

****

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2019级4班**

**姓　　名 钟宇哲**

**学　　号 22920192204338**

**实验时间 2021年3月19日**

**2021 年 3 月 19 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。

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

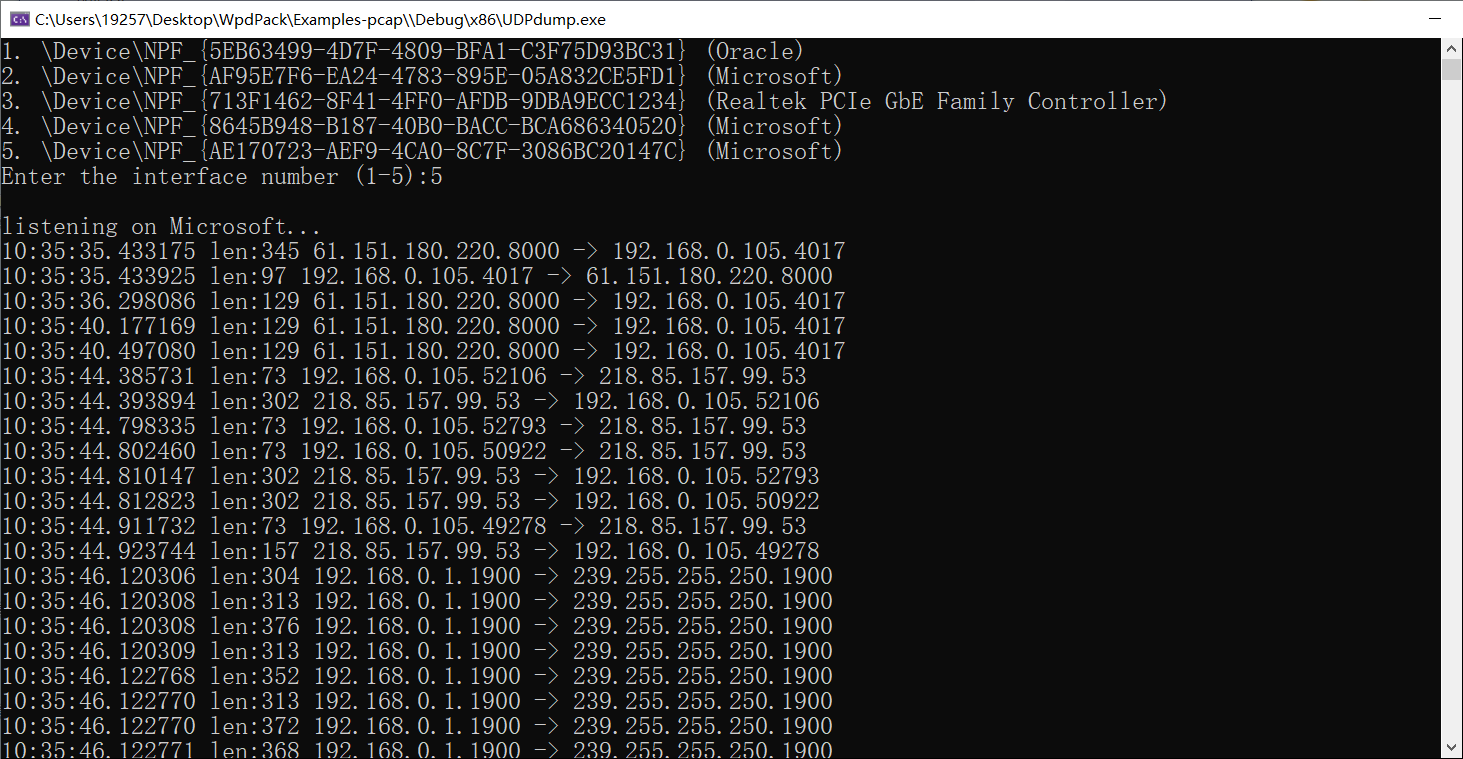
操作系统：Windows 10

编程语言：C++语言

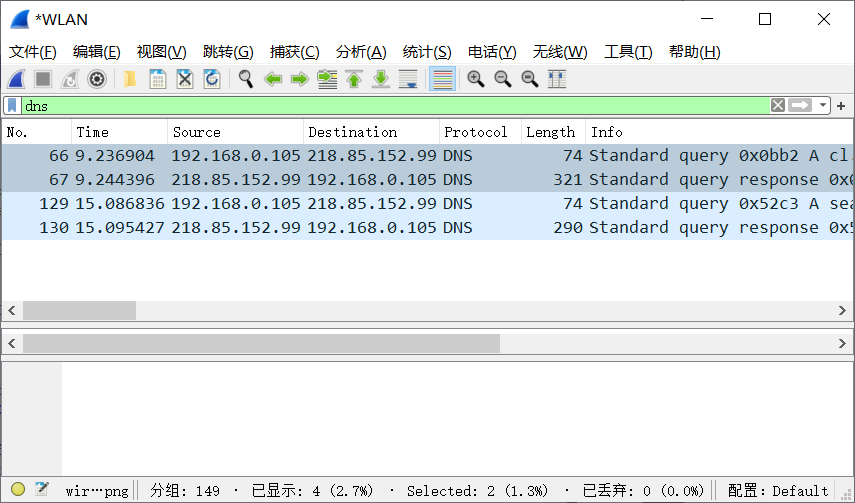
# 实验结果

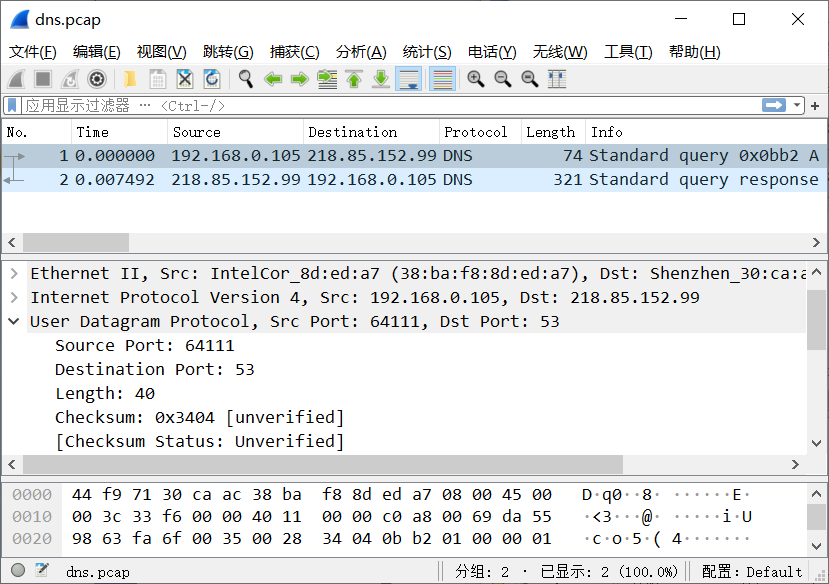
1. 示例程序

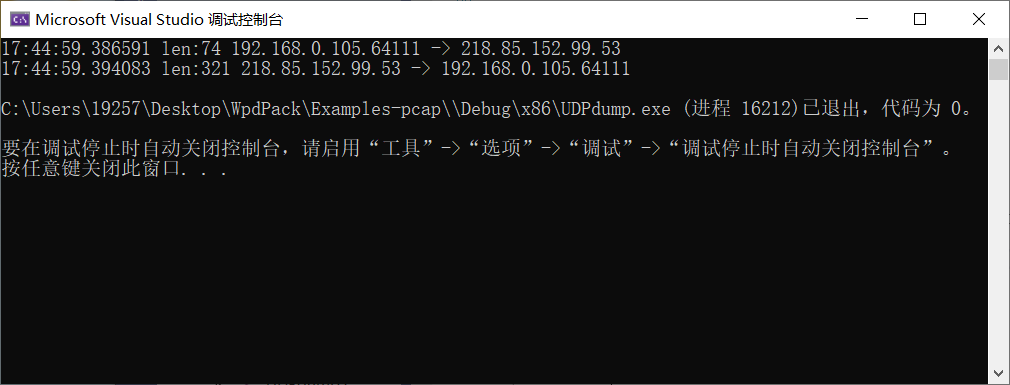
（1）直接运行



（2）利用Wireshark调试





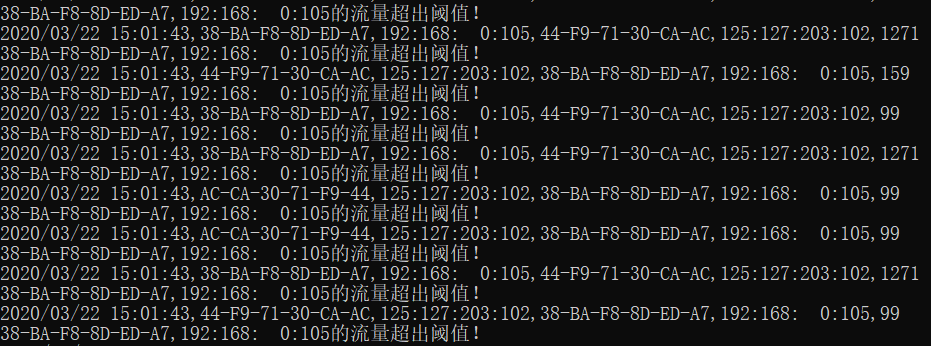


1. 实验要求程序

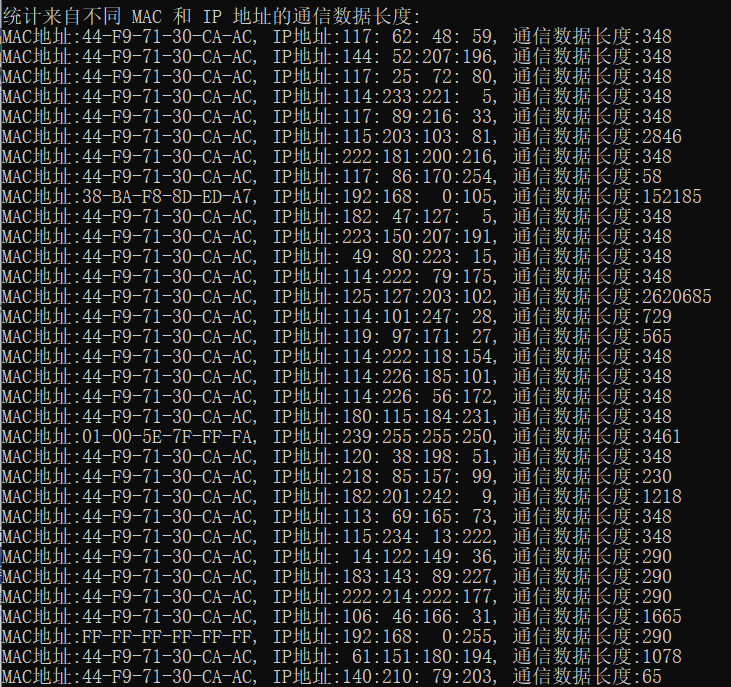
（1）在文件上输出日志

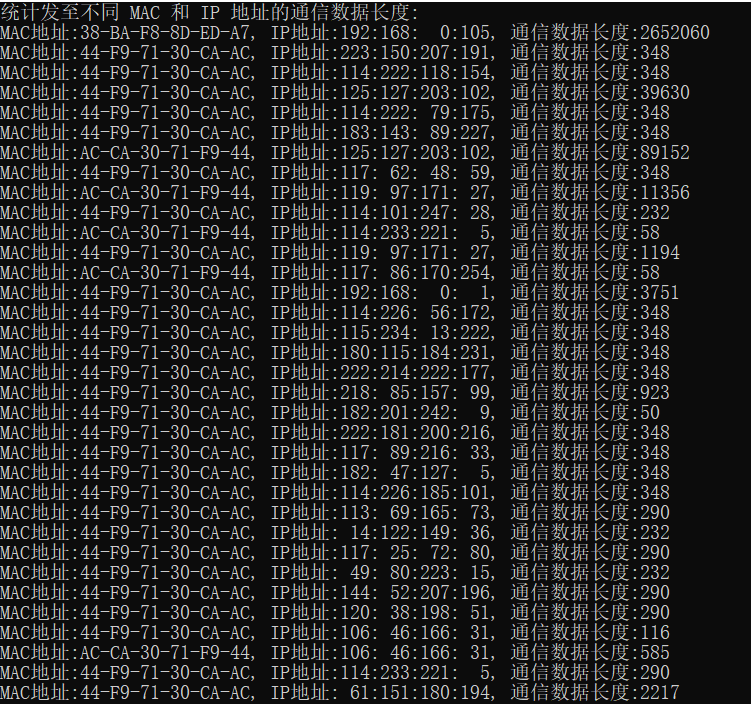


（2）流量告警（0.5M为例截图）



（3）统计来自/发至不同 MAC 和 IP 地址的通信数据长度（30s为例截图）





# 实验总结

通过这次实验学习了如何使用WinPCAP库监听网卡的数据流、统计流量、统计数据长度以及如何用Wireshark测试监听程序，此外，也更加了解数据包的格式及属性，为下次实验打下基础。