厦門大學

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 陈芸衣

学　　号 24320182203182

实验时间 2020 年 3 月 25 日

2020 年 3 月 31 日

1 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.

2 实验环境

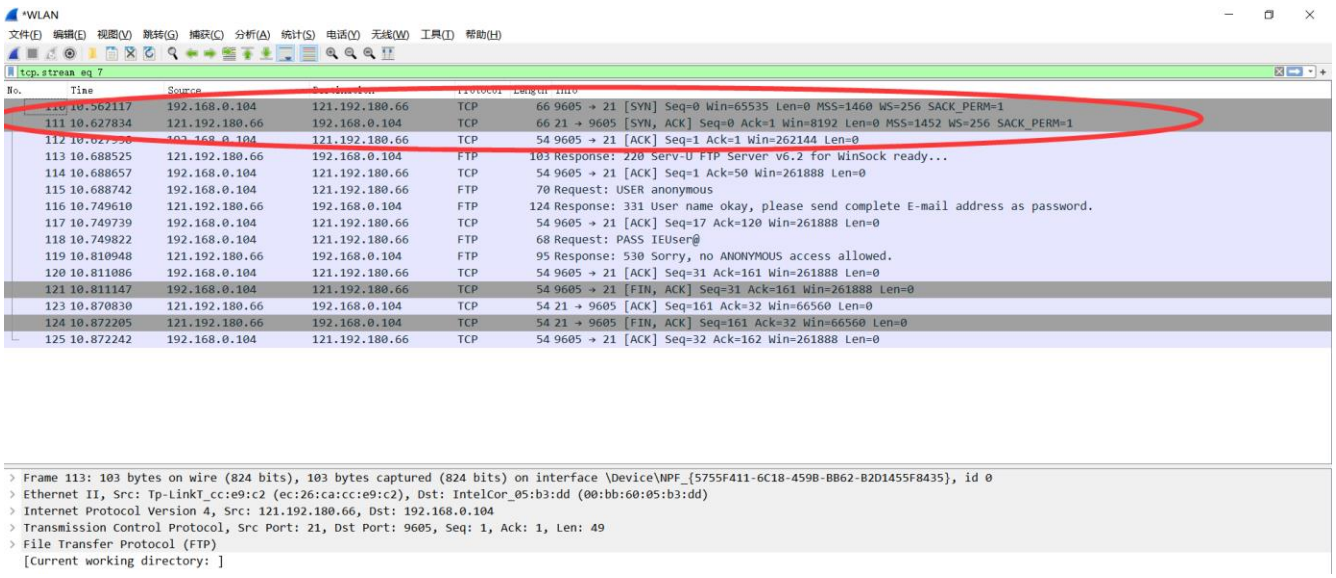
Windows10，wirehark，VS2017

3 实验结果

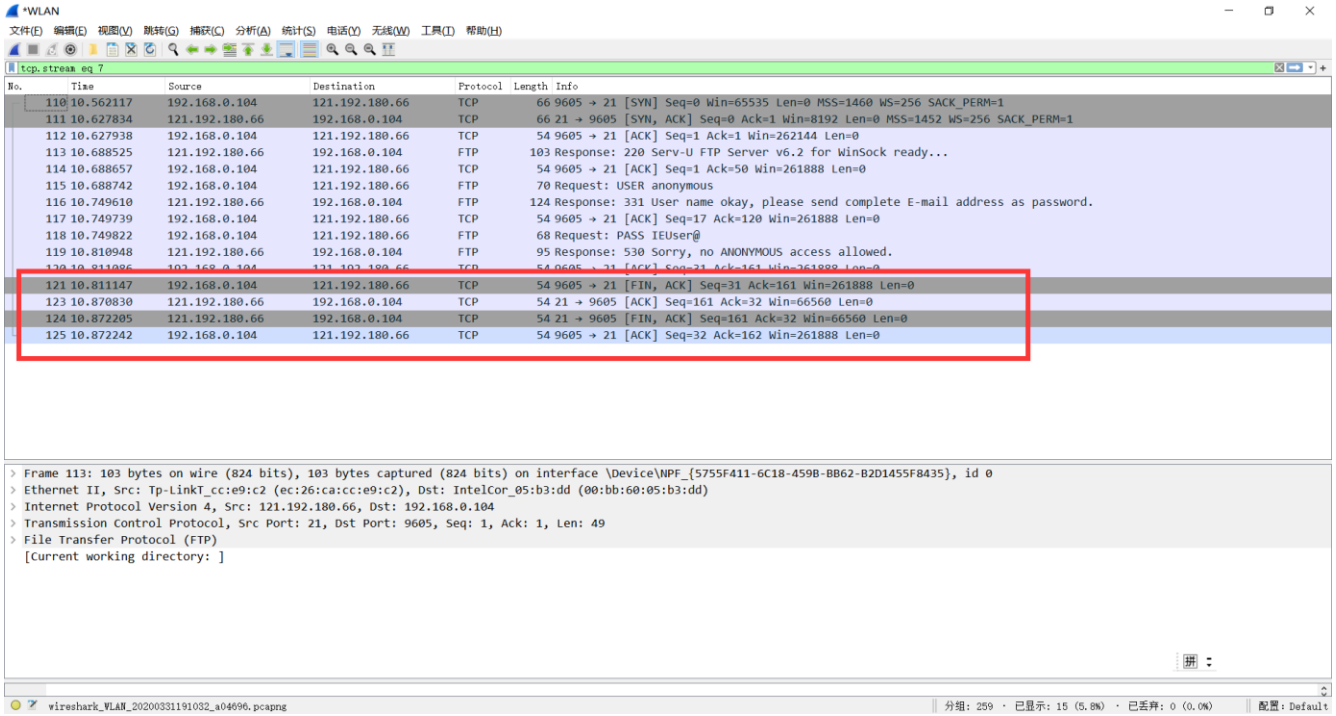
用 Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程：

追踪 tcp 流，三次握手建立连接的记录如下：（第一次握手信号 SYN：seq=0;第二次握手信号 SYN+ACK：seq=0,ack=1;第三次握手握手信号 ACK：seq=1,ack=1）

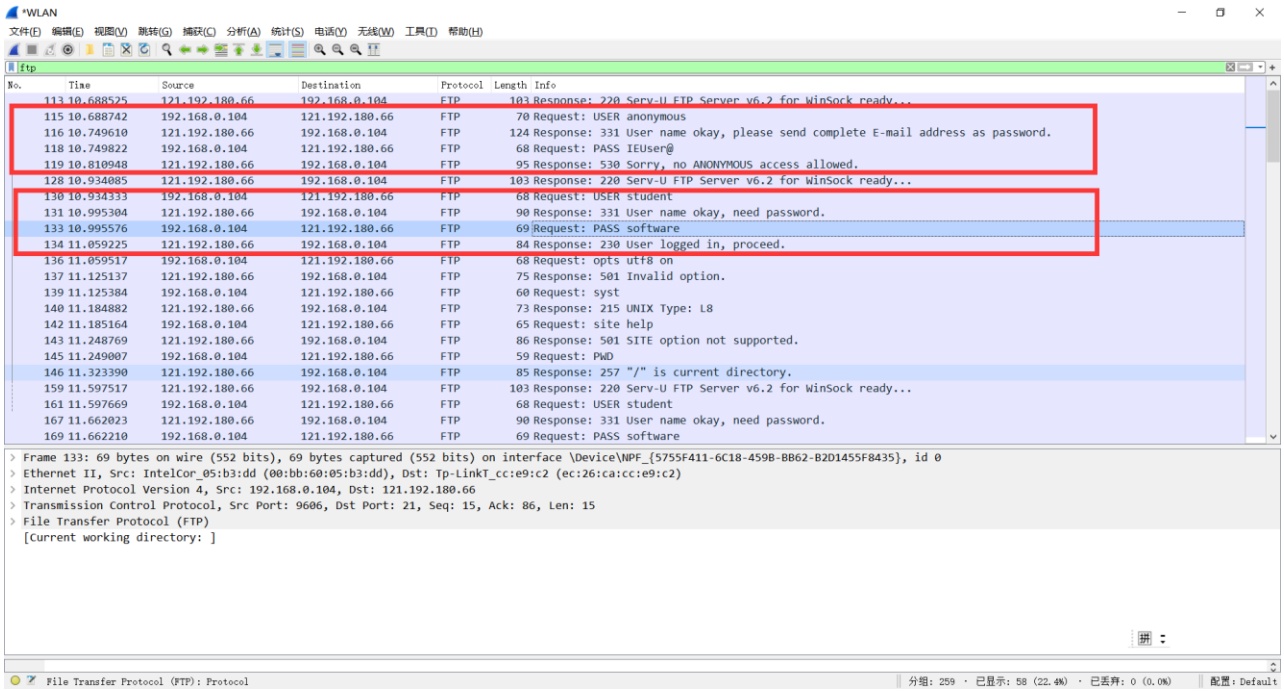
拥塞窗口：cwnd　　拥塞的标志：重传计时器超时，连续收到 3 个冗余 ACK



四次挥手如下[FIN,ACK]、[ACK]、[FIN,ACK]、[ACK]信号：

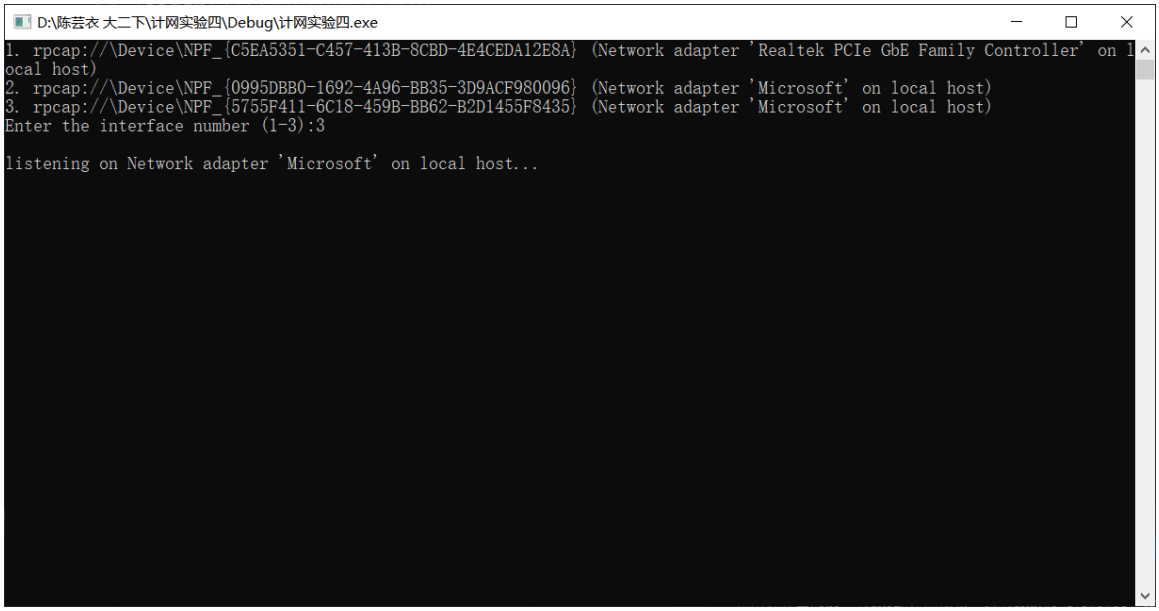


用 Wireshark 侦听并观察 FTP 数据（过滤器过滤 得到 ftp 数据）：登录名以“USER”开头，口令以“PASS”开头，可提取用户名和密码。登录成功以“230”开头，登录失败以“530”开头，以此判断登录是否成功。

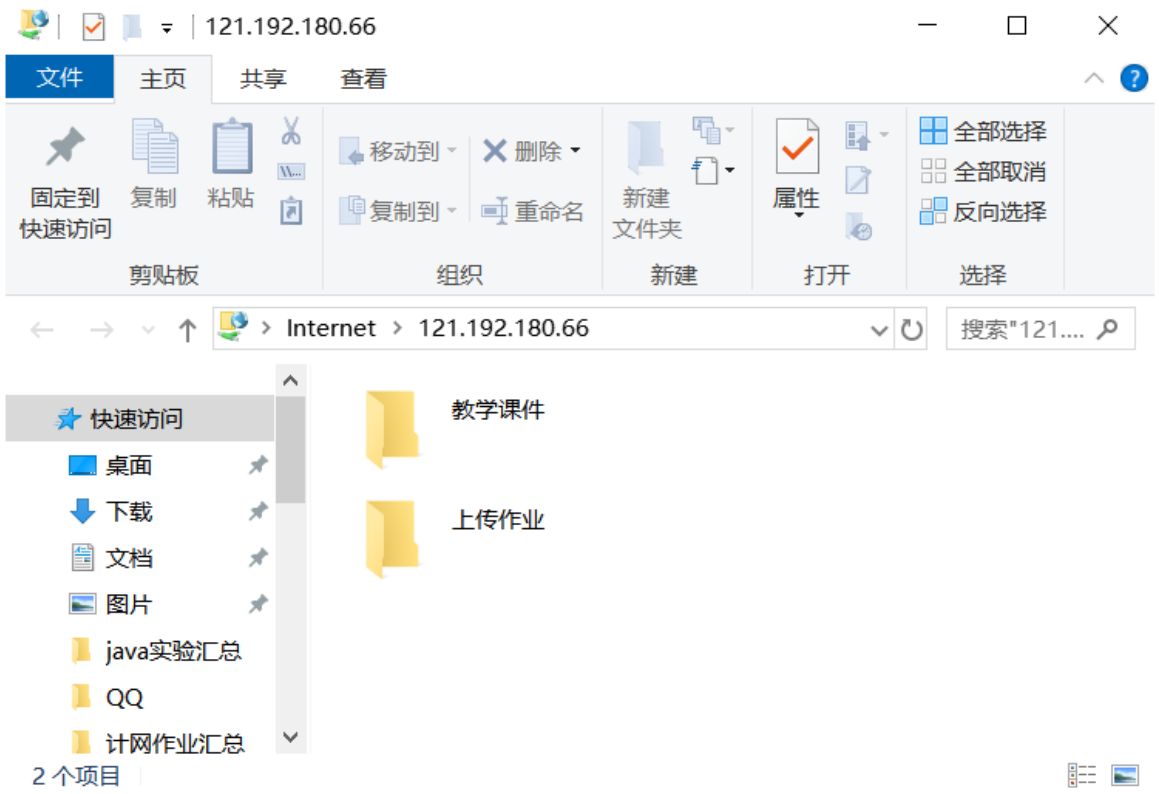


基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流：

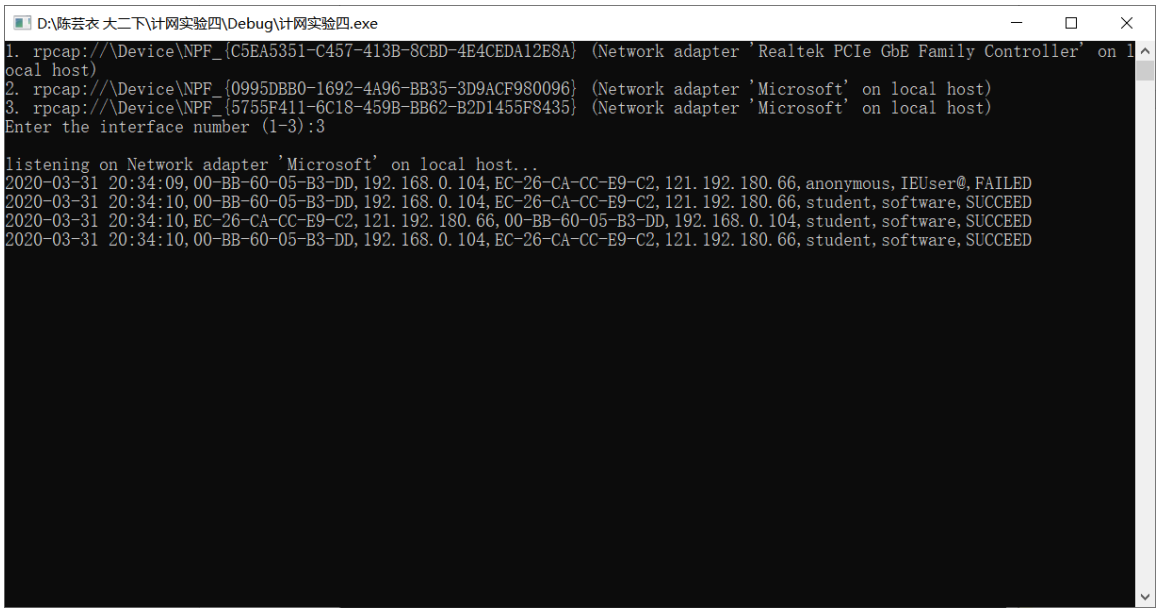
运行程序，选择接口：



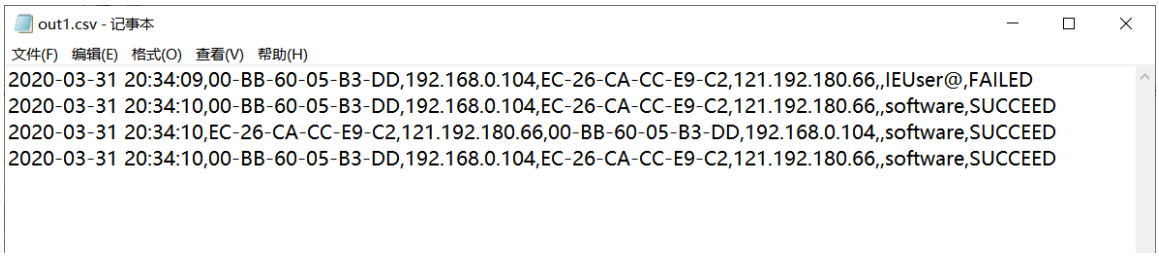
登录 FTP：



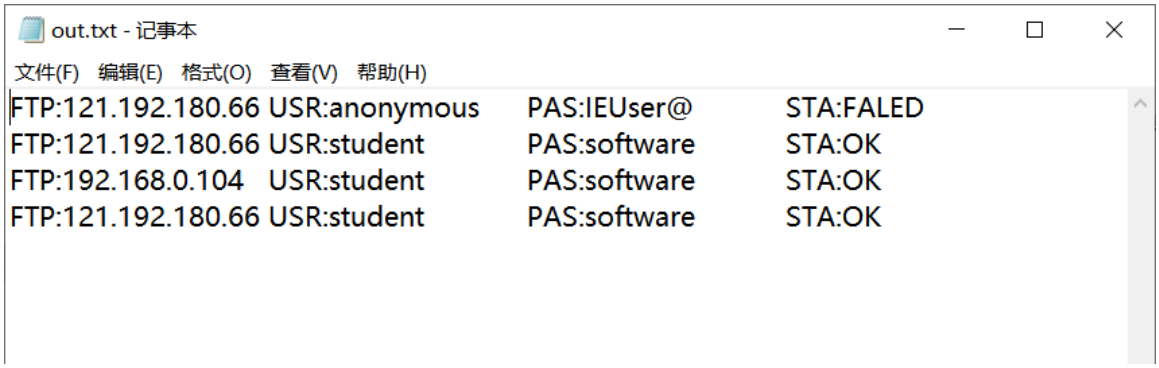
监听 FTP 数据流:



Out.csv:



以 “FTP USER PAS STA ”格式输出：



4 实验总结

通过本次实验对 TCP 数据段有了更直观深刻的理解，学会在 wireshark 中用过滤器过滤数据，分析其建立连接的三次握手和撤销连接的四次挥手信号。学会用 wireshark 侦听并观察 ftp 数据，提取用户名、密码，观察登录成功情况。编写程序实现了监听网络上的 FTP 数据流。