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　刘明成

学　　号　24320182203236

实验时间　2020 年 3 月 21 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，对超过给定阀值（如：1MB）的流量进行告警。

程序在文件上输出形如下列 CSV 格式的日志：

时间、源　MAC、源　IP、目标 MAC、目标 IP、帧长度（以逗号间隔）

2015-03-14　13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,1536

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。（未能完成）

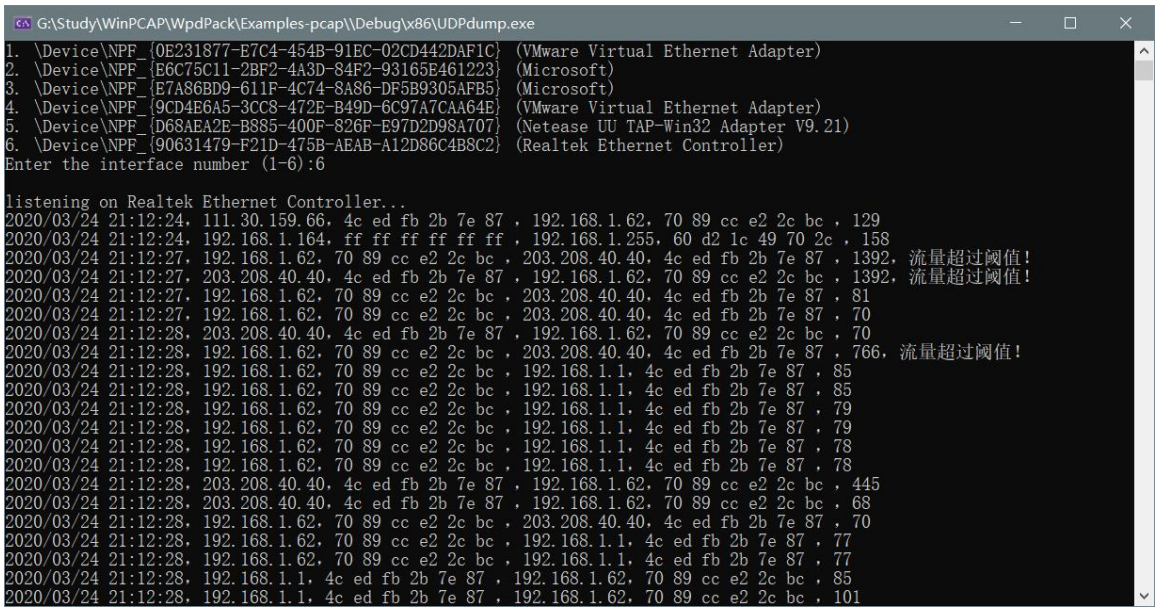
2 实验环境

实验机：Windows10 x64 位

软件：　Visual Studio 2019（WinPCAP 库）

编程语言：C

3 实验结果



4 实验总结

学会了如何使用 WinPCAP 库侦听并分析网络上数据流的 IP 地址以及 MAC 地址等，了解了一些有关 Wireshark 以及 Omnipeek 等软件的知识。