关于CTF压缩包的那些事

原创

绿冰壶 于 2021-05-14 15:11:32 发布 739 收藏 6

关于CTF压缩包的那些事

前言

CTF比赛中经常会给你各种各样奇怪加密方式的压缩包，这里基于合天相关课程学习小小的总结一下，可能不全，持续更新

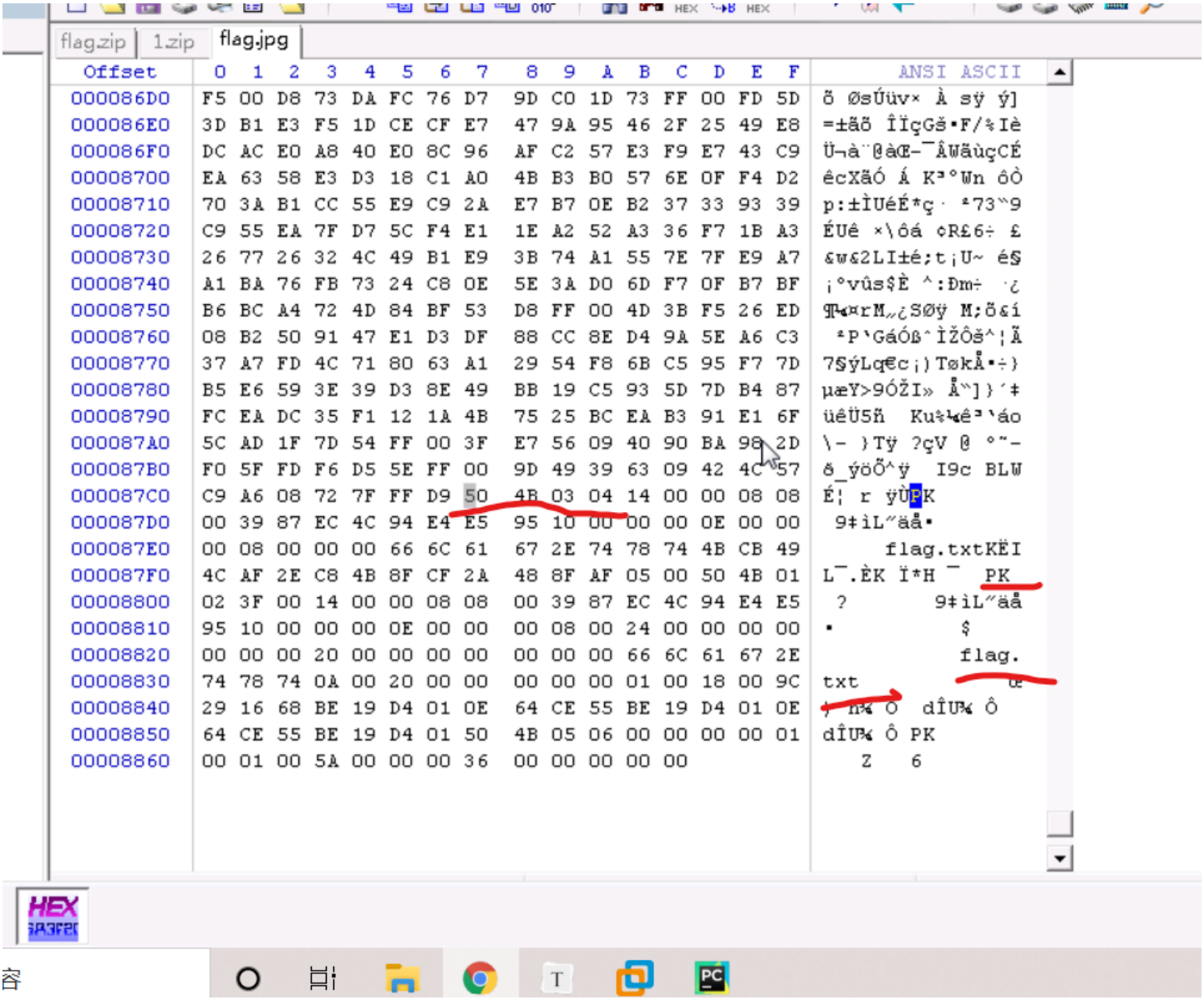
利用进制转换隐藏信息

给你一大串十六进制字符串

你发现是50 4B 03 04 开头的，他其实是个压缩包，放入winhex改后缀保存即可得到zip文件，zip文件里有flag

作为冗余信息藏在其他文件中

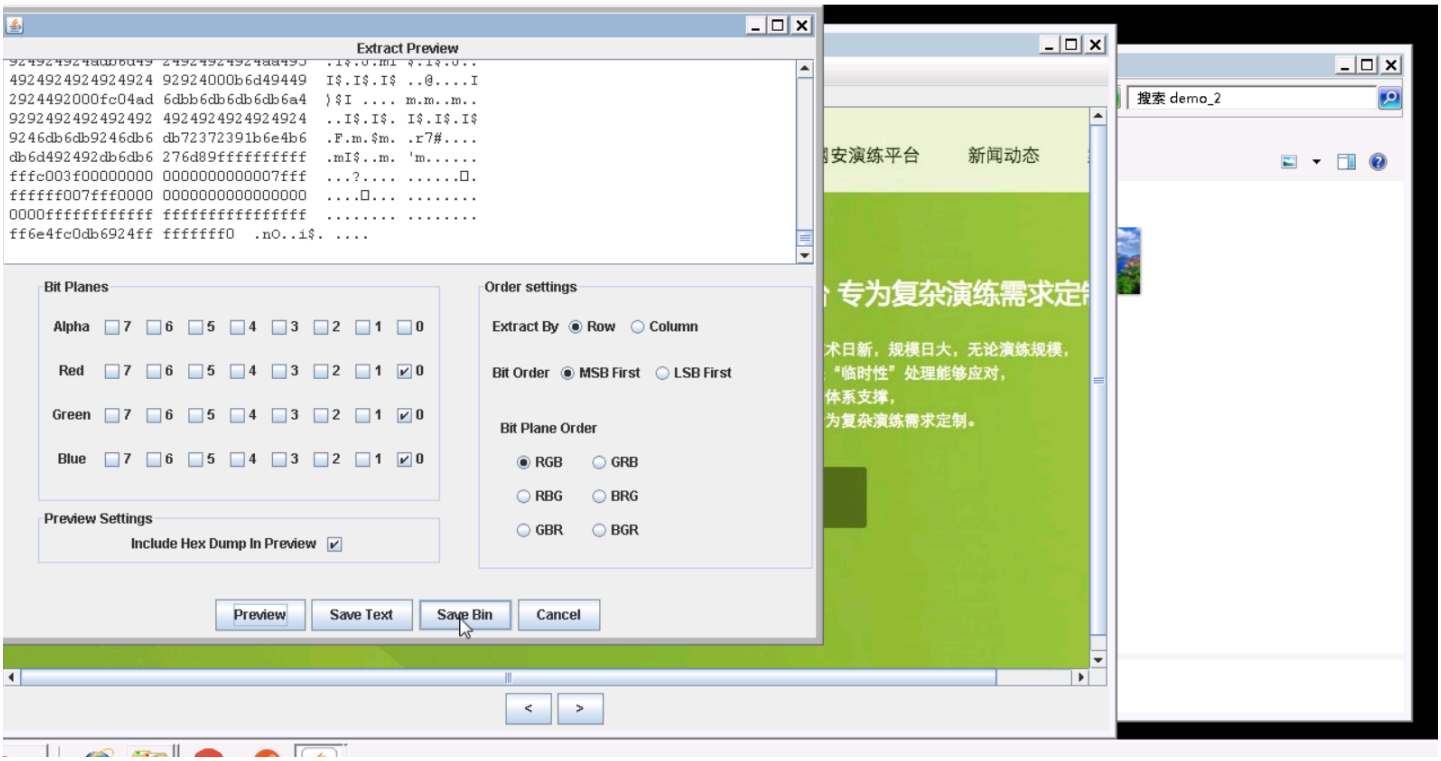
winhex打开，搜索该文件文件尾，看后面是否还有压缩包文件头



解决方式，直接将后缀名改为zip解压

利用隐写隐藏在其他文件中

LSB为常规隐写算法，使用stegsolve



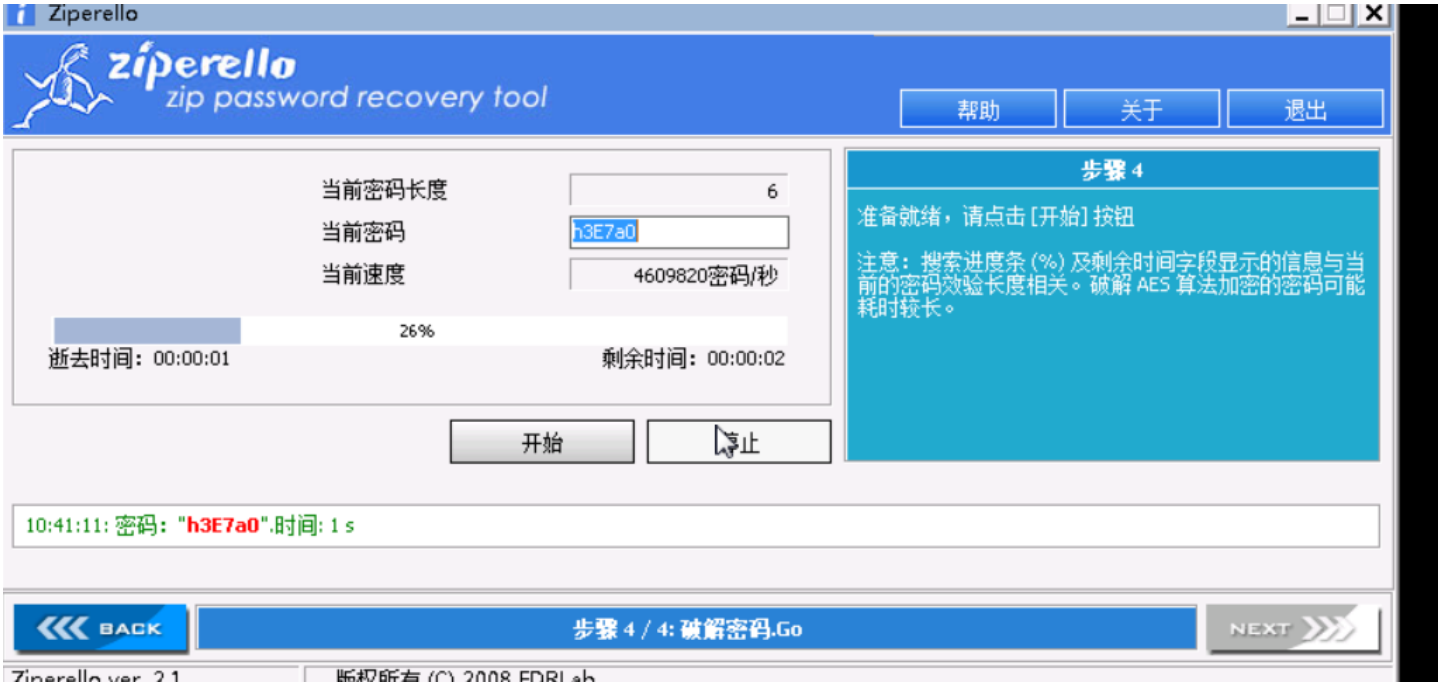
暴力破解

使用ARCHPR暴力破解

使用掩码攻击

安装ziperello

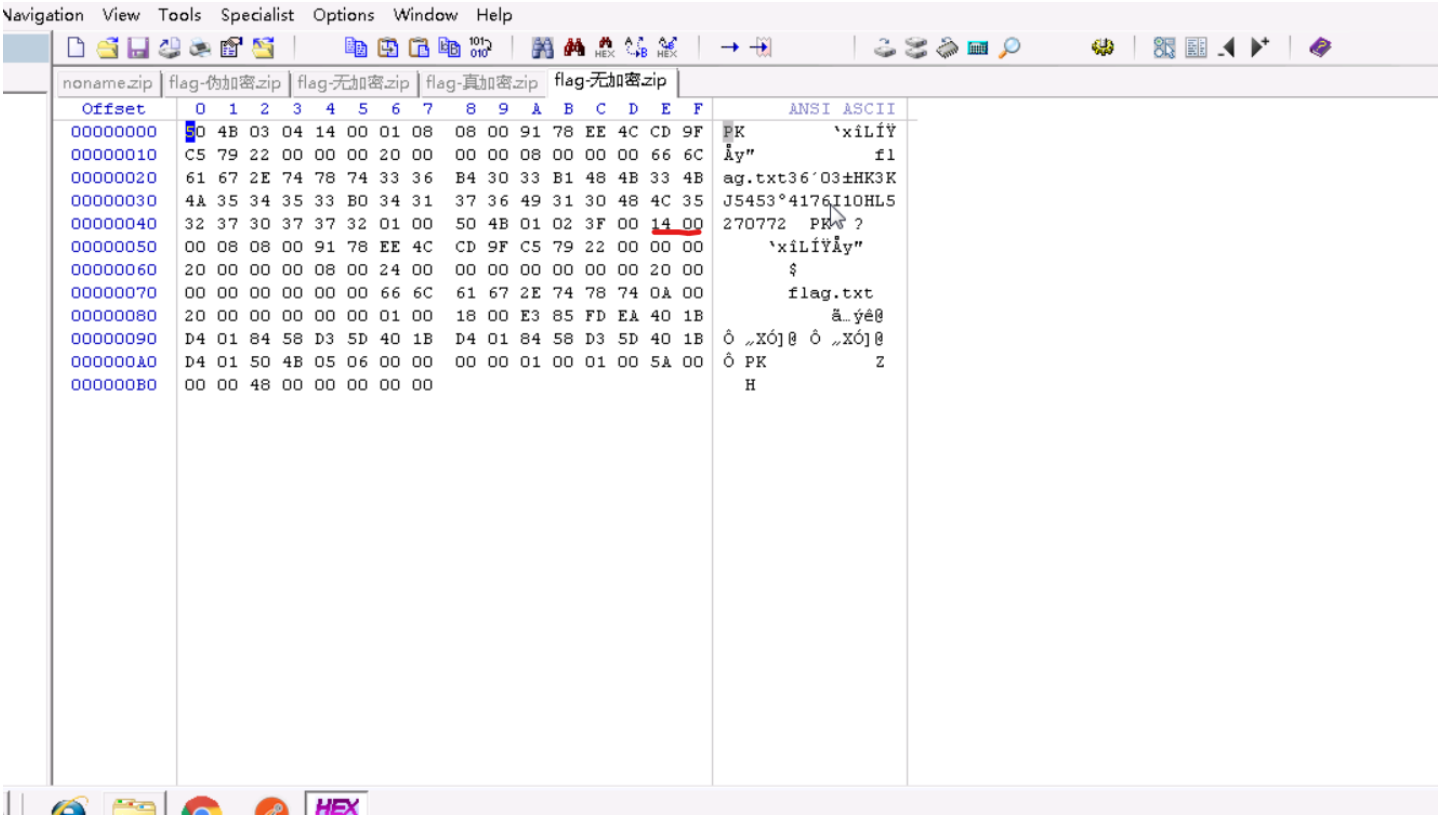
选择要解密的文件，选择基于模板的破解



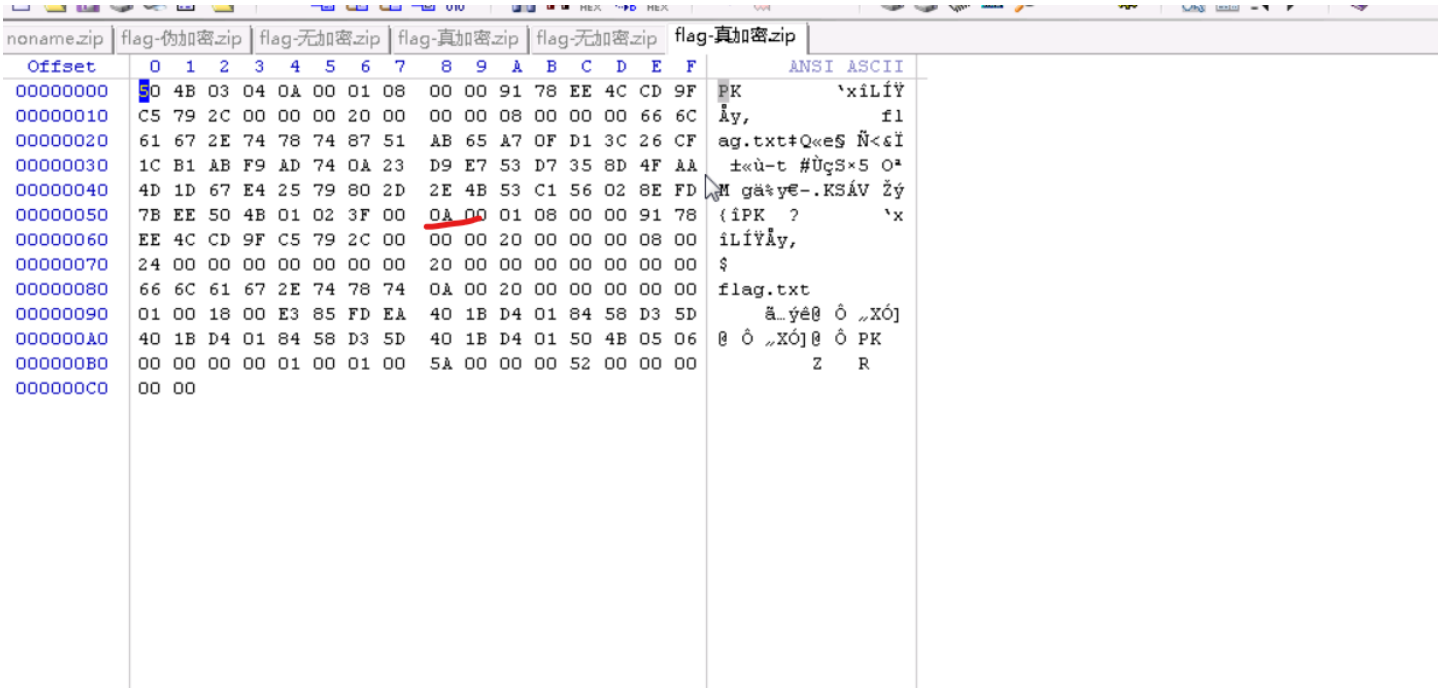
zip伪加密

区分是否为伪加密，关键是看zip头50 4B 01 02 后第三个十六进制位

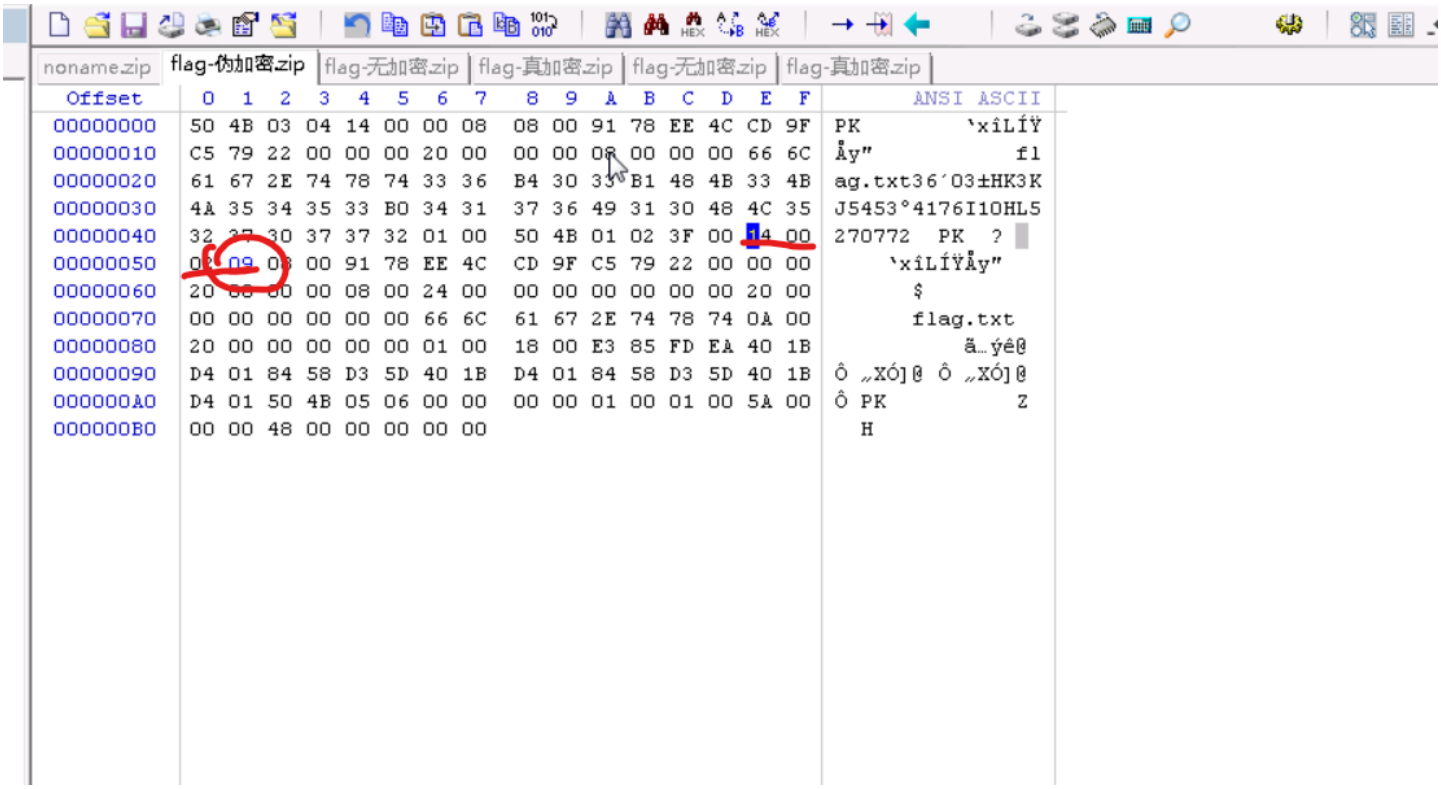
这是没有加密的情况



这是加密的情况，第三位为0A说明为真加密



这是伪加密的情况，第三位上与无加密一致，但是第六位为奇数，这就造成了伪加密



因此将第六位（圆圈区域）改回偶数则破解了伪加密

明文攻击

当你不知道一个zip的密码，但你有zip中的某个文件（文件大小大于128Byte）时可以进行明文攻击

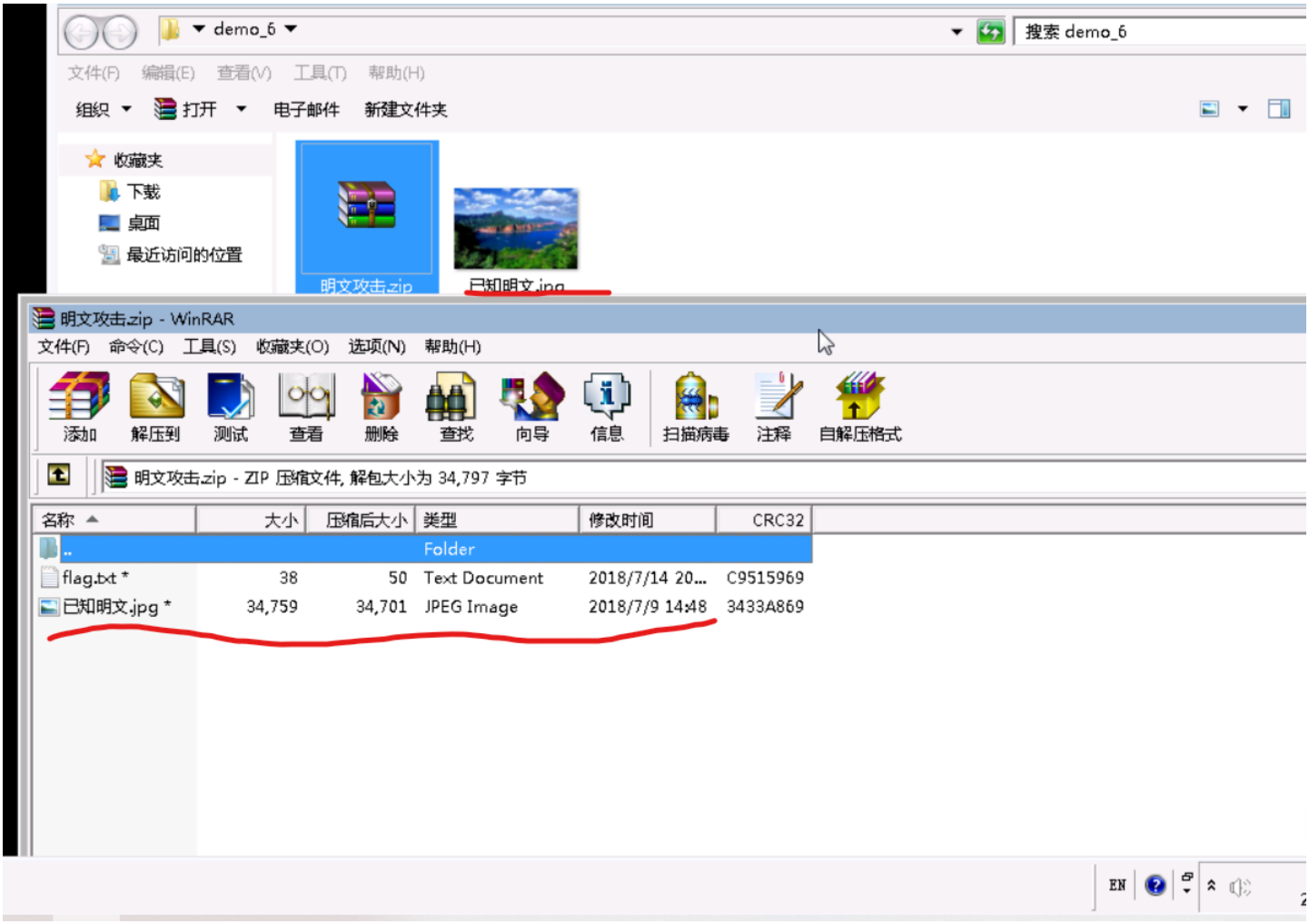
原理

在压缩文件时输入的密码，首先被转换成3个32bit的key，所有文件的key是一样的，如果我们能找到这3个key 就能解开该压缩包的所有文件。**简而言之，同一个zip压缩包中的所有文件都是使用同一个加密密钥来加密的，找到密钥即可解密压缩包**

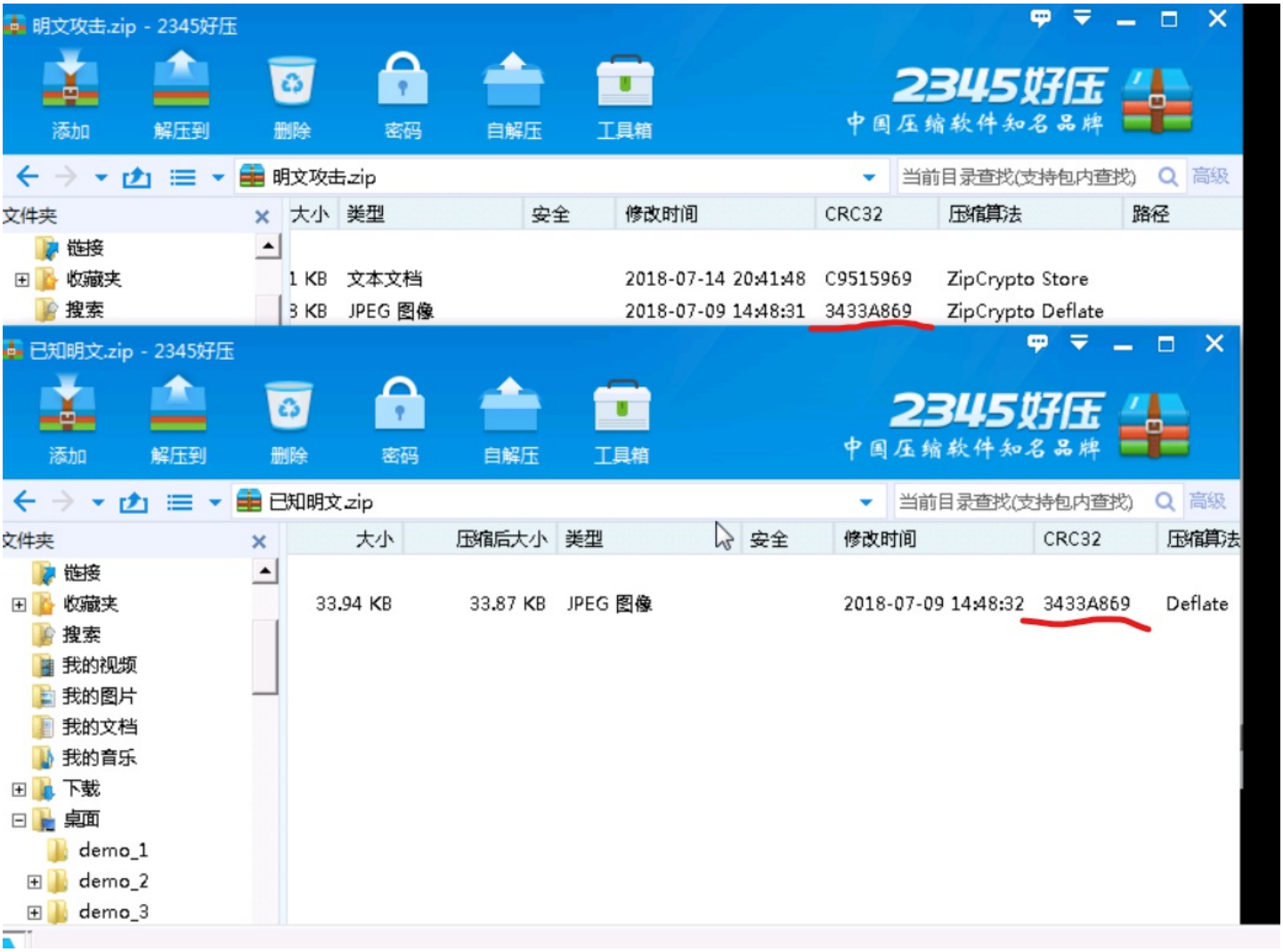
那么如何找这个密钥呢？利用我们所有的zip中的某个文件 。我们把该文件用同样的压缩软件，同一种方式进行无密码的压缩，然后比较压缩后文件的crc32值，如果相同则说明我们成功了。

攻击实例：

发现已知明文是明文攻击zip中的一个文件。于是我们无密码把已知明文压缩一下



对比两个压缩文件中“已知明文.jpg”的CRC32值，如果一致，就可以进行明文攻击，如果不一致，则换一种压缩方式继续比较



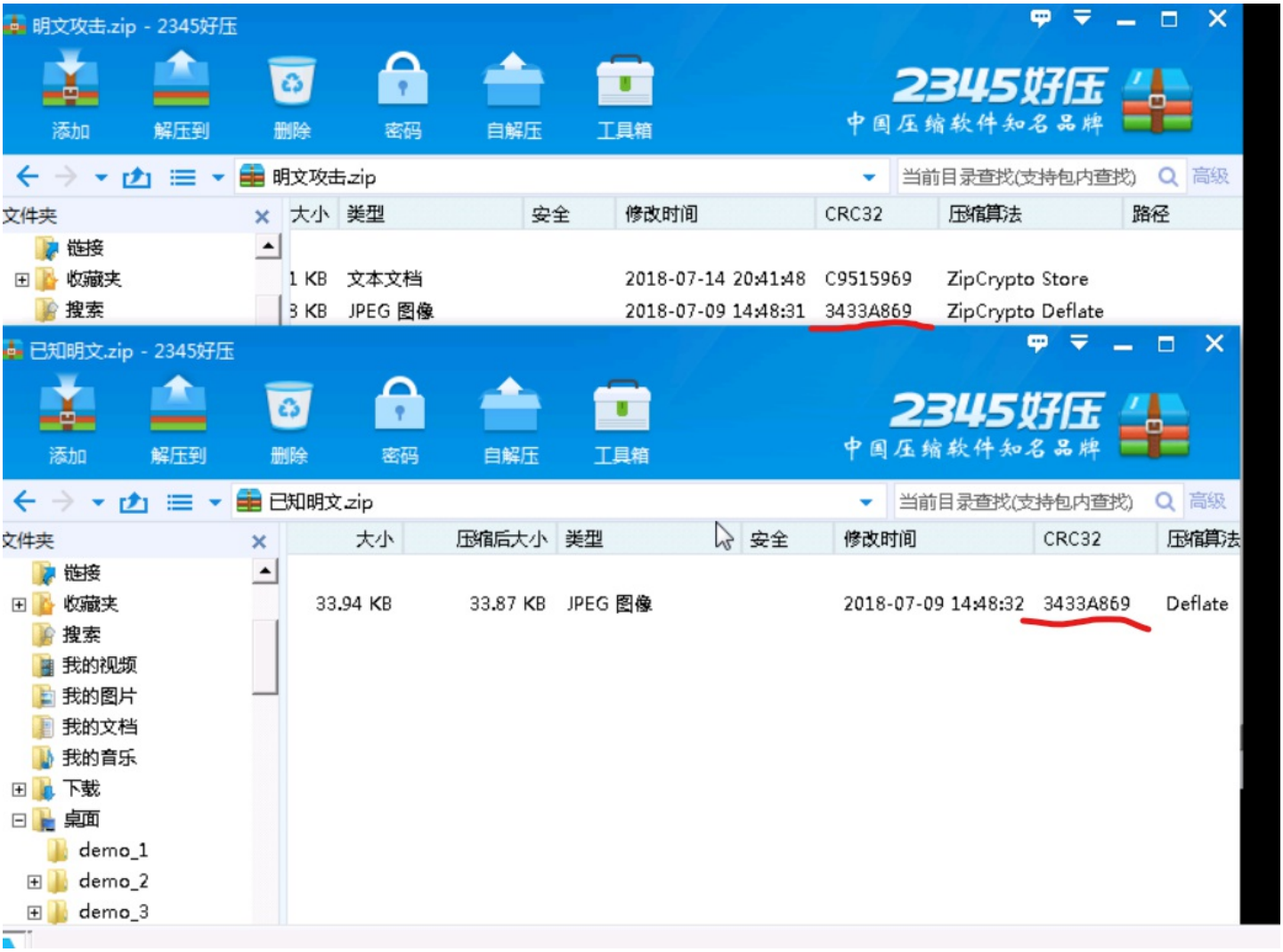
对比是一致的，下面开始明文攻击

使用AZPR软件


Advanced ZIP Password Recovery
Open
Save
Start !
Stop
Benchmark
Help
About
Quit
Encrypted ZIP-file
Type of attack
Plain-text
Range
Length
Dictionary
Plain-text
Auto-save
Options
Advanced
Plain-text options
Plain-text file path:
Start from:
Key0:
Key1:
Key2:
Allow using binary file as a plain-text ZIP archive
Status window
2021/5/14 15:05:19 - AZPR version 4.00 build 24 launched, unregistered version, some features disabled
Current password:
Time elapsed:
Progress indicator
Average speed:
Time remaining:
0%
AZPR version 4.00 (c) 1997-2005 ElcomSoft Co.Ltd.

!

得到flag



CRC32碰撞

crc32原理

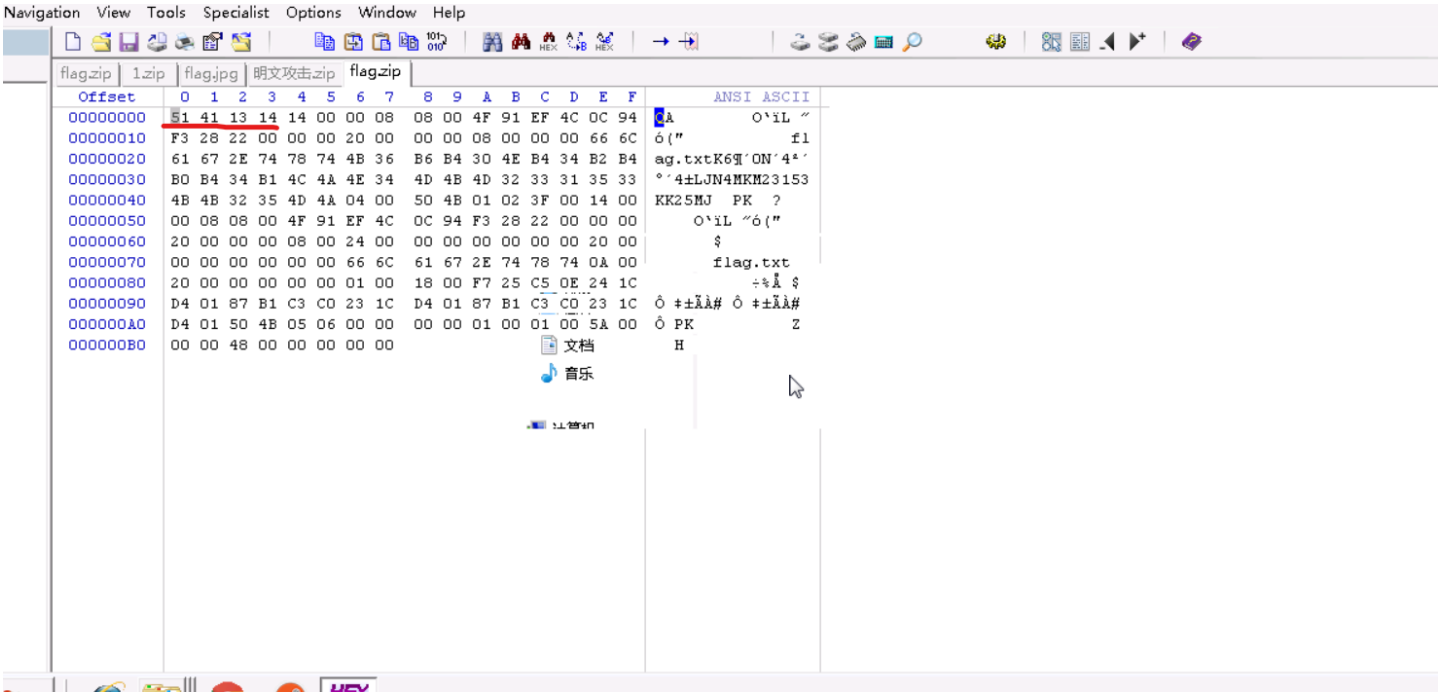
CRC32:CRC本身是“冗余校验码”的意思，CRC32则表示会产生一个32bit（8位十六进制数）的校验值。在产生CRC32时，源数据块的每一位都参与了运算，因此即使数据块中只有一位发生改变也会得到不同的CRC32值，利用这个原理我们可以直接爆破出加密文件的内容。

但是CRC32值也存在被碰撞的可能，也就是会出现内容不一样但是CRC32值一样的情况，所以利用CRC32碰撞的方法得知压缩文件的内容，一般是在被压缩的文件很小的情况下，在CTF中一般为4个字节。

文件修复

打开压缩包尝试解压 提示损坏

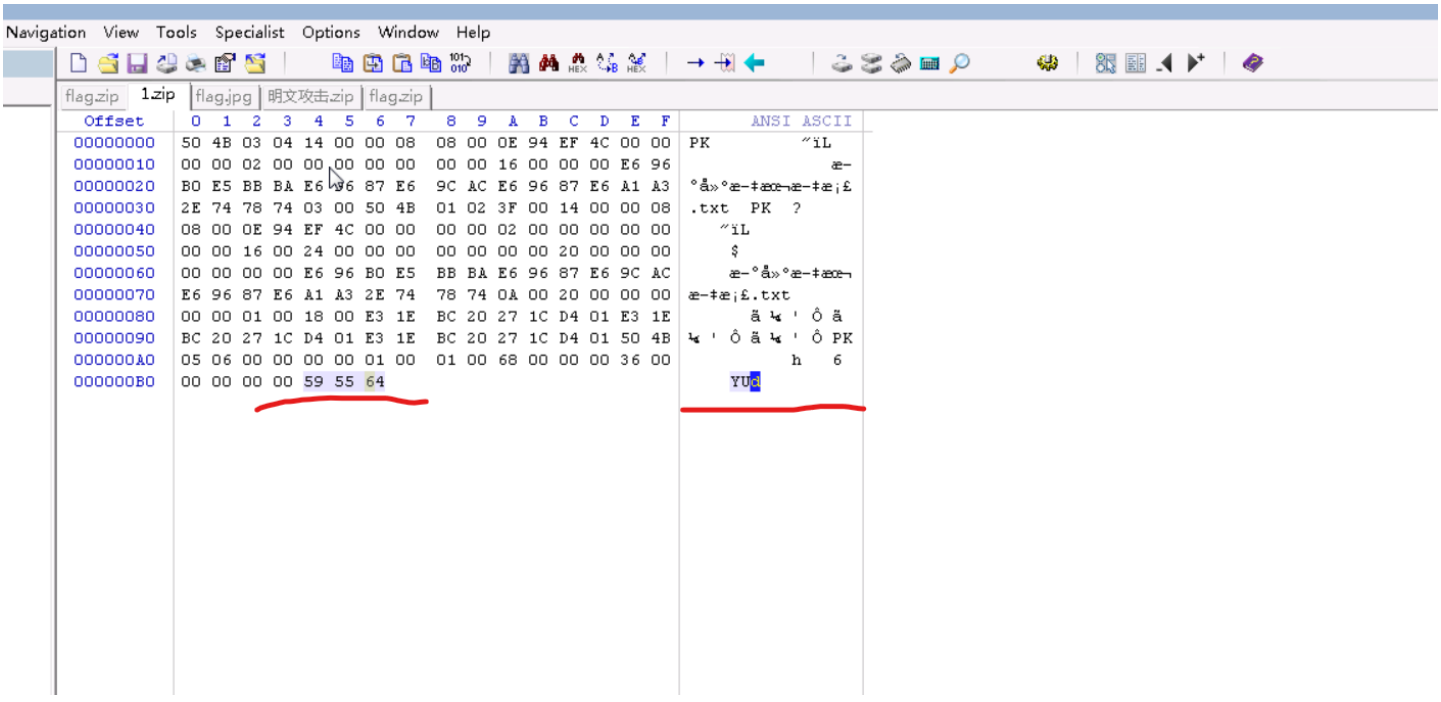
用winhex打开该文件



zip的文件头为50 4B 03 04 且为固定值，这里应该是文件头被篡改了，我们将他改回来，再次解压，就可以得到flag了。

冗余数据拼接

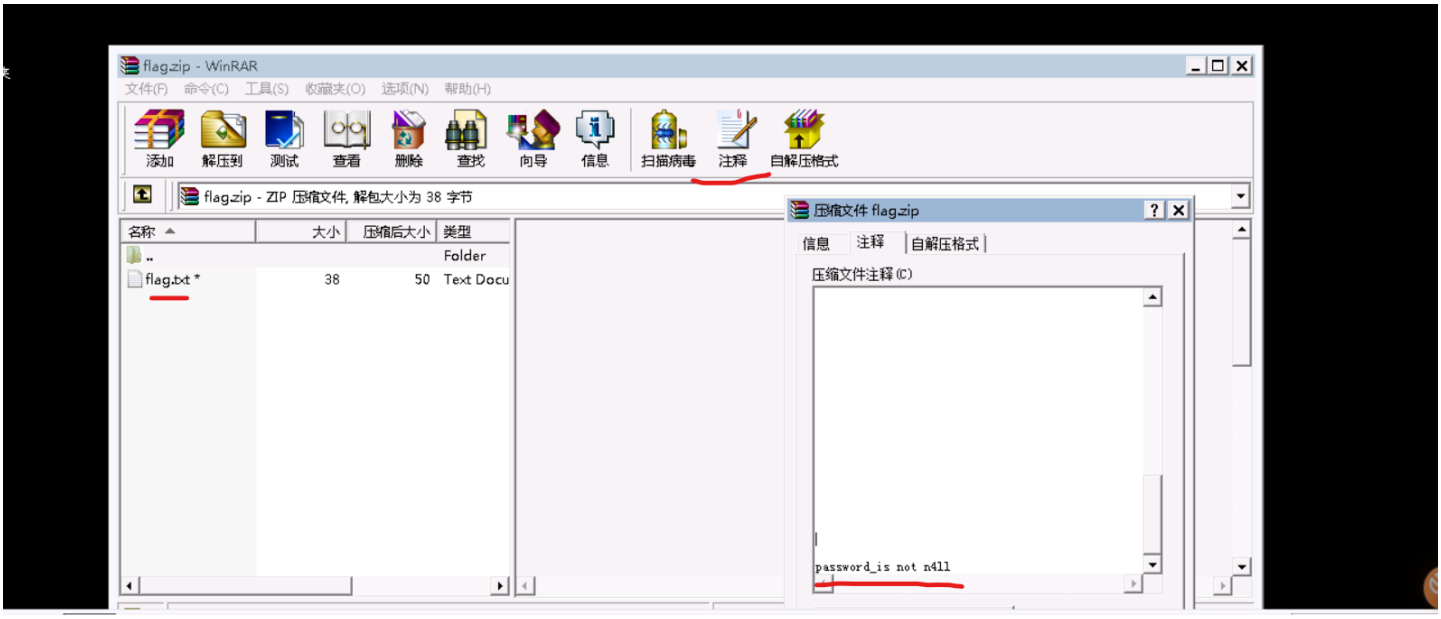
504B0506”，且通常带有18字节（在预备知识中我们将每个偏移量视作一位，也是一个字节）的冗余数据，总共长度一般为22个字节，所以这个套路就是将隐藏信息分为多片隐藏在多个压缩包的结尾



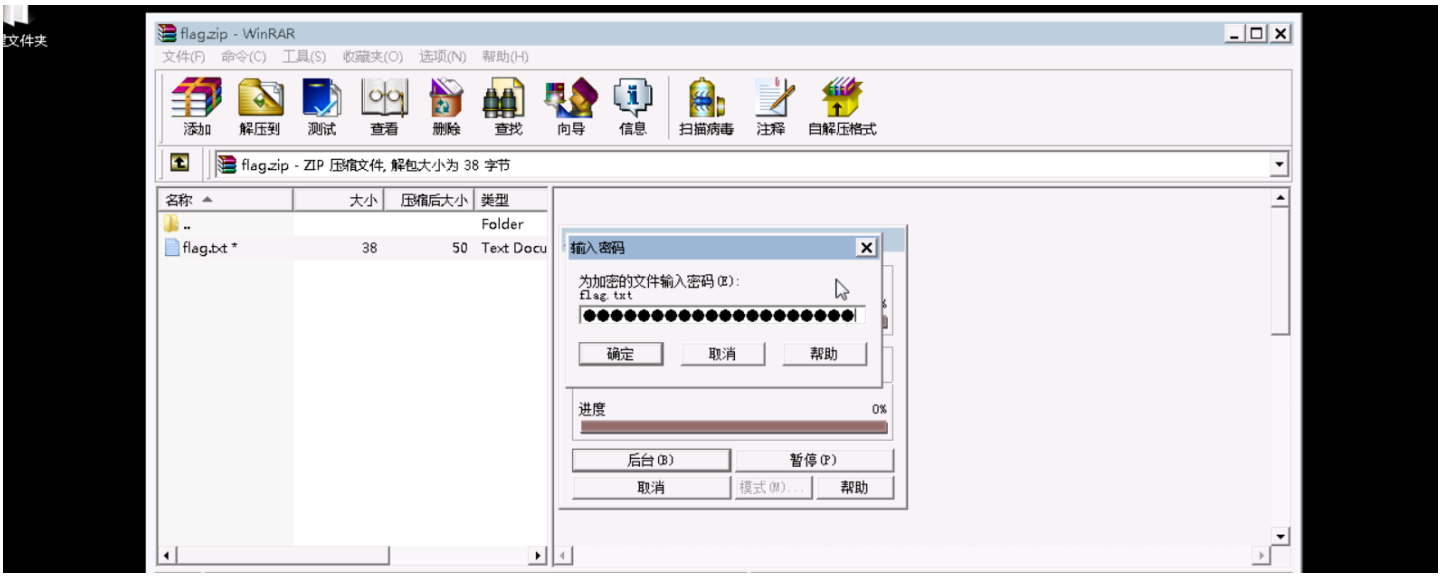
打开四个压缩包 发现22字节后都有三字节的冗余数据，拼接起来得到base64字符串

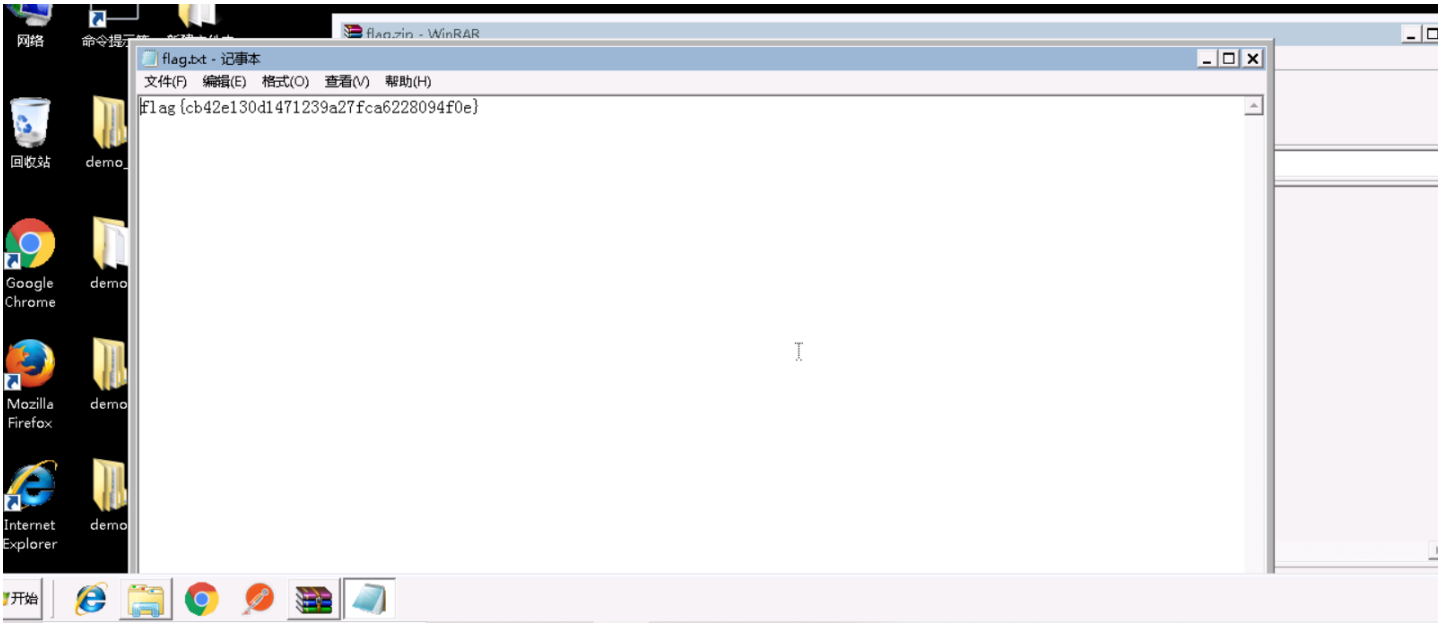
注释隐藏密码

有些压缩包带有注释，注释中可能藏有好东西，嘿嘿

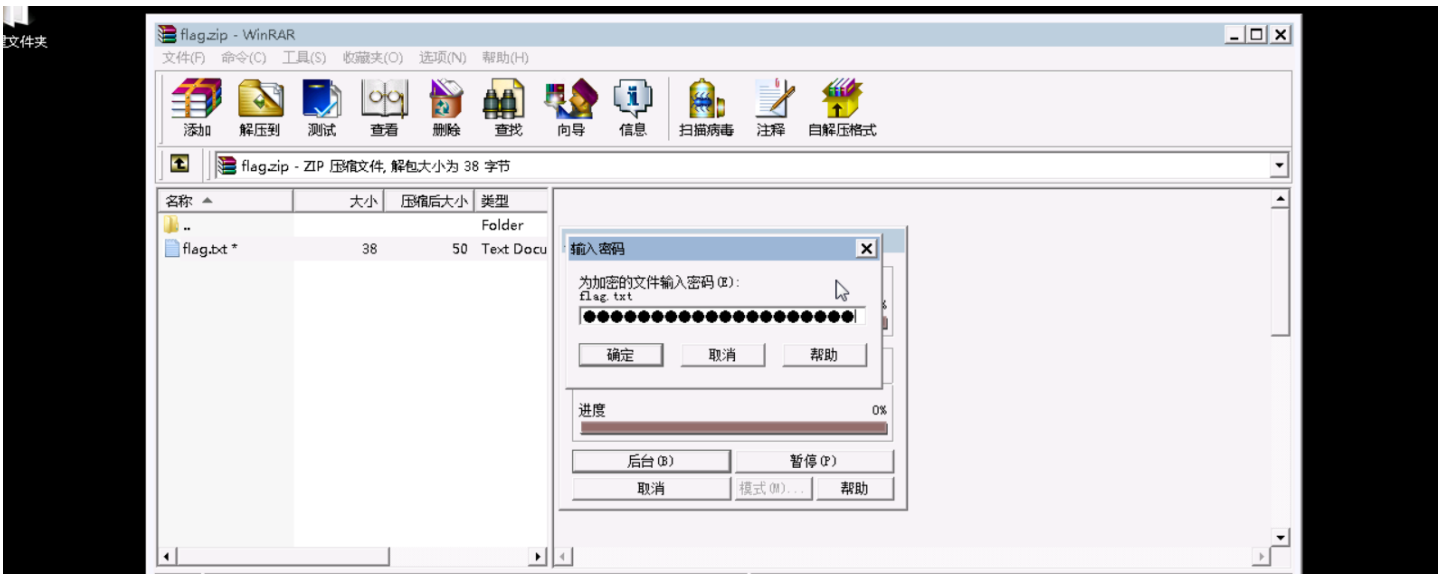


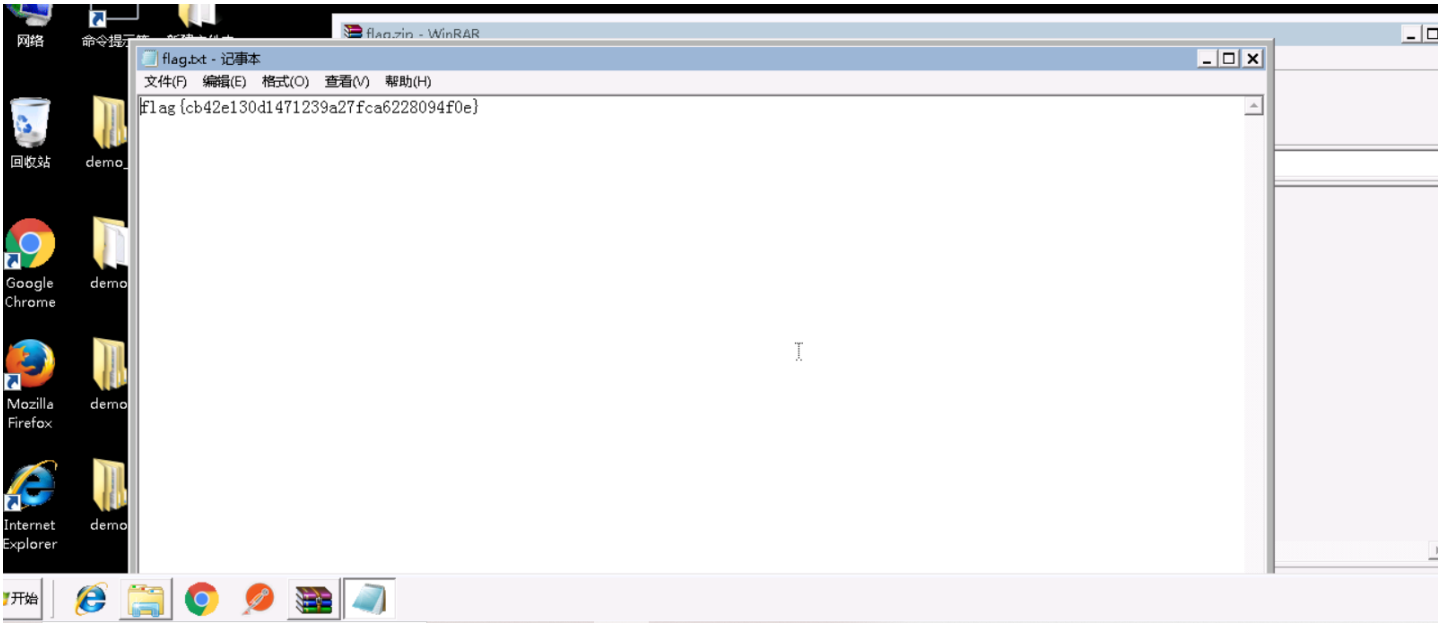
例如这个注释里就有压缩包密码，





例如这个注释里就有压缩包密码，




网络
回收站
demo
Google Chrome
Mozilla Firefox
Internet Explorer
flag.zip - WinRAR
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{cb42e130d1471239a27fca6228094f0e}
开始