

****

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1班**

**姓　　名 陈智涛**

**学　　号** 22920192204179

**实验时间 2021年**4**月**02**日**

**2021 年** 4 **月** 13 **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. 材料清单上传在代码托管平台上；
5. 在学期末将报告按“CNI-E1-00020190000000-张三”的命名后（其中E1是Experiment 1的缩写），压缩为zip文件，作为附件，以“计算机网络-实验报告-00020190000000-张三”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。

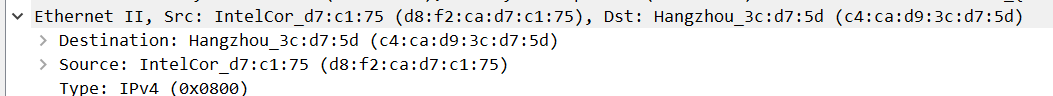
# 实验环境

Win10,C++

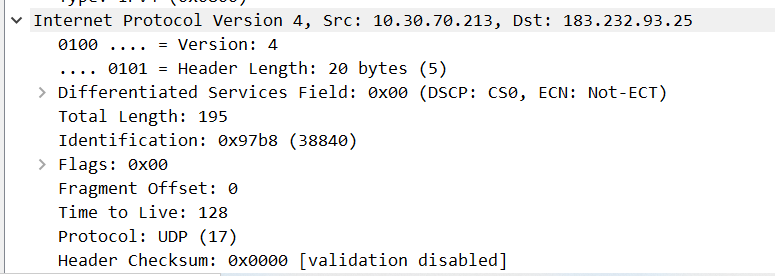
# 实验结果

1.网络协议层次嵌套

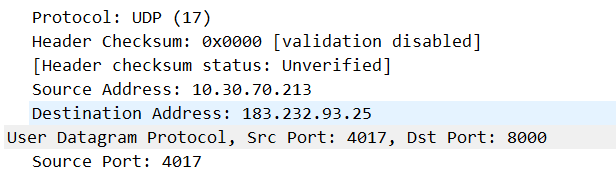
（1）数据链路层：以太网



（2）网络层：ip



（3）传输层：udp

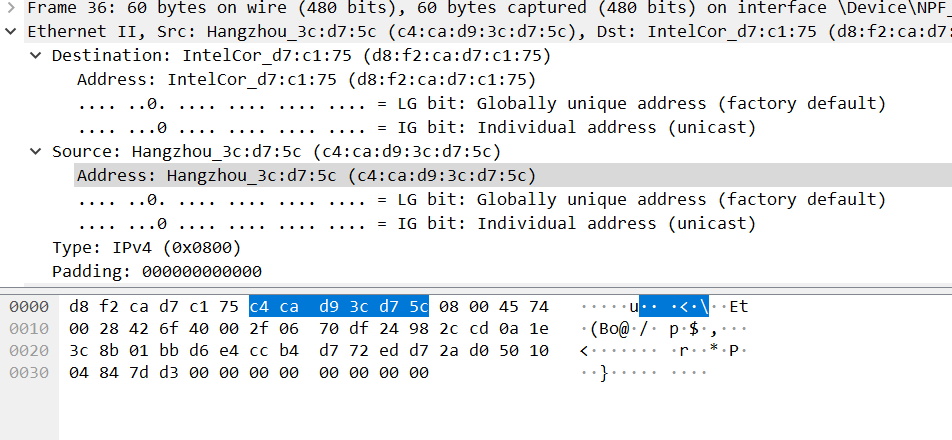


tcp的帧格式

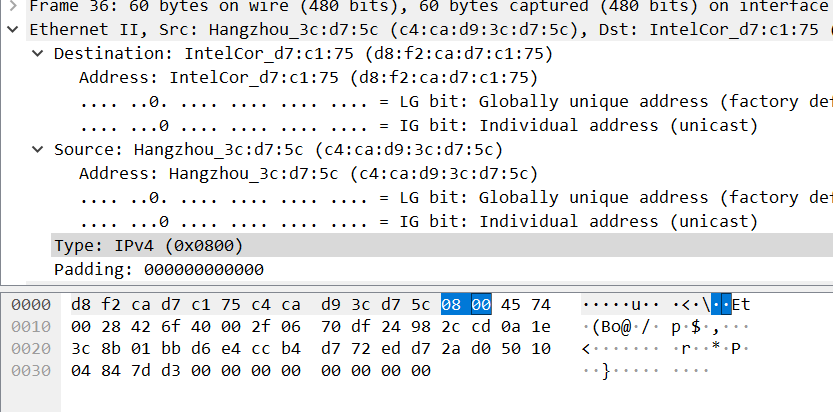
目的mac地址

# 

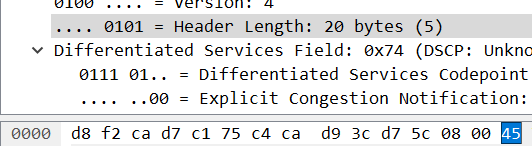
源mac地址



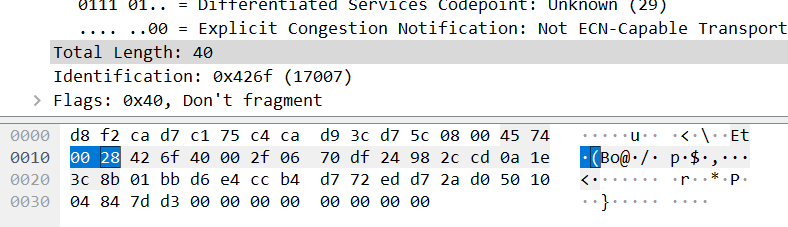
协议类型

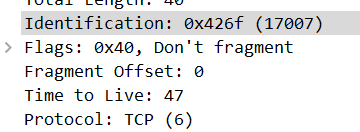


头部长度

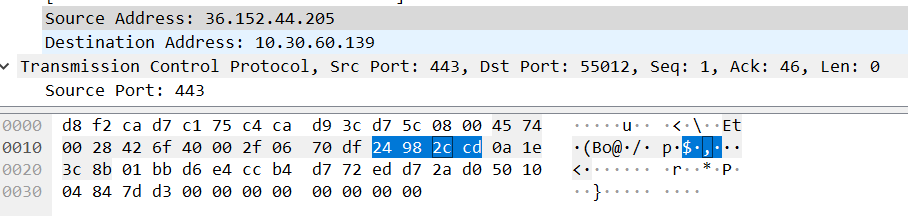


总长度



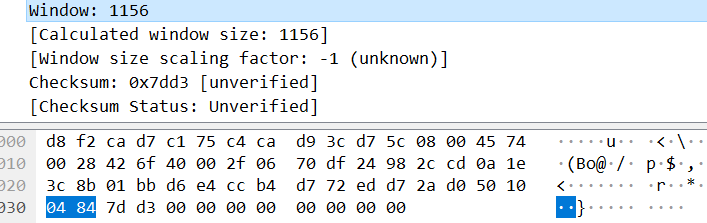


源目的地址（其后8位16进制数为目的地址）

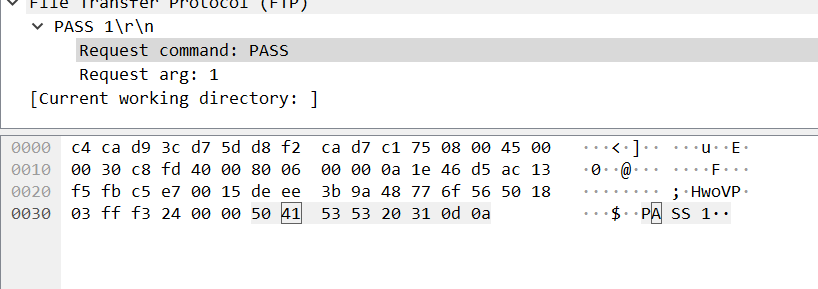


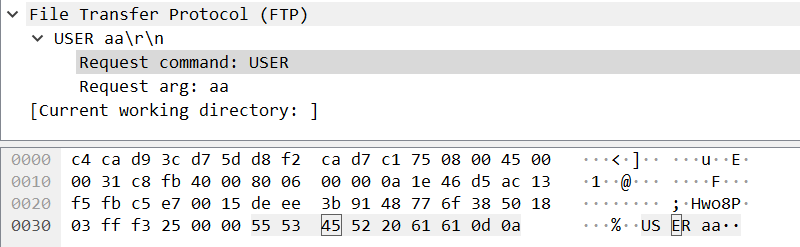
之后为源和目的地址的端口号

Tcp窗口



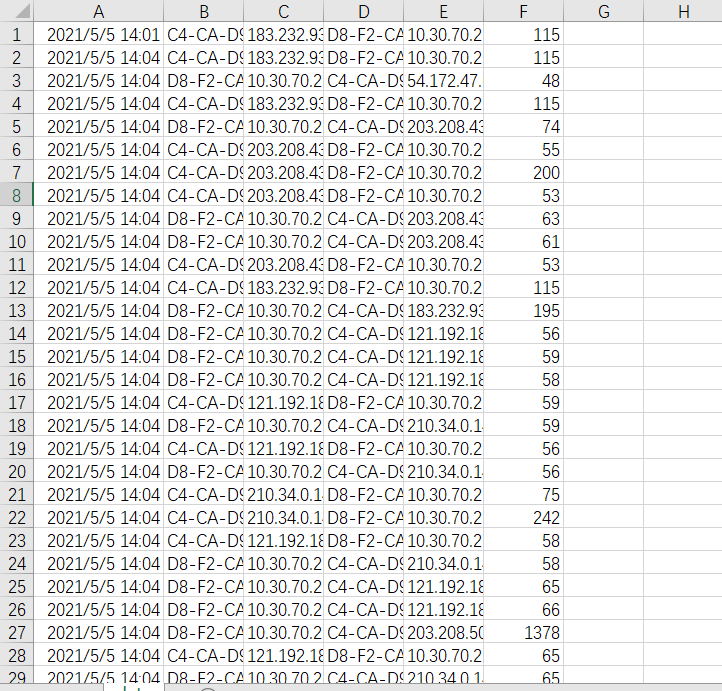
ftp与tcp基本一致，最后多了信息部分：



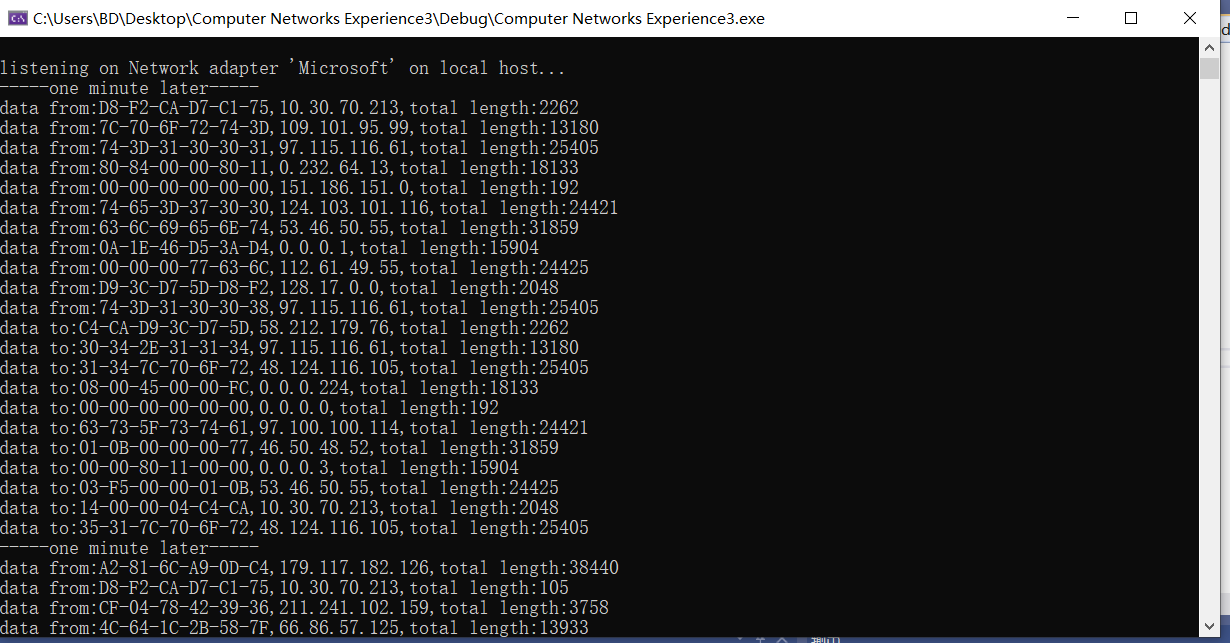


3.程序输出的截图：

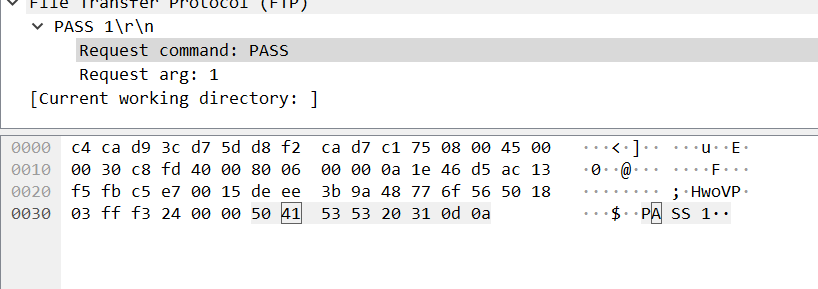
在CSV内的输出

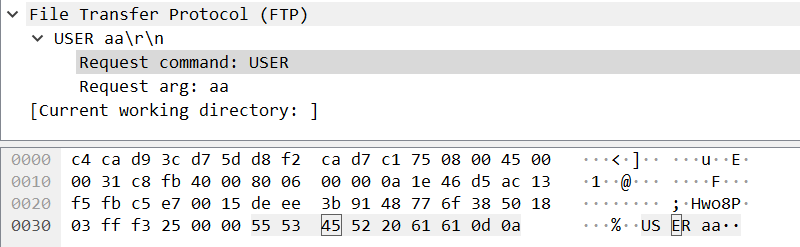


每分钟从不同来源接受的包长度：

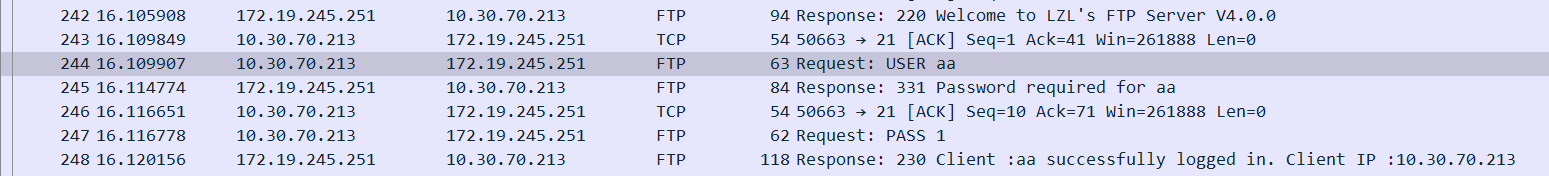


4. 登录：账号前有信息：USER 密码前有信息：PASS，下一条是传输登录成功或失败的信息。





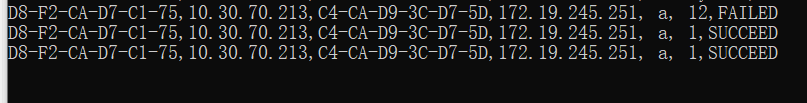
成功：（230）

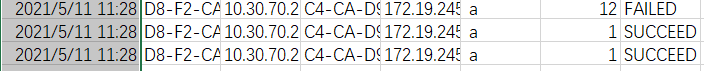


失败：（530）



4. 程序运行结果：





# 实验代码

本次实验的代码已上传于以下代码仓库：[Ko1toYuu/Computer-Network-Experience5 (github.com)](https://github.com/Ko1toYuu/Computer-Network-Experience5)

# 实验总结

通过实验的收获，真实总结，勿长篇大论。