

****

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**

# 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）

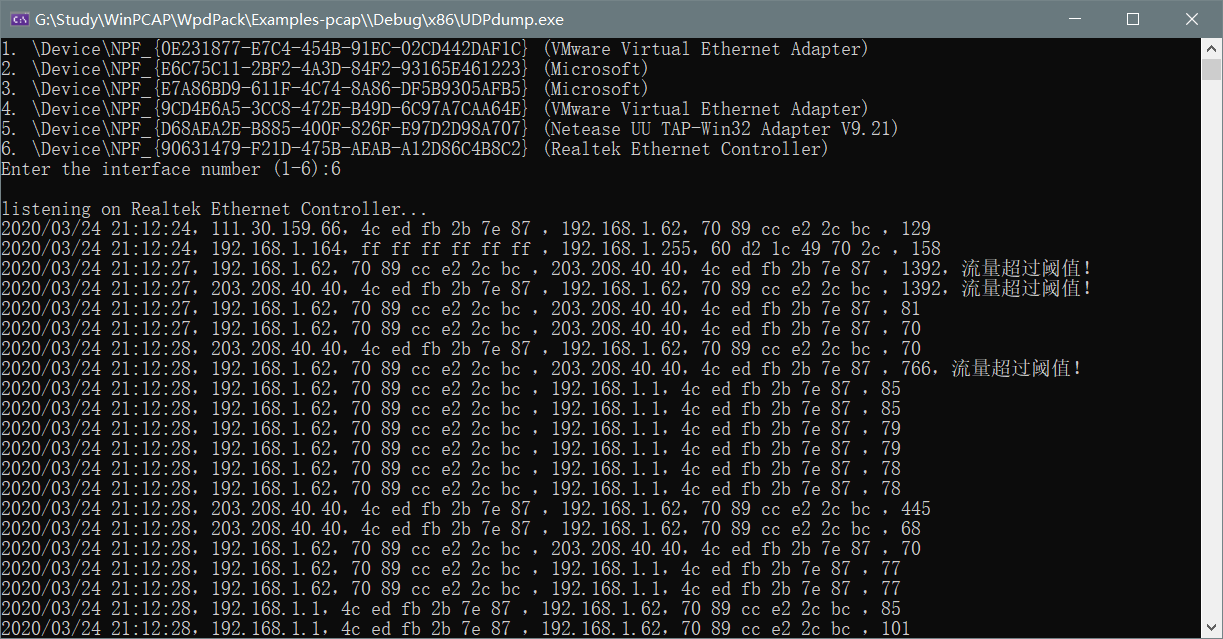
# 实验环境

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。