

****

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 陈渝璇**

**学　　号 24320182203181**

**实验时间 2020年3月11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。

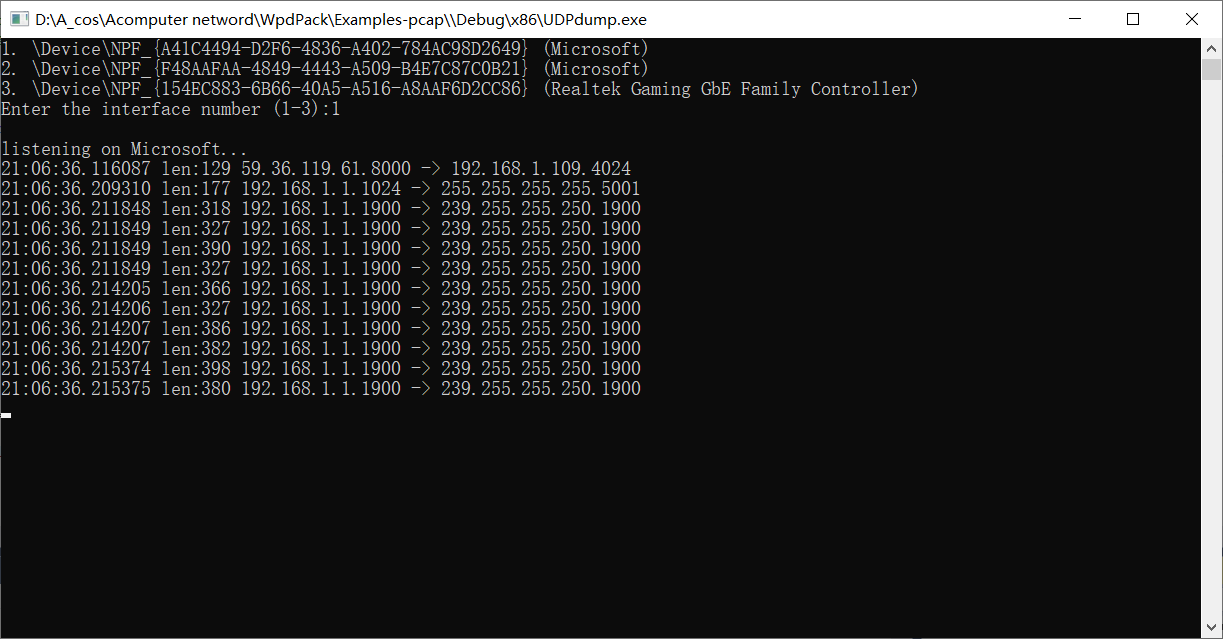
# 实验环境

操作系统：Window10

编程语言：c语言

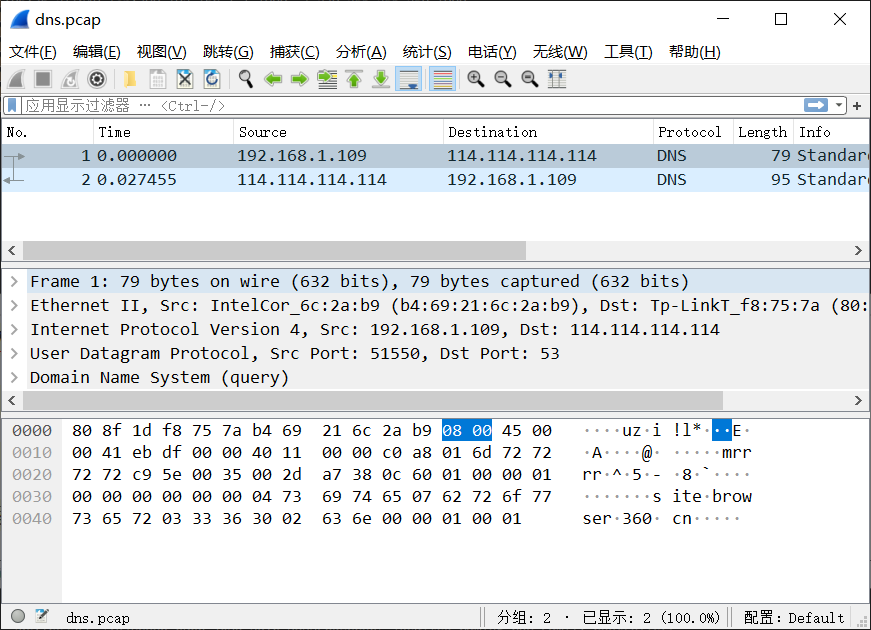
# 实验结果

1示例代码运行测试：

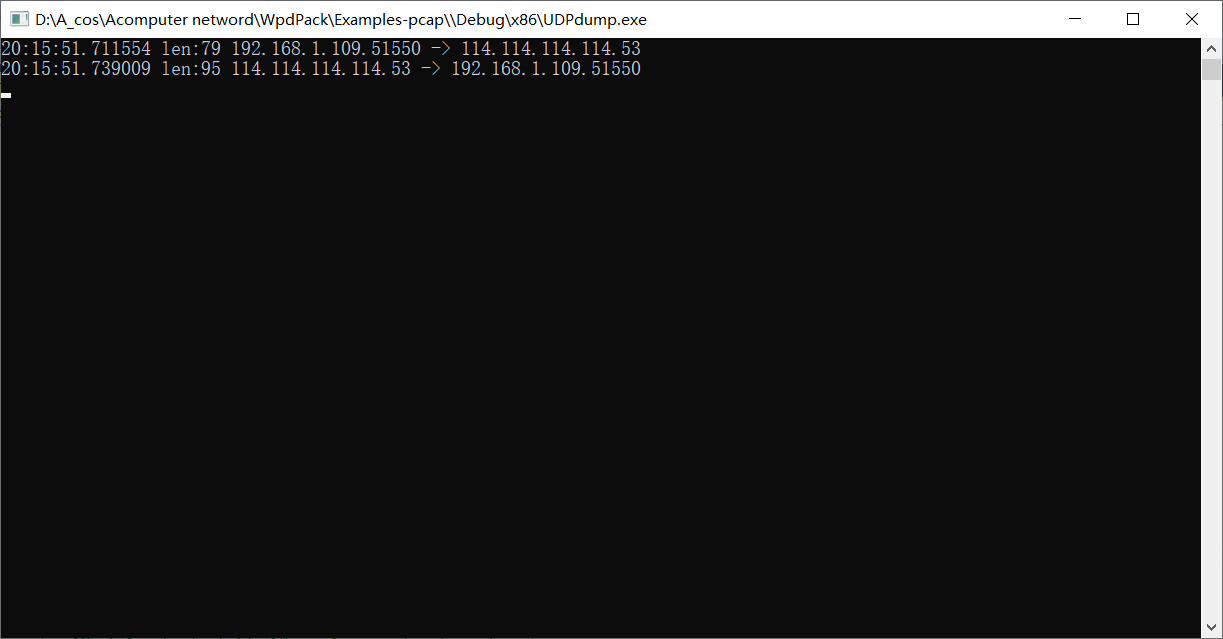


2.Wireshark调试

dns.pcap文件内容

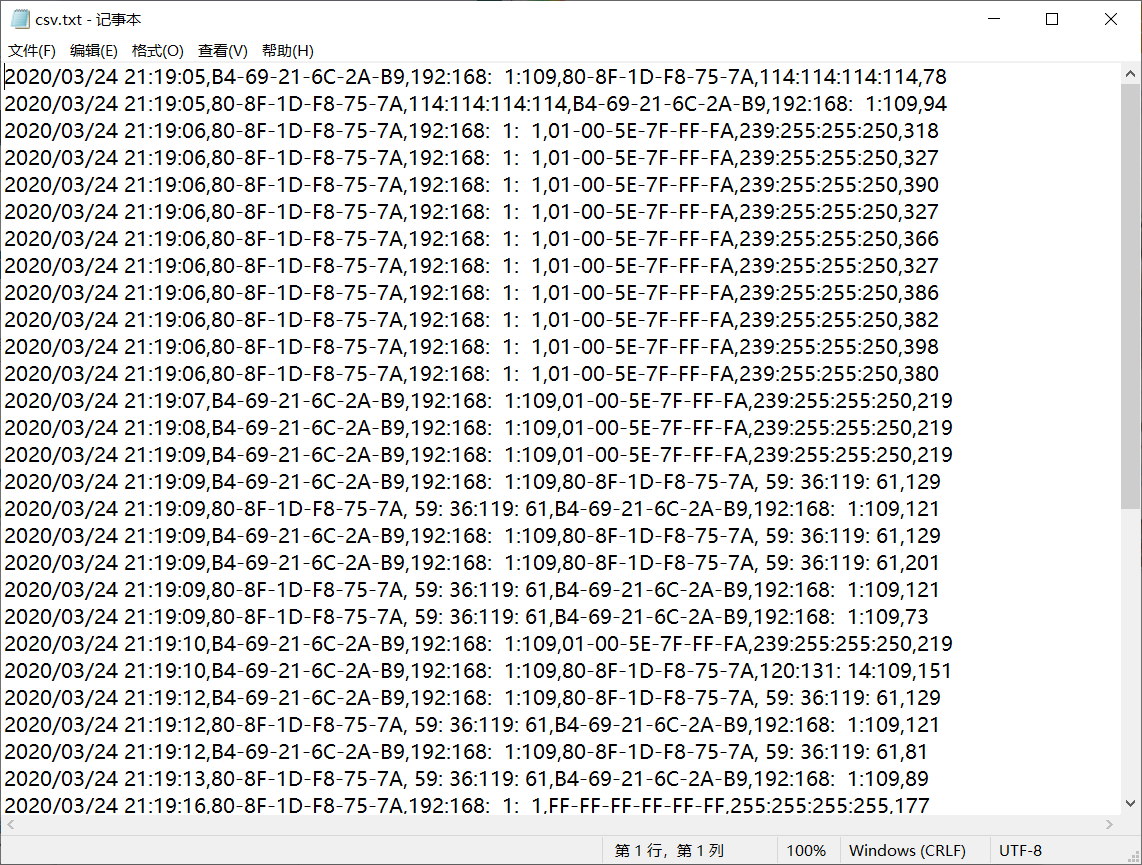
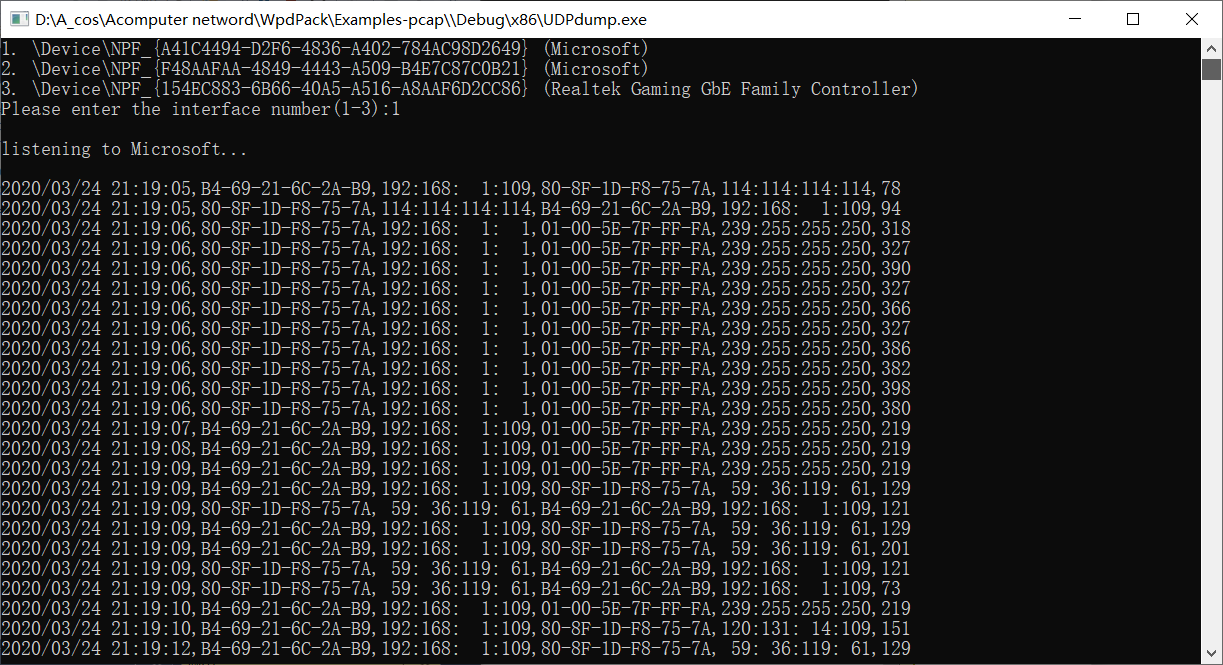


代码测试结果（调试）

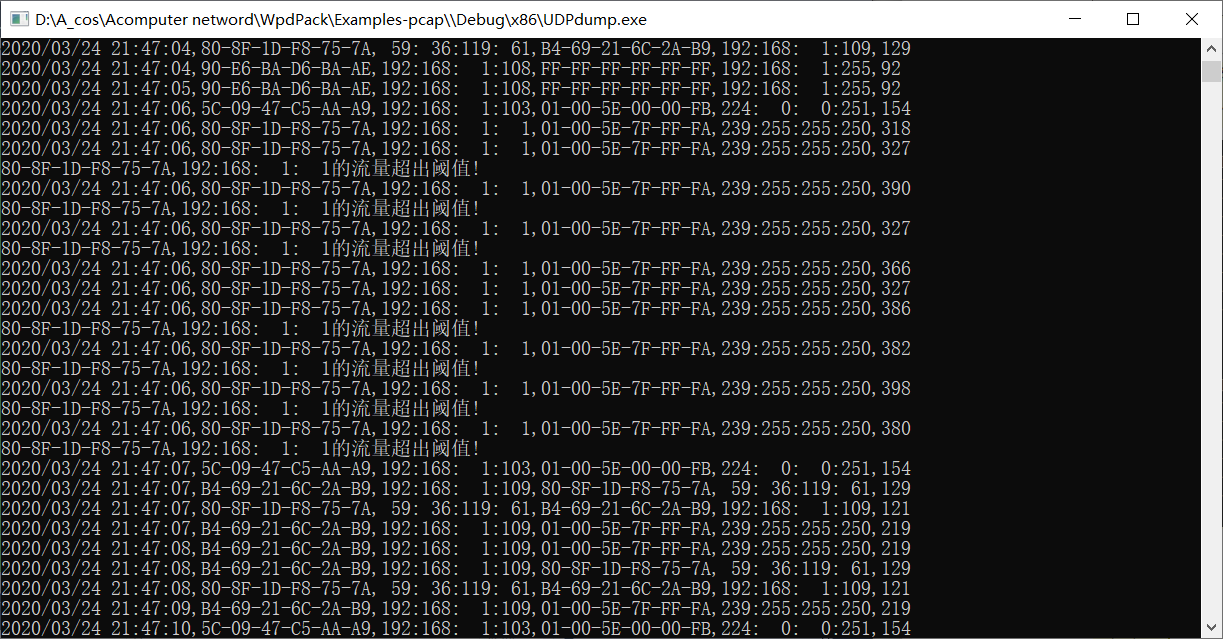


3.代码运行

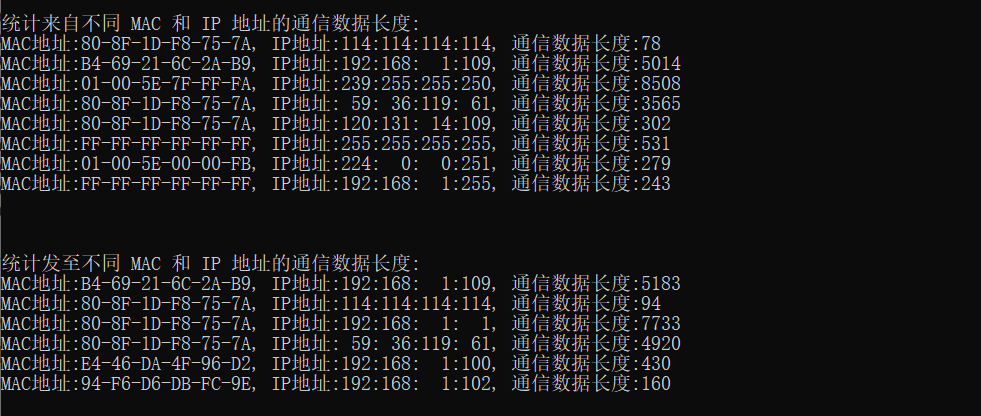
（1）监听运行结果以及输出至txt文件



（2）流量预警（1kb)



（3）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。



# 实验总结

通过这次实验，学会使用Wireshark监听网络上的数据流，弄清数据包的属性和MAC地址、IP地址的所在位置。统计流量做出流量预警，统计通信长度，也学会调用time来获取当前时间来实现实验。