

****

软 件 学 院

《计算机网络》实验报告

**题　　目 用WinPCAP监听并解析FTP命令**

**姓　　名 陈奕培**

**学　　号 22920202202879**

**班　　级 计网2班**

**实验时间 2022/4/15**

**2022 年 4 月 15 日**

# 实验目的

通过捕获并解析 FTP 连接的建立于与断开过程的数据帧，达到以下目的：

熟悉并学会分析 TCP 连接的建立、断开过程；

熟悉常见的 FTP 命令，熟悉并学会分析 FTP 连接的建立、断开过程；

掌握使用代码实现解析以太网数据帧的技能，提高编码能力。

# 实验环境

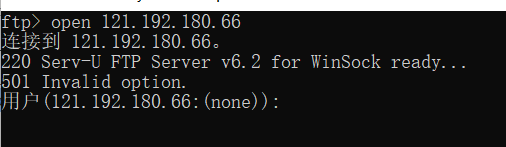
操作系统：Win11

编程语言：C++

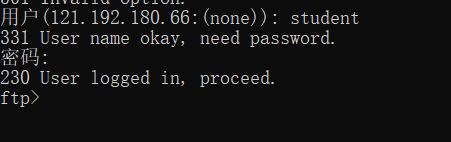
# 实验结果

**-2（接下来的操作全部基于该步）**

（1）open 121.192.180.66



（2）输入用户名和密码



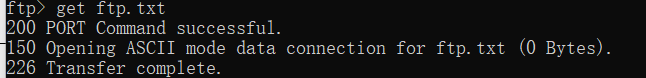
（3）lcd指定本地文件夹



（4）cd进入指定文件夹



（5）get下载内容



（6）quit退出

（7）查看结果

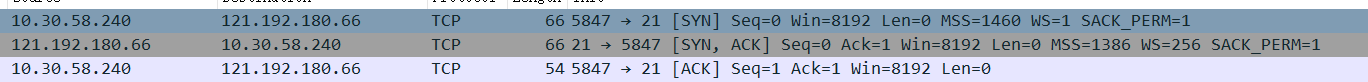


**-1**

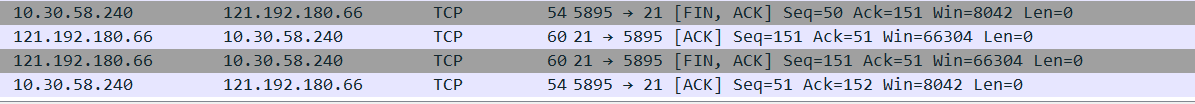
设定过滤条件，重复-2的打开和关闭操作



输入open时，Wireshark抓到的3次握手包



输入quit时，Wireshark抓到的4次挥手包

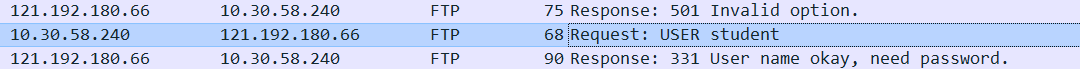


**0**

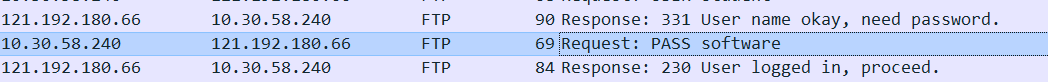
设定过滤条件



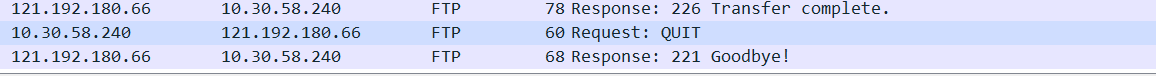
USER指令



PASS指令



QUIT指令



**1**

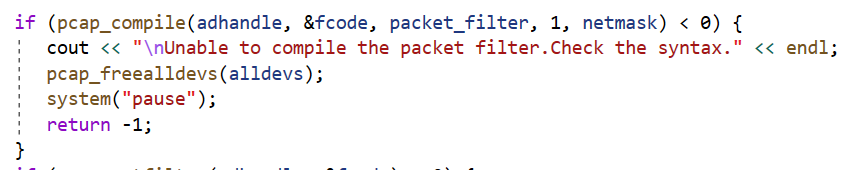
设置过滤条件，使用pcap库给的函数过滤，或使用自己的代码过滤

（1）使用库的函数过滤

过滤条件

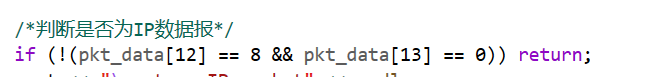


设置过滤

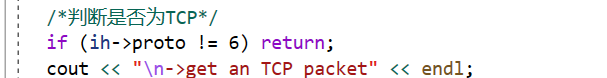


（2）自己的代码过滤

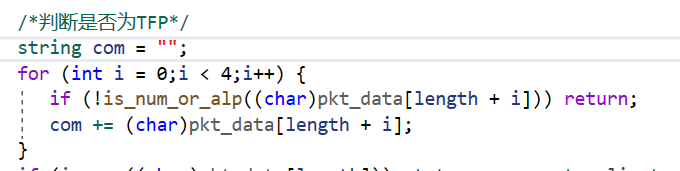
第一层，通过帧的类型是否为0800，过滤出IP数据报



第二层，通过IP报头的协议类型，判断是否为TCP



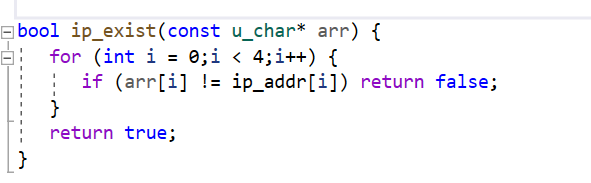
第三层，当TCP头后紧接的四位数据是字母、数字或空格，可认为它是FTP数据，用com来记录指令或回应的类型



**2**

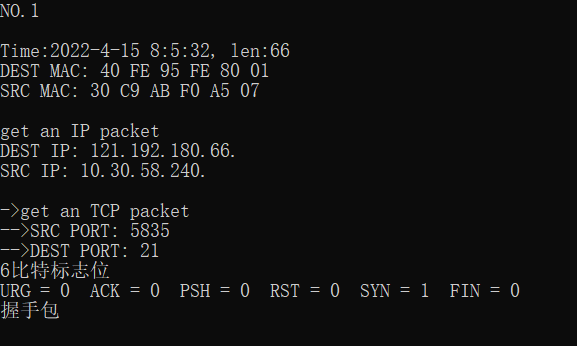
通过函数比对设定的IP地址，来过滤指定IP地址



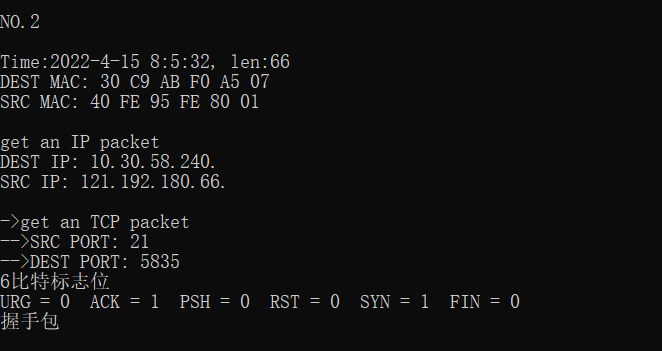


登录FTP时，捕获到三个握手包

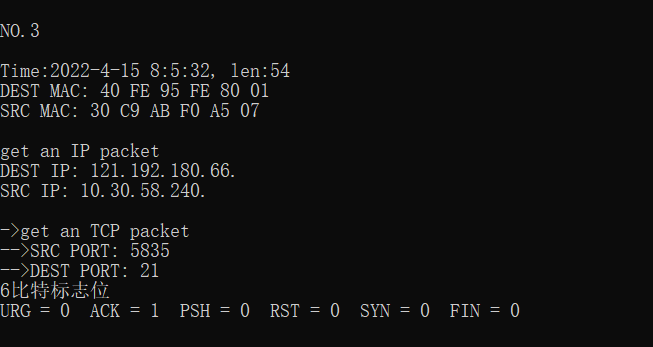
（1）本机to 121.192.180.66，SYN = 1



（2）121.192.180.66 to本机，SYN = 1，ACK = 1

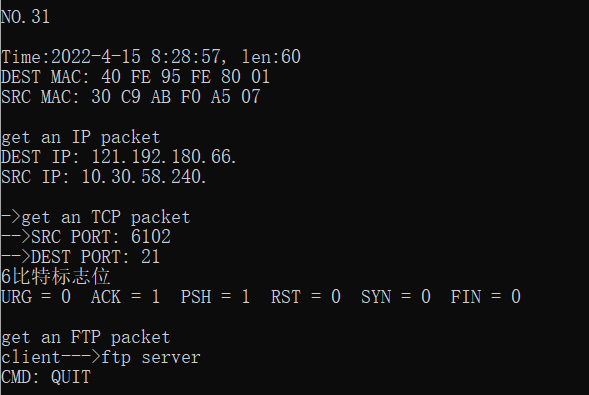


（3）本机to 121.192.180.66，ACK = 1

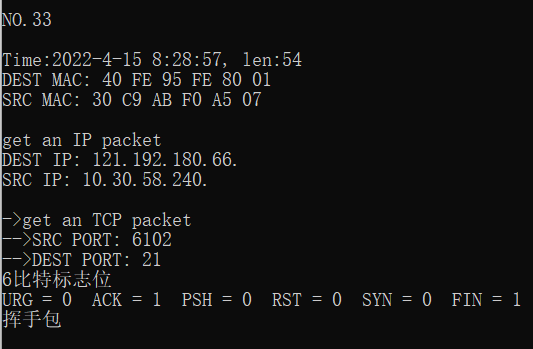


输入QUIT时，捕获到四个挥手包

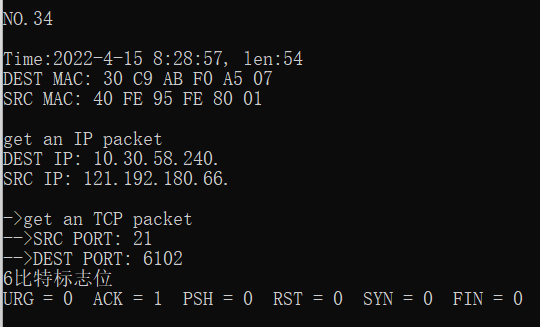
（1）输入quit指令

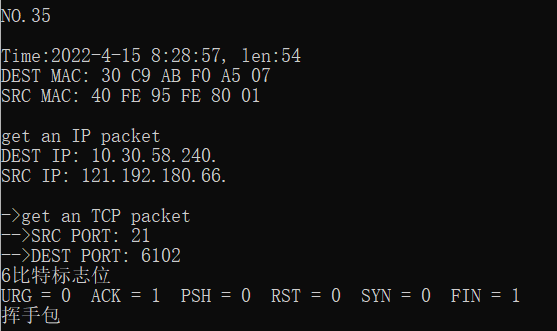


（2）本机 to 121.192.180.66，发送一个ACK = 1，FIN = 1的挥手包，对上一个包的确认有效，申请断开连接

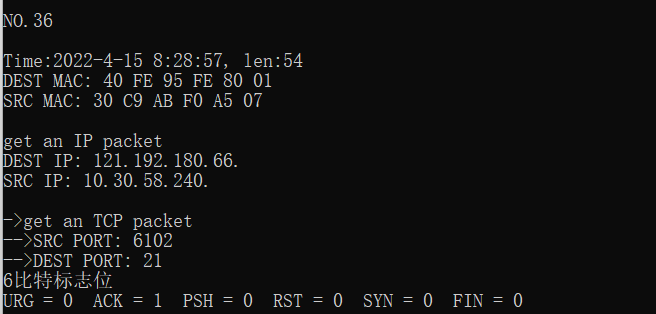


（3）121.192.180.66 to 本机，发送一个ACK = 1确认包和一个ACK = 1，FIN = 1的挥手包



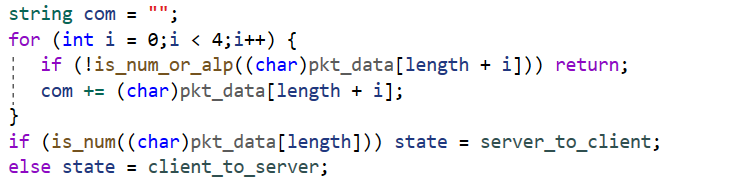


（4）本机 to 121.192.180.66，发送最后一个确认包

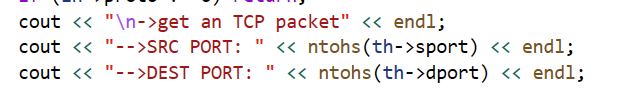


**3**

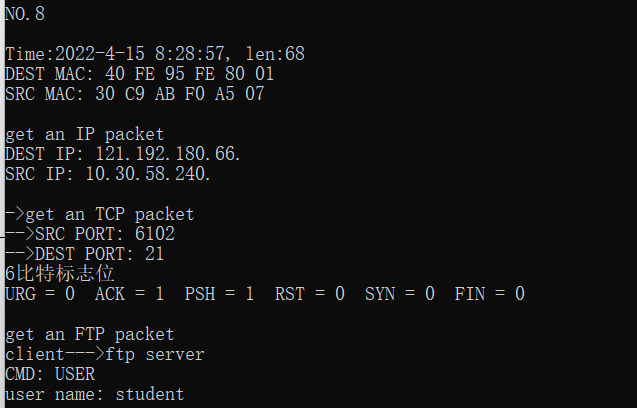
（1）通过1中过滤时得到的com是字母还是数字来判断该条报文是client的指令还是sever的回应



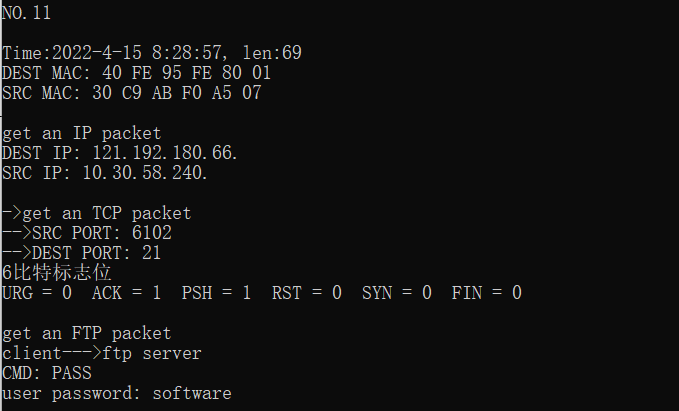
通过TCP头部的端口来得到端口号



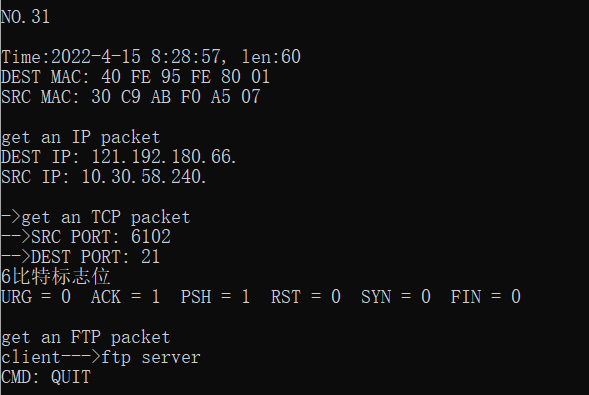
USER命令



PASS命令

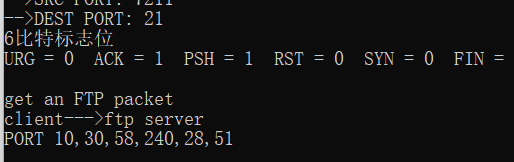


QUIT命令

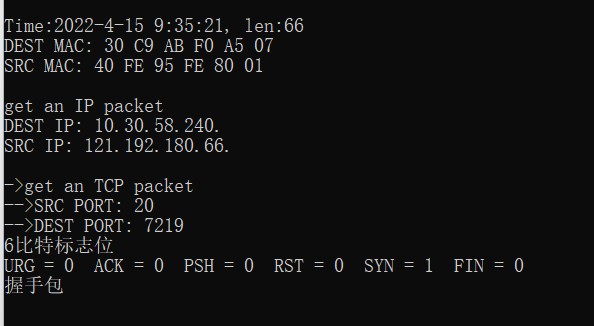


（2）由上面可得出指令是在server的21端口和client的6102端口进行的

当数据传输的时候，client发送一个端口号



由server to client重新建立了一个连接



使用的是server的20端口和client的7219端口

# 实验总结

掌握了以命令行登录FTP的方式

对IP数据报和TCP数据的头部更加了解

在传输FTP之前需要先建立TCP连接，结束时会断开TCP连接

TCP的三次握手、四次挥手的过程，以及其标志位的作用和含义

FTP的指令传输的端口和数据传输的端口不是同一个