解题步骤：

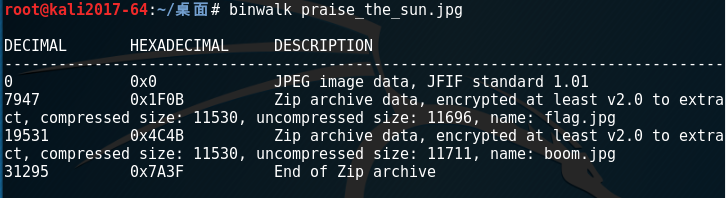
解压压缩包得到两个文件



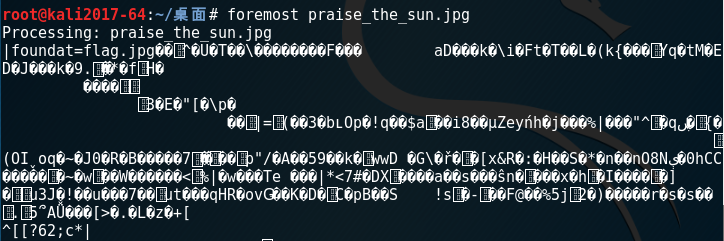
继续解压boom.zip得到boom.jpg图片文件



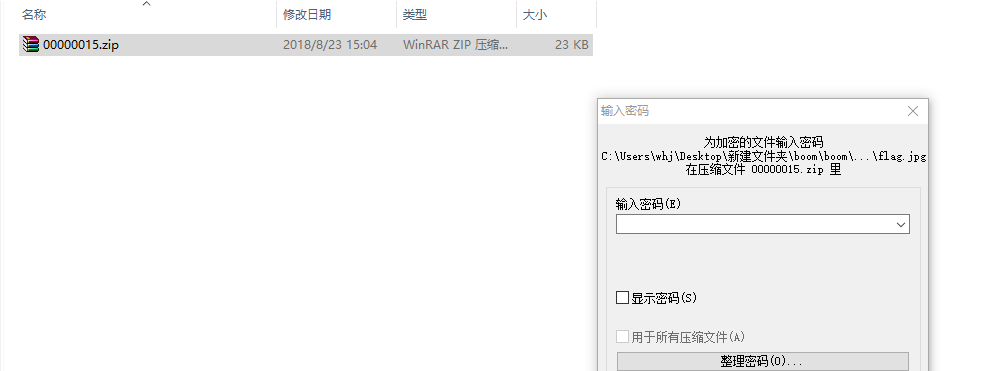
分析图片文件结构，发现压缩包



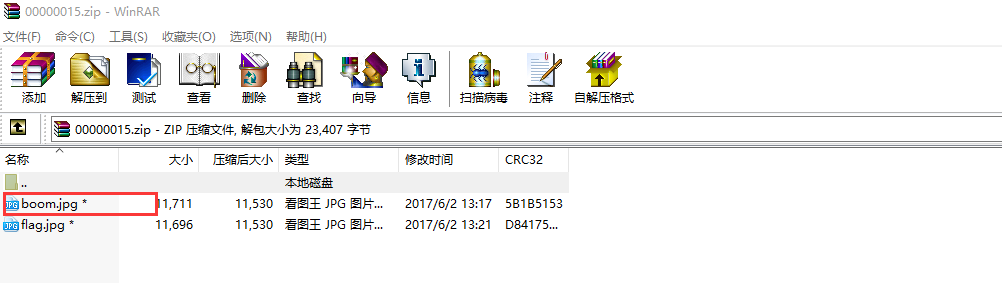
提取出来



解压，发现需要密码



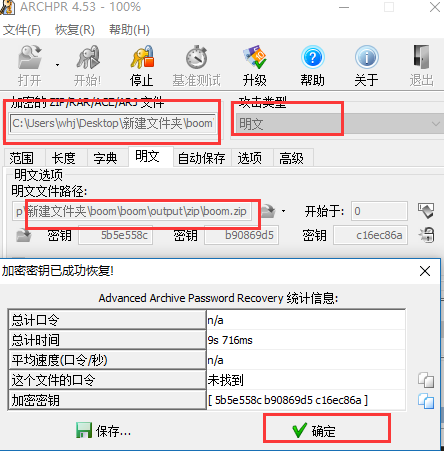
在压缩包里面发现boom.jpg文件



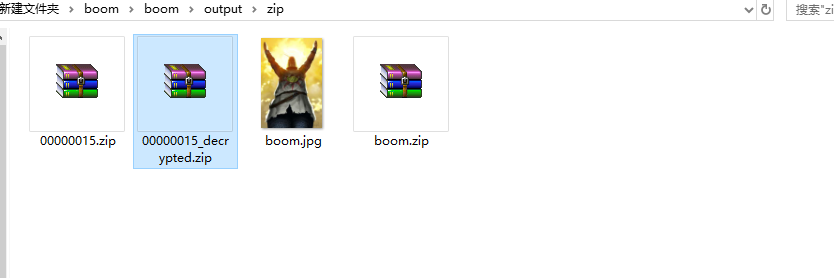
可以尝试明文攻击，将已知的明文文件添加为zip压缩包



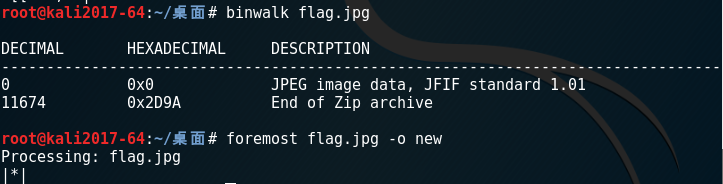
利用Advanced Archive Password Recovery进行明文攻击



得到新的decrypted压缩文件



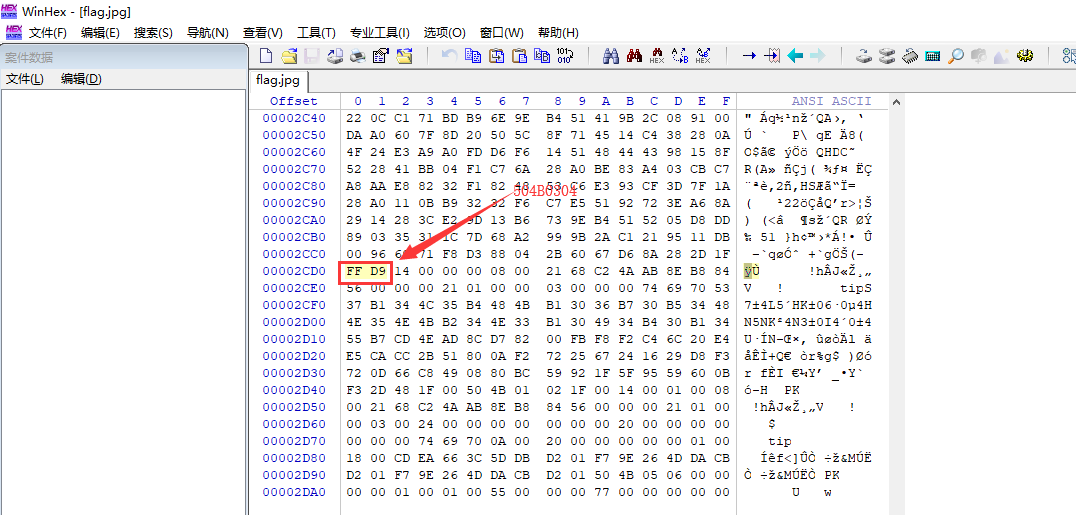
解压得到两张图片文件，对flag.jpg进行分析，发现压缩包并且提取



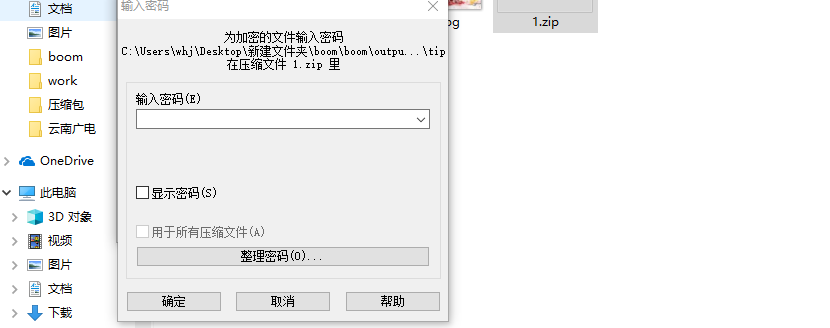
但是么有压缩包



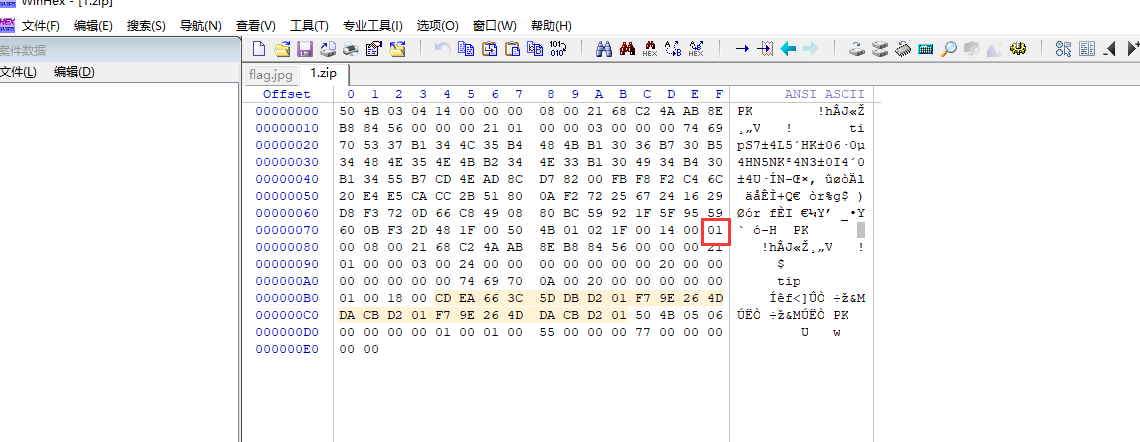
用winhex打开，发现压缩包文件头被破坏，添加文件头



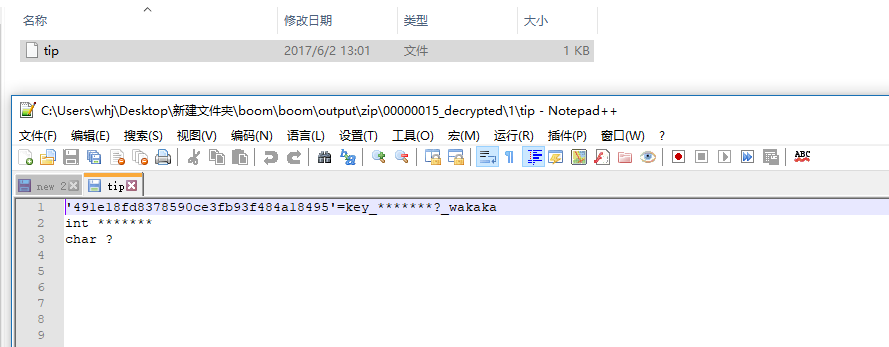
提取压缩文件，解压发现需要密码



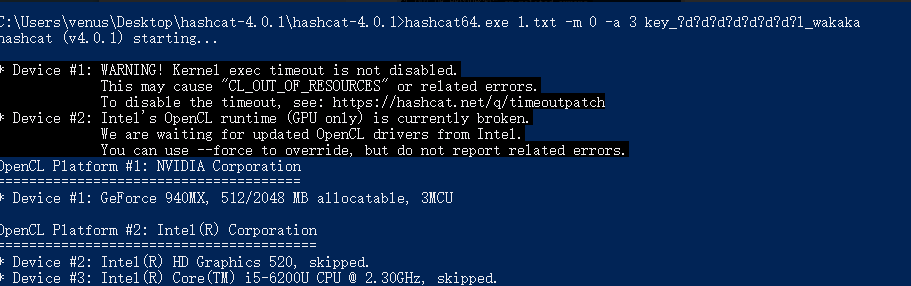
尝试修复伪加密，标志位改为基数改为偶数

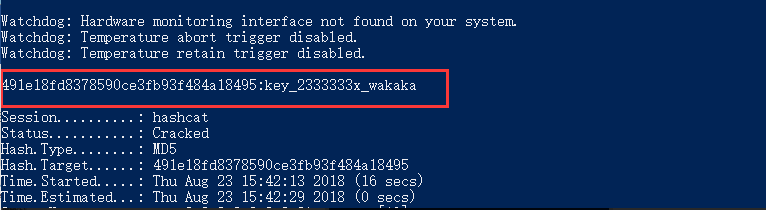


解伪加密后，解压德大tip文件



根据提示进行md5掩码攻击，可以用hashcat完成





得到最后的明文，即flag

也可以利用python脚本进行爆破，脚本如下

#'491e18fd8378590ce3fb93f484a18495'=key\_\*\*\*\*\*\*\*?\_wakaka

#int \*\*\*\*\*\*\*

#char ?

import hashlib

str\_src=list('key\_\*\*\*\*\*\*\*?\_wakaka')

str\_md5='491e18fd8378590ce3fb93f484a18495'

str1\_list=list('abcdefghijklmnopqrstuvwxyz')

str2\_list = list('0123456789')

for a in range(len(str2\_list)):

str\_src[4]=str2\_list[a]

for b in range(len(str2\_list)):

str\_src[5]=str2\_list[b]

for c in range(len(str2\_list)):

str\_src[6]=str2\_list[c]

for d in range(len(str2\_list)):

str\_src[7]=str2\_list[d]

for e in range(len(str2\_list)):

str\_src[8]=str2\_list[e]

for f in range(len(str2\_list)):

str\_src[9]=str2\_list[f]

for g in range(len(str2\_list)):

str\_src[10]=str2\_list[g]

for h in range(len(str1\_list)):

str\_src[11]=str1\_list[h]

stry\_md5=str(hashlib.md5(''.join(str\_src)).hexdigest())

if stry\_md5 == str\_md5:

print ''.join(str\_src),stry\_md5

