

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 捕获并分析帧和IP报文**

**班　　级 软件工程2018级1班**

**姓　　名 郑钧元**

**学　　号 34520182201779**

**实验时间 2020年3月15日**

**2020 年 3 月 16 日**

# 实验目的

捕获并分析以太网的帧，获取目标与源网卡的MAC地址

• 了解认识获取本机地址

• 了解认识并获取远端MAC地址

‒ WinPCAP实现截取报文调试并处理

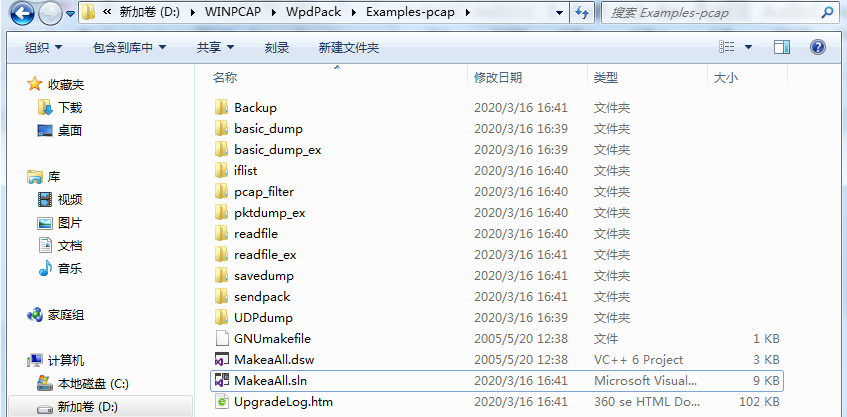
# 实验环境

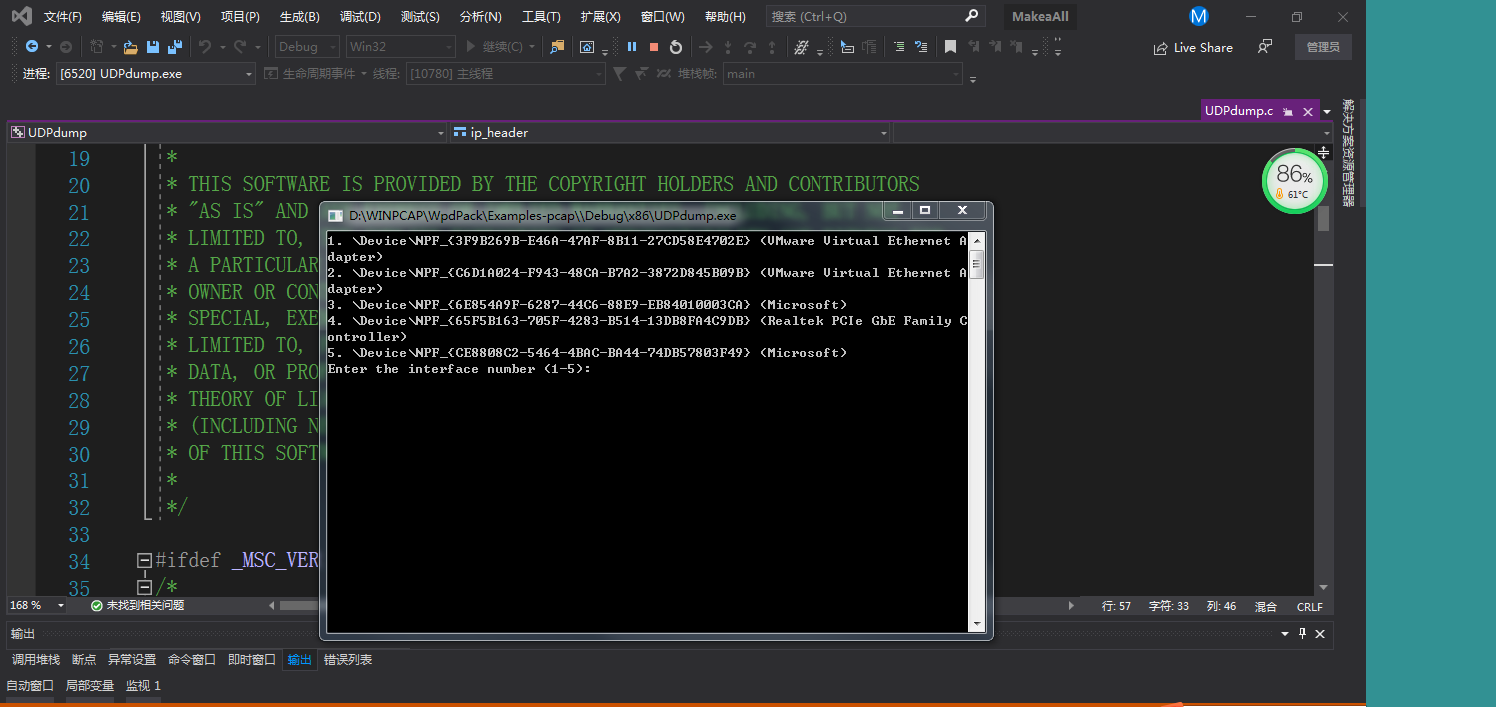
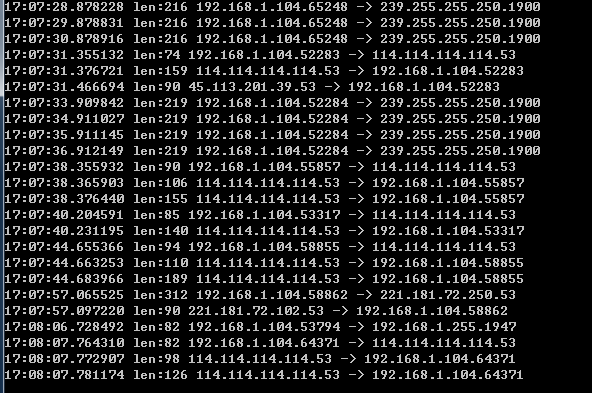
Windows 64位操作系统 WinPCAP Visual Studio 2019

编程语言 C 软件：WinPcap 科来数据包播放器 以及Wireshark软件

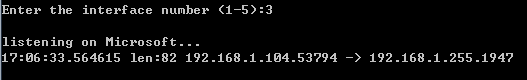
# 实验结果

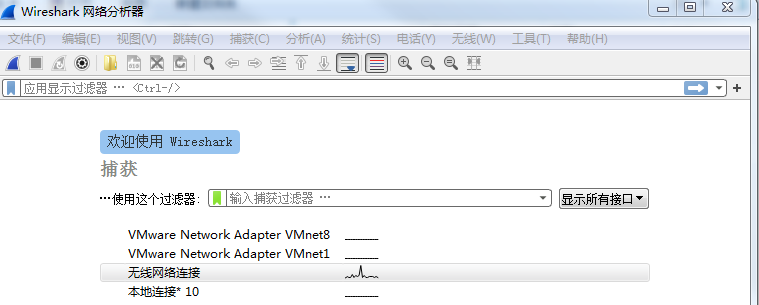
WinPcap 安装官网：<https://www.winpcap.org/> 安装所需的WinPcap和WpdPack

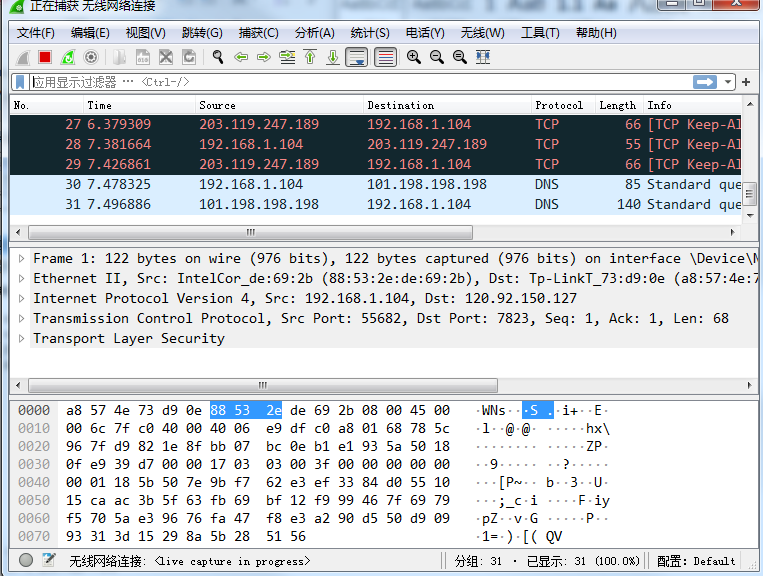
选取并用Visual Studio 2019 启动MakeaAll.sin项目程序。

对UDPdump.exe文件执行F10断点调试获取运行的main()文件并对它进行运行，得到5个网卡。

随机选取调试，得到结果……

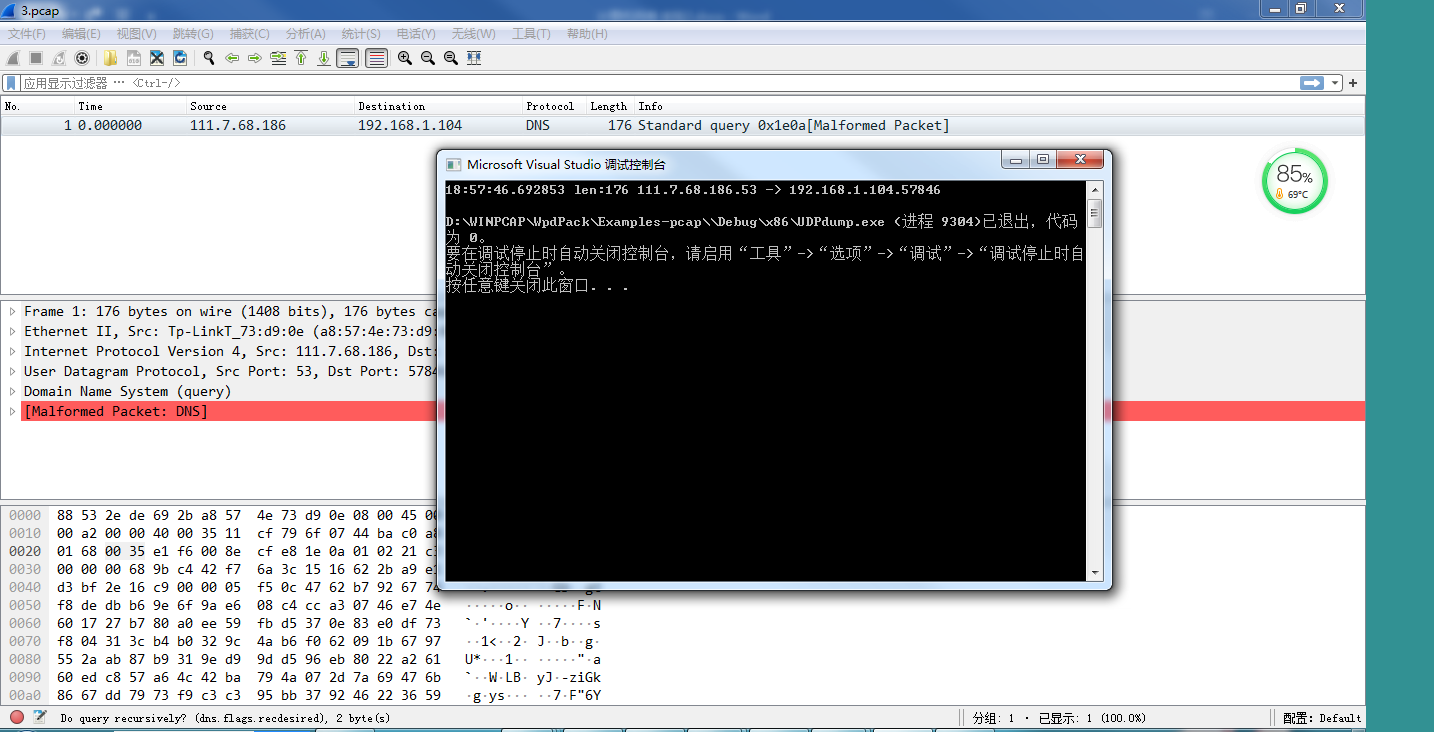


WireShark 安装+下载 <https://www.wireshark.org/download.html>



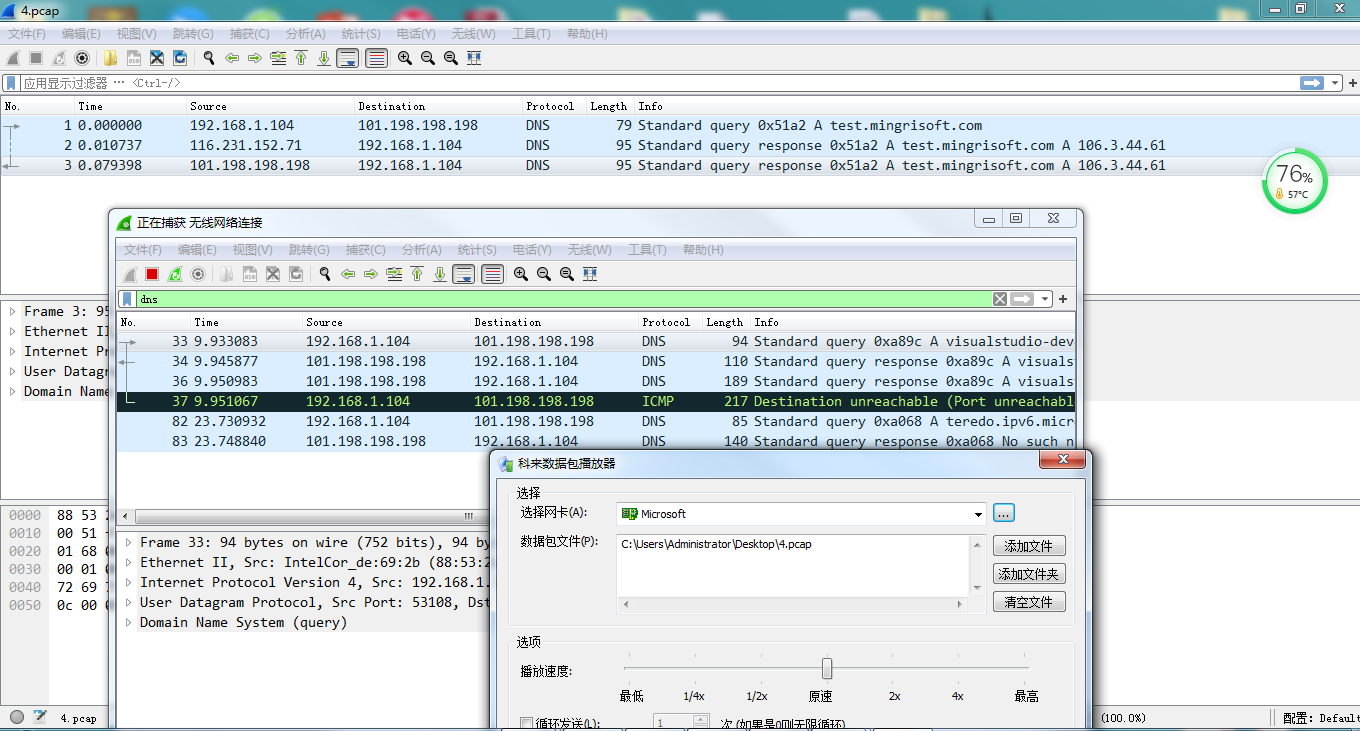
选择无线网络连接

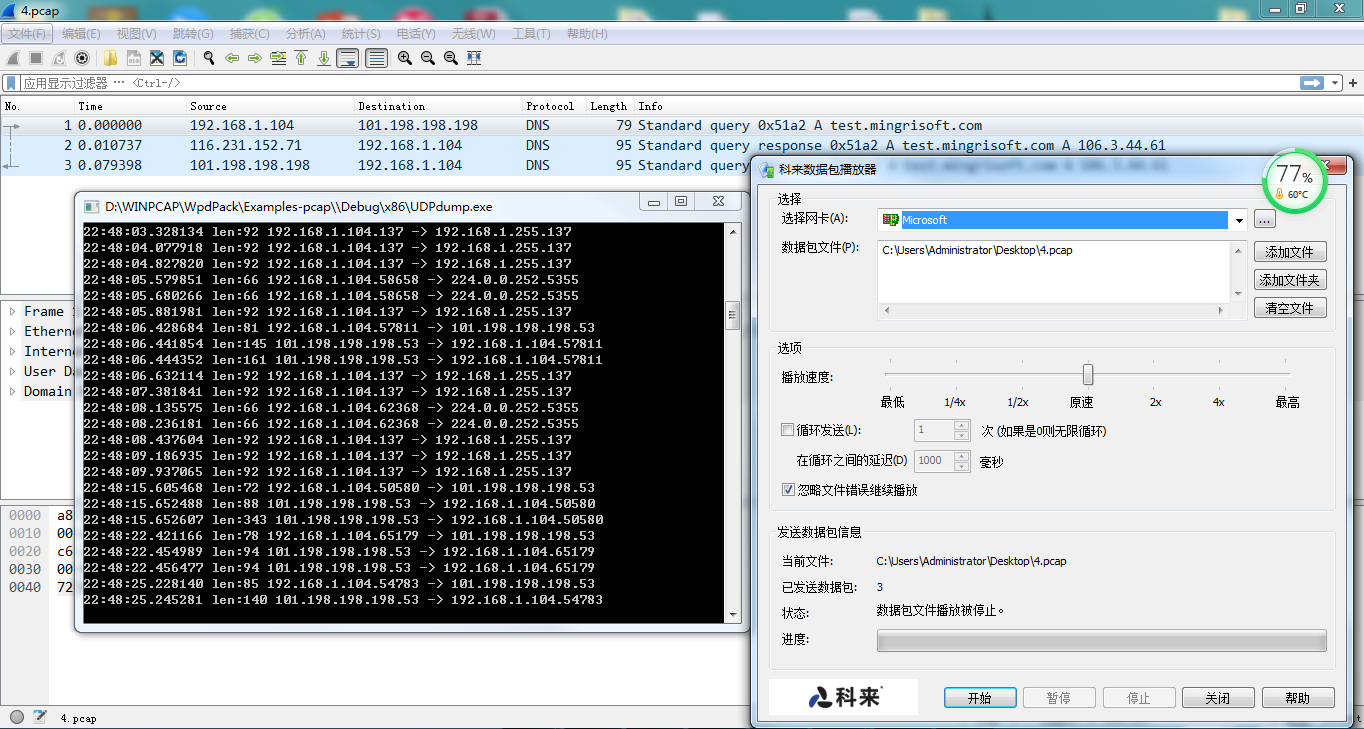
选取某一段作为报文导出并保存到目的文件夹

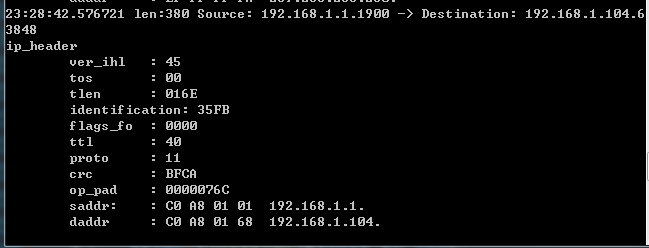
更改UDPdump.c文件以适配相应的报文。（可以从对应项目同级目录中找到readfile.c文件并截取/\* Open the capture file \*/段函数并copy在UDPdump.c中），运行程序，得到结果。

图：与报文内容基本一致

网卡模式验证报文：搭设服务器+科来数据包（安装目录<http://www.colasoft.com.cn/download/capsa_tool_pktplayer.php>）

打开科来数据包播放器，检查网卡后，单击添加文件的按钮，把之前保存的.pcap文件选定，最后再播放的同时打开Wireshark，观察到其显示出之前储存的.pcap文件的数据和报文。

再次运行程序，先播放科来数据包的文件，发现出现的文字在Visual Studio的.c文件中（后：.pcap文件 左前：C编译调试程序界面 右：运行的科来数据包播放器）

结合之前样例，对同样的C文件进行追加和改进，把原始定义的整个结构体的相关系数进行输出，得到更多的相关系数的处理、可视化，最后再执行运行，发现也是与相同原来的.pcap文件相同的Source 和Destination：

# 实验总结

本次实验涉及的应用软件范围广，初次接触网络编程自然比较陌生。需要下载一定的网络软件以进行调试和处理。其中比较重要的是Visual Studio 的开发应用，选取运行，以及相关辅助软件对报文的截取，编程中，我们对WinPcap包下的C文件，科来数据包播放器，以及Wireshark软件都进行了一定的实际操作和处理，发现报文可以实现截取，观察发现相同数据，表明成功。但是同时我们也不能避免一定的误码等问题发生。