

# 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 用 PCAP 库侦听并解析 FTP 口令

班 级 软件工程 2018 级 3 班

姓 名 沈黄隽

学 号 24320182203260

实验时间 2020 年 3 月 11 日

2020 年 3 月 24 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 WinPACP 库侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地址

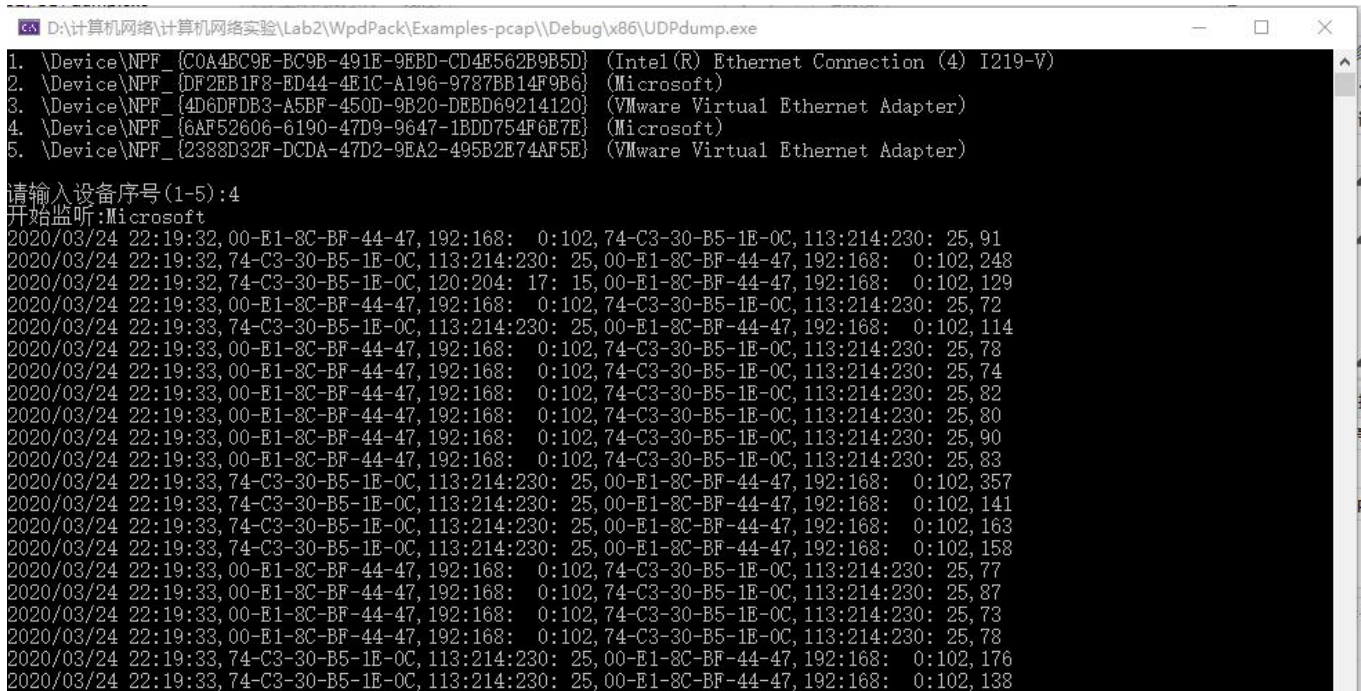
## 2 实验环境

操作环境：Visual Studio 2019、WpdPack

编程语言：C 语言

## 3 实验结果

1、基于 WinPCAP 工具包制作程序，实现监听网络上的数据流，解析发送方与接收方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值的流量进行告警。其中流量阈值为 0.5M，统计数据的时间长度间隔为 20 秒。



```
D:\计算机网络\计算机网络实验\Lab2\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. \Device\NPF_{COA4BC9E-BC9B-491E-9EBD-CD4E562B9B5D} (Intel(R) Ethernet Connection (4) I219-V)
2. \Device\NPF_{DF2EB1F8-ED44-4E1C-A196-9787BB14F9B6} (Microsoft)
3. \Device\NPF_{4D6DFDB3-A5BF-450D-9B20-DEBD69214120} (VMware Virtual Ethernet Adapter)
4. \Device\NPF_{6AF52606-6190-47D9-9647-1BDD754F6E7E} (Microsoft)
5. \Device\NPF_{2388D32F-DCDA-47D2-9EA2-495B2E74AF5E} (VMware Virtual Ethernet Adapter)

请输入设备序号(1-5):4
开始监听:Microsoft
2020/03/24 22:19:32, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 91
2020/03/24 22:19:32, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 248
2020/03/24 22:19:32, 74-C3-30-B5-1E-0C, 120:204: 17: 15, 00-E1-8C-BF-44-47, 192:168: 0:102, 129
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 72
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 114
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 78
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 74
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 82
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 80
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 90
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 83
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 357
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 141
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 163
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 158
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 77
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 87
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 73
2020/03/24 22:19:33, 00-E1-8C-BF-44-47, 192:168: 0:102, 74-C3-30-B5-1E-0C, 113:214:230: 25, 78
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 176
2020/03/24 22:19:33, 74-C3-30-B5-1E-0C, 113:214:230: 25, 00-E1-8C-BF-44-47, 192:168: 0:102, 138
```

2.每隔一段时间（20s），程序统计来自不同 MAC 和 IP 地址的通信数据长度，并以“Mac Address，IP Address，通信数据长度”的格式显示在输出流显示出来

统计来自不同 MAC 和 IP 地址的通信数据长度：

```
Mac Address :74-C3-30-B5-1E-0C, IP Address:120:204: 17: 15, 通信数据长度:421
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:214:230: 25, 通信数据长度:1283
Mac Address :00-E1-8C-BF-44-47, IP Address:192:168: 0:102, 通信数据长度:5158
Mac Address :00-E1-8C-BF-44-47, IP Address:239:255:255:250, 通信数据长度:3464
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:215: 2:222, 通信数据长度:166
Mac Address :74-C3-30-B5-1E-0C, IP Address:221:181: 72:250, 通信数据长度:312
```

统计发至不同 MAC 和 IP 地址的通信数据长度：

```
Mac Address :00-E1-8C-BF-44-47, IP Address:192:168: 0:102, 通信数据长度:2187
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:214:230: 25, 通信数据长度:3691
Mac Address :74-C3-30-B5-1E-0C, IP Address:120:204: 17: 15, 通信数据长度:1161
Mac Address :74-C3-30-B5-1E-0C, IP Address:192:168: 0: 1, 通信数据长度:3464
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:215: 2:222, 通信数据长度:306
```

统计来自不同 MAC 和 IP 地址的通信数据长度：

```
Mac Address :74-C3-30-B5-1E-0C, IP Address:120:204: 17: 15, 通信数据长度:421
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:214:230: 25, 通信数据长度:1515
Mac Address :00-E1-8C-BF-44-47, IP Address:192:168: 0:102, 通信数据长度:6436
Mac Address :00-E1-8C-BF-44-47, IP Address:239:255:255:250, 通信数据长度:3464
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:215: 2:222, 通信数据长度:166
Mac Address :74-C3-30-B5-1E-0C, IP Address:221:181: 72:250, 通信数据长度:312
Mac Address :01-00-5E-7F-FF-FA, IP Address:239:255:255:250, 通信数据长度:219
```

统计发至不同 MAC 和 IP 地址的通信数据长度：

```
Mac Address :00-E1-8C-BF-44-47, IP Address:192:168: 0:102, 通信数据长度:2633
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:214:230: 25, 通信数据长度:4195
Mac Address :74-C3-30-B5-1E-0C, IP Address:120:204: 17: 15, 通信数据长度:1935
Mac Address :74-C3-30-B5-1E-0C, IP Address:192:168: 0: 1, 通信数据长度:3464
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:215: 2:222, 通信数据长度:306
```

统计来自不同 MAC 和 IP 地址的通信数据长度：

```
Mac Address :74-C3-30-B5-1E-0C, IP Address:120:204: 17: 15, 通信数据长度:1148
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:214:230: 25, 通信数据长度:1824
Mac Address :00-E1-8C-BF-44-47, IP Address:192:168: 0:102, 通信数据长度:9280
Mac Address :00-E1-8C-BF-44-47, IP Address:239:255:255:250, 通信数据长度:6928
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:215: 2:222, 通信数据长度:166
Mac Address :74-C3-30-B5-1E-0C, IP Address:221:181: 72:250, 通信数据长度:312
Mac Address :01-00-5E-7F-FF-FA, IP Address:239:255:255:250, 通信数据长度:876
```

统计发至不同 MAC 和 IP 地址的通信数据长度：

```
Mac Address :00-E1-8C-BF-44-47, IP Address:192:168: 0:102, 通信数据长度:4326
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:214:230: 25, 通信数据长度:5497
Mac Address :74-C3-30-B5-1E-0C, IP Address:120:204: 17: 15, 通信数据长度:3477
Mac Address :74-C3-30-B5-1E-0C, IP Address:192:168: 0: 1, 通信数据长度:6928
Mac Address :74-C3-30-B5-1E-0C, IP Address:113:215: 2:222, 通信数据长度:306
```



3、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）

```

csv.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2020/03/24 22:22:26,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,120:204: 17: 15,81
2020/03/24 22:22:29,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,120:204: 17: 15,81
2020/03/24 22:22:34,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,91
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,248
2020/03/24 22:22:34,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,120:204: 17: 15,81
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,309
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,321
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,381
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,297
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,345
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,317
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,375
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,373
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,377
2020/03/24 22:22:34,74-C3-30-B5-1E-0C,192:168: 0: 1,00-E1-8C-BF-44-47,239:255:255:250,369
2020/03/24 22:22:35,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,73
2020/03/24 22:22:35,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,74
2020/03/24 22:22:35,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,78
2020/03/24 22:22:35,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,164
2020/03/24 22:22:35,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,77
2020/03/24 22:22:35,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,75
2020/03/24 22:22:35,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,176
2020/03/24 22:22:35,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,361
2020/03/24 22:22:35,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,78
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,87
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,406
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,358
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,360
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,84
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,79
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,83
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,128
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:215: 2:222,87
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,144
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,270
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,72
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:215: 2:222,79
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:215: 2:222,00-E1-8C-BF-44-47,192:168: 0:102,144
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,248
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:215: 2:222,00-E1-8C-BF-44-47,192:168: 0:102,162
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,162
2020/03/24 22:22:36,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,94
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,189
2020/03/24 22:22:36,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129
2020/03/24 22:22:42,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,74
2020/03/24 22:22:42,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,135
2020/03/24 22:22:54,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129
2020/03/24 22:22:58,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,94
2020/03/24 22:22:58,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,200
2020/03/24 22:23:00,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129
2020/03/24 22:23:02,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,169
2020/03/24 22:23:02,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,120:204: 17: 15,97
2020/03/24 22:23:02,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,120:204: 17: 15,81

```



2020/03/24 22:23:02,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,89  
 2020/03/24 22:23:02,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:06,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,221:181: 72:250,312  
 2020/03/24 22:23:09,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,75  
 2020/03/24 22:23:09,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,142  
 2020/03/24 22:23:12,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:14,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:19,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:20,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:37,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,74  
 2020/03/24 22:23:37,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,122  
 2020/03/24 22:23:38,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:38,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:40,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,79  
 2020/03/24 22:23:40,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,127  
 2020/03/24 22:23:49,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:23:49,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,74  
 2020/03/24 22:23:49,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,255  
 2020/03/24 22:23:54,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,129  
 2020/03/24 22:24:00,00-E1-8C-BF-44-47,192:168: 0:102,01-00-5E-7F-FF-FA,239:255:255:250,219  
 2020/03/24 22:24:01,00-E1-8C-BF-44-47,192:168: 0:102,01-00-5E-7F-FF-FA,239:255:255:250,219  
 2020/03/24 22:24:02,00-E1-8C-BF-44-47,192:168: 0:102,01-00-5E-7F-FF-FA,239:255:255:250,219  
 2020/03/24 22:24:02,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,120:204: 17: 15,81  
 2020/03/24 22:24:02,74-C3-30-B5-1E-0C,120:204: 17: 15,00-E1-8C-BF-44-47,192:168: 0:102,89  
 2020/03/24 22:24:03,00-E1-8C-BF-44-47,192:168: 0:102,01-00-5E-7F-FF-FA,239:255:255:250,219  
 2020/03/24 22:24:05,00-E1-8C-BF-44-47,192:168: 0:102,74-C3-30-B5-1E-0C,113:214:230: 25,71  
 2020/03/24 22:24:05,74-C3-30-B5-1E-0C,113:214:230: 25,00-E1-8C-BF-44-47,192:168: 0:102,468

#### 4、流量超过阈值（0.5M）告警部分代码示例

```

//流量超过阈值告警
for (int i = 0; i < flow_alarm_list->length; ++i) {
    if ((flow_alarm_list->HEAD + i)->total >= LIMIT) {
        printf("%02X-%02X-%02X-%02X-%02X-%02X, %3d:%3d:%3d:%3d的流量超出阈值! \n",
            (flow_alarm_list->HEAD + i)->MAC.byte0,
            (flow_alarm_list->HEAD + i)->MAC.byte1,
            (flow_alarm_list->HEAD + i)->MAC.byte2,
            (flow_alarm_list->HEAD + i)->MAC.byte3,
            (flow_alarm_list->HEAD + i)->MAC.byte4,
            (flow_alarm_list->HEAD + i)->MAC.byte5,
            (flow_alarm_list->HEAD + i)->IP.byte0,
            (flow_alarm_list->HEAD + i)->IP.byte1,
            (flow_alarm_list->HEAD + i)->IP.byte2,
            (flow_alarm_list->HEAD + i)->IP.byte3);
    }
}

```

## 4 实验总结

基于 WinPCAP 工具包制作程序，实现监听网络上的数据流，解析发送方与接收方的 MAC 和 IP 地址，统计来自不同 Mac 和 IP 地址的通信数据长度，对帧监听以及收发有了更深入的了解