

****

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 卜英乔**

**学　　号 24320182203164**

**实验时间 2020年3月24日**

**2020 年 3 月 31 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。

# 最终在文件上输出形如下列 CSV 格式的日志：

# 时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否

# 2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7DD5-72,192.168.33.2,student,software,SUCCEED

# 2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7DD5-72,192.168.33.2,student,software1,FAILED

# 实验环境

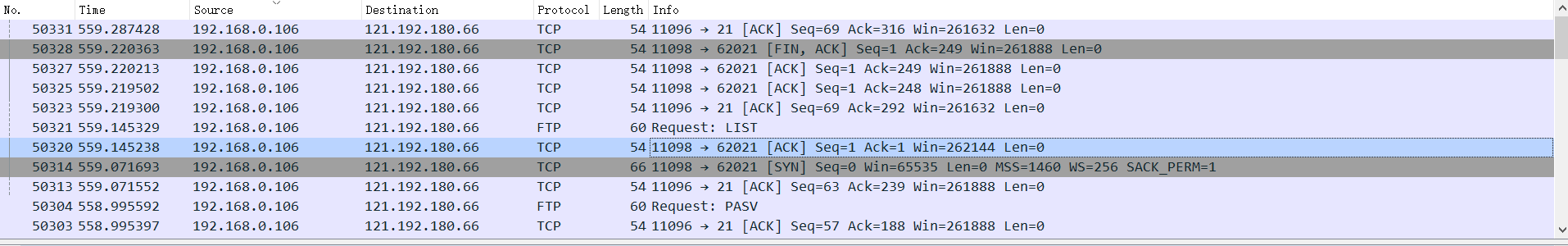
操作系统：WIN10

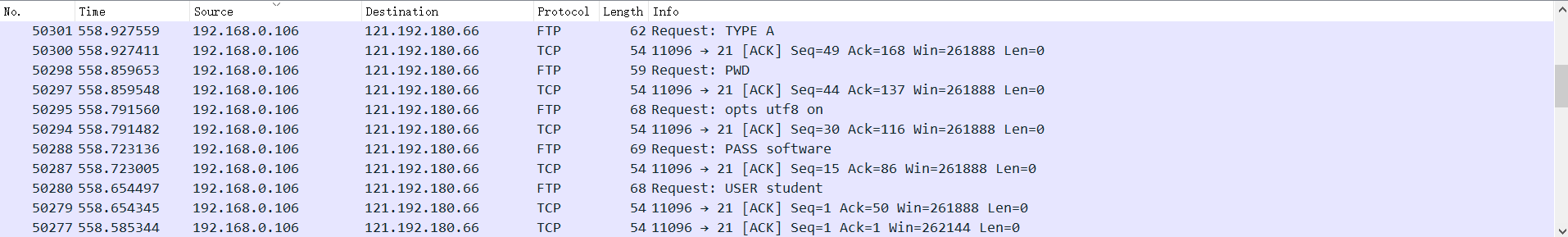
运行环境： winpcap包、visual studio

编程语言：C++

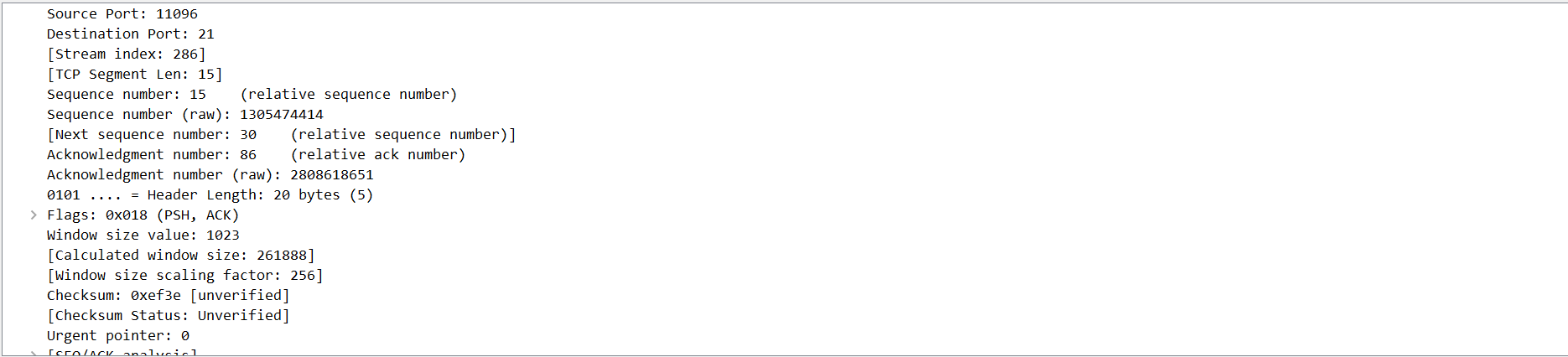
# 实验结果

主机先向FTP服务器发送连接请求，SYN=1,seq=0服务器回复ACK，再次确认连接，本机再次向ftp发送ACK, ACK=1,ack=1,seq=1



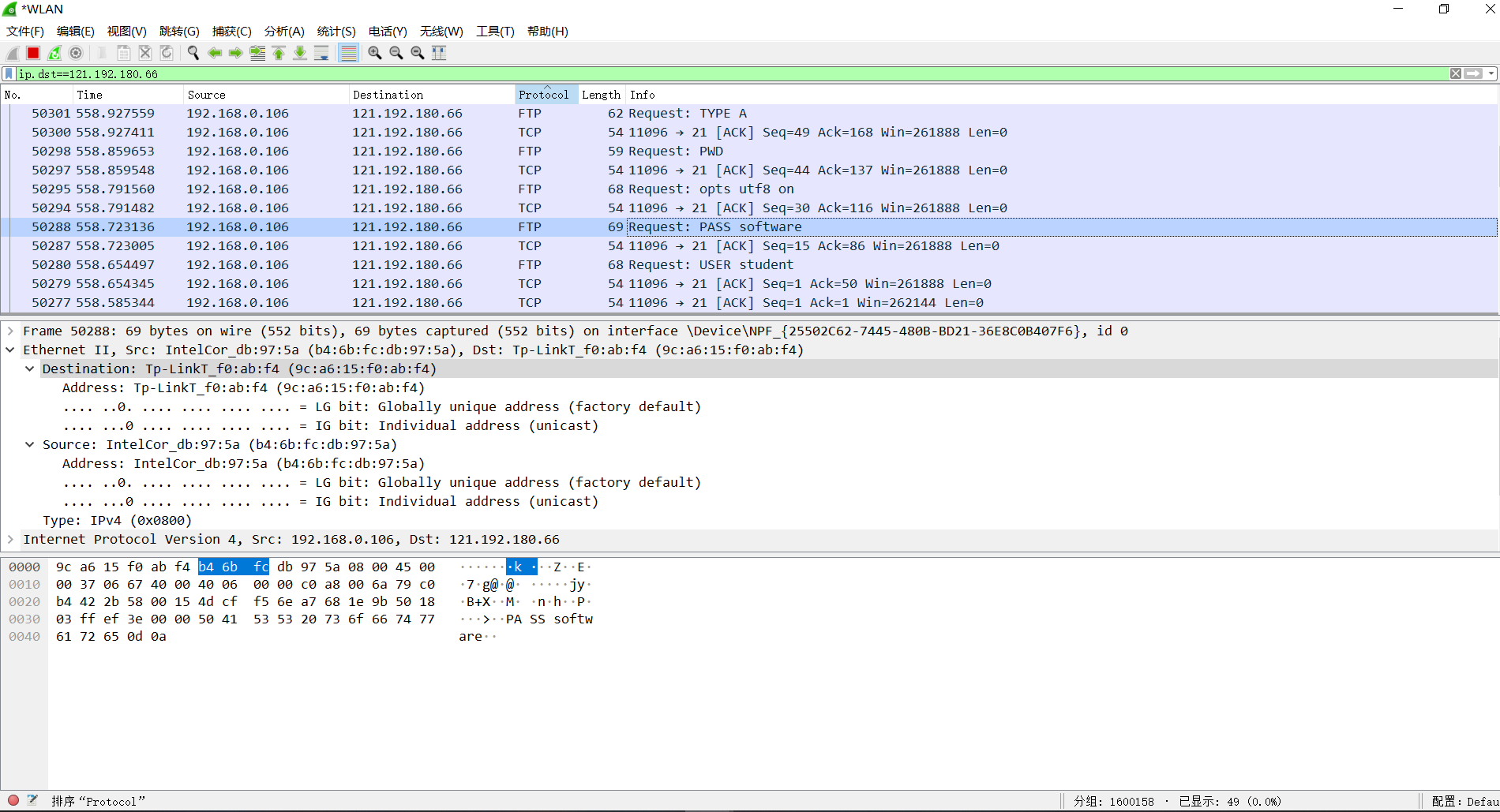


连接的撤除，先给ftp服务器发送FIN=1,seq=69,ack=316,服务器回复ACK, ACK=249, seq=69,此时由于没有数据要传输，客户端给服务器发送一个FIN=1, ACK=1, seq=69, ack=249,在这之后服务器继续给客户发送ACK, ACK=1, seq=249, ack=69,然后连接撤除。



报文段由源端口号+目的端口号+发送数据序列号+确认序列号+标识符+保留位+校验和+报头长度+可选项组成。

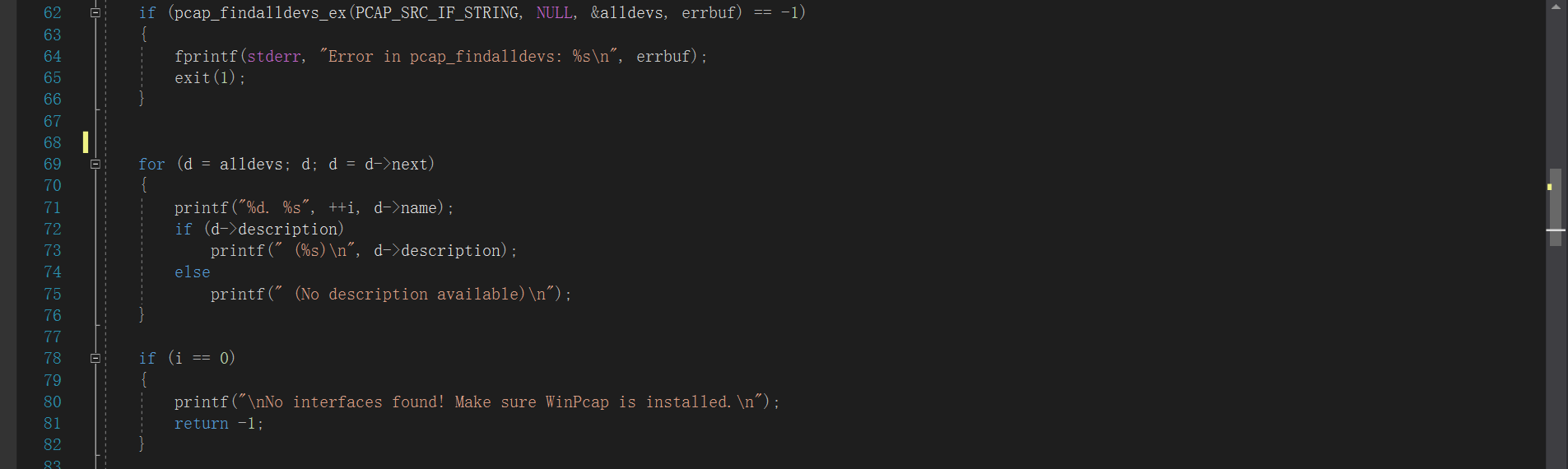
用Wireshark侦听FTP数据，登陆学院FTP，报文特征：



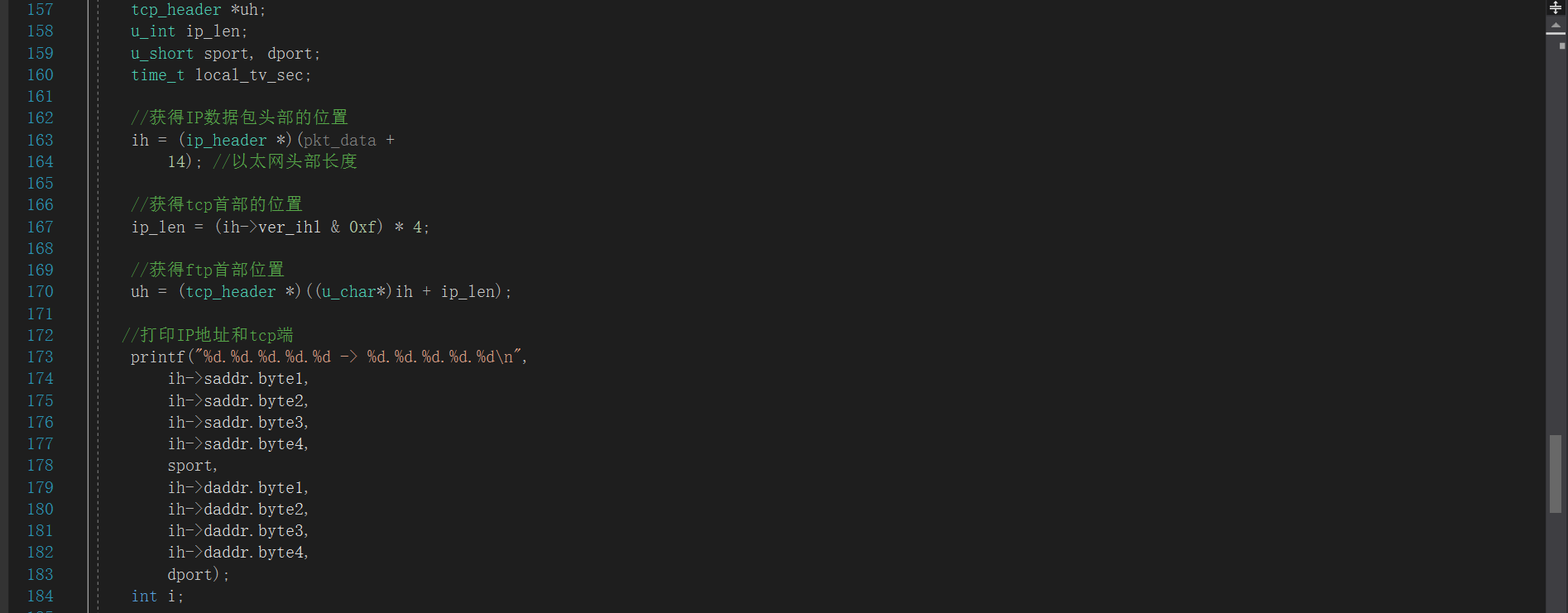
FTP登陆的时候先发送用户名，然后服务器提示用户名正确需要密码，然后再发送密码，如果密码正确，服务器返回状态码，则登陆成功，如果服务器返回提示，则登陆失败。

使用winpcap编程

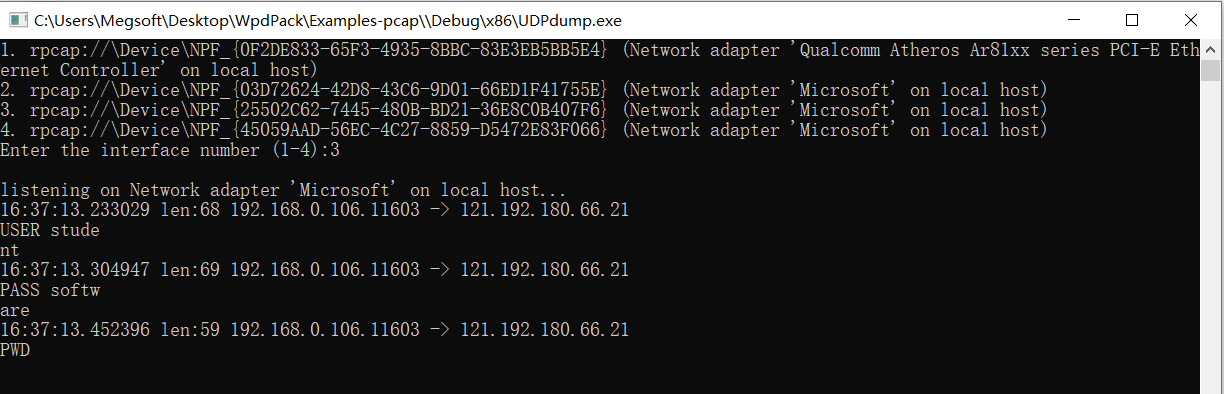
获得设备列表，并打印设备



获取IP、TCP、FTP位置



最终结果如图，登录学院的ftp：



# 实验总结

实验中了解TCP三次握手和四次断开连接之间的关系。三次握手的目的是建立可靠的通信信道，说到通讯，简单来说就是数据的发送与接收，而三次握手最主要的目的就是双方确认自己与对方的发送与接收机能正常。