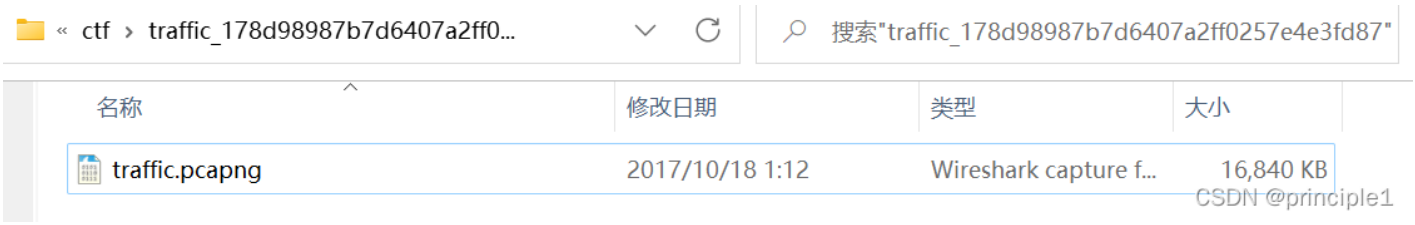
第三届上海市大学生网络安全大赛 流量分析

原创

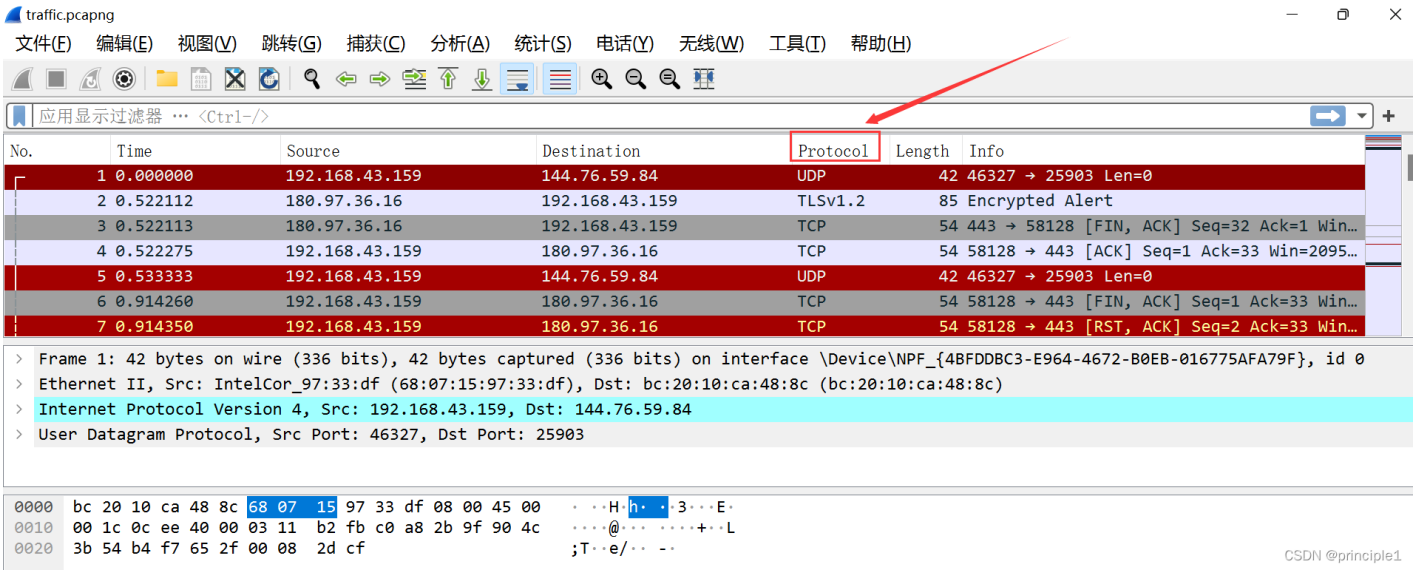
principle1 于 2021-12-28 12:26:39 发布 2412 收藏
文章标签： web安全 安全

关于这个writeup是写给初学者的，重点在于如何利用工具。

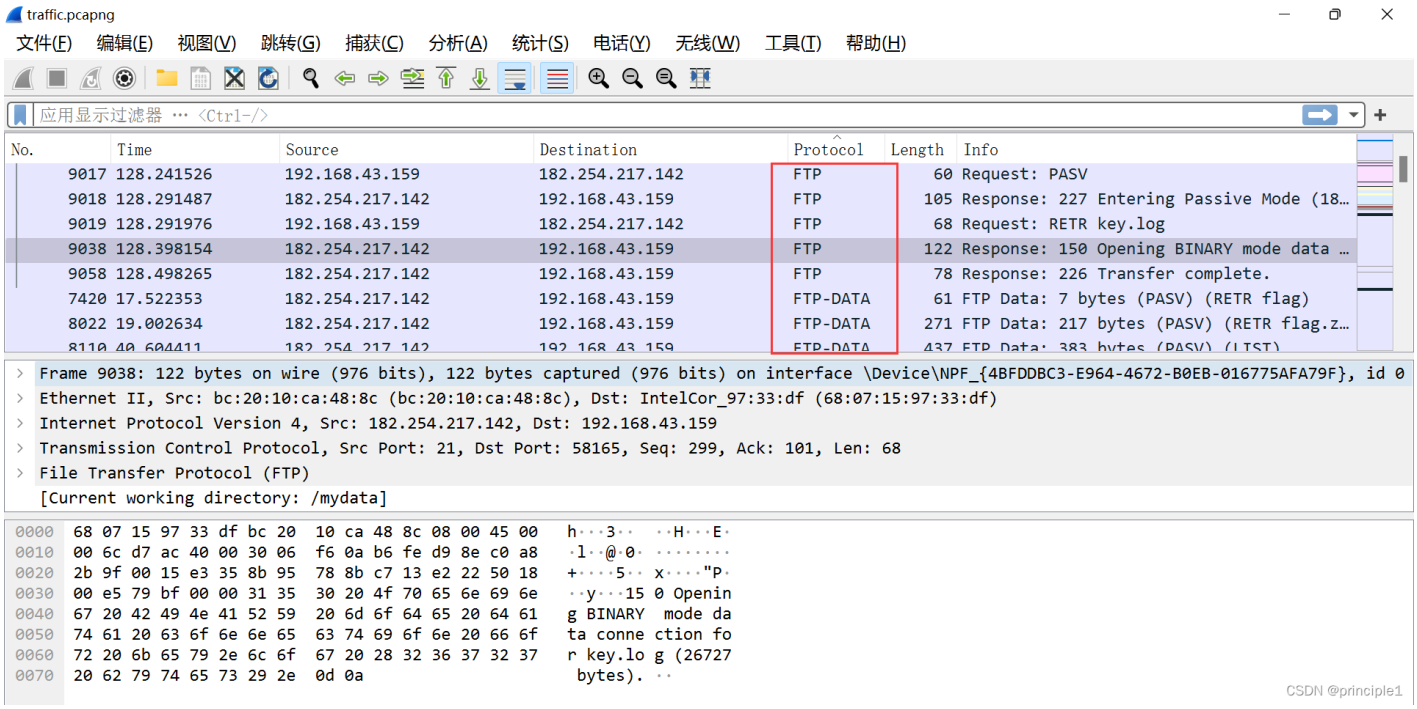
该题目下载文件打开后是一个抓包文件



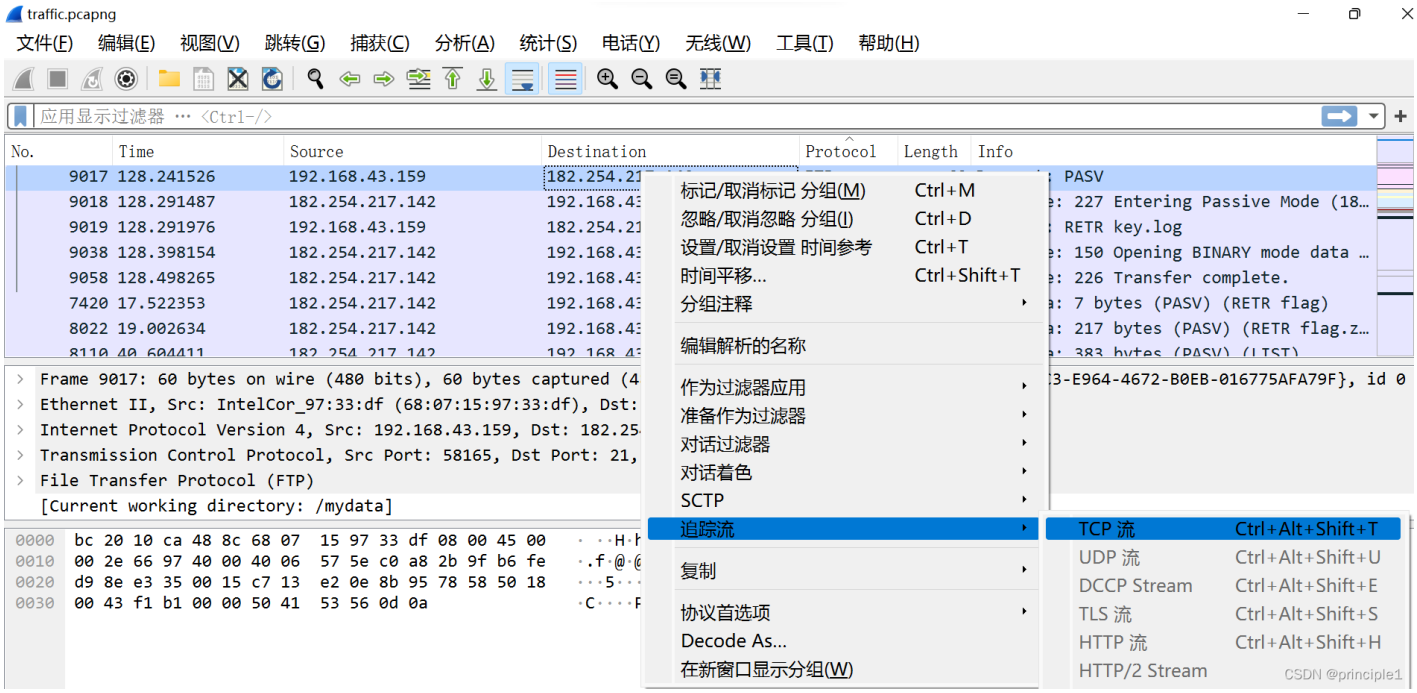
使用wireshark打开 ，wireshark下载地址：Wireshark - Download (softonic.com)

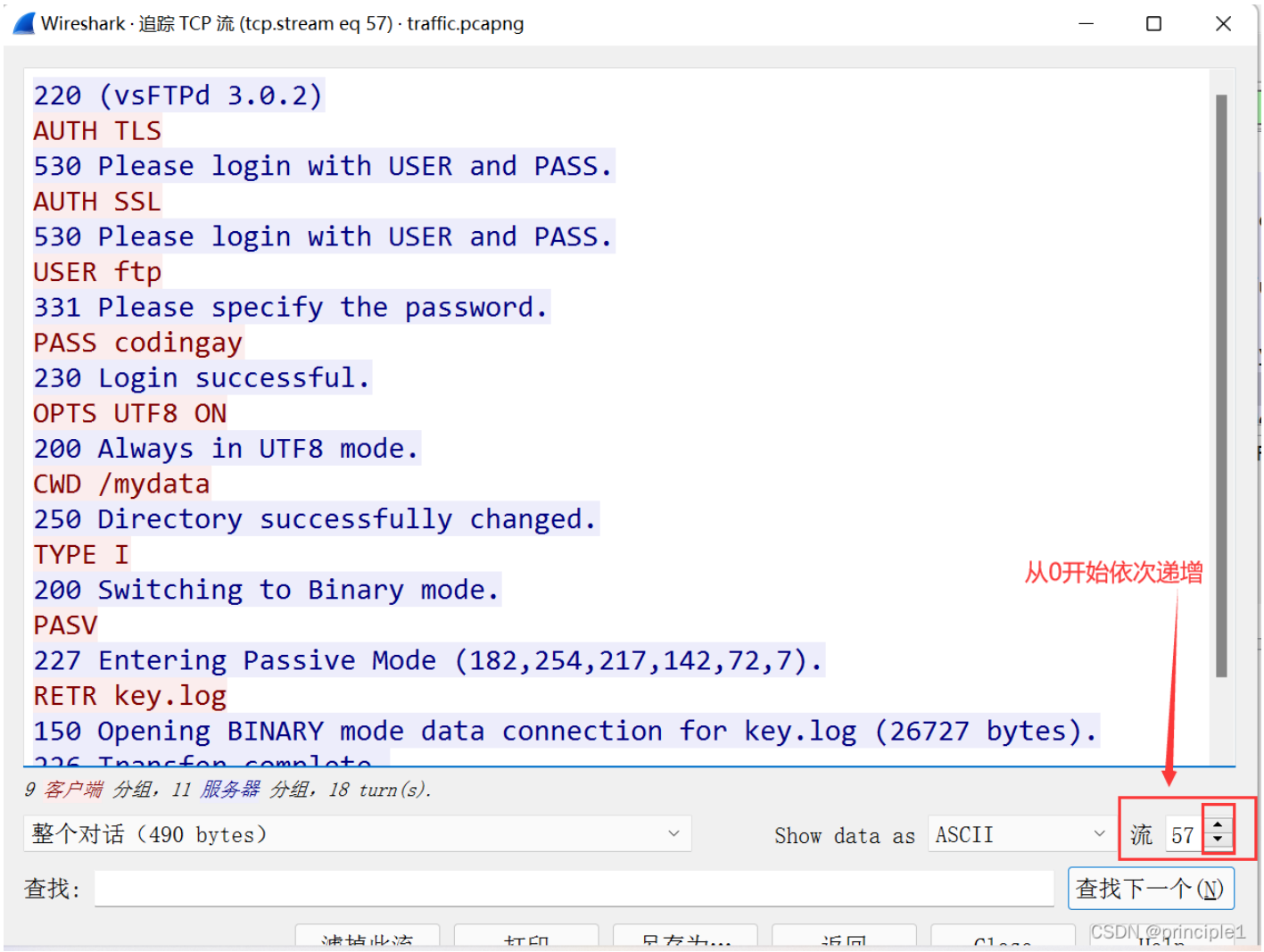


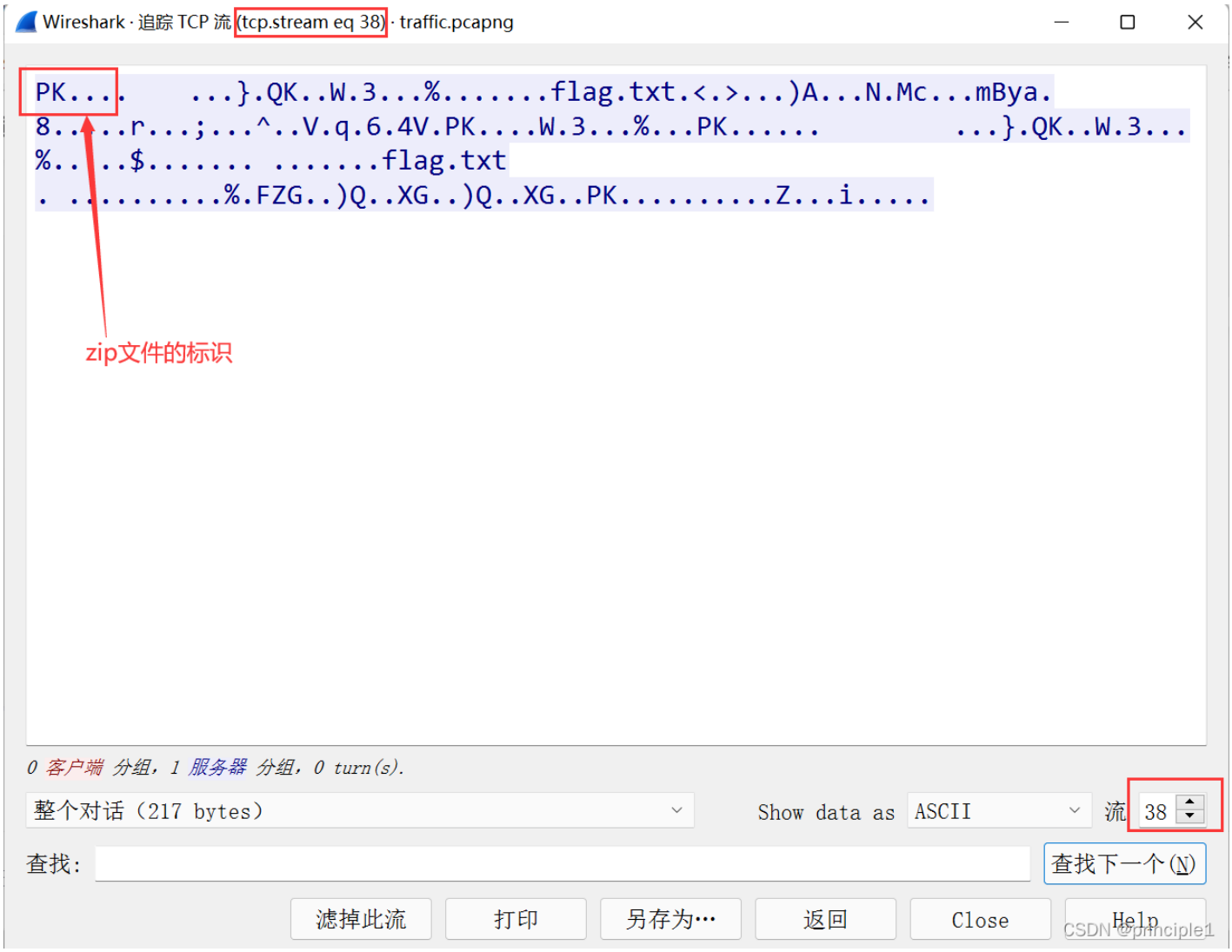
点击Protocol后，会对协议的名称按字母排序，可以初略看一下使用了哪些协议



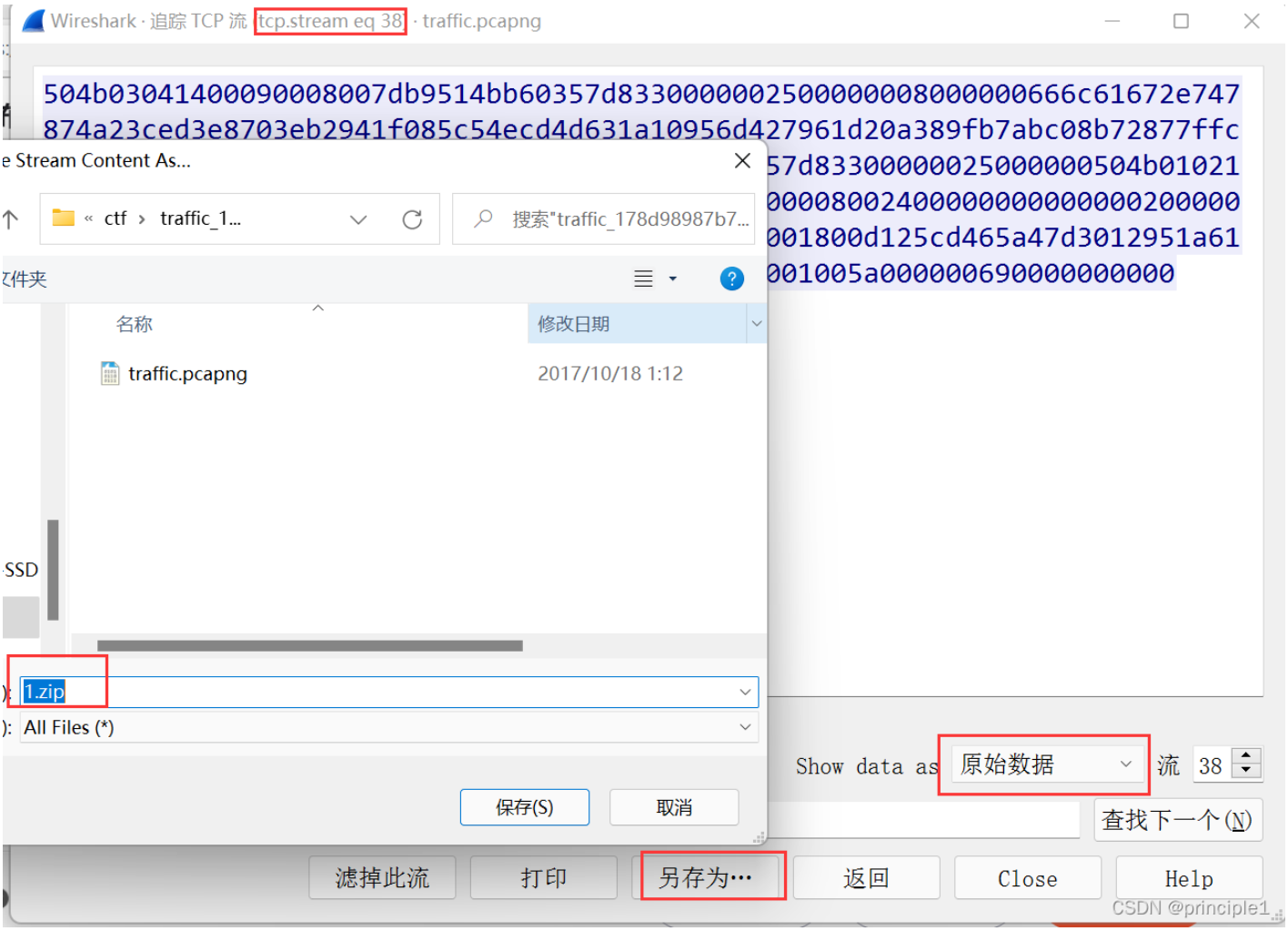
ftp协议用于文件传输，可以点击 右键 -> 追踪流 -> TCP流




Wireshark · 追踪 TCP 流 (tcp.stream eq 57) · traffic.pcapng
220 (vsFTPd 3.0.2)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER ftp
331 Please specify the password.
PASS codingay
230 Login successful.
OPTS UTF8 ON
200 Always in UTF8 mode.
CWD /mydata
250 Directory successfully changed.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (182,254,217,142,72,7).
RETR key.log
150 Opening BINARY mode data connection for key.log (26727 bytes).
从0开始依次递增
9 客户端 分组，11 服务器 分组，18 turn(s).
整个对话（490 bytes）
Show data as
ASCII
流
57
查找:
查找下一个(N)
CSDN @principle1

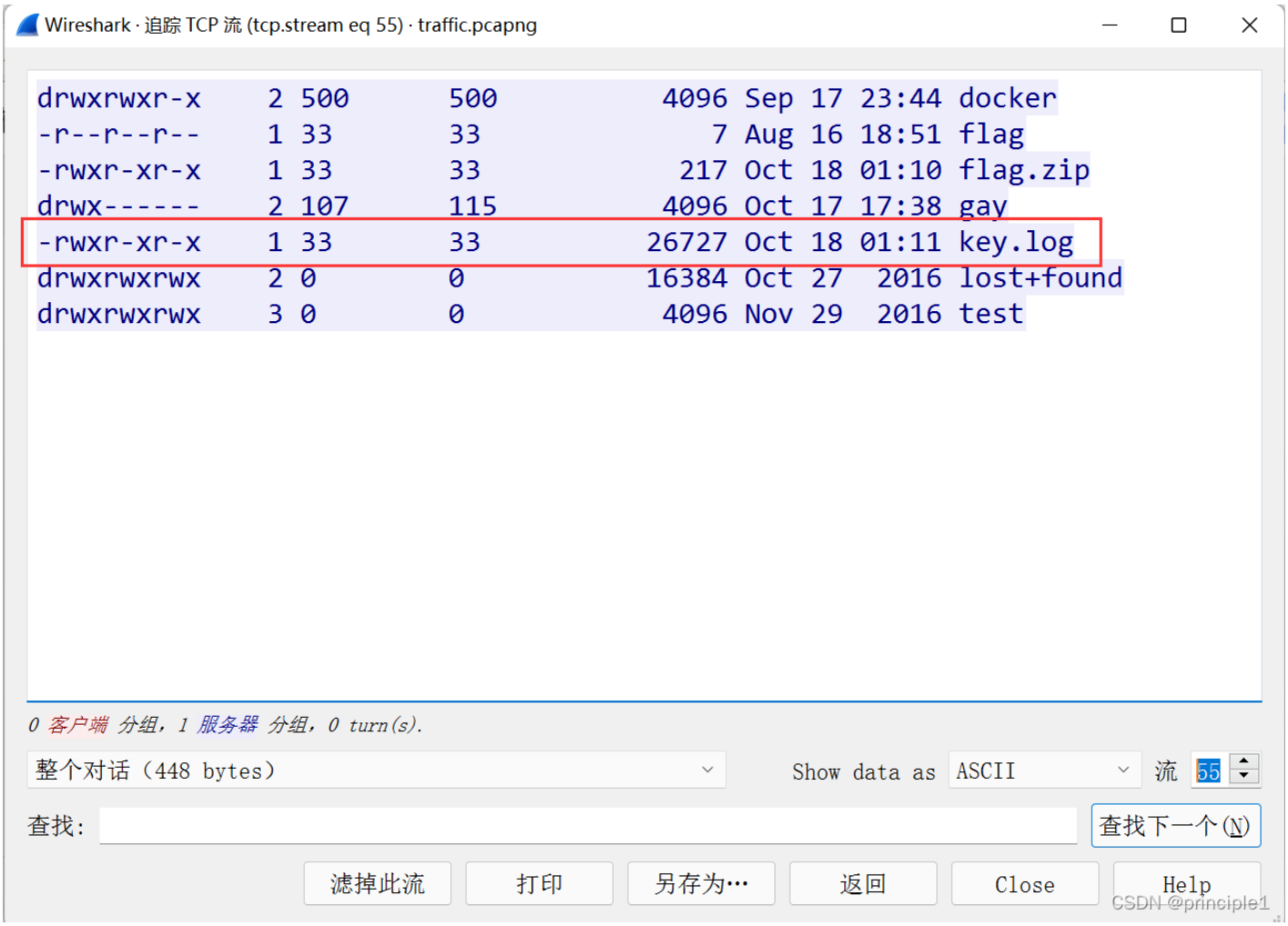


把 ‘Show data as’ 的值修改为 ‘原始数据’ 后，保存该zip文件为1.zip

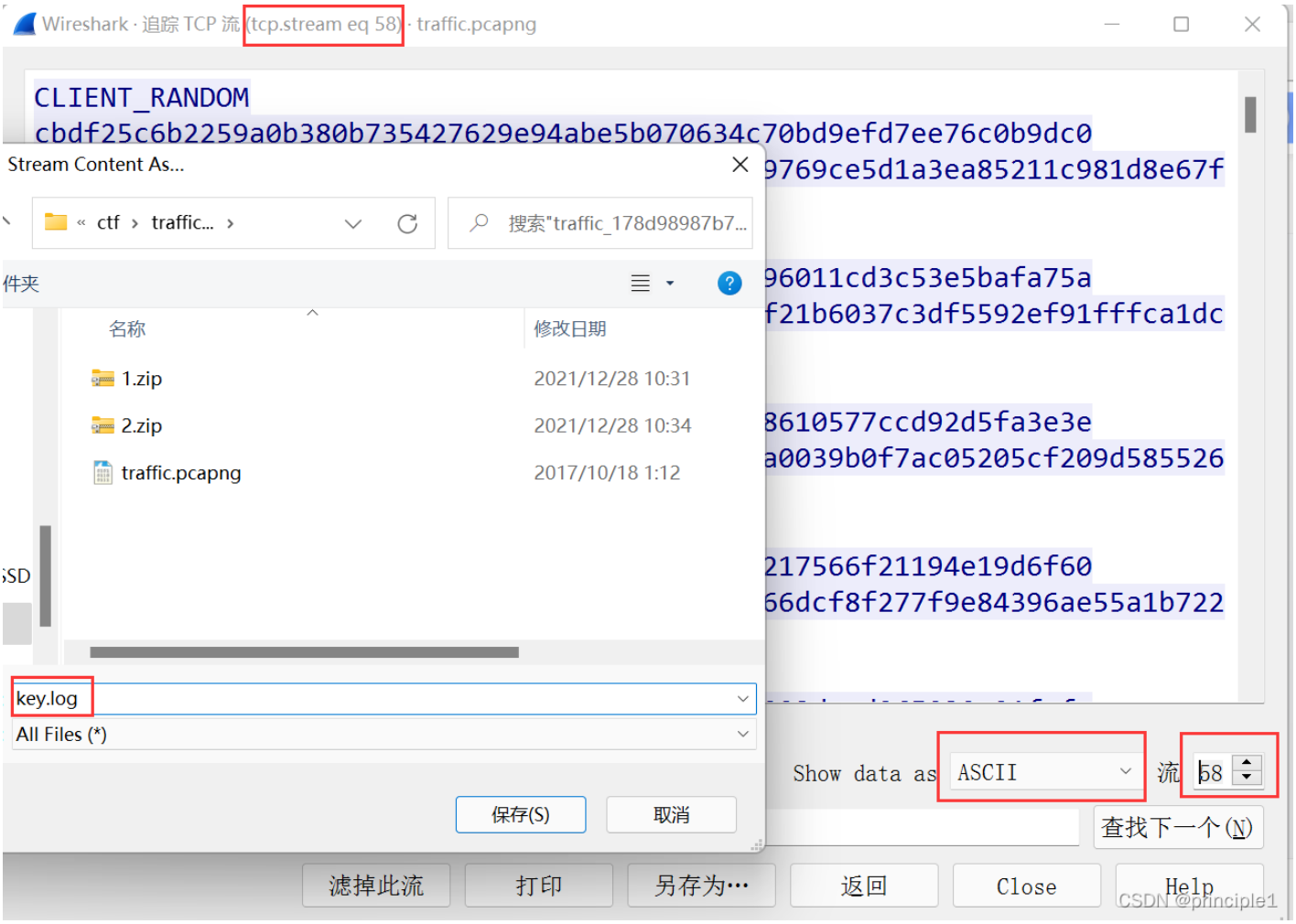


继续往后翻tcp流可以发现还有一个zip文件，按照同样的方式下载下来保存为2.zip

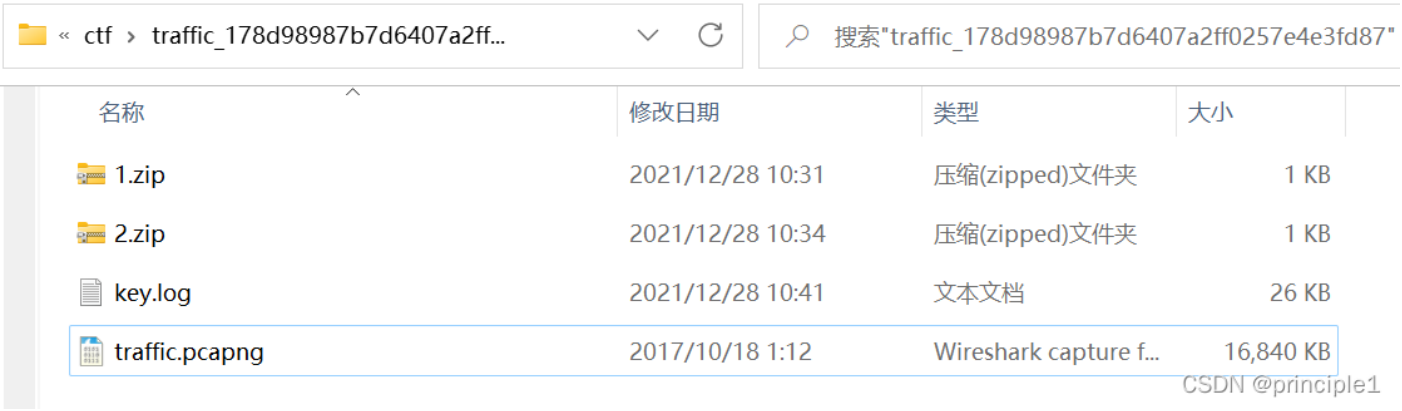
往下翻，可以看到还有一个key.log的文件，该文件能解密出wireshark里面的https的数据流，找到该文件并下载下来



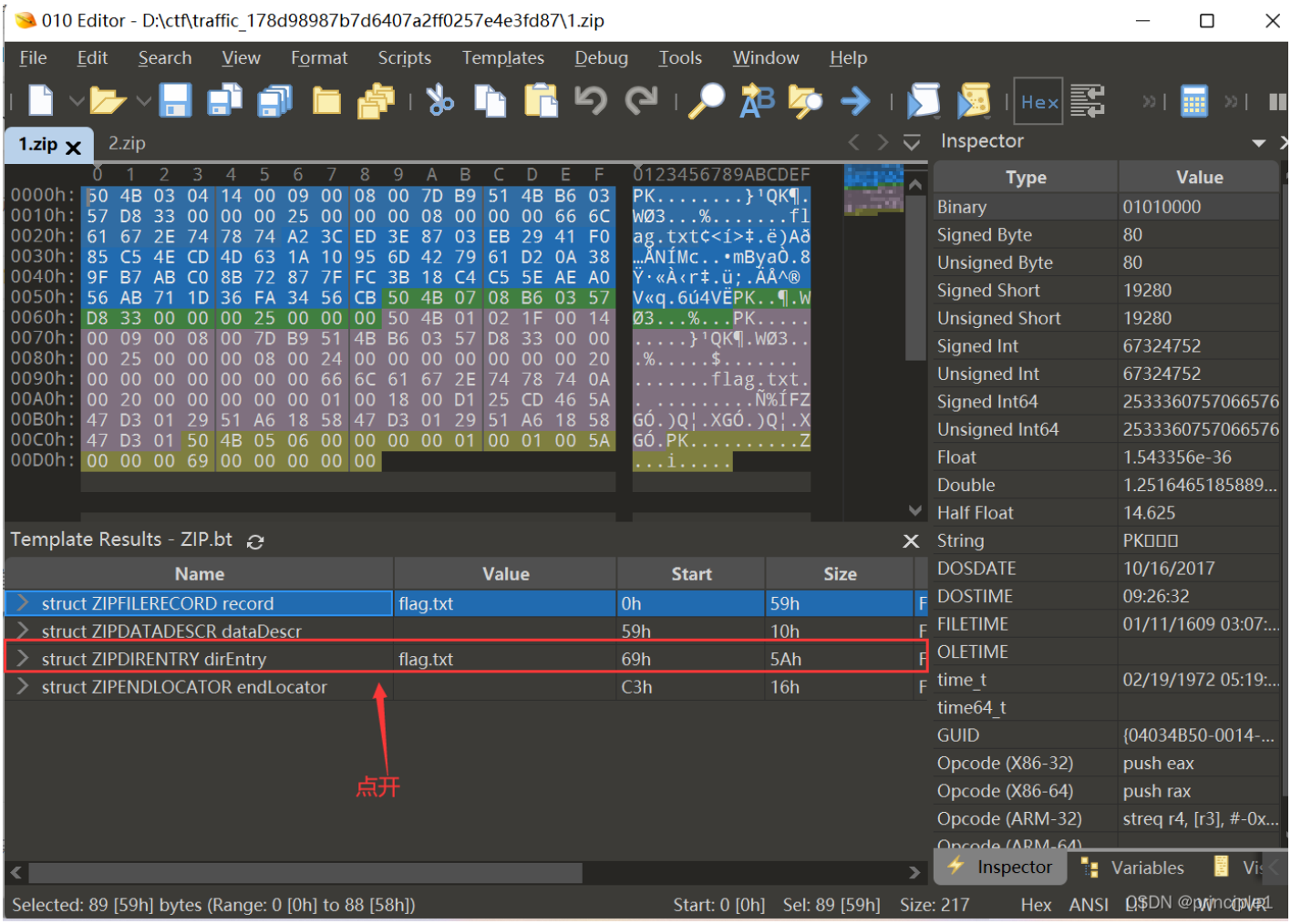
找到key.log后直接下载



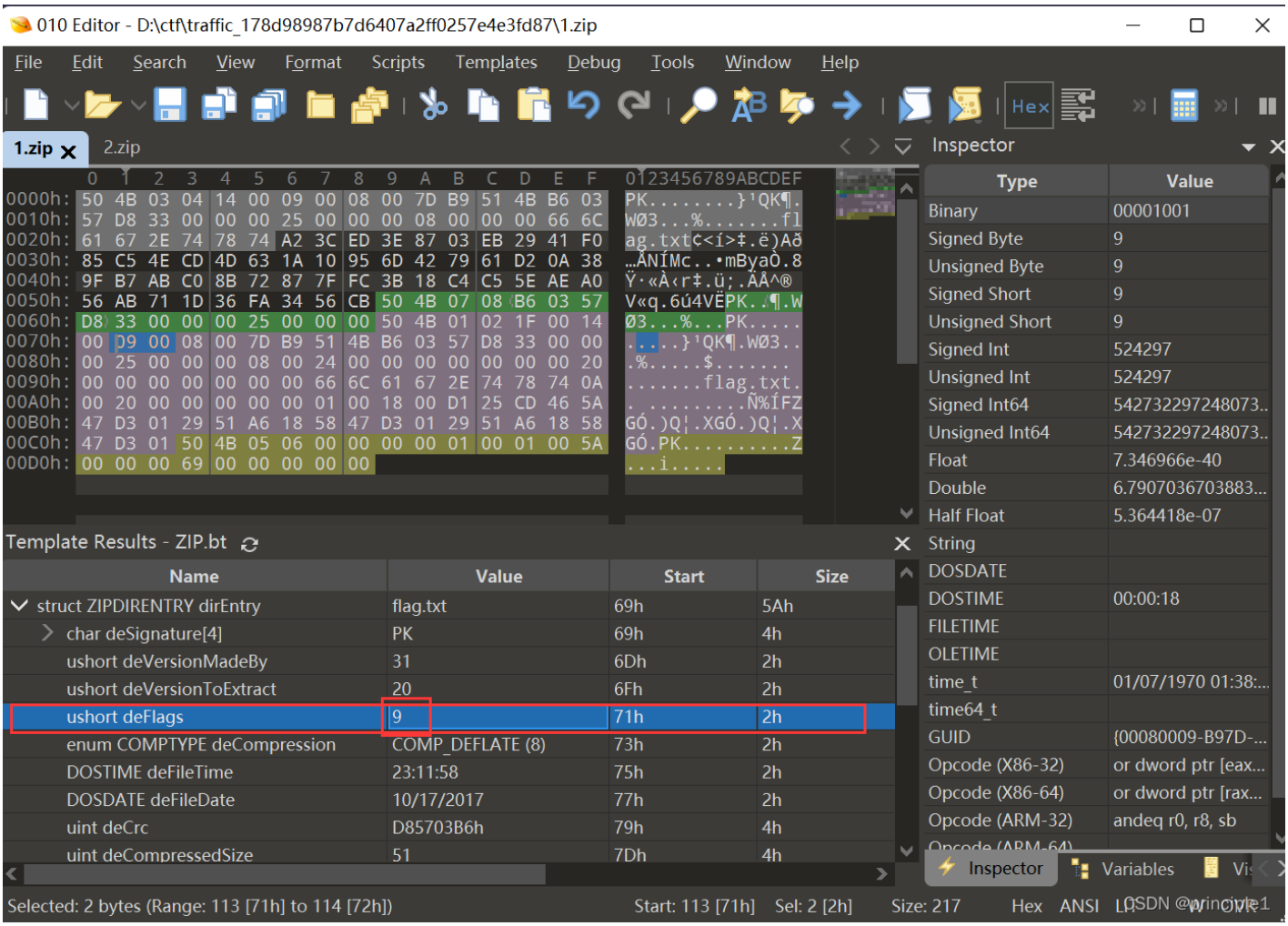
现在我们下载了两个zip文件和一个key.log文件，解压发现zip文件被加密了



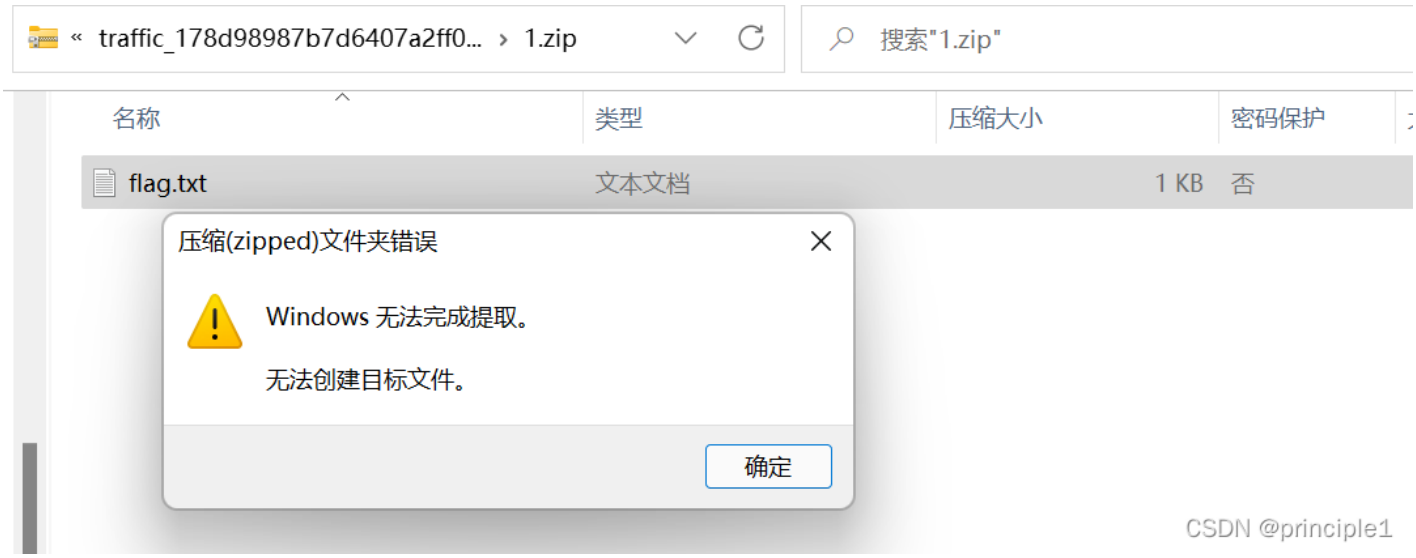
首先考虑是否是zip伪加密，用010editor打开文件，010editorde1的下载链接（SweetScape Software Inc - Download 010 Editor），破解文件使用的是脚本之家里面的（下载时并没有发现捆绑文件，下载后时一个zip文件，不用解压直接提取破解文件后删除zip文件就行）



ushort deFlags这个字段与zip伪加密有关，奇数为加密，偶数为没有加密，尝试把9改为0，保存后打开zip文件查看是否已经解密，若出现错误，记得把0改回来之后再保存文件，否则文件破坏后无法解题。

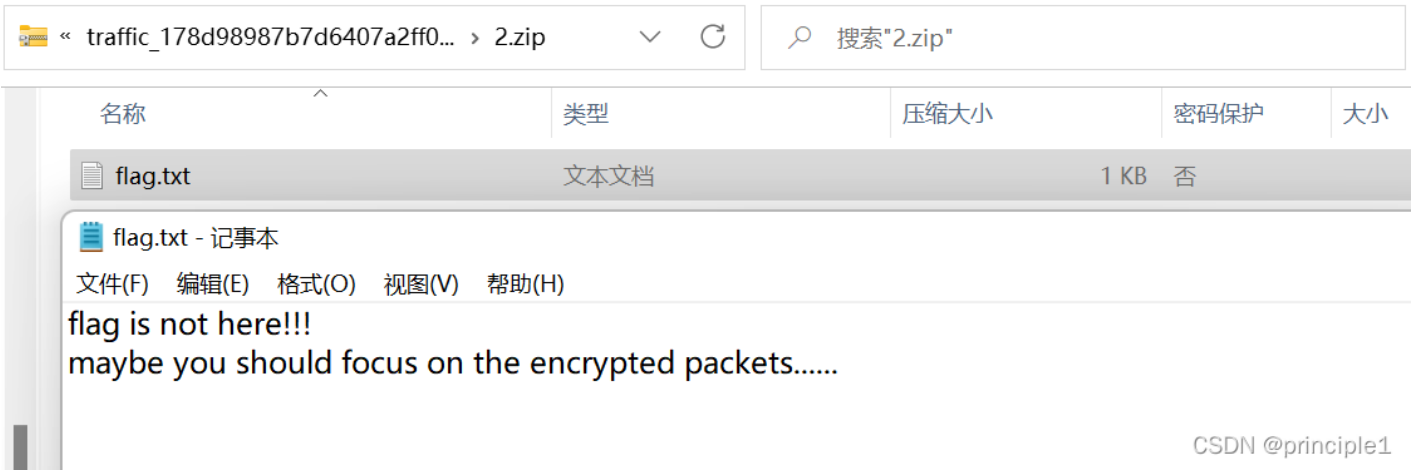


1.zip



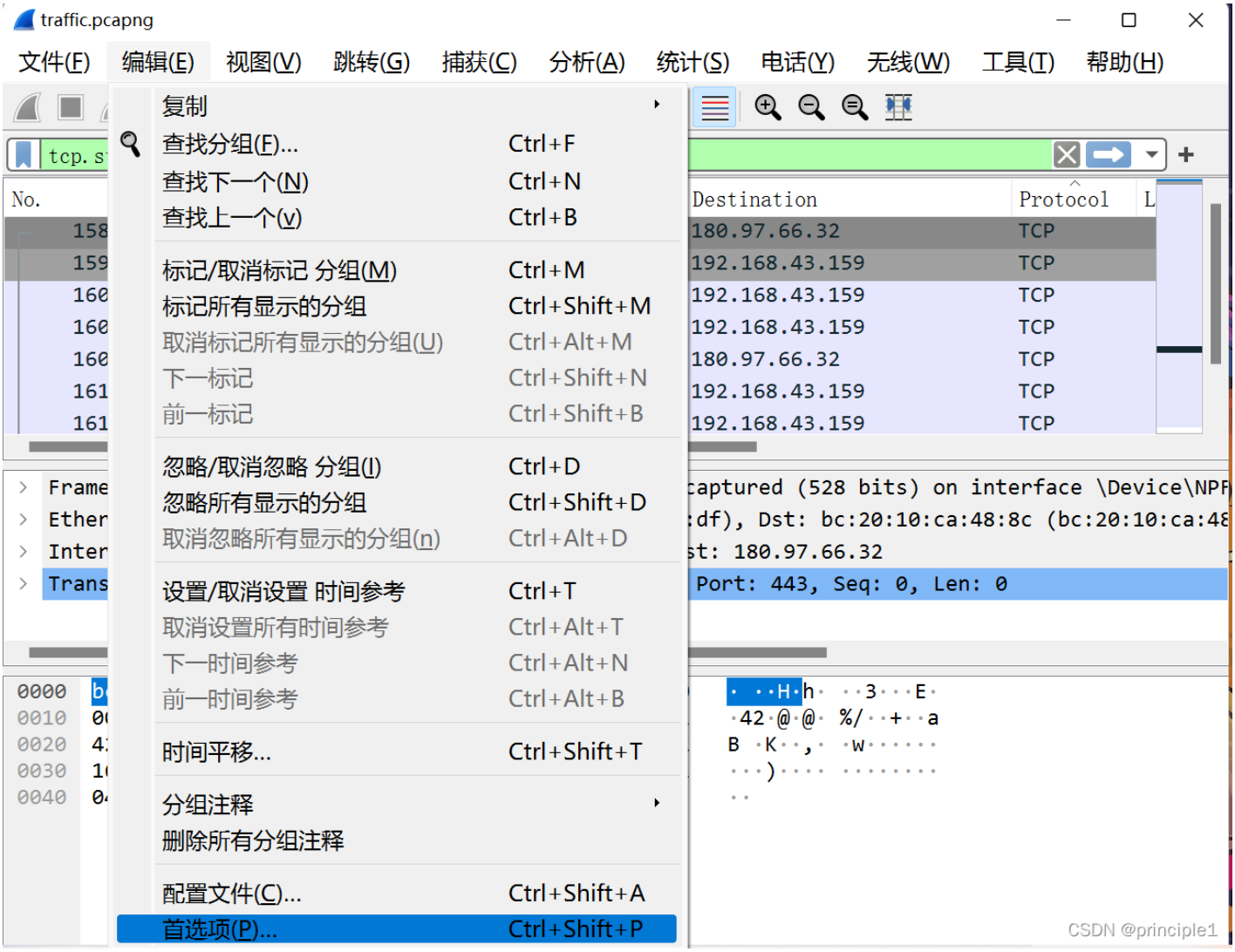
说明1.zip文件不是伪加密，记得把0改成9，还原文件

2.zip



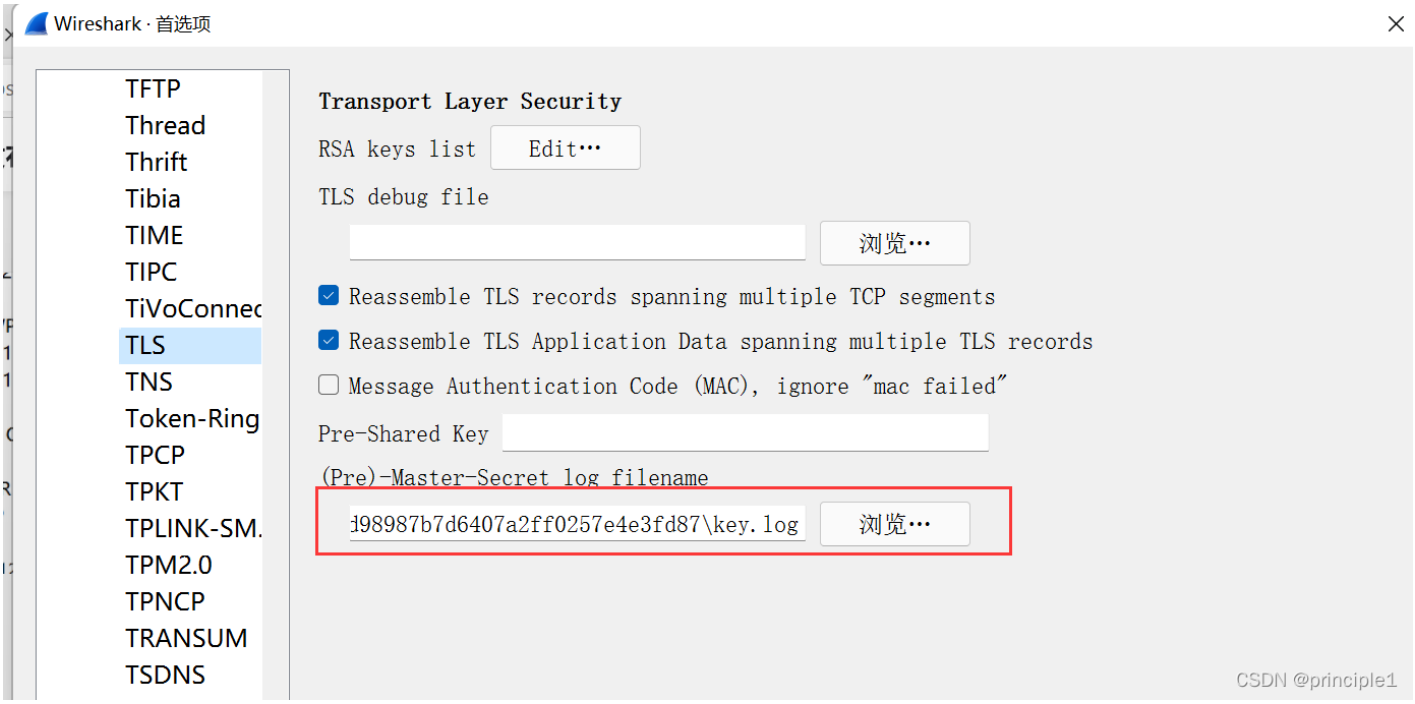
说明 2.zip是伪加密文件，但是该flag.txt中没有flag，然而有提示关注加密包，我们还有一个key.log文件，可以导入wireshark解密https的数据流

打开wireshark，依次点击 编辑->首选项

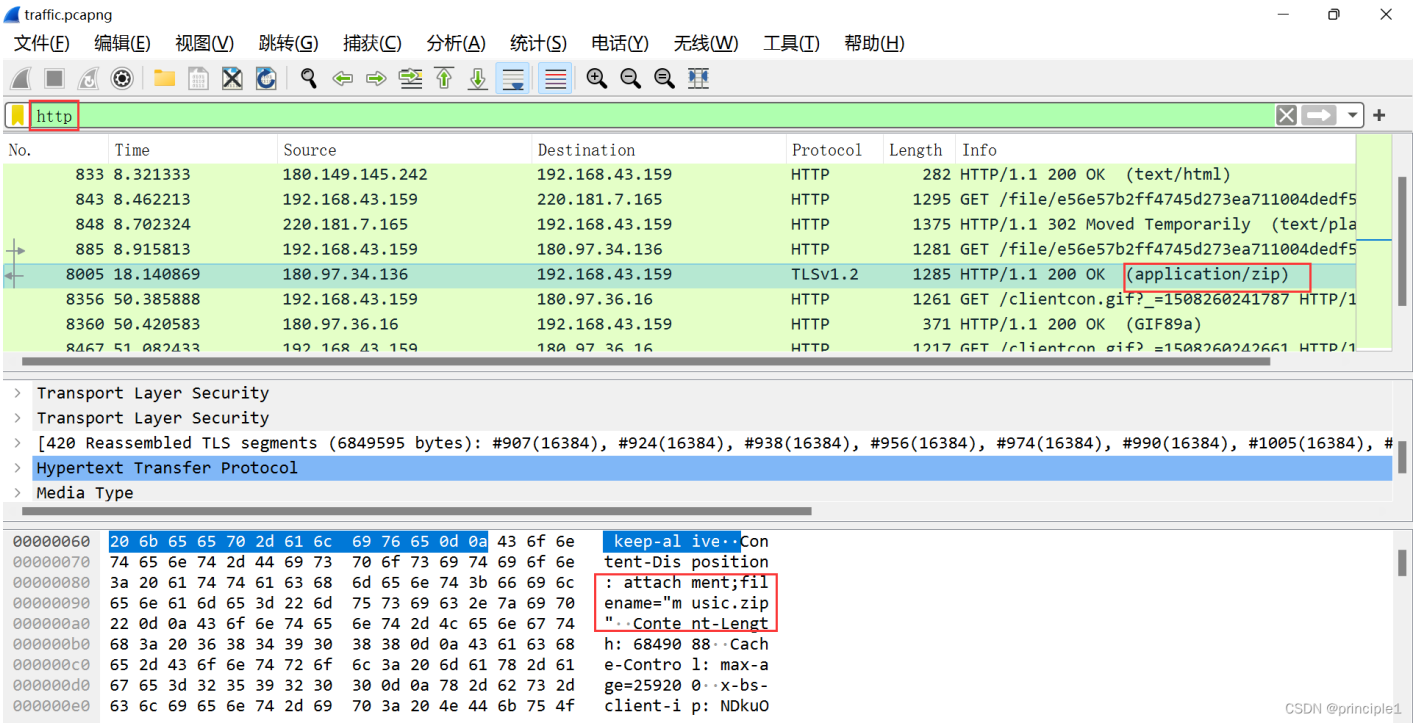


点击Protocols，有 SSL 就找 SSL，没有 SSL 就找 TLS

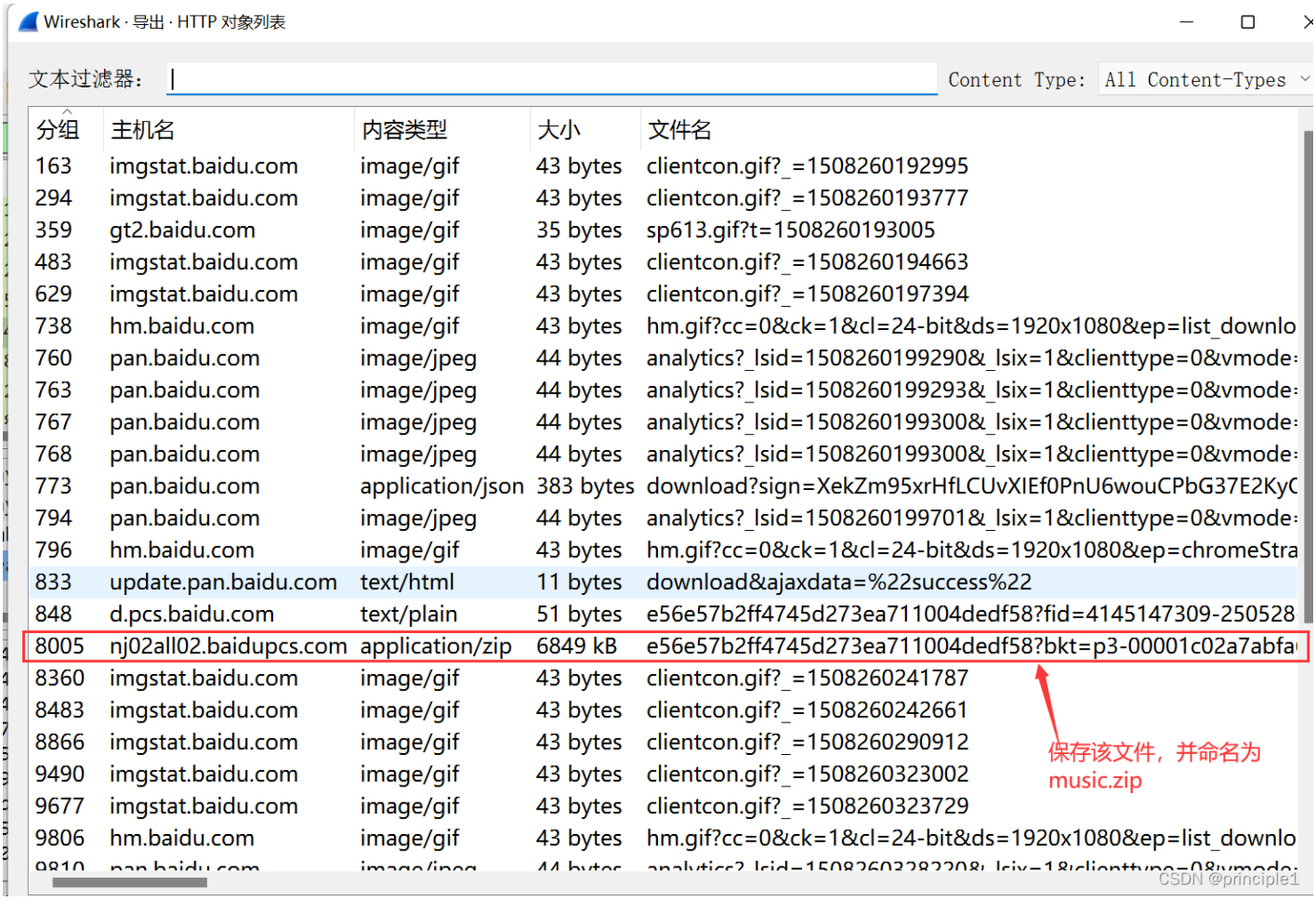
在这里导入下载了的key.log



过滤http，找到一个加密的下载链接，文件名为 music.zip，把该文件保存下来

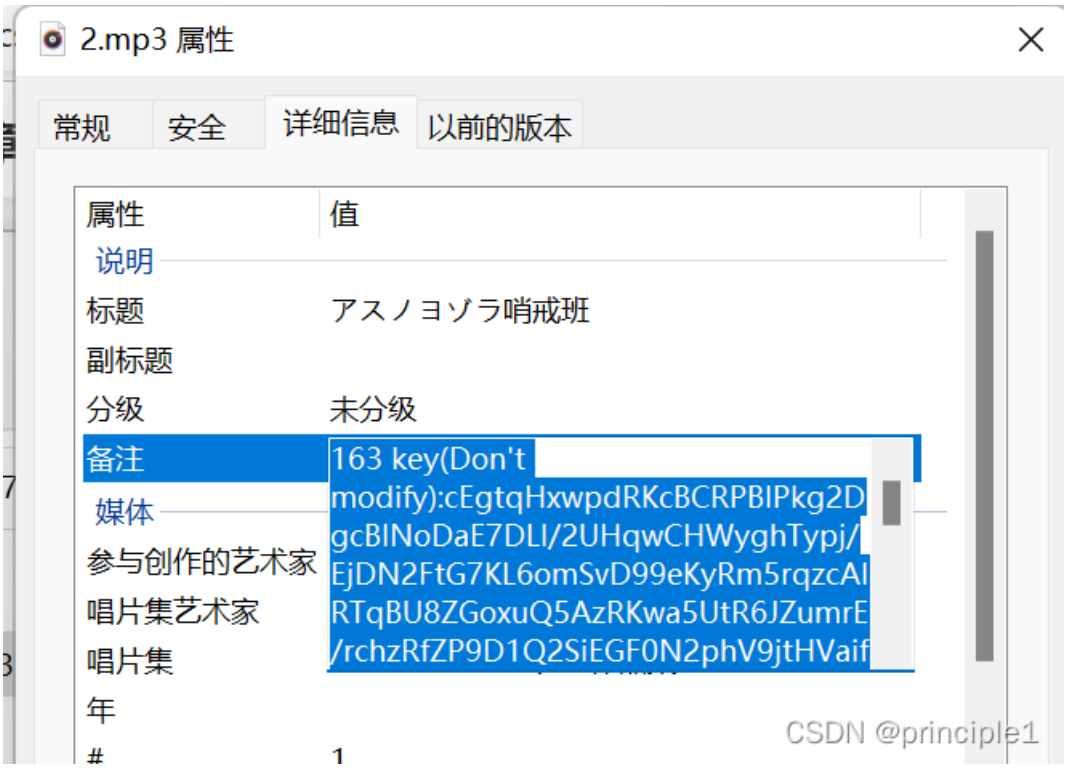


点击 文件 -> 导出对象 -> HTTP

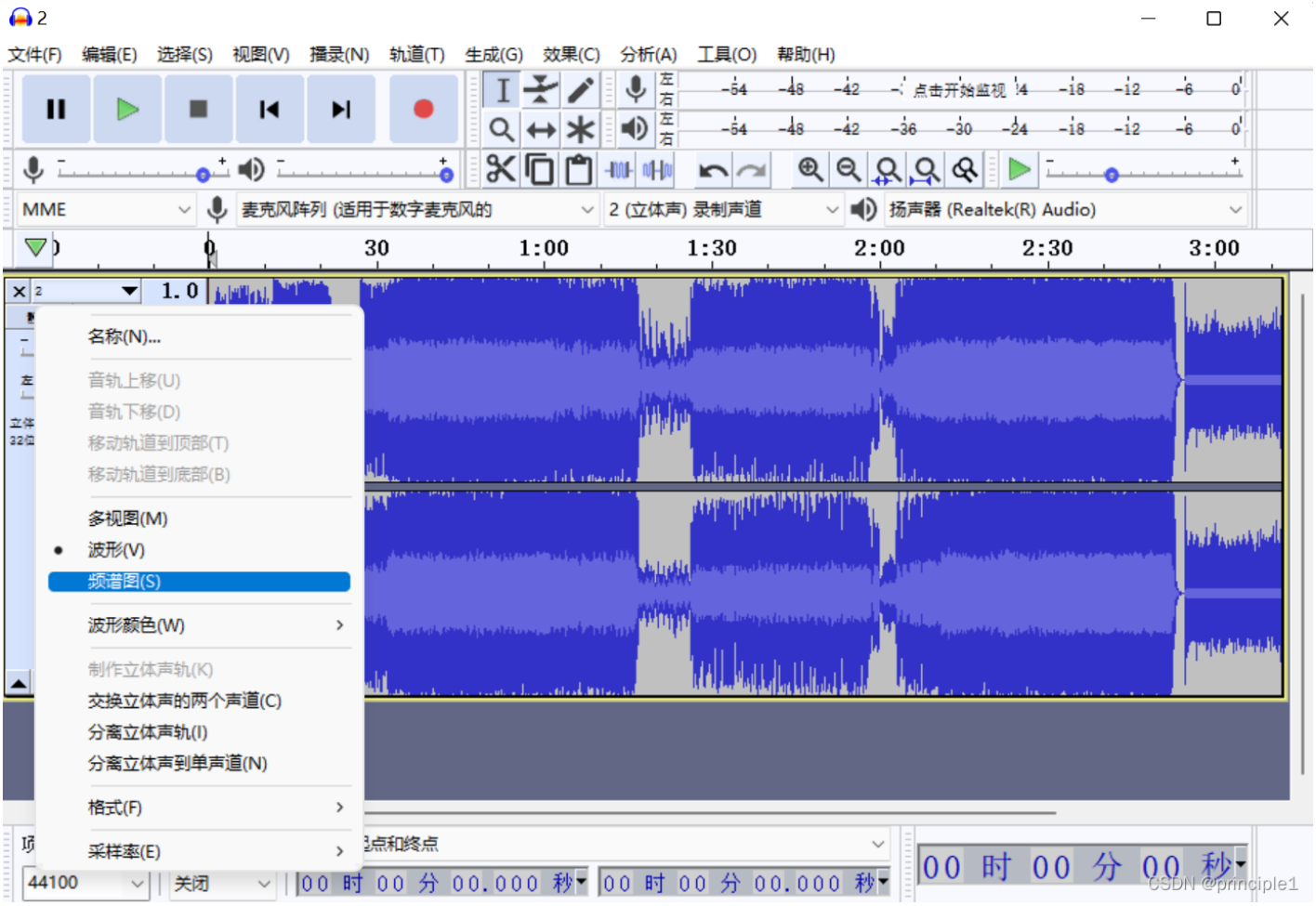


解压后发现是一个音频文件

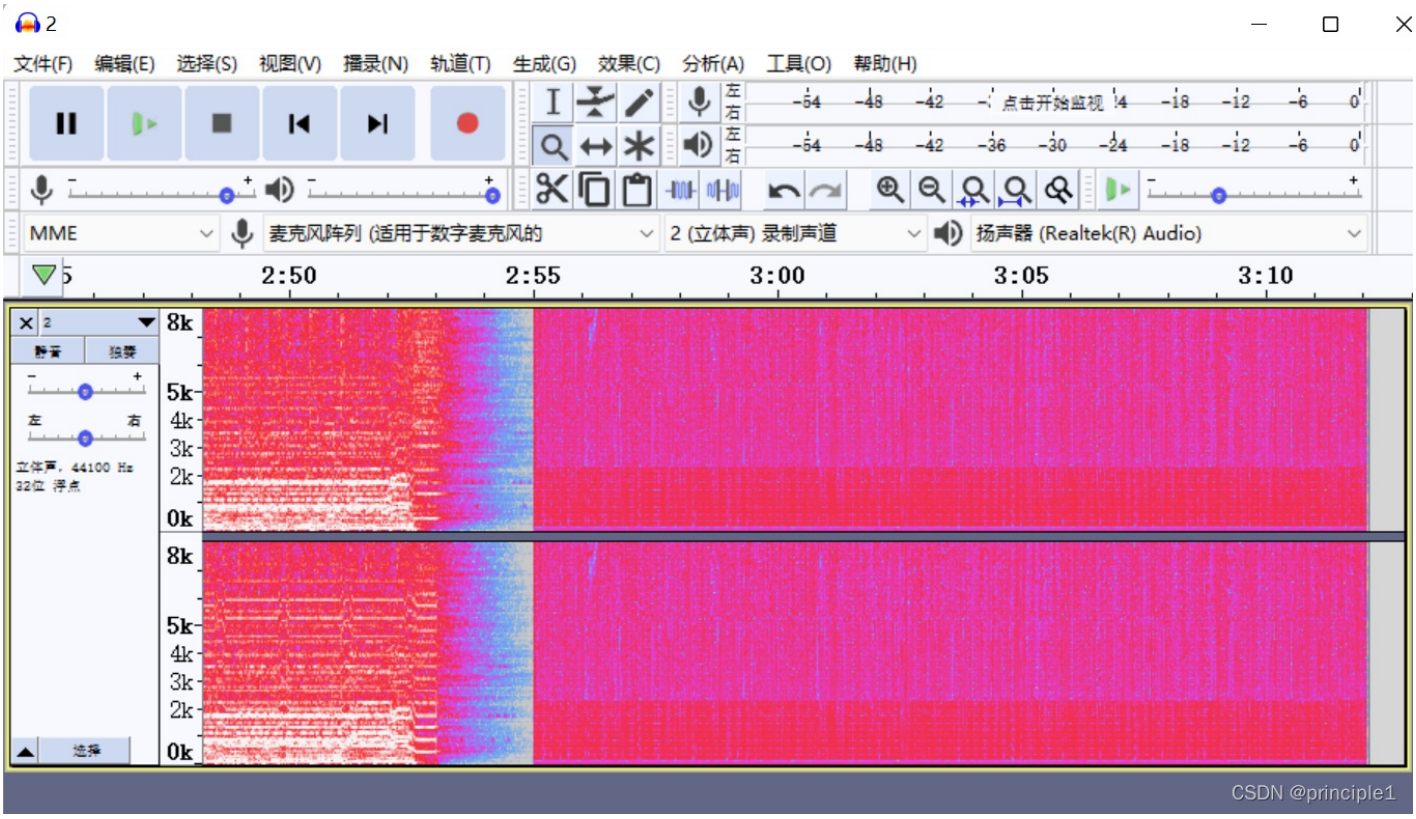
右键属性，发现base64编码，解码是乱码



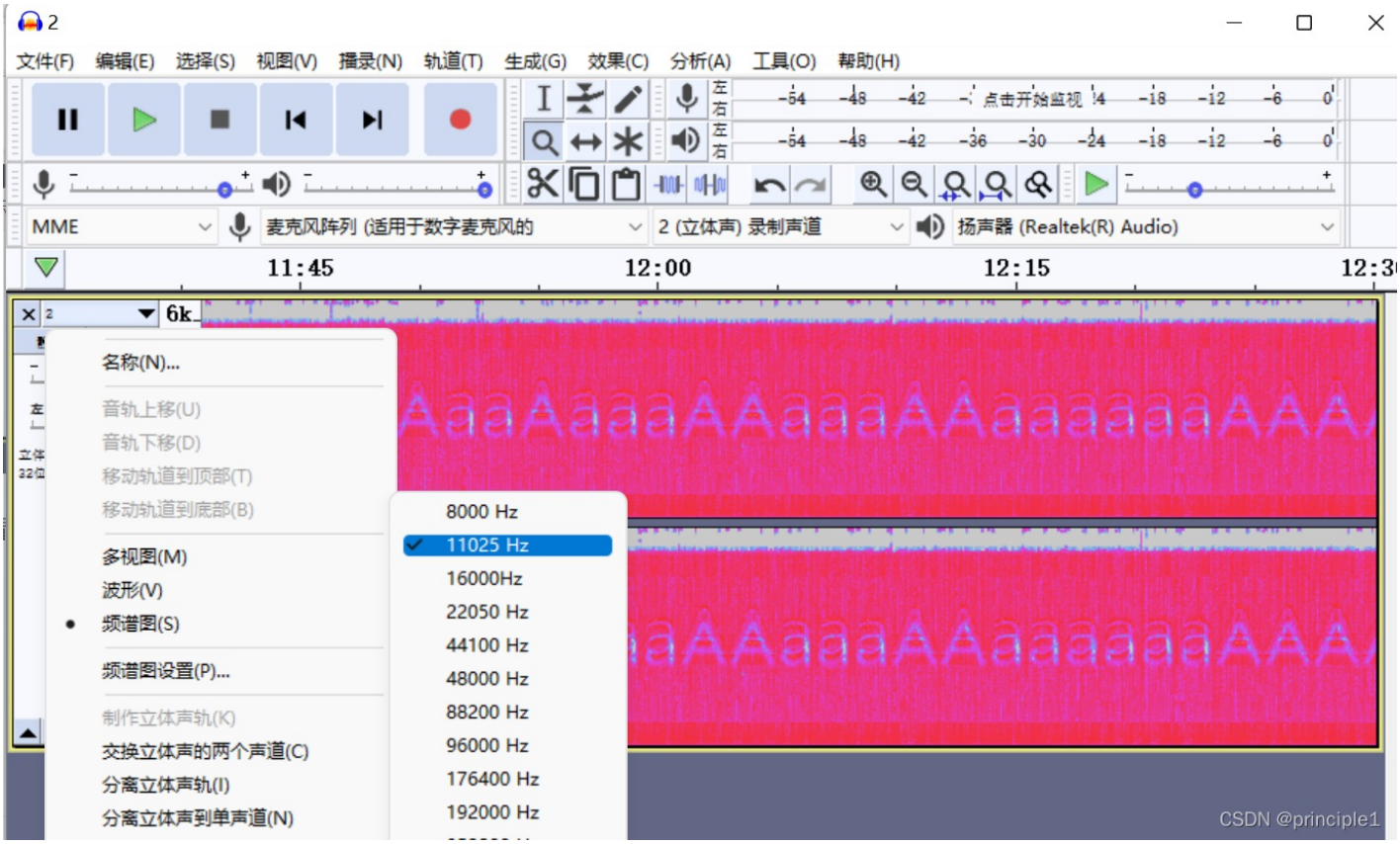
使用 Audacity打开音频，下载地址（Download – Audacity），查看频谱图，点击 2右侧的倒三角，下拉找到频谱图，点击它



听音频发现是后半部分有杂音，可以点击放大镜，左击放大，右击缩小



什么也看不出，可以调节采样率，在找到频谱图的下拉框最下方，从最小的数值开始尝试，发现11025Hz是最清晰的



读取其中内容（Key：AaaAaaaAAaaaAAaaaaaaAAAAAaaaaaaa!）

尝试把该密码去解密 1.zip