# CTF-Crypto 与 Misc 方向的学习（一）

## 前言

接触信息安全专业后便从学长的介绍中知道了CTF比赛的相关事宜，并且对其产生了兴趣，参加了NewStarCTF2024的公开赛，对其有了一定程度的进一步了解。在11月的课余闲暇时间进行学习后，我将自己自学的一些收获与感悟总结在此文档中。

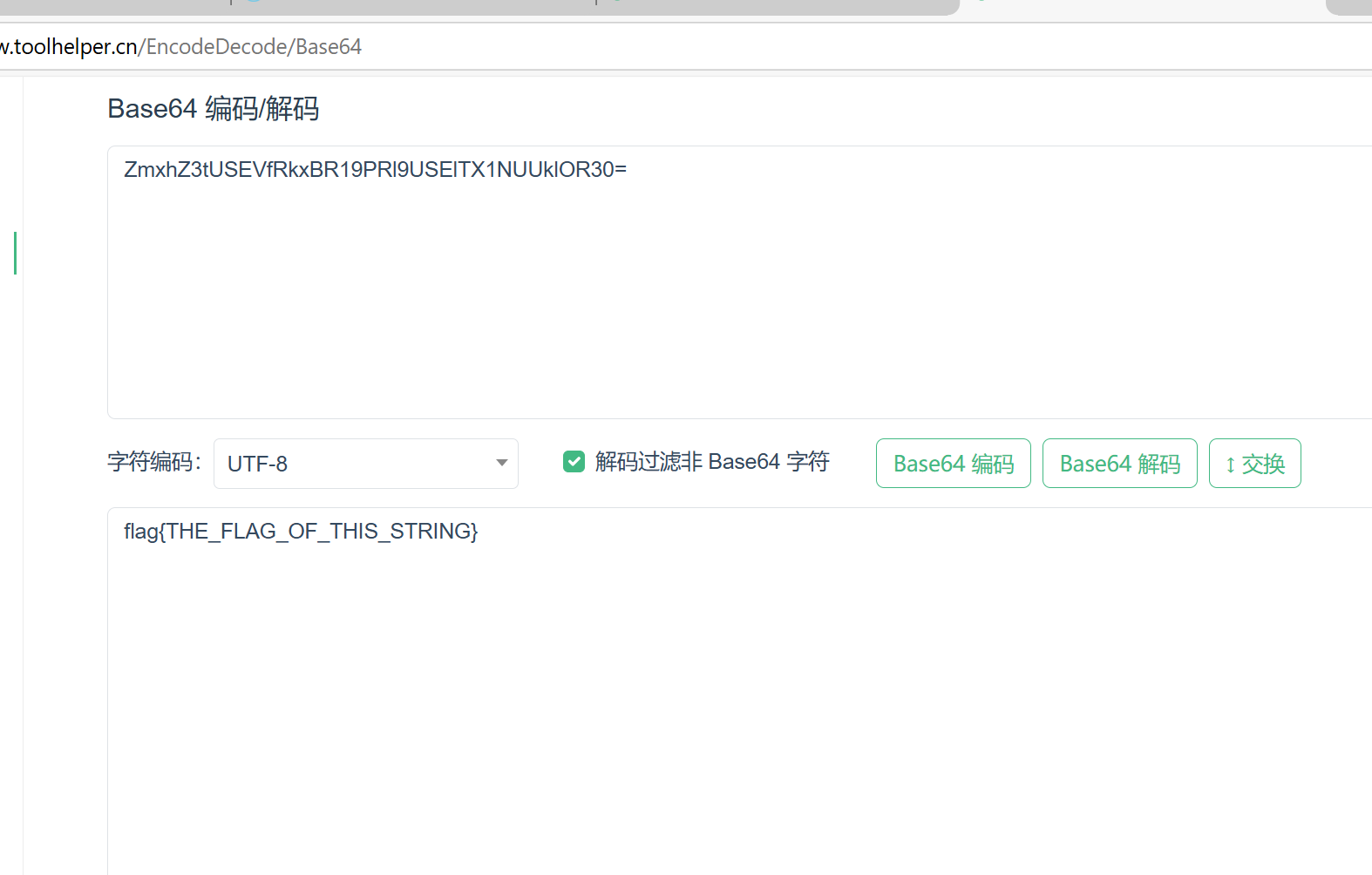
主要刷题网站：buuctf：[BUUCTF在线评测](https://buuoj.cn/)

主要使用工具：[锤子在线工具网 - 首页](https://www.toolhelper.cn/)、[md5在线解密破解,md5解密加密](https://www.cmd5.com/default.aspx)

Visual studio code、RSAtool、010editor、wireshark、Stegslove、ARCHPR、QR\_research、搜索引擎等。

## Crypto

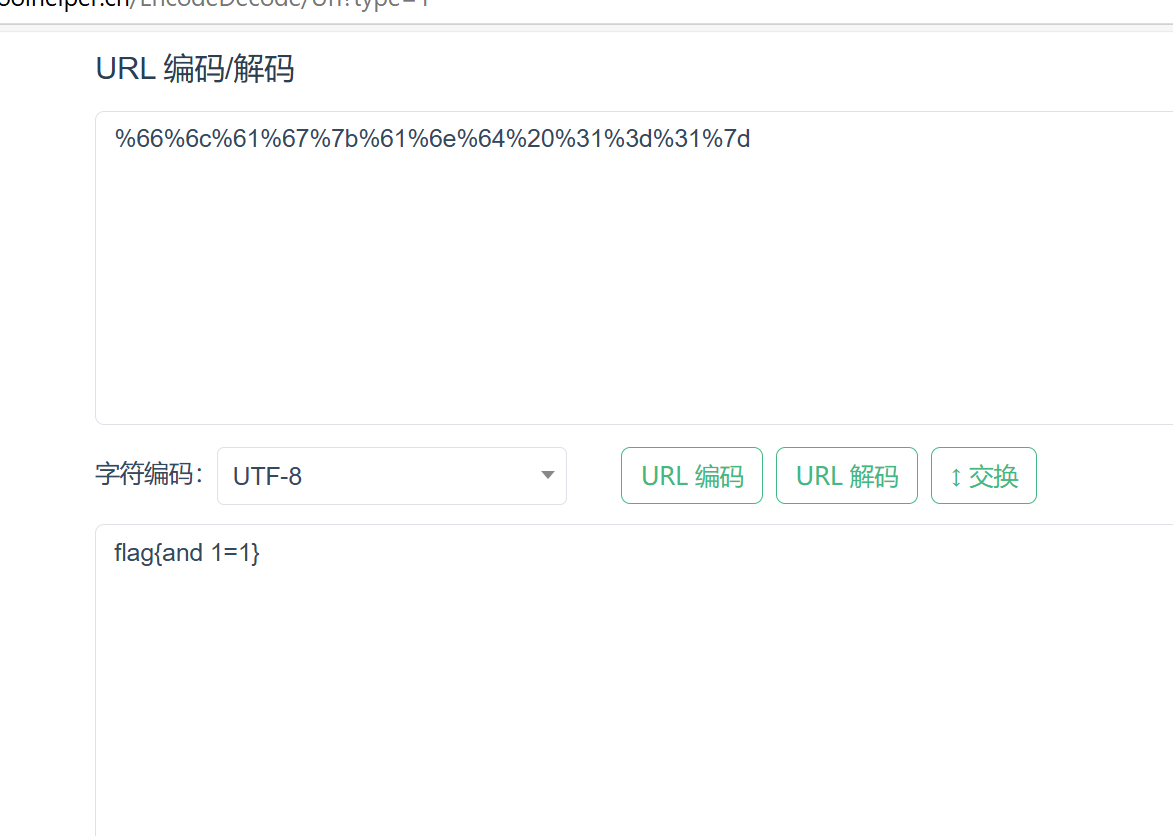
1. 一眼就解密

不难发现符合Base64的格式，将其用在线工具进行解密后得到flag。

1. MD5

由题意可知为MD5加密，使用MD5在线解密工具解密得到flag。

1. Url编码

使用URL解码对其解码得到flag。

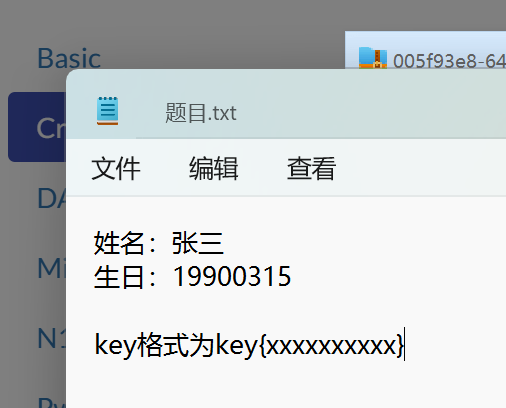
1. 看我回旋踢

猜测为凯撒密码，经过前面flag的明文与密文对应可以推断出偏移值为13，得到flag。

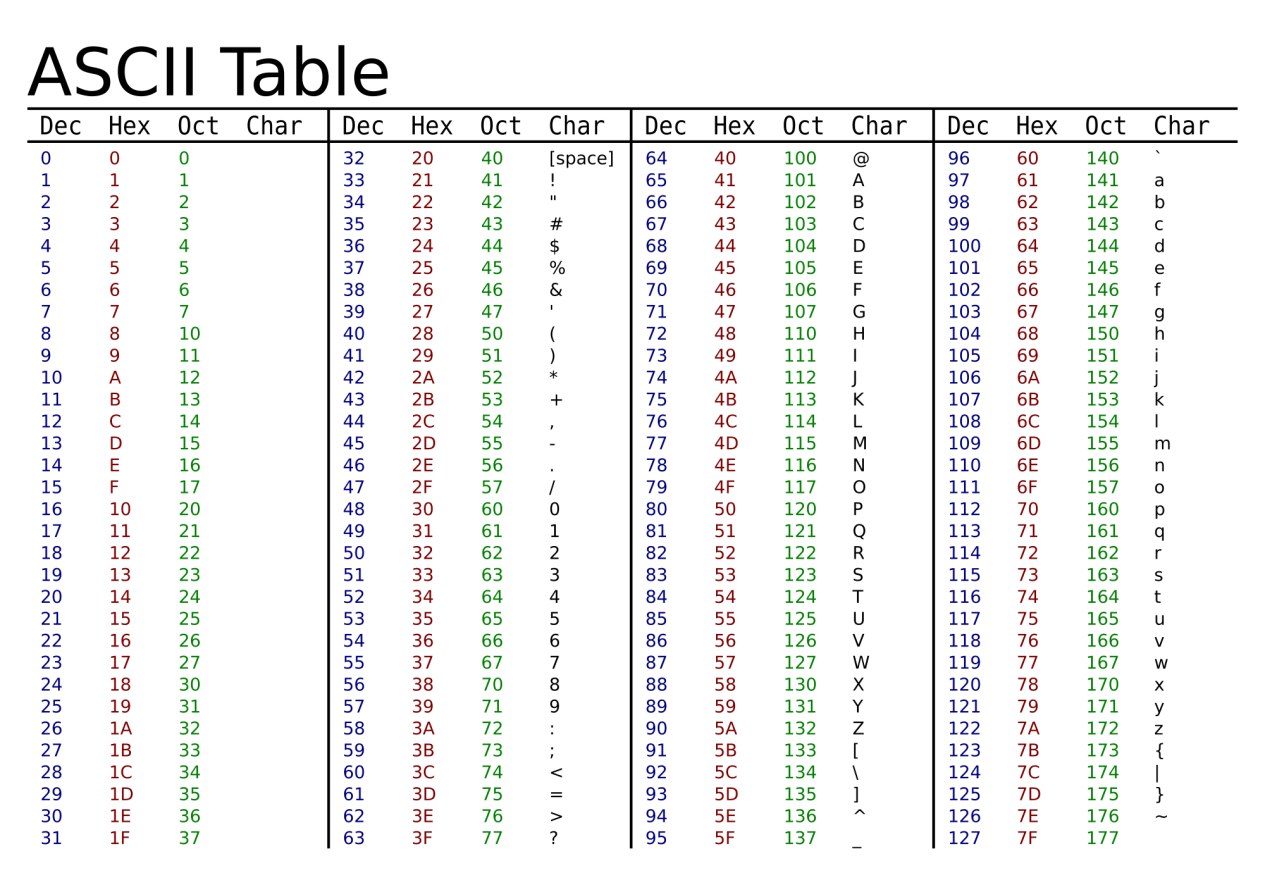
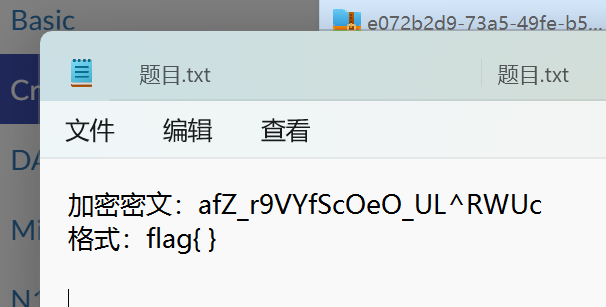
1. 摩丝

如题意，摩斯密码。

1. Password

十位数密码，猜测为zs19900315

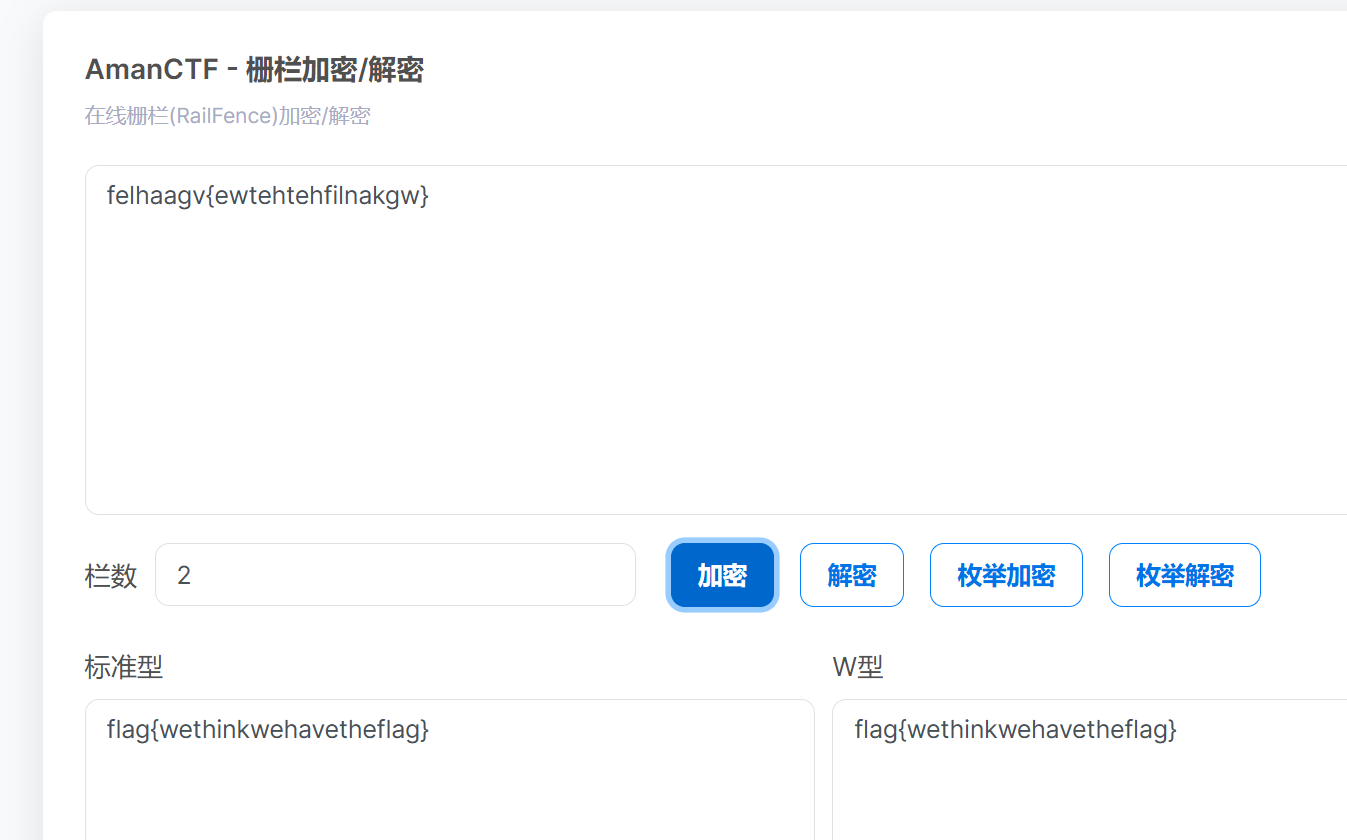
1. 变异凯撒

这题说是变异凯撒，联想到位移密码。对照ASCII表，得到位移依次为5、6、7、8，所以偏移值从5开始递增，写一个简单的程序，得到flag。

1. Quoted\_printable

使用Quoted printable在线解码工具，得到flag。

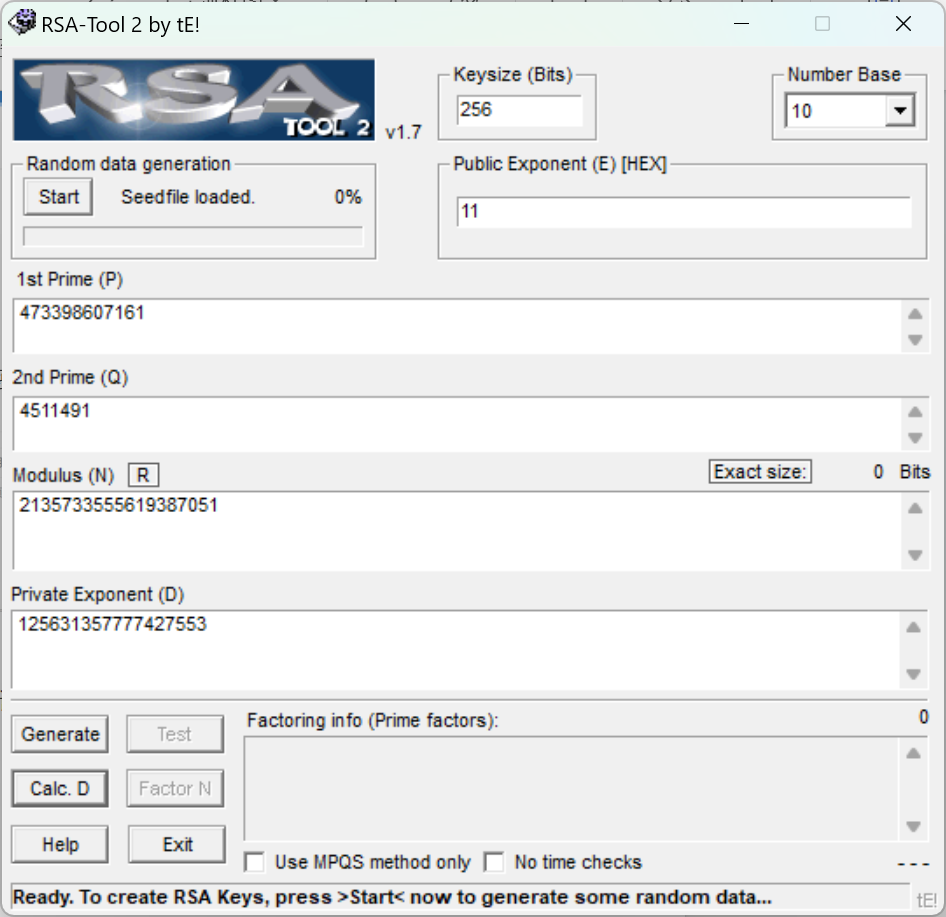
1. 篱笆墙的影子

根据“篱笆”想到栅栏，用栅栏密码在线工具进行解密，得到flag。

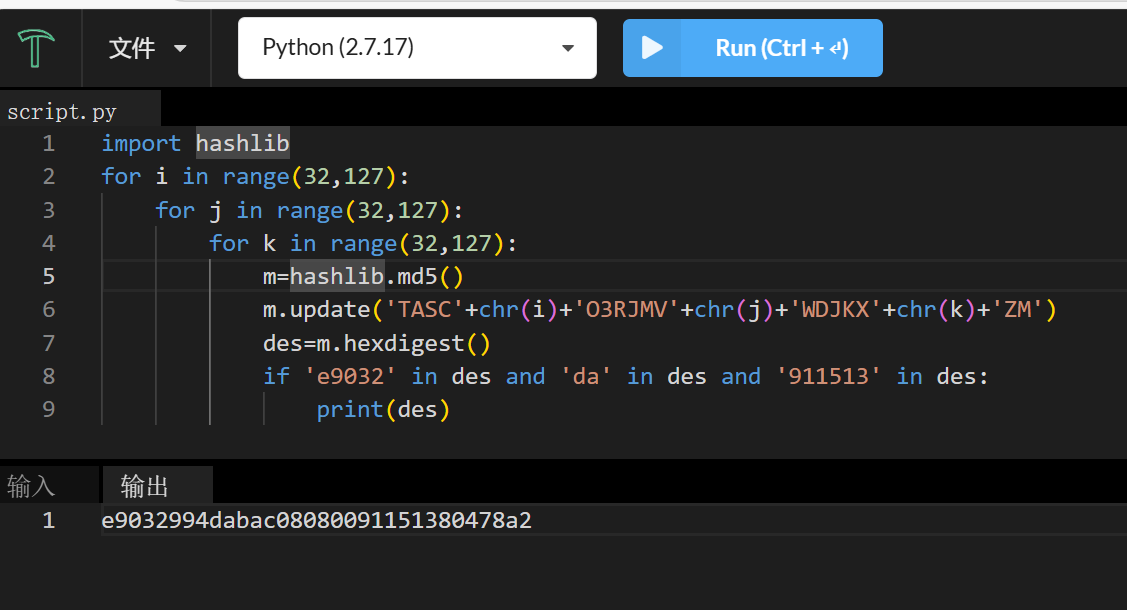
1. Rabbit

由题意为rabbit加密，用在线rabbit解密工具得到flag。

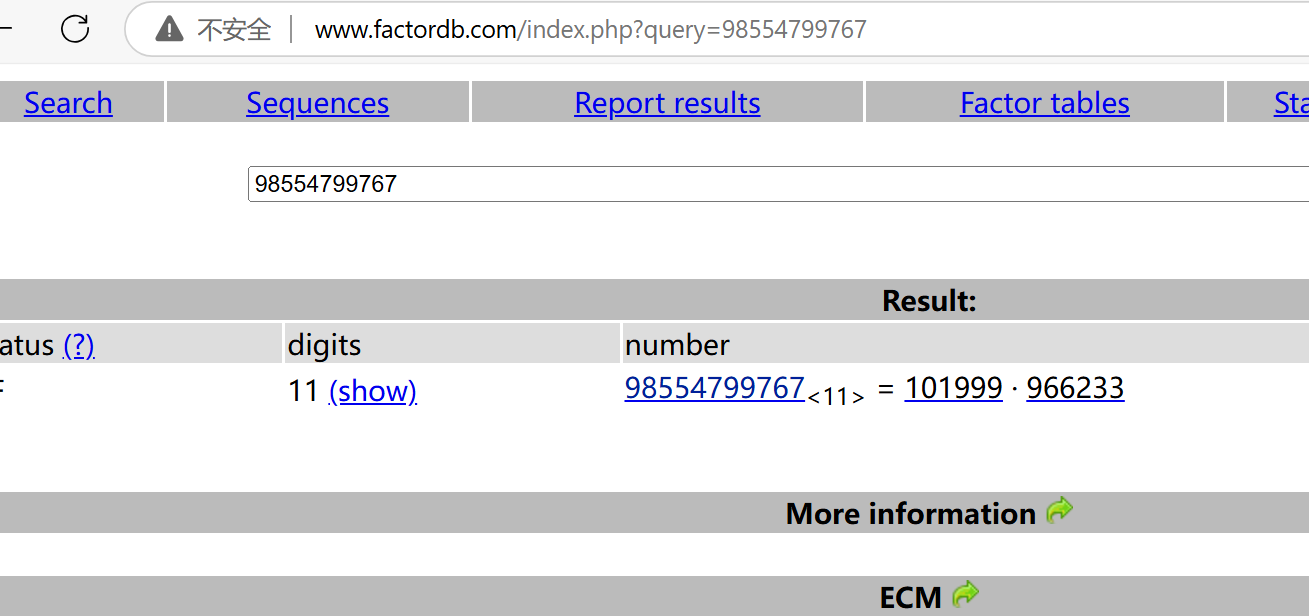
1. RSA

由题意，此题考察了RSA加密的相关知识。使用RSAtool进行求解，注意将数据格式改为10进制，密钥e转换为16进制。

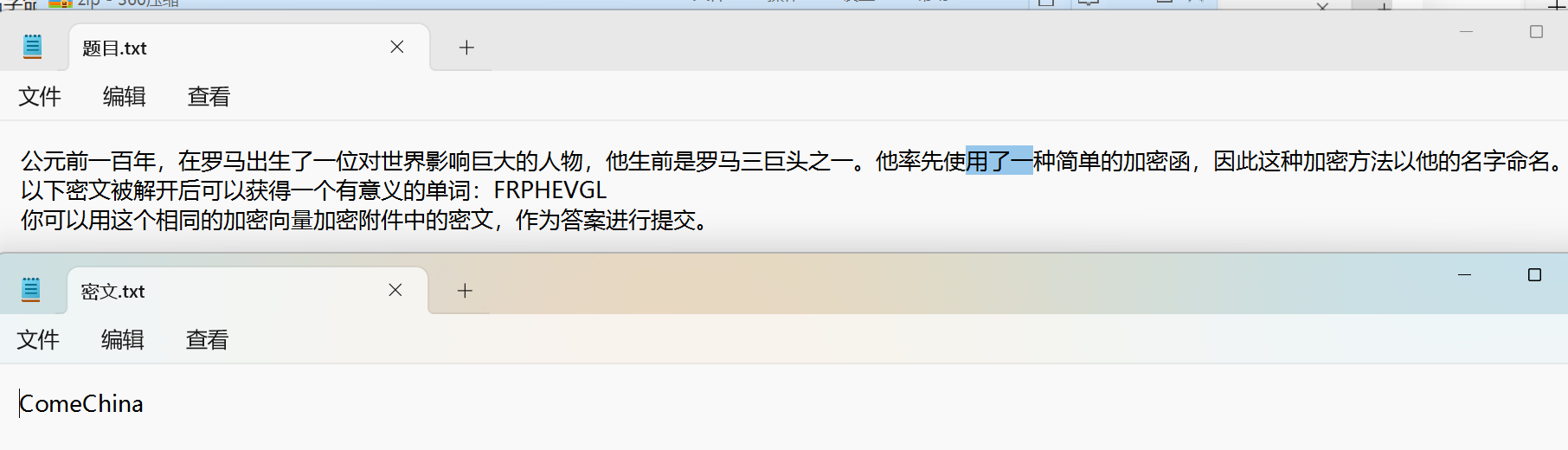
1. 丢失的MD5

下载附件，得到代码。运行后得到flag。（很奇怪3.x版本的python会报错，而使用2.x版本的就能得到结果）

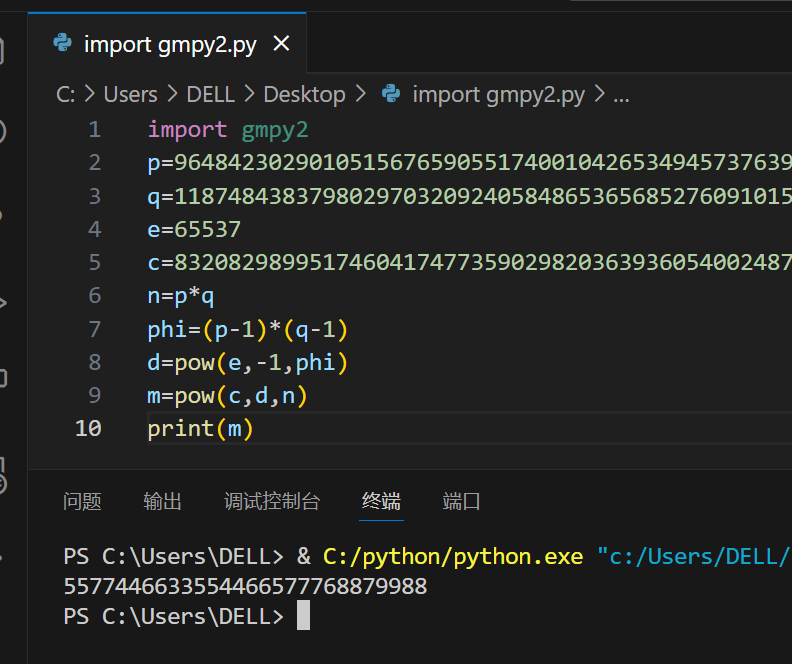
1. Alice和Bob

如题意，将大整数用工具分解，再将其进行MD5的32位小写哈希，得到flag。

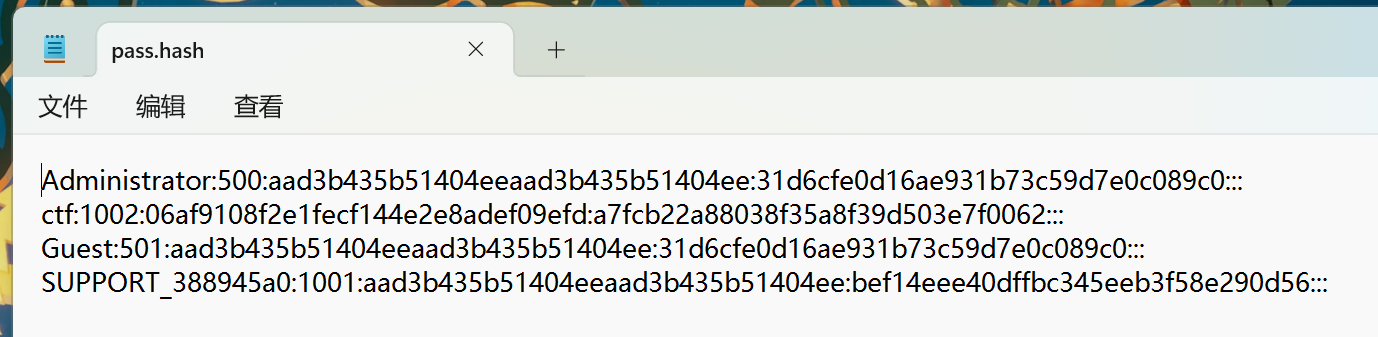
1. 大帝的密码武器

下载后用010editor修改文件格式后打开。由题意，对其不断使用凯撒密码，当偏移值为13时为有意义。将密文进行13位的偏移，得到flag。

1. Rsarsa

本体考察RSA算法，编写一个简单的代码即可。

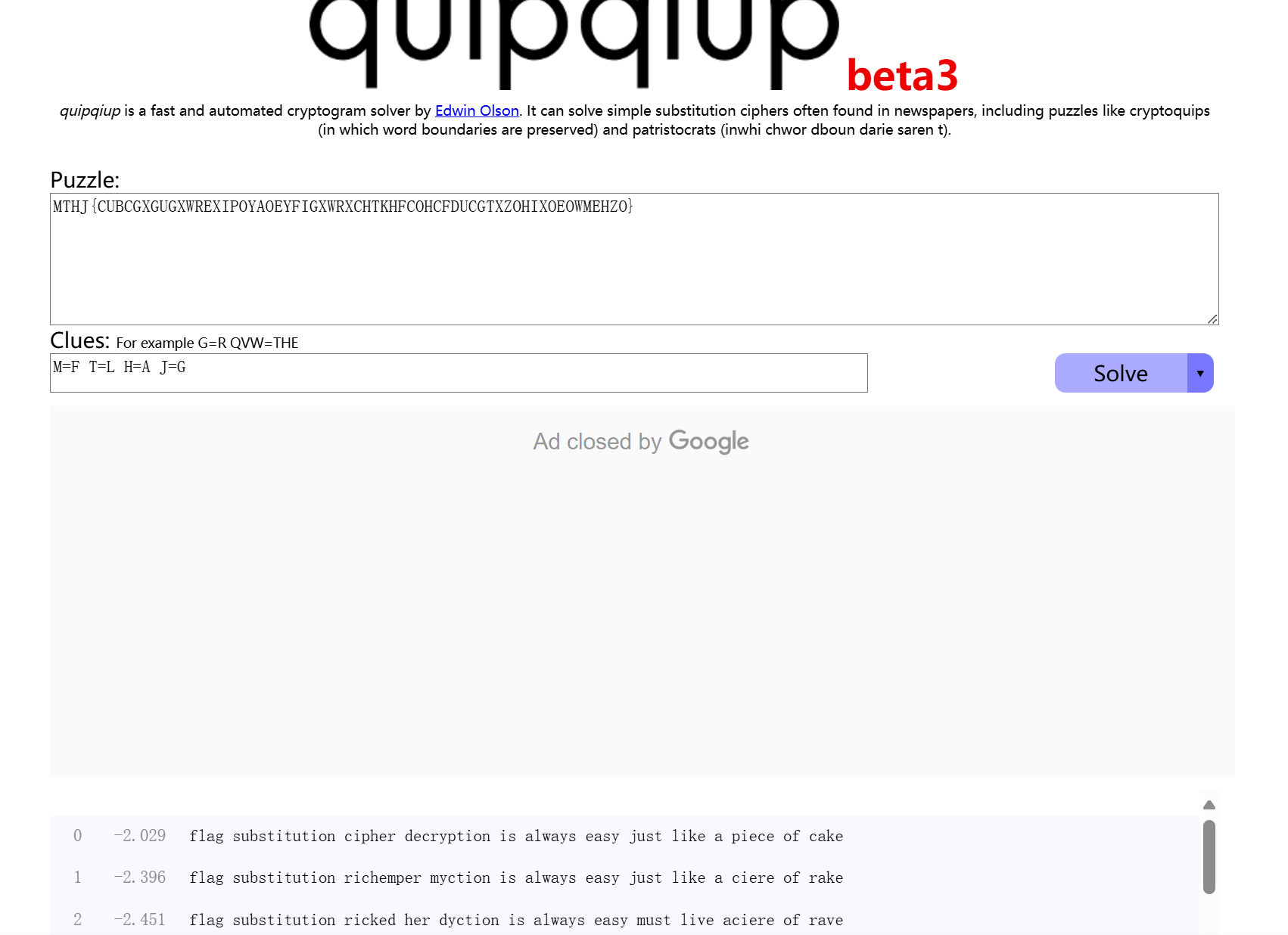
1. Windows系统密码

Windows储存的密码Hash值。1、3、4为相同的，故猜测为第二个的密码，解密后得到flag。

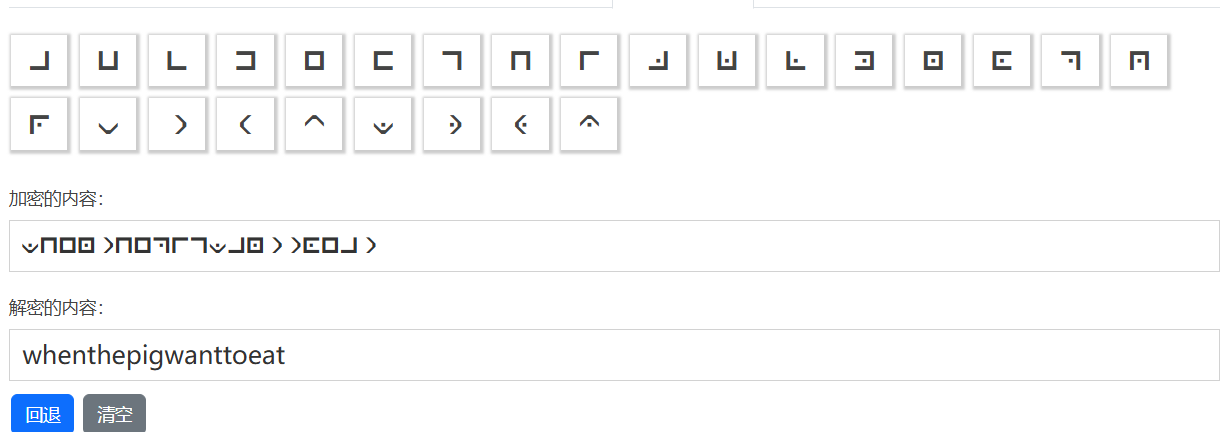
1. 信息化时代步伐

由题意，推测为中文电码，使用在线工具进行解密，发现确实是一句话（出自邓小平）且符合题目，故为flag。

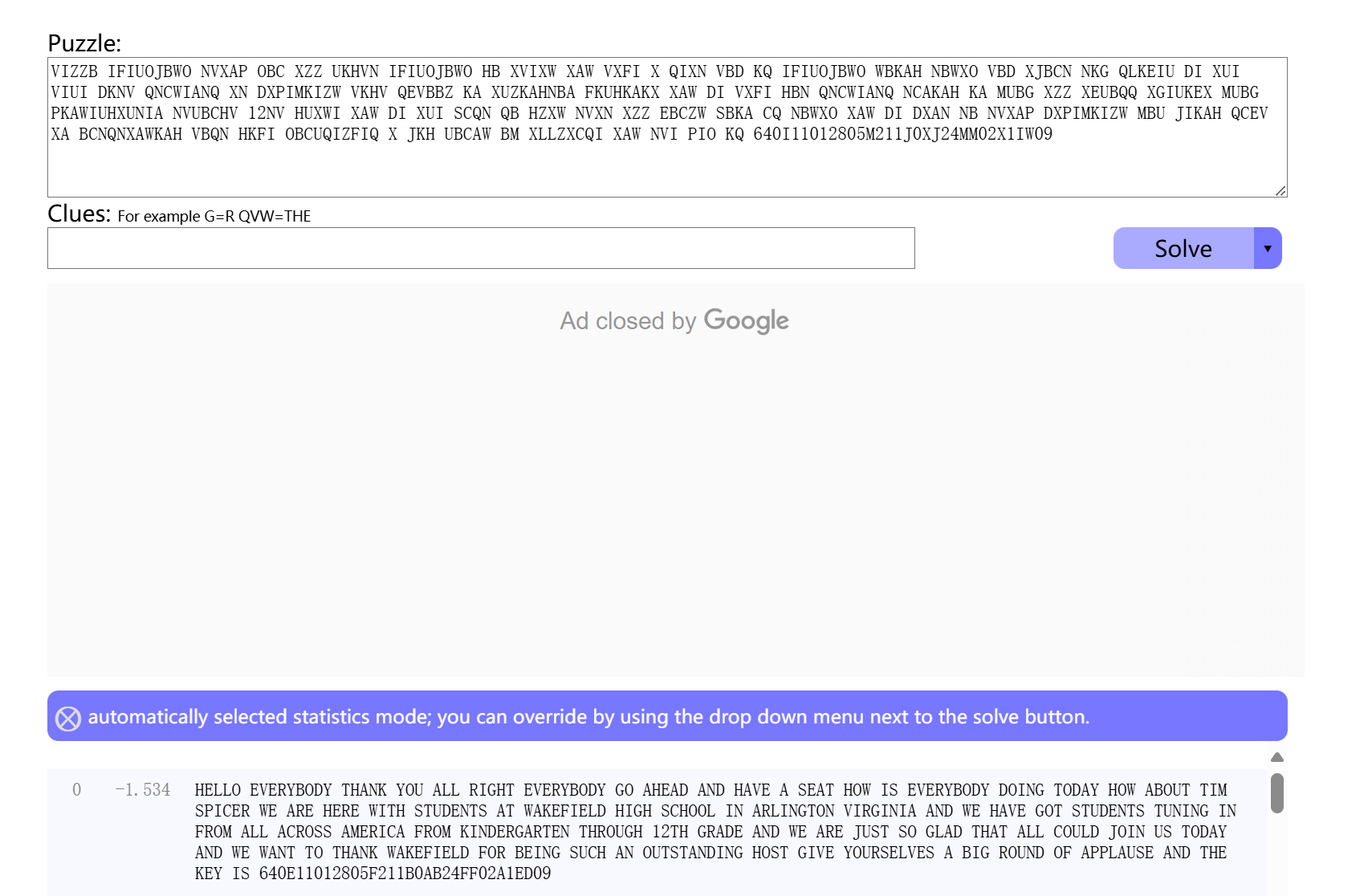
1. 凯撒？替换？呵呵

替换类密码，使用网站[quipqiup - cryptoquip and cryptogram solver](https://quipqiup.com/)解密，找出符合逻辑的一句（一般是第一句），记得将大写改为小写并删去空格。

1. 萌萌哒的八戒

猪圈密码。

1. 世上无难事

替换密码。还是使用[quipqiup - cryptoquip and cryptogram solver](https://quipqiup.com/)解密。

## Misc

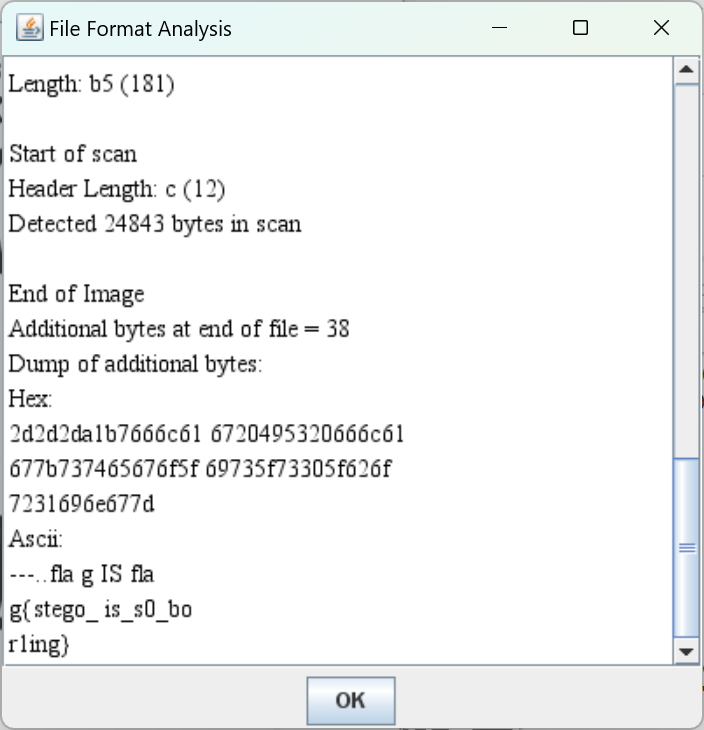
1. SIGNIN

签到题。

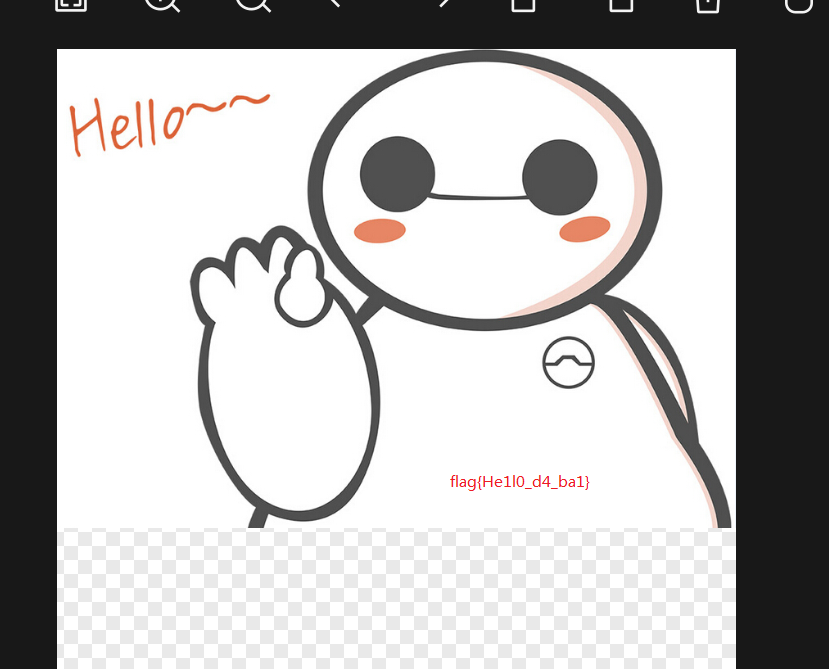
1. 金三胖

用Stegslove读取帧。（用将军的GIF好难绷）

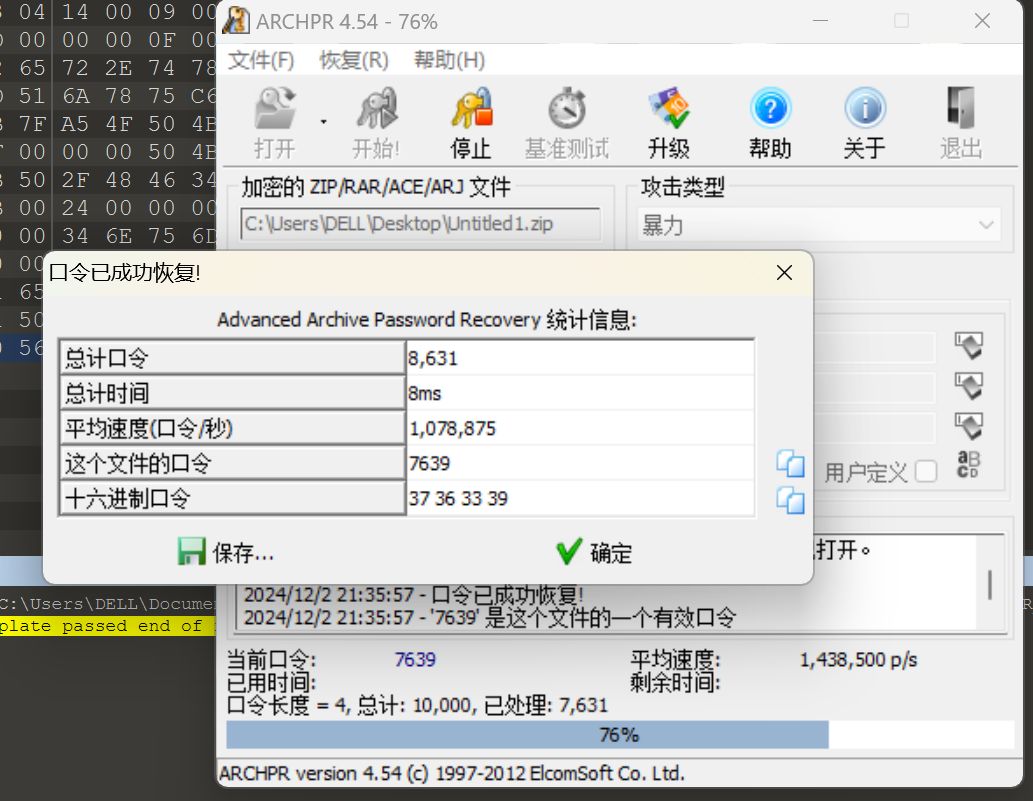
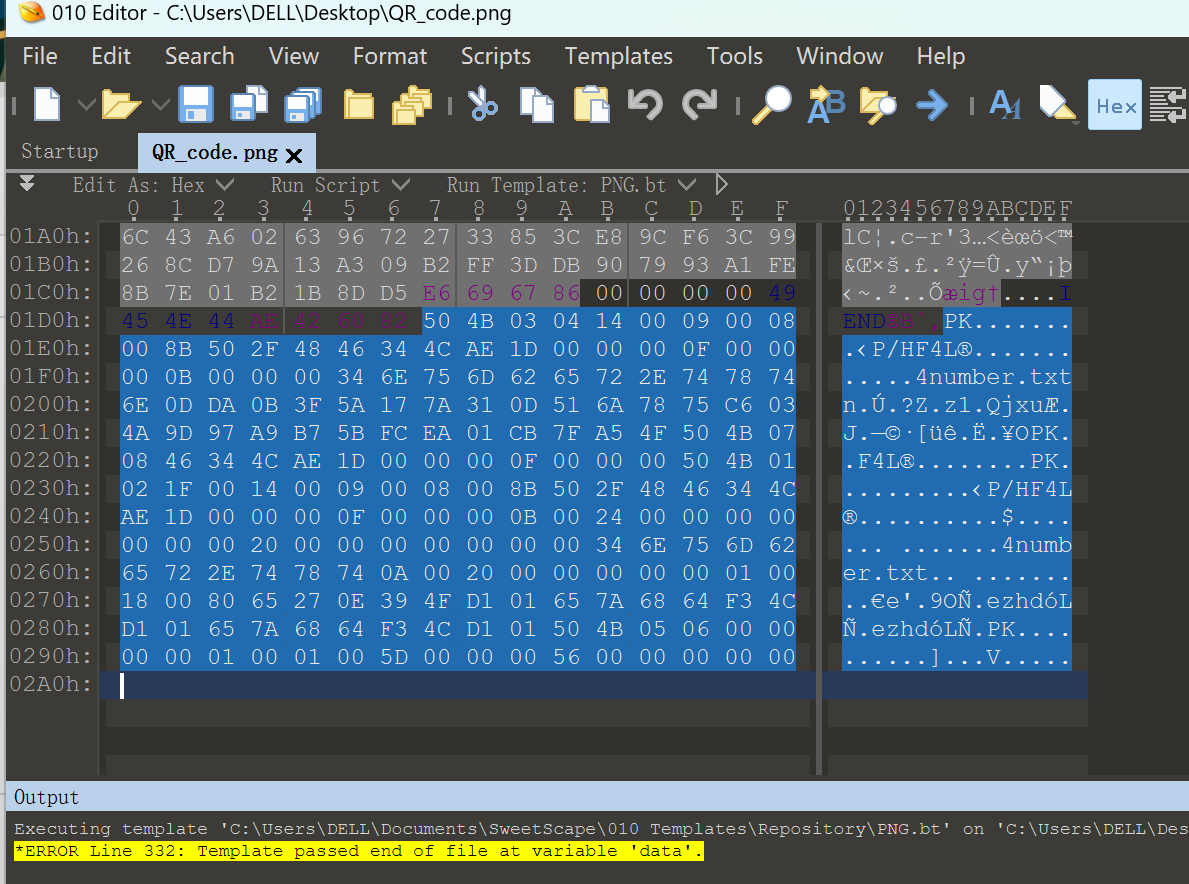
1. 你居然赶我走

Stegsolve分析。

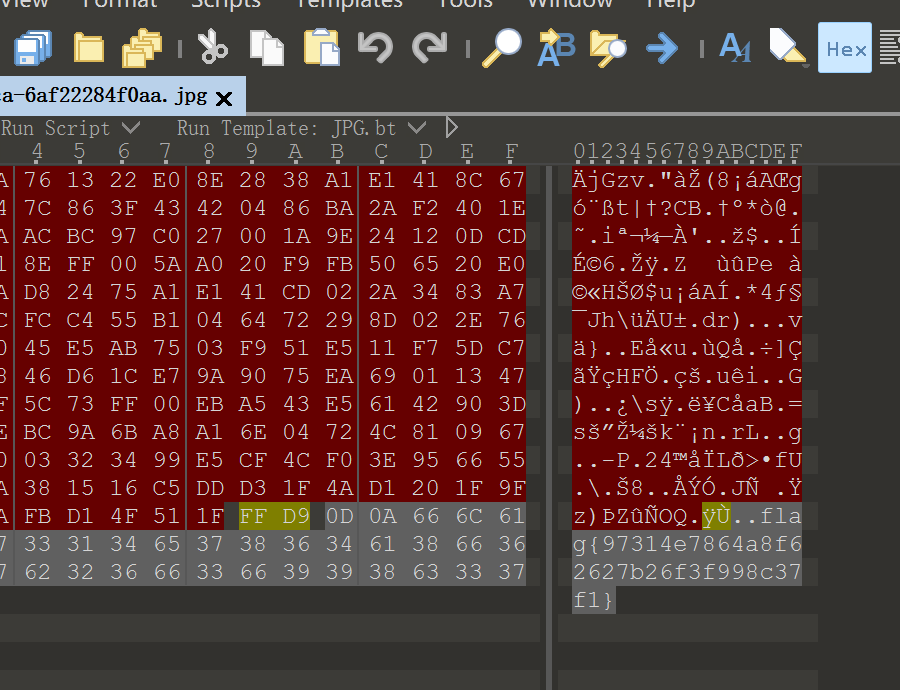
1. 大白

PNG宽高隐写，用010editor或者winhex修改其高度为A7，得到flag。（因为我CRC检验打开图片出问题，于是暴力修改）

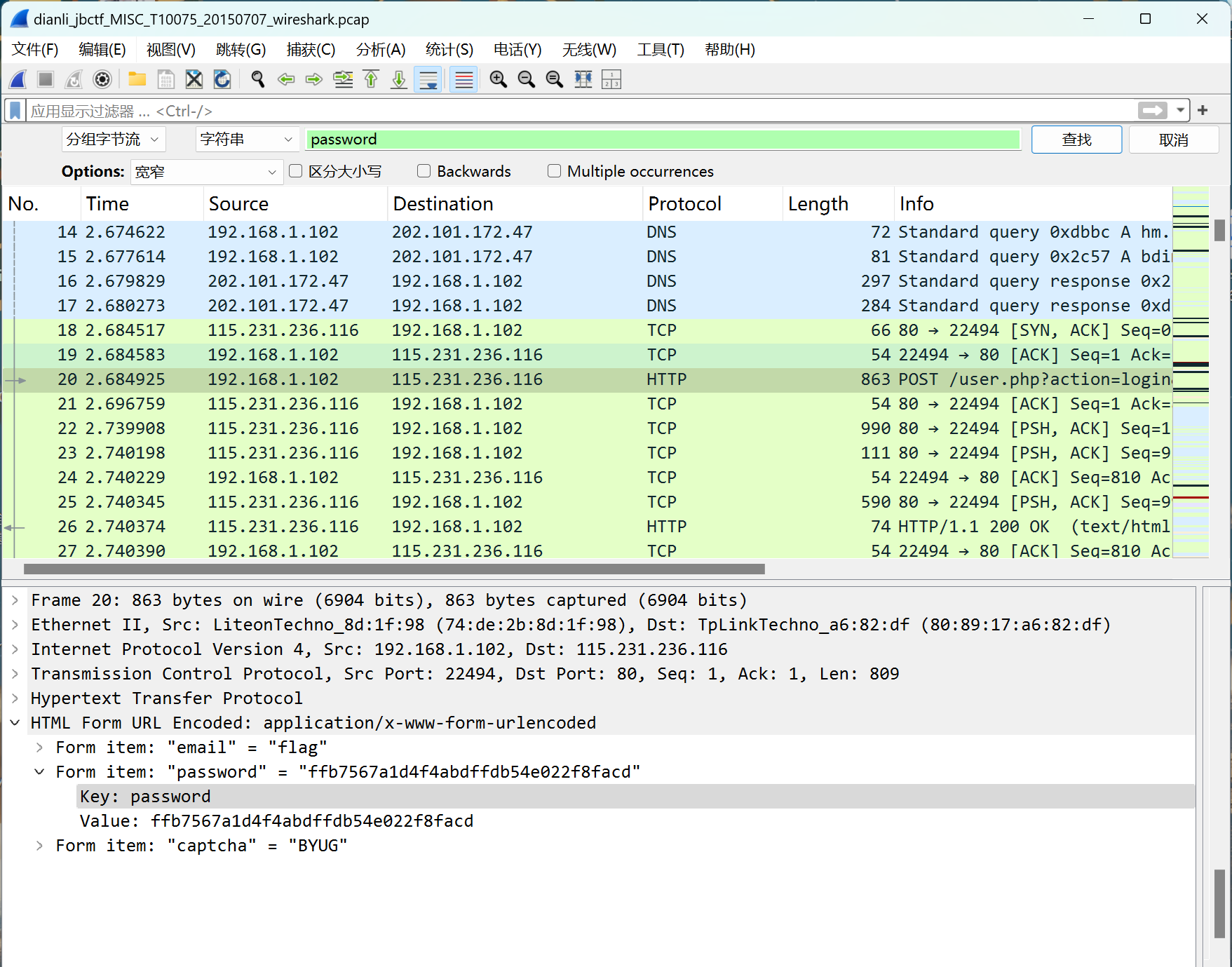
1. 二维码

直接扫，没有。用010editor打开，发现隐藏了一个压缩包（50 4B 03 04开头）。把后面的复制到新文件并导出为.zip，用ARCHPR破解压缩包密码。

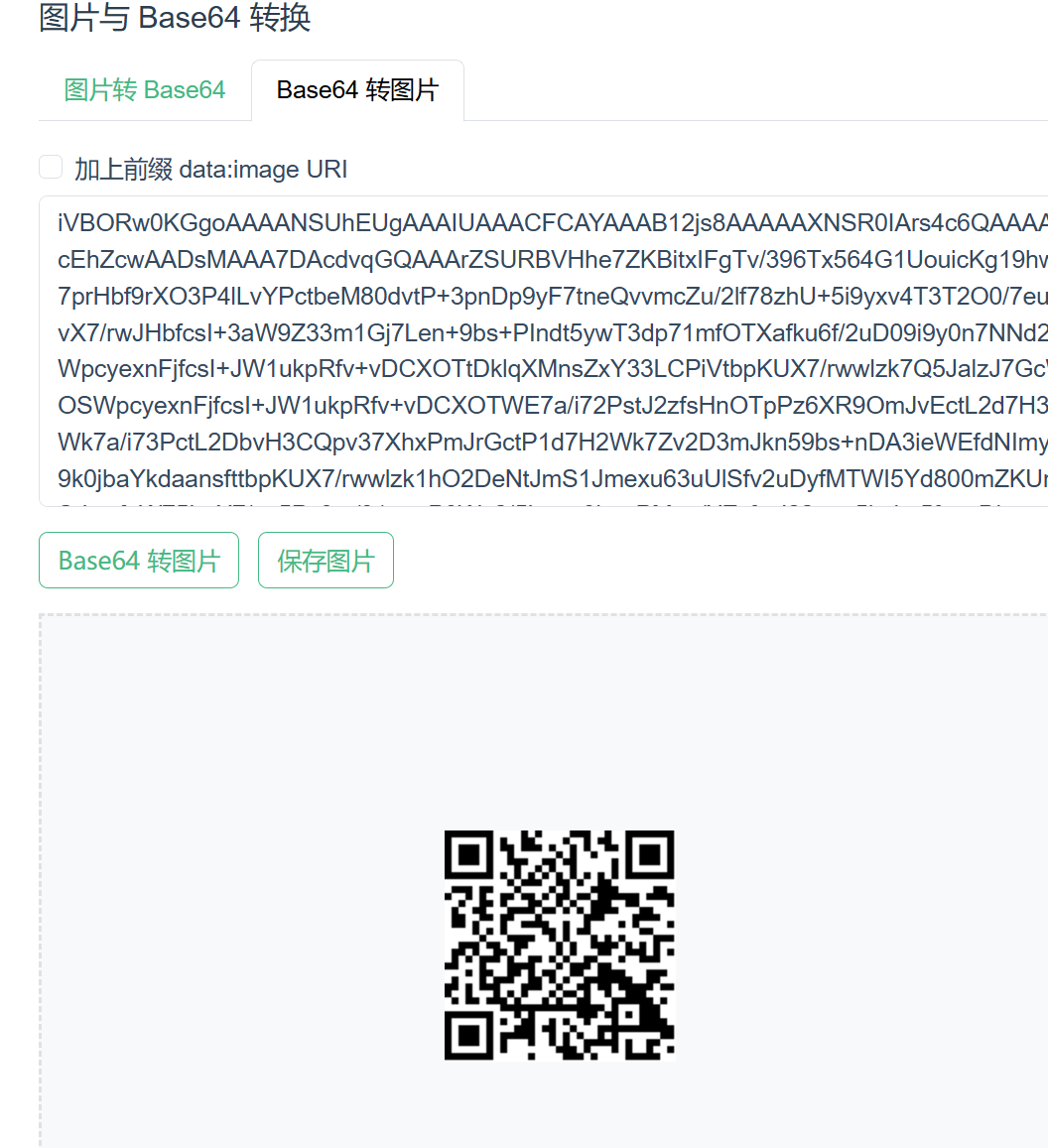
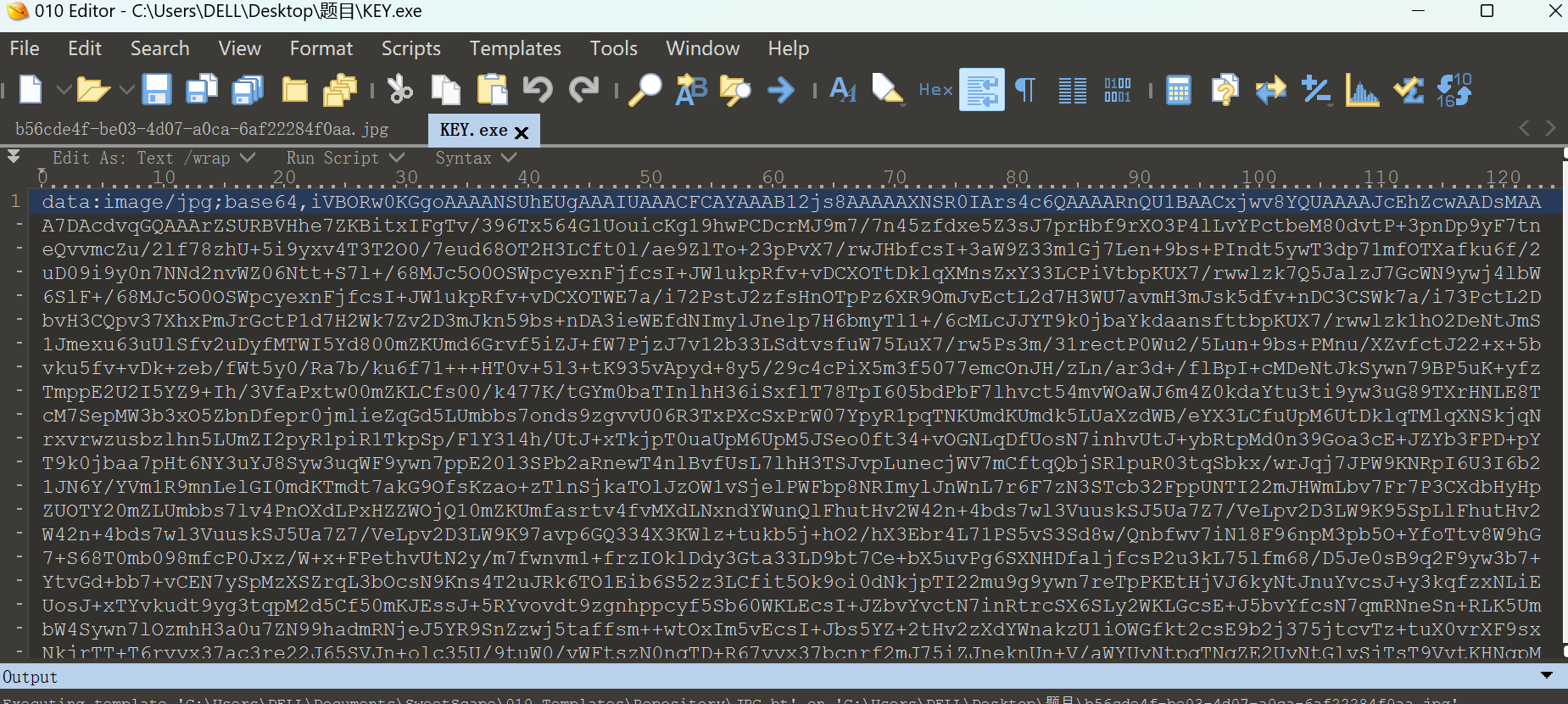
1. 乌镇峰会种图

010editor打开，最下面直接发现flag。

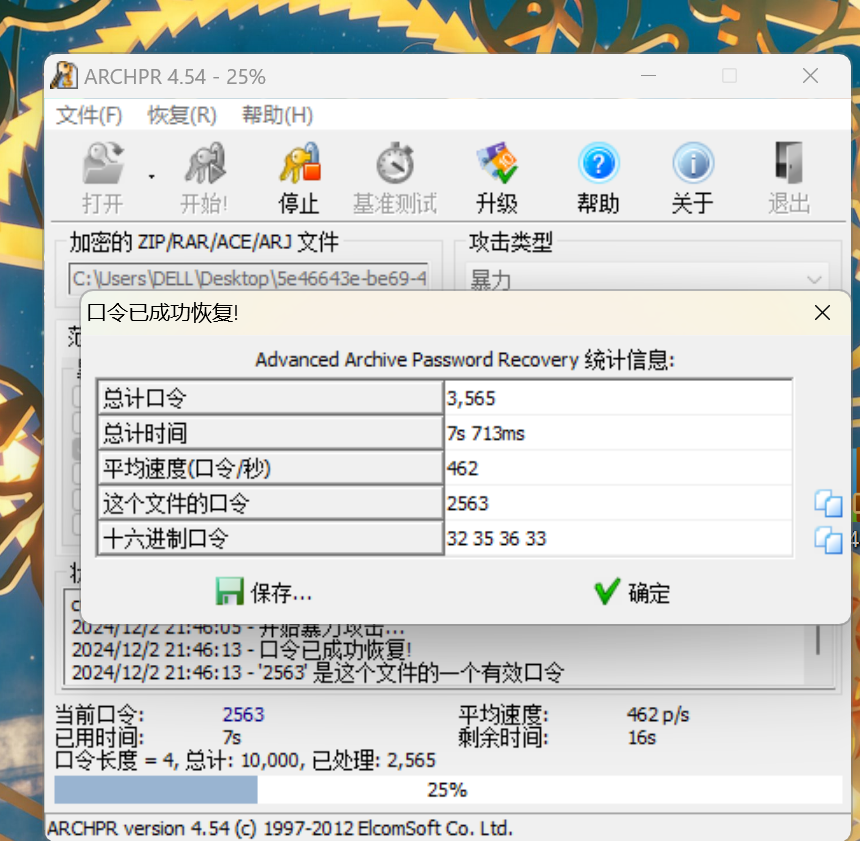
1. Wireshark

根据题意去检索“password”，即为flag。

1. N种方法解决

010editor打开，将其复制用Base64转图片，再用QR research工具，得到flag。

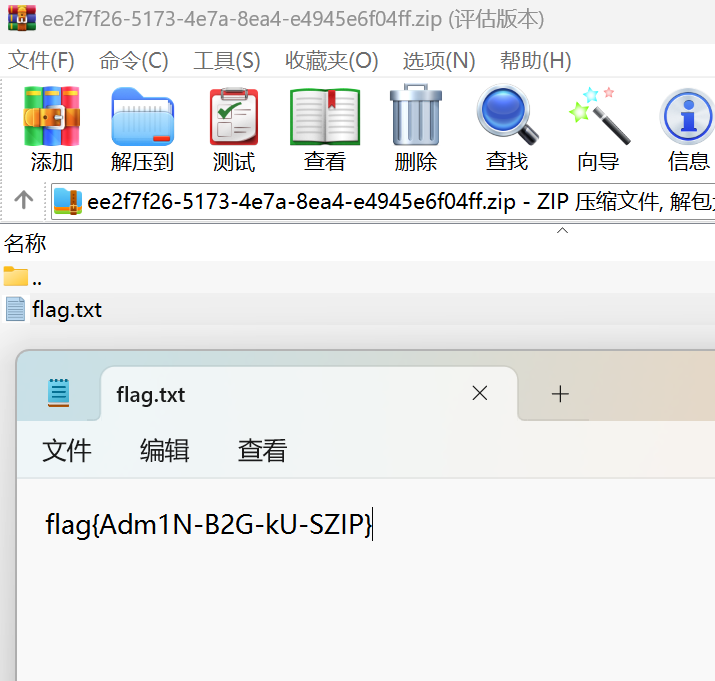
1. 基础破解

ARCHPR破解密码，得到后用Base64解码，得到flag。

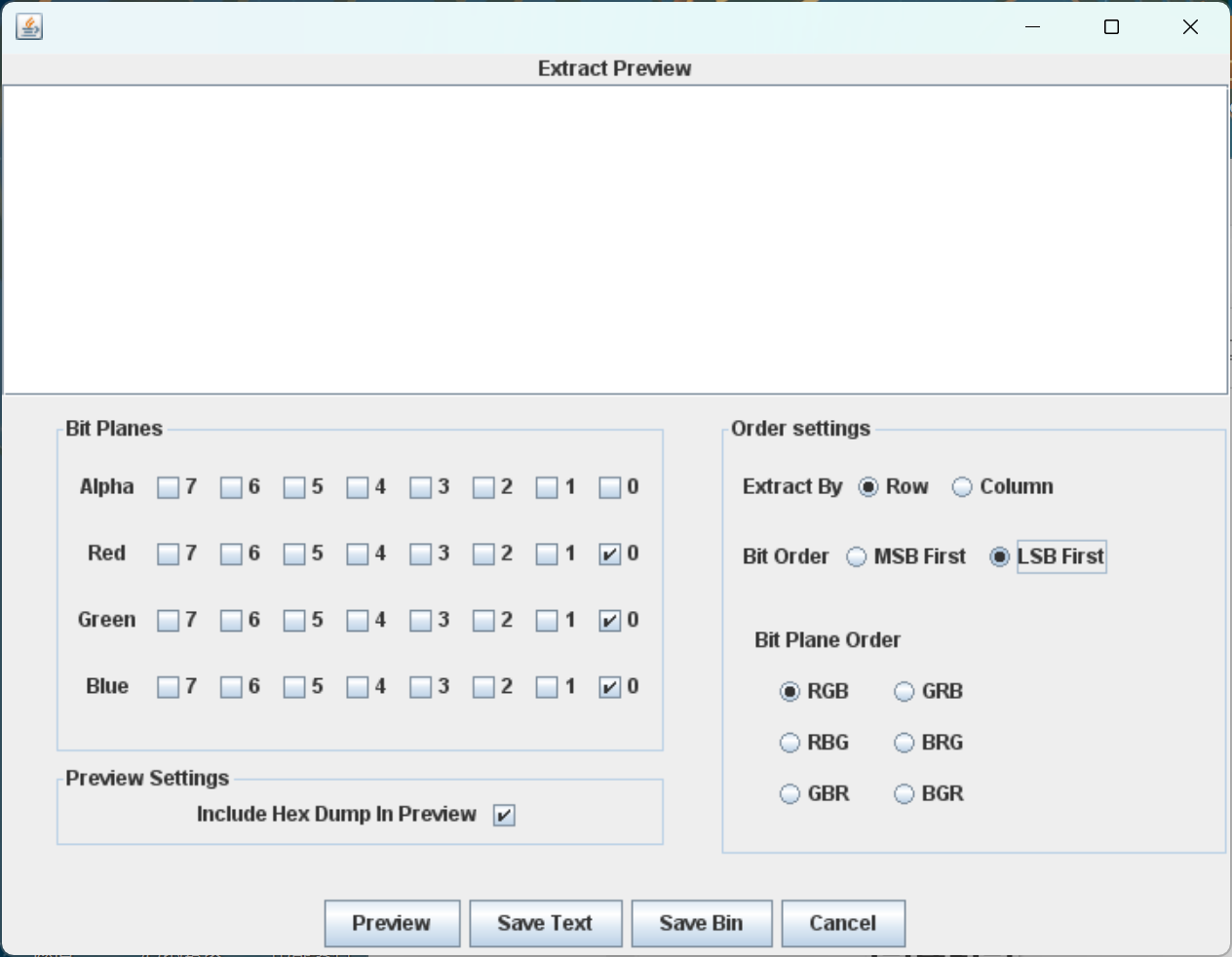
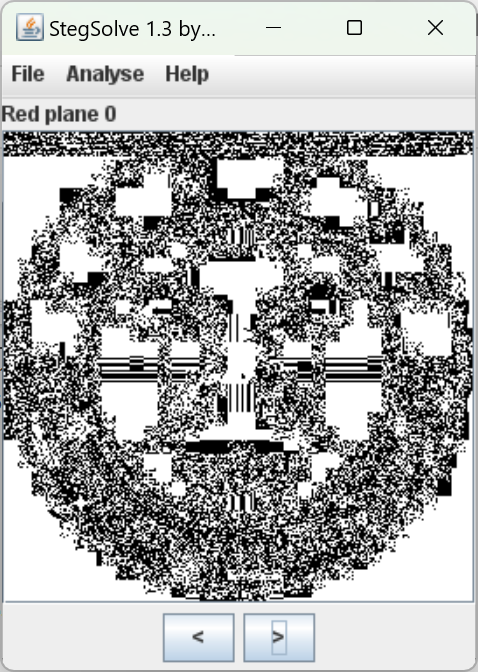
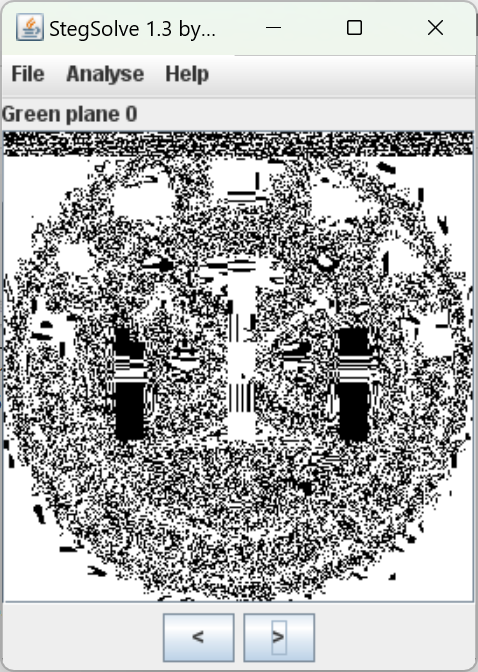
1. 图片中的秘密

打开图片属性界面，“备注”发现flag。

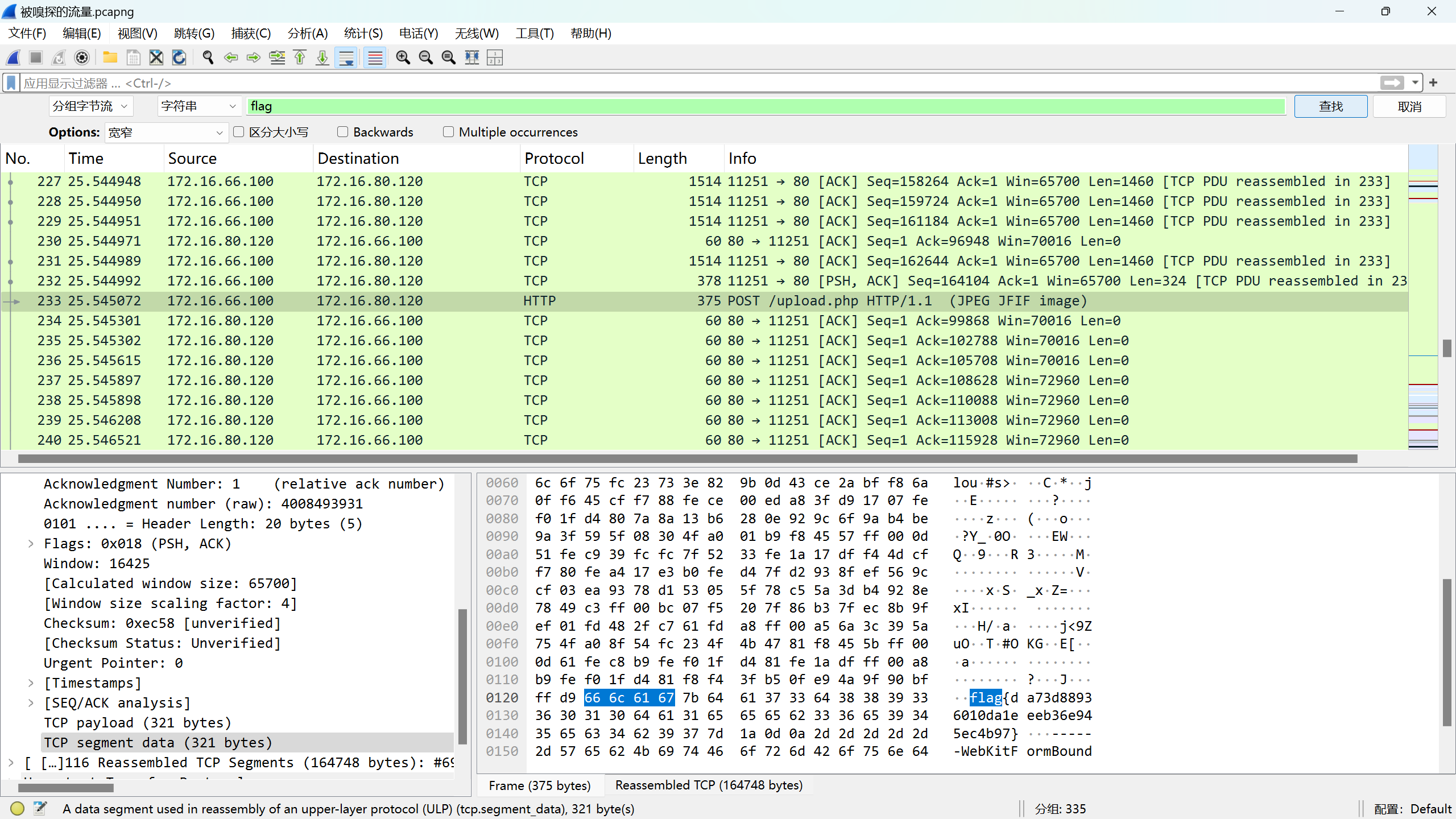
1. Zip伪加密

由题意，文件是伪加密，用010editor打开，将50 4B 01 02后面的09修改为00，使其变为正常文件，得到flag。

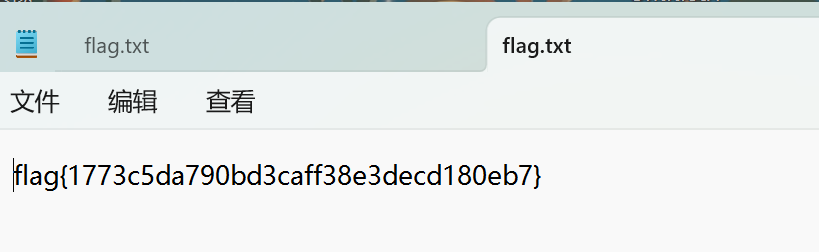
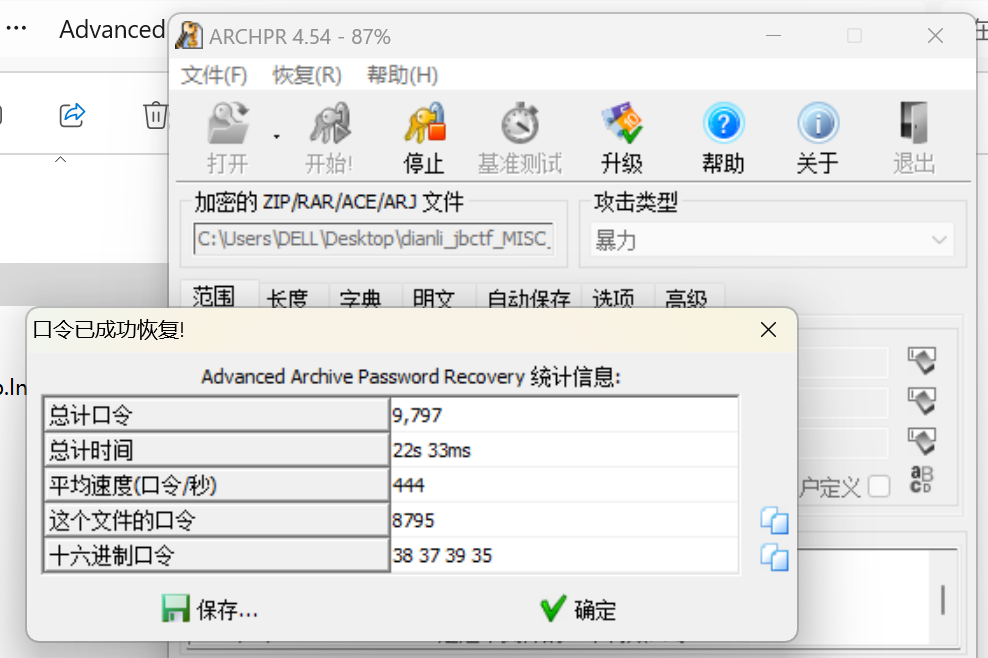
1. LSB

考察LSB隐写，用Stegslove处理。发现蓝、绿、红三个最低通道最上面有东西，进入data extract，勾选对应最低位，save bin，扫码。

1. 被嗅探的流量

wireshark打开后搜索flag。

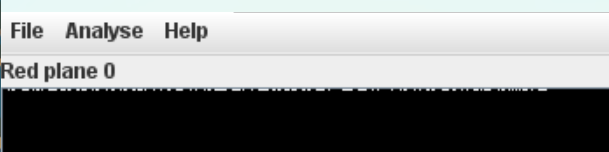
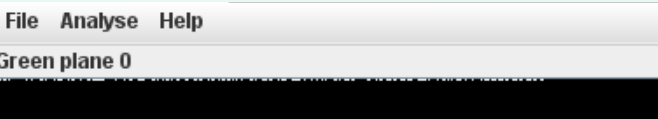
1. Rar

ARCHPR破解。

1. Qr

直接扫码。

1. 镜子里面的世界

Stegsolve打开，处理方法与12题类似。直接preview可以发现flag。

## 结语

这一个月感觉事情不少，忙忙碌碌中抽空学了不少东西，本来还想学web，但是似乎没看懂基础的教学。感觉自己要学习的东西还是很多，以后还要更加认真学。