

****

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1班**

**姓　　名 罗贤甫**

**学　　号 24320182203245**

**实验时间 2020年3月14日**

**2020 年 3 月 4 日**

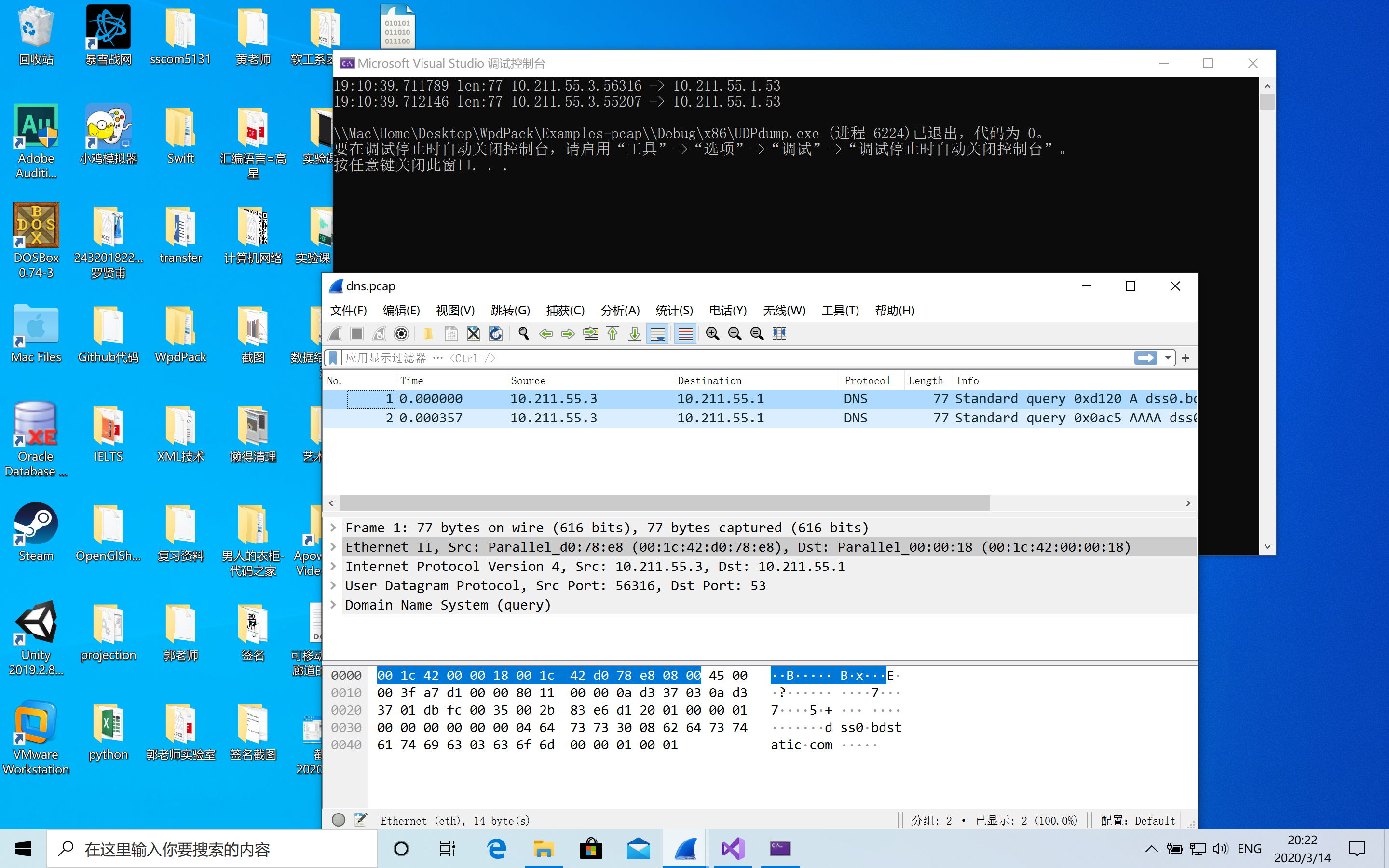
# 实验目的

用WinPCAP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，并加以记录与统计，对超过给定阀值的流量进行警告。

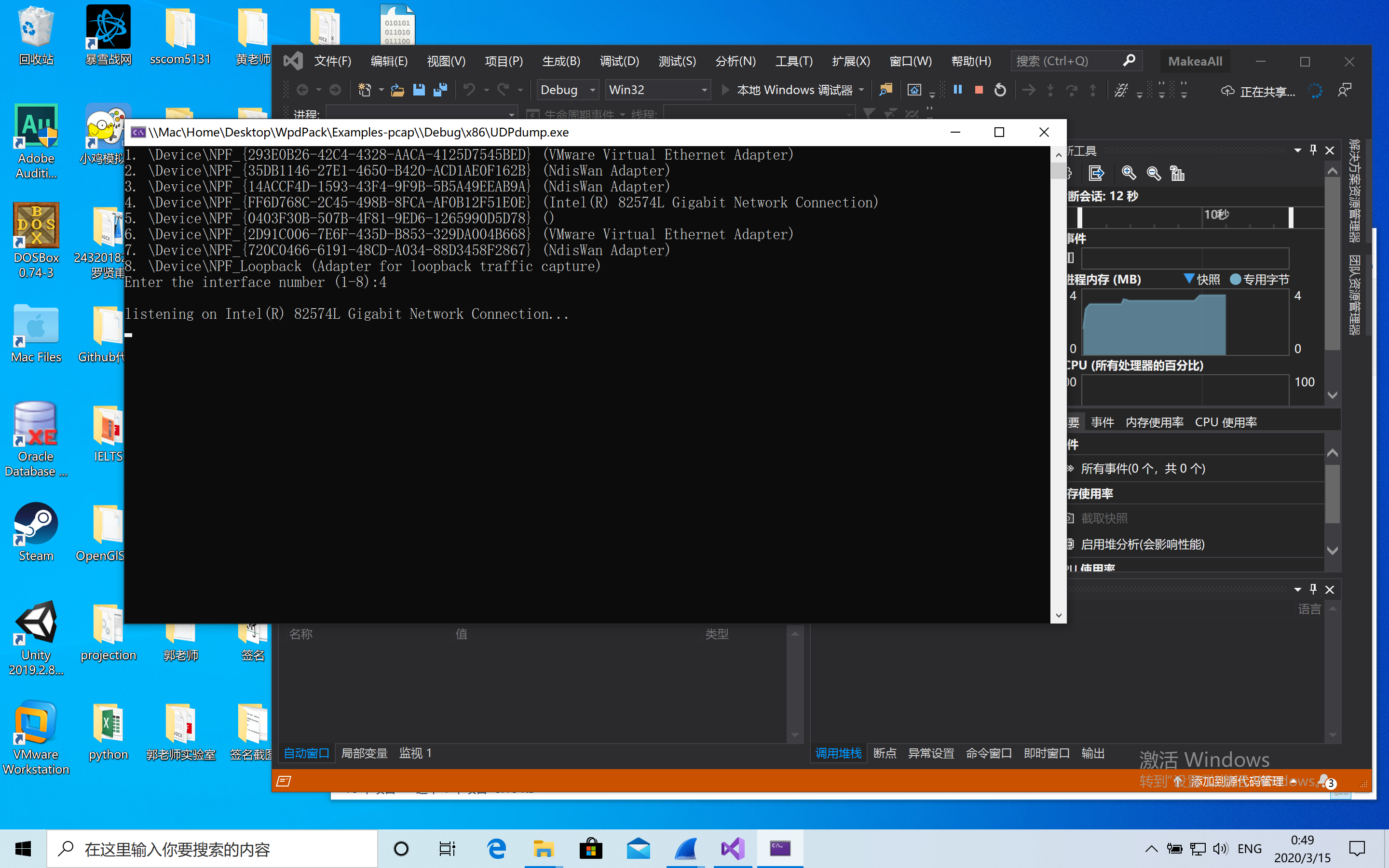
# 实验环境

Win10系统，Visual Studio 2019，WireShark软件，C语言

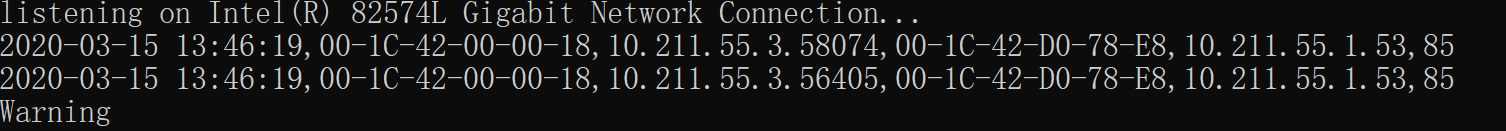
# 实验结果

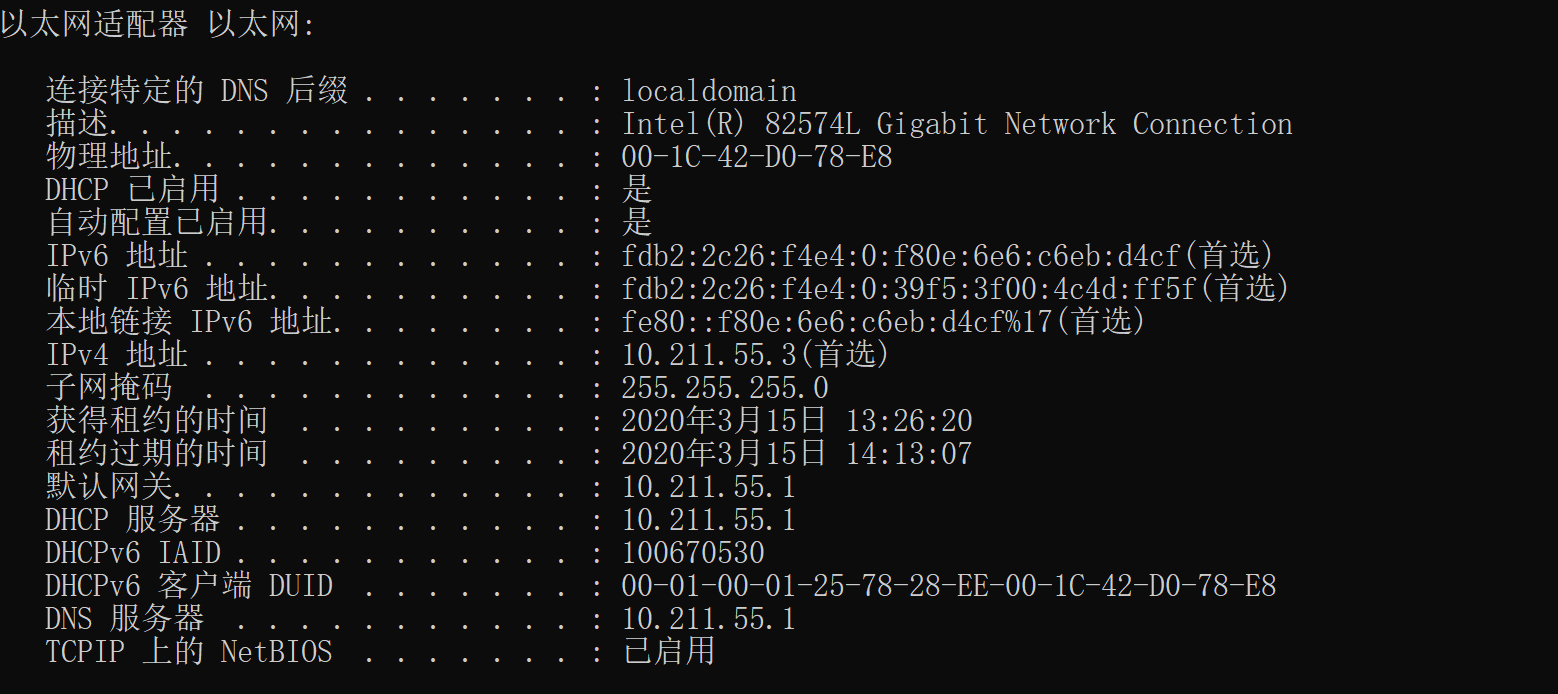


通过WireShark捕捉并加以实验



选择网卡编号



取阀值为256，在超过256时会发出警告，并按照实验手册输出时间，源MAC、源IP、目标MAC、目标IP、帧长度（以逗号间隔）达到实时监听的功能

在命令行窗口查看无限局域网 MAC 地址和 IP，与上述结果对照检查，结果正 确

# 实验总结

本次实验利用WireShark先捕获部分数据来调试，帮助我更好理解更好阅读本应有难度的代码，而老师的解说视频更是帮助我好好研究。通过这次实验，我对MAC地址以及IP地址都有了更深层次的理解，也更加理解网卡的运行过程。