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 陈怡心

学　　号 24320182203180

实验时间 2020 年 3 月 11 日

2020 年 3 月 22 日

1 实验目的

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。

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

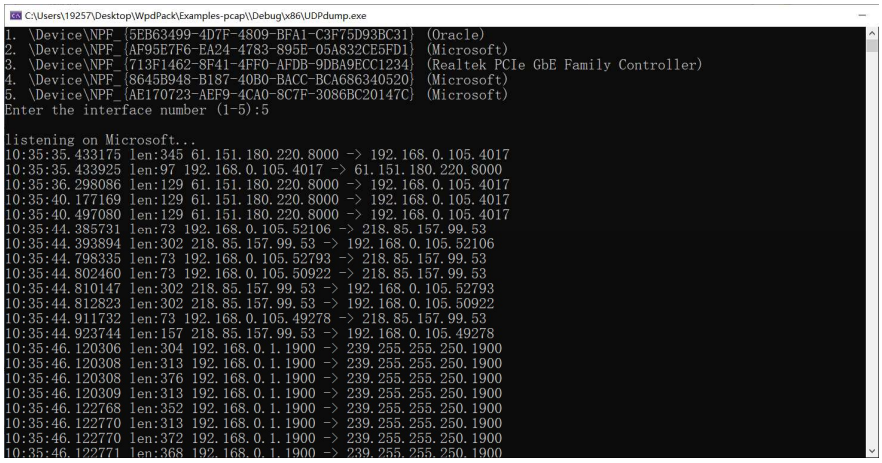
操作系统：Windows 10

编程语言：C 语言

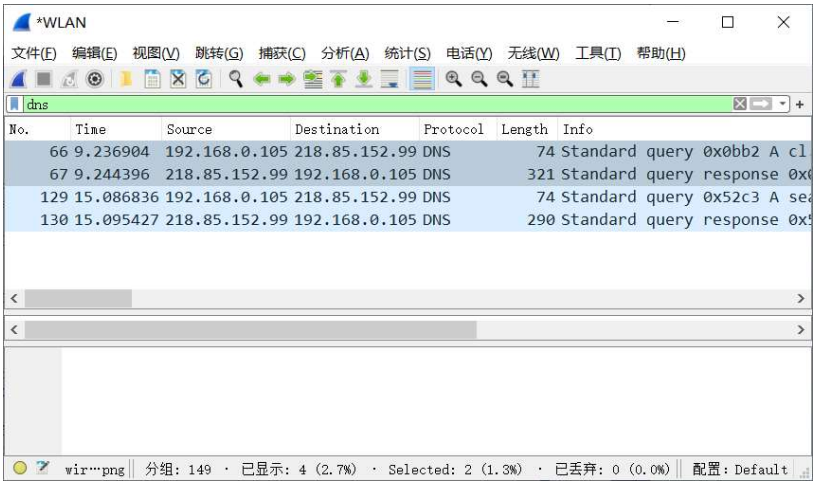
3 实验结果

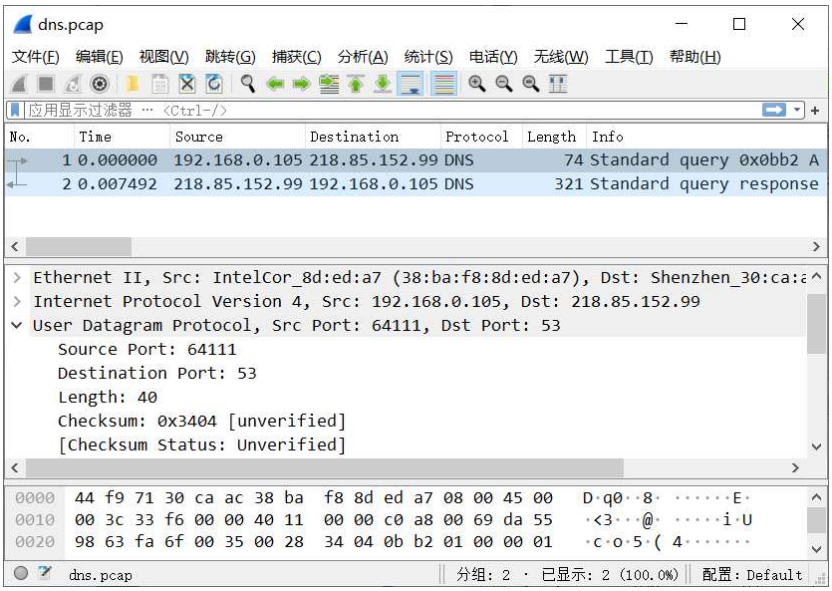
1、示例程序

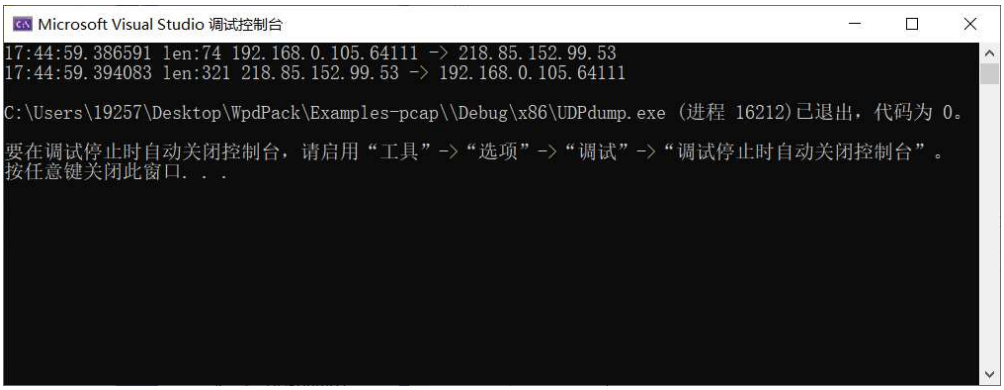
（1）直接运行



（2）利用 Wireshark 调试







2、实验要求程序

（1）在文件上输出日志

（2）流量告警（0.5M 为例截图）

（3）统计来自/发至不同 MAC 和 IP 地址的通信数据长度（30s 为例截图）

```
统计来自不同 MAC 和 IP 地址的通信数据长度:
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 62: 48: 59, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:144: 52:207:196, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 25: 72: 80, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:114:233:221:  5, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 89:216: 33, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:115:203:103: 81, 通信数据长度:2846
MAC地址:44-F9-71-30-CA-AC, IP地址:222:181:200:216, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 86:170:254, 通信数据长度:58
MAC地址:38-BA-F8-8D-ED-A7, IP地址:192:168:  0:105, 通信数据长度:152185
MAC地址:44-F9-71-30-CA-AC, IP地址:182: 47:127:  5, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:223:150:207:191, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址: 49: 80:223: 15, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:114:222: 79:175, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:125:127:203:102, 通信数据长度:2620685
MAC地址:44-F9-71-30-CA-AC, IP地址:114:101:247: 28, 通信数据长度:729
MAC地址:44-F9-71-30-CA-AC, IP地址:119: 97:171: 27, 通信数据长度:565
MAC地址:44-F9-71-30-CA-AC, IP地址:114:222:118:154, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:114:226:185:101, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:114:226: 56:172, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:180:115:184:231, 通信数据长度:348
MAC地址:01-00-5E-7F-FF-FA, IP地址:239:255:255:250, 通信数据长度:3461
MAC地址:44-F9-71-30-CA-AC, IP地址:120: 38:198: 51, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:218: 85:157: 99, 通信数据长度:230
MAC地址:44-F9-71-30-CA-AC, IP地址:182:201:242:  9, 通信数据长度:1218
MAC地址:44-F9-71-30-CA-AC, IP地址:113: 69:165: 73, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:115:234: 13:222, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址: 14:122:149: 36, 通信数据长度:290
```

```
统计发至不同 MAC 和 IP 地址的通信数据长度:
MAC地址:38-BA-F8-8D-ED-A7, IP地址:192:168:  0:105, 通信数据长度:2652060
MAC地址:44-F9-71-30-CA-AC, IP地址:223:150:207:191, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:114:222:118:154, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:125:127:203:102, 通信数据长度:39630
MAC地址:44-F9-71-30-CA-AC, IP地址:114:222: 79:175, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:183:143: 89:227, 通信数据长度:348
MAC地址:AC-CA-30-71-F9-44, IP地址:125:127:203:102, 通信数据长度:89152
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 62: 48: 59, 通信数据长度:348
MAC地址:AC-CA-30-71-F9-44, IP地址:119: 97:171: 27, 通信数据长度:11356
MAC地址:44-F9-71-30-CA-AC, IP地址:114:101:247: 28, 通信数据长度:232
MAC地址:AC-CA-30-71-F9-44, IP地址:114:233:221:  5, 通信数据长度:58
MAC地址:44-F9-71-30-CA-AC, IP地址:119: 97:171: 27, 通信数据长度:1194
MAC地址:AC-CA-30-71-F9-44, IP地址:117: 86:170:254, 通信数据长度:58
MAC地址:44-F9-71-30-CA-AC, IP地址:192:168:  0:  1, 通信数据长度:3751
MAC地址:44-F9-71-30-CA-AC, IP地址:114:226: 56:172, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:115:234: 13:222, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:180:115:184:231, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:222:214:222:177, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:218: 85:157: 99, 通信数据长度:923
MAC地址:44-F9-71-30-CA-AC, IP地址:182:201:242:  9, 通信数据长度:50
MAC地址:44-F9-71-30-CA-AC, IP地址:222:181:200:216, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 89:216: 33, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:182: 47:127:  5, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:114:226:185:101, 通信数据长度:348
MAC地址:44-F9-71-30-CA-AC, IP地址:113: 69:165: 73, 通信数据长度:290
MAC地址:44-F9-71-30-CA-AC, IP地址: 14:122:149: 36, 通信数据长度:232
MAC地址:44-F9-71-30-CA-AC, IP地址:117: 25: 72: 80, 通信数据长度:290
MAC地址:44-F9-71-30-CA-AC, IP地址: 49: 80:223: 15, 通信数据长度:232
```

4 实验总结

通过这次实验学习了如何使用 WinPCAP 库监听网卡的数据流、统计流量、统计数据长度以及如何用 Wireshark 测试监听程序，此外，也更加了解数据包的格式及属性，为下次实验打下基础。