

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验四　观察TCP报文段并侦听分析FTP协议**

**班　　级 软件工程2018级1班**

**姓　　名 罗贤甫**

**学　　号 24320182203245**

**实验时间 2020年3月31日**

**2020 年 3 月 31 日**

# 实验目的

用 Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程，观察段 ID、 窗口机制和拥塞控制机制等。将该过程截图在报告中。

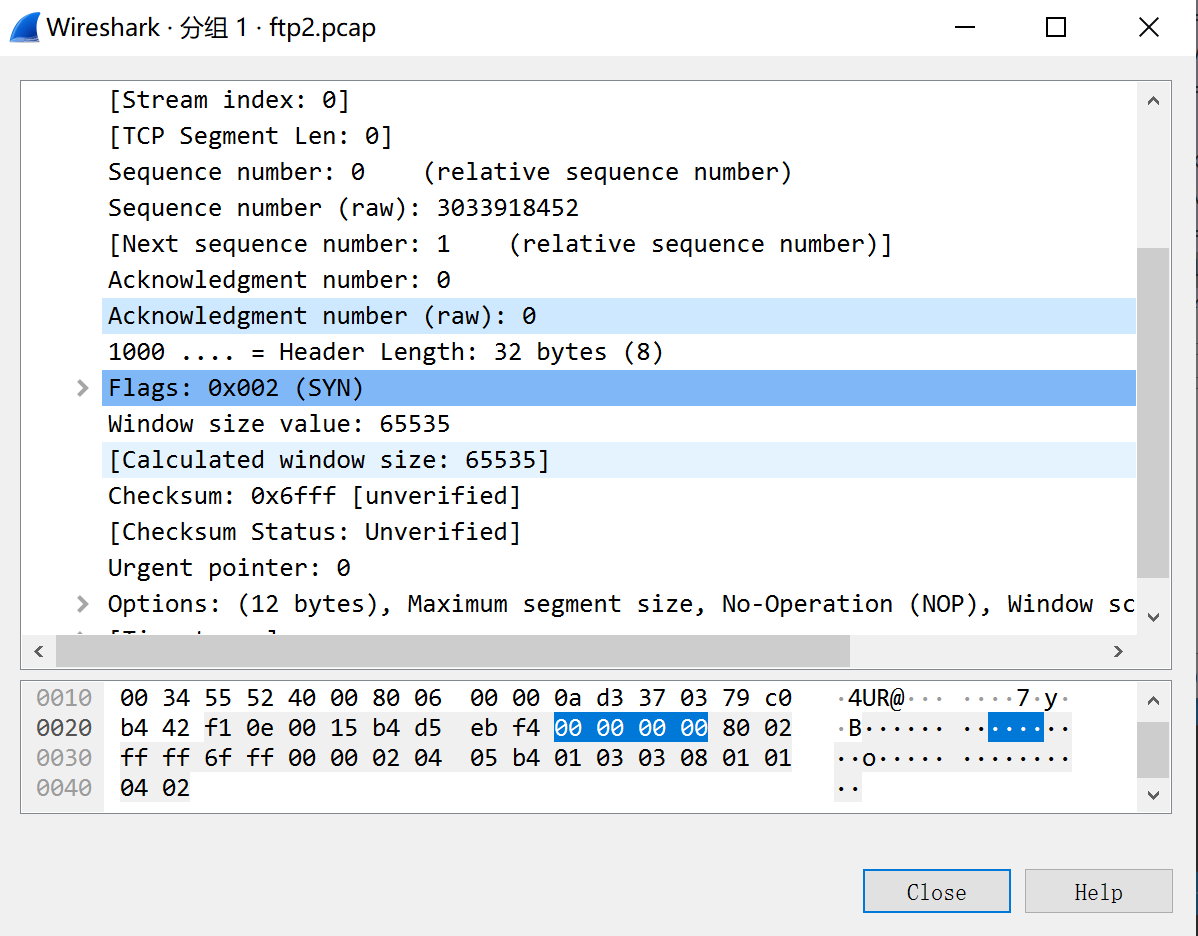
用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征， 再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

# 实验环境

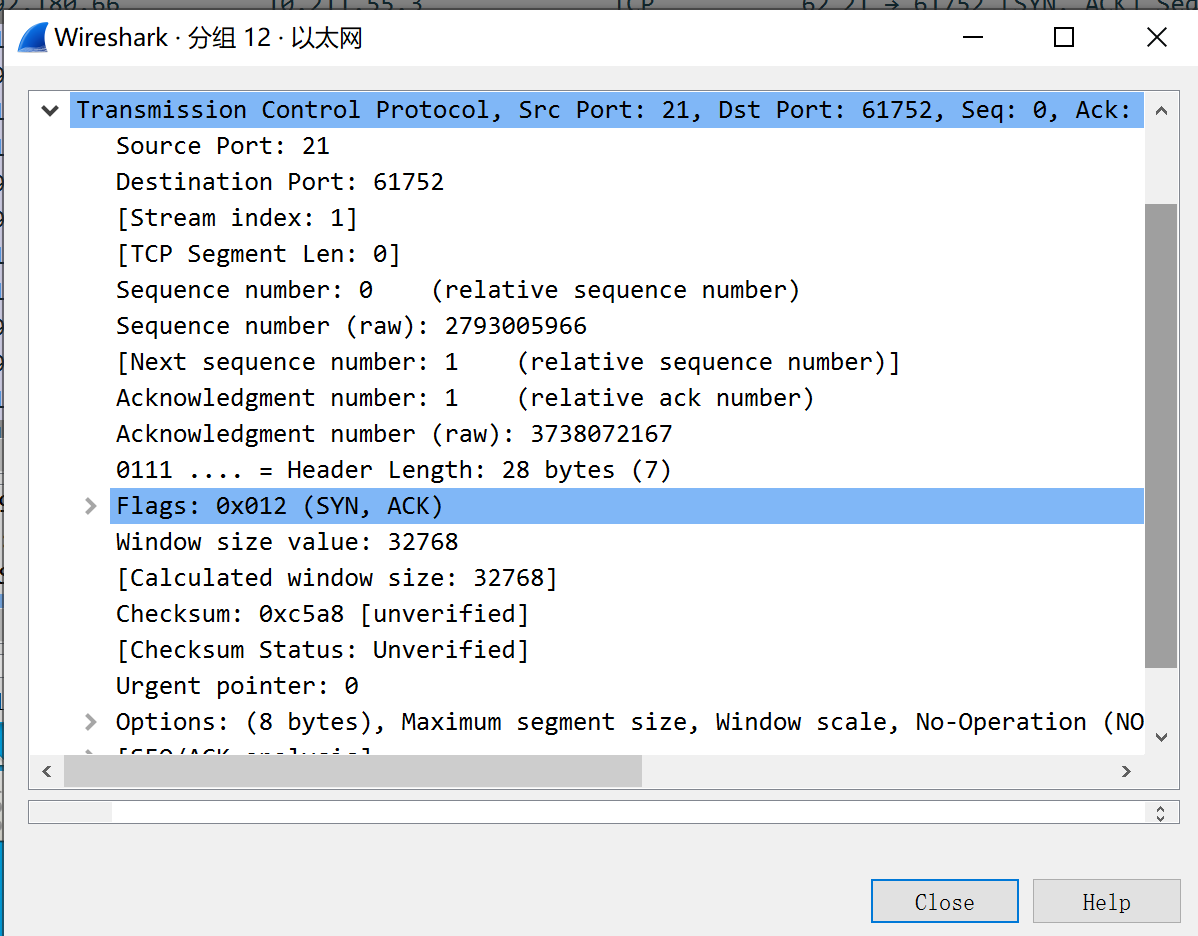
Win10系统，Visual Studio 2019，WireShark软件，C语言

# 实验结果

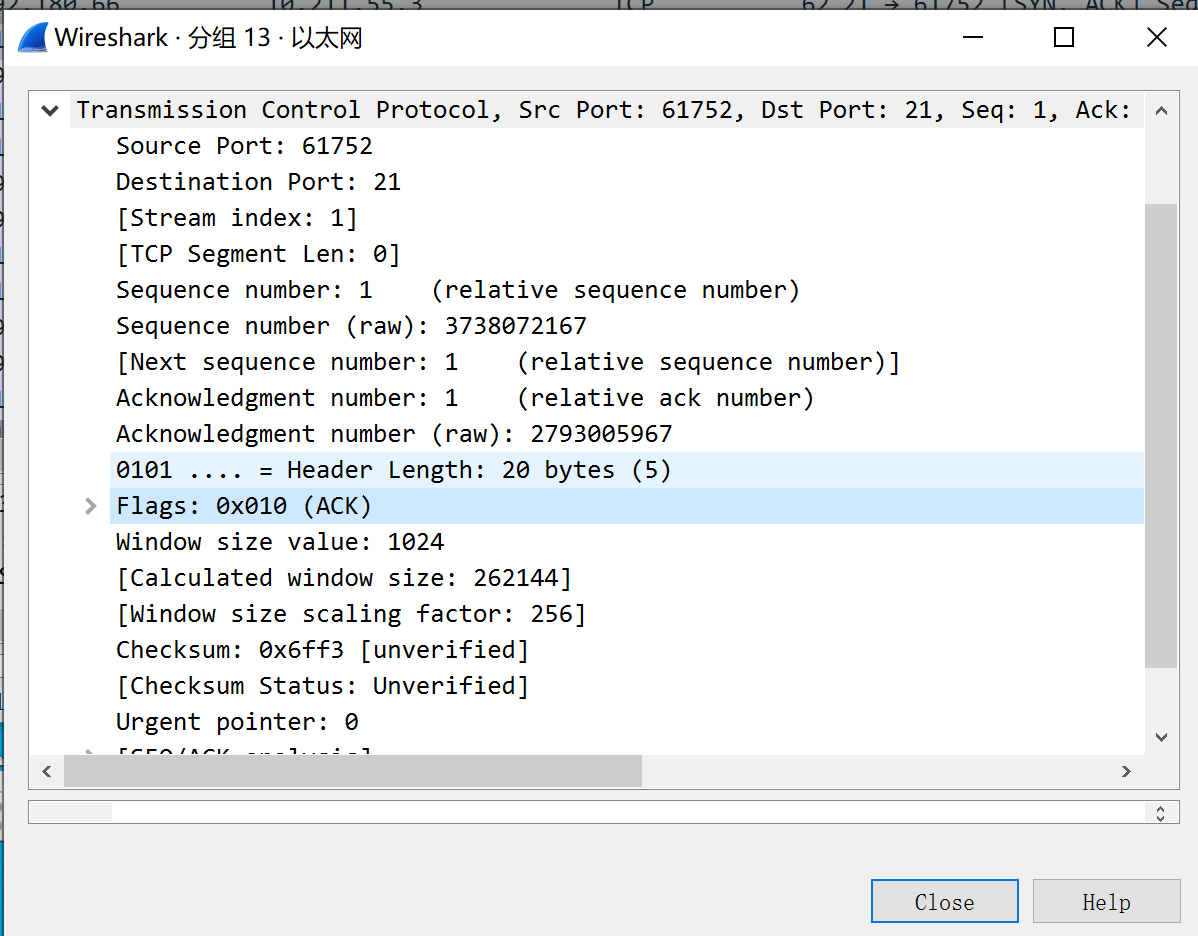
1. 本机向ftp服务器申请连接，flag=SYN



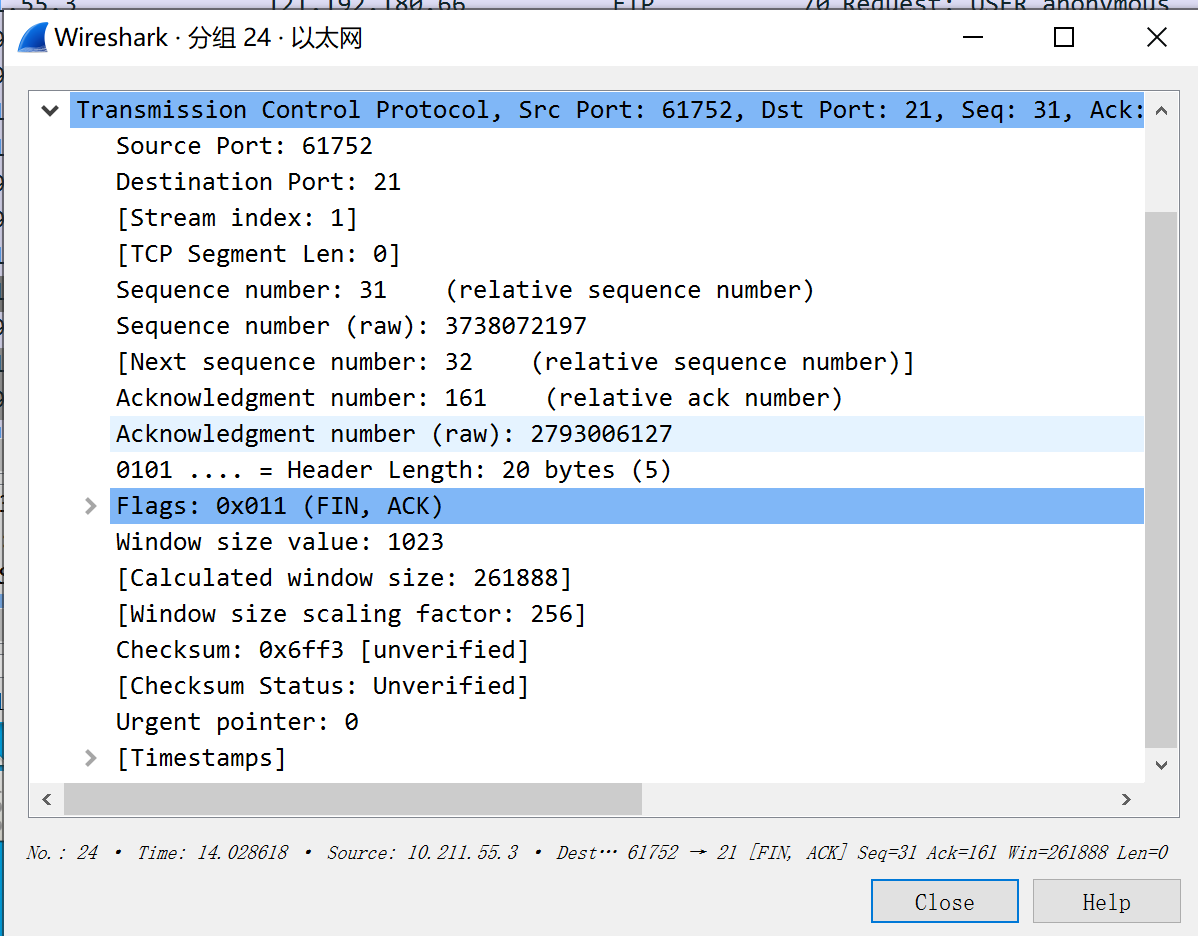
1. ftp服务器回复本机，flag=SYN，ACK



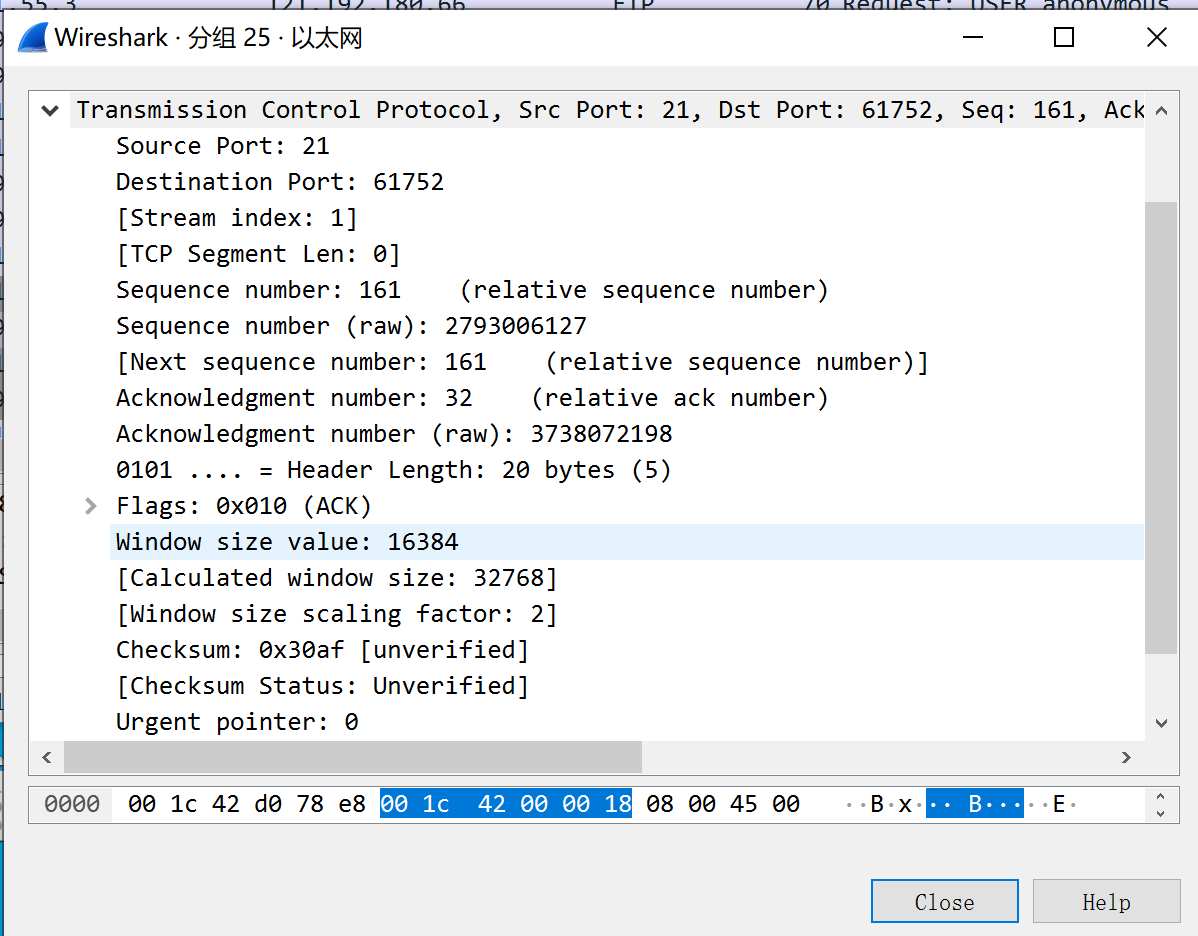
1. 本机收到，答复FTP服务器，flag=ACK



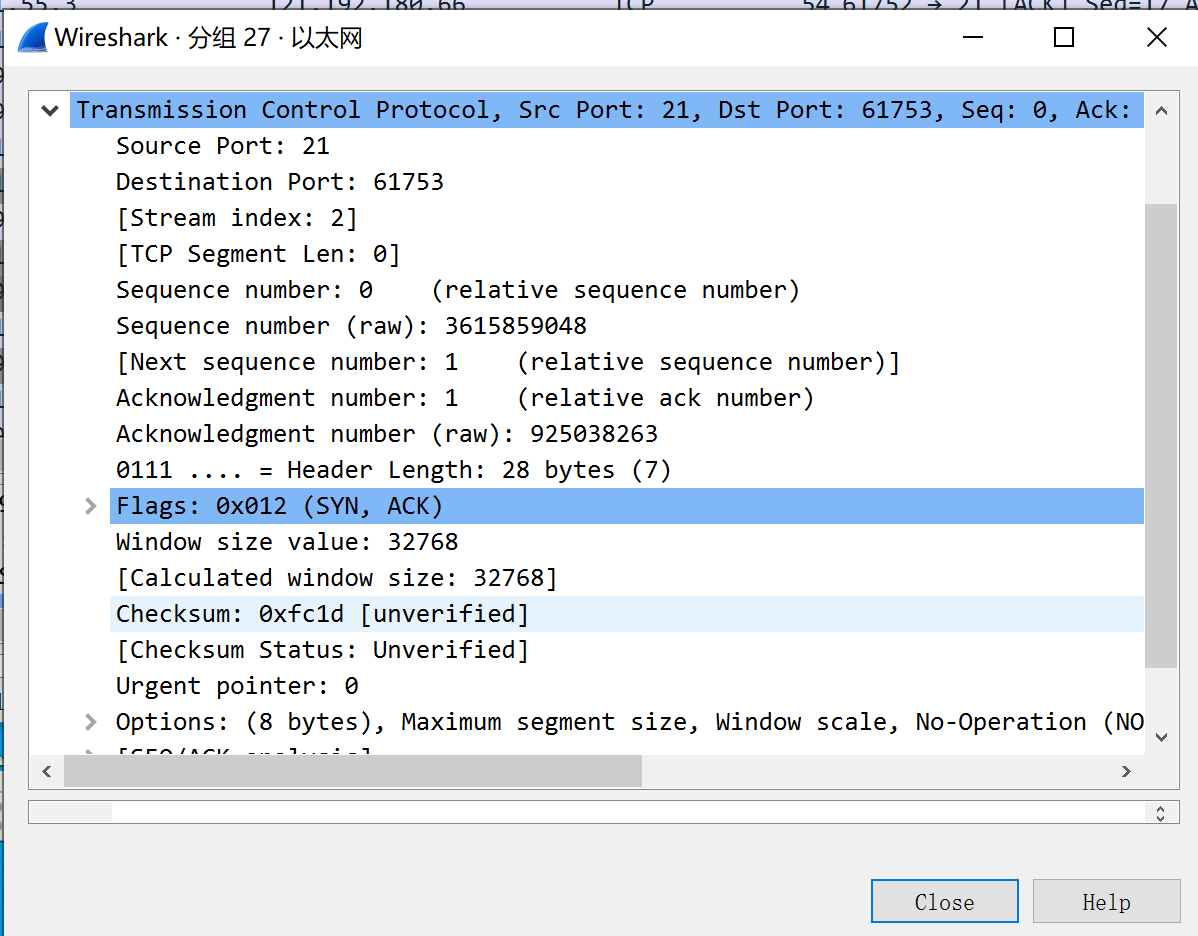
1. 本机向ftp申请断开，flag=FIN，ACK



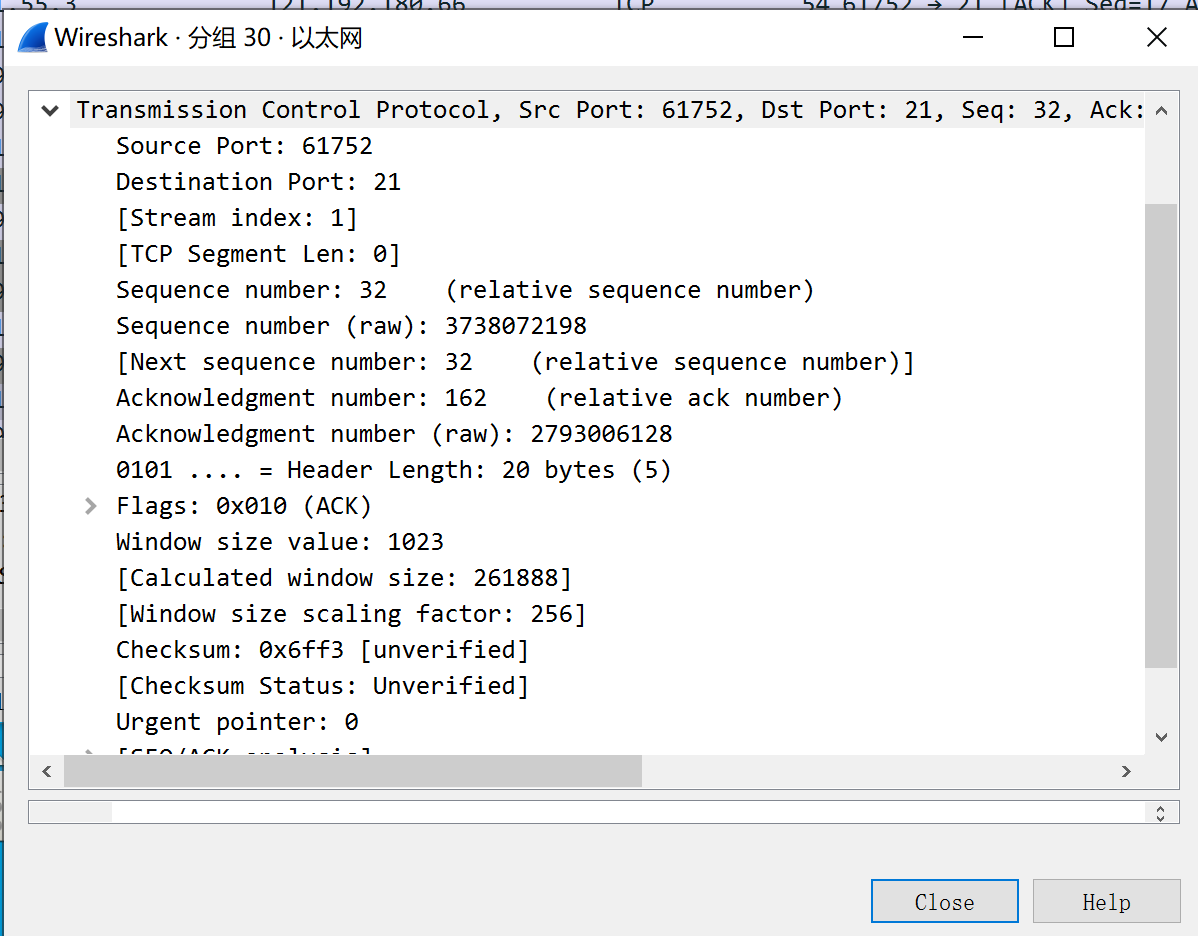
1. ftp收到申请答复本机，flag=ACK



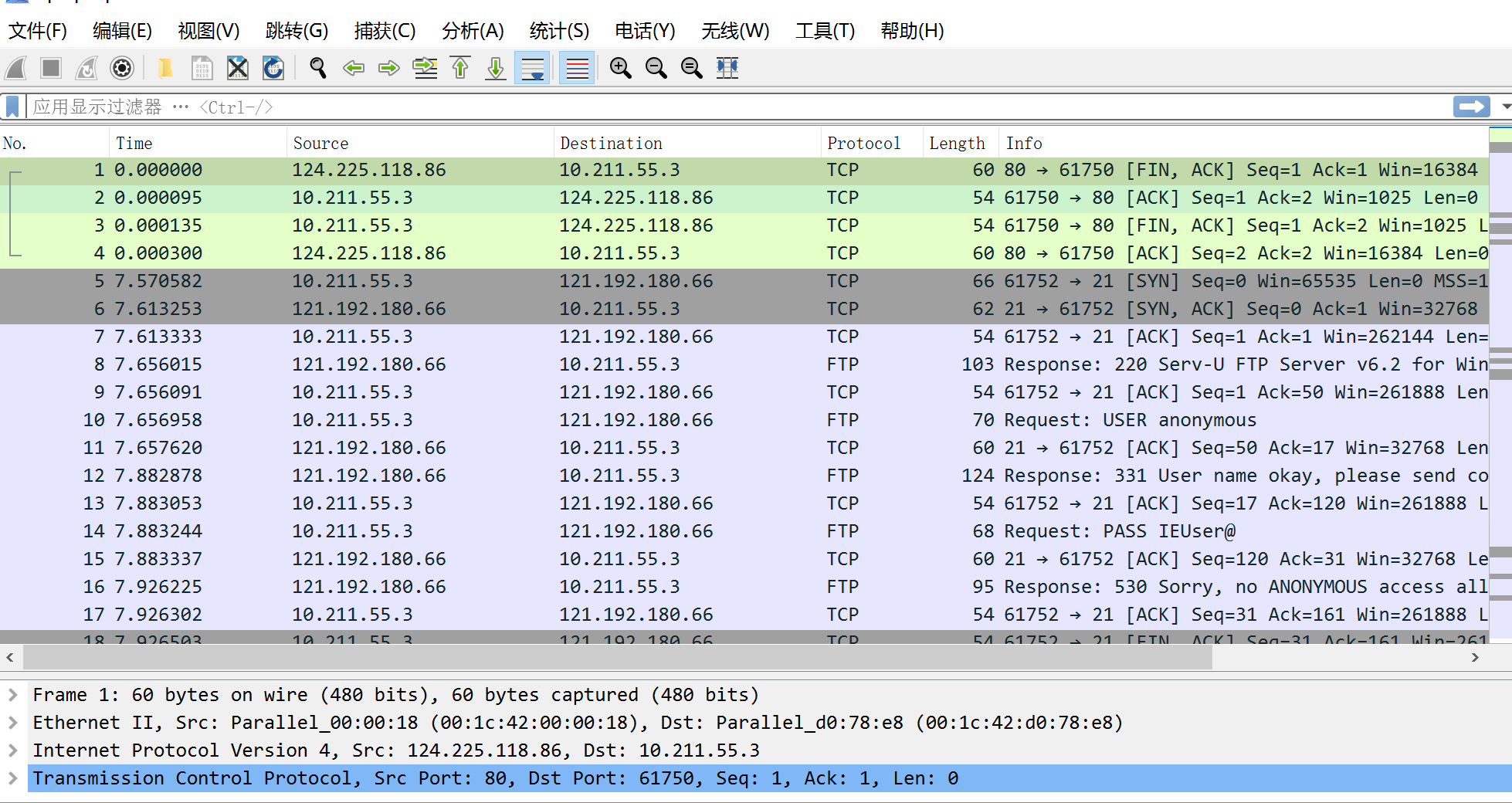
1. ftp服务器已经断开与本机的连接，向本机发信，flag=FIN，ACK



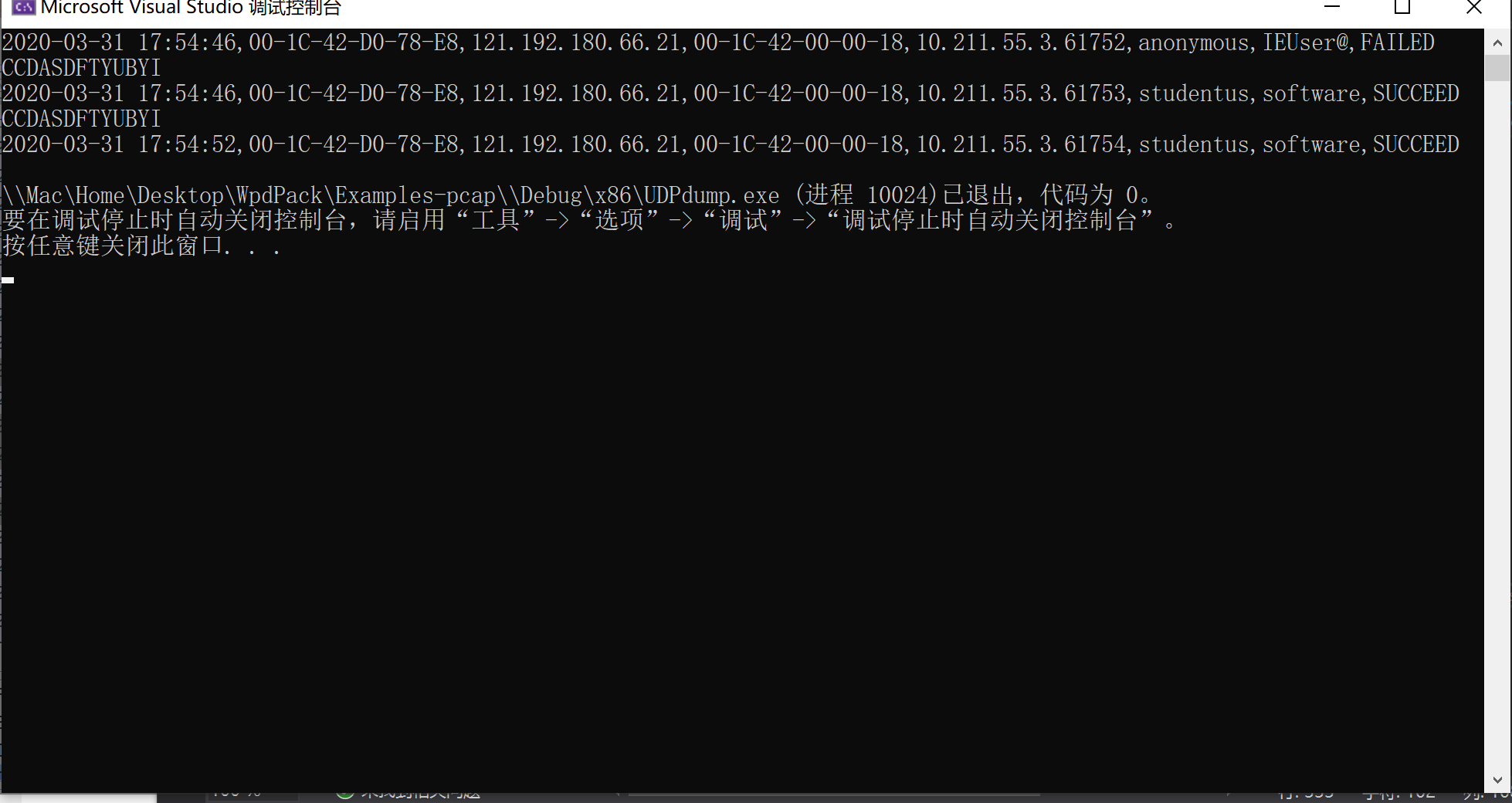
1. 本机收到，断开与ftp服务器连接，向ftp服务器返信，flag=ACK

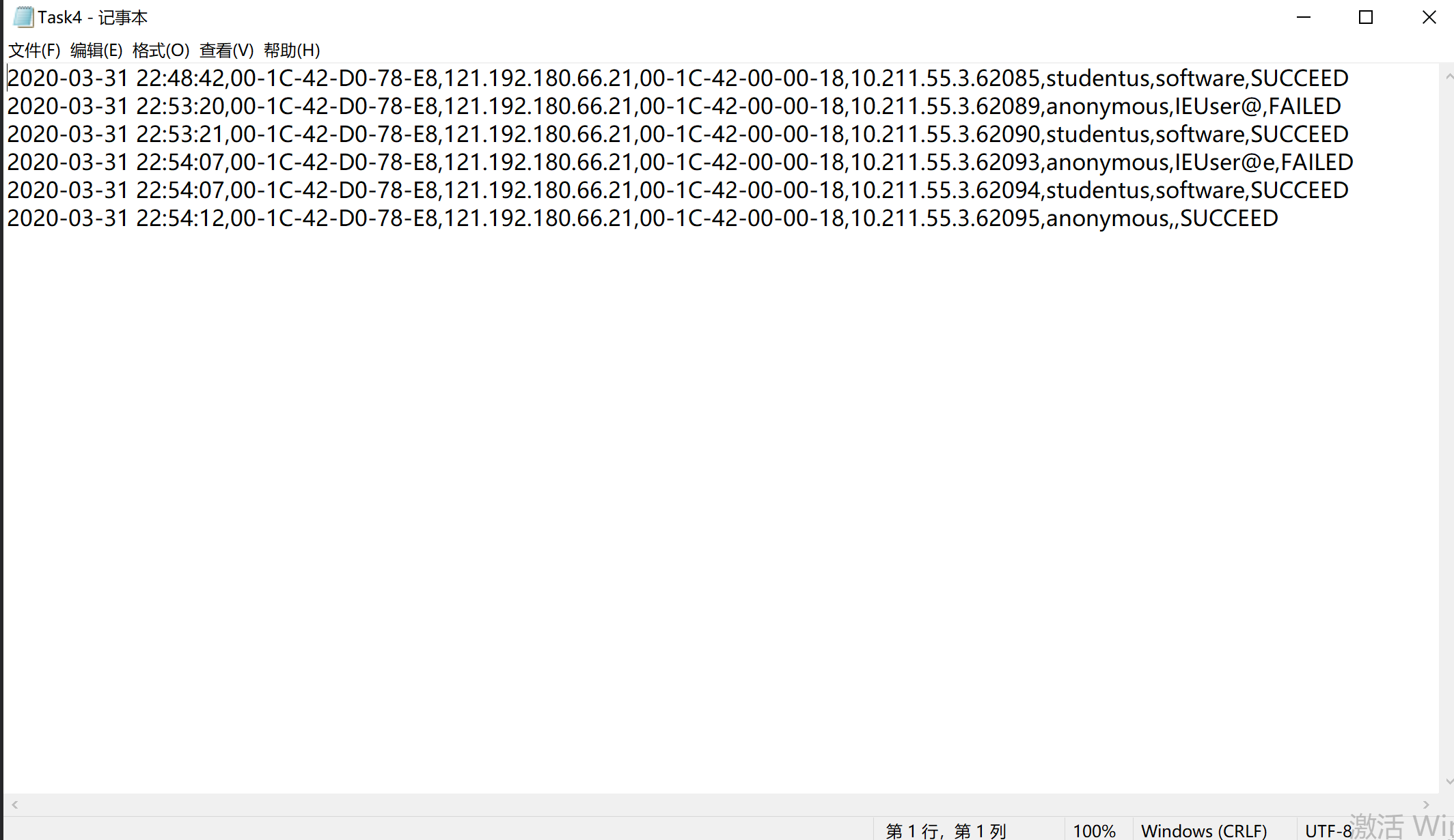


利用WireShark来捕获相关数据，用于程序分析



编写程序后运行，得到结果：



在实时条件下监听,输出到文件中

# 实验总结

本次实验于上次实验相似，难度上有所提升，帮助我更好地理解网络传输过程中的不同位置上的数据代表的含义也帮助我理解网络上的 FTP 数据流，解析协议内容，并作记录与统计，对用户登录行为进行记录。