

****

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3班**

**姓　　名 宋润涵**

**学　　号 24320182203266**

**实验时间 2020年3月25日**

**2020 年 3 月 29 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。

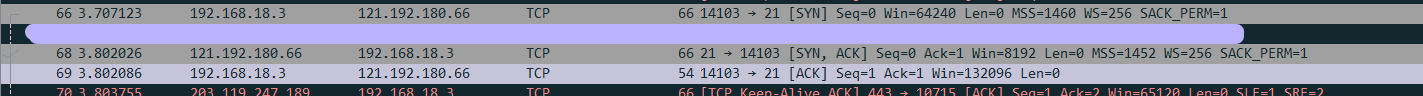
用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征， 再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网 络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

# 实验环境

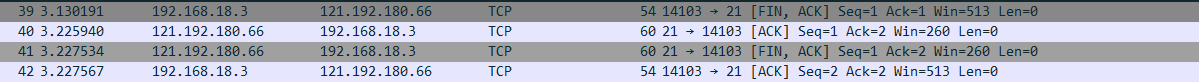
Windows 10，Visual Studio 2019，WinPcap 4.1.2，C++

# 实验结果

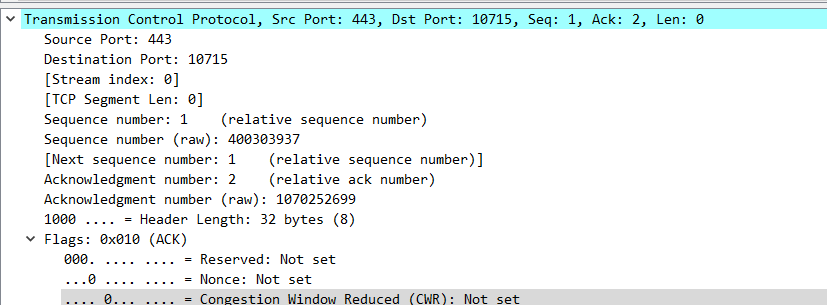
建立TCP连接



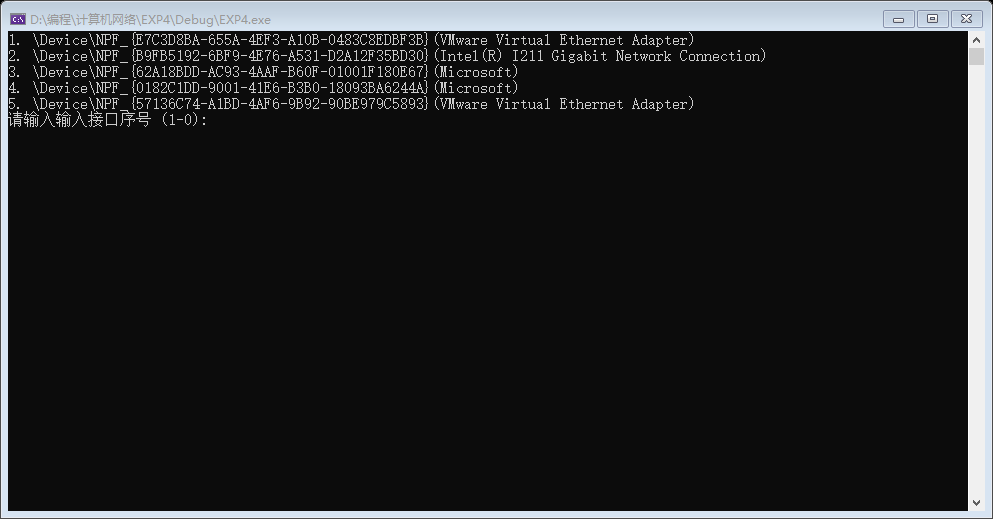
断开TCP连接



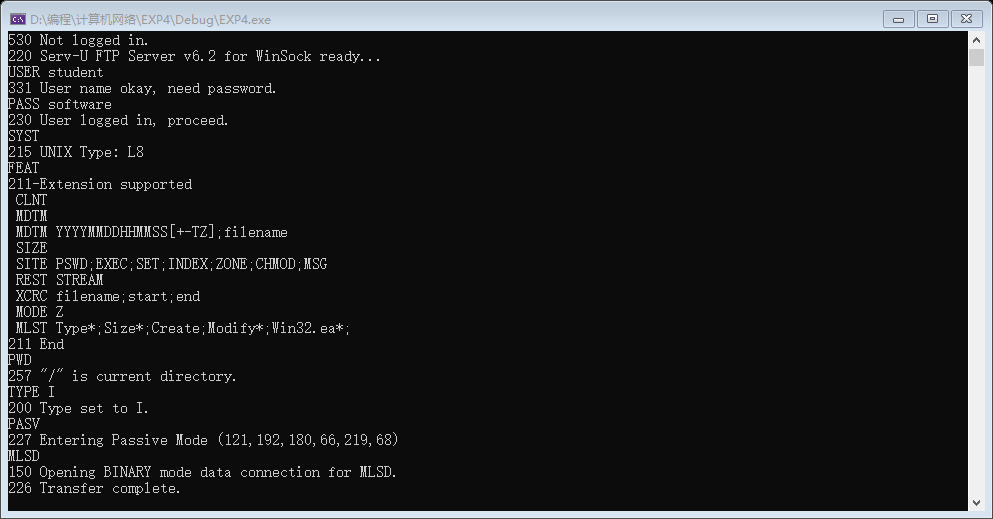
段ID拥塞控制等等



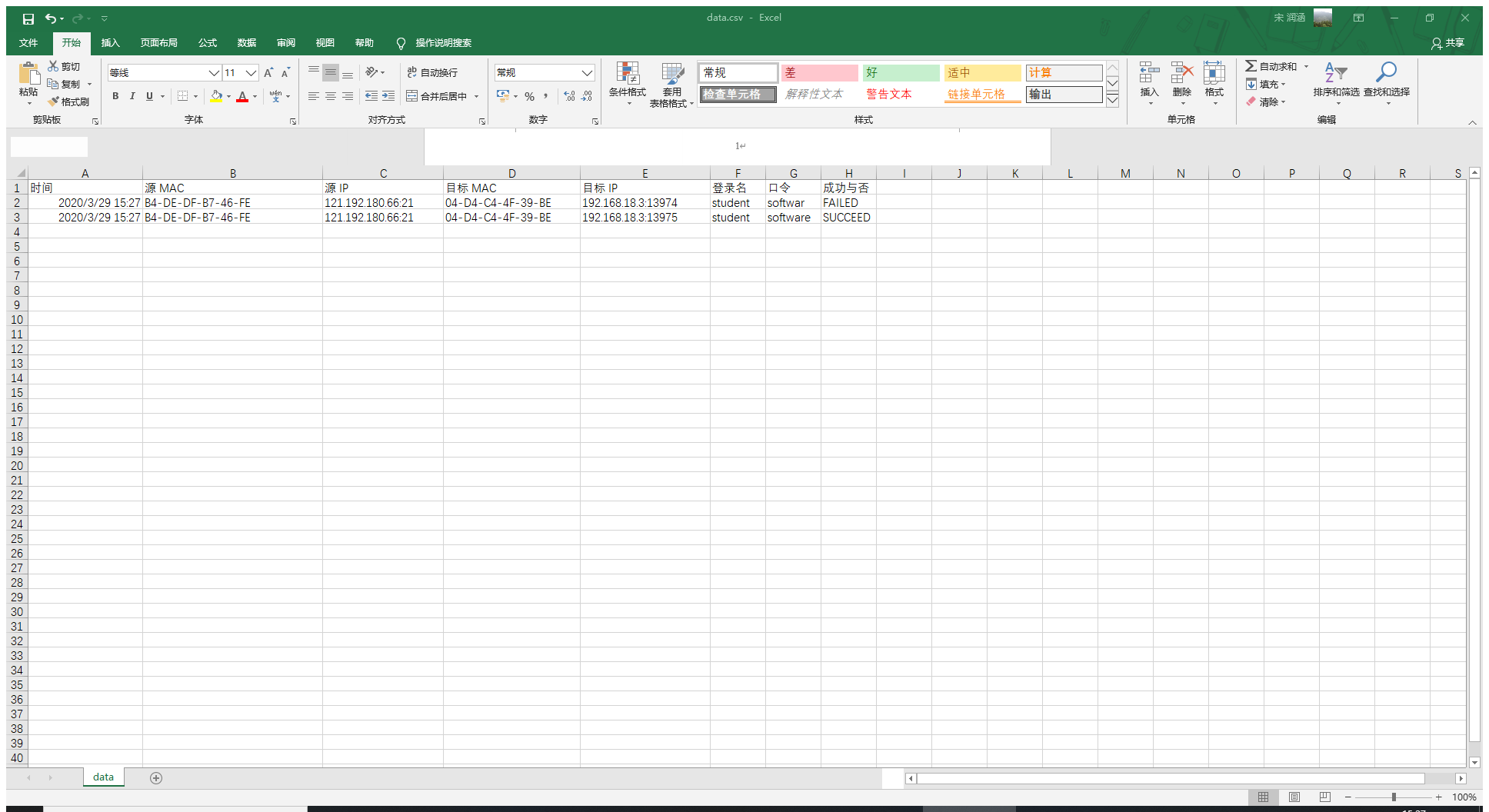
程序启动界面，输入需要监听的端口号后进入监听模式。



程序会监听FTP命令，并将命令显示出来，按ESC退出监听程序



程序会将登录信息保存在CSV文件中



# 实验总结

TCP是一种较为可靠的传输协议，他是面向连接的。在此过程中他会进行三次握手（建立连接），四次挥手（撤除连接）。

本次实验使我对WinPcap的过滤系统有了进一步的了解，包括编译过滤器（compile）和设置过滤器（setFilter）

FTP拥有主动模式和被动模式两种传输模式，其中21号端口是用来给服务端发送命令。在被动模式中服务器会给出一个端口用来传送数据。主动模式中，这个端口由客户端给出。