

****

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**

**姓　　名 张浩然**

**学　　号 24320182203323**

**实验时间 2020年3月31日**

**2020年4月4日**

# 实验目的

了解TCP协议和FTP协议的报文特征

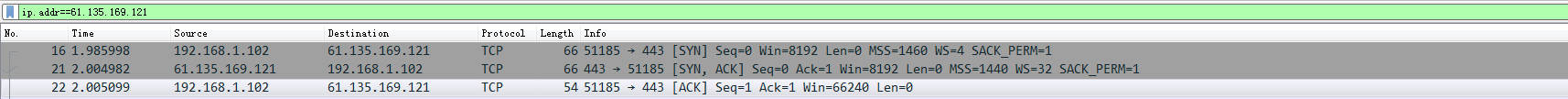
# 实验环境

Windows NT ,Visual Studio, Winpcap, Wireshark

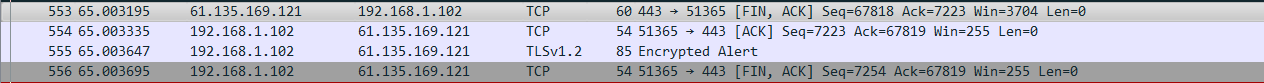
# 实验结果

1. Wireshark侦听

建立连接的过程（三次握手）：

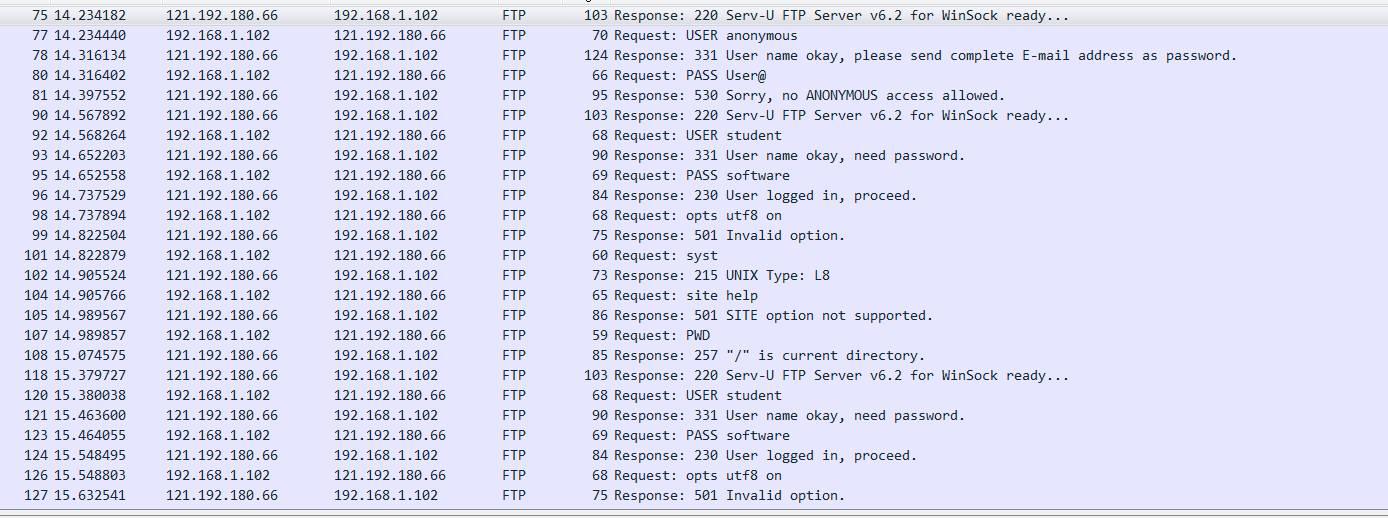


连接撤销的过程（四次挥手）：

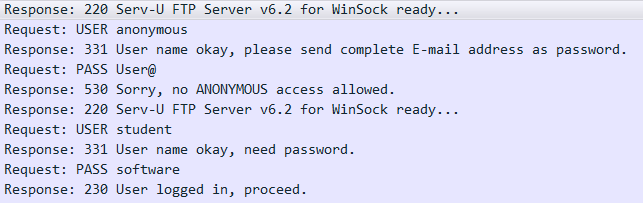


（貌似是服务器主动与浏览器撤销了连接，所以只看到了两次相关联的数据包，且有一次发生了重复）

观察FTP连接过程：



与登录有关的上下文：

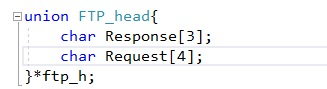


提取到有用信息——Request：USER后跟用户名，PASS后跟密码；

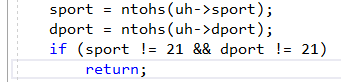
Response：230成功，530失败

1. 编写程序

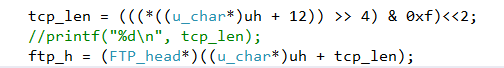
定义一个联合，用于提取状态码



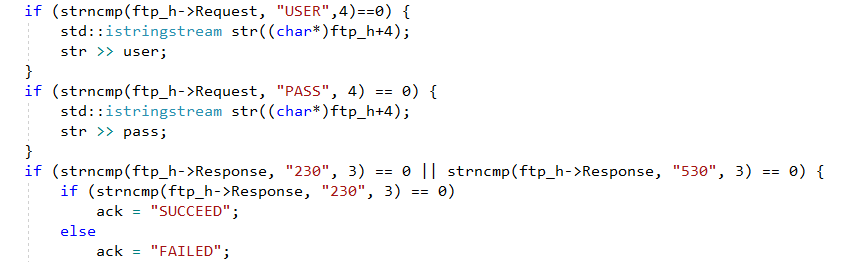
通过端口过滤FTP数据包



获取TCP段长度，并依据偏移找到FTP头

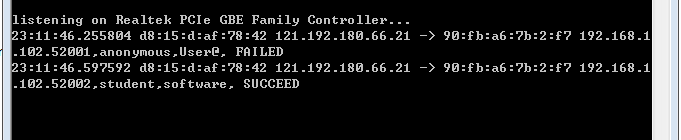


根据关键字分析连接状态并记录登录信息



当收到Response时输出user 和pass

运行结果：



源码上传至Github.

# 实验总结

开始计算TCP长度时忘记是以4字节为一个单位了

****