Writeup-2020安洵杯-Misc题：开始抑郁

原创

Y5neKO 于 2020-09-08 01:14:48 发布 90 收藏 1
文章标签： python 信息安全 软件测试 ffmpeg bug

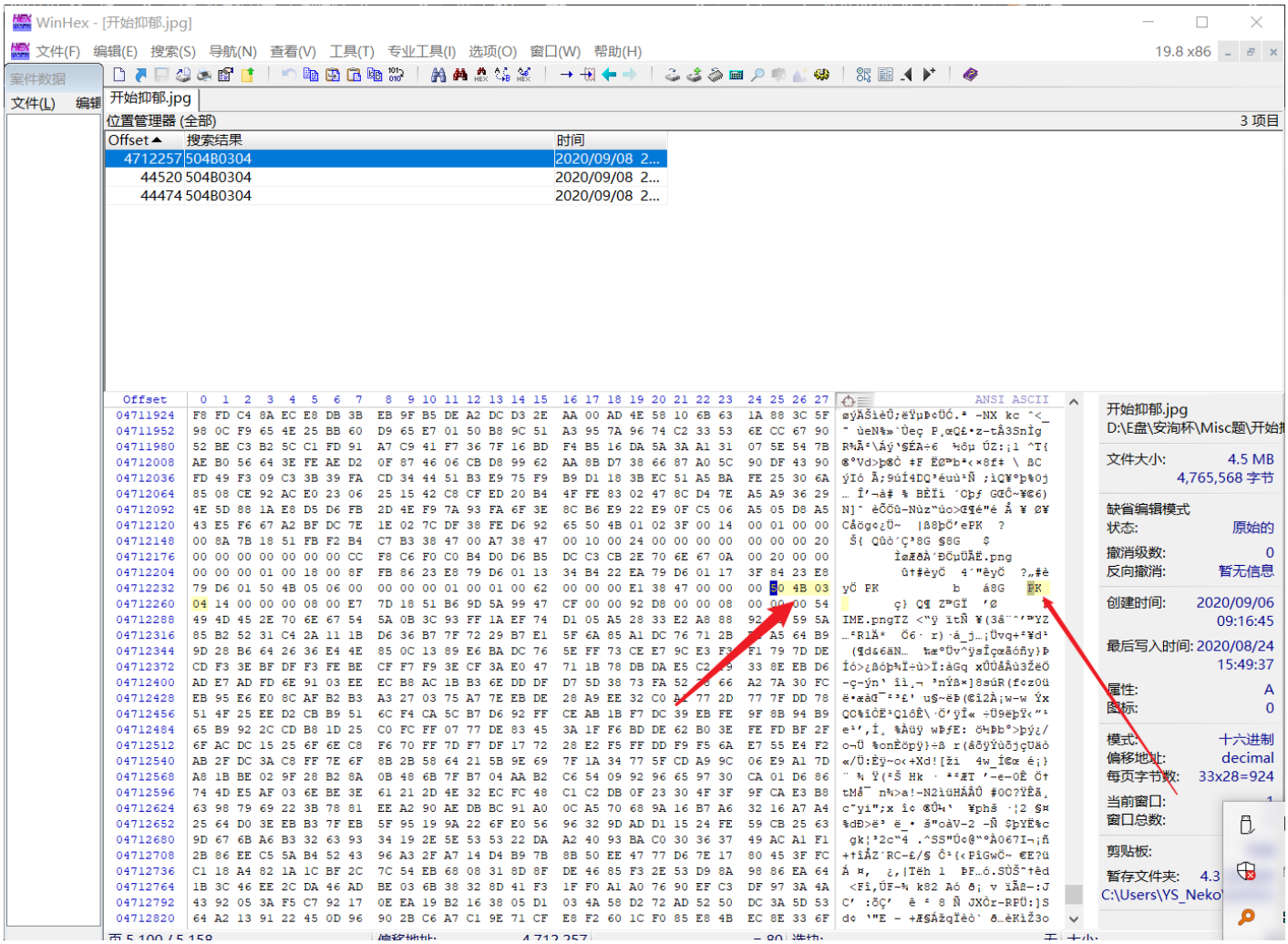
不说了，到点了，我tm直接开始抑郁！

题目描述：开始抑郁

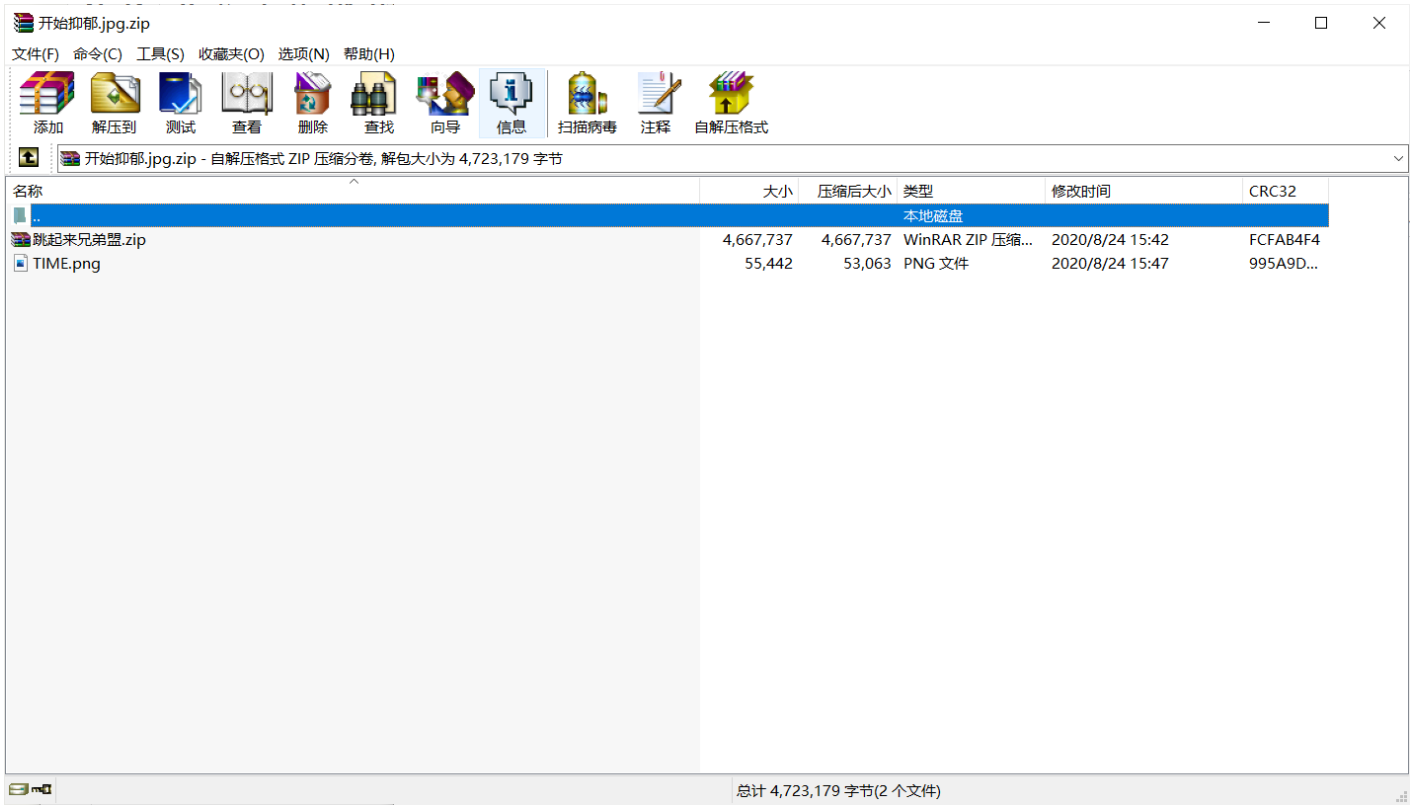
附件下载

打开压缩包发现一张图片，解压出来，直接查看没有发现异常

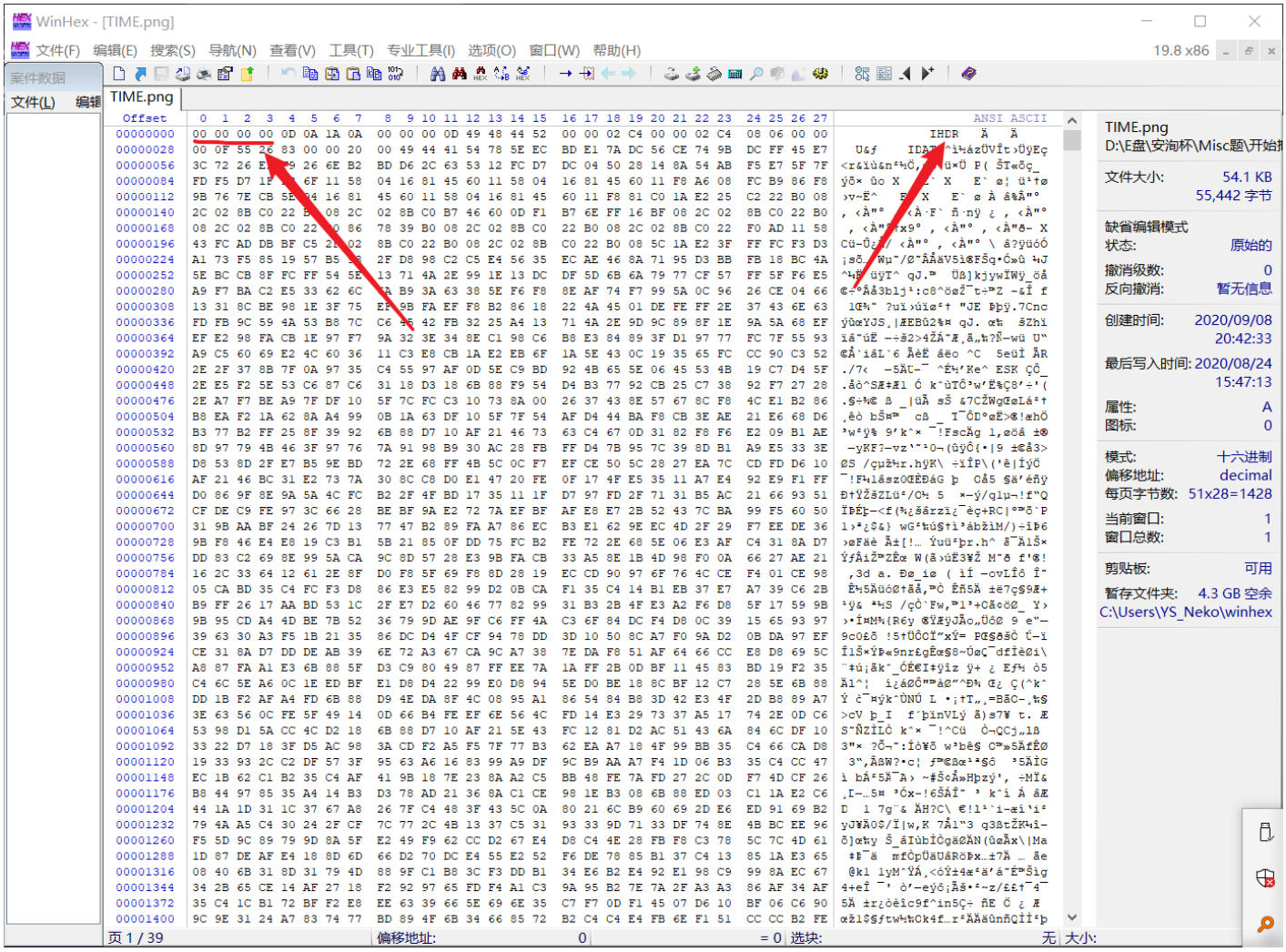
观察图片大小发现过大，4.5M，推测为混合了其他文件



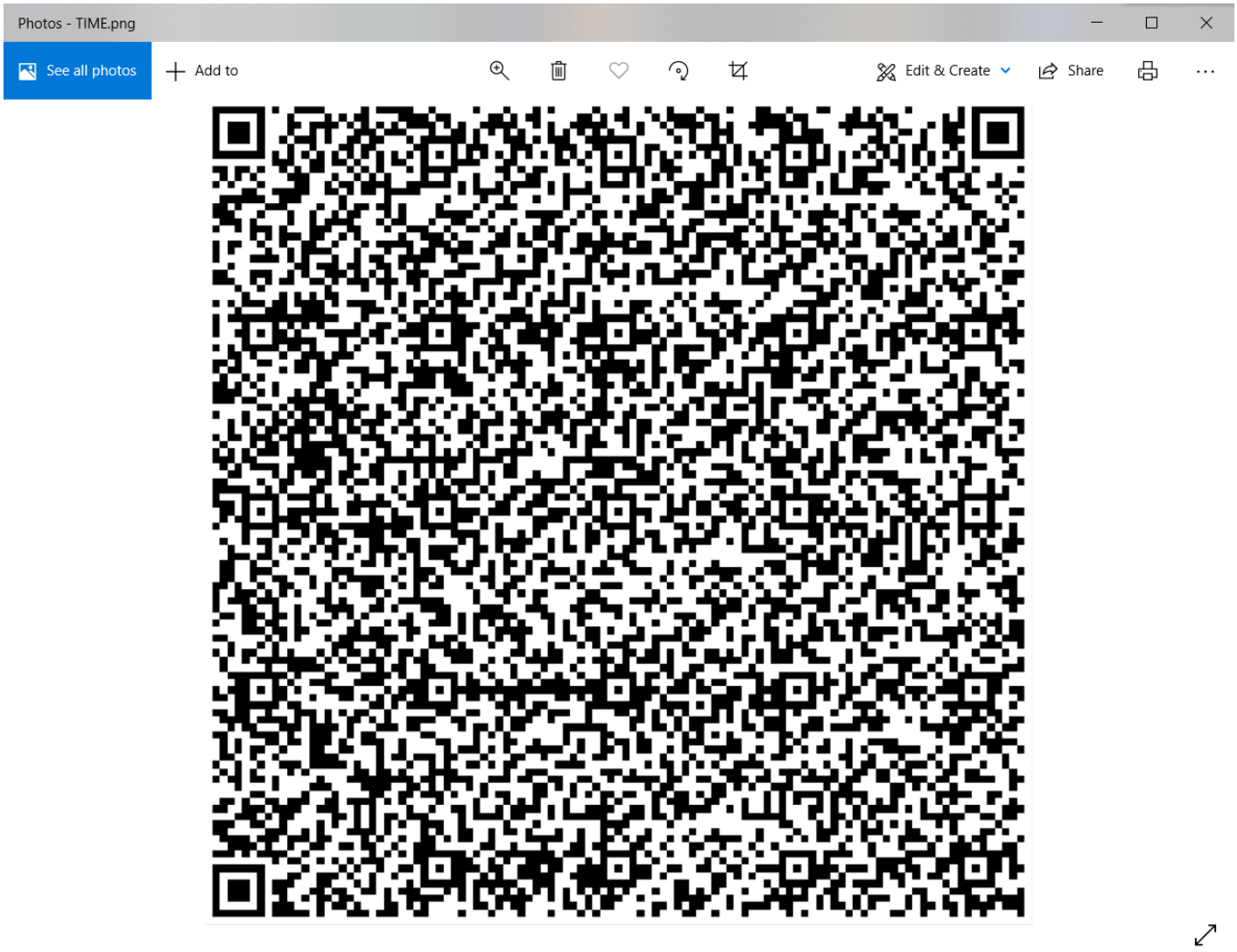
发现zip文件头，直接将格式改为zip解压得到两个文件



首先打开压缩包，发现是加密的，打开图片TIME.png，发现无法正常打开，推测需要修复，Winhex打开



发现IHDR数据块和空缺的文件头，修复文件头保存后成功打开*PS：IHDR为png特有的数据块*



二维码解码得到

```
++++++++[>>++>++++>++++++>++++++++>++++++++++>++++++++++++>++++++++++++++>++++++++++++++++>++++++++++++++++
```

这是一种叫Brainfuck的编码，解码得到

```
[!+[]+!+[]]+[+[]]+[!+[]+!+[]]+[+[]]+[+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+[!+[]+!+[]]+[!+[]+!+[]+
```

明显Jsfuck，继续解码

```
[!+[]+!+[]]+[+[]]+[!+[]+!+[]]+[+[]]+[+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+
[]+!+[]]+[!+[]+!+[]]+[!+[]+!+[]+!+[]+!+[]]+[+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+
[!+[]+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+[+[]]+[+[]]
"20200824152800"
```

结果类似是时间，应该是压缩包密码，但是密码错误
我们将这个时间拿去转时间戳得到：

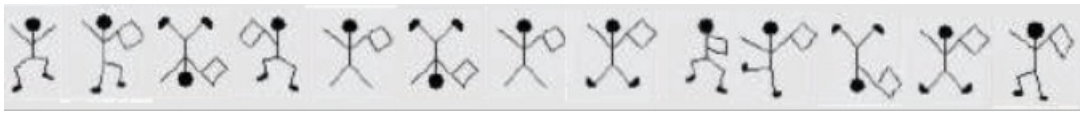
```
1598254080
```

现在： 1599576976 控制： 停止

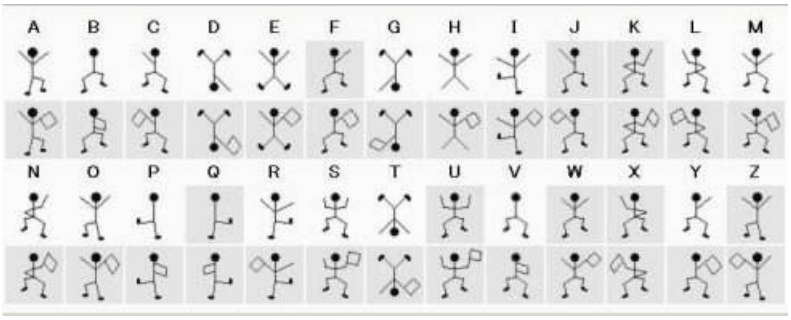
时间戳 1599576768 秒(s) 转换 » 北京时间

时间 202008241528 北京时间 转换 » 1598254080 秒(s)

利用时间戳成功解压压缩包得到一张图片

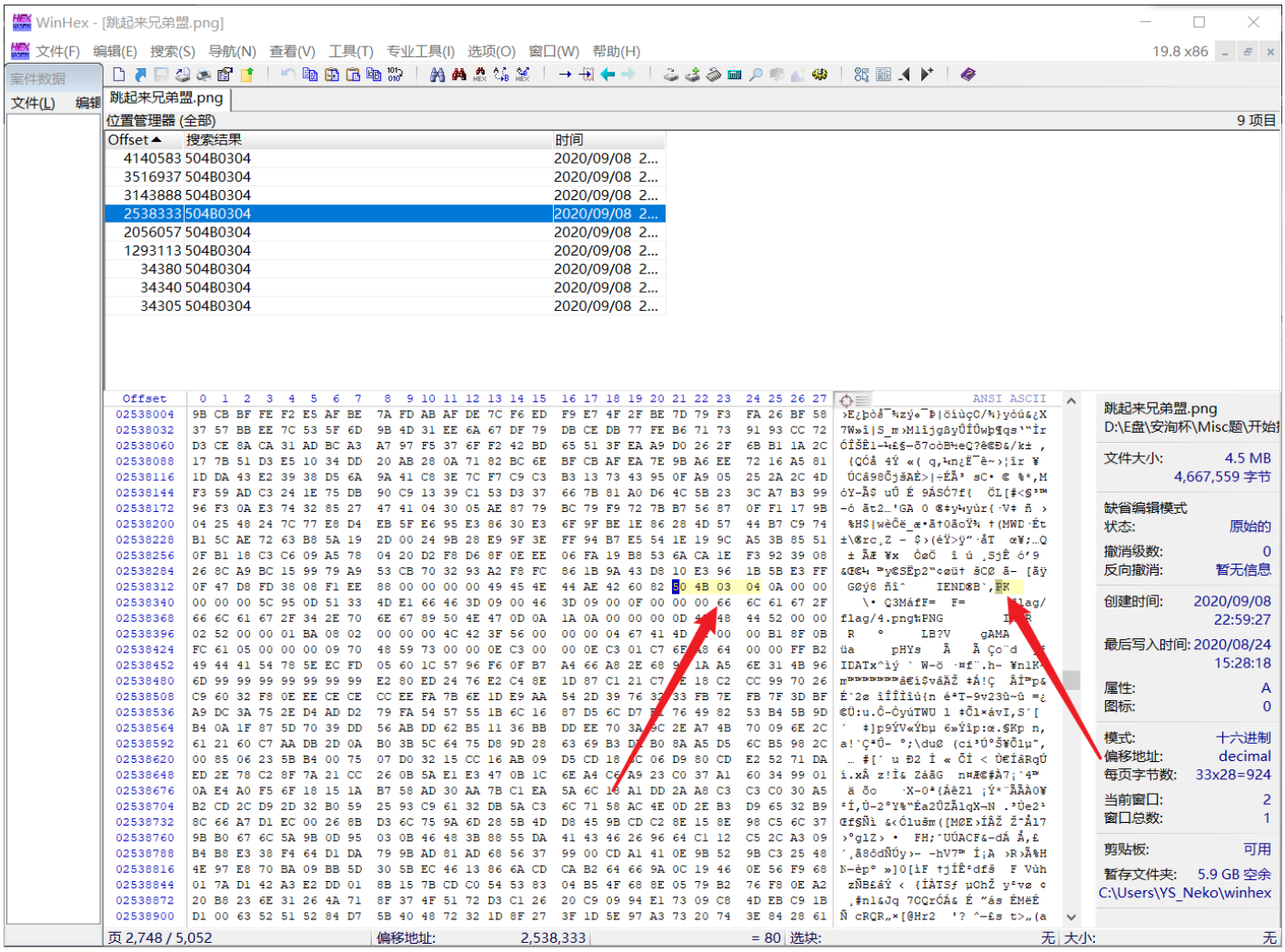


经查找这是出自福尔摩斯探案集中的跳舞的人密码，密码对应为

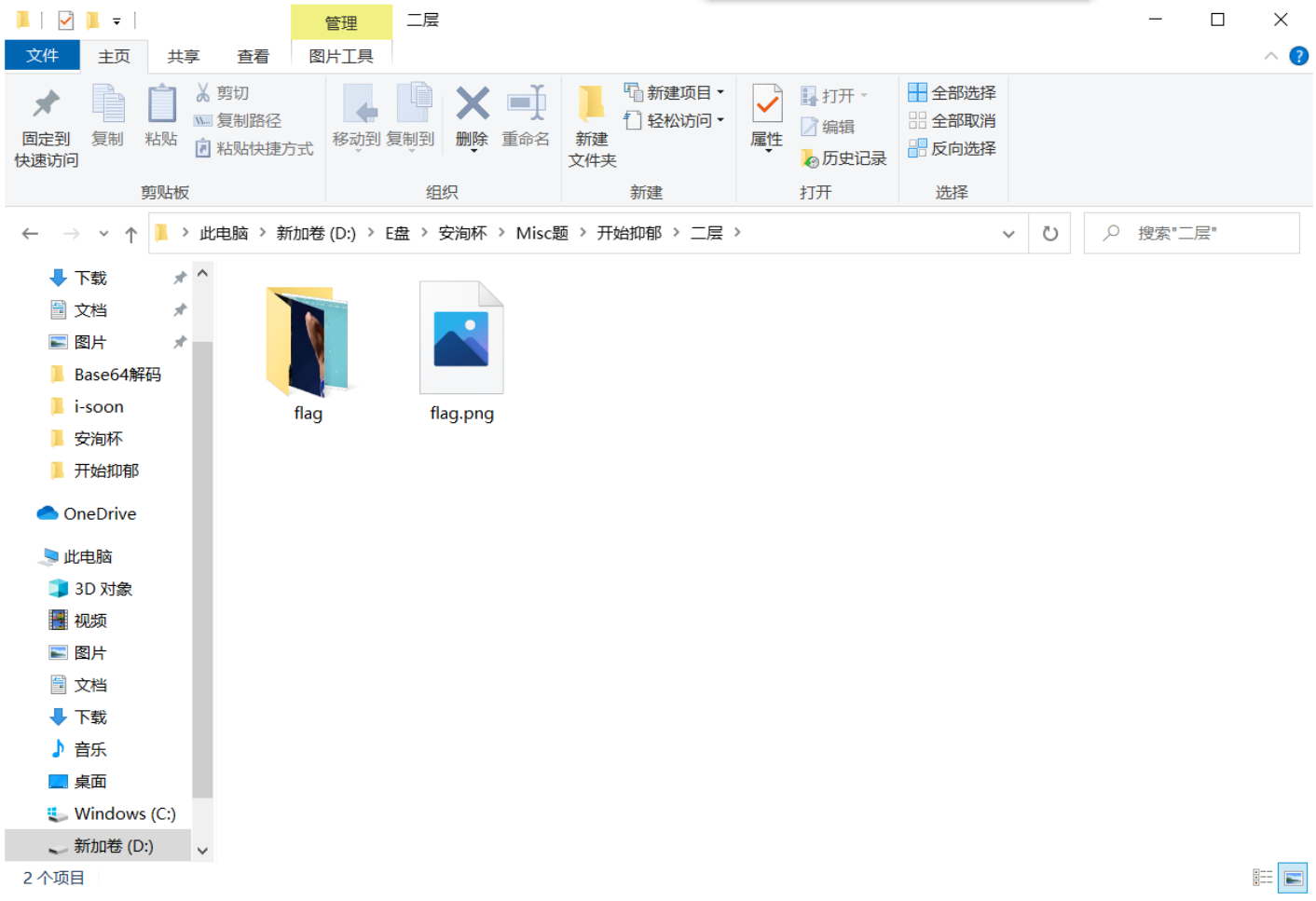


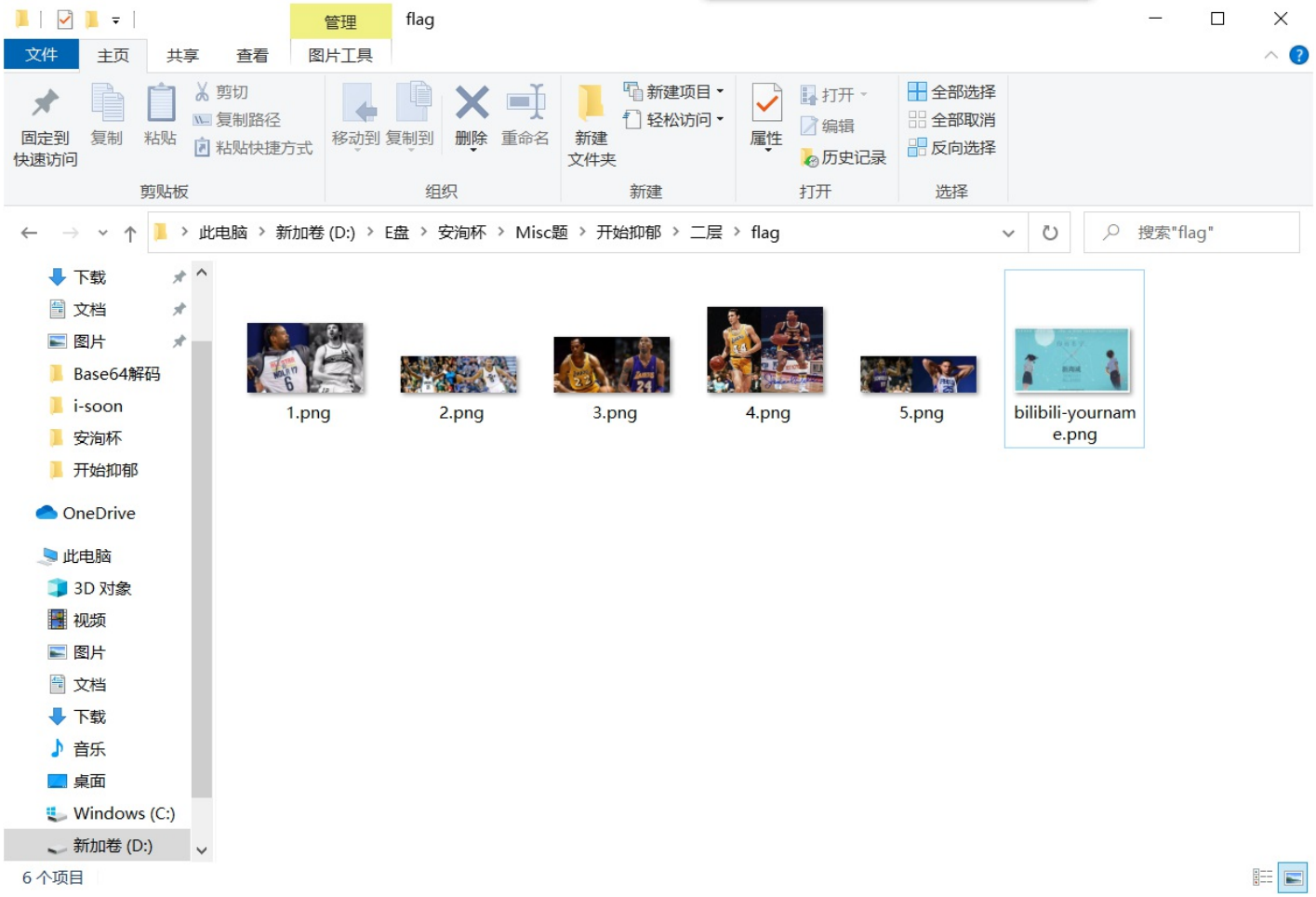
解密为：WATCHTHEVIDEO(观看这个视频)

然后查看图片信息发现图片大小明显过大，4.45M，放进Winhex打开再次发现zip文件头



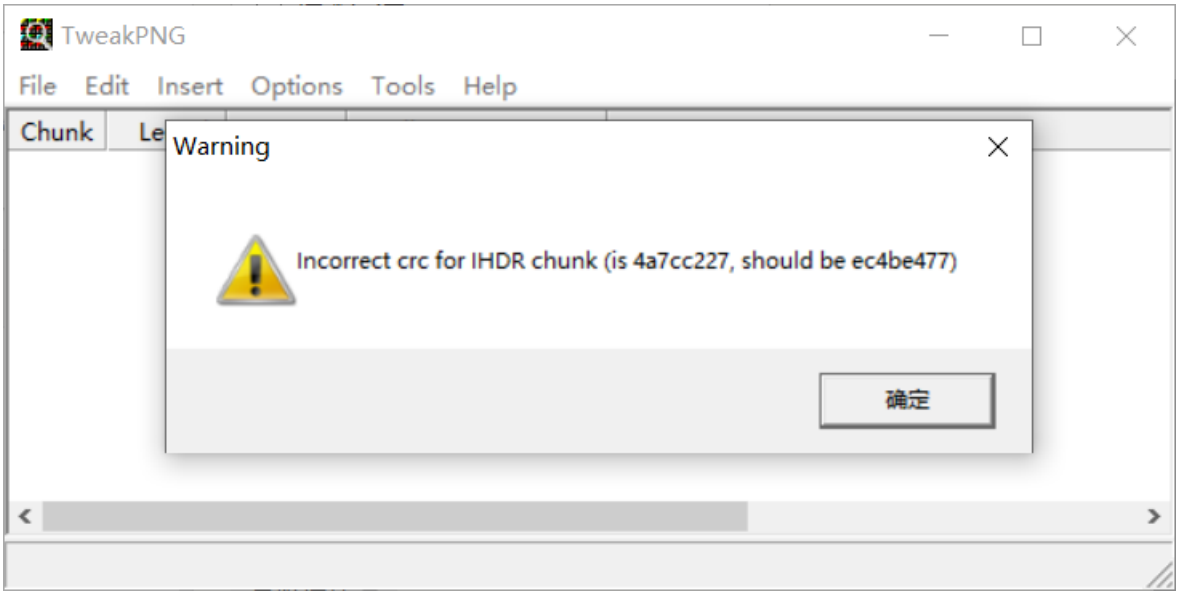
修改后缀为zip后打开得到几张图片



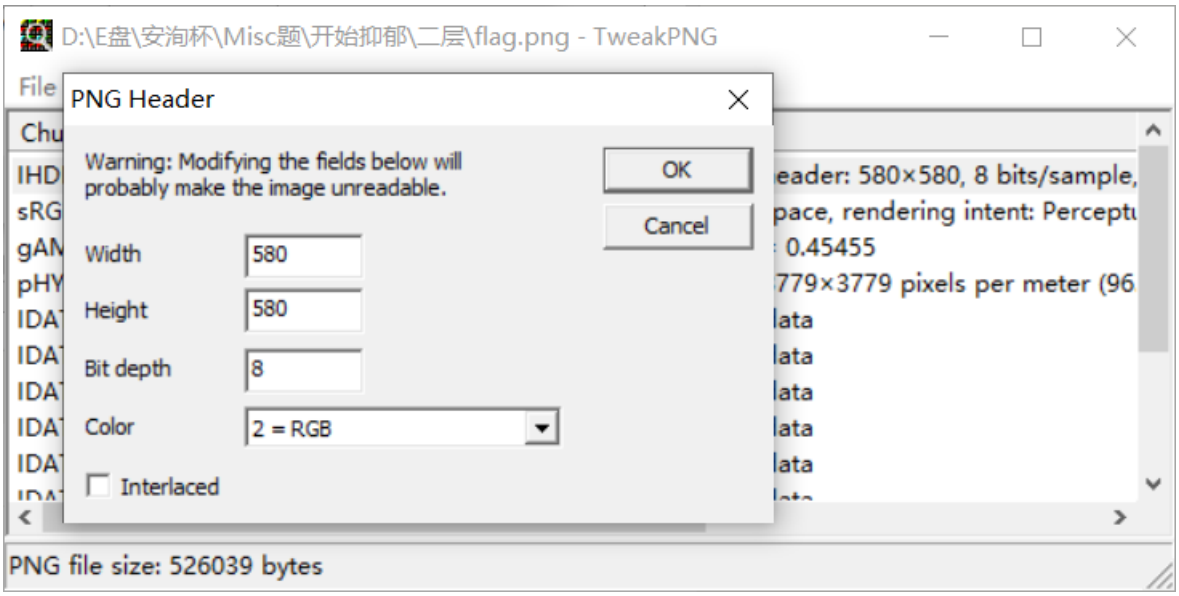


其中flag.png无法打开，Winhex打开发现又是缺少文件头，补充后打开得到一个表情包

观察图片发现少了一截，用TweakPNG校验发现数据块异常



双击IHDR块修改图片宽高得到flag格式

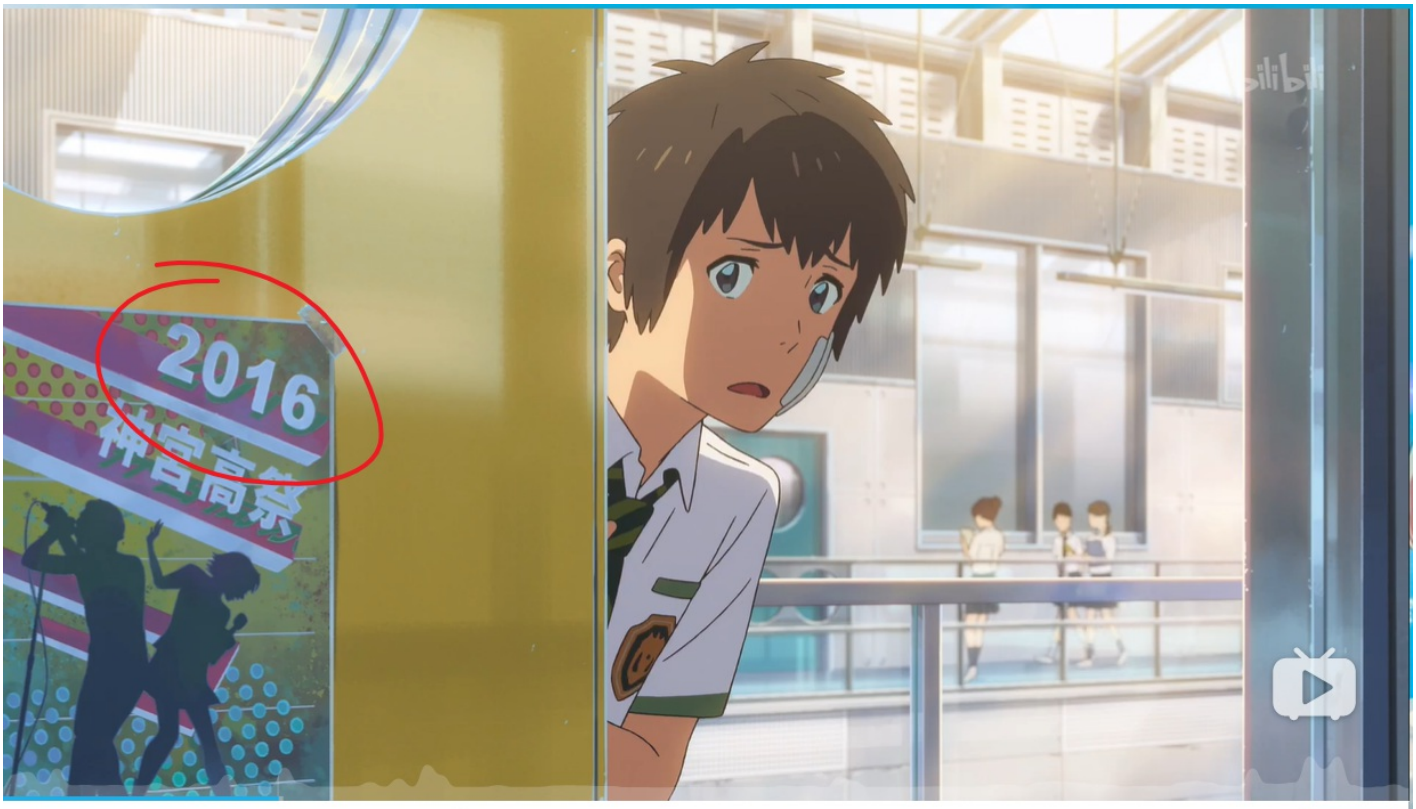



```
flag格式：{1234-1234-ABCDEFGHI-ABCDEFGHIJK-1234}
```

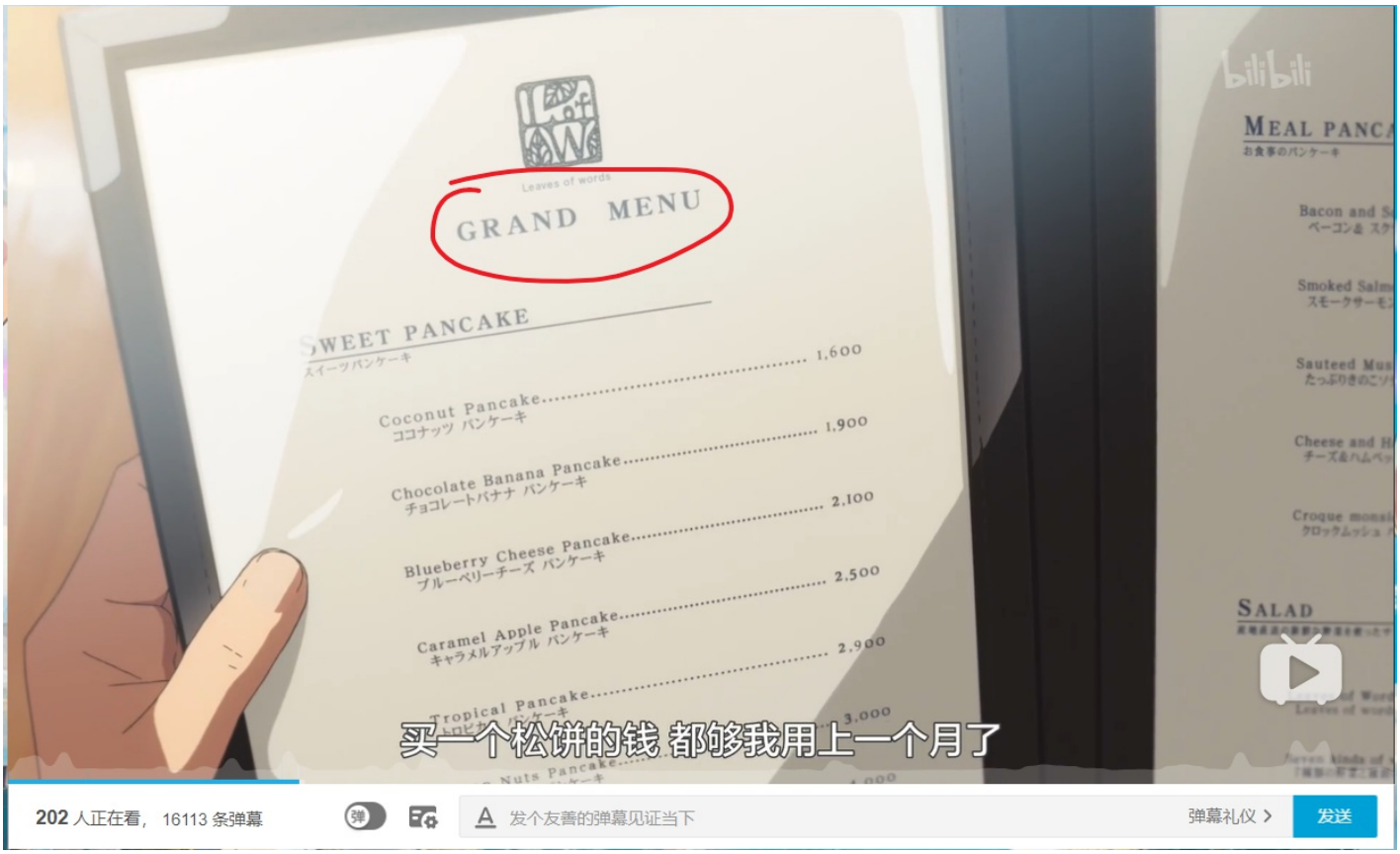
得到格式后通过flag文件夹里的几张图片分别获取每段flag
flag文件夹里有六张图片，前五张图片球星的编号分别对应Bilibili中电影《你的名字》的五个时间片段，分别为

> 6分12秒/21分05秒/22分24秒/44分52秒/93分25秒

193 人正在看， 16110 条弹幕 弹 发个友善的弹幕见证当下 弹幕礼仪 > 发送



193 人正在看， 16113 条弹幕 弹 发个友善的弹幕见证当下 弹幕礼仪 > 发送


GRAND MENU
SWEET PANCAKE
Coconut Pancake 1,600
Chocolate Banana Pancake 1,900
Blueberry Cheese Pancake 2,100
Caramel Apple Pancake 2,500
Tropical Pancake 2,900
SALAD
bilibili
买一个松饼的钱 都够我用上一个月了
202 人正在看， 16113 条弹幕
发个友善的弹幕见证当下
弹幕礼仪 >
发送


bilibili
202 人正在看， 16113 条弹幕
发个友善的弹幕见证当下
弹幕礼仪 >
发送

将五个线索填入flag格式并大写，得到最终flag：

```
flag{1200-2016-GRANDMENU-RCHITECTURE-1335}
```