

****

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**

**姓 名 杨浩然**

**学 号 24320182203309**

**班 级 软件工程2018级2班**

**实验时间 2020年3月26日**

**2020 年 3 月 26 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。将该过程截图在报告中。

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，

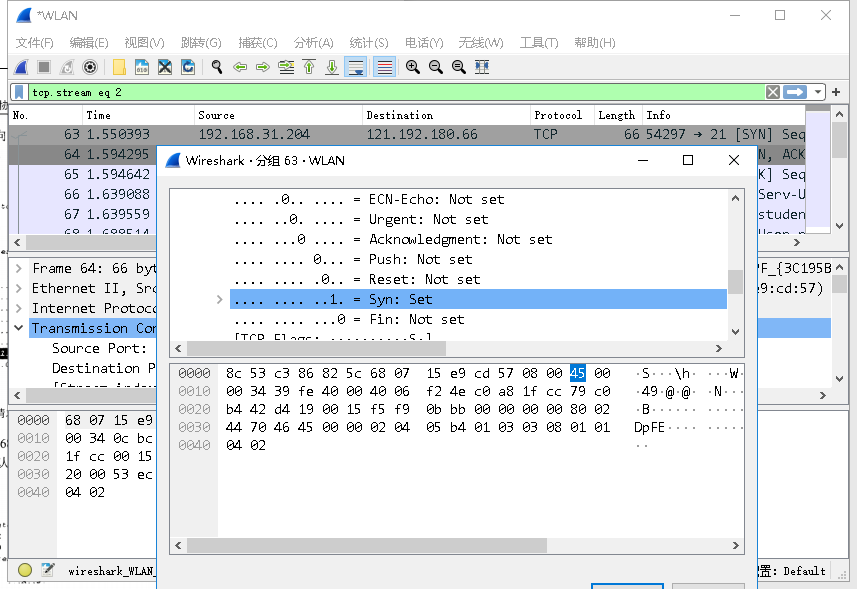
再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

# 实验环境

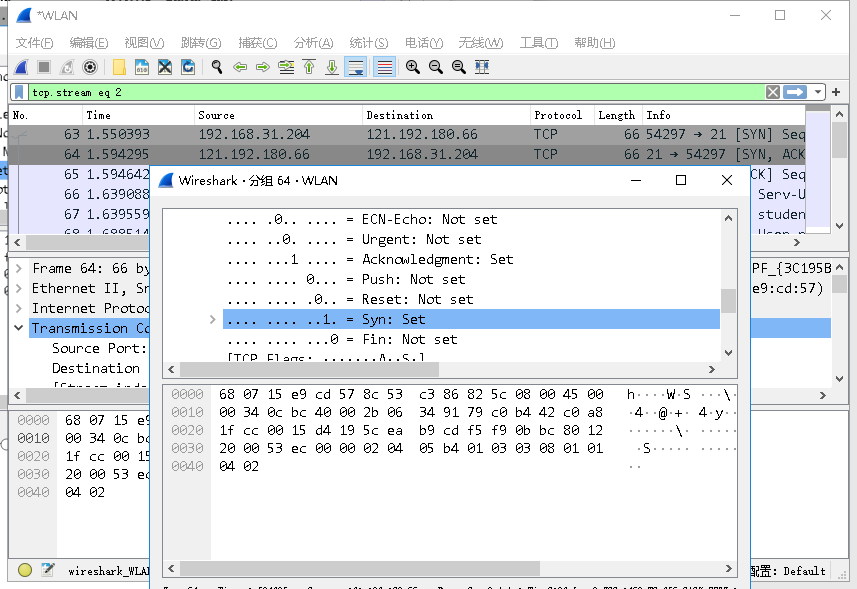
Win10，C++。

# 实验结果

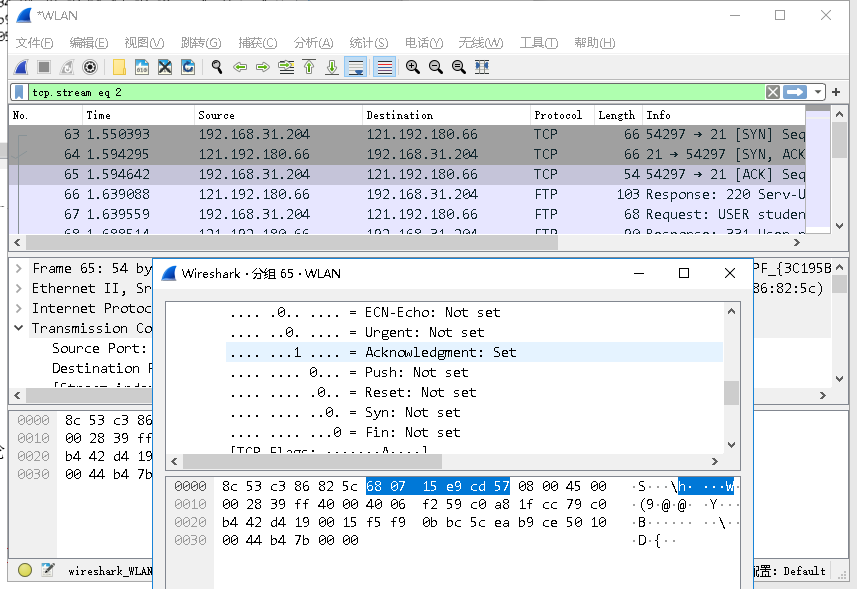
第一个数据包是本机192.168.31.204向FTP发送连接请求，标志位中只有Syn



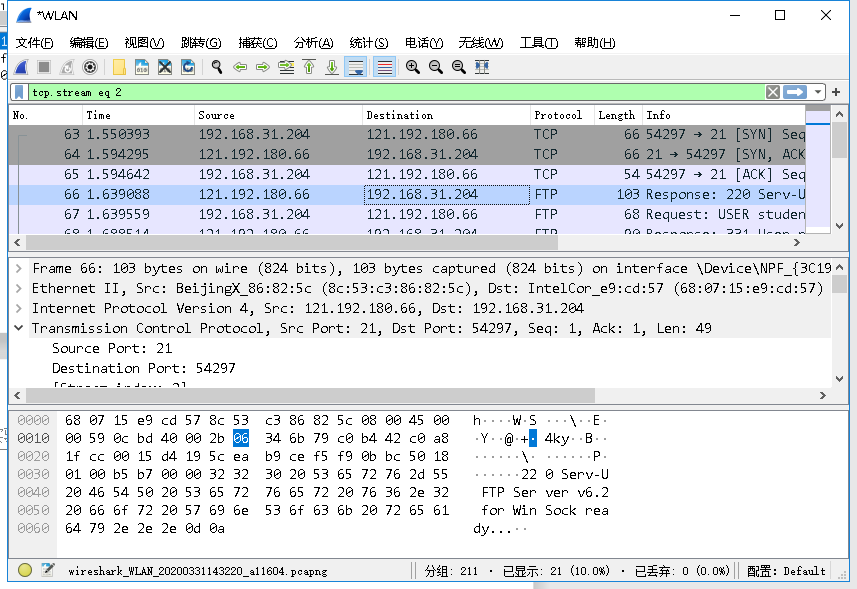
第二个数据包是FTP服务器发来的握手信号，里面有同步位和确认位



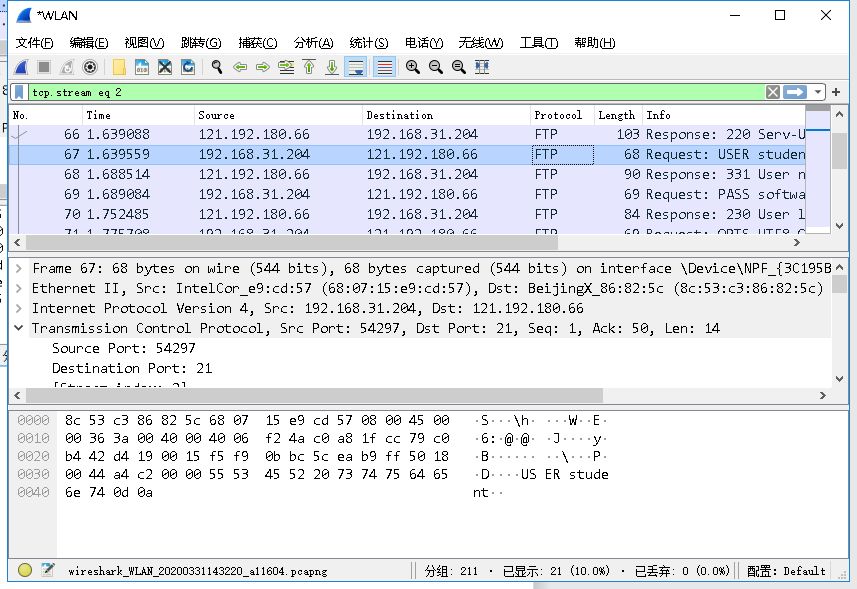
第三个数据包是本机发出的，里面只有一个确认位，也就是做再次确认



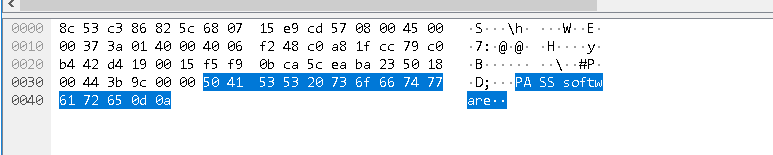
第四个数据包是FTP服务器发来的欢迎语句



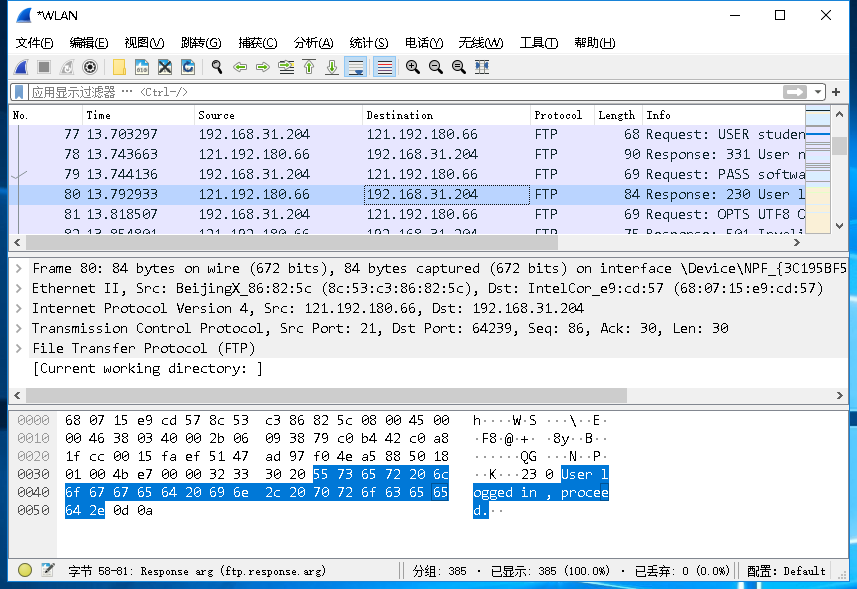
第五个数据包中含用户名



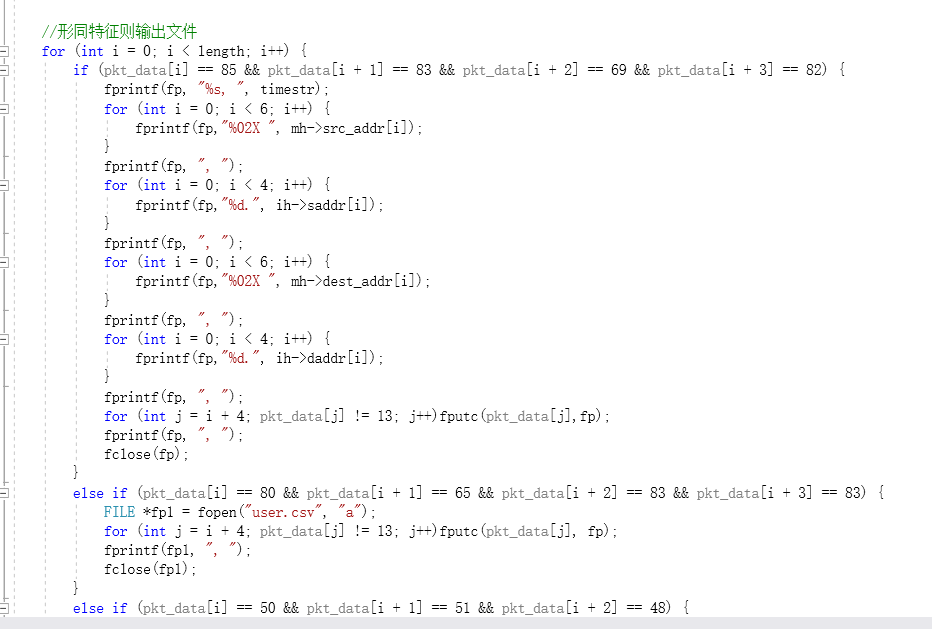
第七个数据包中含密码



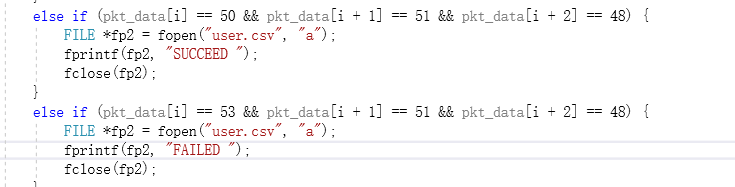
如果登陆成功则以230开头



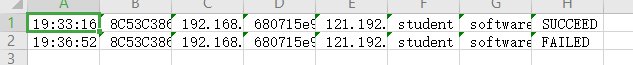
找到用户名及密码前分别有USER和PASS，通过遍历每个包的内容进行筛选



出现230则成功登入，530则失败登入。以数据ASCLL码值对应



得到结果



# 实验总结

TCP建立过程分为三次握手，第一次是客户端发起连接，客户端TCP发送一个

Syn同步记号，申请和服务器连接。

第二次是服务器确认了客户端的Syn，发送Acknowledgement记号和一个Syn同步记号。

第三次是客户端确认服务器的Ack和Syn记号，向服务器发送Ack，成功建立连接。

每次传输的TCP数据包中格式都如版本号4位，数据包头部长度4位，服务类型8位，总长16位，重组标识16位等。最后才是用户数据。