

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　基于 PCAP 库侦听并分析网络流量**

**班　　级 软件工程2019级4班**

**姓　　名 郑志豪**

**学　　号 22920192204336**

**实验时间 2021年6月05日**

**2021 年 6 月 05 日**

填写说明

1. 本文件为Word模板文件，建议使用Microsoft Word 2019打开，在可填写的区域中如实填写；
2. 填表时，勿破坏排版，勿修改字体字号，打印成PDF文件提交；
3. 文件总大小尽量控制在1MB以下，勿超过5MB；
4. 应将材料清单上传在代码托管平台上；
5. 在学期最后一节课前按要求打包发送至cni21@qq.com。

# 实验目的

通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。 掌

握用 Wireshark 观察网络流量并辅助网络侦听相关的编程； 掌握用 Libpcap 或

WinPcap 库侦听并处理以太网帧和 IP 报文的方法；熟悉以太网帧、 IP 报文、 TCP

段和 FTP 命令的格式概念， 掌握 TCP 协议的基本机制； 熟悉帧头部或 IP 报文头

部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各字段和 FTP

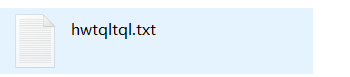
控制命令的指令和数据的含义。

# 实验环境

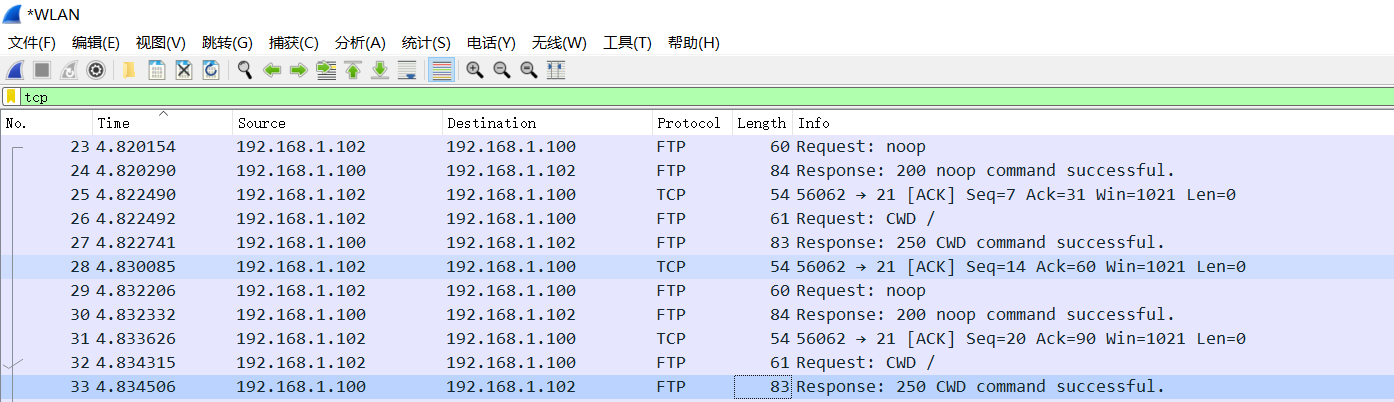
Windows10

C语言

# 实验结果

实验文件操作：在本机搭建一个<ftp://192.168.100的服务器后，在局域网内用IP为192.168.102>的客户端上传文件

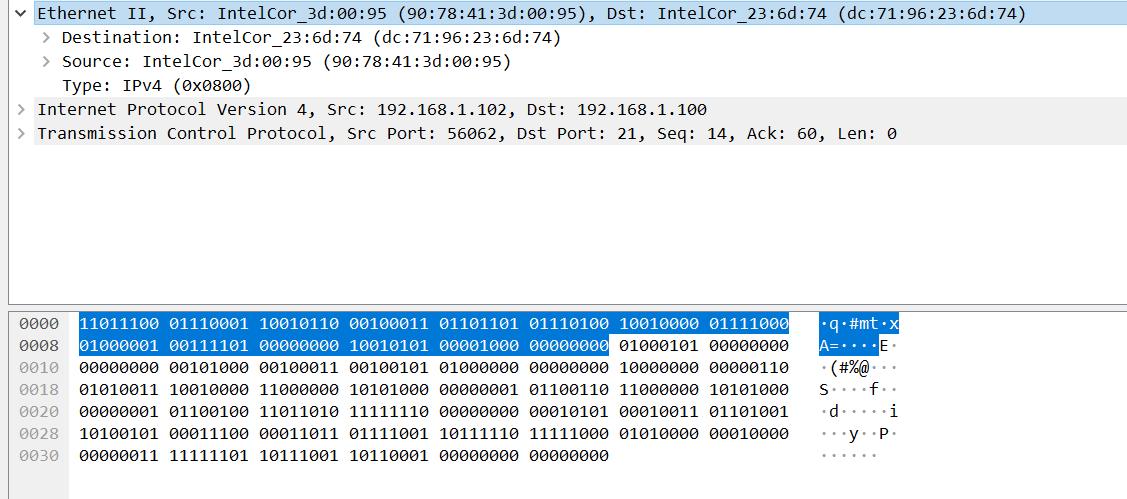
用wireshark侦听并获取报文

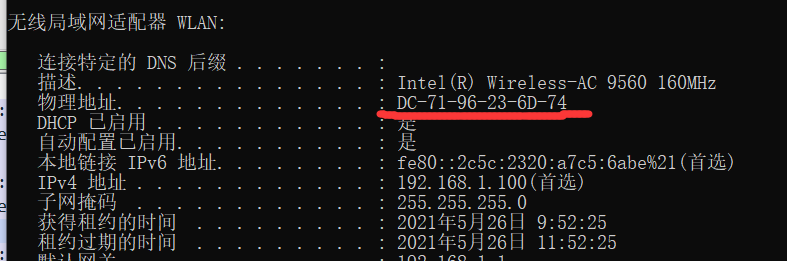


1. 用侦听解析软件观察数据格式。

随意点开一个TCP报文查看格式：

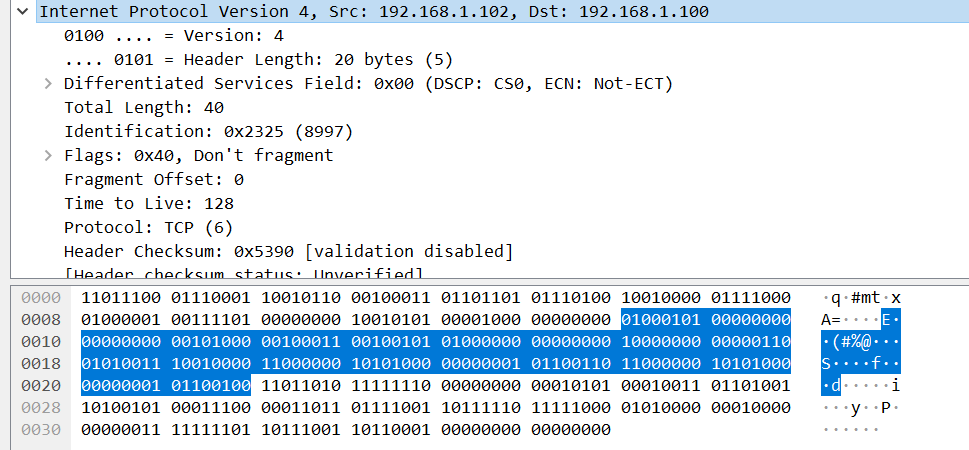
1）MAC帧格式，前6字节为目的地址（本机mac地址），再6字节为源地址，再2字节为类型说明（IPV4）





（图） 本机mac地址

2）ipv4报文格式



第一个字节前半0100代表版本为IPV4，后半0101代表头长度为20字节（5\*4个byte）

三四字节代表IP首部+后续数据之和的总长度 40字节

五字节表示标识，表示已经产生了8997个数据报

六七字节前3位为分片标志符，中间位为1表示不分片，后13位为片偏移，不分片则为0

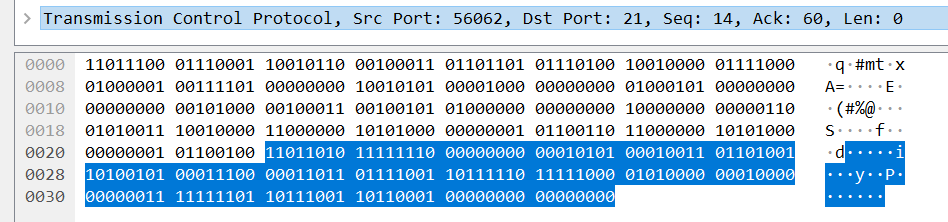
八字节为生存时间TTL为128

九字节为协议，6表示TCP

十十一字节为首部校验和。

后续字节为源地址与目的地址

3）TCP报文格式



开头四个字节为源端口56062与目的端口21（各占两字节）

再后四个字节为序号字段seq

再后四个字节为确认号字段ack

再后两字节中前四位为首部长度（数据偏移量），再六位为保留字段，最后六位为标志位，此处ACK为1。

再后两字节为窗口字段，它指出了现在允许对方发送的数据量。

再后两字节为校验和，检验首部与数据。

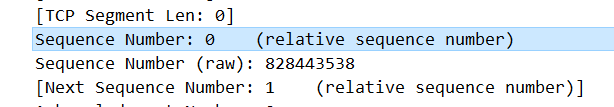
再后两字节为紧急指针字段，指出文本中紧急数据共有多少字节。

因为只是一条确认报文，无数据段

2、用侦听解析软件观察 TCP 机制

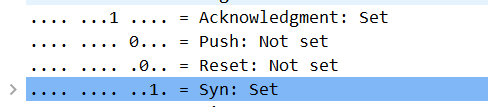
以time为顺序参考，依次打开报文

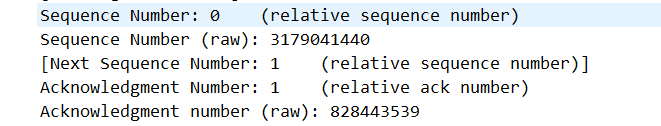
1. 客户端向服务端发送SYN=1的连接请求报文并附带seq



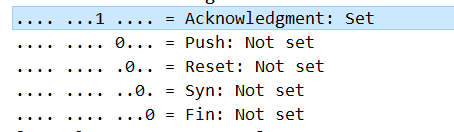


1. 服务端发送ACK=1，SYN=1，ack（客户端的next seq）的确认报文并附带seq

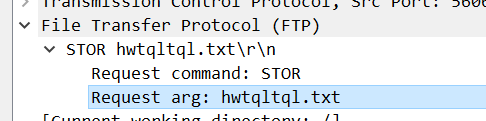




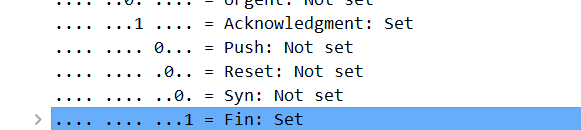
1. 客户端向服务器发送确认包ACK=1，ack（服务端的next seq），然后建立起TCP连接。



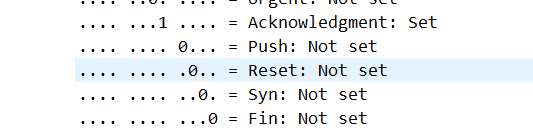
1. 传送文件



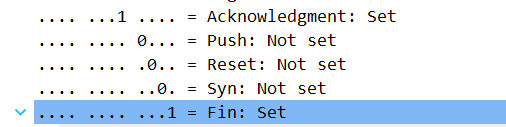
1. 客户端向服务端发送FIN=1的终止报文



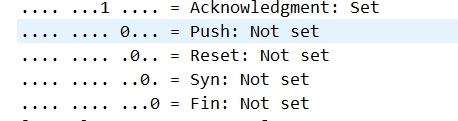
1. 服务端发送ACK=1的确认报文



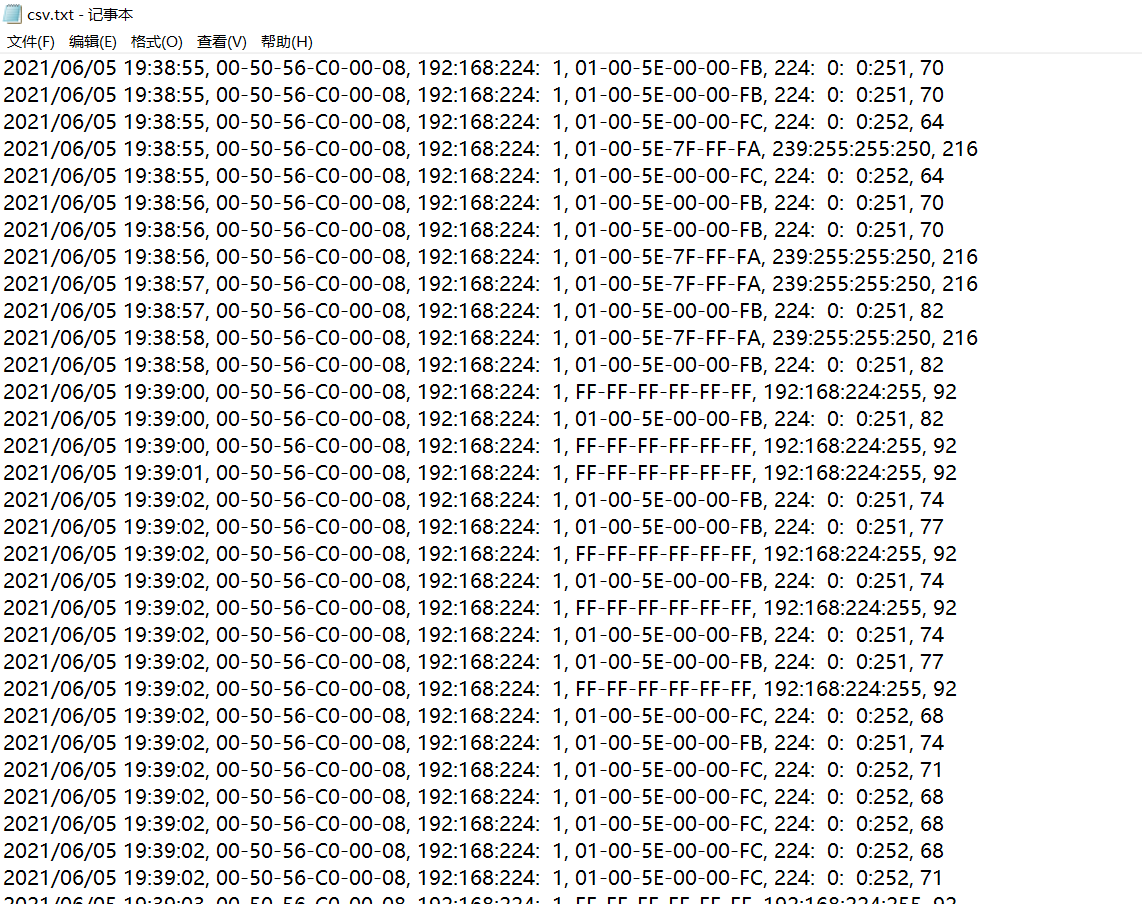
7）服务端发送FIN=1的终止报文



1. 客户端发送ACK=1的确认终止报文



3. 用 Libpcap 或 WinPcap 库侦听网络数据



4 观察 FTP 数据

ftp 数据报文是利用 tcp 协议传输的，登陆时所传输的登录信息是放在 tcp 报文

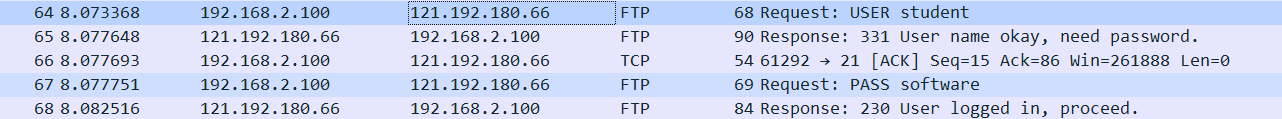
的数据中。

以 530 开头，表示登录失败，以 230 开头表示登录成功。

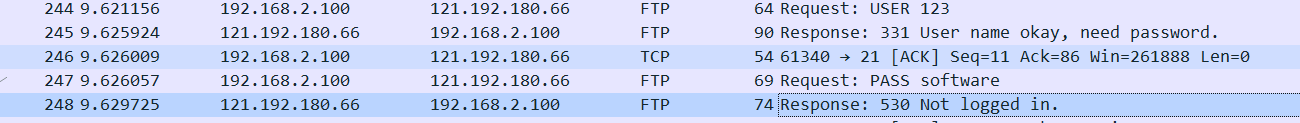
其中登录信息

用户名和密码是分开传送，先认定用户名有效，后认定密码有效。

登录成功的数据报：



登录失败的数据报：



# 实验代码

本次实验的代码已上传于以下代码仓库：https://github.com/zzh221/cnet-exp3

# 实验总结

掌握了 tcp 报文格式与连接过程

掌握了 ftp 登录时的通信过程

掌握了怎么使用 wireshark 观察网络流量，并辅助进行网络监听相关的编程

掌握了使用 winpcap 库监听处理以太网帧和 ip 报文的方法等计算机网络的基础

知识和网络编程方法。