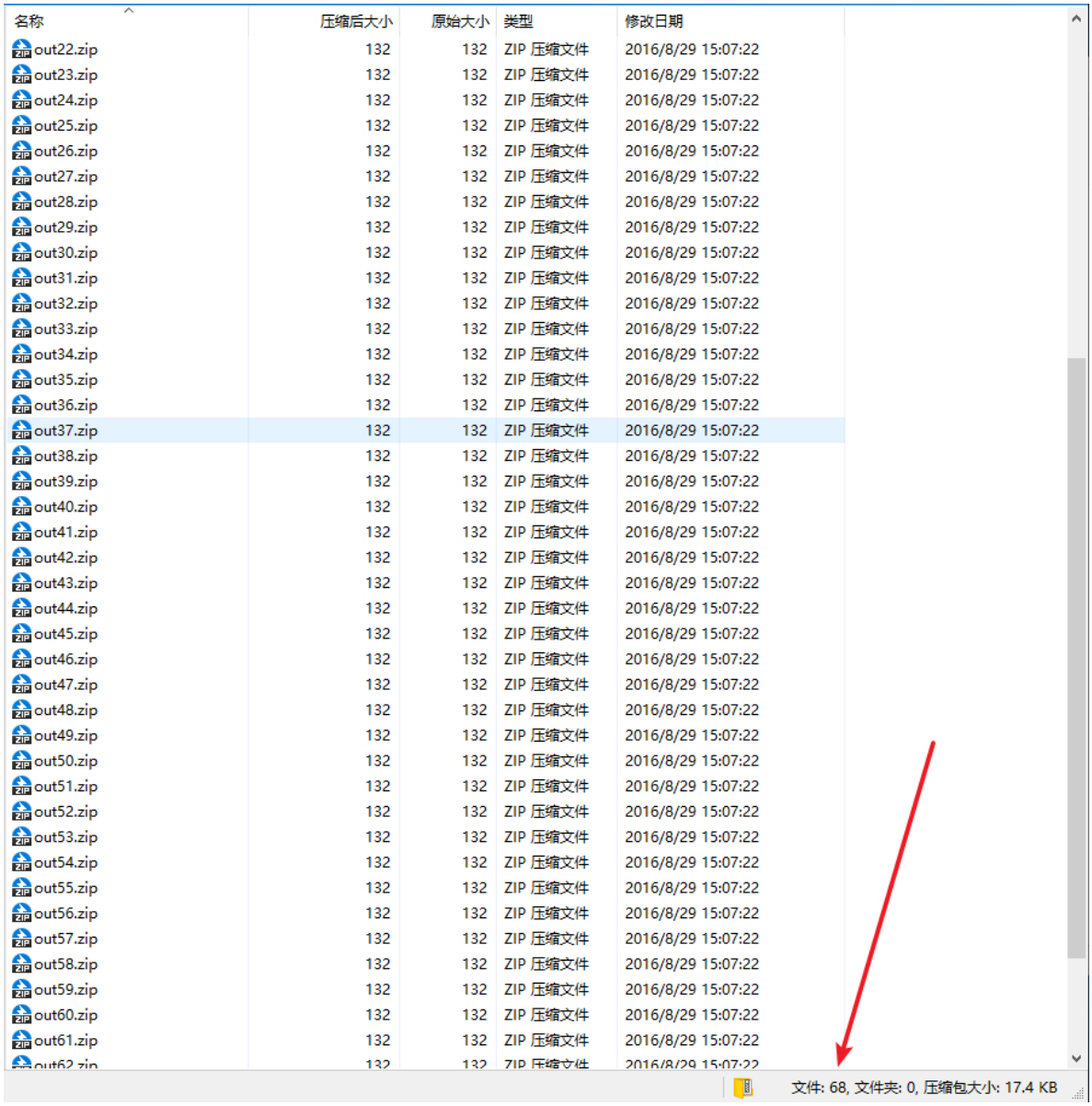
好多压缩包-writeup

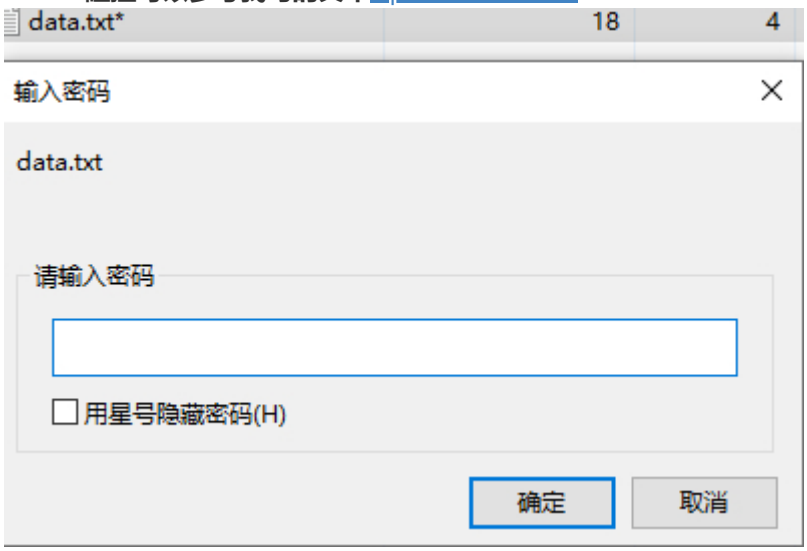
打开题目

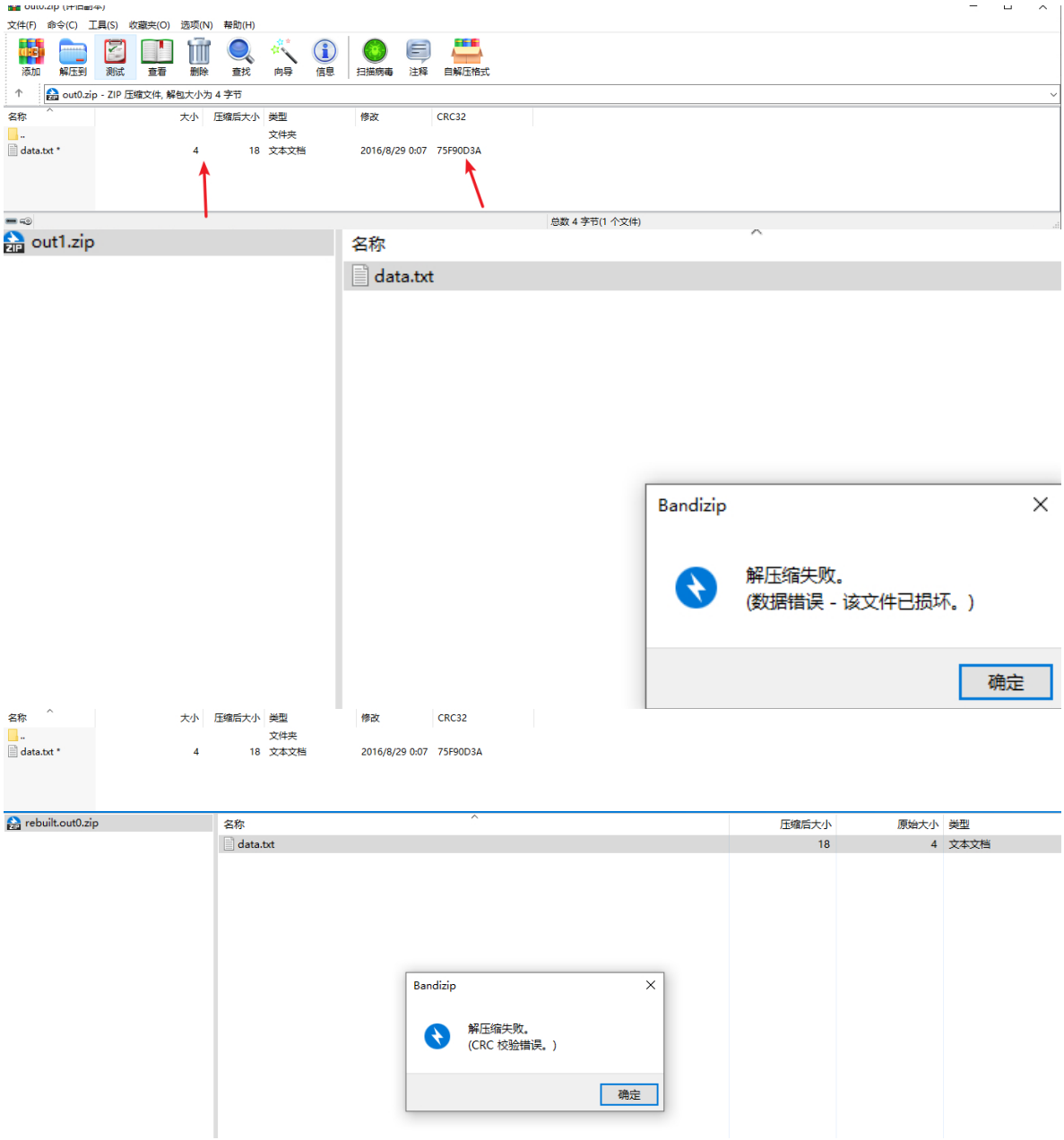
得到一个压缩包附件，进行解压，查看到里面有68个压缩包



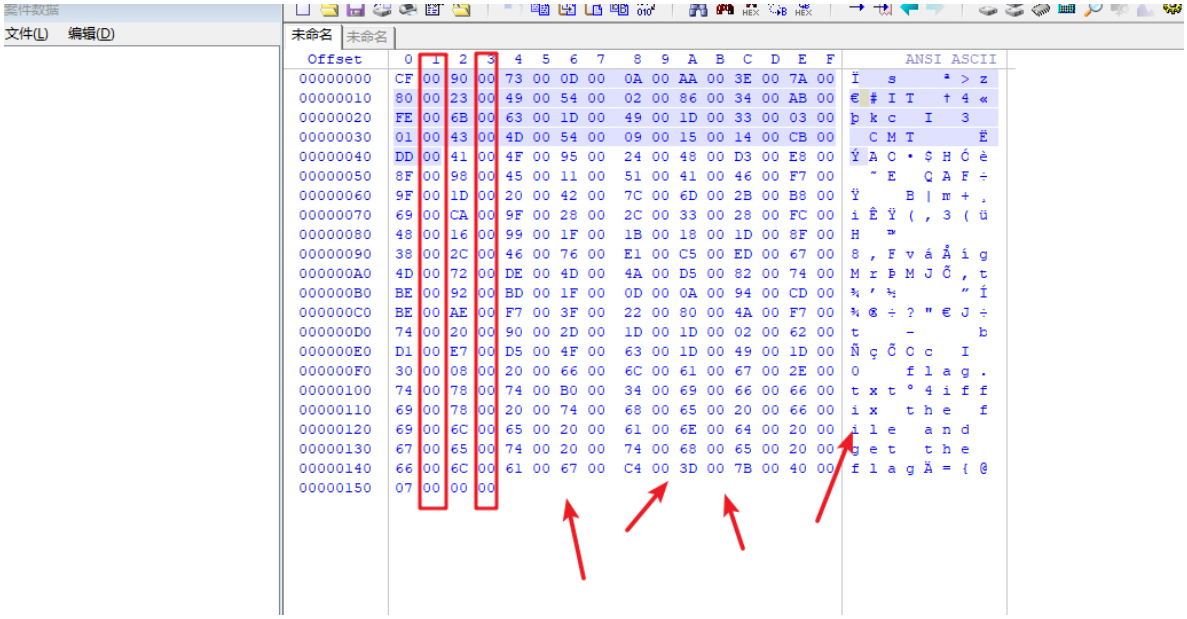
打开68个文件发现里面每个压缩包里都有一个四个字节大小的txt文档（加密），首先尝试下是不是**伪加密**，发现不是尝试下爆破无果。。。然后想了下，这么多压缩包，不可能让我们爆破吧，尝试下**crc32碰撞**

CRC32碰撞可以参考我写的文章zip压缩包--加密篇





分析里面得文件得四个字节，想着应该是英文，中文字符得话跟爆破没区别...
猜测里面为四个字符（英文），获取zip文件得crc32值，进行crc碰撞
碰撞出来发现是一串base64，拿去解密(有些网站解码不了，解码了也是有问题的，多尝试几个)，放入winhex，发现导入进去的时候老是有问题，我不知道怎么处理，莫名其妙的多了很多空格，搜索了下感觉他们很顺利的就放进去了



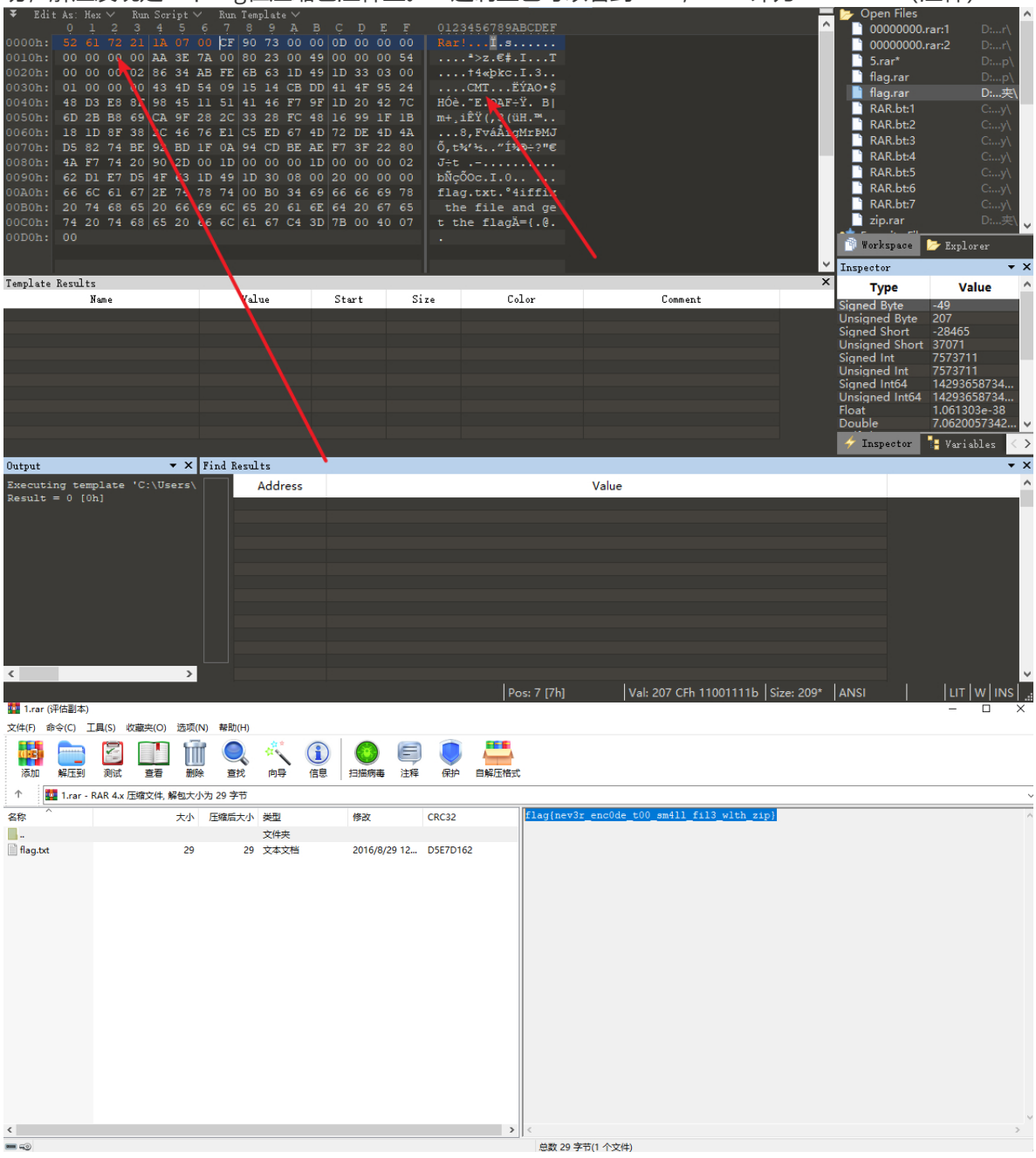
尝试多次发现无果。然后无奈就自己写python实现直接base64解密后直接写入文件里

python脚本：

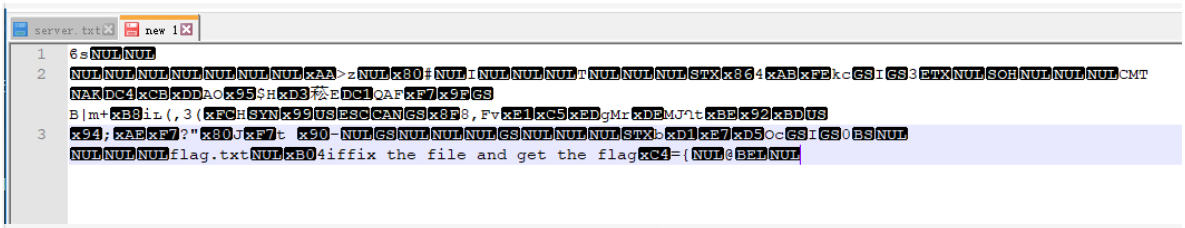
```
# coding:utf-8

import binascii
import string
import zipfile
import base64

dicts = string.printable  # 可打印字符的字符串。ascii码33-126号


def collision_crc(crc):
    global out_file
    for a in dicts:
        for b in dicts:
            for c in dicts:
                for d in dicts:
                    strings = a + b + c + d
                    strings = strings.encode('utf-8')
                    if crc == (binascii.crc32(strings)):
                        out_file.write(strings.decode('utf-8'))
                        # print(strings)
                        return
                        # 以上定义一个方法，组合随机字符与CRC进行碰撞，判断如果相等及写入文件


def obtain_zip():
    for i in range(68):
        file = 'out' + str(i) + '.zip'
        zip_file = zipfile.ZipFile(file, 'r')  # 读取创建zip_file对象
        get_crc = zip_file.getinfo('data.txt')  # 压缩文件夹里的data.txt文件，获取文档内指定的文件信息
        crc = get_crc.CRC
        #  以上定义一个方法，获取68个zip的CRC的值
        collision_crc(crc)  # 再调用collision方法传参
```

```
out_file = open('out.txt', 'w')
obtain_zip()
out_file.close()

out_file2 = open('out.txt', 'r')

with open('flag.rar', 'wb') as rar:
    rar.write(base64.b64decode(out_file2.read()))    # 二进制将转换后的base64位写入文件
```

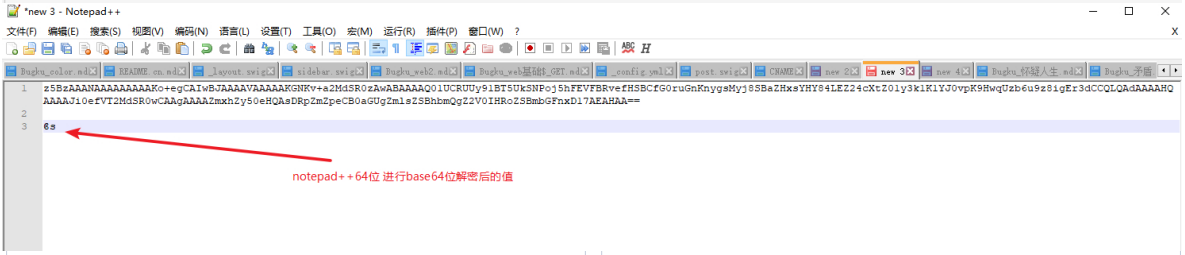
运行完成后将写出的文件，打开发现打开失败，导入16进制编辑器，观察数据，发现存在rar的文件尾C4 3D 7B 00 40 07 00，但缺少文件头，于是补上rar的文件头52 61 72 21 1A 07 00，发现文件修复成功，解压发现是一个flag在压缩包注释上。二进制上也可以看到CMT，CMT即为comment（注释）



这里说明下我之前base64导入进去的出现的问题，因为心里一直纳闷，所以去多次尝试发现需要利用notepad++32位的进行base64解密，就可以得到正确的值，保存为.rar文件，然后进行导入十六进制编辑工具里是可以实现的。（之前用的时notepad++64位的会出现解密不出来的情况，几个在线工具解密出来的值都是错误的或者跟上面导进去不知道为什么多了很多空格这些）这里举几个对比：



notepad++32位base64解密后的值



6s

z5BzAAANAAAAAAAAAKo+egCAIwBJAAAAVAAAAAKGNKv+a2MdSR0zAwABAAAAQ
01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfG0ruGnKnygsMyj8SBaZHxsYHY84LEZ24
cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0w
CAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZmlsZSBhbmQgZ2V0IHRoZSBmbG
FnxD17AEAHAA==

请将要加密或解密的内容复制到以下区域

Ï□s□□
□□□□□□□ª>z□□#□I□□□T□□□□□4«þkc□I□3□□□□□□CMT □□
ËÝAO□$HÓè□□E□QAF÷□□ B|m+¸iÊ□(,3(üH□□□□□□□8,FváÅígMrÞMJÕ□t¾□½□
□Í¾®÷?"□J÷t □-□□□□□□□□□□bÑçÕOc□I□0□□ □□□flag.txt□°4iffix the file and get the
flagÄ={□@□□

BASE64加密 BASE64解密