# 一、题目描述

题目链接：

https://buuoj.cn/challenges#[ACTF%E6%96%B0%E7%94%9F%E8%B5%9B2020]%E6%98%8E%E6%96%87%E6%94%BB%E5%87%BB

题目来源平台：buuctf

题目名称：[ACTF新生赛2020]明文攻击

题目描述：明文攻击

题目类型：MISC

题目附件：

FLAG：flag{3te9\_nbb\_ahh8}

# 二、解题工具

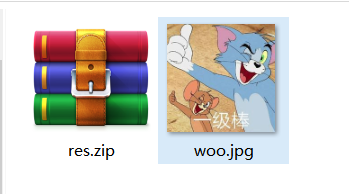
|  |  |  |  |
| --- | --- | --- | --- |
| 工具类型 | 工具名称 | 版本 | 备注 |
| 基础环境 | Windows | 10 |  |
|  |  |  |
| 工具 | Winhex | 19.6 |  |
| Winrar |  |  |
| ARHPR |  | 用来进行明文攻击 |
| 脚本 |  |  |  |
|  |  |  |
|  |  |  |

# 三、解题过程

（详细说明CTF赛题的解题过程，分步骤说明）

### 步骤1

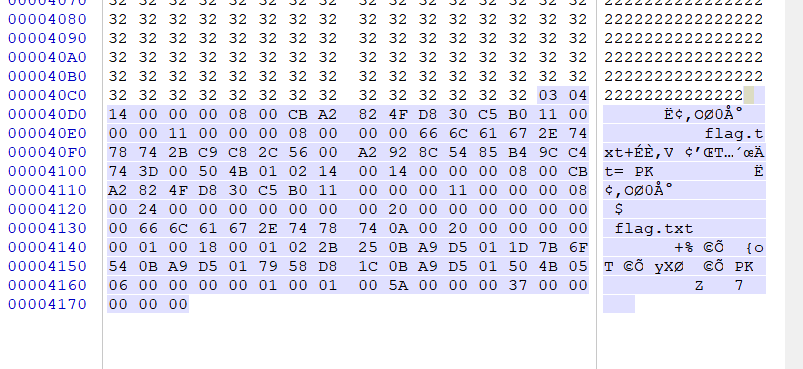
将得到的压缩包解压得到一个压缩包和一个图片



### 步骤2

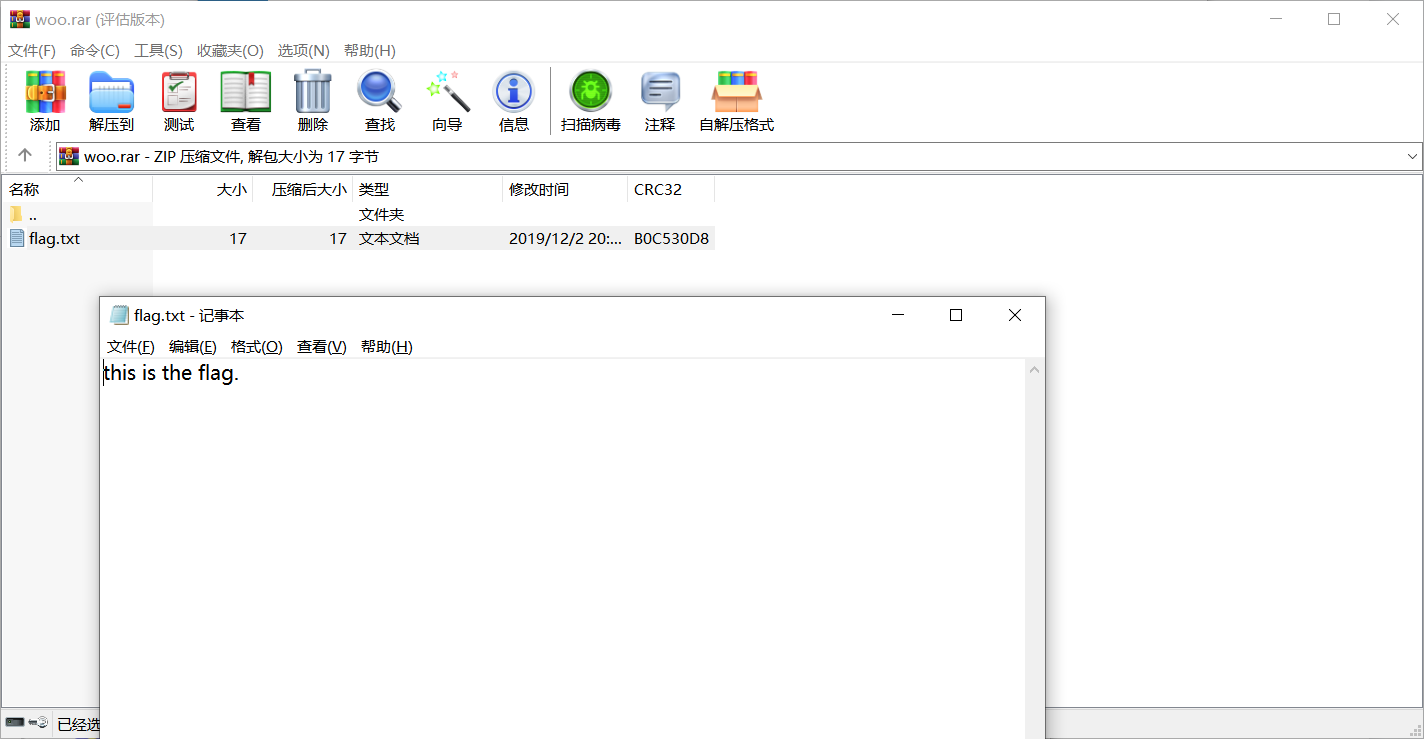
将图片抛进winhex里面

滑到最下面可以看到一个去掉部分文件头的压缩包，且命名为flag



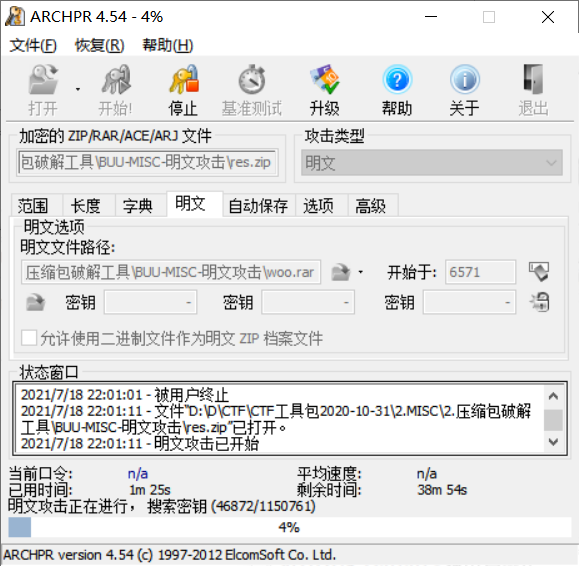
### 步骤3

对这一段字段进行处理，得到一个假的flag，但是该文件作为明文文件在后续会使用（由res.zip文件中包含同名称文本文件判断）



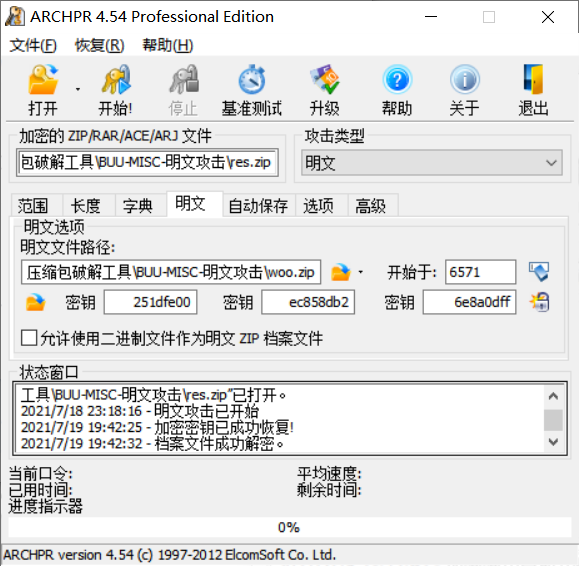
**步骤4**

题目给出的线索仍然是明文攻击，因此以上面这个文件作为明文文件，把两个文件放到ARCHPR中跑（明文文件后缀要改成zip，因为后面没截图所以没替换）。



### 步骤5

解密后得到：



打开档案文件得到flag：

