

****

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2班**

**姓　　名 林正男**

**学　　号 20420172201787**

**实验时间 2020年3月25日**

**2020 年 3 月 27 日**

# 实验目的

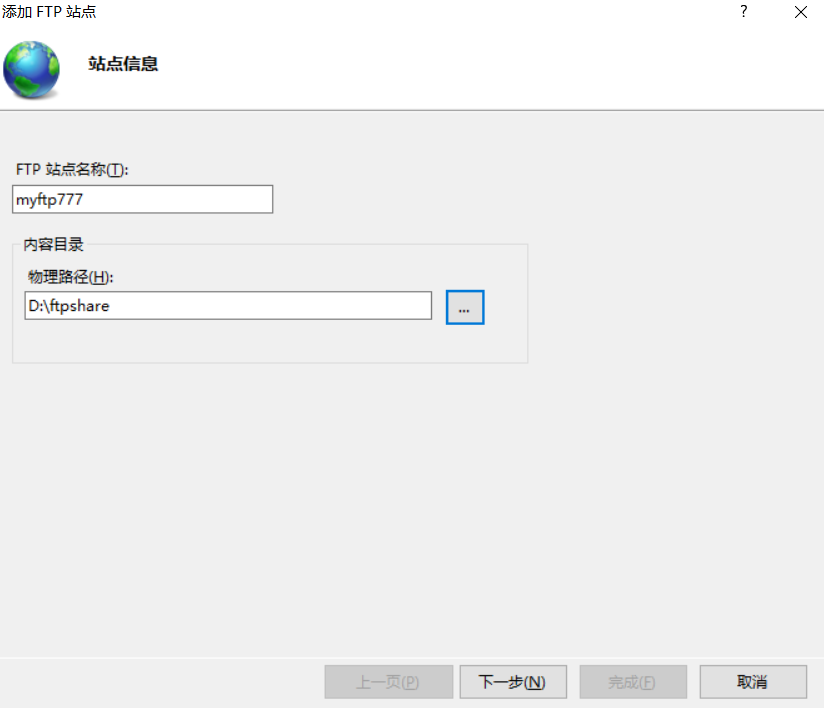
1.用Wireshark侦听并观察TCP数据段。观察其建立和撤除连接的过程，观察段ID、 窗口机制和拥塞控制机制等。

2. 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。

# 实验环境

Windows10 c++ wireshark

# 实验结果

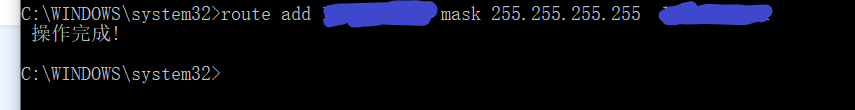


创建自己的ftp



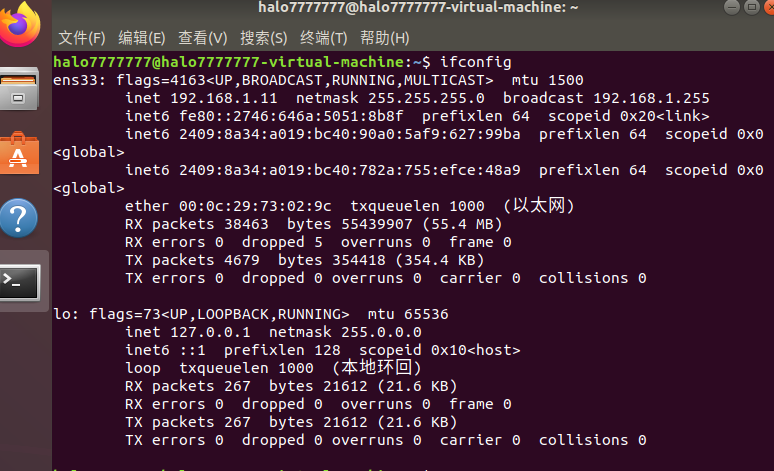
授权一个名user的用户，口令为123

但因为都是一台计算机的地址，wireshark或者编写的winpcap程序只能检测到经由网卡的数据传输，无法检测到localhost的数据传输。

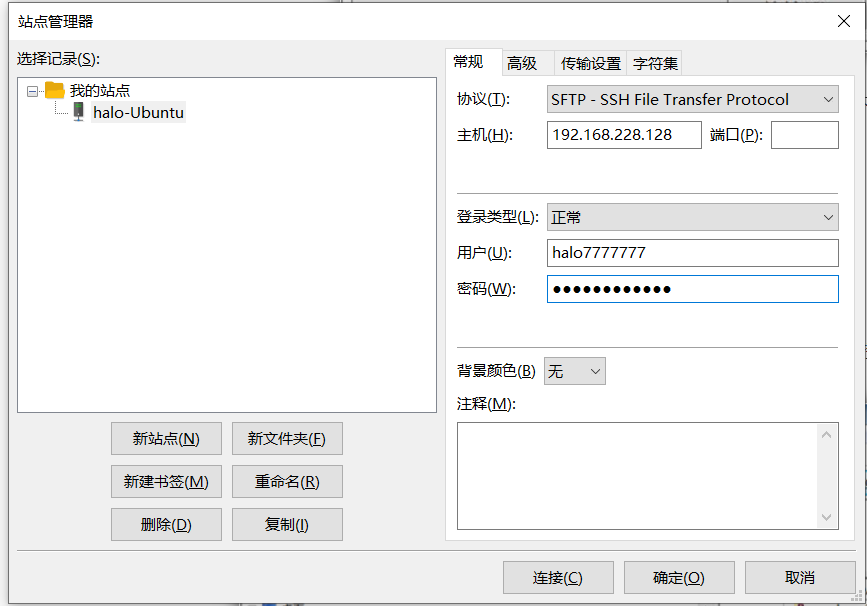


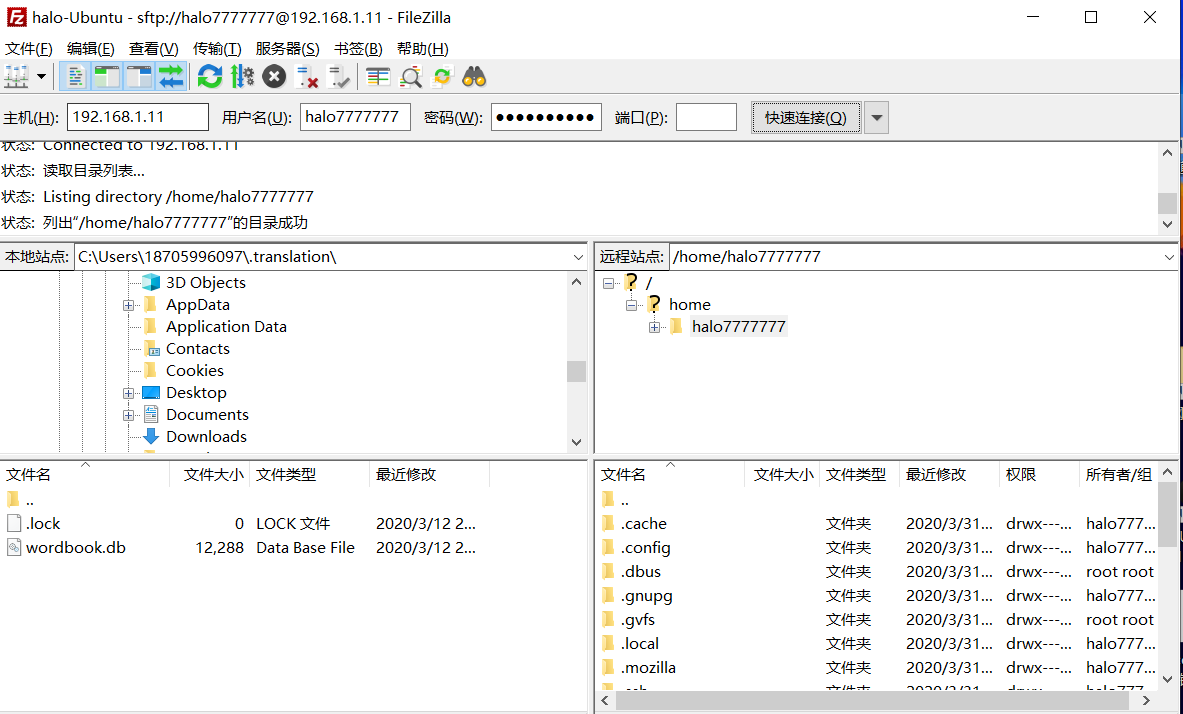
改变IP地址，使传输的数据经由网卡，但ftp也会因为其改变而无法打开，

使用虚拟机Ubuntu系统

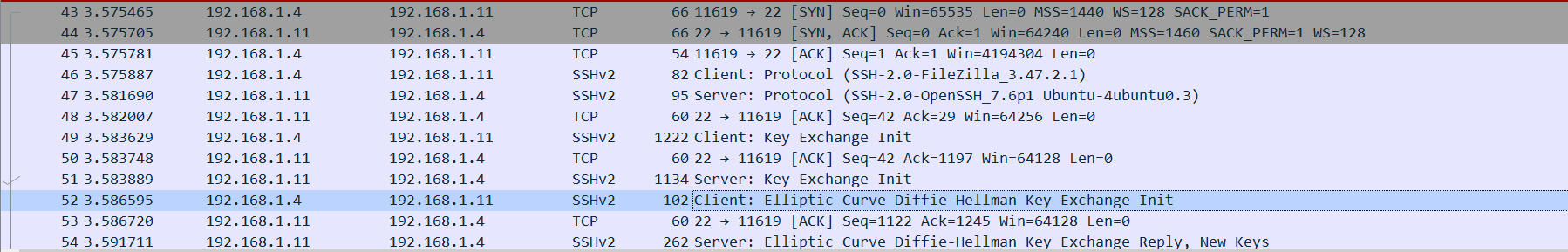


虚拟地址为192.168.1.11



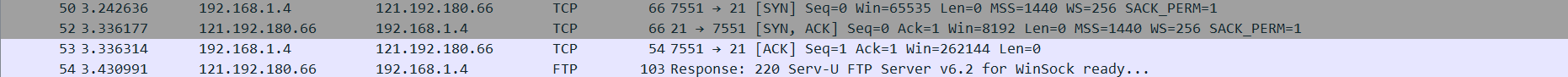


使用FileZilla创建与虚拟主机的ftp连接

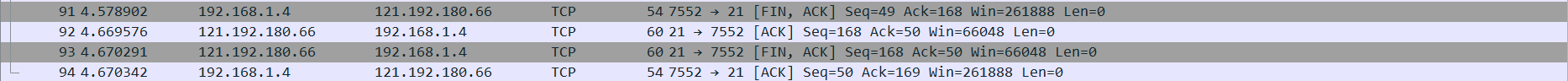


可观察到三次握手等情况，因为连接时协议为SFTP所以为SSHV2

接下来使用学院ftp



图示即为与ftp建立连接的三次握手过程，第4条即为ftp消息已建立连接



图示即为四次挥手与ftp服务器断开连接







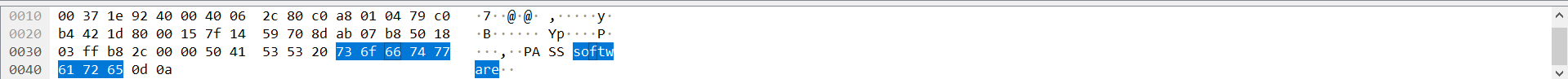


图示即为滑动窗口实现流量控制



慢开始与拥塞避免

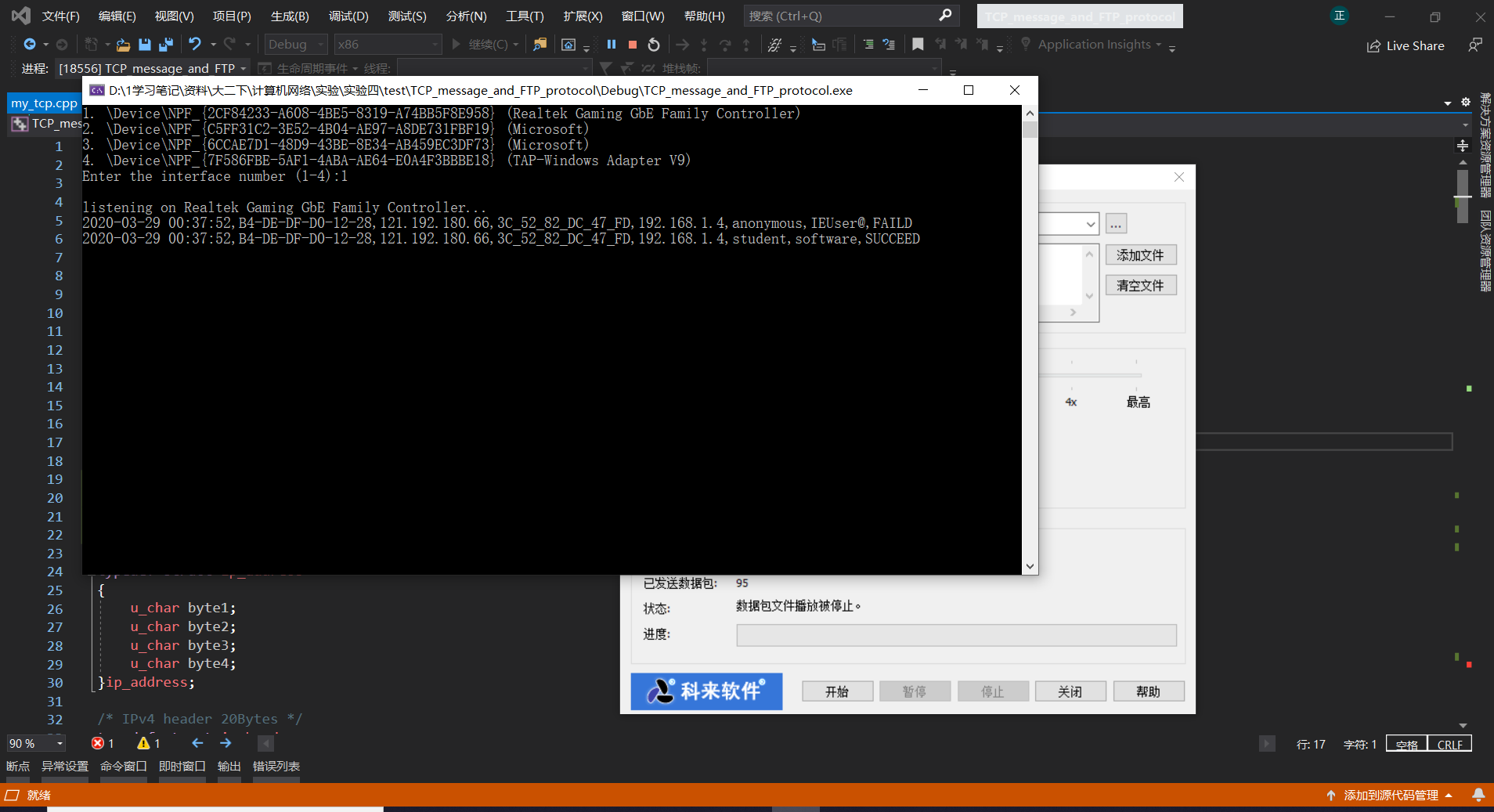






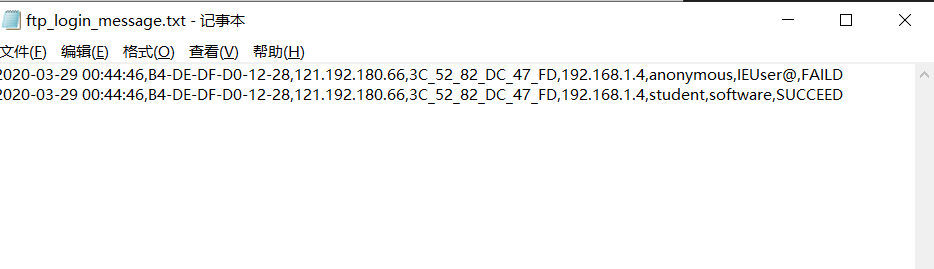
图示即为用户名，口令，即连接成功提示头部分别为USER，PASS，230

连接失败头部为530



在终端测试输出

第一次是匿名访问，由于学院ftp没有开启所以失败，第二次正确账户，口令成功连接



重定向将CSV格式日志输出到文件

# 实验总结

1.学会了通过过滤器获得TCP信号的方法

2.学习了TCP中的三次握手四次挥手的原理

3.学习了TCP的窗口流量控制与拥塞控制方法