

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验3 用PCAP库监听并分析网络流量**

**班　　级 软件工程2018级1班**

**姓　　名 王奕飞**

**学　　号 24320182203286**

**实验时间 2020年3月25日**

**2020 年 3 月 25 日**

# 实验目的

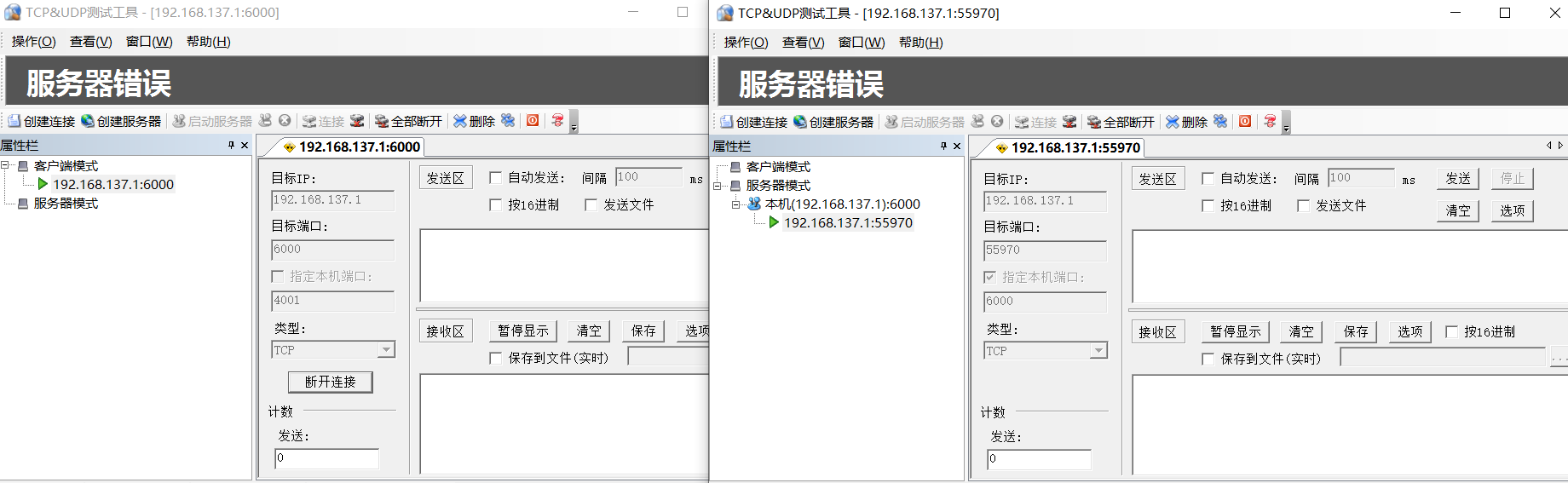
# 实验环境

Visual studio 2017

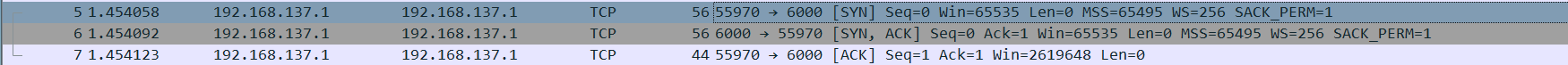
# 实验结果

1. 观察TCP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

通过TCP&UDP测试工具 在本机上分别建立服务器和客户端，并进行连接



三次握手连接：



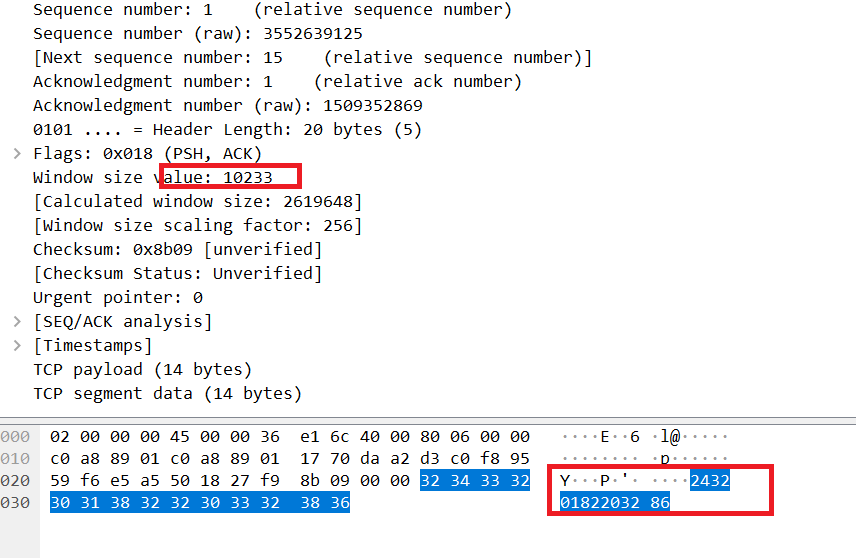
第一次握手，客户端发送一个TCP，标志位为SYN=1

第二次握手，服务器向客户端返回一个数据包，SYN=1，ACK=1

第三次握手，客户端收到服务器发来的包后检查确认序号。若正确，客户端会再向服务器端发送一个数据包，SYN=0，ACK=1

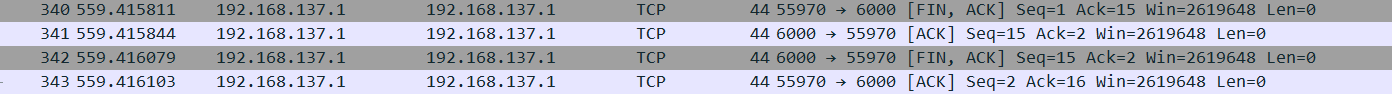
发送24320182203286

捕获到这一帧



捕获到内容，红框内分别为窗口的大小和发送的内容

断开连接



四次挥手断开连接

第一次挥手：客户端给服务器发送TCP包，用来关闭客户端到服务器的数据传送。将标志位FIN和ACK置为1

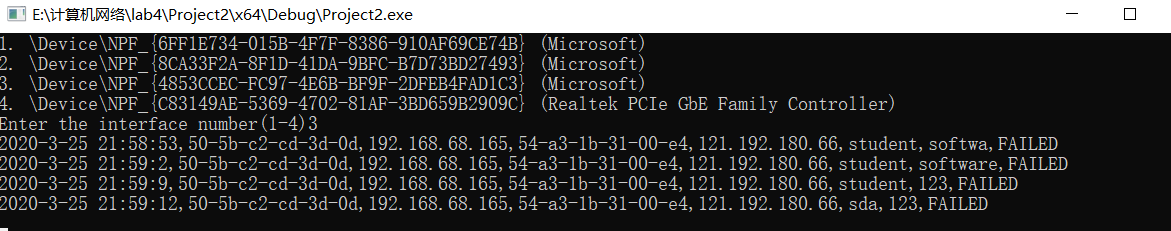
第二次挥手：服务器收到这个FIN，发回一个ACK，seq=收到的ACK+1，ACK=收到的FIN

第三次挥手：服务器关闭与客户端的连接，发送一个FIN给客户端

第四次挥手：客户端发回ACK报文确认。

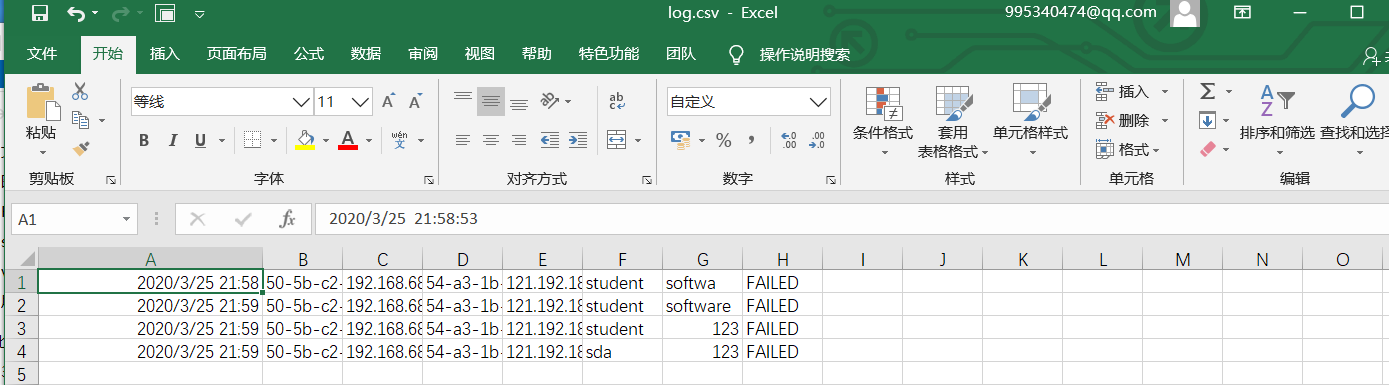
（2）。基于 WinPCAP 工具包制作程序，实现监听网 络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

选择端口并且对ftp进行解析



主要方法就是暴力搜索 对每一个ftp的数据包，搜索是否有USER 或者 PASS这几个字母，匹配到，则后面就是对应的用户名和密码

输出到csv文件



# 实验总结

对tcp的头部有了一个更清晰的了解，以及对于tcp/ip协议的三次握手，四次挥手的过程认识更加清晰。FTP的报文头，以及各个格式理解更加深刻