

****

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 陈芸衣**

**学　　号 24320182203182**

**实验时间 2020年3月11日**

**2020 年 3 月 2４ 日**

# 实验目的

用 WinPCAP捕获并分析以太网的帧，获取目标与源网卡的MAC 地址

基于 WinPCAP 工具包制作程序，实现监听网络上的数据流，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/s）的流量进行告警。

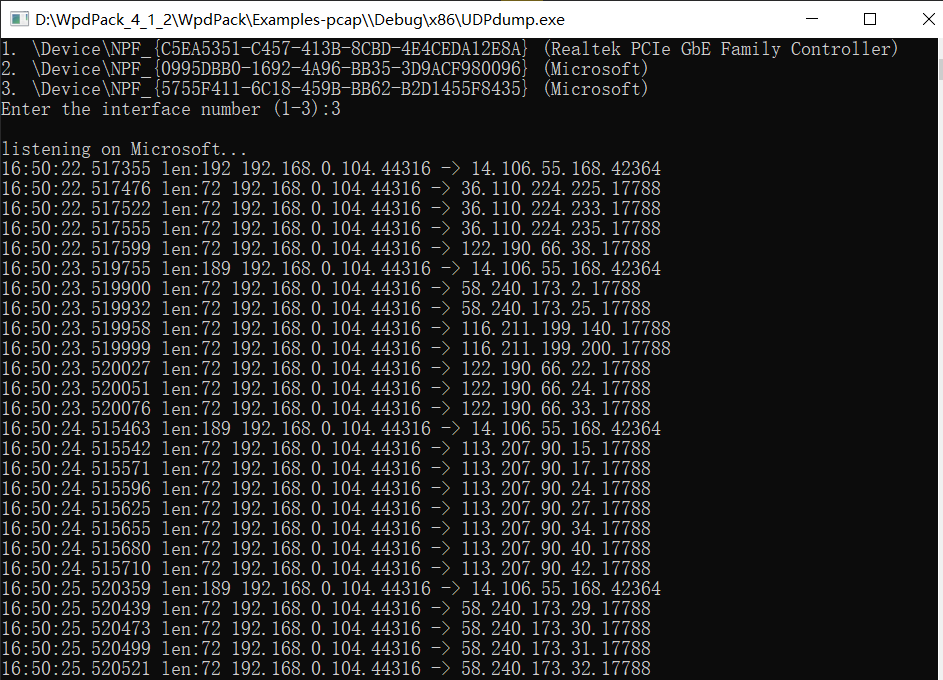
# 实验环境

操作系统:Windows 10

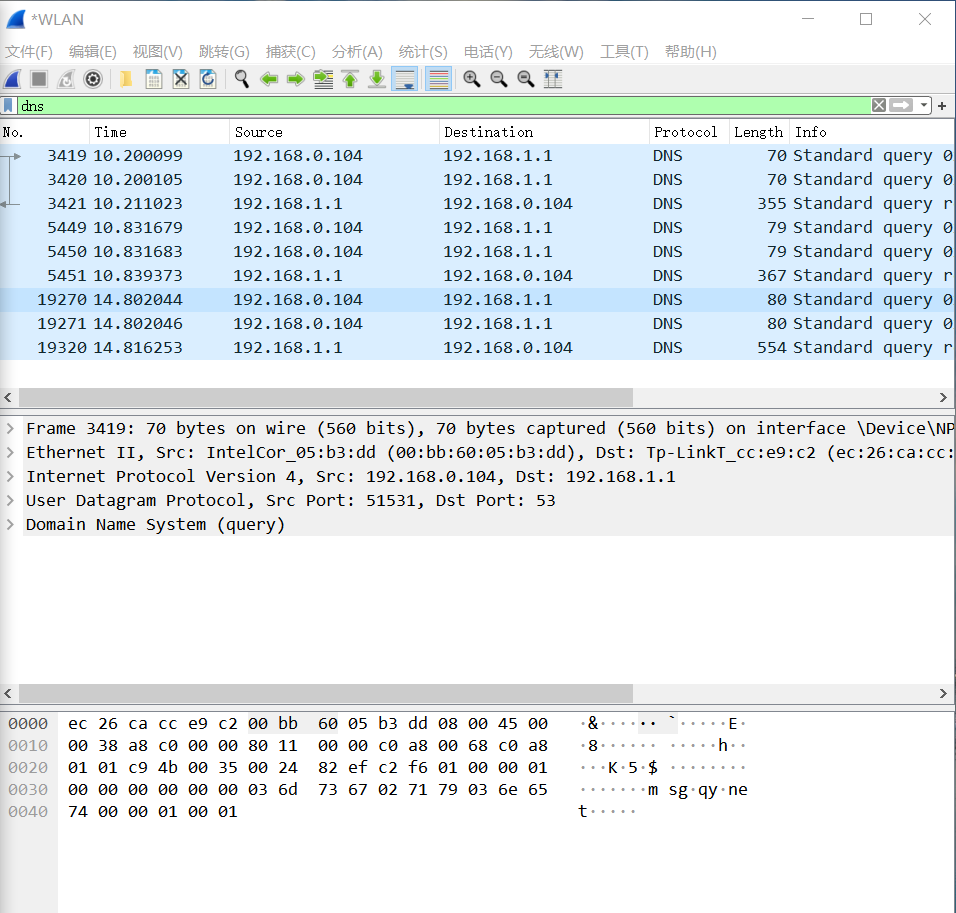
编程语言:C语言

# 实验结果

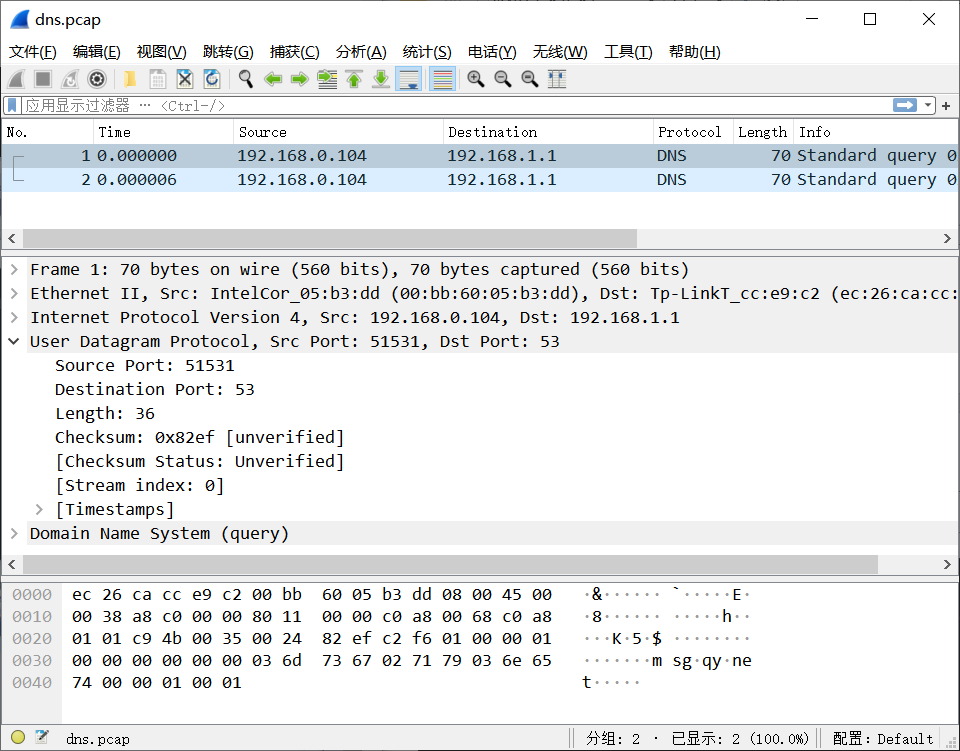
（1）在VS直接运行：

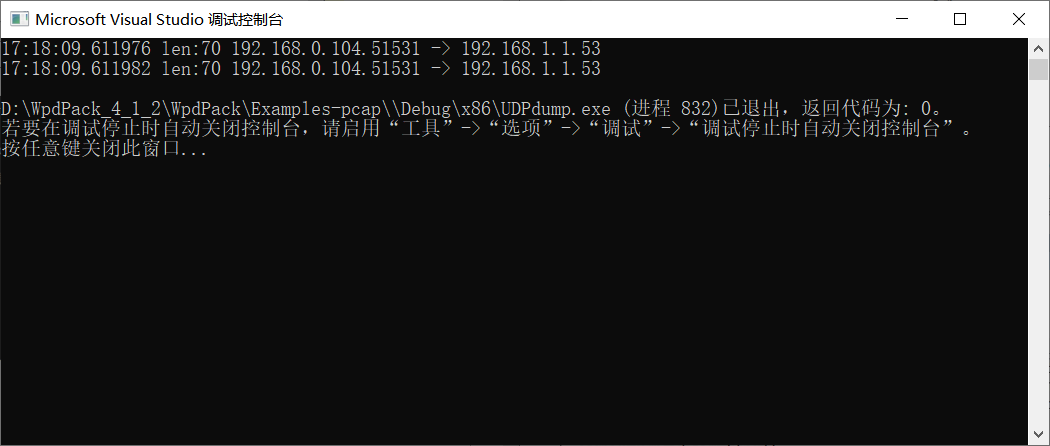


（2）使用Wireshark调试：

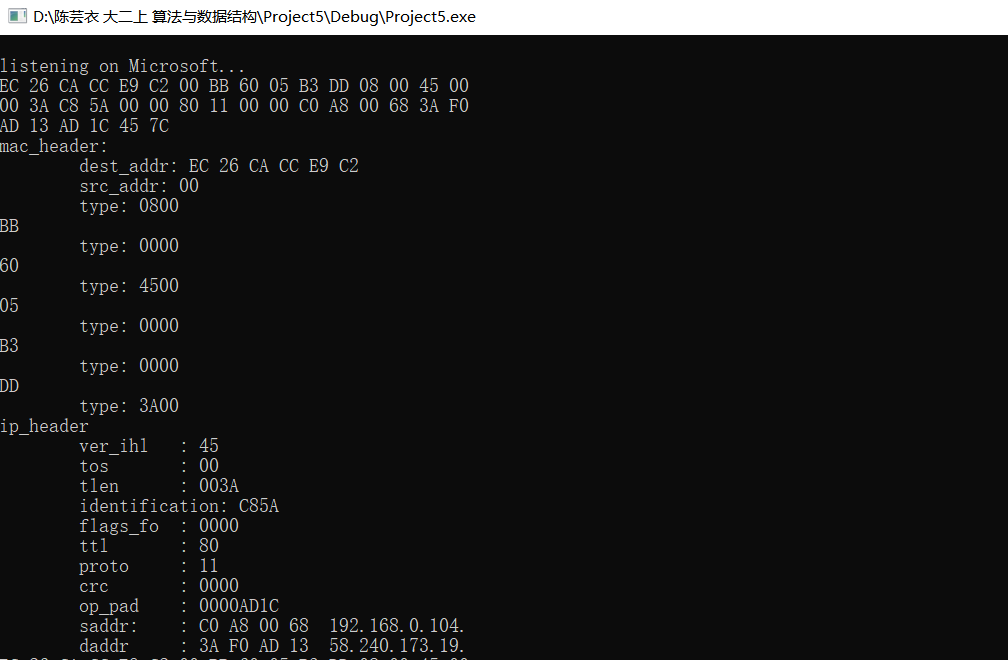


dns.pcap:

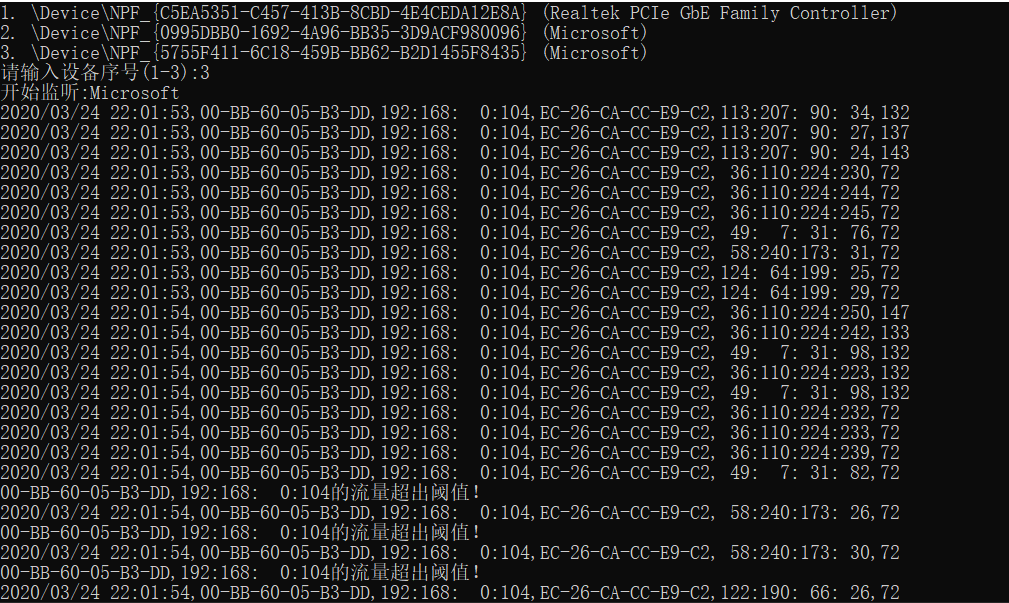




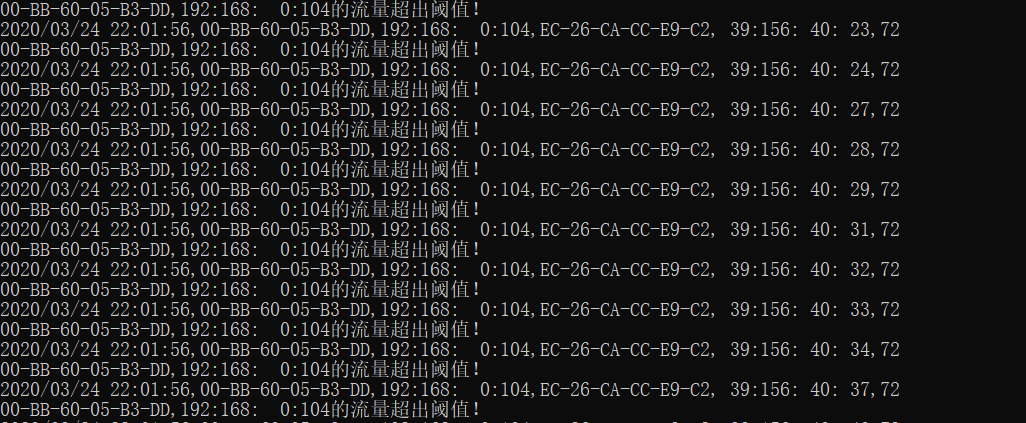
（2）程序运行结果：



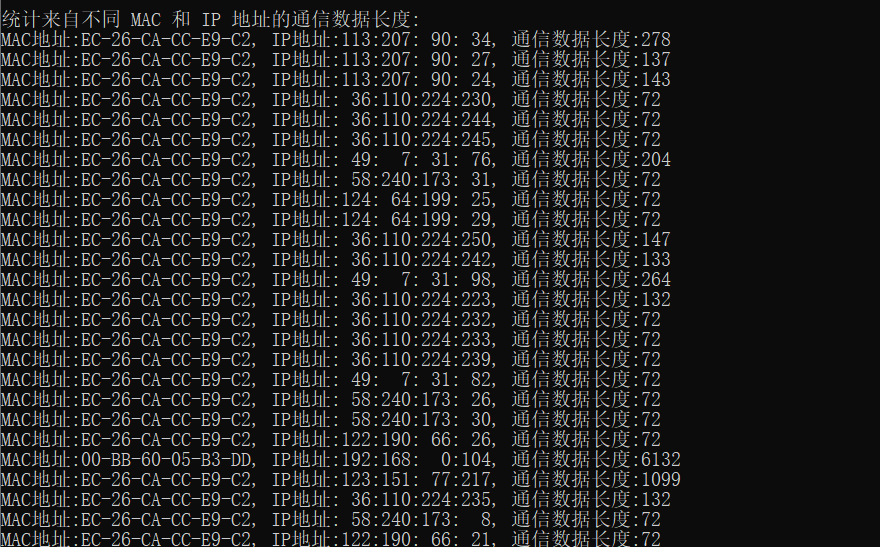
开始监听：



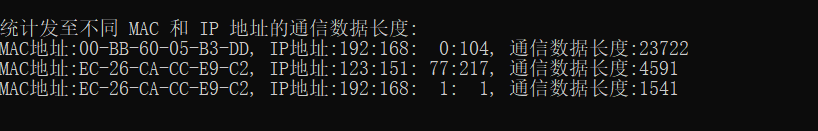
流量超出阈值：



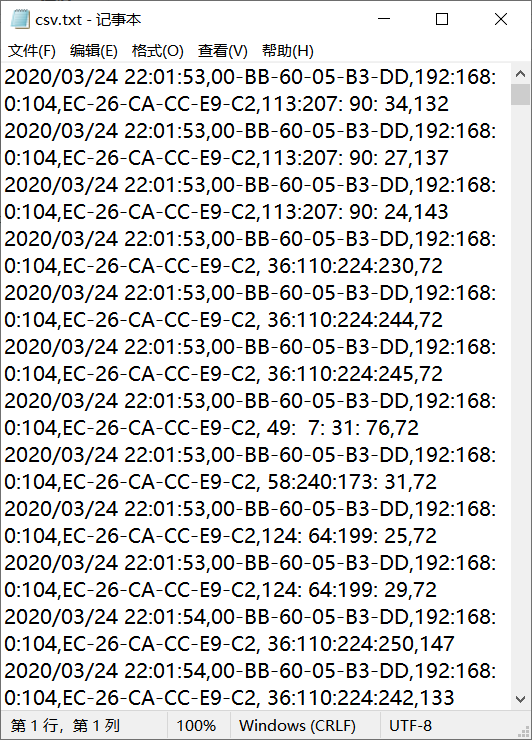
统计来自不同MAC和IP地址的通信数据长度：



统计发自不同MAC和IP地址的通信数据长度：



Csv.txt内容：



# 实验总结

通过本次实验，学会了用WinPCAP库监听并分析以太网的帧，记录目标与源MAC和IP地址。用基于WinPCAP的工具包，制作程序，统计网络上的数据流、流量等，此外，用wireshark测试监听程序。对计算机的MAC和IP地址有了更直观的理解。