

廈門大學



信息学院软件工程系

《计算机网络》实验报告

题 目 实验三 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。

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 IP 报文的方法;熟悉以太网帧、IP 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 IP 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) 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：

```
1. \Device\NPF_{7F1DC9D5-055C-4A00-BAB0-C521DC0CE357} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{320CF581-9C83-47D1-8FEB-F59AD4EC5A8F} (VMware Virtual Ethernet Adapter)
3. \Device\NPF_{842DDECA-BCFA-4D2C-8DD1-7A57701FC5E3} (Microsoft)
4. \Device\NPF_{88345B8C-2C28-46AD-9168-E04A6D674C81} (Microsoft)
Enter the interface number (1-4):1

listening on VMware Virtual Ethernet Adapter...
11:34:09.147630 len:215 192.168.153.1.50041 -> 239.255.255.250.1900
11:34:10.153732 len:215 192.168.153.1.50041 -> 239.255.255.250.1900
11:34:11.158566 len:215 192.168.153.1.50041 -> 239.255.255.250.1900
11:34:12.169195 len:215 192.168.153.1.50041 -> 239.255.255.250.1900
```

(2) 到 Wireshark 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

捕获

...使用这个过滤器: 显示所有接口

本地连接* 12	—
本地连接* 11	—
本地连接* 10	—
WLAN 2	∧∧

No.	Time	Source	Destination	Protocol	Length
98	14.546549	10.30.40.210	210.34.0.18	DNS	72
99	14.546573	10.30.40.210	210.34.0.18	DNS	74
100	14.546573	10.30.40.210	210.34.0.18	DNS	71
101	14.546750	10.30.40.210	210.34.0.18	DNS	74

(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:

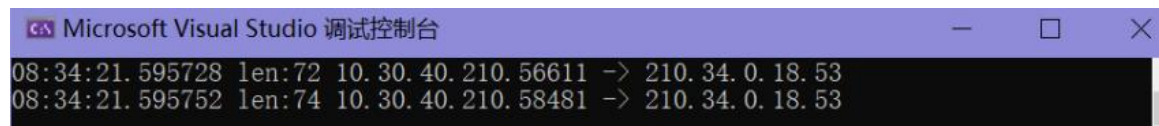
```
#else
/* Open the capture file */
if ((adhandle = pcap_open_offline("C:\\Users\\COCO\\Desktop\\wiresharkFile.pcap",
    errbuf
    // error buffer
)) == NULL)
{
    fprintf(stderr, "\nUnable to open the file.\n");
    return -1;
}

/* read and dispatch packets until EOF is reached */
pcap_loop(adhandle, 0, packet_handler, NULL);

pcap_close(adhandle);
#endif

return 0;
}
```

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



```
Microsoft Visual Studio 调试控制台
08:34:21.595728 len:72 10.30.40.210.56611 -> 210.34.0.18.53
08:34:21.595752 len:74 10.30.40.210.58481 -> 210.34.0.18.53
```

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。