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　用 PCAP 库侦听并分析网络流量

班　　级 软件工程 2018 级 2 班

姓　　名 李成洋

学　　号 24320182203220

实验时间 2020 年 3 月 22 日

2020 年 3 月 22 日

1 实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第一部分。
用 WinPCAP 或 libPcap 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，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告 警。对 Linux 用户，可以使用 libpcap 编程实现。
程序在文件上输出形如下列 CSV 格式的日志：
时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔）
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D572,192.168.33.2,1536 每隔一段时间（如 1 分钟），程序统计来自不同 MAC 和 IP 地址的通信数据长度， 统计发至不同 MAC 和 IP 地址的通信数据长度。

2 实验环境

Windows10

语言：C++

3 实验结果

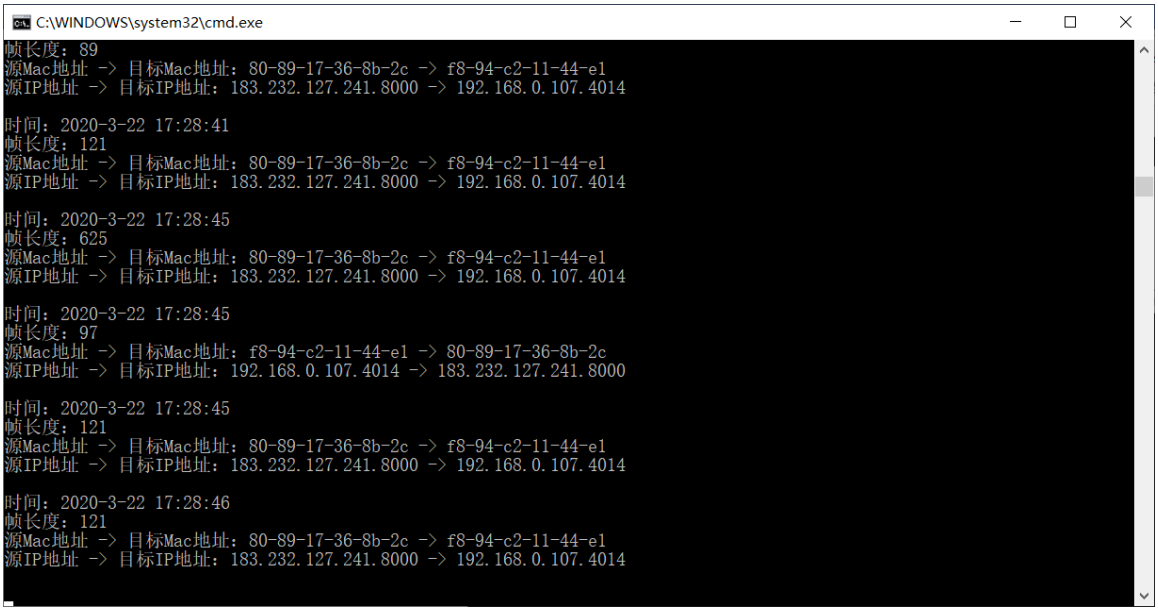
1. 用 IPCONFIG.EXE 显示计算机中网络适配器的 IP 地址、子网掩码及默认网关

```
C:\Users\HP>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : DESKTOP-5CF6086
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

无线局域网适配器 本地连接* 1:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址. . . . . . . . . . . . . : F8-94-C2-11-44-E2
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 本地连接* 3:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   物理地址. . . . . . . . . . . . . : FA-94-C2-11-44-E1
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   物理地址. . . . . . . . . . . . . : 00-50-56-C0-00-01
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::89d1:aef0:a8b2:bcd4%4(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.75.1(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
```

2. 通过 WinPcap 分析以太网的帧，记录目标与源 MAC 和 IP 地址：

   运行结果如下：

```
C:\WINDOWS\system32\cmd.exe
所有网络设备如下:
1. 网卡名: \Device\NPF_{DC0E184B-5410-45FA-9BDA-D23E4B00AB83}网卡描述: (VMware Virtual Ethernet Adapter)
2. 网卡名: \Device\NPF_{B8BA0E4E-4934-470E-B15F-22A4346213BC}网卡描述: (Microsoft)
3. 网卡名: \Device\NPF_{150BF340-48D8-4E67-831D-45F1BDB79720}网卡描述: (VMware Virtual Ethernet Adapter)
4. 网卡名: \Device\NPF_{B316C15E-EA30-434D-A91B-858ADC1CE879}网卡描述: (Microsoft)
5. 网卡名: \Device\NPF_{657D7CAD-9B0A-44A5-95BD-D689EADEC42C}网卡描述: (Microsoft)

请输入你要监听的网卡序号(1—5): 5

正在监听Microsoft...
时间: 2020-3-22 17:22:06
帧长度: 121
源Mac地址 -> 目标Mac地址: 80-89-17-36-8b-2c -> f8-94-c2-11-44-e1
源IP地址 -> 目标IP地址: 183.232.127.241.8000 -> 192.168.0.107.4014

时间: 2020-3-22 17:22:14
帧长度: 125
源Mac地址 -> 目标Mac地址: f8-94-c2-11-44-e1 -> 80-89-17-36-8b-2c
源IP地址 -> 目标IP地址: 192.168.0.107.5000 -> 58.251.121.55.8000

时间: 2020-3-22 17:22:15
帧长度: 83
源Mac地址 -> 目标Mac地址: f8-94-c2-11-44-e1 -> 80-89-17-36-8b-2c
源IP地址 -> 目标IP地址: 192.168.0.107.64529 -> 192.168.1.1.53

时间: 2020-3-22 17:22:15
帧长度: 147
源Mac地址 -> 目标Mac地址: 80-89-17-36-8b-2c -> f8-94-c2-11-44-e1
源IP地址 -> 目标IP地址: 192.168.1.1.53 -> 192.168.0.107.64529
```

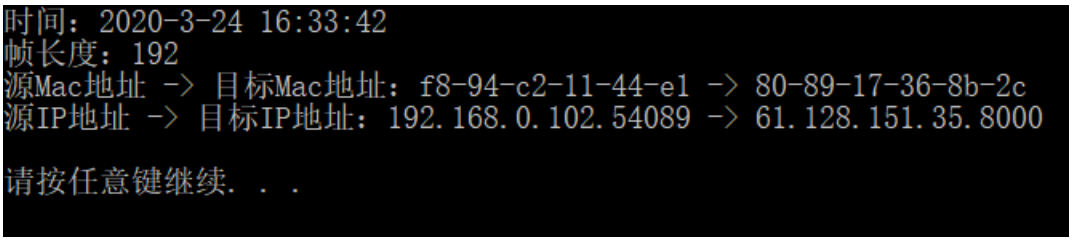


同时设置流量预警，当帧长度大于 1024 时预警：

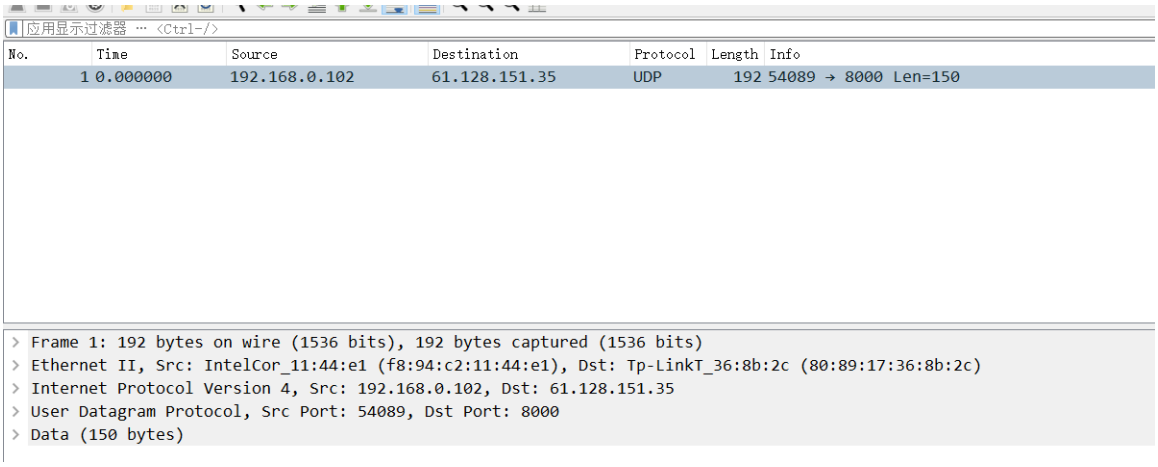
```
//输出数据包的长度
cout << "帧长度：" << header->len << endl;
//当流量超过1M时，发出警告
if (header->len > 1024)cout << "Warning: Transmission over 1024." << endl;
```

3. 通过 wireshark 把选中的报文导出为.pcap 文件

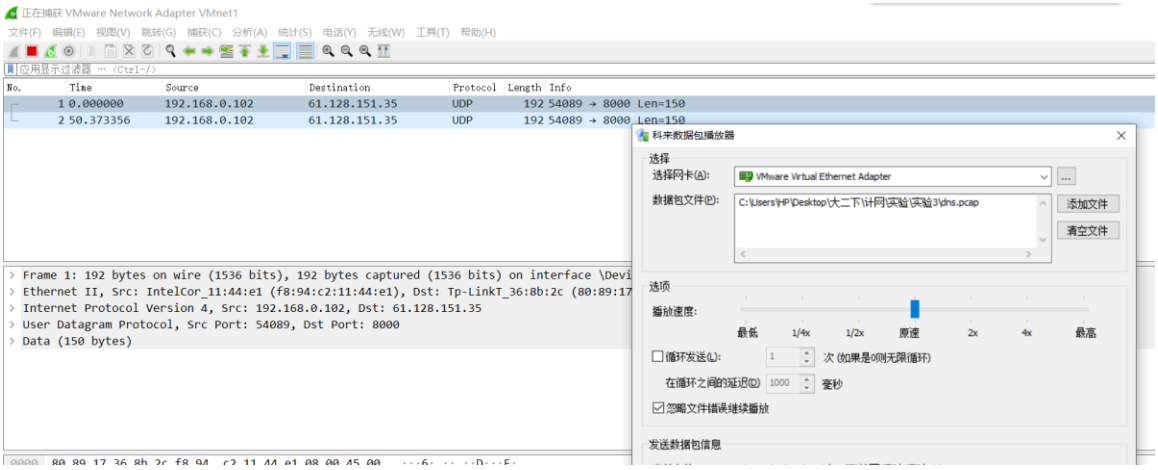
通过 readfile 中的读 pcap 文件代码读取 dns.pcap 结果如下：



对比.pcap文件：



4. 用科来数据包播放器发送报文



4 实验总结

本次实验的主要收获是：通过学习 WinPcap 里的示例代码，对数据报头部格式，UDP 头部协议格式，Mac 地址和 IP 地址有了更多的了解。知道了获取数据包的大致流程为：获取所有网络设备，然后跳转到所选择的适配器，打开适配器，之后再检查链路层，确认支持以太网后设置掩码和筛选器，对数据进行筛选。之后就调用回调函数抓取包。虽说目前对这个过程有了一个大致的了解，但是若细究这里面的

相关原理，我还不能说清楚，同时老师在视频中说的调试方式还只是进行了简单的尝试，后续还需要更多的尝试和学习。