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 1 班

姓　　名 周宇

学　　号 24320182203335

实验时间 2020 年 3 月 31 日

2020 年 3 月 31 日

1 实验目的

侦听并观察 TCP 数据段和 FTP 数据

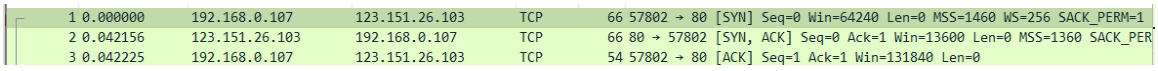
2 实验环境

Windows10 wireshark winpcap

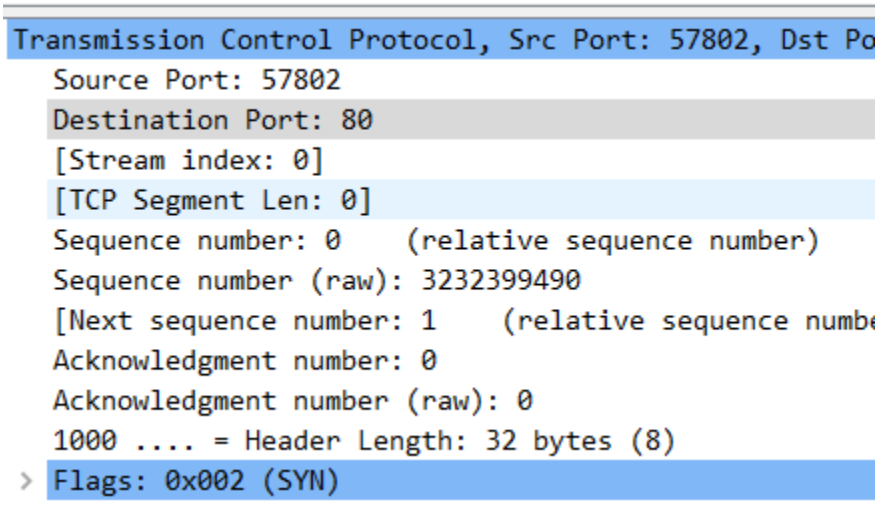
3 实验结果

用 WireShark 侦听 TCP 数据段

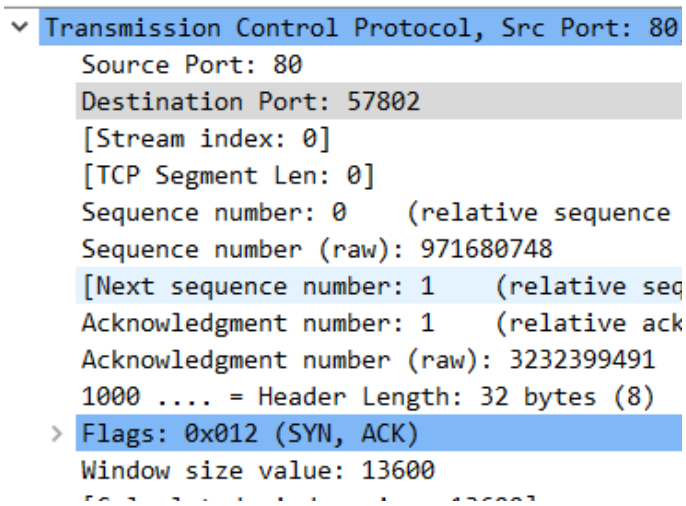
TCP 的三次握手建立连接



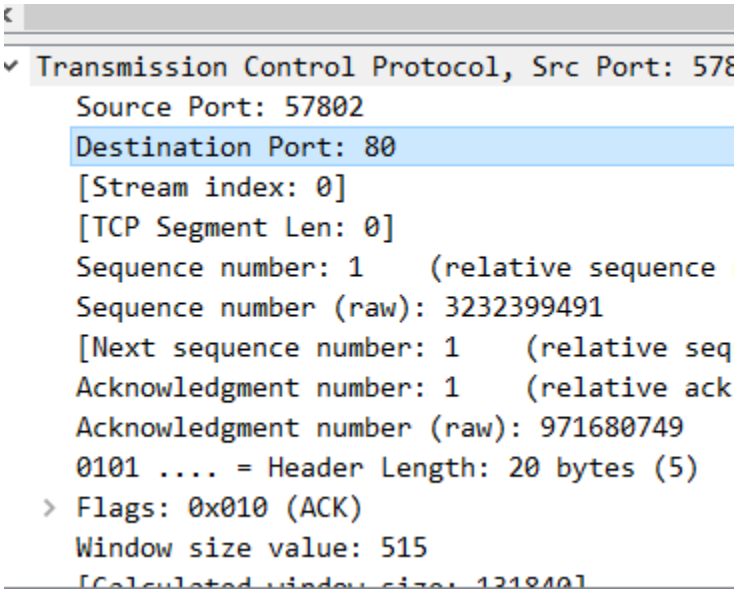
第一次握手：客户端发送一个 TCP，标志位为 SYN，序列号为 0



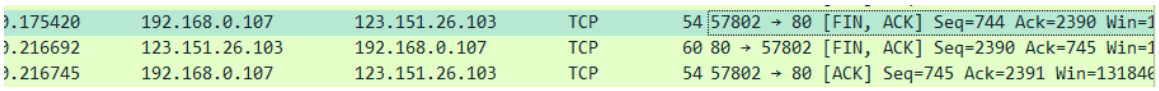
第二次握手：服务器发回确认包, 标志位为 SYN,ACK. 将确认序号设置为客户的 I S N 加 1（0+1=1）



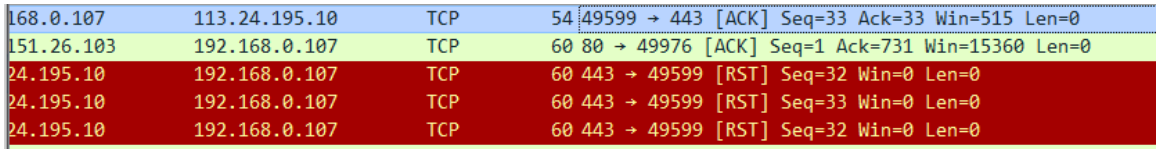
第三次握手：客户端再次发送确认包 SYN 标志位为 0,ACK 标志位为 1.



TCP 理论上四次挥手断开连接（只抓到 3 个，百度：因为服务器端在给客户端传回的过程中，将两个连续发送的包进行了合并）

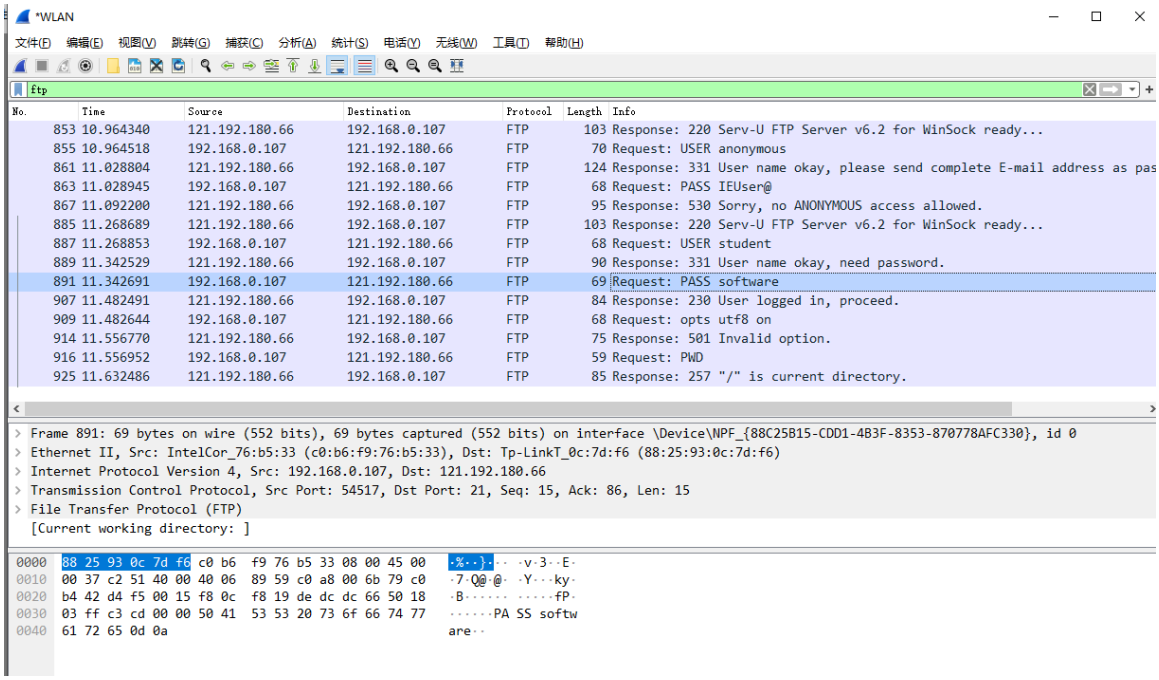


TCP 的窗口机制和拥塞控制机制：



零窗口暂停数据流，直到收到服务端的窗口更新，告知大小已经增加了才继续接收数据。

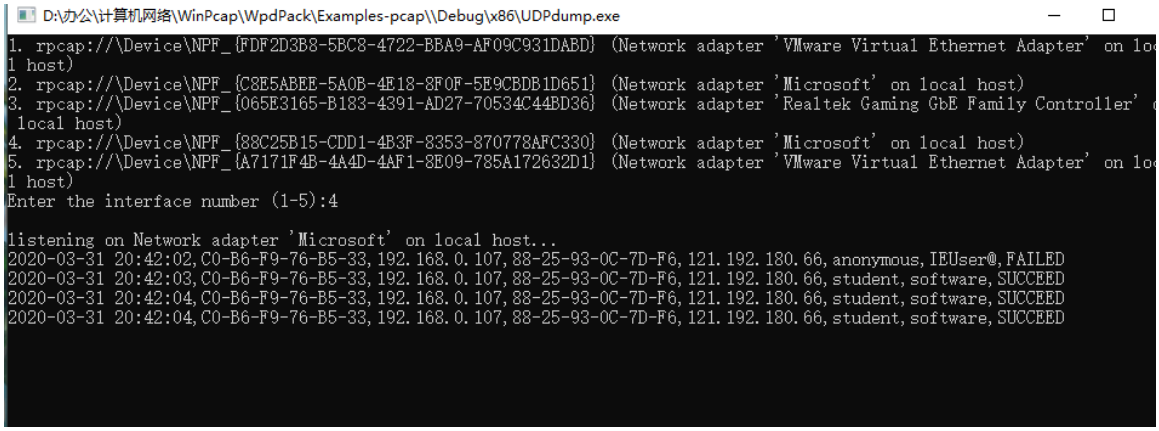
用 Wireshark 侦听 FTP 数据



用户名前为 USER，中间为用户名，后面为 0d0a（回车换行）

密码前为 PASS，中间为密码，后面为 0d0a

提取：匹配 USER/PASS 和 0d0a 之间的



4 实验总结

通过实验对 TCP 报文的握手协议以及滑动窗口机制和拥塞控制有了理解，了解到服务器以稳定速率传输的原理；对 FTP（学院）的侦听和分析，获取到了内容，观察得到了用户名和密码的获取方法及其他信息。搭建了本地的 FTP 但在设置用户名和密码的时候由于系统问题（不支持本地用户和角色的更改）导致无法侦听到信息。