

****

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3班**

**姓　　名 宋润涵**

**学　　号 24320182203266**

**实验时间 2020年3月11日**

**2020 年 3 月 15 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，对超过给定阈值（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：

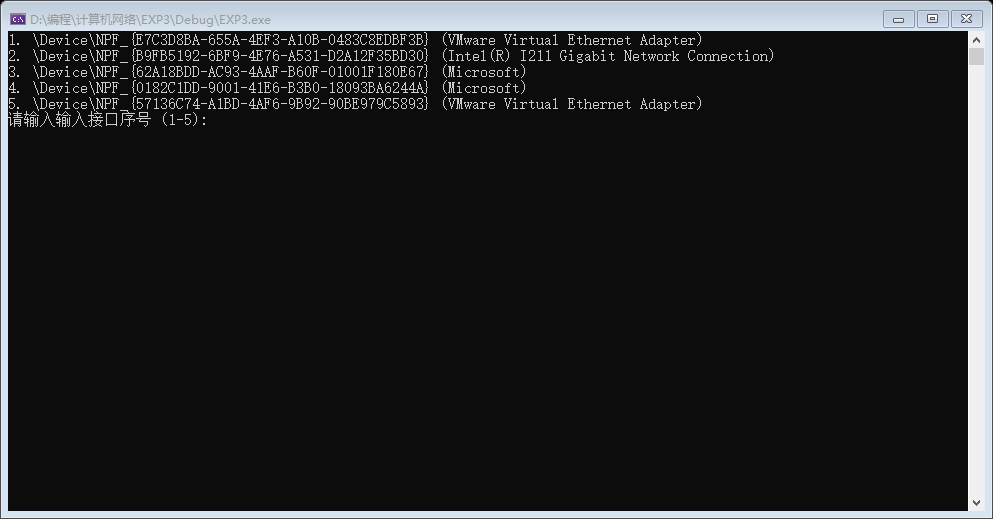
时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔）

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D572,192.168.33.2,1536 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。

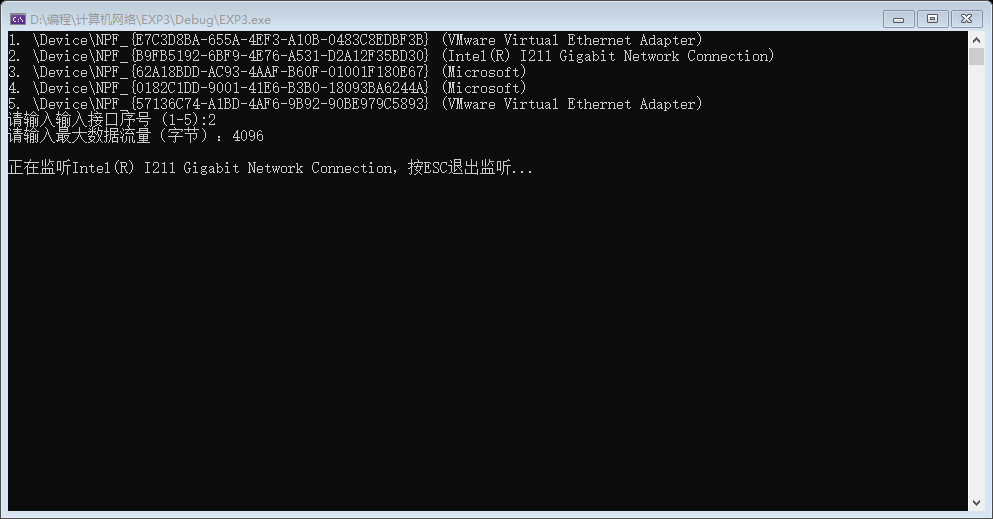
# 实验环境

Windows 10，Visual Studio 2019，C++，WinPcap 4.1.2。

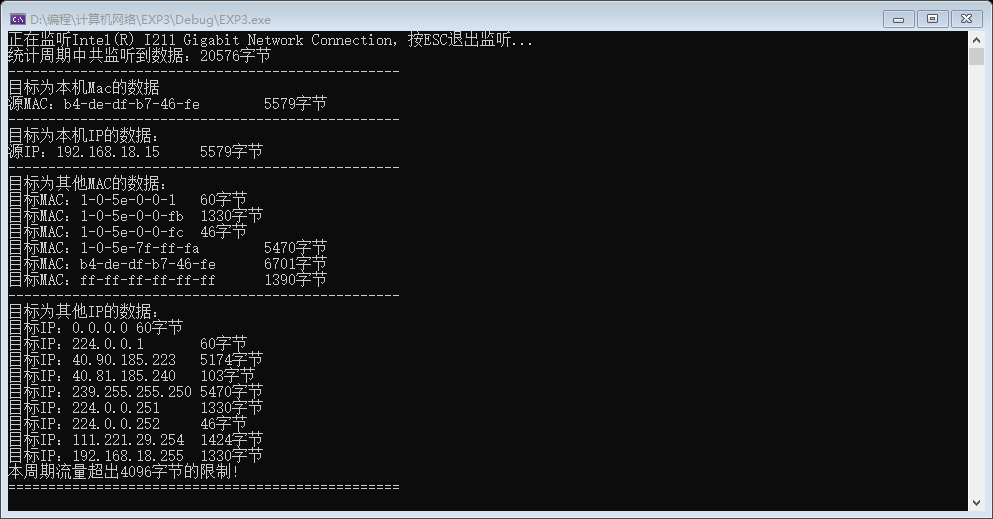
# 实验结果



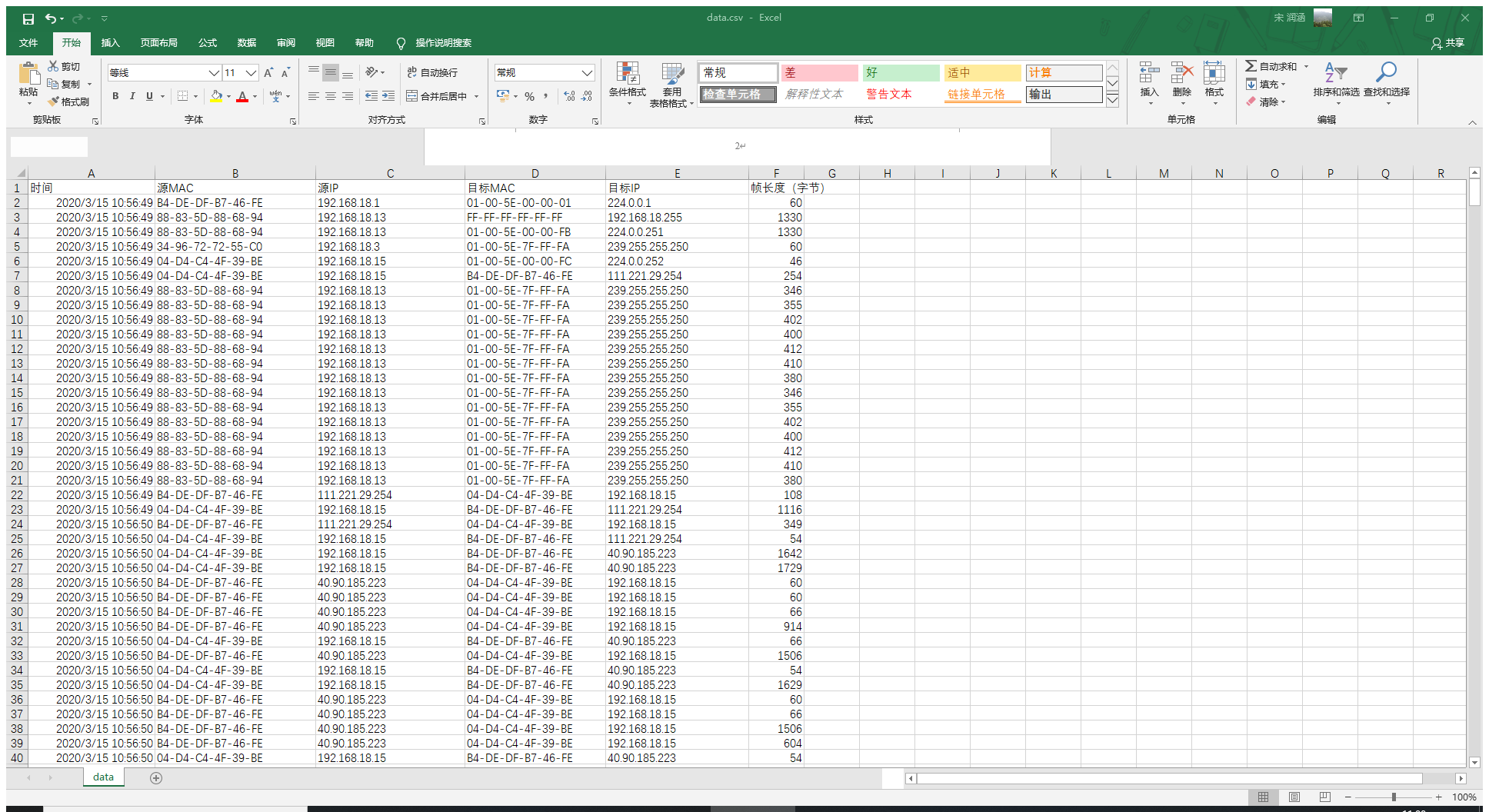
选择需要监听的适配器名称。



再输入流量限制后程序就会开始监听，按ESC可以退出。



每个周期程序都会输出统计数据。如果本周期的流量超出了限制，程序会给予提示。



程序监听到的网络流量会被保存为CSV文件

# 实验总结

本次实验使用了颇有年代感的WinPcap。在使用的时候加深了对于函数指针（回调函数）的理解。另外也发现了IP地址不光可以同结构体表示，也可以用4字节整数表示。

除此以外还学习了如何设计使用定时器（虽然不是异步），如何使用C++的map等。