厦門大學

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 3 班

姓　　名 王栎

学　　号 22920192204283

实验时间 2021 年 3 月 31 日

1、 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

1 实验环境

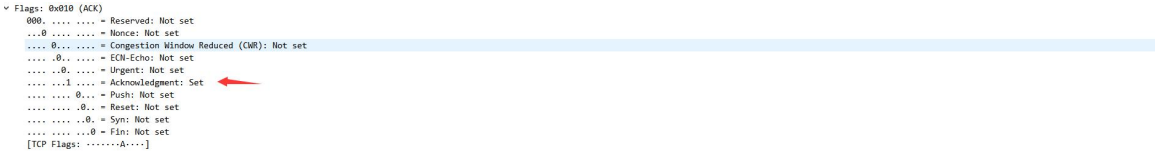
Windows10

2 实验结果

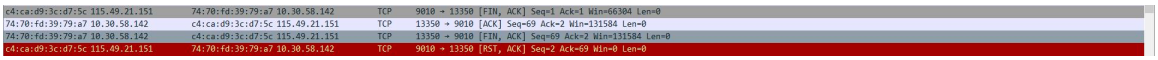
从上往下依次为物理层，数据链路层，网络层，传输层的相关信息

Tcp 第一次握手

第二次握手



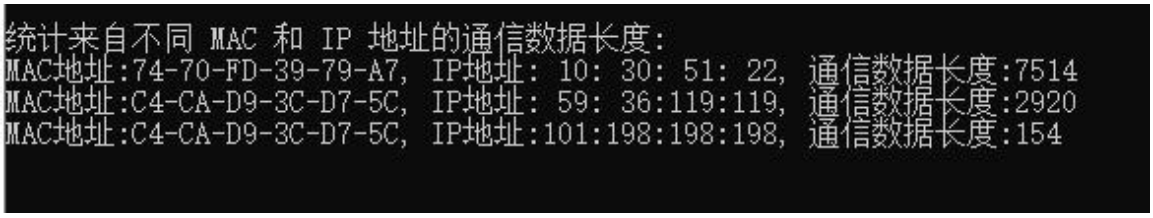
第三次握手



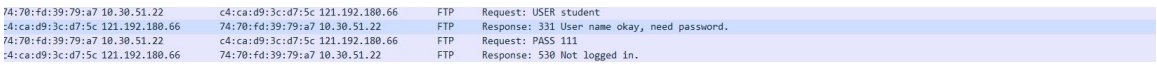
客户端断开链接，四次挥手

```
2021/03/31 16:09:24,C4-CA-D9-3C-D7-5C, 59: 36:119:119,74-70-FD-39-79-A7, 10: 30: 51: 22,129
2021/03/31 16:09:25,74-70-FD-39-79-A7, 10: 30: 51: 22,C4-CA-D9-3C-D7-5C,101:198:198:198,73
2021/03/31 16:09:25,74-70-FD-39-79-A7, 10: 30: 51: 22,C4-CA-D9-3C-D7-5C,101:198:198:198,73
2021/03/31 16:09:25,C4-CA-D9-3C-D7-5C,101:198:198:198,74-70-FD-39-79-A7, 10: 30: 51: 22,100
2021/03/31 16:09:25,C4-CA-D9-3C-D7-5C,101:198:198:198,74-70-FD-39-79-A7, 10: 30: 51: 22,132
2021/03/31 16:09:25,C4-CA-D9-3C-D7-5C, 59: 36:119:119,74-70-FD-39-79-A7, 10: 30: 51: 22,129
2021/03/31 16:09:26,C4-CA-D9-3C-D7-5C, 59: 36:119:119,74-70-FD-39-79-A7, 10: 30: 51: 22,129
```

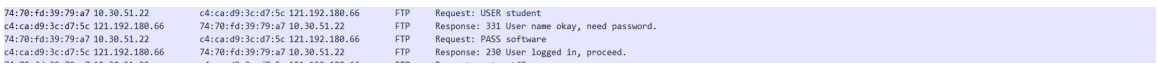
文件输出日志



统计长度



检测 ftp，错误输入



检测 ftp，正确输入

3 实验代码

本次实验的代码已上传于以下代码仓库：https://github.com/aLily11/cnii

4 实验总结

通过这次实验学习用 WinPCAP 库监听网卡的数据流、统计流量、统计数据长度以及如何用 Wireshark 测试监听程序