**题目名称：信工福尔摩斯**

**类型：Misc**

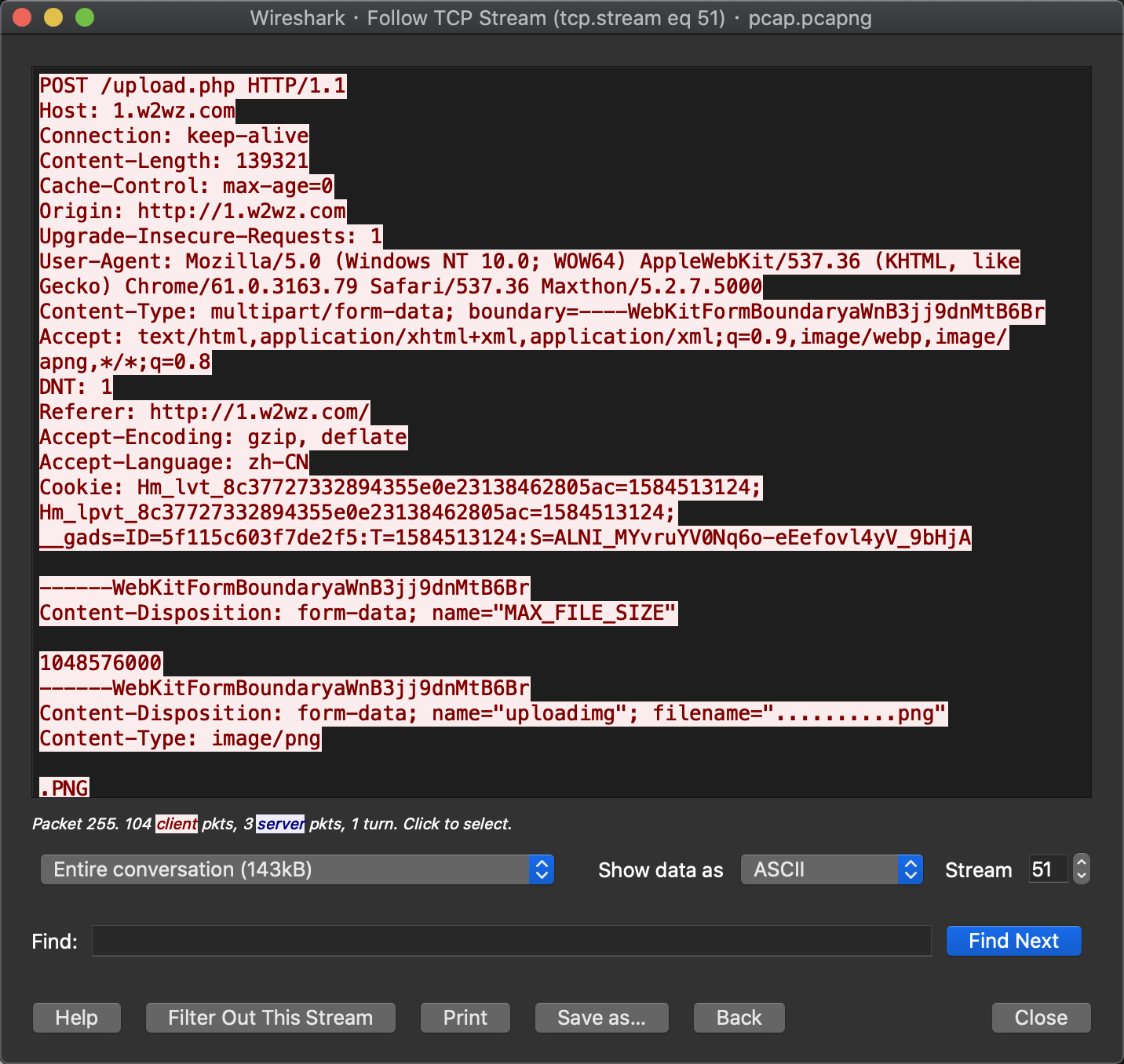
**介绍：**

本题为一个杂项的套娃题，杂糅了多个杂项的考点。

**解题步骤：**

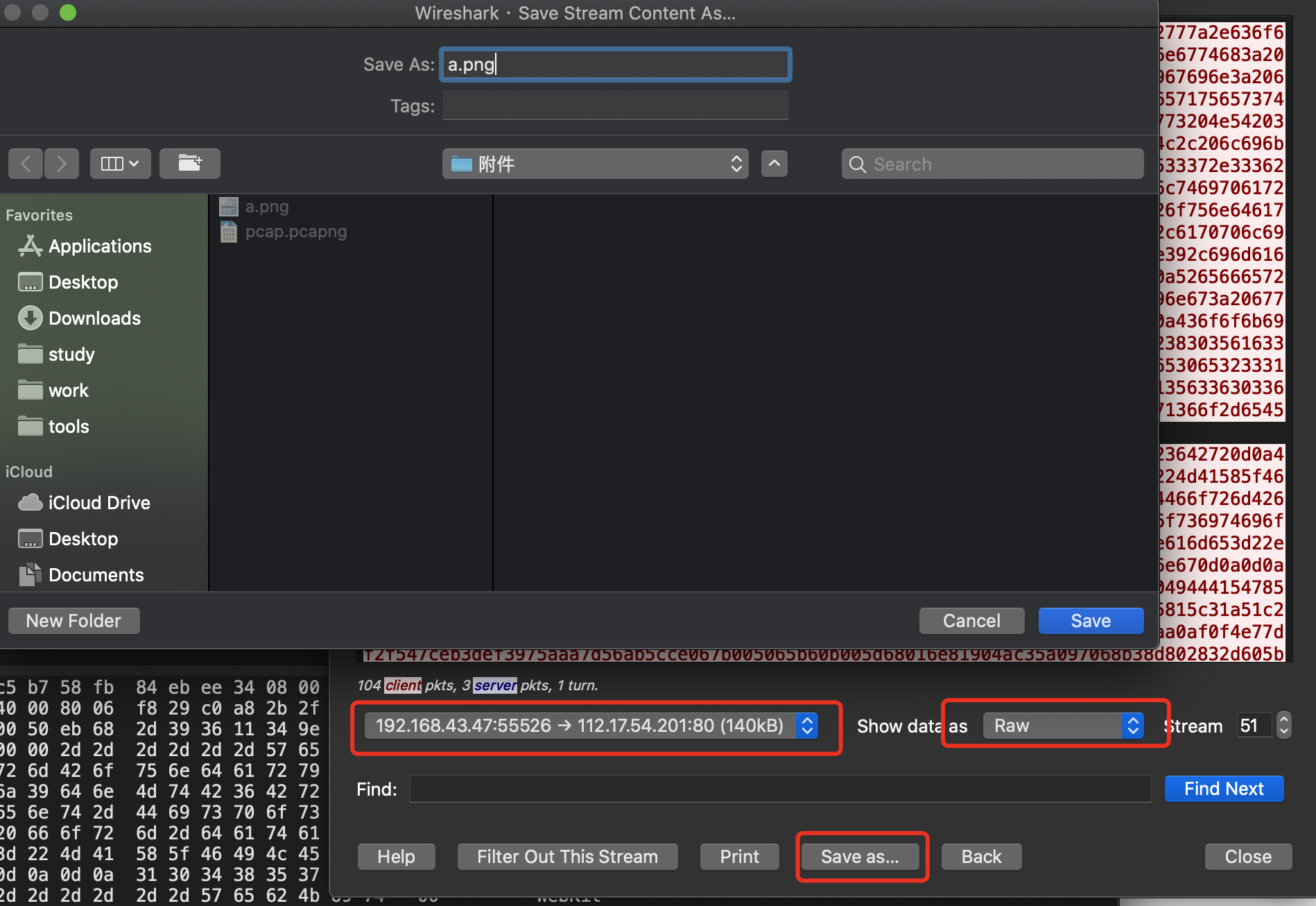
**第一步：**wireshark打开流量包

发现可疑的点在于upload.php，追踪流量。

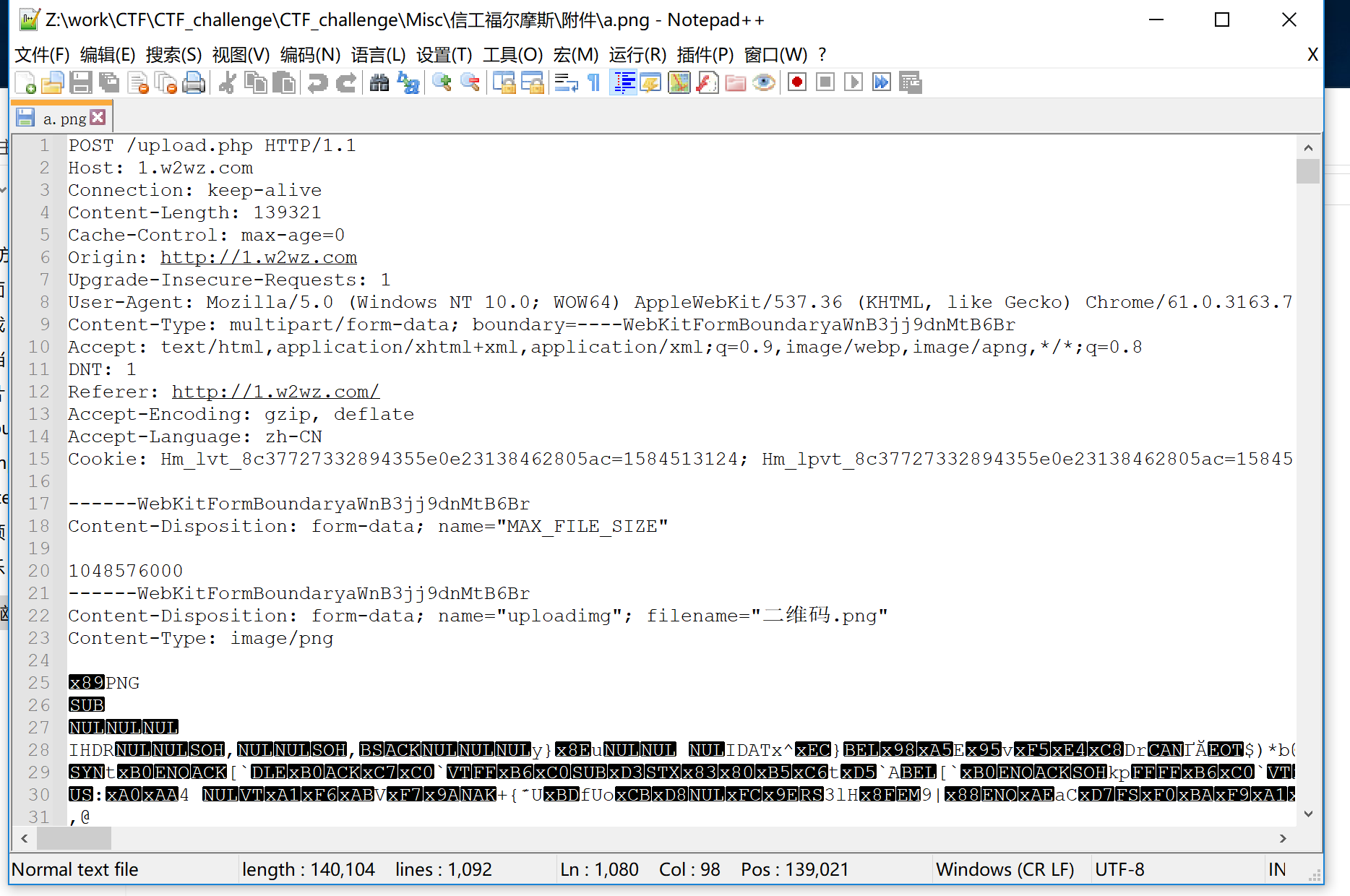


请求包中上传了一张图片

以原始数据raw形式查看保存



**第二步：**使用notepad++或者其他文本编辑恢复图片（注意很多文本编辑软件会有编码问题）



删除非png内容



成功拿到上传的图片。这个扫码可以扫但是没有意义～因为你把二维码恢复成可以扫的形式也不会给flag的。

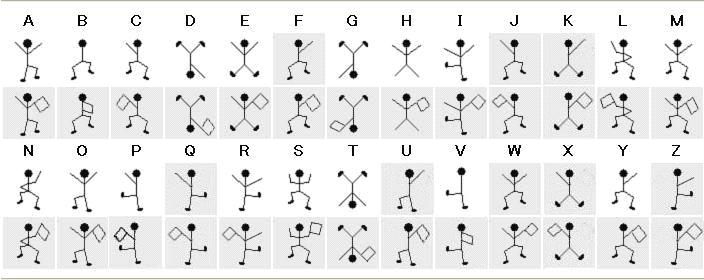
**第三步：**binwalk分析

直接binwalk -e 暴力拆分



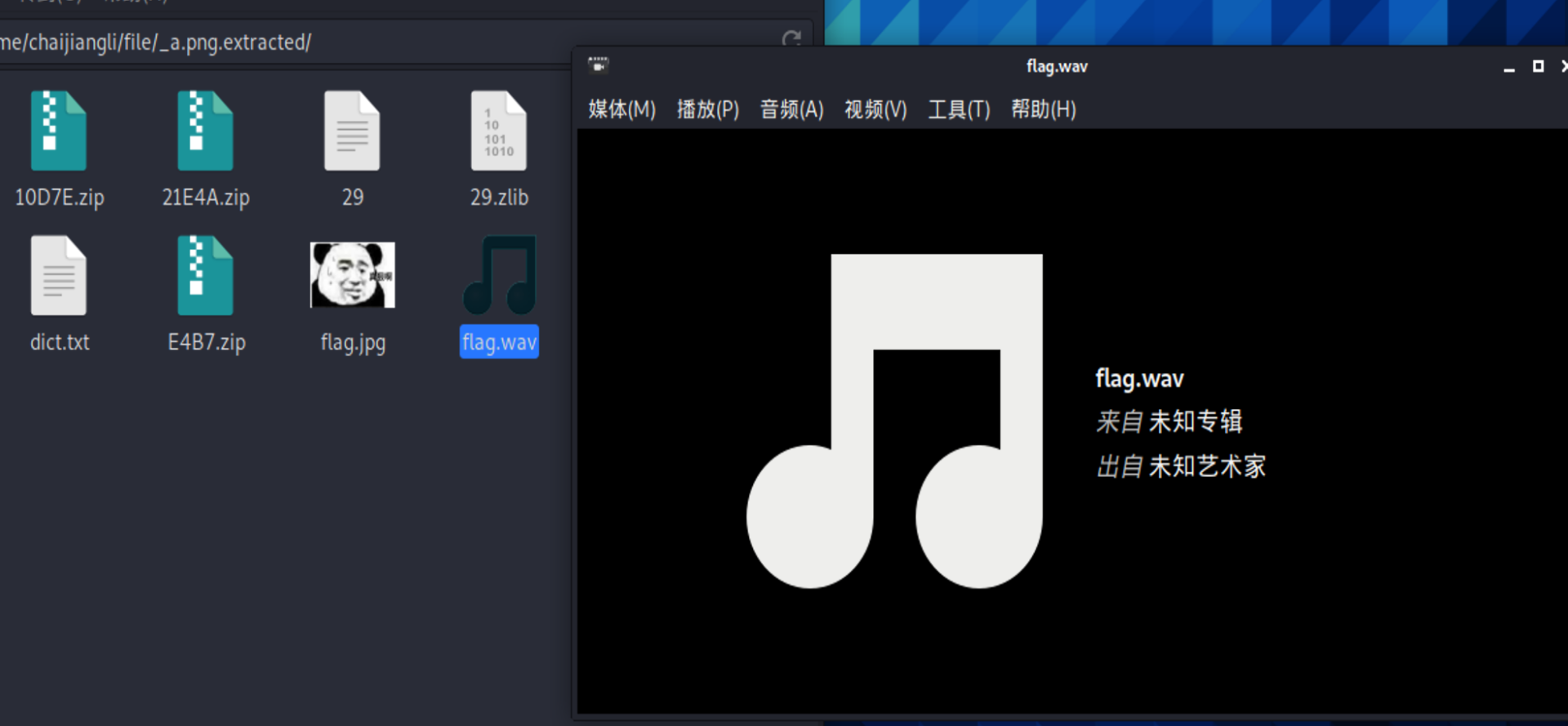
**第四步：**分析得到存在flag.wav被加密压缩了，还有舞动的小人密码，猜测舞动的小人解密即为压缩包密码





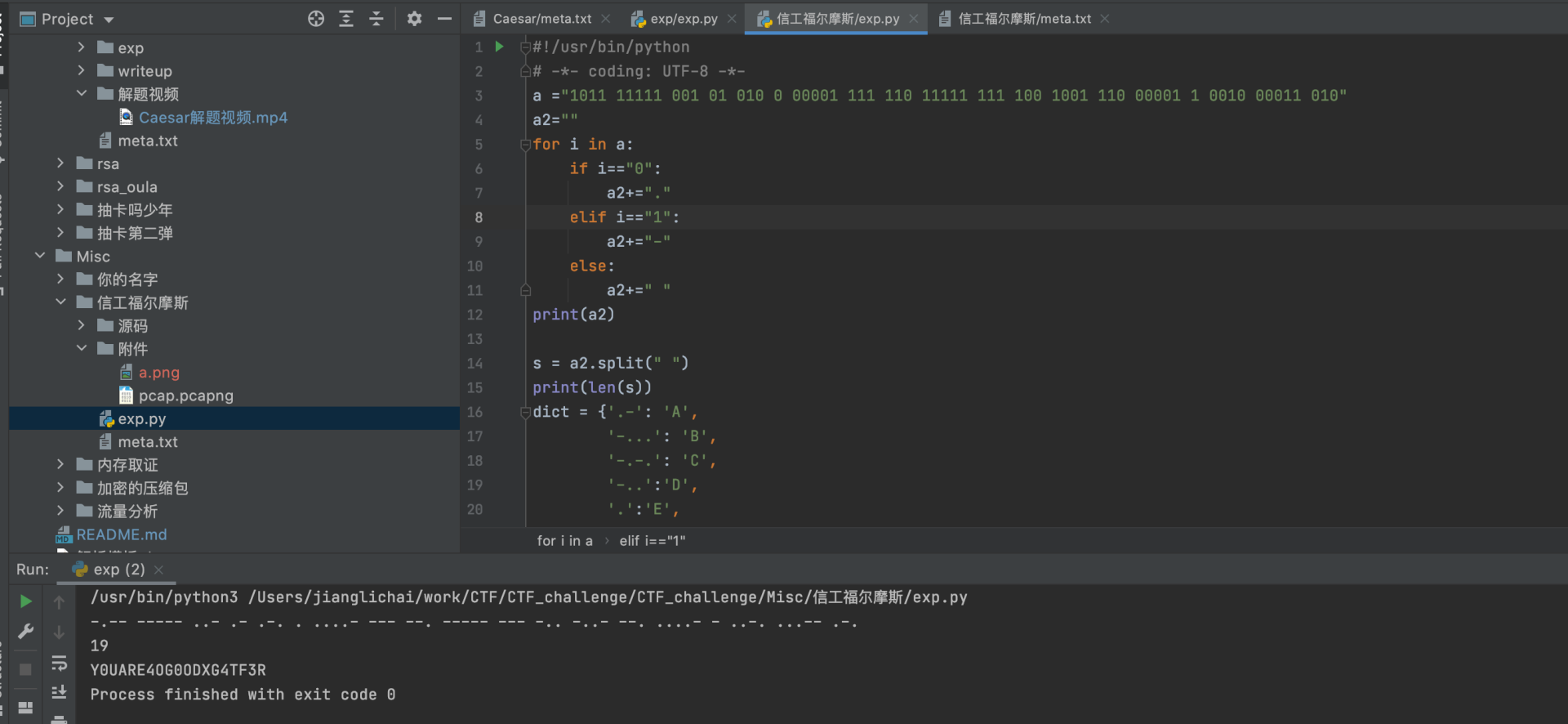
舞动的小人解密为YOUARESOGOOD

**第五步：**解压缩包得到flag.wav



音频为摩斯电码。

**第六步：**解摩斯电码得到flag



**简要总结：**了解如何从流量包提取文件、文件分析、舞动的小人加密、摩斯电码。