Hgame week1 ---Conner

WEB

1.easy auth

2.蛛蛛

3.Tetris plus

CRYPTO

1.easy RSA

MISC

1.这个压缩包有点麻烦

2.好康的流量

3.群青(其实是幽灵东京)

web

1.easy_auth

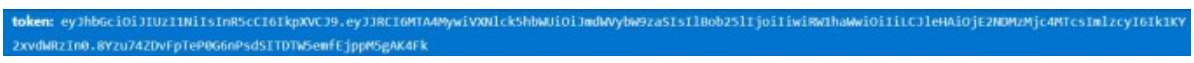
吐槽：WWW,这个auth根本不easy

诶嘿QWQ写完的时候，过了两天了，灰溜溜跑去再看一眼

阿巴阿巴，一开始毫无思路

注册无用，登进去打开f12，依旧无从下手

学习各种带登录界面的web题后准备康了一眼



哦豁，有个taken，跟JWT类的题挺像的

找个网站翻译翻译，什么叫做惊喜

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JJRCI6MTA4MywiVXNlck5hbWUiOiJmdWVybW9za
SIsIlBob25lIjoiIiwiRW1haWwiOiIiLCJleHAi
OjE2NDMzMjc4MTcsImlzcyI6Ik1KY2xvdWRzIn0
.8Yzu74ZDvFpTeP0G6nPsdSITDTW5emfEjppM5g
AK4Fk
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

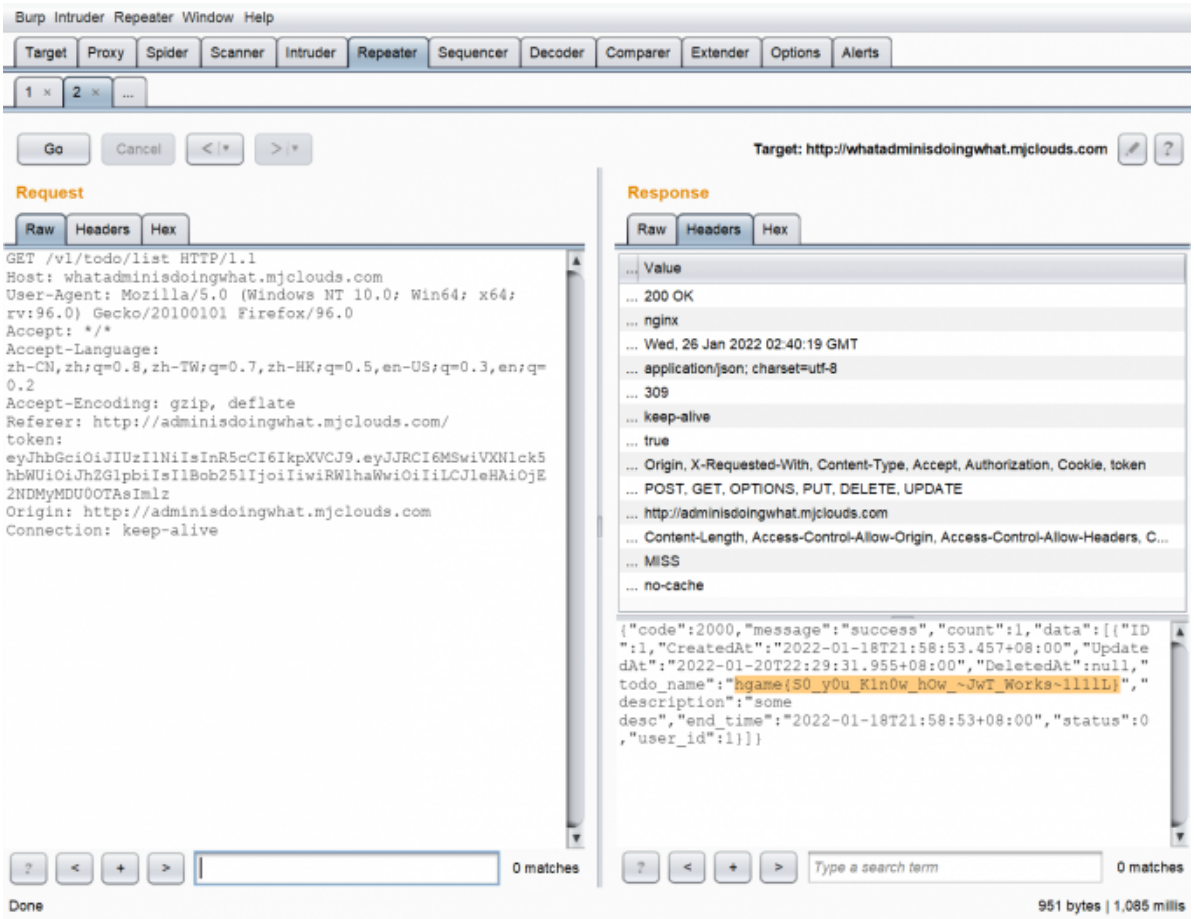
```
{
  "ID": 1083,
  "UserName": "fuermosi",
  "Phone": "",
  "Email": "",
  "exp": 1643327817,
  "iss": "MJclouds"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) secret base64 encoded
```

好活，齐全了，准备改一改ID和username就准备改个包提交了，中途看的几篇文章都说要爆破JWT的key一下，还去虚拟机里用jwtcrack爆破了三个小时，没结果，结果一问学长这题是不用的,泪目了

之后就比较方便了，抓包改包，把id改为1，username改为admiin,记得加个"sub":"admin"，再次生成一个token 放回去，放个结果



在这里返回的头文件里就能找到flag了

2.蛛蛛

做出来的第一题，谢谢出题学长，给我做下去的信心

一开始乱点，后面打开f12乱点，www,点到四十多页太累了就写了爬虫，往后爬了一百页

```python
import requests
from lxml import etree


url="https://game.summ3r.top/Tetris/index.html"
headers={
"user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36",
}
resp=requests.get(url,headers=headers)
#print(url[:47:])
print(resp.text)

# for i in range(100):
#     et = etree.HTML(resp.text)
#     a=et.xpath("//body/a/@href")
#     for text in a:
#         if (text!=""):
#             key=text
#             break
#     next=url[:42:]+key
#     print(f"第{i+23}页",next)
#     resp=requests.get(next,headers=headers)
```

爬虫的代码在注释里啦，让他返回了一百多页处的地址，点进去一看，f12，任务结束。

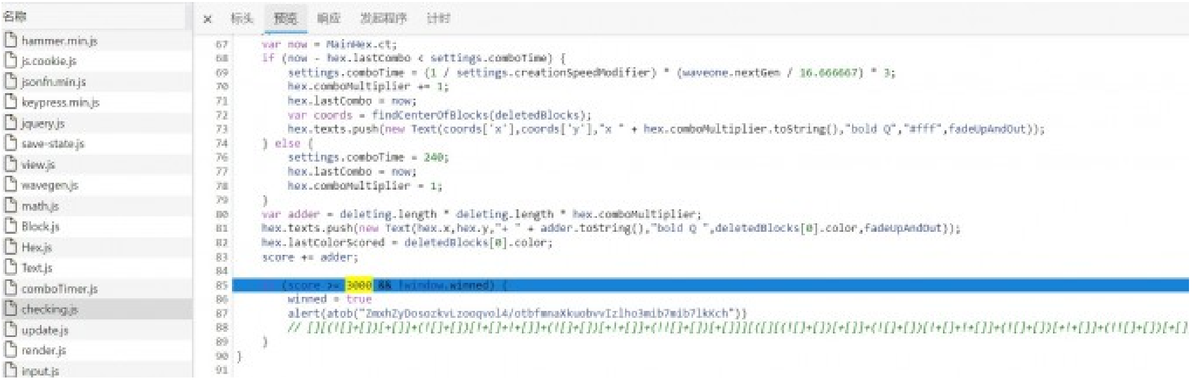
3.Tetris plus

游戏挺好玩的，他说不能三千分，我就先试着玩了玩，实际上可以，嘿嘿

就是总提醒我flag被隐藏起来了，f12一波找不到，继续玩，系统估计放弃抵抗，玩到了7000多分（滑稽）

后面经过学习，认为这种游戏的考点仍是JS代码审计，那么让我康康你的js

找出来是很帅，过程很狼狈，敲了像flag,2999,3000等关键字，在js文件里一个一个找，好不容易找到如图的那下面alert里的奇怪东西解个码，发现就是提醒我们flag被隐藏起来的那句，心情又悲痛起来



最后，找到学长提示注释有用，一看这么一大串的放弃了，后来做crypto的时候看到 jsufck，回来把他扔到控制器里一跑，flag出现可喜可贺！！！

CRYPTO

1.easy RSA

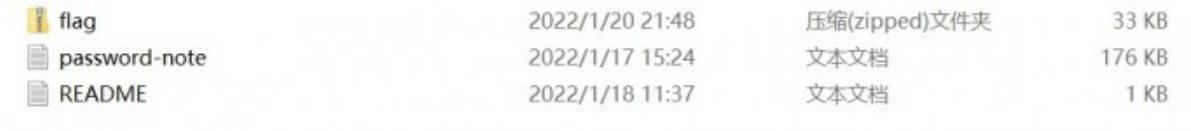
这题一开始也以为挺难的，主要没看懂，学习一波简单的rsa，看到加密脚本里的注释突然悟到了，分别对应了e,p,q,c，问题是算出每一组数的d，就写了个脚本跑了一下，结束。

MISC

1.这个压缩包有点麻烦

唔，拿到了个压缩包，连第一次解包都要密码离谱啊，第一次的密码是我爆破出来的，用ARCHPR暴力破解了十多分钟，这一段确实不会，会好好看官方wp的。

第一步结束，得到



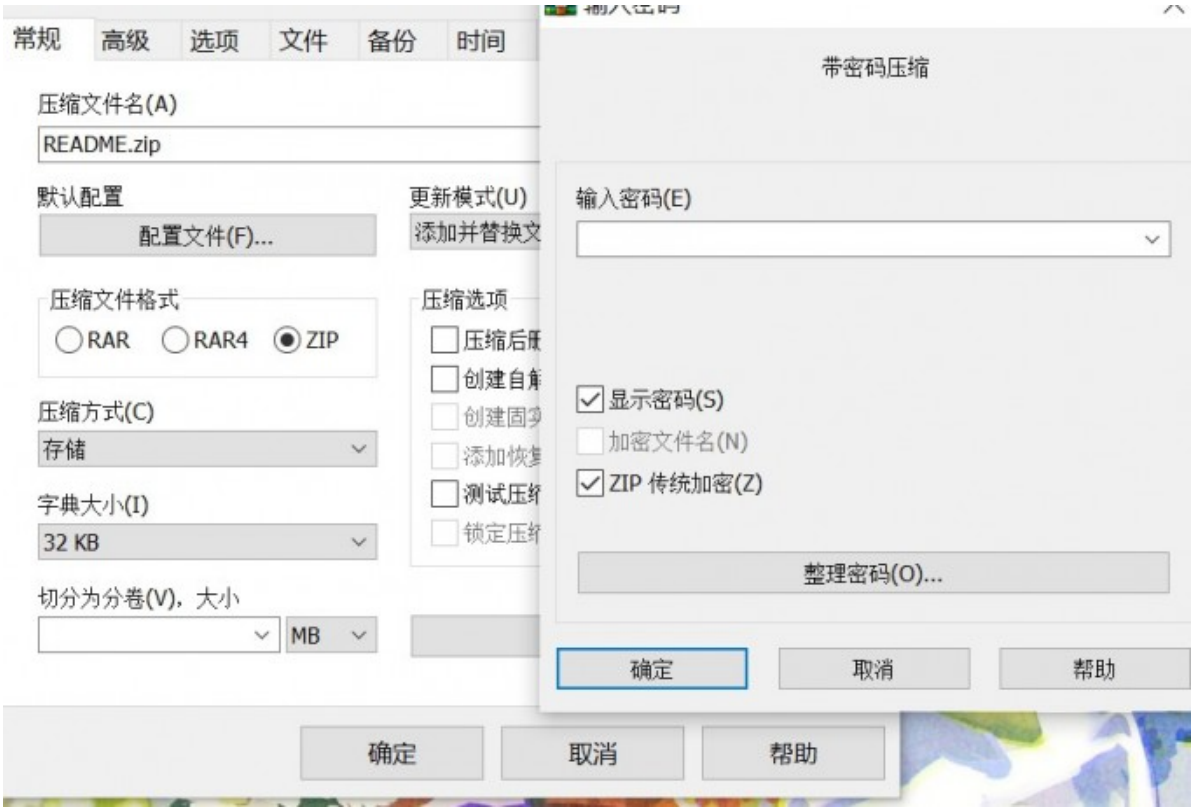
所有的密码都在password-note里面啦，用字典攻击，几秒就结束了。

进入下一个安装包！这提示QWQ

全是英文，不太好懂，最难理解的是store的意思。

由于压缩包内README和外面压缩后README的crc32值一样，判断是用明文攻击

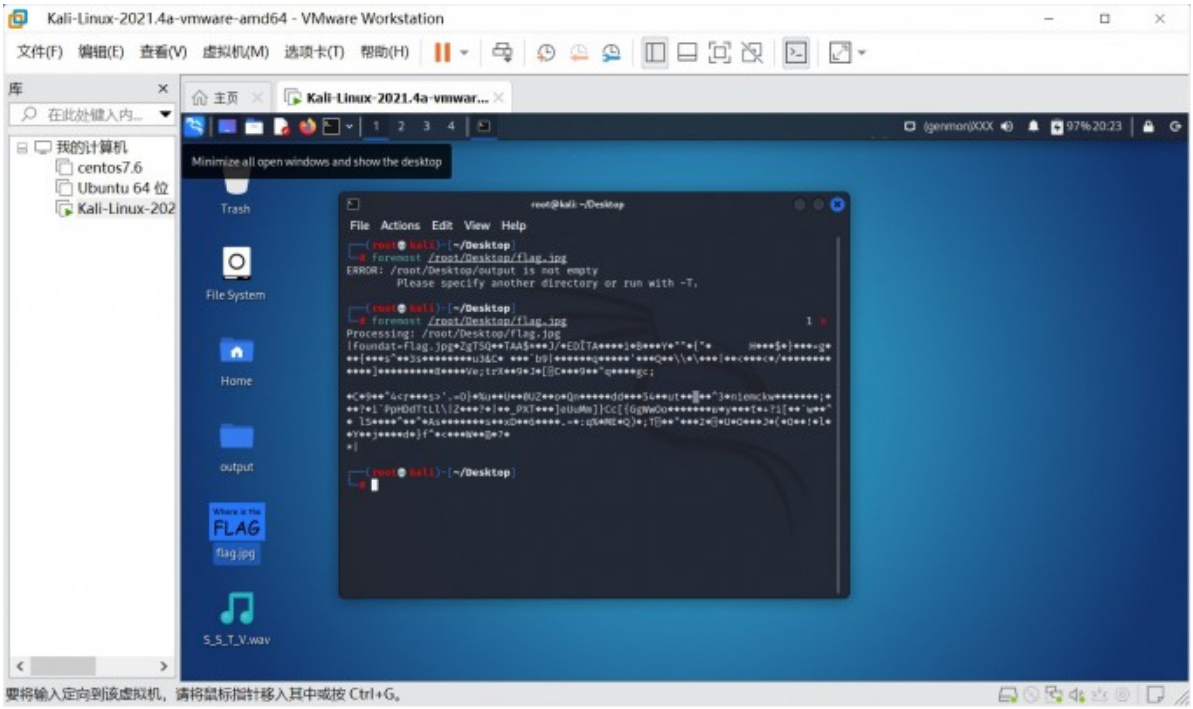
其中过程比较忐忑，明文攻击一直说哪里不行，不给我弄，恼羞成怒了，属于是。最后发现是压缩方式要用存储，对应了提示里的stores



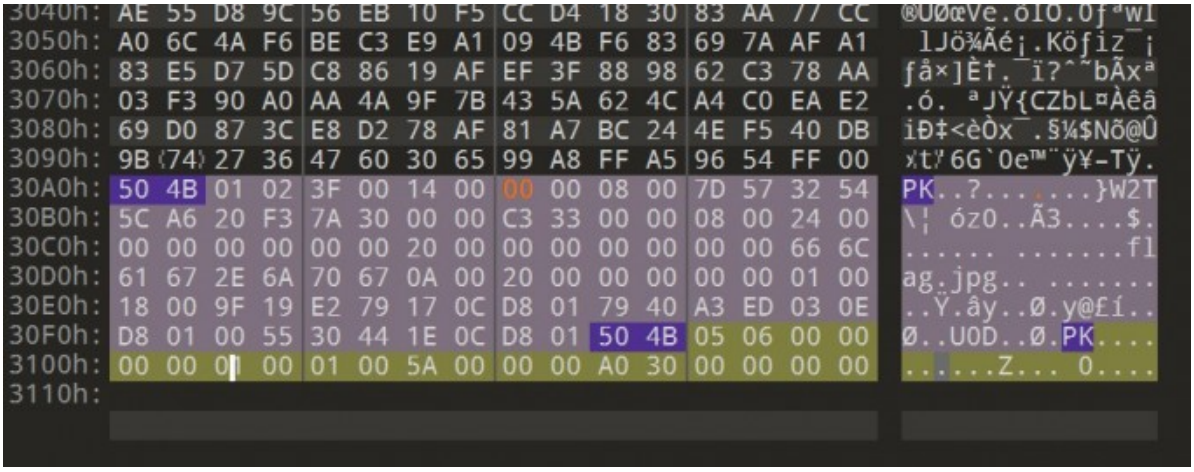
把README.zip和FLAG.zip都扔进去，破解个5，6分钟得到密匙，保存一下弄出来的文件夹，就是不用加密的压缩包啦

点进去拿到图片，又毫无思绪了

查看属性也不对，elif也没，用010 Editor康一康，好家伙咋还有PK呢着码里面，丢到foremost 里分离一下



得到output文件夹，TM还是一样的感觉，output里面仍是熟悉的照片，呦西，再来一次明文，啊这里压缩后,crc不一样的，眼泪流了下来。



整了一会儿，把压缩包在放到101里看一看，看看是不是伪压缩，感觉挺像，把几处09改成00保存为zip格式，再次打开，ok了

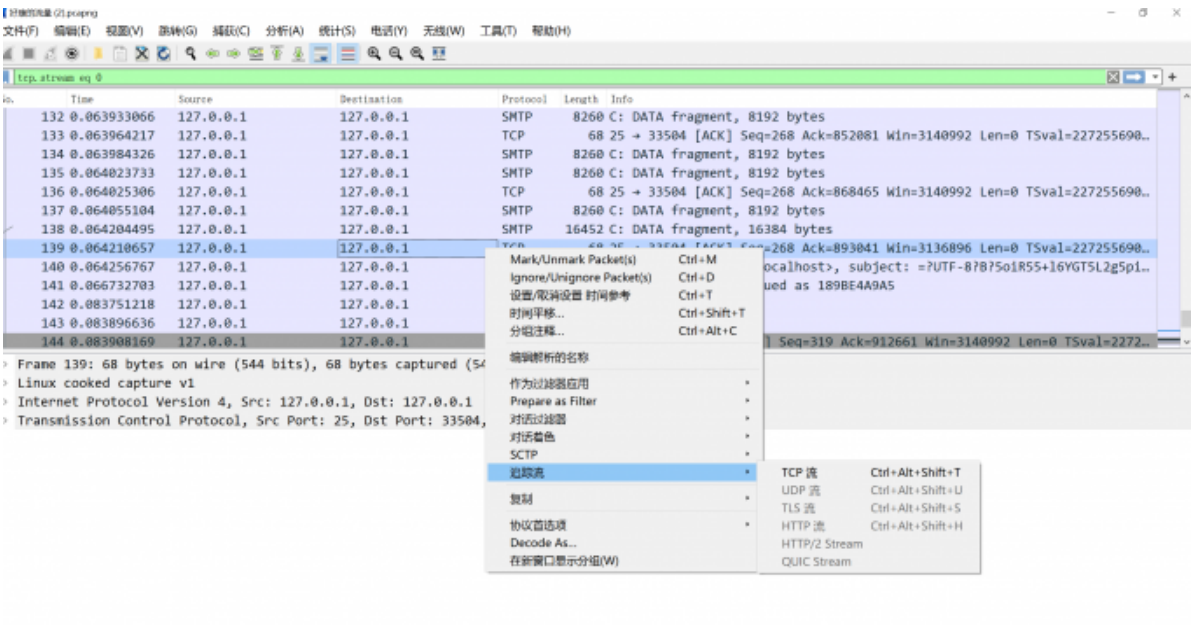
得到flag!!!

hgame{W0w!_y0U_Kn0w_z1p_3ncrYpt!}

2.好康的流量

这题令我一度绝望，摸了好几天才弄出来，学长一说校外的师傅门三分钟结束战斗，更痛苦了。

首先，拿到流量包，学习一下流向分析。



对我们的TCP流狠狠追踪一波

得到下面一长串

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 好康的流量 (2).pcapng

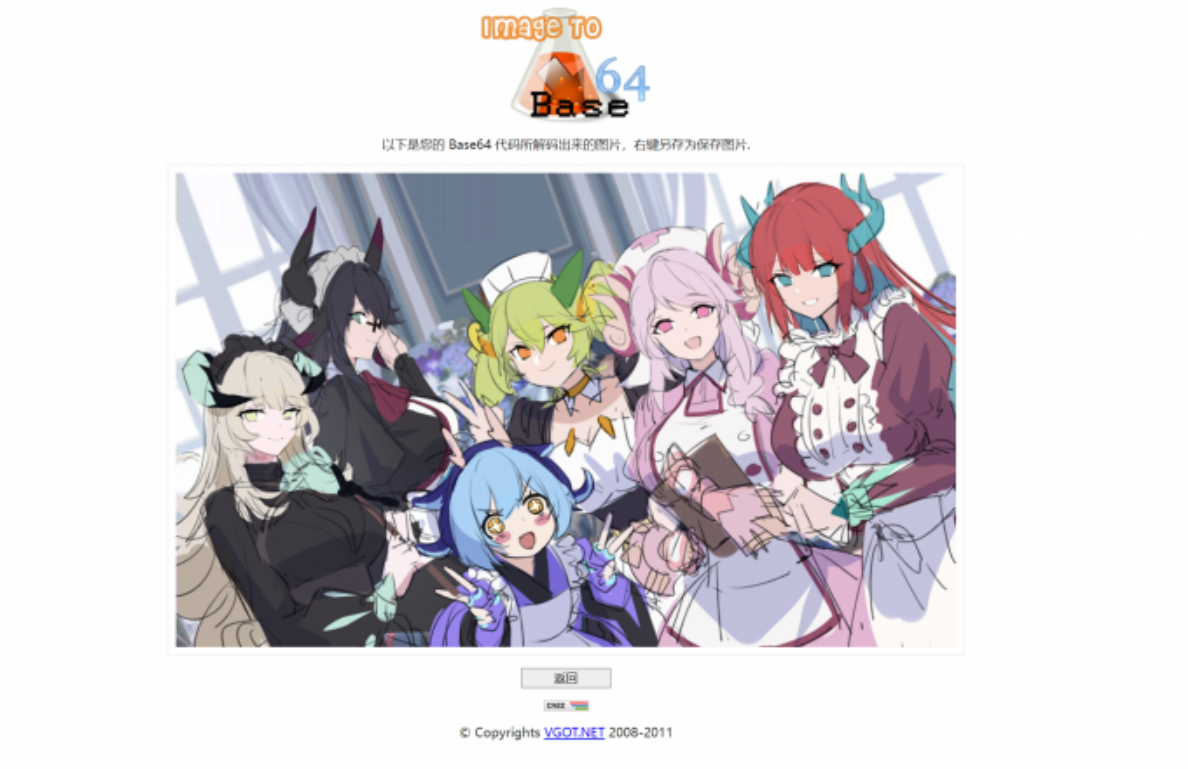
```
Content-Type: text/plain; charset=gbk; format=flowed
Content-Transfer-Encoding: 7bit



--------------C749C3423D3952356F67A368
Content-Type: image/png;
 name="=?UTF-8?B?5rap5Zu+LnBuZw==?="
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename*=UTF-8''%E6%B6%A9%E5%9B%BE%2E%70%6E%67

iVBORw0KGgoAAAANSUhEUgAAA2MAAAIPCAYAAAD+cAacAAEAAElEQVR4nOz9eZBlWX7XCX7O
du99vseSkftamZVZWaWSVJtUqpJKIIEaAU0bIGiaMZuxXgzNYNPMwHTb9Fib0TYDA3RrpmEG
EKIQaGGQUCPQioS2kkpb7VVS7bkvkREZkRHh4dt7dzvnzB+/c++7z/25h7tHRGZkdvzSPCPC
33t3e/eec36/7/f3apP/cGnoooAEDkDv99xuoma5KDh99xJLizkmanmhlT+69+0b72v3fXv
o27nqNud8/4QIuOm5vL6NhvrE5roaXcC46pkc2tCXTeAosgdC4s5AONxRVU2xBZMYSjyDJc5
sNA0LdVOTdu0xBgPPi5AKYV1lnwxw40sSiloFEppDJYszyiKAlc4iIE61NQ7Jc2kIZpINBAb
iIByCuUVIQZ8CIQ6AlHOtzuUCLTpH1ahFMQY8crTli1eeUIIhDpACzrTWCwmNyilCDHSVp5W
tXjtiY28T6GwuWF1NOLMvStYNFtbE8aTmth0++uuw/TfMULrW8qyptqpCTrS1tuU5SWUuvZ9
FoG2e6GFrckOG5slW+MKlaXrmT4fQ2Bnc4MQG2KM8lrargoGZwuKxSUW11blu0vHt+Q9d65a
sKrfT6gDSydWufdtjxNjmP/9Hng/K0LtOfvC16gmY1SmUUBbK65u1WxWY6JXrCwWmFyxOa7Z
aRt8I2cdQ8C3DU1V4ictQSuCNYDGtoa15RGn1hZZKDKUgjK2bG5WjMuGVu9zvLuP+yY8b3Pj
evdzvdvdb/u7Y/d2rnUcx72+19rumzSs0SwWGUtFhlGwMy5Z39hke1zivZ95bzcPoTTGWVyW
Y5yF9MwqBbkzrC0WZNawNa4YVw1FnrO2ssIoz9M+DasrK6ytrJI5d8gjlX3EGCmrkvWrV9na
3sbHSIiB8WTCzqTEWc1i4agbz1bZ0viI0hoVI01TU453qKuSGEK/Za0U1mW40QiXFyhjUUQU
kdwZlkcZ1ihGBJYWRjz42JNorffOJQdFlOM3RrG4kHNidQljNJeubHHx0hZNG9DaQgQfIt57
fNviQ4AYUQqsteR5TjHKyTKHtQatNUoplFL9MXnv8V7mDKXox9S29bRtIMaIMRqtNcZonLMs
LeasLucsjBxGp/c3nq3tkitXJ5RlSzjk+TpnOLk64szpRfLcsrlVcfHSNpvbFSHs3YZKnykK
S4xQlg1NG/ZueJ/QWrG8lHPn6UWWF3N88EyqhnHlGVee1gemk+3gc0pROMvKUsHyosNZjUr3
2XWF6v93C0Y88J9v1jjoWezXFNcRSileeO0yL7xyjjvvugv/2nkee/wJ8iw72jgwZ7sfe/lV
/vnnvsKfevuD/MV3vO26tjeMmfXUIcOHyPZOzeX1MVs7dXp2jh4KcJlhdSlnaSGtd2rPeNIw
njQ0recGneahQmuF0YrMGYrcsriQsbSQkWcGrQ93jbSKEGVEnXkhhkgTPXWTBuy3UCilsGjy
zGJTwqEU6KgxuUY5BURJbqqAVkp+n6UJO0RCiH3CoYNMPPK5a0eMkagDMYRp0qIgEokxElTA
q5T0OIXRBh1kYgRQXt4//MpU/1/6d5QbVg3eMfMvpeS4M40OacJ10wVJjNPzU8jEopWe2QdE
```

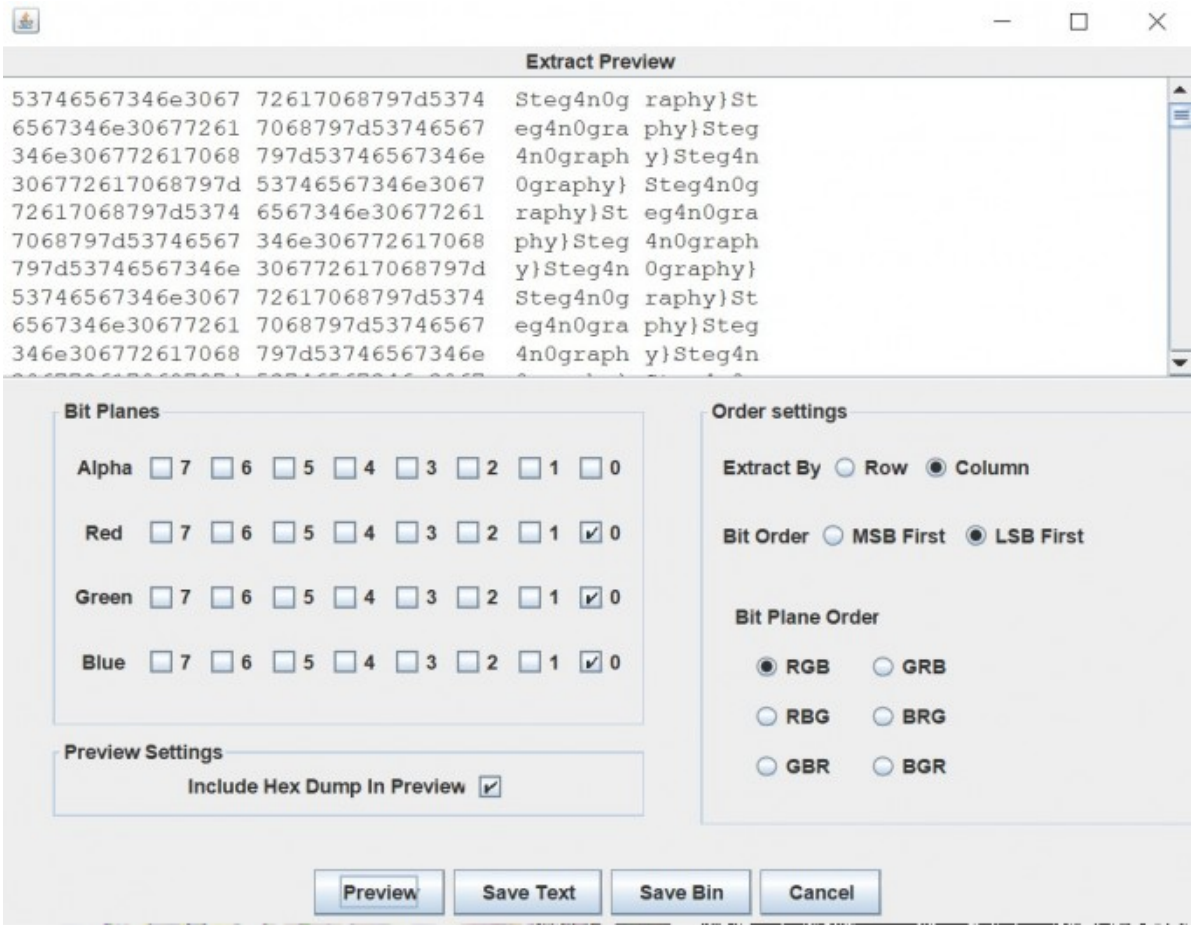
根据一天的学习，着好康的png就是这段乱码，丢到好用的网址里用base64生成图片



让我们对这张图片分析一下，下载stegsolve,顺便装的java环境，哭，我这是为了这醋才报的饺子。

一直左点左点，找到第一个条形码，扫出来得到一半flag

革命尚未完成，呜呜呜，到这里我是拒绝做下去的打开analyse里的data extract，一开始我就是LSB冲的，换了半天色到也没什么结果，过了一天试到column，终于行了，让我们拼接拼接，得到flag了



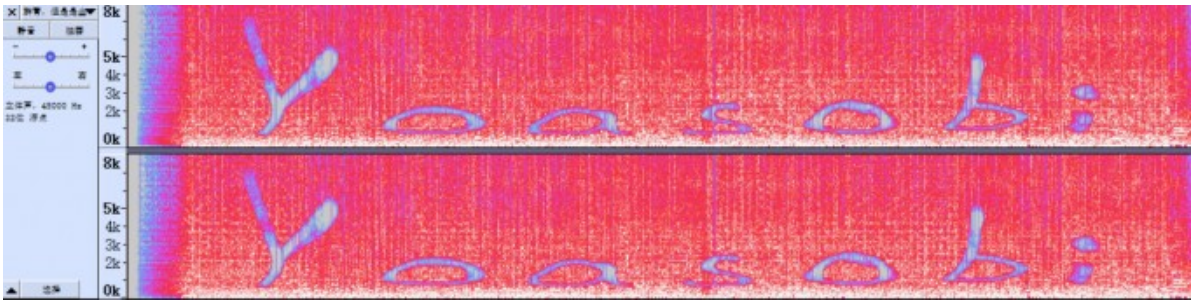
3.群青(其实是幽灵东京)

群青好耶!

为了这歌，也得做，点开一听，幽灵东京，QWQ

先保存吧，再次学习音频隐写

使用Audacity，波谱，频谱看一看



有了Yoasobi这些字，不知道有什么用处先记着，

再打开101再康康

why not try try Slienteye。说了我就下一个呗

打开slienteye,decode，没有隐藏信息.....

心情是蔚蓝色，天空是千纸鹤。后来突然想到这Yoasobi还没用过，使用密码Yoasibi

解开了，给了个网址，www,还有（对了，密码记得输两遍）

打开嘛，还能有什么办法，得到SSTV一个文件，一听挺离谱的，不是我这个活人可以欣赏的。网上所以搜SSTV————慢扫描电视

电脑上下载了MMSSTV试试太糊了，还是手机上robot36靠谱

扫描二维码，落幕，week1结束，呜呜呜勉强留在第一页，下周继续努力吧QWQ