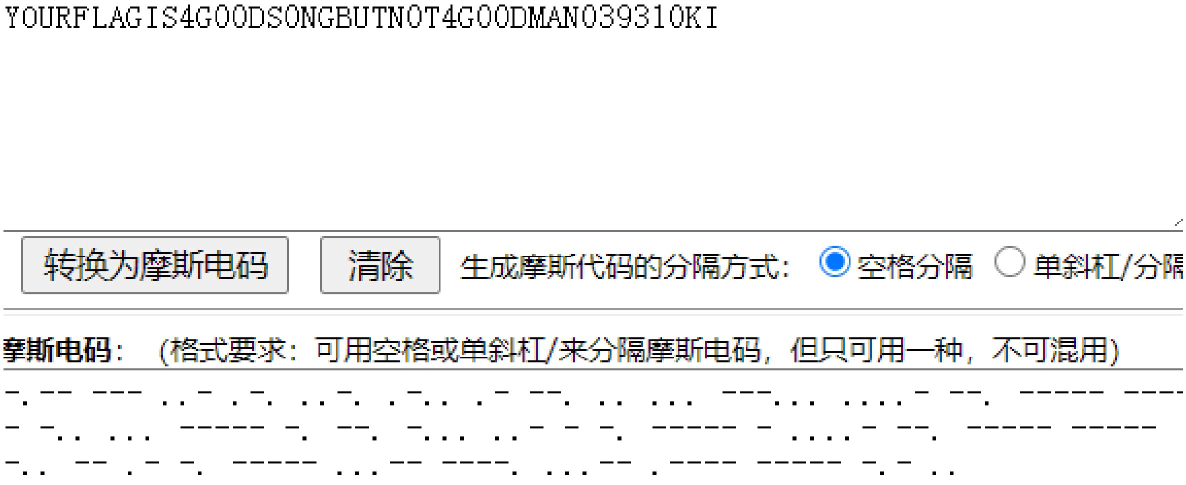
在850hz处找到条状的频谱图



显然为摩斯电码，短者为.长者为- 较长的空隙为字符的分隔

```
-.-- --- ..- .-. ..-. .-.. .- --. .. ... ---... ....- --. ----- ----- -.. ... --
--- -. --. -... ..- - -. ----- - ....- --. ----- ----- -.. -- .- -. ----- ...--
----. ...-- .---- ----- -.- ..
```

找个在线转换的工具丢进去得到flag



YOURFLAGIS4G00DS0NGBUTN0T4G00DMAN039310KI

生成摩斯代码的分隔方式：● 空格分隔 ○ 单斜杠/分隔

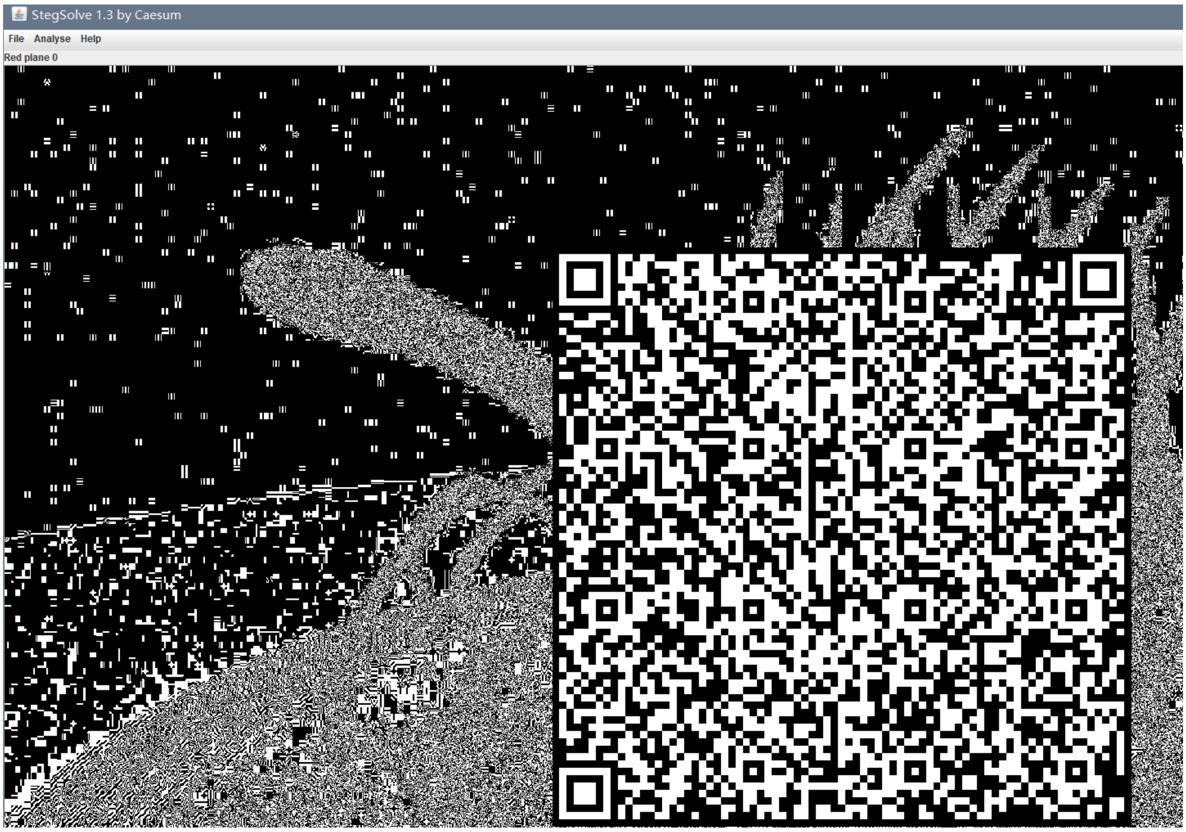
摩斯电码：（格式要求：可用空格或单斜杠/来分隔摩斯电码，但只可用一种，不可混用）

```
-.-- --- ..- .-. ..-. .-.. .- --. .. ... ---... ....- --. ----- ----
- -.. ... ----- -. --. -... ..- - -. ----- - ....- --. ----- -----
-.. -- .- -. ----- ...-- ----. ...-- .---- ----- -.- ..
```

根据题目中flag格式的提示得到flag为hgame{4G00DS0NGBUTN0T4G00DMAN039310KI}

Hallucigenia

使用常见的图片隐写查看工具stegsolve发现R G B的末位各有一张二维码，（扫出来是一样的



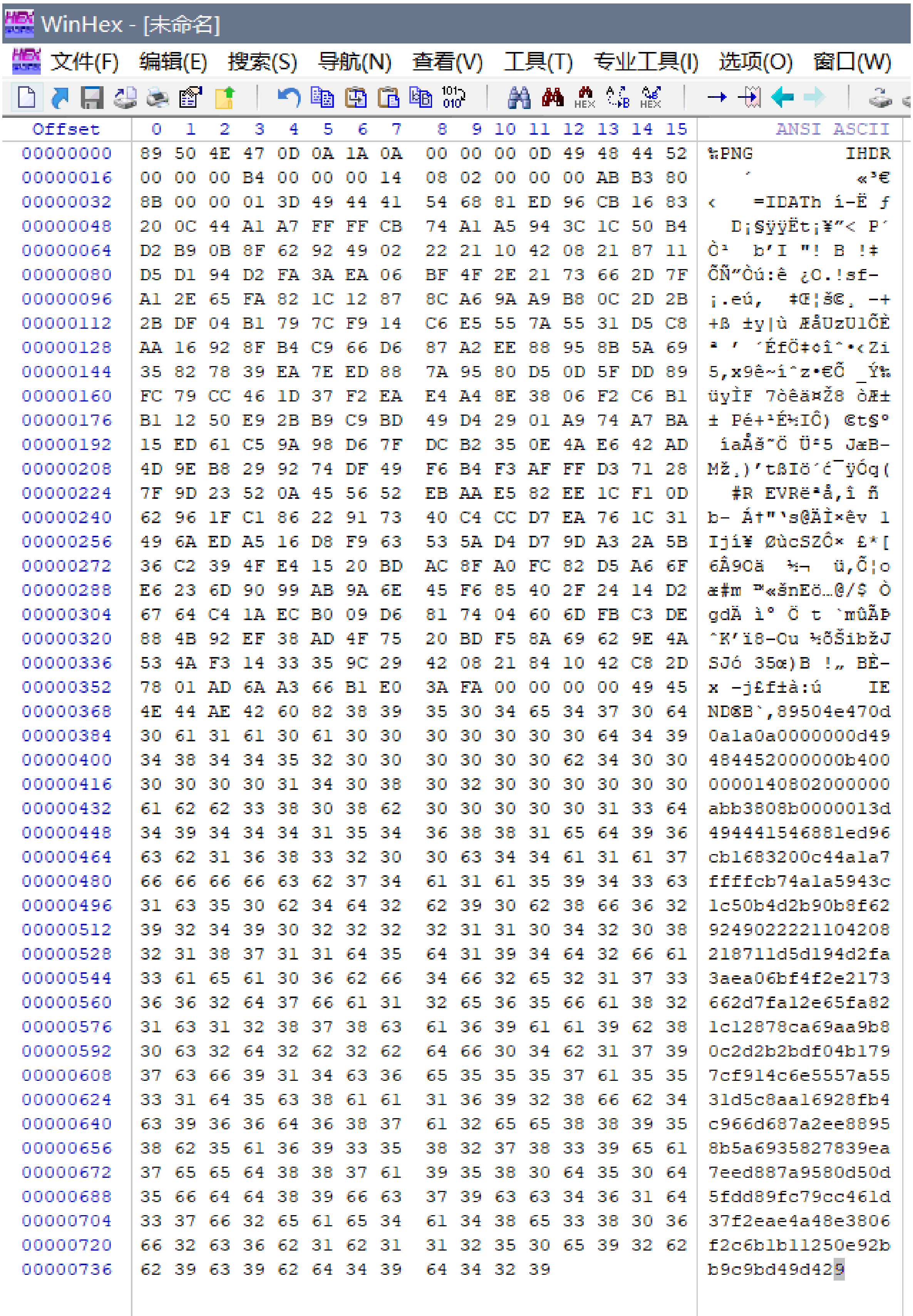
扫出的信息为

gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAEdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrL0gFeRPOcI2WyqjndfUWlNj+dgWpe1qSTEcdurXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQISICSZJijwu50rRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAtAAAAFJESEkNAAAAChoKDUdOUIk=

看到末尾的等号猜测为base64编码

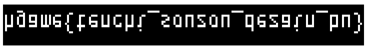
丢到在线解码器中得到乱码，注意到末尾为“gnp”即png格式的文件头倒序

结合题面提示，倒序转为16进制丢到winHex里保存

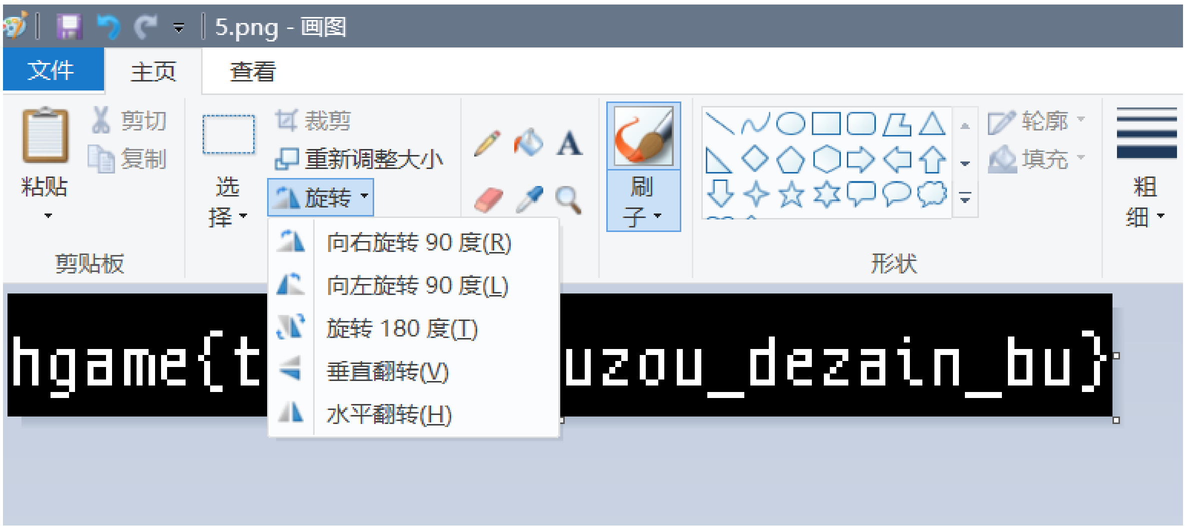

WinHex - [未命名]
文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W)

```
  Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15    ANSI ASCII
00000000   89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52   ‰PNG        IHDR
00000016   00 00 00 B4 00 00 00 14  08 02 00 00 00 AB B3 80      ´         «³€
00000032   8B 00 00 01 3D 49 44 41  54 68 81 ED 96 CB 16 83   ‹   =IDATh í–Ë ƒ
00000048   20 0C 44 A1 A7 FF FF CB  74 A1 A5 94 3C 1C 50 B4     D¡§ÿÿËt¡¥”< P´
00000064   D2 B9 0B 8F 62 92 49 02  22 21 10 42 08 21 87 11   Ò¹  b’I "! B !‡
00000080   D5 D1 94 D2 FA 3A EA 06  BF 4F 2E 21 73 66 2D 7F   ÕÑ”Òú:ê ¿O.!sf-
00000096   A1 2E 65 FA 82 1C 12 87  8C A6 9A A9 B8 0C 2D 2B   ¡.eú‚  ‡Œ¦š©¸ -+
00000112   2B DF 04 B1 79 7C F9 14  C6 E5 55 7A 55 31 D5 C8   +ß ±y|ù ÆåUzU1ÕÈ
00000128   AA 16 92 8F B4 C9 66 D6  87 A2 EE 88 95 8B 5A 69   ª ’ ´ÉfÖ‡¢îˆ•‹Zi
00000144   35 82 78 39 EA 7E ED 88  7A 95 80 D5 0D 5F DD 89   5‚x9ê~íˆz•€Õ _Ý‰
00000160   FC 79 CC 46 1D 37 F2 EA  E4 A4 8E 38 06 F2 C6 B1   üyÌF 7òêä¤Ž8 òÆ±
00000176   B1 12 50 E9 2B B9 C9 BD  49 D4 29 01 A9 74 A7 BA   ± Pé+¹É½IÔ) ©t§º
00000192   15 ED 61 C5 9A 98 D6 7F  DC B2 35 0E 4A E6 42 AD    íaÅš˜Ö Ü²5 JæB-
00000208   4D 9E B8 29 92 74 DF 49  F6 B4 F3 AF FF D3 71 28   Mž¸)’tßIö´ó¯ÿÓq(
00000224   7F 9D 23 52 0A 45 56 52  EB AA E5 82 EE 1C F1 0D     #R EVRëªå‚î ñ
00000240   62 96 1F C1 86 22 91 73  40 C4 CC D7 EA 76 1C 31   b– Á†"‘s@ÄÌ×êv 1
00000256   49 6A ED A5 16 D8 F9 63  53 5A D4 D7 9D A3 2A 5B   Ijí¥ ØùcSZÔ× £*[
00000272   36 C2 39 4F E4 15 20 BD  AC 8F A0 FC 82 D5 A6 6F   6Â9Oä  ½¬  ü‚Õ¦o
00000288   E6 23 6D 90 99 AB 9A 6E  45 F6 85 40 2F 24 14 D2   æ#m ™«šnEö…@/$ Ò
00000304   67 64 C4 1A EC B0 09 D6  81 74 04 60 6D FB C3 DE   gdÄ ì° Ö t `mûÃÞ
00000320   88 4B 92 EF 38 AD 4F 75  20 BD F5 8A 69 62 9E 4A   ˆK’ï8-Ou ½õŠibžJ
00000336   53 4A F3 14 33 35 9C 29  42 08 21 84 10 42 C8 2D   SJó 35œ)B !„ BÈ-
00000352   78 01 AD 6A A3 66 B1 E0  3A FA 00 00 00 00 49 45   x -j£f±à:ú    IE
00000368   4E 44 AE 42 60 82 38 39  35 30 34 65 34 37 30 64   ND®B`‚89504e470d
00000384   30 61 31 61 30 61 30 30  30 30 30 30 30 64 34 39   0a1a0a0000000d49
00000400   34 38 34 34 35 32 30 30  30 30 30 30 62 34 30 30   484452000000b400
00000416   30 30 30 30 31 34 30 38  30 32 30 30 30 30 30 30   0000140802000000
00000432   61 62 62 33 38 30 38 62  30 30 30 30 30 31 33 64   abb3808b0000013d
00000448   34 39 34 34 34 31 35 34  36 38 38 31 65 64 39 36   49444154688 1ed96
00000464   63 62 31 36 38 33 32 30  30 63 34 34 61 31 61 37   cb1683200c44a1a7
00000480   66 66 66 66 63 62 37 34  61 31 61 35 39 34 33 63   ffffcb74a1a5943c
00000496   31 63 35 30 62 34 64 32  62 39 30 62 38 66 36 32   1c50b4d2b90b8f62
00000512   39 32 34 39 30 32 32 32  32 31 31 30 34 32 30 38   9249022221104208
00000528   32 31 38 37 31 31 64 35  64 31 39 34 64 32 66 61   218711d5d194d2fa
00000544   33 61 65 61 30 36 62 66  34 66 32 65 32 31 37 33   3aea06bf4f2e2173
00000560   36 36 32 64 37 66 61 31  32 65 36 35 66 61 38 32   662d7fa12e65fa82
00000576   31 63 31 32 38 37 38 63  61 36 39 61 61 39 62 38   1c12878ca69aa9b8
00000592   30 63 32 64 32 62 32 62  64 66 30 34 62 31 37 39   0c2d2b2bdf04b179
00000608   37 63 66 39 31 34 63 36  65 35 35 35 37 61 35 35   7cf914c6e5557a55
00000624   33 31 64 35 63 38 61 61  31 36 39 32 38 66 62 34   31d5c8aa16928fb4
00000640   63 39 36 36 64 36 38 37  61 32 65 65 38 38 39 35   c966d687a2ee8895
00000656   38 62 35 61 36 39 33 35  38 32 37 38 33 39 65 61   8b5a6935827839ea
00000672   37 65 65 64 38 38 37 61  39 35 38 30 64 35 30 64   7eed887a9580d50d
00000688   35 66 64 64 38 39 66 63  37 39 63 63 34 36 31 64   5fdd89fc79cc461d
00000704   33 37 66 32 65 61 65 34  61 34 38 65 33 38 30 36   37f2eae4a48e3806
00000720   66 32 63 36 62 31 62 31  31 32 35 30 65 39 32 62   f2c6b1b11250e92b
00000736   62 39 63 39 62 64 34 39  64 34 32 39               b9c9bd49d429
```

、



根据题面提示用画图上下镜像翻转得flag

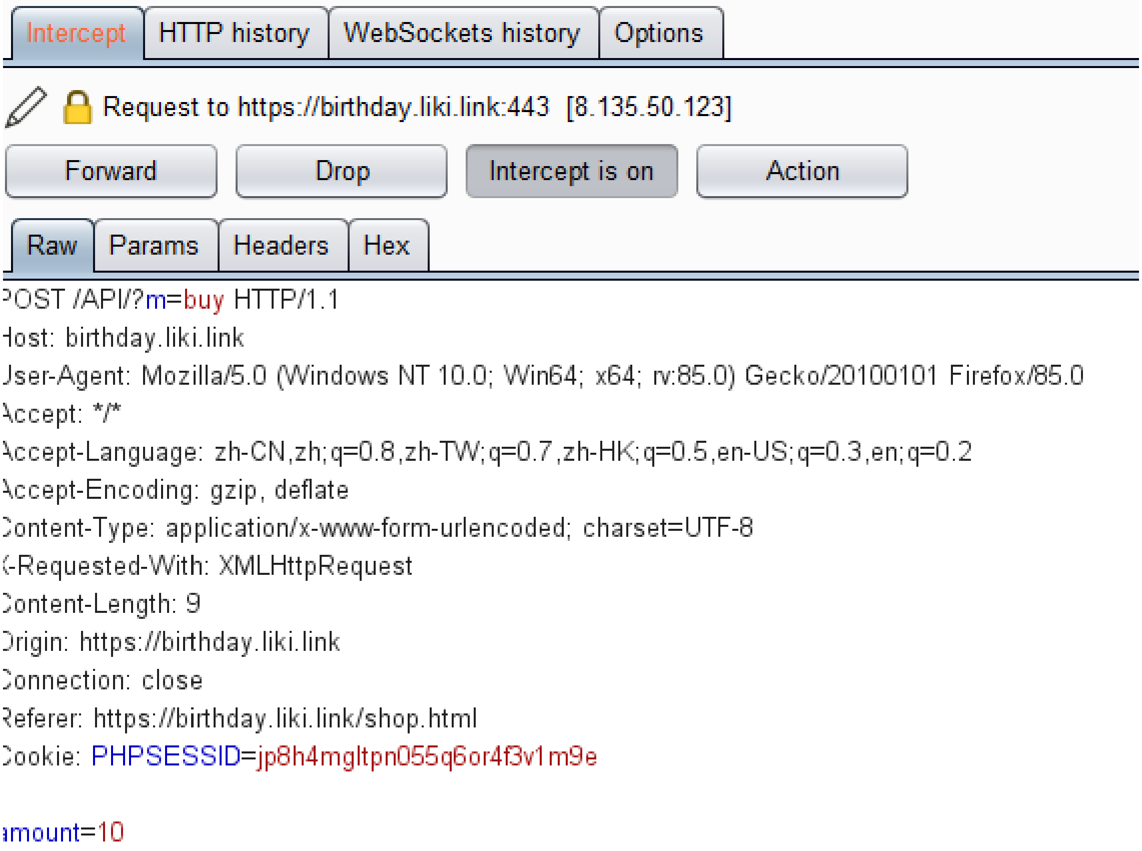


Web

Liki的生日礼物

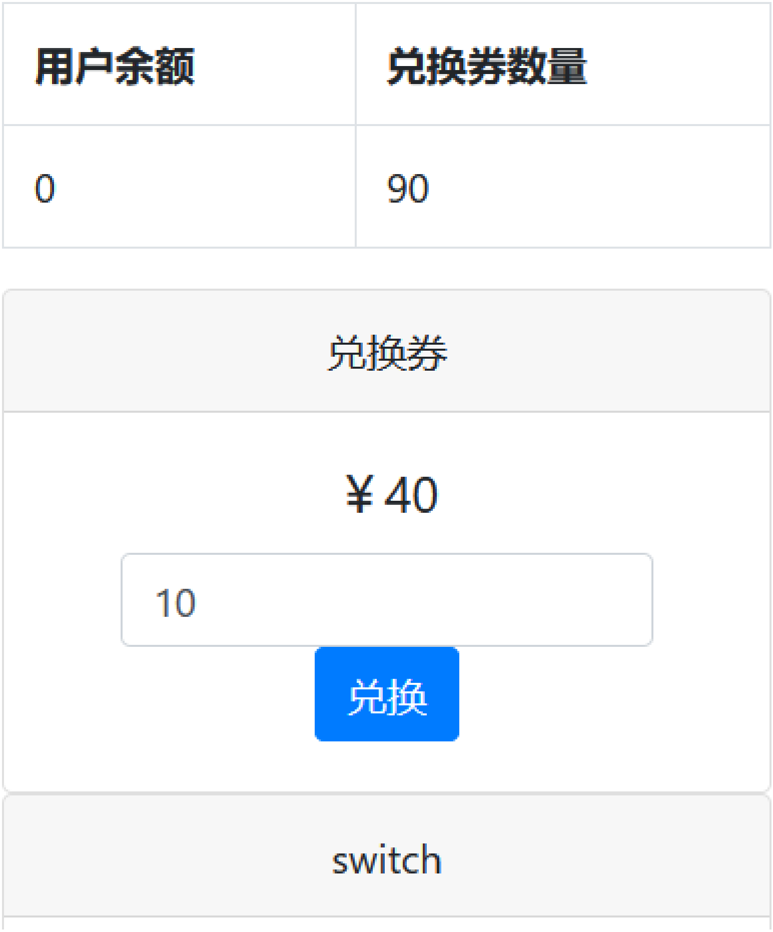
学长提示为条件竞争 搜索完了解了一下

一次兑换10张 猛点兑换 用burpsuite拦截所有请求



```
POST /API/?m=buy HTTP/1.1
Host: birthday.liki.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 9
Origin: https://birthday.liki.link
Connection: close
Referer: https://birthday.liki.link/shop.html
Cookie: PHPSESSID=jp8h4mgltpn055q6or4f3v1m9e

amount=10
```

再将所有的包发出去，得到大量兑换券

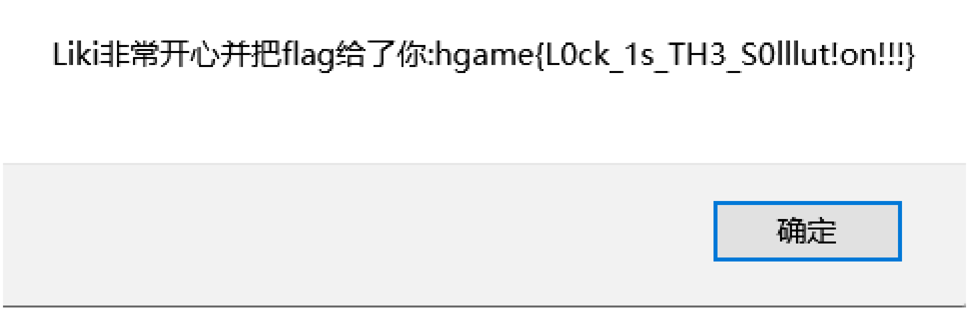


用户余额	兑换券数量
0	90

兑换券

￥40

10

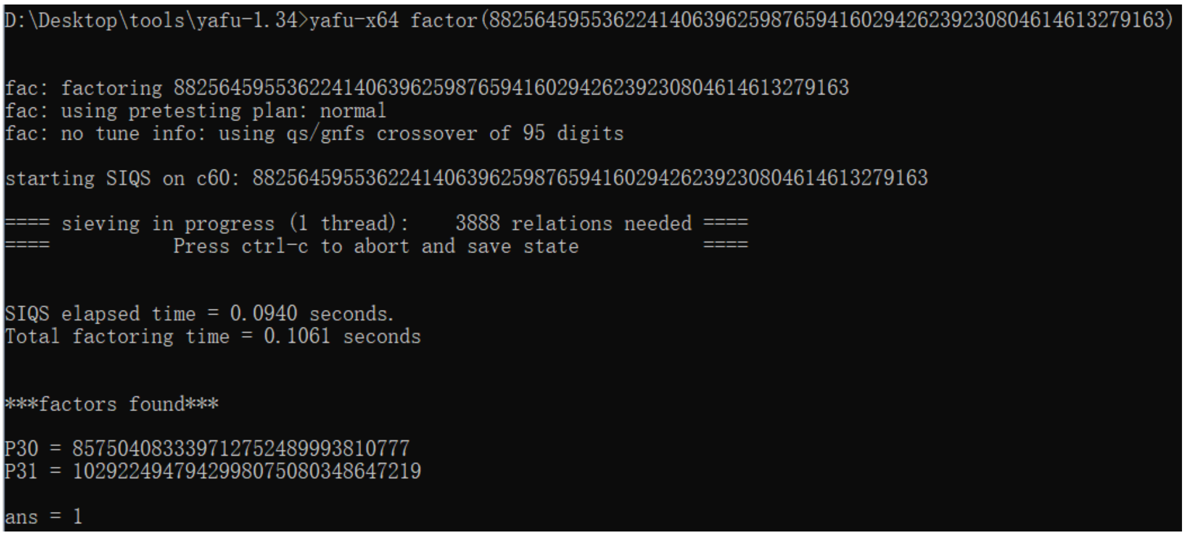


Liki非常开心并把flag给了你:hgame{L0ck_1s_TH3_S0lllut!on!!!}

Crypto

WhitegiveRSA

先用yafu将n分解为两个质数的乘积



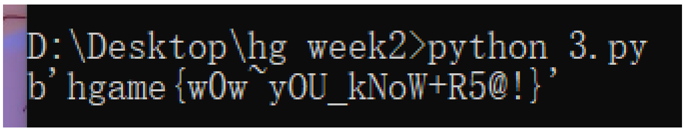
```
D:\Desktop\tools\yafu-1.34>yafu-x64 factor(882564595536224140639625987659416029426239230804614613279163)


fac: factoring 882564595536224140639625987659416029426239230804614613279163
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits

starting SIQS on c60: 882564595536224140639625987659416029426239230804614613279163

==== sieving in progress (1 thread):    3888 relations needed ====
====           Press ctrl-c to abort and save state           ====


SIQS elapsed time = 0.0940 seconds.
Total factoring time = 0.1061 seconds


***factors found***

P30 = 857504083339712752489993810777
P31 = 1029224947942998075080348647219

ans = 1
```

直接找了一个py脚本

https://blog.csdn.net/dchua123/article/details/105444230?utm_medium=distribute.pc_relevant_download.none-task-blog-baidujs-1.nonecase&depth_1-utm_source=distribute.pc_relevant_download.none-task-blog-baidujs-1.nonecase

```python
import libnum
from Crypto.Util.number import long_to_bytes
d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)
string = long_to_bytes(m)
print(string)
```

把n e c p q代入运行即可



```
D:\Desktop\hg week2>python 3.py
b'hgame{w0w~yOU_kNoW+R5@!}'
```