# 厦門大學



# 信息学院软件工程系

《计算机网络》实验报告

题	目	实验三捕获并分析帧和 IP 报文
班	级	数字媒体技术
姓	名,	陈海玲
学	号	35820212203215
实验时间		2024年10月18日

2024年10月18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。

## 1 实验目的

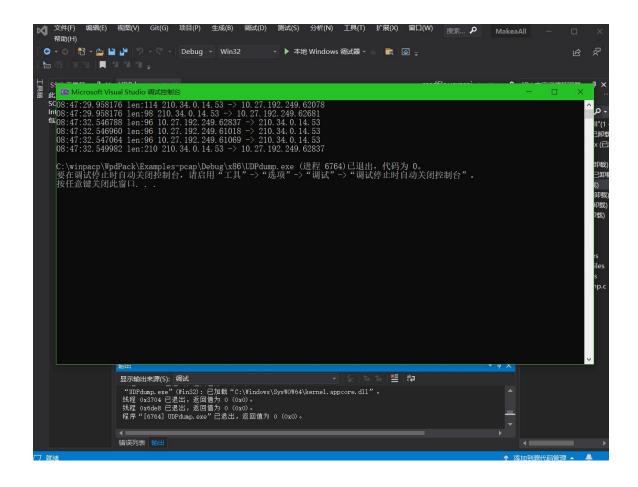
通过完成实验,理解数据链路层、网络层、传输层和应用层的基本原理。掌握用 Wireshark 观察网络流量并辅助网络侦听相关的编程;掌握用 Libpcap 或 WinPcap 库侦听并处理以太网帧和 I 报文的方法;熟悉以太网帧、P 报文、TCP 段和 FTP 命令的格式概念,掌握 TCP 协议的基本机制;熟悉帧头部或 皿 报文头部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念,熟悉段头部各字段和 FTP 控制命令的指令和数据的含义。

#### 2 实验环境

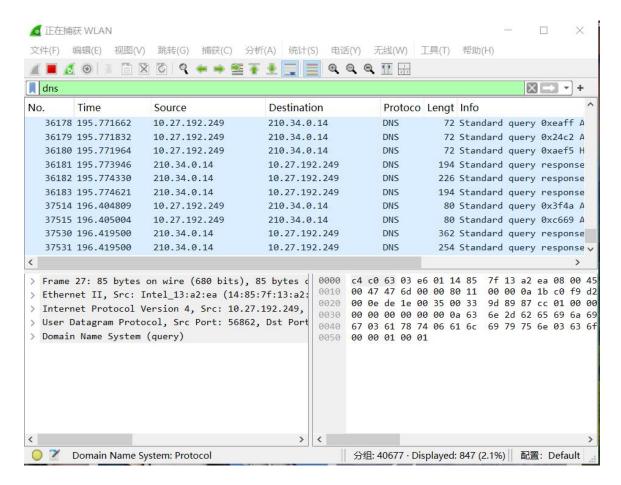
Windows10

#### 3 实验结果

- (1) 下载 winpacp、wireshark 以及科来数据包播放器。
- (2) 打开并且运行示例程序 UDPdump 项目,具体运行结果如下:



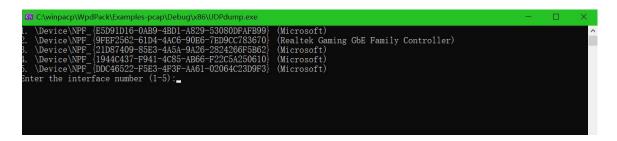
(2) 打开 wireshark,选择 WLAN 连接,在应用显示过滤器中输入 dns,则可以看到开始捕获数据包。选择前几个并且到处特定分则来保存文件,命名为"dns.pcap"



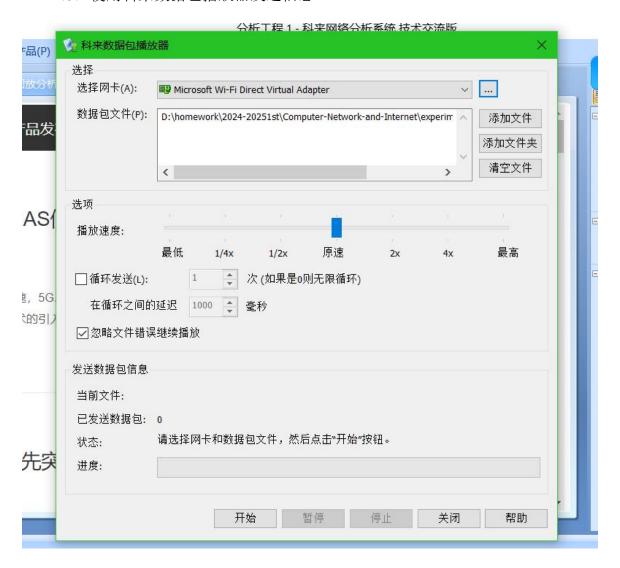
(3) 修改 UDPdump 项目的代码,根据同一文件目录下的 readfile 工程的文件 读取 pcap 文件的代码段,使得 UDPdump 项目可以读取 pcap 文件。具体代码修改 如下:

```
向 readfile (已卸载)
                                                                                             n readfile ex (已卸载)
if ((adhandle = pcap_open_offline("D:\\homework\\2024-20251st\\Computer-Network-and-Inter
                                                                                             [] savedump (已卸载)
   errbuf
                                                                                             🗋 sendpack (已卸载)
                           // error buffer
)) = NH(1)
                                                                                              ™ UDPdump
                                                                                               ■■引用
    fprintf(stderr, "\nUnable to open the file.\n");
                                                                                                🛅 外部依赖项
                                                                                                🔁 Header Files
                                                                                                Resource Files
                                                                                                Source Files
                                                                                               D DPdump.c
pcap_loop(adhandle, 0, packet_handler, NULL);
pcap_close(adhandle);
return 0;
```

(4) 运行如下,可以看到成功输出了之前保存的 pcap 文件:



(5) 使用科来数据包播放器发送信息



### 4 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

## 5 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。