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 陈渝璇

学　　号 **24320182203181**

实验时间 **2020** 年 **3** 月 **11** 日

2020 年 **3** 月 **24** 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。

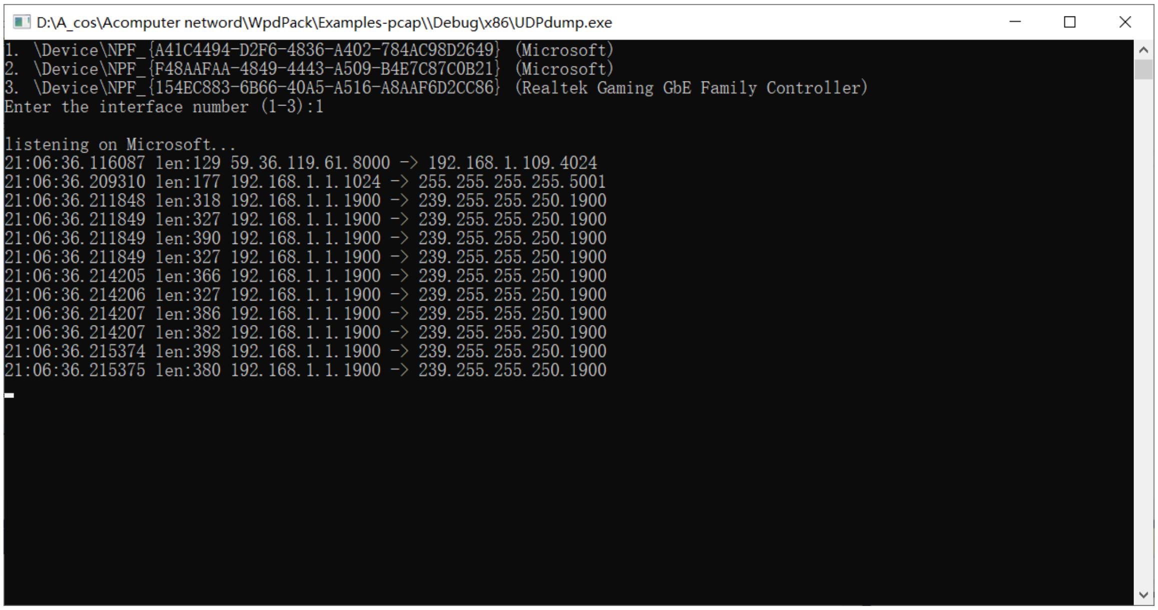
2 实验环境

操作系统：Window10

编程语言：c 语言

3 实验结果

1 示例代码运行测试：

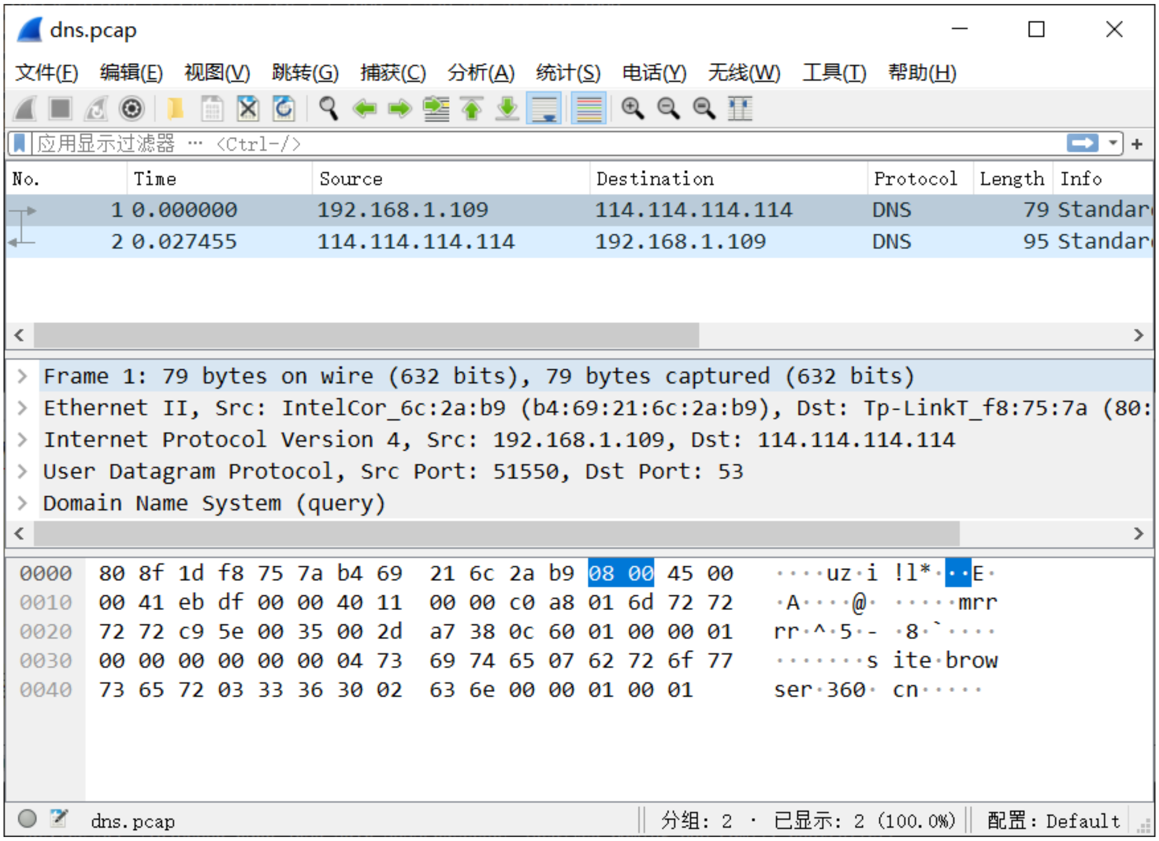


D:\A_cos\Acomputer netword\WpdPack\Examples-pcap\\Debug\x86\UDPdump.exe

```
1.  \Device\NPF_{A41C4494-D2F6-4836-A402-784AC98D2649}  (Microsoft)
2.  \Device\NPF_{F48AAFAA-4849-4443-A509-B4E7C87C0B21}  (Microsoft)
3.  \Device\NPF_{154EC883-6B66-40A5-A516-A8AAF6D2CC86}  (Realtek Gaming GbE Family Controller)
Enter the interface number (1-3):1

listening on Microsoft...
21:06:36.116087 len:129 59.36.119.61.8000 -> 192.168.1.109.4024
21:06:36.209310 len:177 192.168.1.1.1024 -> 255.255.255.255.5001
21:06:36.211848 len:318 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.211849 len:327 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.211849 len:390 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.211849 len:327 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.214205 len:366 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.214206 len:327 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.214207 len:386 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.214207 len:382 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.215374 len:398 192.168.1.1.1900 -> 239.255.255.250.1900
21:06:36.215375 len:380 192.168.1.1.1900 -> 239.255.255.250.1900
```

2.Wireshark 调试

dns.pcap 文件内容

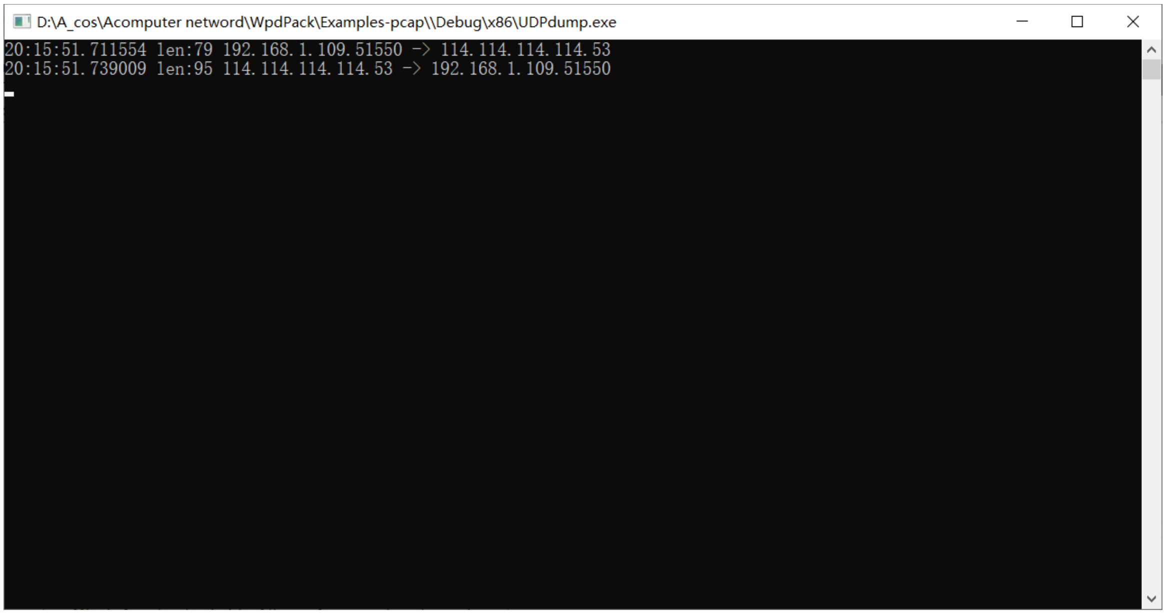

dns.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time        Source            Destination       Protocol  Length  Info
    1 0.000000    192.168.1.109     114.114.114.114   DNS           79  Standar
    2 0.027455    114.114.114.114   192.168.1.109     DNS           95  Standar
```

```
> Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Ethernet II, Src: IntelCor_6c:2a:b9 (b4:69:21:6c:2a:b9), Dst: Tp-LinkT_f8:75:7a (80:
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 114.114.114.114
> User Datagram Protocol, Src Port: 51550, Dst Port: 53
> Domain Name System (query)
```

```
0000  80 8f 1d f8 75 7a b4 69  21 6c 2a b9 08 00 45 00   ····uz·i !l*···E·
0010  00 41 eb df 00 00 40 11  00 00 c0 a8 01 6d 72 72   ·A····@· ·····mrr
0020  72 72 c9 5e 00 35 00 2d  a7 38 0c 60 01 00 00 01   rr·^·5·- ·8·`····
0030  00 00 00 00 00 00 04 73  69 74 65 07 62 72 6f 77   ·······s ite·brow
0040  73 65 72 03 33 36 30 02  63 6e 00 00 01 00 01      ser·360· cn·····
```

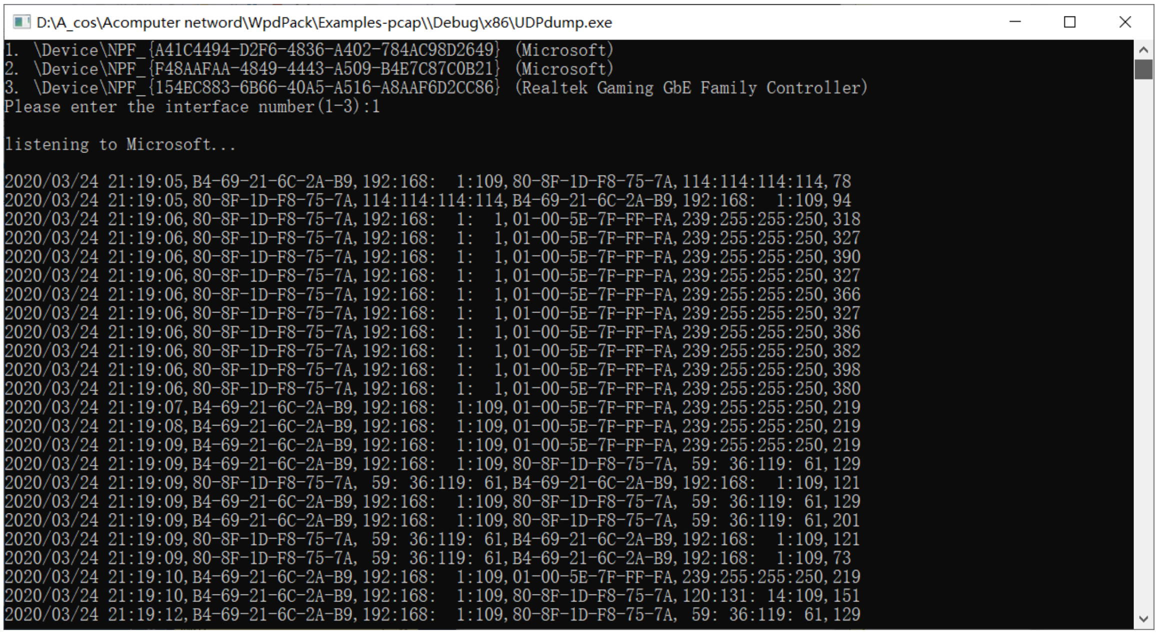
代码测试结果（调试）


D:\A_cos\Acomputer netword\WpdPack\Examples-pcap\\Debug\x86\UDPdump.exe

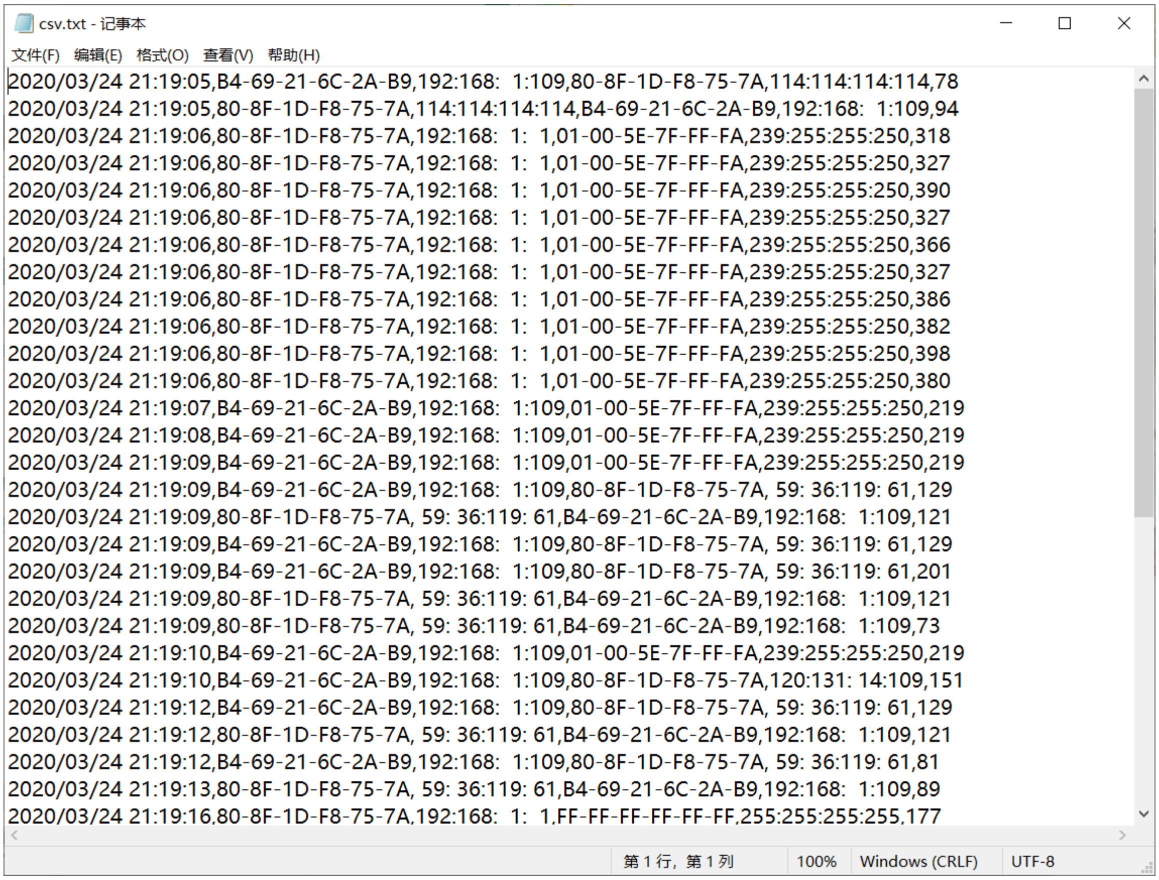
```
20:15:51.711554 len:79 192.168.1.109.51550 -> 114.114.114.114.53
20:15:51.739009 len:95 114.114.114.114.53 -> 192.168.1.109.51550
```

3.代码运行

（1）监听运行结果以及输出至 txt 文件

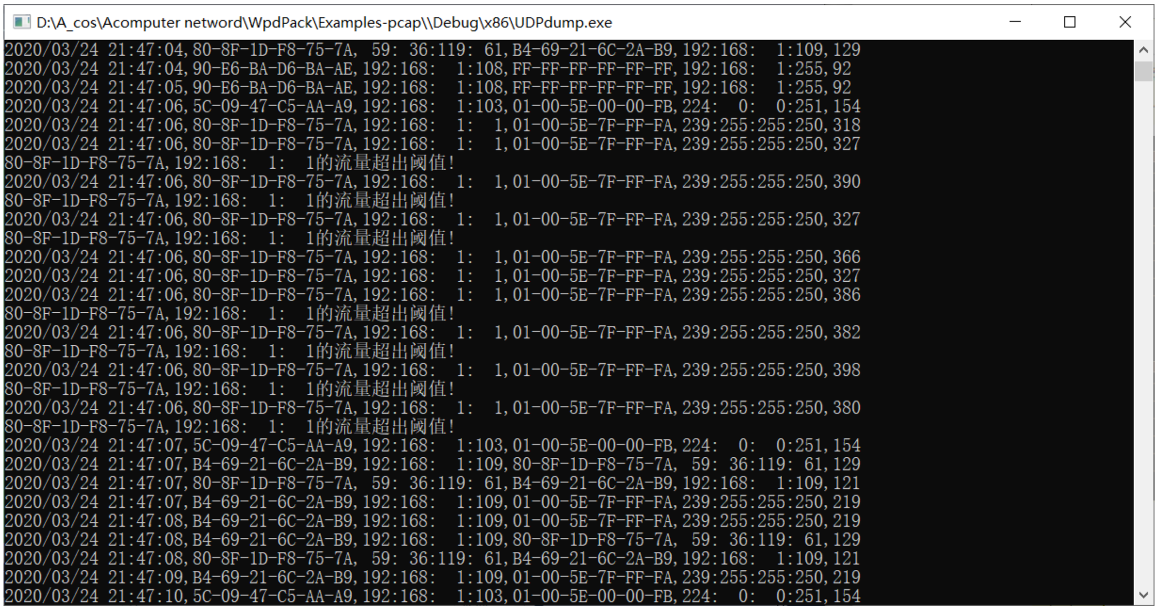

D:\A_cos\Acomputer netword\WpdPack\Examples-pcap\\Debug\x86\UDPdump.exe

```
1.  \Device\NPF_{A41C4494-D2F6-4836-A402-784AC98D2649}  (Microsoft)
2.  \Device\NPF_{F48AAFAA-4849-4443-A509-B4E7C87C0B21}  (Microsoft)
3.  \Device\NPF_{154EC883-6B66-40A5-A516-A8AAF6D2CC86}  (Realtek Gaming GbE Family Controller)
Please enter the interface number(1-3):1

listening to Microsoft...

2020/03/24 21:19:05,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A,114:114:114:114,78
2020/03/24 21:19:05,80-8F-1D-F8-75-7A,114:114:114:114,B4-69-21-6C-2A-B9,192:168:  1:109,94
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,318
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,390
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,366
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,386
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,382
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,398
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,380
2020/03/24 21:19:07,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:08,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:19:09,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,201
2020/03/24 21:19:09,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:19:09,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,73
2020/03/24 21:19:10,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:10,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A,120:131: 14:109,151
2020/03/24 21:19:12,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
```



```
2020/03/24 21:19:05,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A,114:114:114:114,78
2020/03/24 21:19:05,80-8F-1D-F8-75-7A,114:114:114:114,B4-69-21-6C-2A-B9,192:168:  1:109,94
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,318
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,390
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,366
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,386
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,382
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,398
2020/03/24 21:19:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,380
2020/03/24 21:19:07,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:08,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:19:09,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:19:09,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,201
2020/03/24 21:19:09,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:19:09,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,73
2020/03/24 21:19:10,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:19:10,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A,120:131: 14:109,151
2020/03/24 21:19:12,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:19:12,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:19:12,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,81
2020/03/24 21:19:13,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,89
2020/03/24 21:19:16,80-8F-1D-F8-75-7A,192:168:  1:  1,FF-FF-FF-FF-FF-FF,255:255:255:255,177
```

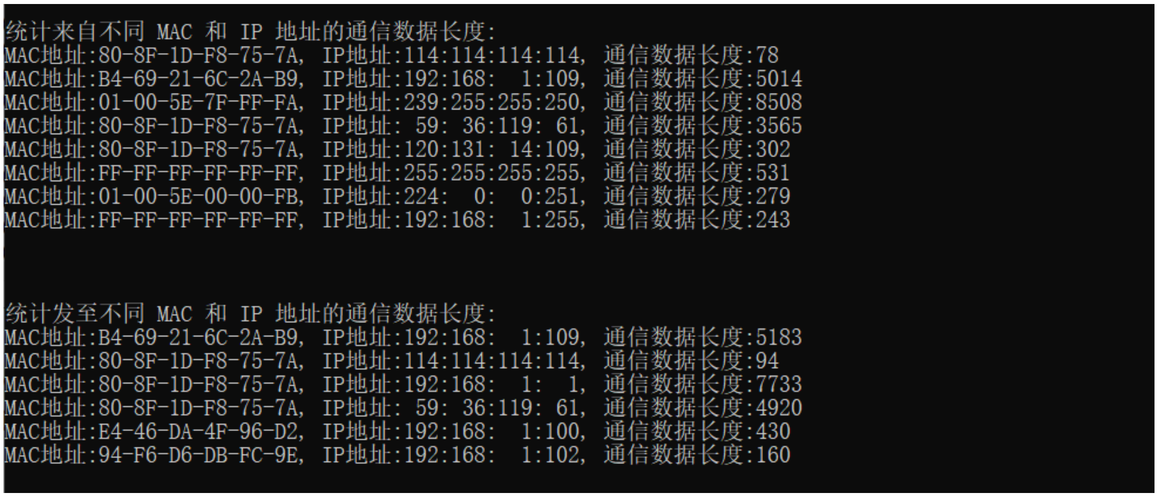
（2）流量预警（1kb)



D:\A_cos\Acomputer netword\WpdPack\Examples-pcap\\Debug\x86\UDPdump.exe

```
2020/03/24 21:47:04,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,129
2020/03/24 21:47:04,90-E6-BA-D6-BA-AE,192:168:  1:108,FF-FF-FF-FF-FF-FF,192:168:  1:255,92
2020/03/24 21:47:05,90-E6-BA-D6-BA-AE,192:168:  1:108,FF-FF-FF-FF-FF-FF,192:168:  1:255,92
2020/03/24 21:47:06,5C-09-47-C5-AA-A9,192:168:  1:103,01-00-5E-00-00-FB,224:  0:  0:251,154
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,318
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,390
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,366
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,327
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,386
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,382
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,398
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:06,80-8F-1D-F8-75-7A,192:168:  1:  1,01-00-5E-7F-FF-FA,239:255:255:250,380
80-8F-1D-F8-75-7A,192:168:  1:  1的流量超出阈值!
2020/03/24 21:47:07,5C-09-47-C5-AA-A9,192:168:  1:103,01-00-5E-00-00-FB,224:  0:  0:251,154
2020/03/24 21:47:07,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:47:07,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:47:07,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:47:08,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:47:08,B4-69-21-6C-2A-B9,192:168:  1:109,80-8F-1D-F8-75-7A, 59: 36:119: 61,129
2020/03/24 21:47:08,80-8F-1D-F8-75-7A, 59: 36:119: 61,B4-69-21-6C-2A-B9,192:168:  1:109,121
2020/03/24 21:47:09,B4-69-21-6C-2A-B9,192:168:  1:109,01-00-5E-7F-FF-FA,239:255:255:250,219
2020/03/24 21:47:10,5C-09-47-C5-AA-A9,192:168:  1:103,01-00-5E-00-00-FB,224:  0:  0:251,154
```

（3）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。



```
统计来自不同 MAC 和 IP 地址的通信数据长度:
MAC地址:80-8F-1D-F8-75-7A, IP地址:114:114:114:114, 通信数据长度:78
MAC地址:B4-69-21-6C-2A-B9, IP地址:192:168:  1:109, 通信数据长度:5014
MAC地址:01-00-5E-7F-FF-FA, IP地址:239:255:255:250, 通信数据长度:8508
MAC地址:80-8F-1D-F8-75-7A, IP地址: 59: 36:119: 61, 通信数据长度:3565
MAC地址:80-8F-1D-F8-75-7A, IP地址:120:131: 14:109, 通信数据长度:302
MAC地址:FF-FF-FF-FF-FF-FF, IP地址:255:255:255:255, 通信数据长度:531
MAC地址:01-00-5E-00-00-FB, IP地址:224:  0:  0:251, 通信数据长度:279
MAC地址:FF-FF-FF-FF-FF-FF, IP地址:192:168:  1:255, 通信数据长度:243


统计发至不同 MAC 和 IP 地址的通信数据长度:
MAC地址:B4-69-21-6C-2A-B9, IP地址:192:168:  1:109, 通信数据长度:5183
MAC地址:80-8F-1D-F8-75-7A, IP地址:114:114:114:114, 通信数据长度:94
MAC地址:80-8F-1D-F8-75-7A, IP地址:192:168:  1:  1, 通信数据长度:7733
MAC地址:80-8F-1D-F8-75-7A, IP地址: 59: 36:119: 61, 通信数据长度:4920
MAC地址:E4-46-DA-4F-96-D2, IP地址:192:168:  1:100, 通信数据长度:430
MAC地址:94-F6-D6-DB-FC-9E, IP地址:192:168:  1:102, 通信数据长度:160
```

4 实验总结

通过这次实验，学会使用 Wireshark 监听网络上的数据流，弄清数据包的属性和 MAC 地址、IP 地址的所在位置。统计流量做出流量预警，统计通信长度，也学会调用 time 来获取当前时间来实现实验。