

****

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 林晖**

**学　　号 24320182203231**

**实验时间 2020年3月11日**

**2020 年 3 月 22 日**

# 实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第一部分。

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。对 Linux 用户，可以使用 libpcap 编程实现。

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,

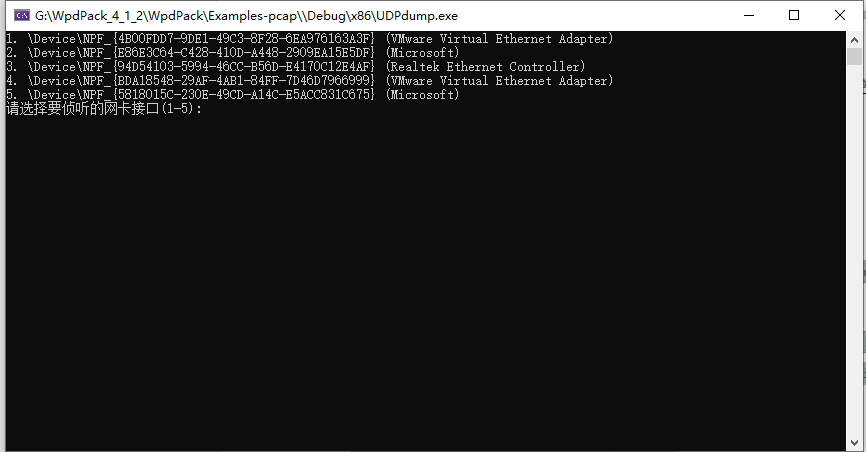
60-36-DD-7D-D5-72,192.168.33.2,1536

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。

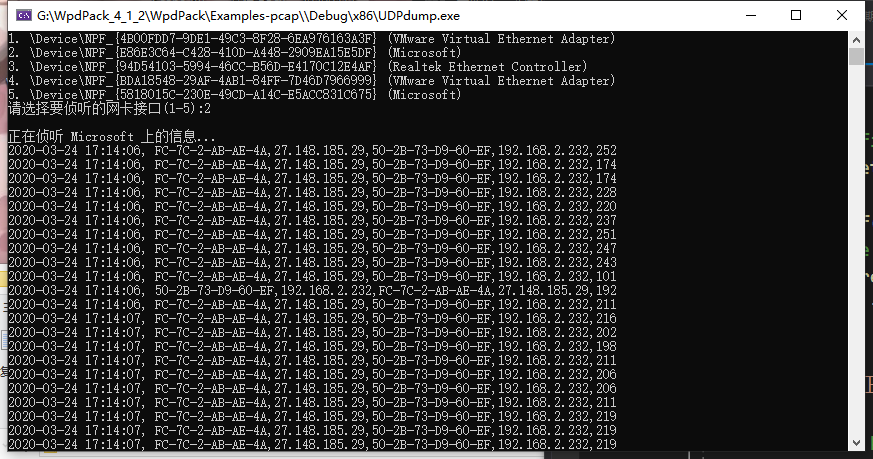
# 实验环境

操作系统：Windows 10，编程语言：C。

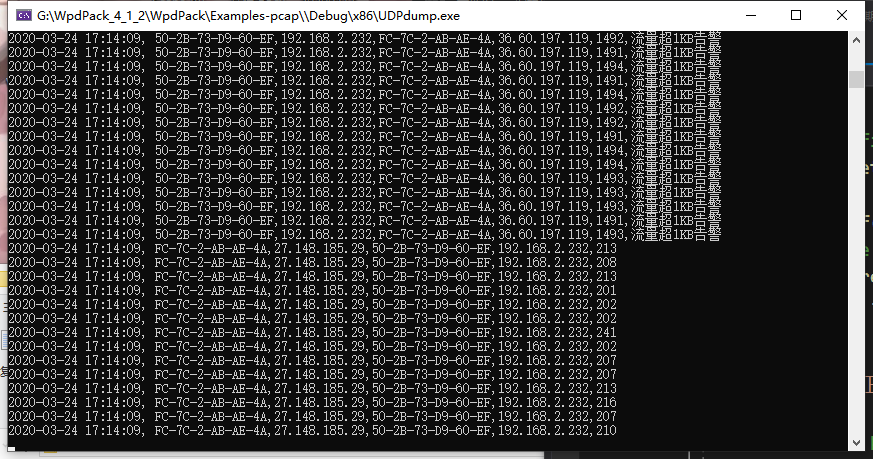
# 实验结果



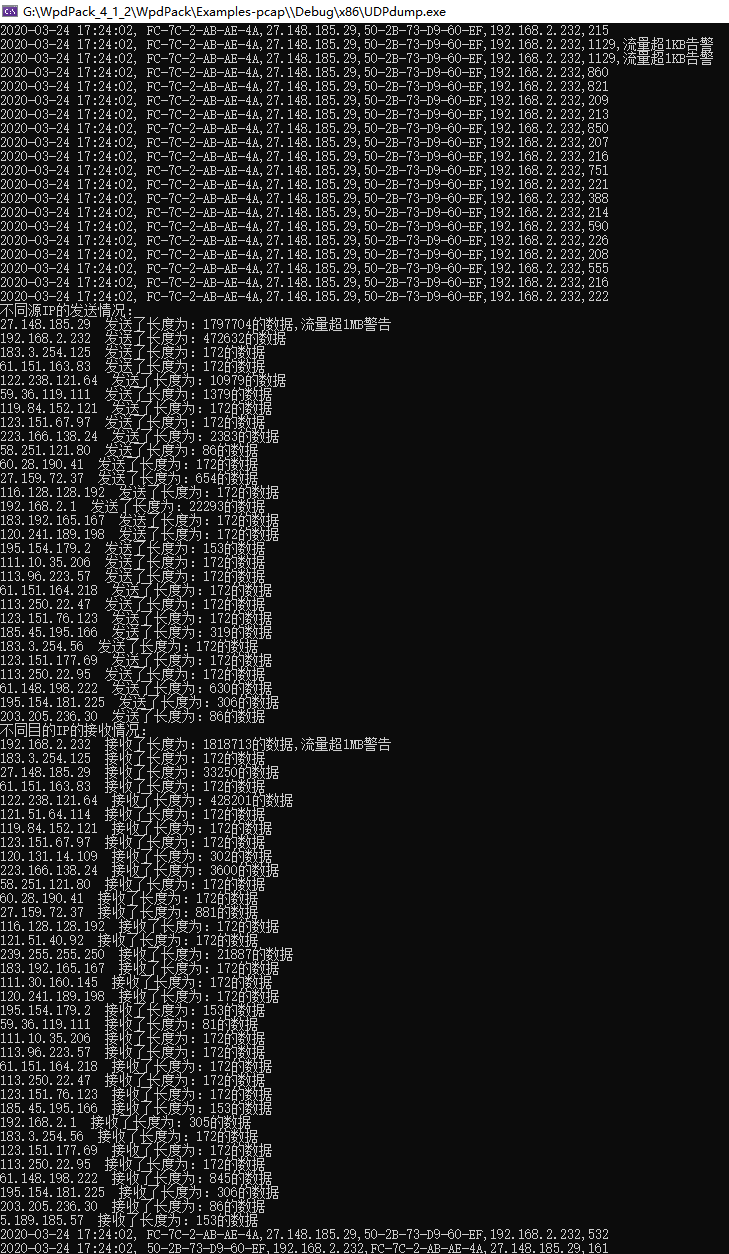
选择网卡界面



接收信息



对于长度超过1024的流量进行告警



每1分钟输出一次统计情况，将源IP发送情况和目的IP的接收情况进行汇报，对流量超过1MB的发送与接收进行警告。

# 实验总结

实际实现了侦听流量和获取MAC、IP地址的操作，并在编程中对数据帧格式有了更好的理解，更清晰地了解了帧格式的划分，过程中也积累了很多编程的知识，例如u\_char类型的相关知识、time.h库的使用等。