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 陈芸衣

学　　号 24320182203182

实验时间 2020 年 3 月 11 日

2020 年 3 月 2 4 日

1 实验目的

用 WinPCAP 捕获并分析以太网的帧，获取目标与源网卡的 MAC 地址

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（如：1MB/s）的流量进行告警。

2 实验环境

操作系统:Windows 10

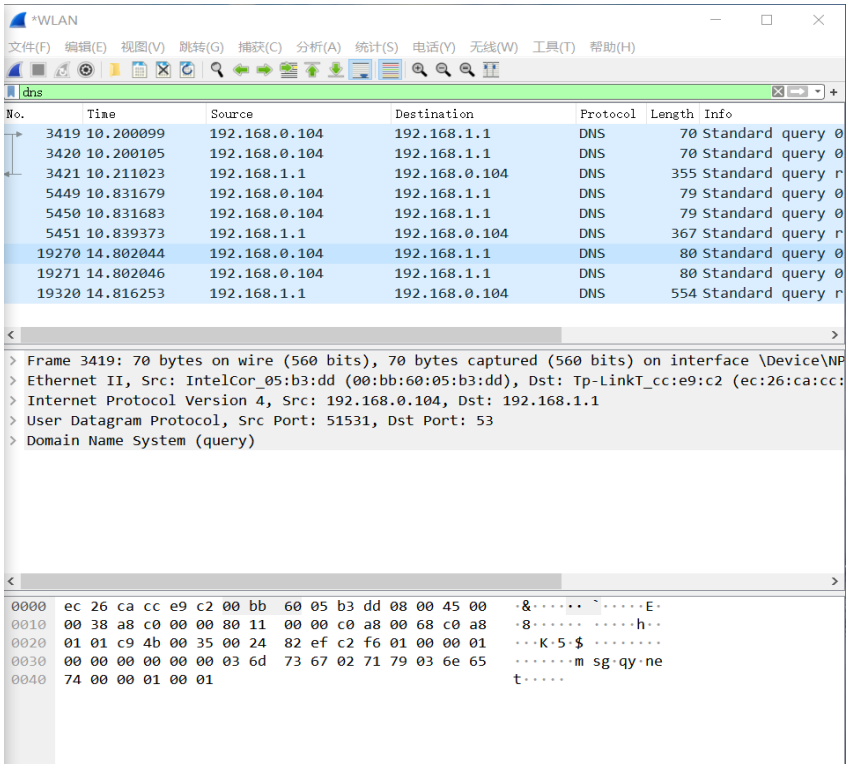
编程语言:C 语言

3 实验结果

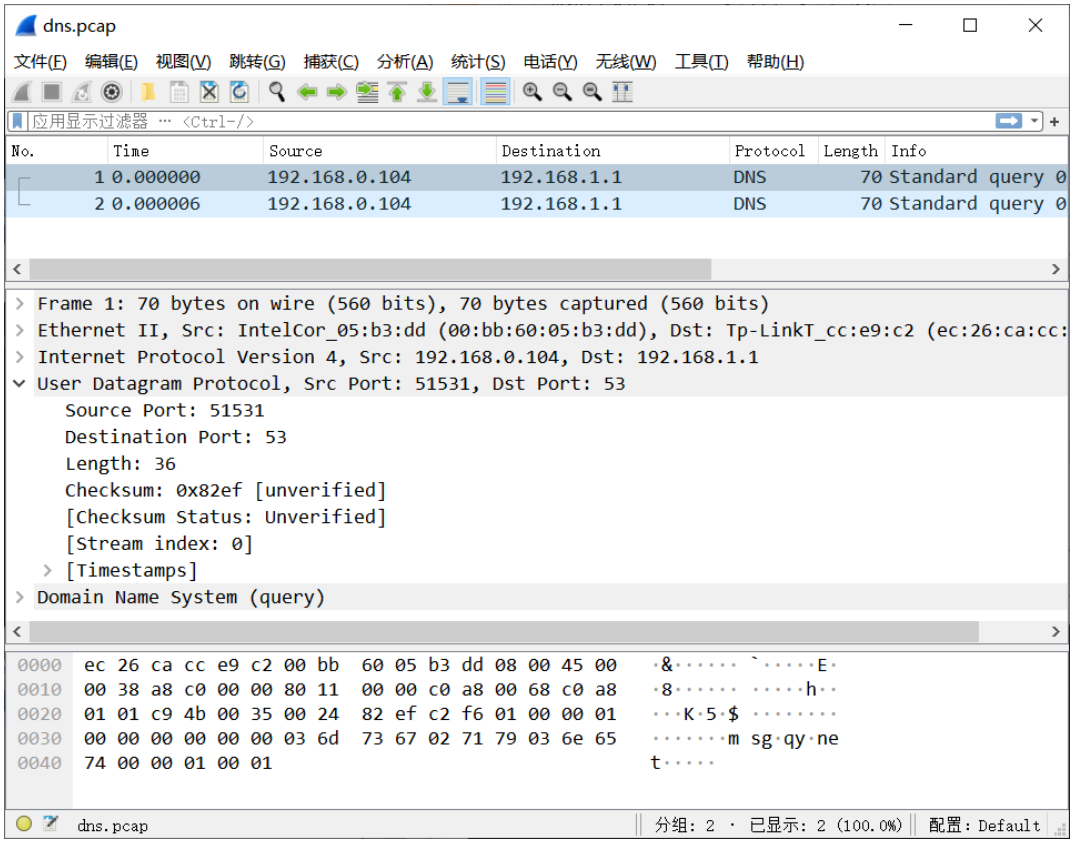
（1）在 VS 直接运行：

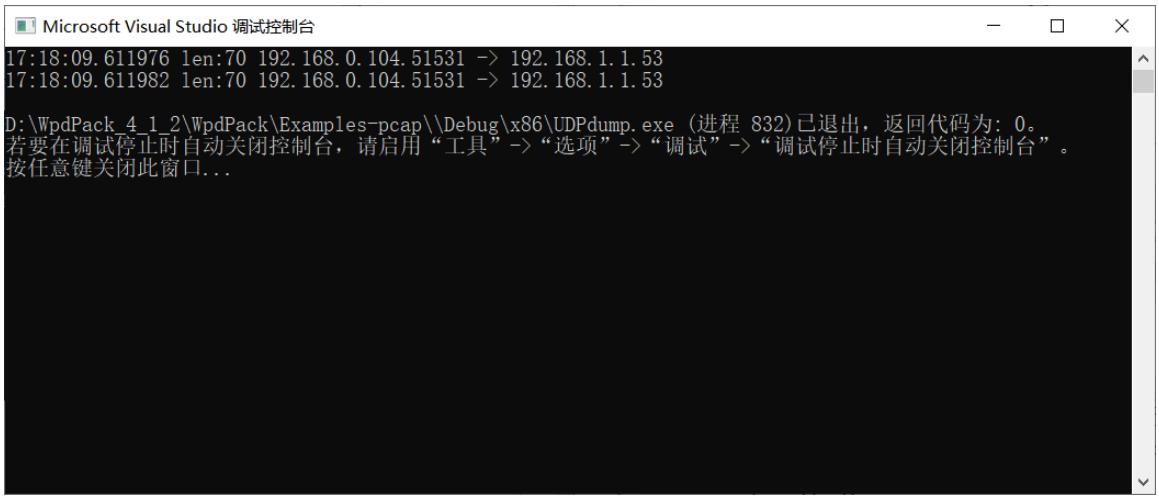
```
D:\WpdPack_4_1_2\WpdPack\Examples-pcap\Debug\x86\UDPdump.exe
1. \Device\NPF_{C5EA5351-C457-413B-8CBD-4E4CEDA12E8A} (Realtek PCIe GbE Family Controller)
2. \Device\NPF_{0995DBB0-1692-4A96-BB35-3D9ACF980096} (Microsoft)
3. \Device\NPF_{5755F411-6C18-459B-BB62-B2D1455F8435} (Microsoft)
Enter the interface number (1-3):3

listening on Microsoft...
16:50:22.517355 len:192 192.168.0.104.44316 -> 14.106.55.168.42364
16:50:22.517476 len:72 192.168.0.104.44316 -> 36.110.224.225.17788
16:50:22.517522 len:72 192.168.0.104.44316 -> 36.110.224.233.17788
16:50:22.517555 len:72 192.168.0.104.44316 -> 36.110.224.235.17788
16:50:22.517599 len:72 192.168.0.104.44316 -> 122.190.66.38.17788
16:50:23.519755 len:189 192.168.0.104.44316 -> 14.106.55.168.42364
16:50:23.519900 len:72 192.168.0.104.44316 -> 58.240.173.2.17788
16:50:23.519932 len:72 192.168.0.104.44316 -> 58.240.173.25.17788
16:50:23.519958 len:72 192.168.0.104.44316 -> 116.211.199.140.17788
16:50:23.519999 len:72 192.168.0.104.44316 -> 116.211.199.200.17788
16:50:23.520027 len:72 192.168.0.104.44316 -> 122.190.66.22.17788
16:50:23.520051 len:72 192.168.0.104.44316 -> 122.190.66.24.17788
16:50:23.520076 len:72 192.168.0.104.44316 -> 122.190.66.33.17788
16:50:24.515463 len:189 192.168.0.104.44316 -> 14.106.55.168.42364
16:50:24.515542 len:72 192.168.0.104.44316 -> 113.207.90.15.17788
16:50:24.515571 len:72 192.168.0.104.44316 -> 113.207.90.17.17788
16:50:24.515596 len:72 192.168.0.104.44316 -> 113.207.90.24.17788
16:50:24.515625 len:72 192.168.0.104.44316 -> 113.207.90.27.17788
16:50:24.515655 len:72 192.168.0.104.44316 -> 113.207.90.34.17788
16:50:24.515680 len:72 192.168.0.104.44316 -> 113.207.90.40.17788
16:50:24.515710 len:72 192.168.0.104.44316 -> 113.207.90.42.17788
16:50:25.520359 len:189 192.168.0.104.44316 -> 14.106.55.168.42364
16:50:25.520439 len:72 192.168.0.104.44316 -> 58.240.173.29.17788
16:50:25.520473 len:72 192.168.0.104.44316 -> 58.240.173.30.17788
16:50:25.520499 len:72 192.168.0.104.44316 -> 58.240.173.31.17788
16:50:25.520521 len:72 192.168.0.104.44316 -> 58.240.173.32.17788
```

（2）使用 Wireshark 调试：



dns.pcap:


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 192.168.0.104 192.168.1.1 DNS 70 Standard query 0
2 0.000006 192.168.0.104 192.168.1.1 DNS 70 Standard query 0
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: IntelCor_05:b3:dd (00:bb:60:05:b3:dd), Dst: Tp-LinkT_cc:e9:c2 (ec:26:ca:cc:
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 51531, Dst Port: 53
Source Port: 51531
Destination Port: 53
Length: 36
Checksum: 0x82ef [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Domain Name System (query)
0000 ec 26 ca cc e9 c2 00 bb 60 05 b3 dd 08 00 45 00
0010 00 38 a8 c0 00 00 80 11 00 00 c0 a8 00 68 c0 a8
0020 01 01 c9 4b 00 35 00 24 82 ef c2 f6 01 00 00 01
0030 00 00 00 00 00 00 03 6d 73 67 02 71 79 03 6e 65
0040 74 00 00 01 00 01
dns.pcap
分组: 2 · 已显示: 2 (100.0%)
配置: Default


Microsoft Visual Studio 调试控制台
17:18:09.611976 len:70 192.168.0.104.51531 -> 192.168.1.1.53
17:18:09.611982 len:70 192.168.0.104.51531 -> 192.168.1.1.53
D:\WpdPack_4_1_2\WpdPack\Examples-pcap\\Debug\x86\UDPdump.exe (进程 832)已退出，返回代码为: 0。
若要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口...

（2）程序运行结果：

```
listening on Microsoft...
EC 26 CA CC E9 C2 00 BB 60 05 B3 DD 08 00 45 00
00 3A C8 5A 00 00 80 11 00 00 C0 A8 00 68 3A F0
AD 13 AD 1C 45 7C
mac_header:
        dest_addr: EC 26 CA CC E9 C2
        src_addr: 00
        type: 0800
BB
        type: 0000
60
        type: 4500
05
        type: 0000
B3
        type: 0000
DD
        type: 3A00
ip_header
        ver_ihl   : 45
        tos       : 00
        tlen      : 003A
        identification: C85A
        flags_fo  : 0000
        ttl       : 80
        proto     : 11
        crc       : 0000
        op_pad    : 0000AD1C
        saddr:    : C0 A8 00 68  192.168.0.104.
        daddr     : 3A F0 AD 13  58.240.173.19.
```

开始监听：

```
1. \Device\NPF_{C5EA5351-C457-413B-8CBD-4E4CEDA12E8A} (Realtek PCIe GbE Family Controller)
2. \Device\NPF_{0995DBB0-1692-4A96-BB35-3D9ACF980096} (Microsoft)
3. \Device\NPF_{5755F411-6C18-459B-BB62-B2D1455F8435} (Microsoft)
请输入设备序号(1-3):3
开始监听:Microsoft
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2,113:207: 90: 34,132
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2,113:207: 90: 27,137
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2,113:207: 90: 24,143
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:230,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:244,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:245,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 49:  7: 31: 76,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 58:240:173: 31,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2,124: 64:199: 25,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2,124: 64:199: 29,72
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:250,147
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:242,133
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 49:  7: 31: 98,132
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:223,132
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 49:  7: 31: 98,132
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:232,72
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:233,72
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 36:110:224:239,72
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 49:  7: 31: 82,72
```

流量超出阈值：

```
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 23,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 24,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 27,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 28,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 29,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 31,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 32,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 33,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 34,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
2020/03/24 22:01:56,00-BB-60-05-B3-DD,192:168:  0:104,EC-26-CA-CC-E9-C2, 39:156: 40: 37,72
00-BB-60-05-B3-DD,192:168:  0:104的流量超出阈值!
```

统计来自不同 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:EC-26-CA-CC-E9-C2, IP地址:113:207: 90: 34, 通信数据长度:278
MAC地址:EC-26-CA-CC-E9-C2, IP地址:113:207: 90: 27, 通信数据长度:137
MAC地址:EC-26-CA-CC-E9-C2, IP地址:113:207: 90: 24, 通信数据长度:143
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:230, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:244, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:245, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 49:  7: 31: 76, 通信数据长度:204
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 58:240:173: 31, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址:124: 64:199: 25, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址:124: 64:199: 29, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:250, 通信数据长度:147
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:242, 通信数据长度:133
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 49:  7: 31: 98, 通信数据长度:264
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:223, 通信数据长度:132
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:232, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:233, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:239, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 49:  7: 31: 82, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 58:240:173: 26, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 58:240:173: 30, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址:122:190: 66: 26, 通信数据长度:72
MAC地址:00-BB-60-05-B3-DD, IP地址:192:168:  0:104, 通信数据长度:6132
MAC地址:EC-26-CA-CC-E9-C2, IP地址:123:151: 77:217, 通信数据长度:1099
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 36:110:224:235, 通信数据长度:132
MAC地址:EC-26-CA-CC-E9-C2, IP地址: 58:240:173:  8, 通信数据长度:72
MAC地址:EC-26-CA-CC-E9-C2, IP地址:122:190: 66: 21, 通信数据长度:72
```

统计发自不同 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:
MAC地址:00-BB-60-05-B3-DD, IP地址:192:168:  0:104, 通信数据长度:23722
MAC地址:EC-26-CA-CC-E9-C2, IP地址:123:151: 77:217, 通信数据长度:4591
MAC地址:EC-26-CA-CC-E9-C2, IP地址:192:168:  1:  1, 通信数据长度:1541
```

Csv.txt 内容：

csv.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2,113:207: 90: 34,132
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2,113:207: 90: 27,137
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2,113:207: 90: 24,143
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 36:110:224:230,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 36:110:224:244,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 36:110:224:245,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 49:  7: 31: 76,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 58:240:173: 31,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2,124: 64:199: 25,72
2020/03/24 22:01:53,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2,124: 64:199: 29,72
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 36:110:224:250,147
2020/03/24 22:01:54,00-BB-60-05-B3-DD,192:168:
0:104,EC-26-CA-CC-E9-C2, 36:110:224:242,133
```

第 1 行，第 1 列 100% Windows (CRLF) UTF-8

4 实验总结

通过本次实验，学会了用 WinPCAP 库监听并分析以太网的帧，记录目标与源 MAC 和 IP 地址。用基于 WinPCAP 的工具包，制作程序，统计网络上的数据流、流量等，此外，用 wireshark 测试监听程序。对计算机的 MAC 和 IP 地址有了更直观的理解。