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　用 PCAP 库侦听并分析网络流量

班　　级 软件工程 2018 级 2 班

姓　　名 汤国枫

学　　号 24320182203270

实验时间 2020 年 3 月 11 日

2020 年　3 月　24　日

1 实验目的

- 用 WinPCAP 或 libPcap 库侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地址
- 基于 WinPCAP 工具包制作程序，实现侦听网络上的数据流，解析发送方与接收 方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告警
- 每隔一段时间（如 1 分钟），程序统计来自不同 MAC 和 IP 地址的通信数据长度， 统计发至不同 MAC 和 IP 地址的通信数据长度

2 实验环境

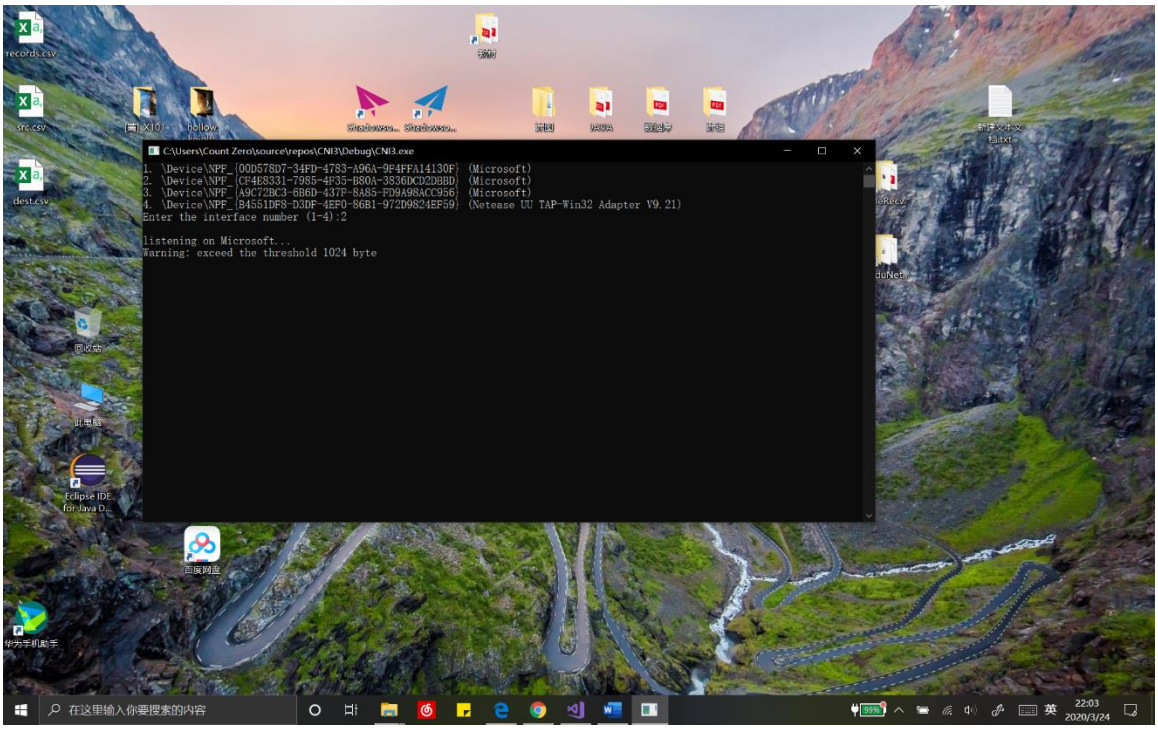
Windows

VS 2017

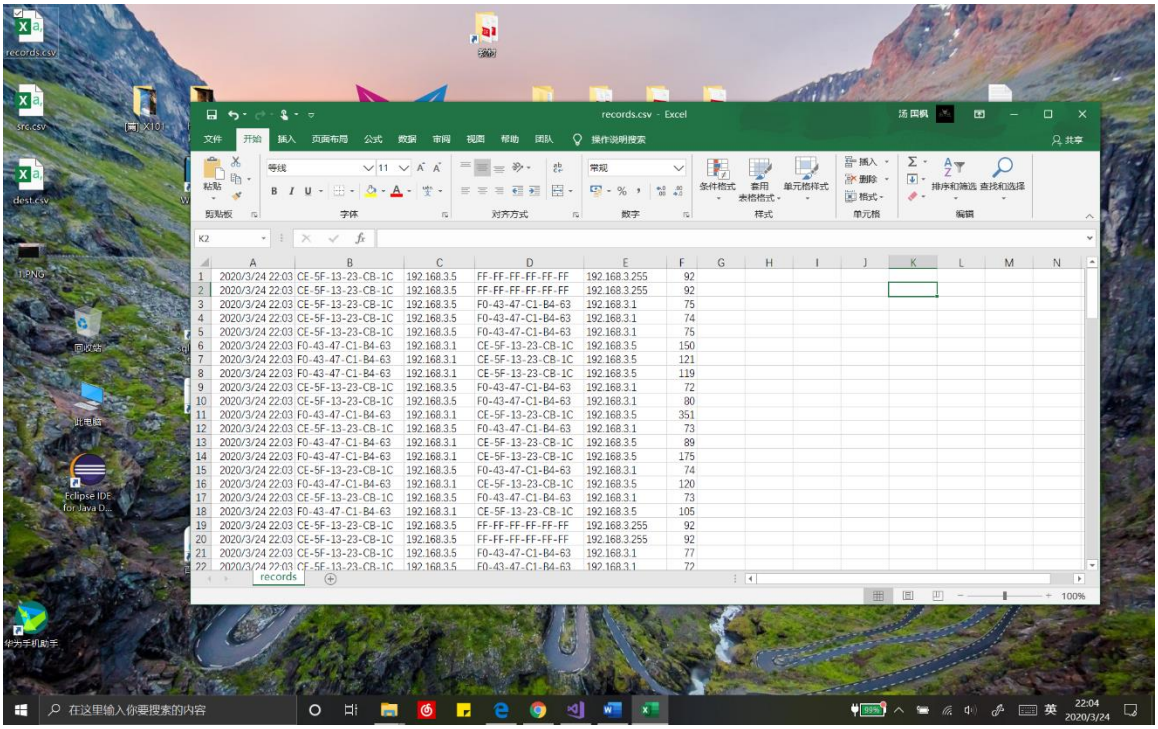
C++

3 实验结果

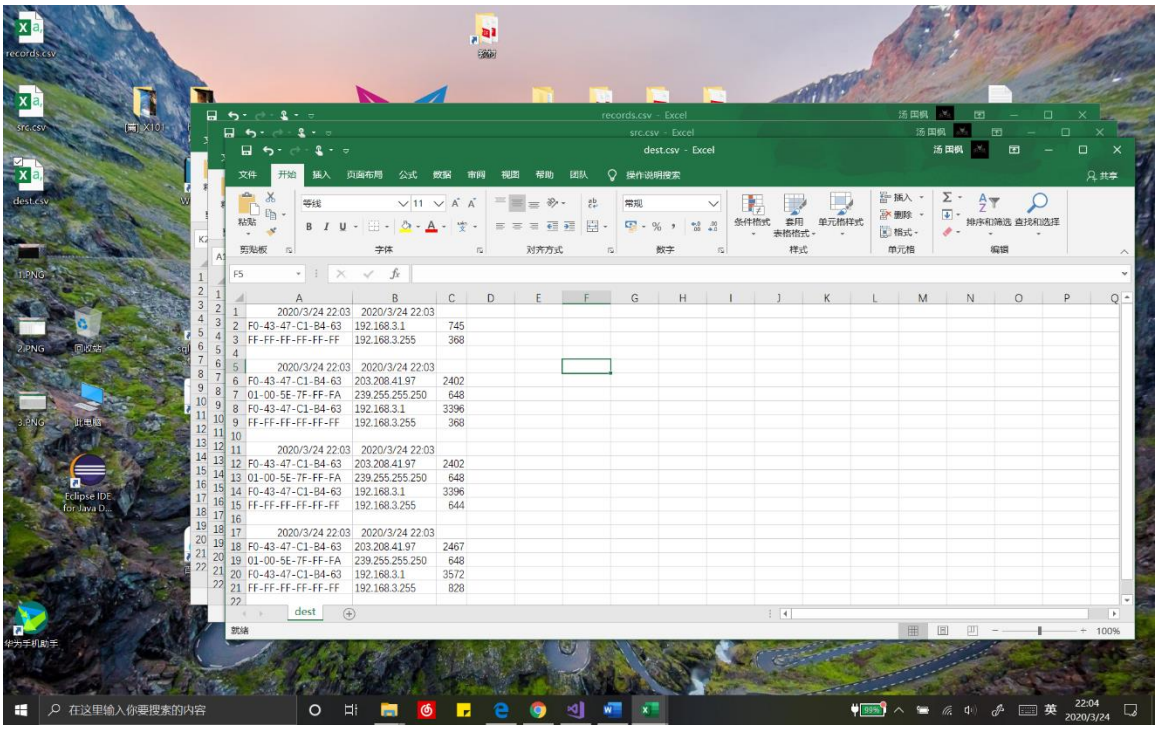
1. 总流量超过给定阈值（1MB）进行警告



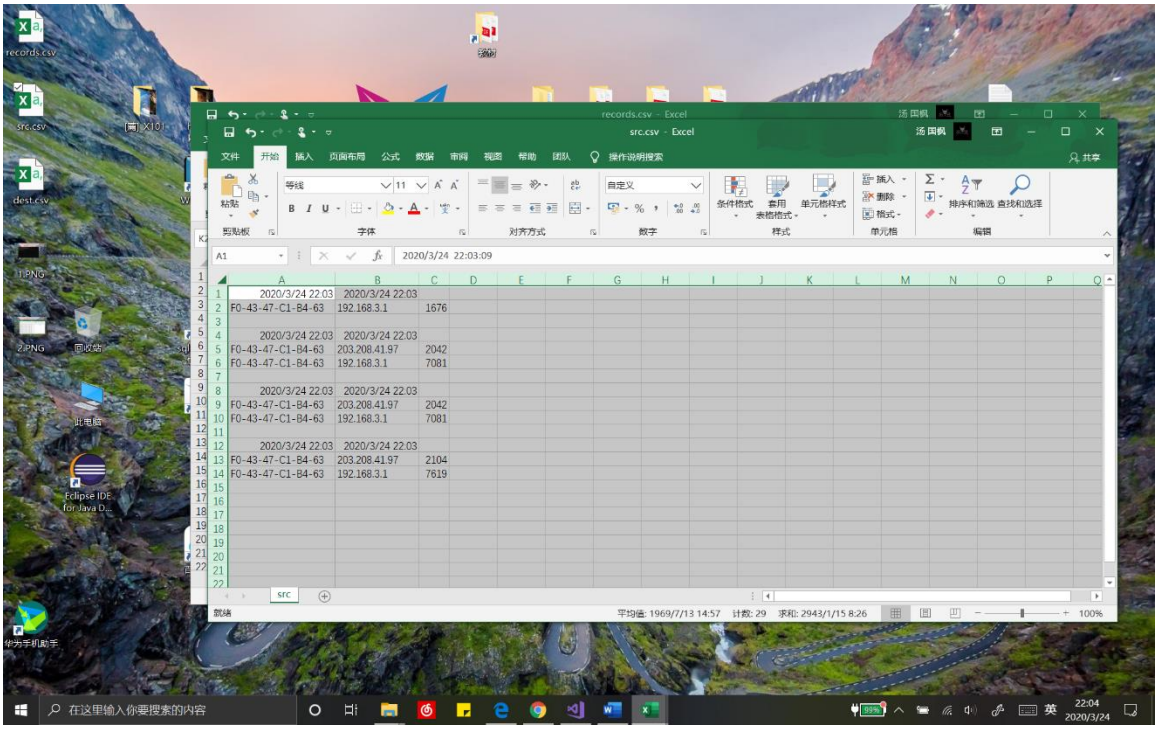
2. 时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度



3. 每隔一段时间（6 秒，没有数据传入则不统计），程序统计来自不同 MAC 和 IP 地址的通信数据长度



4. 统计发至不同 MAC 和 IP 地址的通信数据长度



4 实验总结

对帧、数据包、报文的知识增加了

学会了 winpcap 的基本使用

学会了一种新的学习方式——阅读别人的项目，要敢于调试、不能放低要求

搜索的能力提高了