

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　基于PCAP库侦听并分析网络流量**

**班　　级 数字媒体技术**

**姓　　名 陈海玲**

**学　　号 35820212203215**

**实验时间 2024年10月11日**

**2024 年 10 月 11 日**

填写说明

1. 本文件为Word模板文件，建议使用Microsoft Word 2019打开，在可填写的区域中如实填写；
2. 填表时，勿破坏排版，勿修改字体字号，打印成PDF文件提交；
3. 文件总大小尽量控制在1MB以下，勿超过5MB；
4. 应将材料清单上传在代码托管平台上；
5. 在学期最后一节课前按要求打包发送至cni21@qq.com。

# 实验目的

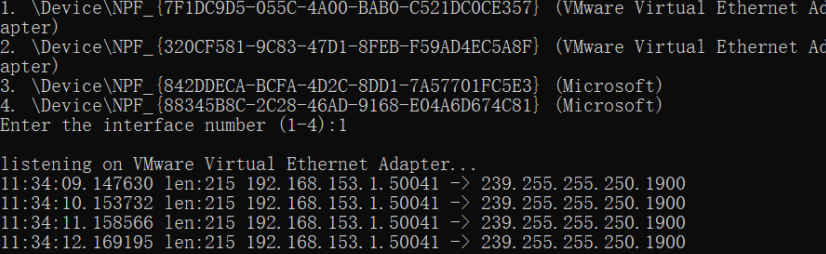
通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。掌握用 Wireshark 观察网络流量并辅助网络侦听相关的编程;掌握用 Libpcap 或WinPcap 库侦听并处理以太网帧和 I 报文的方法;熟悉以太网帧、P 报文、TCP段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制;熟悉帧头部或 皿 报文头部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念,熟悉段头部各字段和 FTP控制命令的指令和数据的含义。

# 实验环境

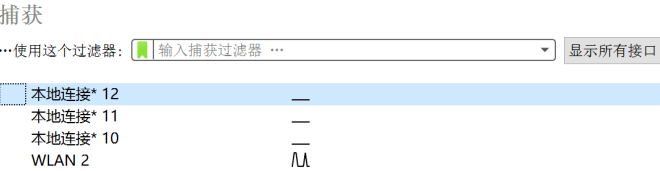
Windows10

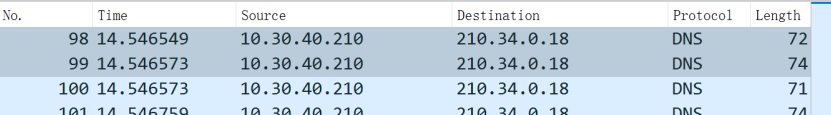
# 实验结果

（1）到winpcap官网（www.winpcap.org）下载程序和帮助文档。打开示例程序中的UDPdump项目，编译运行，运行截图如下：

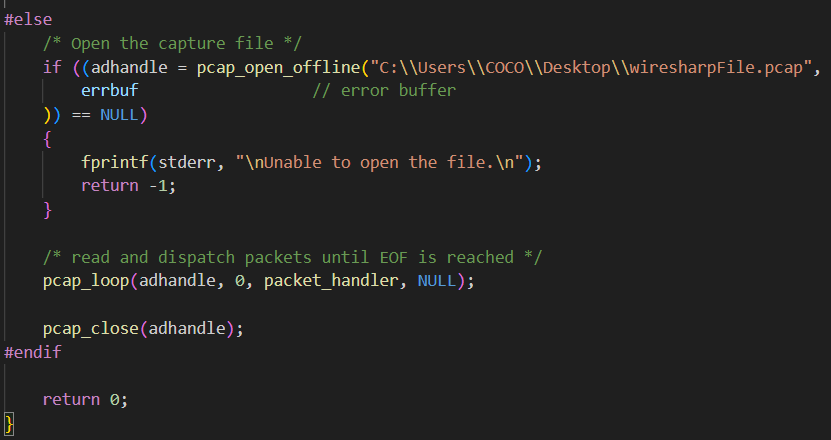


（2）到WirShark官网下载软件，安装后打开，可以看到现有的几个连接，点击WLAN2则开始捕获WLAN2上的数据包。在左上角输入dns可以过滤出dns。打开一个网页可以看到有数据包传输。 选中前2个记录，然后选择“文件”“导出特定分组”把文件保存下来，命名为wiresharkFile.pcap

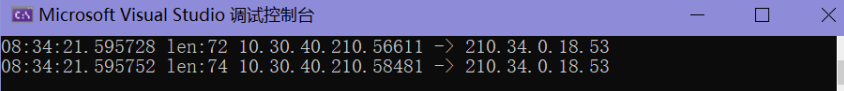




（3）修改UDPdump项目的代码，根据同一文件目录下的readfile工程的文件的读取pcap文件的代码段，使得UDPdump项目可以读取pcap文件。代码添加在return 0;之前，如下图：



运行截图如下，可以看到成功读取了（2）保存的wiresharkFile.pcap文件。



# 实验代码

本次实验的代码已上传于以下代码仓库：https://github.com/abanumber2/Computer-Network-and-Internet/tree/master

# 实验总结

本次实验通过使用 WinPcap 库和 WireShark 工具，展示了如何抓取、分析网络流量并保存为PCAP文件，再通过修改UDPdump项目代码实现读取和分析PCAP文件的功能，提供了实际动手操作的机会，增强了对网络数据捕获和分析的理解。