计算机网络实验报告

实验： 实验 2

专业： 计算机科学与技术

班级： 1 班

姓名： 姚怀聿

学号： 22920202204632

2022 年 10 月 15 日

目　　录

一、　实验目的 3

二、　实验内容 3

任务 1: 捕获和分析有线以太网数据包 3

1.1 分析 MAC 帧 3

1.2 分析 IP 数据报首部 5

1.3 观察 IP 分片 9

1.4 ICMP 协议分析（以 ping 指令为例）..... 13

1.5 tracert 工作原理分析 17

1.6 ARP 协议分析 20

任务 2: 捕获和分析 802.11 数据 31

2.1 搭建实验环境 31

2.2 构建无线环境，捕获无线数据包、分析 802.11 数据..... 32

任务 3: 探索 Wireshark 更多功能和其它抓包工具(选做) 35

探索 Wireshark 更多功能 35

三、　实验小结 41

一、 实验目的

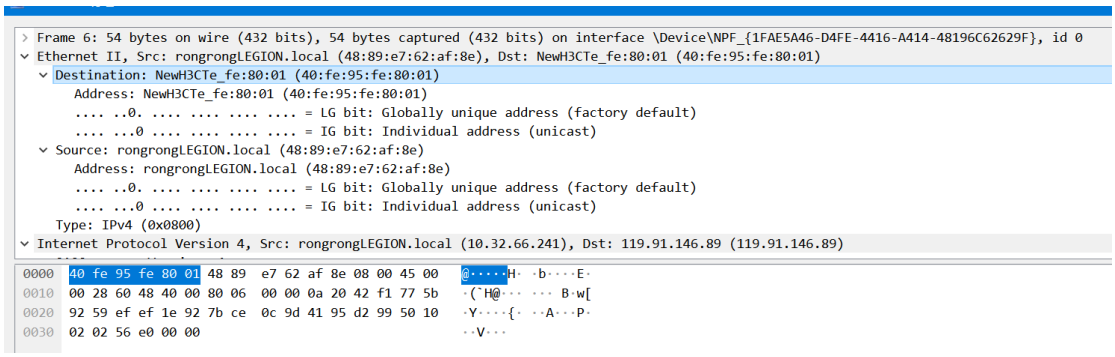
- 学习捕获和分析网络数据包
- 掌握以太网 MAC 帧、802.11 数据帧和 IPv4 数据包的构成，了解各字段的含义
- 掌握 ICMP 协议，ping 和 tracert 指令的工作原理
- 掌握 ARP 协议的请求/响应机理

二、 实验内容

任务 1：捕获和分析有线以太网数据包

准备步骤:学习 WireShark 基本操作

1.1 分析 MAC 帧



开头六个字节是以太网 MAC 帧的目的地址，以该 MAC 帧为例，其目的地址为 NewH3CTe_fe :80:01(40:fe:95:fe:80:01)。

```
> Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{1FAE5A46-D4FE-4416-A414-48196C62629F}, id 0
v Ethernet II, Src: rongrongLEGION.local (48:89:e7:62:af:8e), Dst: NewH3CTe_fe:80:01 (40:fe:95:fe:80:01)
  v Destination: NewH3CTe_fe:80:01 (40:fe:95:fe:80:01)
      Address: NewH3CTe_fe:80:01 (40:fe:95:fe:80:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: rongrongLEGION.local (48:89:e7:62:af:8e)
      Address: rongrongLEGION.local (48:89:e7:62:af:8e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: rongrongLEGION.local (10.32.66.241), Dst: 119.91.146.89 (119.91.146.89)

0000  40 fe 95 fe 80 01 48 89  e7 62 af 8e 08 00 45 00   @·····H· ·b····E·
0010  00 28 60 48 40 00 80 06  00 00 0a 20 42 f1 77 5b   ·(`H@··· ··· B·w[
0020  92 59 ef ef 1e 92 7b ce  0c 9d 41 95 d2 99 50 10   ·Y····{· ··A···P·
0030  02 02 56 e0 00 00                                  ··V···
```

接下来六个字节是以太网 MAC 帧的源地址，以该 MAC 帧为例，其源地址为 rongrongLEGION.local(48:89:e7:62:af:8e)，也即该电脑的本地地址。

```
> Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{1FAE5A46-D4FE-4416-A414-48196C62629F}, id 0
v Ethernet II, Src: rongrongLEGION.local (48:89:e7:62:af:8e), Dst: NewH3CTe_fe:80:01 (40:fe:95:fe:80:01)
  v Destination: NewH3CTe_fe:80:01 (40:fe:95:fe:80:01)
      Address: NewH3CTe_fe:80:01 (40:fe:95:fe:80:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: rongrongLEGION.local (48:89:e7:62:af:8e)
      Address: rongrongLEGION.local (48:89:e7:62:af:8e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: rongrongLEGION.local (10.32.66.241), Dst: 119.91.146.89 (119.91.146.89)

0000  40 fe 95 fe 80 01 48 89  e7 62 af 8e 08 00 45 00   @·····H· ·b····E·
0010  00 28 60 48 40 00 80 06  00 00 0a 20 42 f1 77 5b   ·(`H@··· ··· B·w[
0020  92 59 ef ef 1e 92 7b ce  0c 9d 41 95 d2 99 50 10   ·Y····{· ··A···P·
0030  02 02 56 e0 00 00                                  ··V···
```

再接下来的两个字节标志了上一层使用的协议类型，如该类型字段的值为 0x0800，表示上层使用的是 IP 数据报。

剩余的所有字节均是 IP 数据报。

值得一提的是，Wireshark 展现给我们的帧中并没有帧检验序列 FCS，这是因为

(a) Wireshark 抓到的帧，是 FCS 校验通过的帧，而帧尾的 FCS 会被硬件去掉，所以没有 FCS；

(b) Wireshark 不会抓取到 FCS 校验失败的帧。

1.2 分析 IP 数据报首部

```
> Frame 73: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{1FAE5A46-D4FE-4416-A414-48196C62629F}, id 0
> Ethernet II, Src: IntelCor_62:af:8e (48:89:e7:62:af:8e), Dst: BeijingX_91:ac:e2 (3c:cd:57:91:ac:e2)
> Internet Protocol Version 4, Src: 192.168.31.229 (192.168.31.229), Dst: 192.168.10.2 (192.168.10.2)
> User Datagram Protocol, Src Port: 50771 (50771), Dst Port: domain (53)
> Domain Name System (query)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ********
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ··S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   *******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

```
v Internet Protocol Version 4, Src: 192.168.31.229 (192.168.31.229), Dst: 192.168.10.2 (192.168.10.2)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 72
    Identification: 0xf03b (61499)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ********
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   *******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

IP 数据报的首部是 4bit 的版本号，以该 IP 数据报为例，其版本号为 4。

```
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 72
    Identification: 0xf03b (61499)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ********
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   *******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

接下来 4bit 是首部长度，以该 IP 数据报为例，其首部长度是 20 字节。

然后是 1 字节的服务类型，以该 IP 数据报为例，其服务类型为 0。

```
> Frame 73: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{1FAE5A46-D4FE-4416-A414-48196C62629F}, id 0
> Ethernet II, Src: rongrongLEGION.local (48:89:e7:62:af:8e), Dst: szshort.weixin.qq.com (3c:cd:57:91:ac:e2)
v Internet Protocol Version 4, Src: rongrongLEGION.local (192.168.31.229), Dst: 192.168.10.2 (192.168.10.2)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 72
    Identification: 0xf03b (61499)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ********
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   *******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

然后是 2 字节长的总长度，以该 IP 数据报为例，其总长度为 72 字节，除去首部固定部分长度 20 字节，表明可变部分长度有 52 字节。

```
v User Datagram Protocol, Src Port: 50771 (50771), Dst Port: domain (53)
    Source Port: 50771 (50771)
    Destination Port: domain (53)
    Length: 52
    Checksum: 0xab7d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (44 bytes)
> Domain Name System (query)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ********
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   *******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

上图显示了可变部分长度为 52 字节。

```
> Frame 73: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{1FAE5A46-D4FE-4416-A414-48196C62629F}, id 0
> Ethernet II, Src: rongrongLEGION.local (48:89:e7:62:af:8e), Dst: szshort.weixin.qq.com (3c:cd:57:91:ac:e2)
v Internet Protocol Version 4, Src: rongrongLEGION.local (192.168.31.229), Dst: 192.168.10.2 (192.168.10.2)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 72
    Identification: 0xf03b (61499)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ********
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   *******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

接下来 2 个字节是标识，以该 IP 数据报为例，其标识为 0xf03b。

```
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: rongrongLEGION.local (192.168.31.229)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ........
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   ·******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

之后 3bit 是标志位，以该 IP 数据报为例，其标志位为 000。

```
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: rongrongLEGION.local (192.168.31.229)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ........
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   ·******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

接下来 13bit 为片偏移，以该 IP 数据报为例，其片偏移为 0。

```
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: rongrongLEGION.local (192.168.31.229)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;···· ........
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   ·******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

接下来 1 字节为生存时间(TTL)，以该 IP 数据报为例，其生存时间

(TTL)为 128s。

```
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: rongrongLEGION.local (192.168.31.229)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;····· ........
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   ·******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

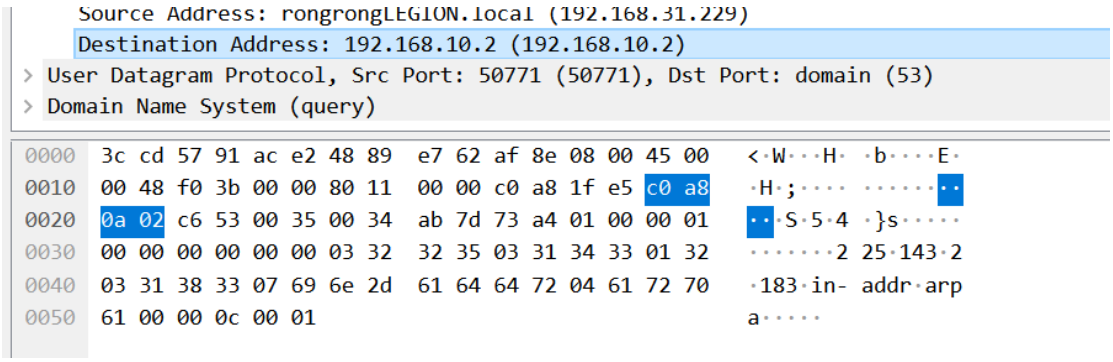
接下来 1 字节为协议，以该 IP 数据报为例，其协议为 UDP。

```
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: rongrongLEGION.local (192.168.31.229)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;····· ........
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   ·******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

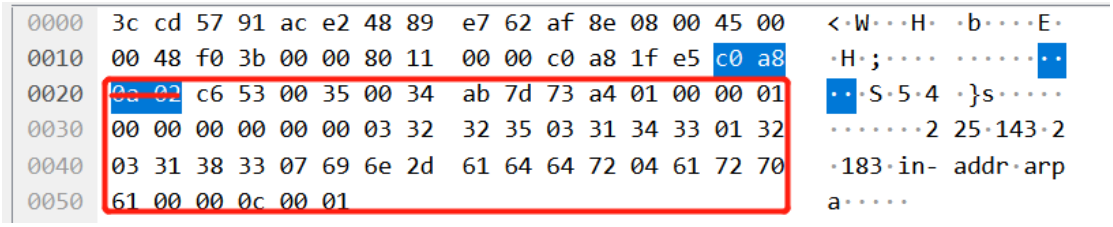
之后的 2 字节为首部检验和，以该 IP 数据报为例，其首部检验和为 0，保留这个数据报。

```
[Header checksum status: Unverified]
Source Address: rongrongLEGION.local (192.168.31.229)
Destination Address: 192.168.10.2 (192.168.10.2)
> User Datagram Protocol, Src Port: 50771 (50771), Dst Port: domain (53)
> Domain Name System (query)

0000  3c cd 57 91 ac e2 48 89  e7 62 af 8e 08 00 45 00   <·W···H· ·b····E·
0010  00 48 f0 3b 00 00 80 11  00 00 c0 a8 1f e5 c0 a8   ·H·;····· ........
0020  0a 02 c6 53 00 35 00 34  ab 7d 73 a4 01 00 00 01   ···S·5·4 ·}s·····
0030  00 00 00 00 00 00 03 32  32 35 03 31 34 33 01 32   ·******2 25·143·2
0040  03 31 38 33 07 69 6e 2d  61 64 64 72 04 61 72 70   ·183·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

接下来 4 字节为源 IP 地址，以该 IP 数据报为例，其源 IP 地址为 192.168.31.229。



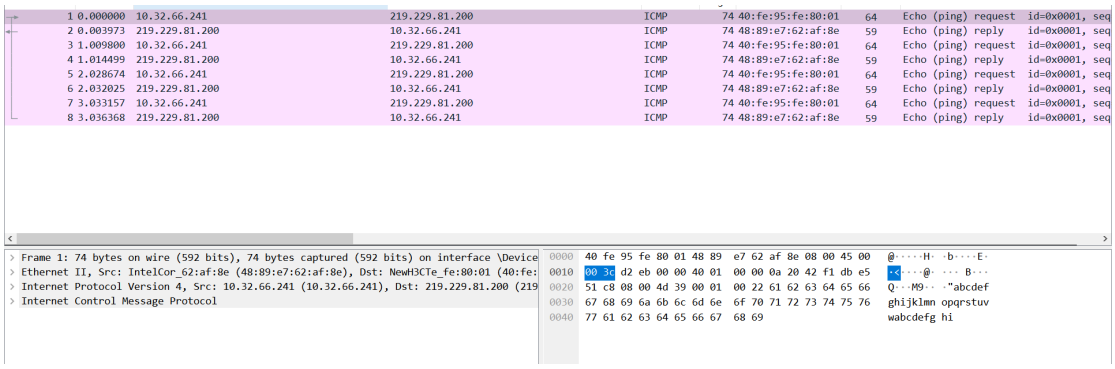
首部固定部分的最后 4 个字节为目的 IP 地址，以该 IP 数据报为例，其目的 IP 地址为 192.168.10.2。



剩余字节均为可变部分。

1.3 观察 IP 分片

a) ping -4 www.xmu.edu.cn



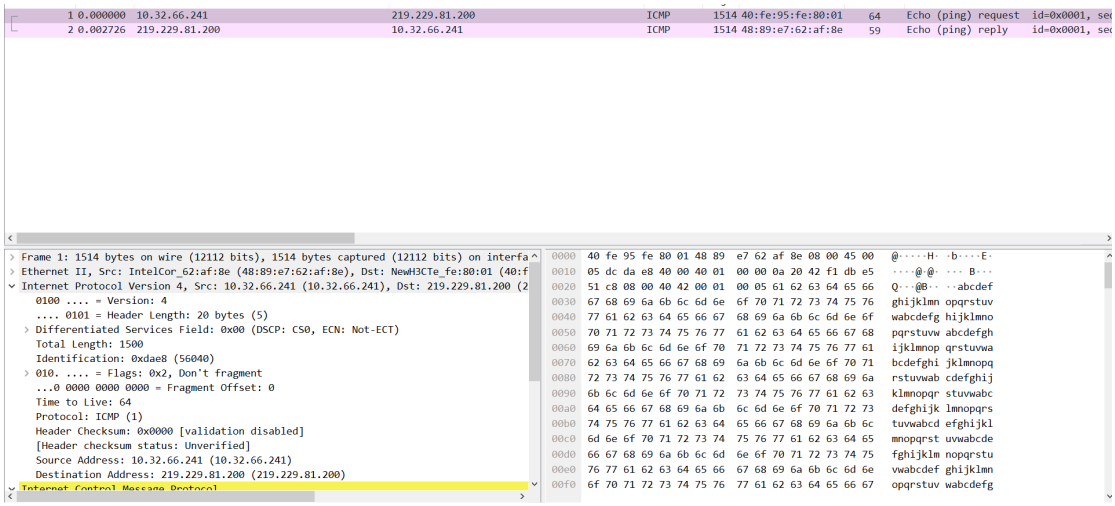
```
C:\Users\rongrong>ping -4 www.xmu.edu.cn

正在 Ping cmsn1.xmu.edu.cn [219.229.81.200] 具有 32 字节的数据:
来自 219.229.81.200 的回复: 字节=32 时间=4ms TTL=59
来自 219.229.81.200 的回复: 字节=32 时间=4ms TTL=59
来自 219.229.81.200 的回复: 字节=32 时间=3ms TTL=59
来自 219.229.81.200 的回复: 字节=32 时间=3ms TTL=59

219.229.81.200 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms，最长 = 4ms，平均 = 3ms
```

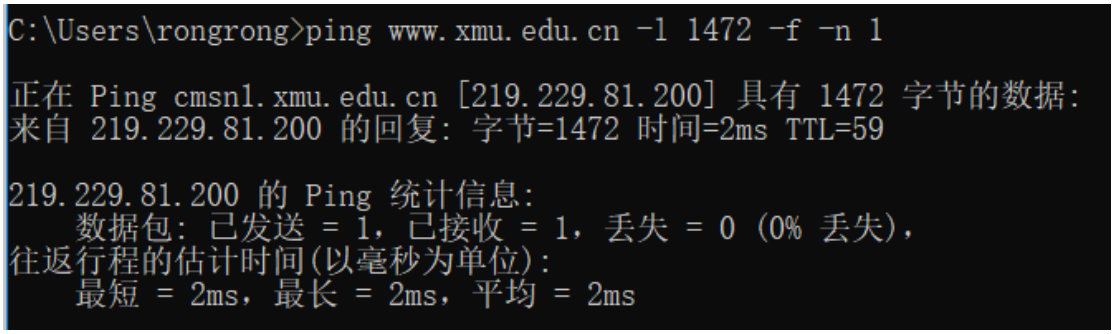
如上图所示，Wireshark 抓包数据显示发送了 4 个数据包、接受了 4 个数据包；终端窗口显示已发送的数据包个数为 4,、已接受的数据包个数为 4。

```
Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
    [Length: 32]

0000  48 89 e7 62 af 8e 40 fe  95 fe 80 01 08 00 45 60   H··b··@· ·····E`
0010  00 3c 6e cc 00 00 3b 01  95 d6 db e5 51 c8 0a 20   ·<n···;· ····Q··
0020  42 f1 00 00 55 5a 00 01  00 01 61 62 63 64 65 66   B···UZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

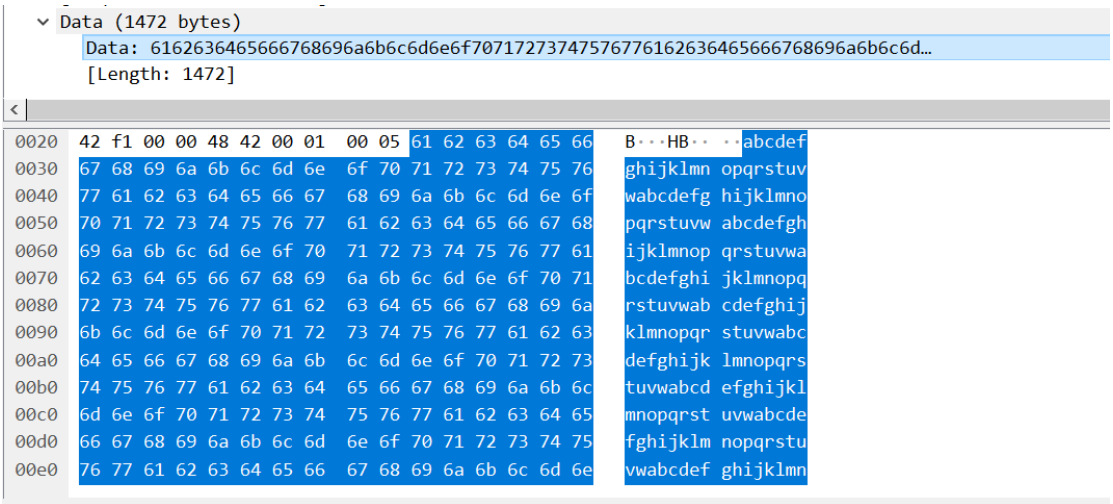
终端窗口显示接收到的字节数为 32，ICMP 报文数据部分长度为 32 字节。

b) ping www.xmu.edu.cn -l 1472 -f -n 1





如上图所示，Wireshark 抓包数据显示发送了 1 个数据包、接收了 1 个数据包；终端窗口显示已发送的数据包个数为 1、已接受的数据包个数为 1。



终端窗口显示接收到的字节数为 1472，ICMP 报文数据部分长度为

1472 字节。

c) ping www.xmu.edu.cn -l 1473 -f -n 1

```
C:\Users\rongrong>ping www.xmu.edu.cn -l 1473 -f -n 1

正在 Ping cmsn1.xmu.edu.cn [219.229.81.200] 具有 1473 字节的数据:
需要拆分数据包但是设置 DF。

219.229.81.200 的 Ping 统计信息:
    数据包: 已发送 = 1，已接收 = 0，丢失 = 1 (100% 丢失)，
```

终端显示“需要拆分数据包但是设置 DF”，指的是数据包大小超过了网络限定 MTU 大小，即不分片对超过 MTU 的长报文无法传输。

d) ping www.xmu.edu.cn -l 1473 -n 1

1	0.000000	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	2001:da8:e800:251c::200	IPv6	1510	40:fe:95:fe:80:01	IPv6 fragment (off=0 more=y ident=0
2	0.000000	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	2001:da8:e800:251c::200	ICMPv6	95	40:fe:95:fe:80:01	Echo (ping) request id=0x0001, seq=
3	0.002345	2001:da8:e800:251c::200	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	IPv6	1510	48:89:e7:62:af:8e	IPv6 fragment (off=0 more=y ident=0
4	0.003383	2001:da8:e800:251c::200	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	ICMPv6	95	48:89:e7:62:af:8e	Echo (ping) reply id=0x0001, seq=8,

```
C:\Users\rongrong>ping www.xmu.edu.cn -l 1473 -n 1

正在 Ping cmsn1.xmu.edu.cn [2001:da8:e800:251c::200] 具有 1473 字节的数据:
来自 2001:da8:e800:251c::200 的回复: 时间=4ms

2001:da8:e800:251c::200 的 Ping 统计信息:
    数据包: 已发送 = 1，已接收 = 1，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 4ms，最长 = 4ms，平均 = 4ms
```

终端输入“ping www.xmu.edu.cn -l 1473 -n 1”从 www.xmu.edu.cn 请求字节长度为 1473 字节的报文，并分片传输。Wireshark 抓包数据接收到两组报文，报文数据长度为 1473 字节。

```
[Response In: 4]
Data (1473 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 96a6b6c6d…
    [Length: 1473]

0000  80 00 75 ba 00 01 00 08  61 62 63 64 65 66 67 68   ··u····· abcdefgh
0010  69 6a 6b 6c 6d 6e 6f 70  71 72 73 74 75 76 77 61   ijklmnop qrstuvwa
0020  62 63 64 65 66 67 68 69  6a 6b 6c 6d 6e 6f 70 71   bcdefghi jklmnopq
0030  72 73 74 75 76 77 61 62  63 64 65 66 67 68 69 6a   rstuvwab cdefghij
0040  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63   klmnopqr stuvwabc
0050  64 65 66 67 68 69 6a 6b  6c 6d 6e 6f 70 71 72 73   defghijk lmnopqrs
0060  74 75 76 77 61 62 63 64  65 66 67 68 69 6a 6b 6c   tuvwabcd efghijkl
0070  6d 6e 6f 70 71 72 73 74  75 76 77 61 62 63 64 65   mnopqrst uvwabcde
0080  66 67 68 69 6a 6b 6c 6d  6e 6f 70 71 72 73 74 75   fghijklm nopqrstu
0090  76 77 61 62 63 64 65 66  67 68 69 6a 6b 6c 6d 6e   vwabcdef ghijklmn
00a0  6f 70 71 72 73 74 75 76  77 61 62 63 64 65 66 67   opqrstuv wabcdefg
00b0  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuvw
```

综上，对比以上四条命令：

(a) ping -4 www.xmu.edu.cn 表示从目的 IP 地址请求默认 32 字节的报文数据，共 4 次。

(b) ping www.xmu.edu.cn -l 1472 -f -n 1 表示从目的 IP 地址请求 1472 字节的报文数据，且设置为不分片，请求 1 次。

(c) ping www.xmu.edu.cn -l 1473 -f -n 1 表示从目的 IP 地址请求 1473 字节的报文数据，且设置为不分片，请求 1 次。

(d) ping www.xmu.edu.cn -l 1473 -n 1 表示从目的 IP 地址请求 1473 字节的报文数据，且设置为分片，请求 1 次。

1.4 ICMP 协议分析（以 ping 指令为例）

执行一次 ping 命令会得到一组 ICMP 请求帧和回应帧。

```
C:\Users\rongrong>ping www.xmu.edu.cn -l 1473 -n 1

正在 Ping cmsn1.xmu.edu.cn [2001:da8:e800:251c::200] 具有 1473 字节的数据:
来自 2001:da8:e800:251c::200 的回复: 时间=3ms

2001:da8:e800:251c::200 的 Ping 统计信息:
    数据包: 已发送 = 1，已接收 = 1，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms，最长 = 3ms，平均 = 3ms
```

No.	Time	Source	Destination	Protocol	Length	Destination	Time to Live	Info
1	0.000000	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	2001:da8:e800:251c::200	IPv6	1510	40:fe:95:fe:80:01		IPv6 fragment (off=0 more=y ident=0
2	0.000000	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	2001:da8:e800:251c::200	ICMPv6	95	40:fe:95:fe:80:01		Echo (ping) request id=0x0001, seq=
3	0.002300	2001:da8:e800:251c::200	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	IPv6	1510	48:89:e7:62:af:8e		IPv6 fragment (off=0 more=y ident=0
4	0.003005	2001:da8:e800:251c::200	240e:67c:1301:71e4:2cd2:1731:37a6:83a1	ICMPv6	95	48:89:e7:62:af:8e		Echo (ping) reply id=0x0001, seq=10

例如，执行上述 ping 命令，得到一组 ICMP 请求帧和回应帧。

```
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x75b8 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 10
    [Response In: 4]
  Data (1473 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 96a6b6c6d…
      [Length: 1473]

0000  80 00 75 b8 00 01 00 0a  61 62 63 64 65 66 67 68   ··u····· abcdefgh
0010  69 6a 6b 6c 6d 6e 6f 70  71 72 73 74 75 76 77 61   ijklmnop qrstuvwa
0020  62 63 64 65 66 67 68 69  6a 6b 6c 6d 6e 6f 70 71   bcdefghi jklmnopq
0030  72 73 74 75 76 77 61 62  63 64 65 66 67 68 69 6a   rstuvwab cdefghij
0040  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63   klmnopqr stuvwabc
0050  64 65 66 67 68 69 6a 6b  6c 6d 6e 6f 70 71 72 73   defghijk lmnopqrs
0060  74 75 76 77 61 62 63 64  65 66 67 68 69 6a 6b 6c   tuvwabcd efghijkl
0070  6d 6e 6f 70 71 72 73 74  75 76 77 61 62 63 64 65   mnopqrst uvwabcde
0080  66 67 68 69 6a 6b 6c 6d  6e 6f 70 71 72 73 74 75   fghijklm nopqrstu
0090  76 77 61 62 63 64 65 66  67 68 69 6a 6b 6c 6d 6e   vwabcdef ghijklmn
00a0  6f 70 71 72 73 74 75 76  77 61 62 63 64 65 66 67   opqrstuv wabcdefg
00b0  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuvw

Frame (95 bytes)    Reassembled IPv6 (1481 bytes)
```

请求帧

```
Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x74b8 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 10
    [Response To: 2]
    [Response Time: 3.005 ms]
  Data (1473 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 96a6b6c6d…
```

回应帧

```
0000  81 00 74 b8 00 01 00 0a  61 62 63 64 65 66 67 68   ··t····· abcdefgh
0010  69 6a 6b 6c 6d 6e 6f 70  71 72 73 74 75 76 77 61   ijklmnop qrstuvwa
0020  62 63 64 65 66 67 68 69  6a 6b 6c 6d 6e 6f 70 71   bcdefghi jklmnopq
0030  72 73 74 75 76 77 61 62  63 64 65 66 67 68 69 6a   rstuvwab cdefghij
0040  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63   klmnopqr stuvwabc
0050  64 65 66 67 68 69 6a 6b  6c 6d 6e 6f 70 71 72 73   defghijk lmnopqrs
0060  74 75 76 77 61 62 63 64  65 66 67 68 69 6a 6b 6c   tuvwabcd efghijkl
0070  6d 6e 6f 70 71 72 73 74  75 76 77 61 62 63 64 65   mnopqrst uvwabcde
0080  66 67 68 69 6a 6b 6c 6d  6e 6f 70 71 72 73 74 75   fghijklm nopqrstu
0090  76 77 61 62 63 64 65 66  67 68 69 6a 6b 6c 6d 6e   vwabcdef ghijklmn
00a0  6f 70 71 72 73 74 75 76  77 61 62 63 64 65 66 67   opqrstuv wabcdefg
00b0  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuvw
```

请求帧和回应帧的差别：

```
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x75b1 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 17
    [Response In: 4]
  Data (1473 bytes)
```

```
Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x74b1 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 17
    [Response To: 2]
    [Response Time: 15.585 ms]
  > Data (1473 bytes)
```

(1) 请求帧的 Type 为：Echo (ping) request (128)；回应帧的 Type 为：Echo (ping) reply (129)

(2) Checksum 检验和不同

(3) 请求帧[Response In: 4]表示回应帧在分组 4；回应帧[Response To: 2]表示请求帧在分组 2

(4) 回应帧有回应时间

(5) 对应 IP 头部的差别：

```
Internet Protocol Version 6, Src: 240e:67c:1301:71e4:2cd2:1731:37a6:83a1 (240e:67c:1301:71e4:2cd2:1731:37a6:83a1), Dst: 2001:da8:e800:251c::2
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 41
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 64
    Source Address: 240e:67c:1301:71e4:2cd2:1731:37a6:83a1 (240e:67c:1301:71e4:2cd2:1731:37a6:83a1)
    Destination Address: 2001:da8:e800:251c::200 (2001:da8:e800:251c::200)
  > Fragment Header for IPv6
  > [2 IPv6 Fragments (1481 bytes): #1(1448), #2(33)]
```

请求帧IP头部

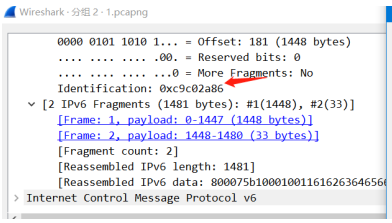
```
Internet Protocol Version 6, Src: 2001:da8:e800:251c::200 (2001:da8:e800:251c::200), Dst: 240e:67c:1301:71e4:2cd2:1731:37a6:83a1 (240e:67c:13
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 41
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 59
    Source Address: 2001:da8:e800:251c::200 (2001:da8:e800:251c::200)
    Destination Address: 240e:67c:1301:71e4:2cd2:1731:37a6:83a1 (240e:67c:1301:71e4:2cd2:1731:37a6:83a1)
  > Fragment Header for IPv6
  > [2 IPv6 Fragments (1481 bytes): #3(1448), #4(33)]
```

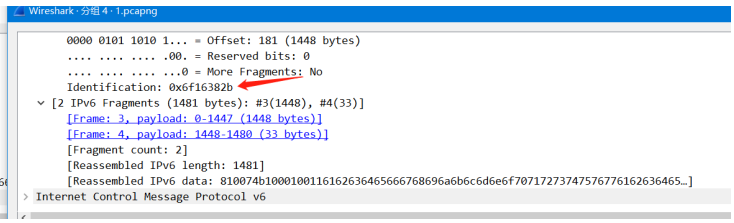
回应帧IP头部

(a) 二者的 Hop Limit 不同，请求帧 IP 头部的 Hop Limit 为 59；回应帧 IP 头部的 Hop Limit 为 64

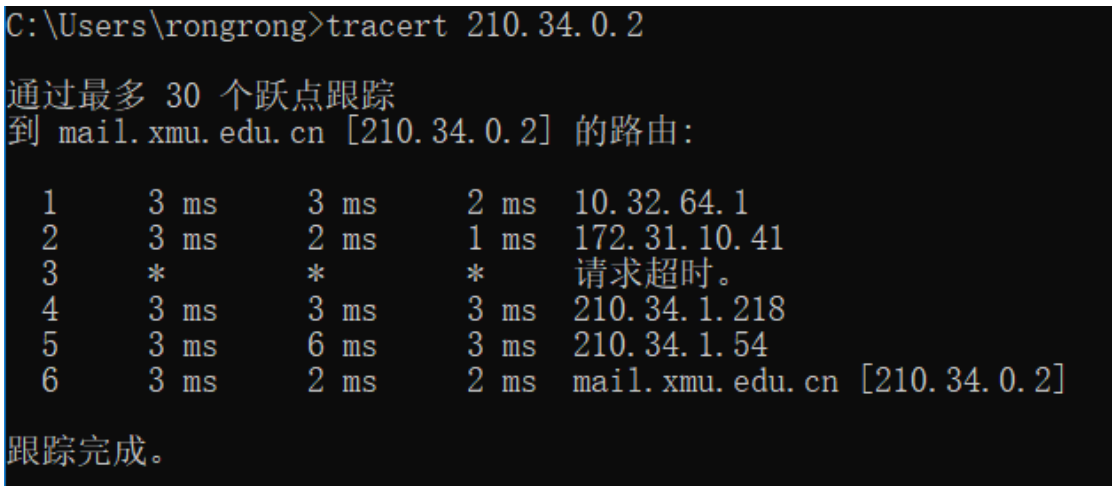
(b) 二者的源地址和目的地址对调

(c) 二者 Fragment Header for IPv6 中的 Identifacation 不同

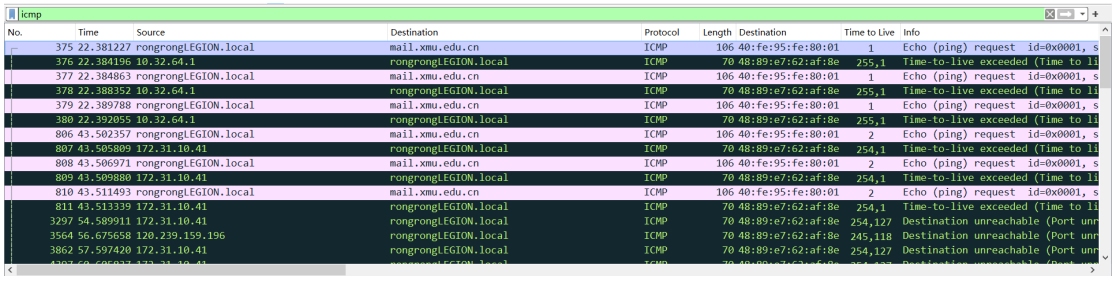




1.5 tracert 工作原理分析

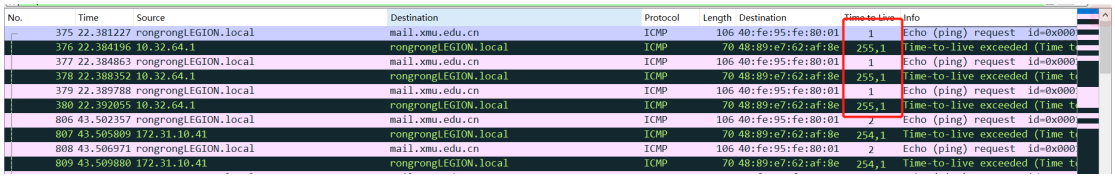


```
C:\Users\rongrong>tracert 210.34.0.2

通过最多 30 个跃点跟踪
到 mail.xmu.edu.cn [210.34.0.2] 的路由:

  1     3 ms     3 ms     2 ms  10.32.64.1
  2     3 ms     2 ms     1 ms  172.31.10.41
  3     *        *        *     请求超时。
  4     3 ms     3 ms     3 ms  210.34.1.218
  5     3 ms     6 ms     3 ms  210.34.1.54
  6     3 ms     2 ms     2 ms  mail.xmu.edu.cn [210.34.0.2]

跟踪完成。
```



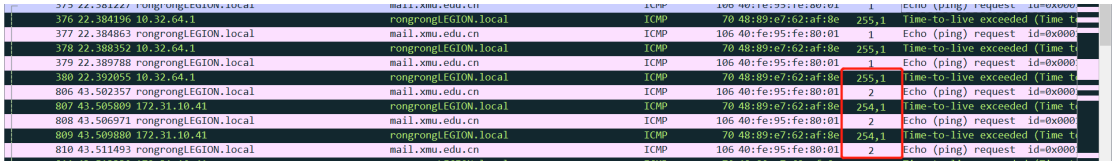
No.	Time	Source	Destination	Protocol	Length	Destination	Time to Live	Info
375	22.381227	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x0001, s
376	22.384196	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time to li
377	22.384863	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x0001, s
378	22.388352	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time to li
379	22.389788	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x0001, s
380	22.392055	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time to li
806	43.502357	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x0001, s
807	43.505809	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time to li
808	43.506971	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x0001, s
809	43.509880	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time to li
810	43.511493	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x0001, s
811	43.513339	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time to li
3297	54.589911	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,127	Destination unreachable (Port unr
3564	56.675658	120.239.159.196	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	245,118	Destination unreachable (Port unr
3862	57.597420	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,127	Destination unreachable (Port unr

Tracert 命令用 IP 生存时间（TTL）字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。



No.	Time	Source	Destination	Protocol	Length	Destination	Time to Live	Info
375	22.381227	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x000
376	22.384196	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time t
377	22.384863	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x000
378	22.388352	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time t
379	22.389788	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x000
380	22.392055	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time t
806	43.502357	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x000
807	43.505809	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time t
808	43.506971	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x000
809	43.509880	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time t

首先，tracert 发送出一个 TTL 是 1 的 IP 数据包到目的地，当路径上的第一个路由器收到这个数据包时，它将 TTL 减 1。此时，TTL 变为 0，所以该路由器会将此数据包丢掉，并送回一个[ICMP time exceeded]消息（包括发 IP 包的源地址，IP 包的所有内容及路由器的 IP 地址），如上图中的前 3 个 TTL 是 1 的 IP 数据包。



376	22.384196	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time t
377	22.384863	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x000
378	22.388352	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time t
379	22.389788	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	1	Echo (ping) request id=0x000
380	22.392055	10.32.64.1	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	255,1	Time-to-live exceeded (Time t
806	43.502357	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x000
807	43.505809	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time t
808	43.506971	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x000
809	43.509880	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time t
810	43.511493	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x000

tracert 收到这个消息后，便知道这个路由器存在于这个路径上，接着 tracert 再送出另一个 TTL 是 2 的数据包，发现第 2 个路由器，如上图中红色框出的 3 个 TTL 是 2 的 IP 数据包。

tracert 每次将送出的数据包的 TTL 加 1 来发现另一个路由器，这个重复的动作一直持续到某个数据包抵达目的地。当数据包到达目的地后，该主机则不会送回 ICMP time exceeded 消息，一旦到达目的地，由于 tracert 通过 UDP 数据包向不常见端口(30000 以上)发送数据包，因此会收到[ICMP port unreachable]消息，故可判断到达目的地。如下图所示：

810	43.511493	rongrongLEGION.local	mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	2	Echo (ping) request id=0x0001, se
811	43.513339	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,1	Time-to-live exceeded (Time to liv
3297	54.589911	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,127	Destination unreachable (Port unre
3564	56.675658	120.239.159.196	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	245,118	Destination unreachable (Port unre
3862	57.597420	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,127	Destination unreachable (Port unre
4397	60.605837	172.31.10.41	rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	254,127	Destination unreachable (Port unre

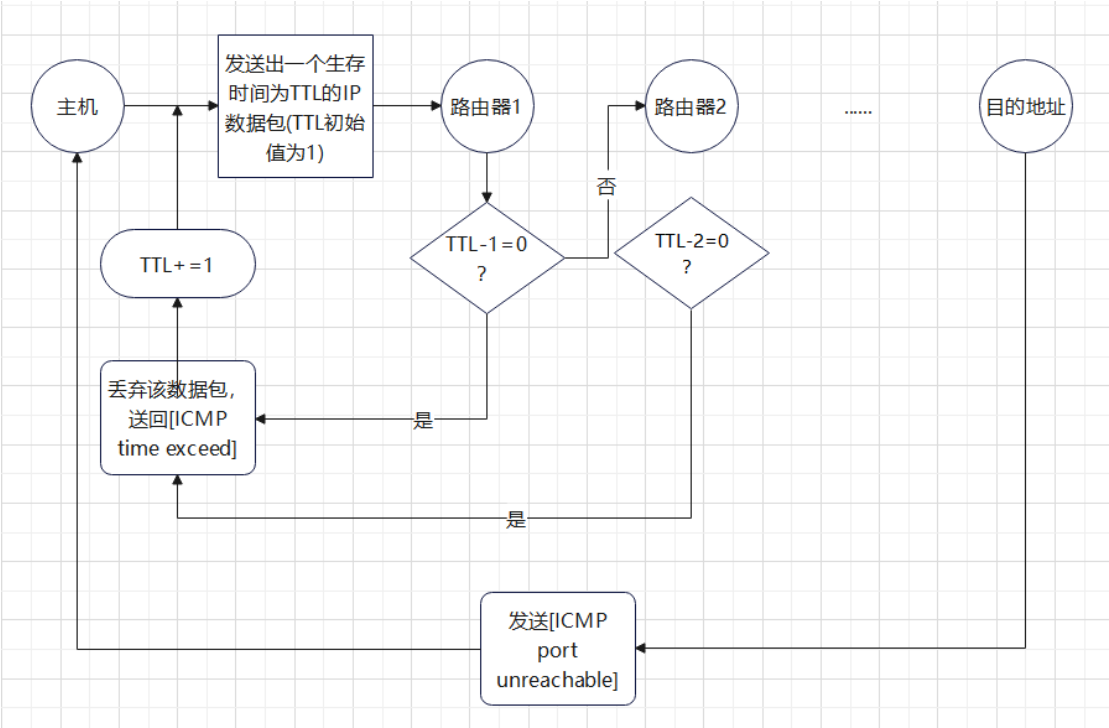
tracert 有一个固定的时间等待响应(ICMP TTL 到期消息)。如果这个

时间过了，它将打印出一系列的*号表明：在这个路径上，这个设备不能在给定的时间内发出 ICMP TTL 到期消息的响应。然后，Tracert 给 TTL 记数器加 1，继续进行。如下图所示：

```
C:\Users\rongrong>tracert 210.34.0.2

通过最多 30 个跃点跟踪
到 mail.xmu.edu.cn [210.34.0.2] 的路由:

  1     3 ms     3 ms     2 ms  10.32.64.1
  2     3 ms     2 ms     1 ms  172.31.10.41
  3     *        *        *     请求超时。
  4     3 ms     3 ms     3 ms  210.34.1.218
  5     3 ms     6 ms     3 ms  210.34.1.54
  6     3 ms     2 ms     2 ms  mail.xmu.edu.cn [210.34.0.2]

跟踪完成。
```

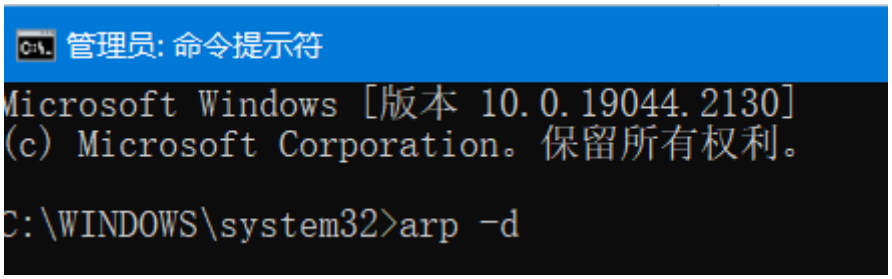
rongrongLEGION.local	ICMP	70	48:89:e7:62:af:8e	251,1	Time-to-live exceeded (Time to live exceeded in transit)
mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	6	Echo (ping) request id=0x0001, seq=51/13056, ttl=6 (reply in 8406)
rongrongLEGION.local	ICMP	106	48:89:e7:62:af:8e	59	Echo (ping) reply id=0x0001, seq=51/13056, ttl=59 (request in 8402)
mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	6	Echo (ping) request id=0x0001, seq=52/13312, ttl=6 (reply in 8408)
rongrongLEGION.local	ICMP	106	48:89:e7:62:af:8e	59	Echo (ping) reply id=0x0001, seq=52/13312, ttl=59 (request in 8407)
mail.xmu.edu.cn	ICMP	106	40:fe:95:fe:80:01	6	Echo (ping) request id=0x0001, seq=53/13568, ttl=6 (reply in 8410)
rongrongLEGION.local	ICMP	106	48:89:e7:62:af:8e	59	Echo (ping) reply id=0x0001, seq=53/13568, ttl=59 (request in 8409)

Tracert 工作原理示意图如下：

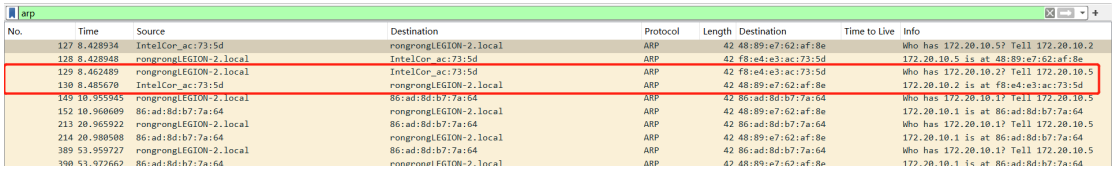


1.6 ARP 协议分析

(1)以管理员身份运行终端窗口，运行`arp -d`命令，清空本机已有的 ARP 缓存

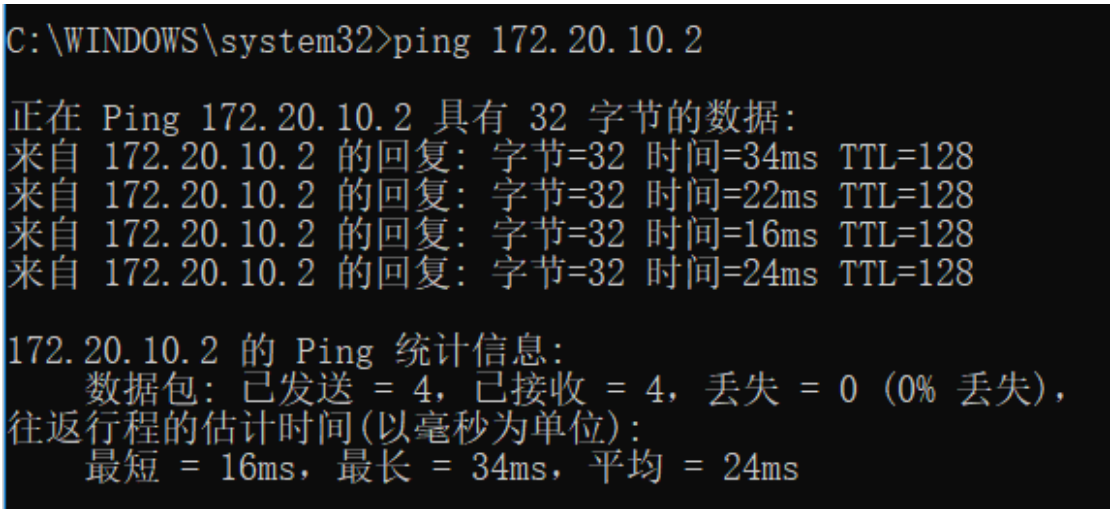


(2)抓包，ping 旁边同学的 ip



No.	Time	Source	Destination	Protocol	Length	Destination	Time to Live	Info
127	8.428934	IntelCor_ac:73:5d	rongrongLEGION-2.local	ARP	42	48:89:e7:62:af:8e		Who has 172.20.10.5? Tell 172.20.10.2
128	8.428948	rongrongLEGION-2.local	IntelCor_ac:73:5d	ARP	42	f8:e4:e3:ac:73:5d		172.20.10.5 is at 48:89:e7:62:af:8e
129	8.462489	rongrongLEGION-2.local	IntelCor_ac:73:5d	ARP	42	f8:e4:e3:ac:73:5d		Who has 172.20.10.2? Tell 172.20.10.5
130	8.485670	IntelCor_ac:73:5d	rongrongLEGION-2.local	ARP	42	48:89:e7:62:af:8e		172.20.10.2 is at f8:e4:e3:ac:73:5d
149	10.955945	rongrongLEGION-2.local	86:ad:8d:b7:7a:64	ARP	42	86:ad:8d:b7:7a:64		Who has 172.20.10.1? Tell 172.20.10.5
152	10.960609	86:ad:8d:b7:7a:64	rongrongLEGION-2.local	ARP	42	48:89:e7:62:af:8e		172.20.10.1 is at 86:ad:8d:b7:7a:64
213	20.965922	rongrongLEGION-2.local	86:ad:8d:b7:7a:64	ARP	42	86:ad:8d:b7:7a:64		Who has 172.20.10.1? Tell 172.20.10.5
214	20.980508	86:ad:8d:b7:7a:64	rongrongLEGION-2.local	ARP	42	48:89:e7:62:af:8e		172.20.10.1 is at 86:ad:8d:b7:7a:64
389	53.959727	rongrongLEGION-2.local	86:ad:8d:b7:7a:64	ARP	42	86:ad:8d:b7:7a:64		Who has 172.20.10.1? Tell 172.20.10.5
390	53.972662	86:ad:8d:b7:7a:64	rongrongLEGION-2.local	ARP	42	48:89:e7:62:af:8e		172.20.10.1 is at 86:ad:8d:b7:7a:64

同学的 ip 为 172.20.10.2



解释 ARP 报文(请求)字段的含义：

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b····· 
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ······H· ·b····· 
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

开头 2 个字节为 Hardware type，该 ARP 报文的 Hardware type 为 Ethernet(1)

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b····· 
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ······H· ·b····· 
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 2 个字节为 Protocol type，该 ARP 报文为例的 Protocol type 为 IPv4

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b····· 
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ······H· ·b····· 
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 1 个字节为 Hardware size，该 ARP 报文的 Hardware size 为 6

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b ·····
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ····· ··H· ·b ·····
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 1 个字节为 Protocol size，该 ARP 报文的 Protocol size 为 4

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b ·····
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ····· ··H· ·b ·····
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 2 个字节为 Opcode，该 ARP 报文的 Opcode 为 request(1)

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b******
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ******H· ·b******
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 6 个字节为 Sender MAC address，该 ARP 报文的 Sender MAC address 为 48:89:e7:62:af:8e

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b******
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ******H· ·b······
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 4 个字节为 Sender IP address，该 ARP 报文的 Sender IP address 为 172.20.10.5

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b ·····
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ····· H· ·b ·····
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 6 个字节为 Target MAC address，该 ARP 报文的 Sender MAC address 为 f8:e4:e3:ac:73:5d

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b ·····
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ····· H· ·b ·····
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

接下来 4 个字节为 Target IP address，该 ARP 报文的 Target IP address 为 172.20.10.2

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Sender IP address: rongrongLEGION-2.local (172.20.10.5)
    Target MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Target IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)

0000  f8 e4 e3 ac 73 5d 48 89  e7 62 af 8e 08 06 00 01   ····s]H· ·b ·····
0010  08 00 06 04 00 01 48 89  e7 62 af 8e ac 14 0a 05   ····· H· ·b ·····
0020  f8 e4 e3 ac 73 5d ac 14  0a 02                     ····s]·· ··
```

解释 ARP 报文(响应)字段的含义：

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ····· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

开头 2 个字节为 Hardware type，该 ARP 报文的 Hardware type 为 Ethernet(1)

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ····· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

接下来 2 个字节为 Protocol type，该 ARP 报文 Protocol type 为 IPv4

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ······· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

接下来 1 个字节为 Hardware size，该 ARP 报文 Hardware size 为 6

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ····· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

接下来 1 个字节为 Protocol size，该 ARP 报文 Protocol size 为 4

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ····· ··· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

接下来 2 个字节为 Opcode，该 ARP 报文的 Opcode 为 request(1)

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ····· ··· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

接下来 6 个字节为 Sender MAC address，该 ARP 报文的 Sender MAC address 为 f8:e4:e3:ac:73:5d

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ····· ··· ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

接下来 4 个字节为 Sender IP address，该 ARP 报文的 Sender IP address 为 172.20.10.2

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ........ ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

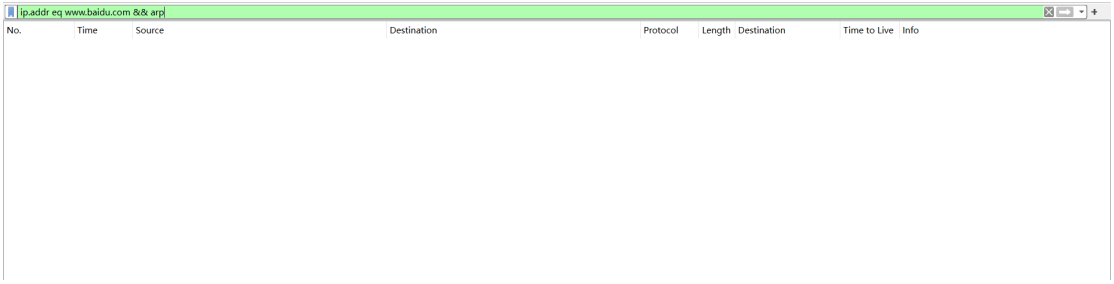
接下来 6 个字节为 Target MAC address，该 ARP 报文的 Sender MAC address 为 48:89:e7:62:af:8e

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ........ ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ··
```

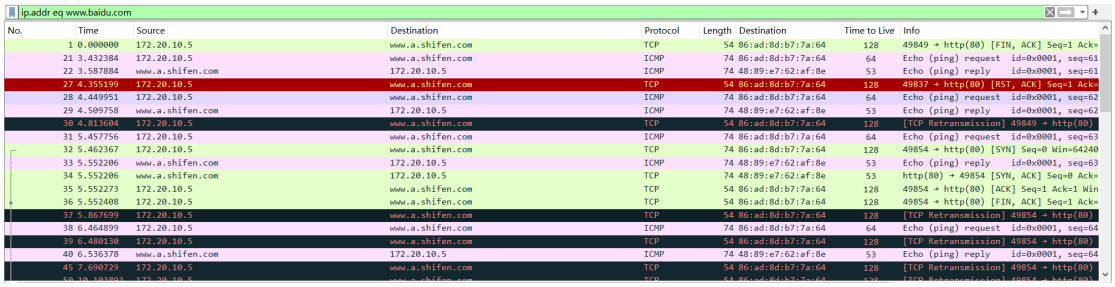
接下来 4 个字节为 Target IP address，该 ARP 报文的 Target IP address 为 172.20.10.5

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (f8:e4:e3:ac:73:5d)
    Sender IP address: 9f05289f-37b8-4a42-b60f-e73aa9d702ad.local (172.20.10.2)
    Target MAC address: rongrongLEGION-2.local (48:89:e7:62:af:8e)
    Target IP address: rongrongLEGION-2.local (172.20.10.5)

0000  48 89 e7 62 af 8e f8 e4  e3 ac 73 5d 08 06 00 01   H··b···· ··s]····
0010  08 00 06 04 00 02 f8 e4  e3 ac 73 5d ac 14 0a 02   ........ ··s]····
0020  48 89 e7 62 af 8e ac 14  0a 05                     H··b···· ····
```

(3)ping www.baidu.com



此处，我们发现这里并没有 arp 报文，但是此处会显示出 ICMP 类型的 IP 数据包以及 TCP 类型的 IP 数据包，如下图所示：

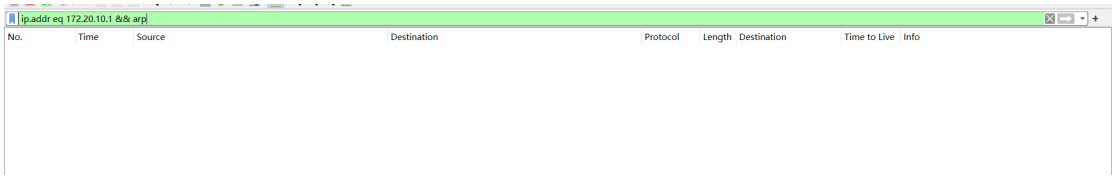


www.baidu.com 并不处于与本地主机的同一个局域网内，我们需要 ping 网关

默认网关如下图：

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   IPv6 地址 . . . . . : 240e:466:2420:6ebc:2d61:5ce3:9964:9bfb
   临时 IPv6 地址. . . . . : 240e:466:2420:6ebc:b5ca:5efb:a521:6ce0
   本地链接 IPv6 地址. . . . . : fe80::2d61:5ce3:9964:9bfb%3
   IPv4 地址 . . . . . : 172.20.10.5
   子网掩码 . . . . . : 255.255.255.240
   默认网关. . . . . : fe80::84ad:8dff:feb7:7a64%3
                                       172.20.10.1
```

```
C:\Users\rongrong>ping 172.20.10.1

正在 Ping 172.20.10.1 具有 32 字节的数据:
来自 172.20.10.1 的回复: 字节=32 时间=7ms TTL=64
来自 172.20.10.1 的回复: 字节=32 时间=3ms TTL=64
来自 172.20.10.1 的回复: 字节=32 时间=7ms TTL=64
来自 172.20.10.1 的回复: 字节=32 时间=7ms TTL=64

172.20.10.1 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms，最长 = 7ms，平均 = 6ms
```



但是也没有任何 ARP 报文。

我们可以结合课本上的工作原理对 ping 同一局域网下的计算机和局域网外的计算机产生的不同影响进行说明：

对于同一局域网下的计算机：

(a) 我们首先清空自己的 arp 缓存，不知道其他任何一个主机的 MAC 地址；

(b) 我们 ping 同一局域网下的一台主机，会在本局域网上请求发送一个 ARP 请求分组；

(c) 得到目的主机的 MAC 地址后，本主机的 ARP 高速缓存得以更新，

将目的主机的 IP 地址和 MAC 地址对应上加入 ARP 高速缓存。

而对于局域网外的计算机：

ARP 用于解决同一个局域网上的主机或路由器的 IP 地址和 MAC 地址的映射问题，如果要找的主机和源主机不在同一个局域网上，源主机就无法解析出另一个局域网上的主机的 MAC 地址。

任务 2：捕获和分析 802.11 数据

2.1 搭建实验环境

实验环境：Ubuntu 64 位虚拟机环境 + USB 无线网卡

(1) 打开终端，安装 Wireshark 软件：

`sudo apt install wireshark`

`sudo apt install wireshark-gtk`

(2) 查询网卡状态：

`iwconfig`

```
rongrong@rongrong-virtual-machine:~/Desktop$ iwconfig
lo        no wireless extensions.

ens33     no wireless extensions.
```

捕获 802.11 帧需要设置网卡为监控模式（即 monitor mode，非混杂模式），但是构建的虚拟机里显示的如上两个网卡都是虚拟机内设的，都不可以设置为监控模式（但是可以设置为混杂模式），所以需要将本地 win10 中的网卡连接到虚拟机中。

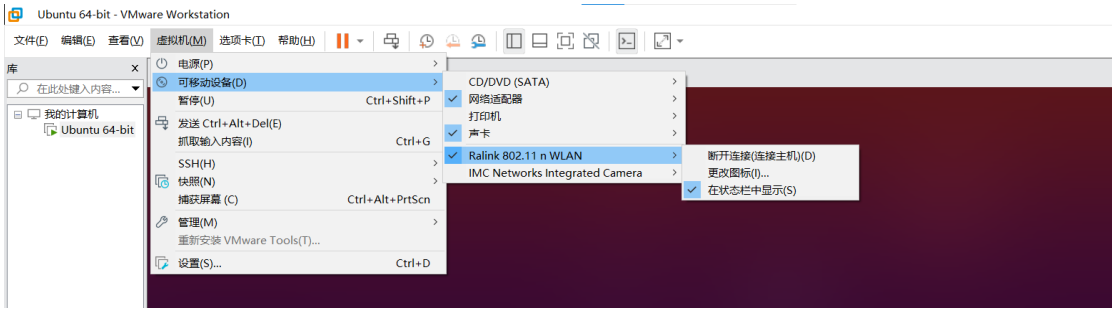
2.2 构建无线环境，捕获无线数据包、分析 802.11 数据

构建无线环境：

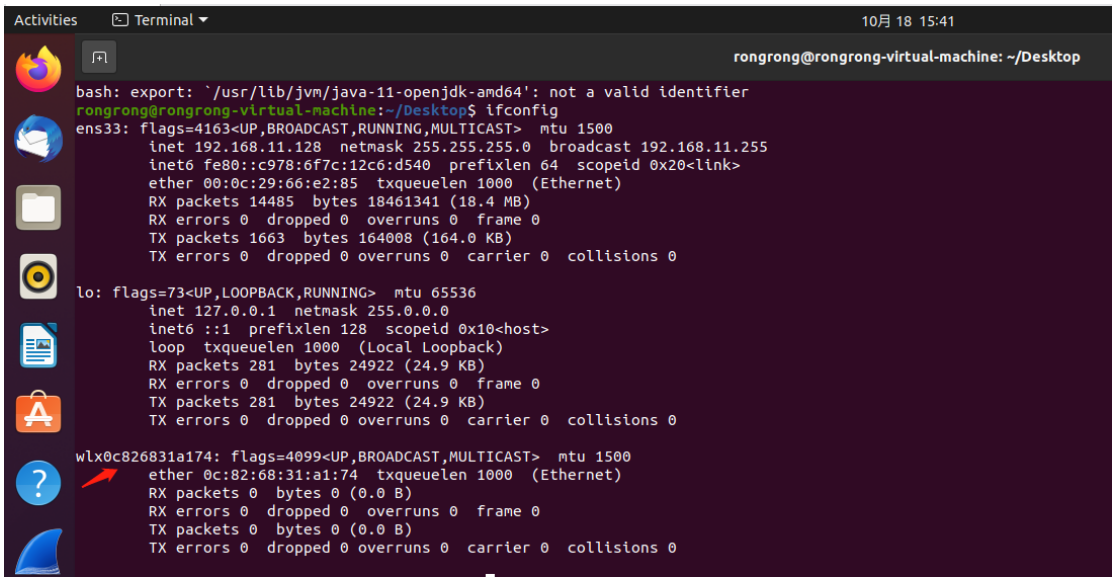
(1) 将 USB 无线网卡插到电脑机箱上

(2) 打开虚拟机里的 Ubuntu 64-bit 系统

(3) 更改设置，使网卡连接到虚拟机上



打开终端，输入 ifconfig，看到多了一个 wlx0c826831a174



无线网卡配置：

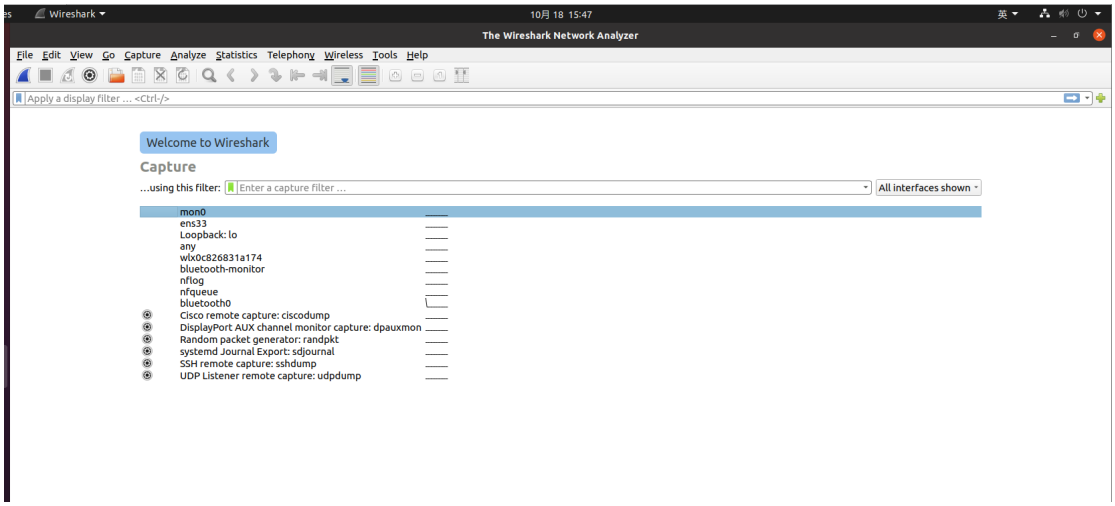
(1) 新建一个虚拟网卡，并将其修改为监听模式

```
rongrong@rongrong-virtual-machine:~/Desktop$ iw wlx0c826831a174 interface add mon0 type monitor
command failed: Operation not permitted (-1)
rongrong@rongrong-virtual-machine:~/Desktop$ sudo iw wlx0c826831a174 interface add mon0 type monitor
[sudo] password for rongrong:
```

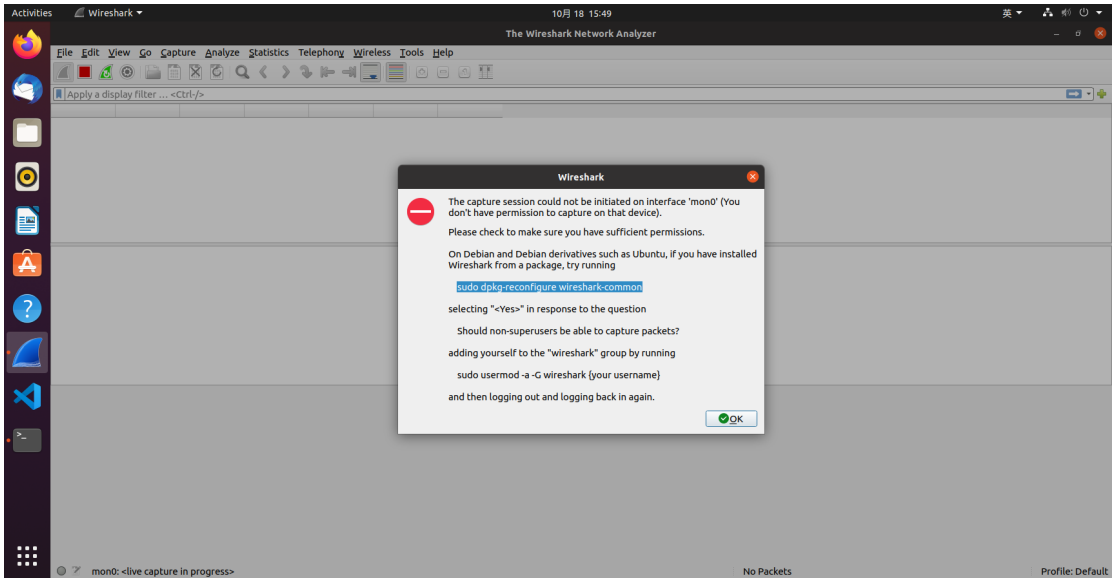
```
rongrong@rongrong-virtual-machine:~/Desktop$ ifconfig mon0 up
SIOCSIFFLAGS: Operation not permitted
rongrong@rongrong-virtual-machine:~/Desktop$ sudo ifconfig mon0 up
rongrong@rongrong-virtual-machine:~/Desktop$
```

(2) 终端输入“wireshark”，打开 Wireshark 软件

可以看到“mon0”，如下图所示：

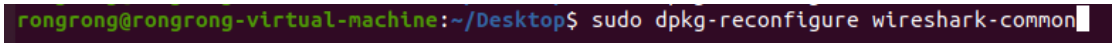


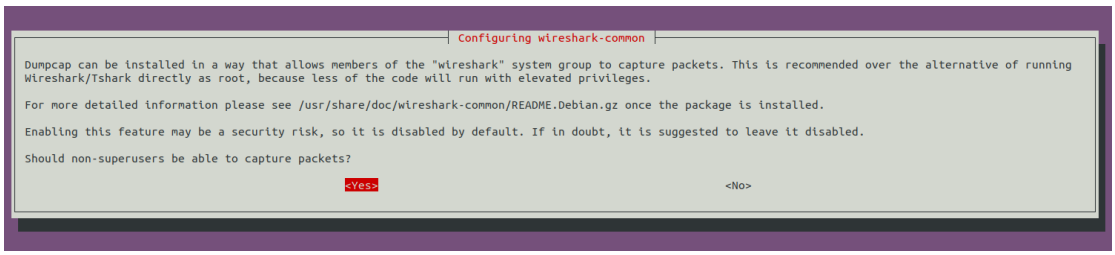
但是这里我们可以并没有看到有上下起伏的折线，应该是哪里有问题，双击尝试一下能否捕捉，果然不行，显示如下：



在终端输入一下指令：

` sudo dpkg-reconfigure wireshark-common `

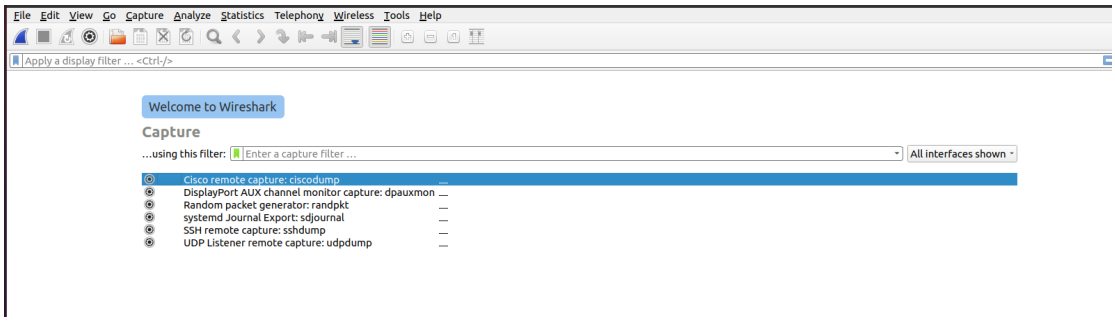




选择 yes

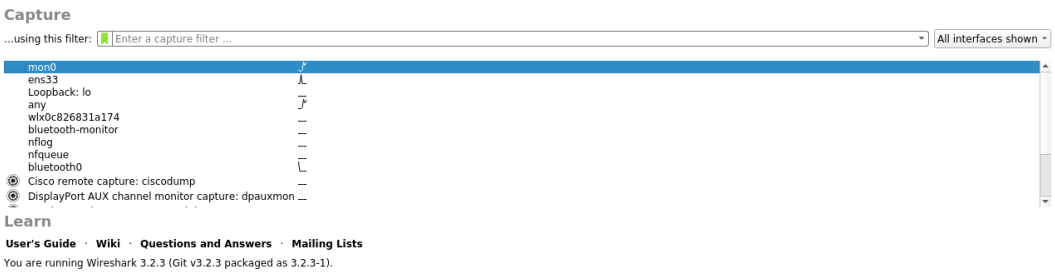
再次打开 wireshark

发现什么端口都没有了，只剩下蓝牙端口，于是重新安装 Wireshark。



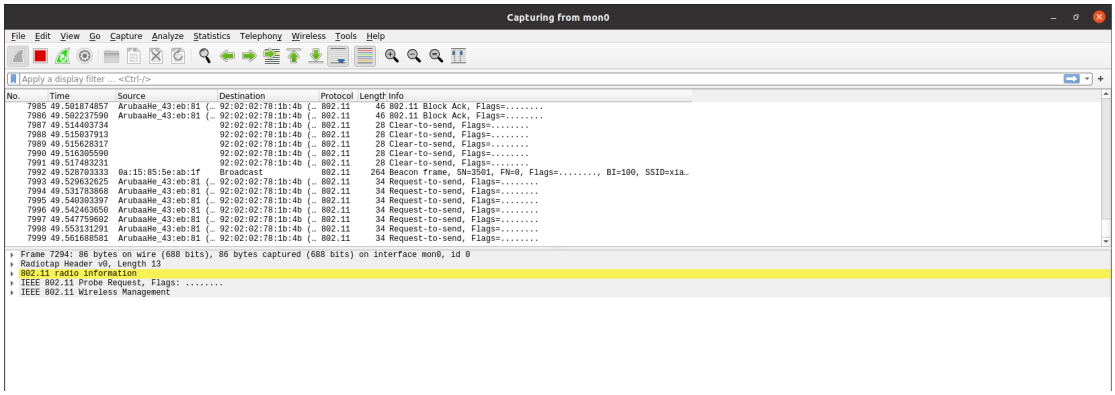
使用 sudo 命令打开 Wireshark

可以看到 mon0 有上下起伏的波形，如下图所示：



捕获和分析 802.11 数据：

双击 mon0 开始捕获，即可捕获到 802.11 数据



捕获到的 802.11 数据如上图所示。

任务 3：探索 Wireshark 更多功能和其它抓包工具(选做)

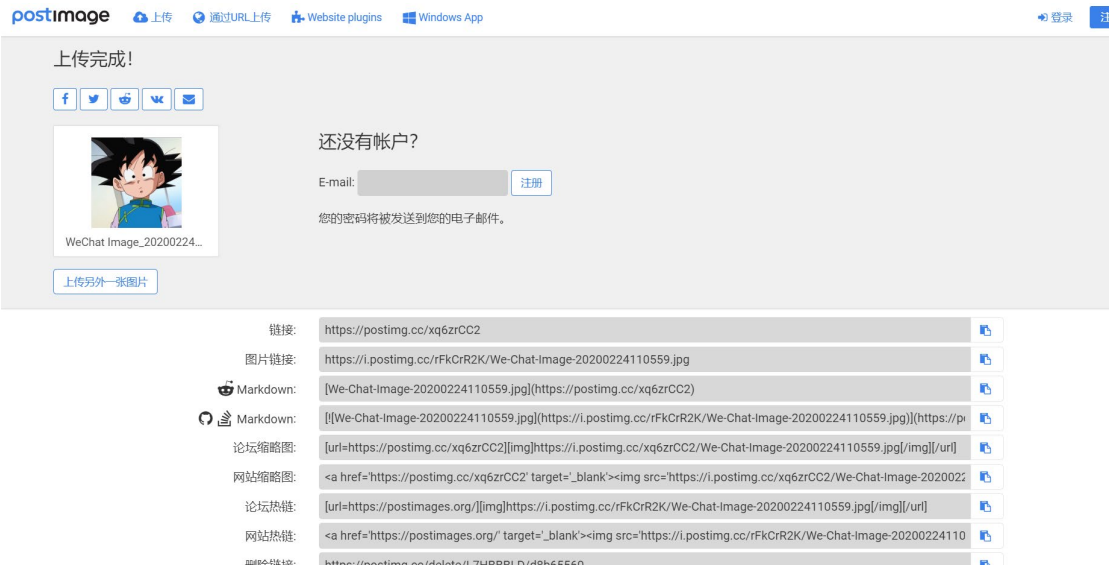
探索 Wireshark 更多功能

(1) 数据流追踪

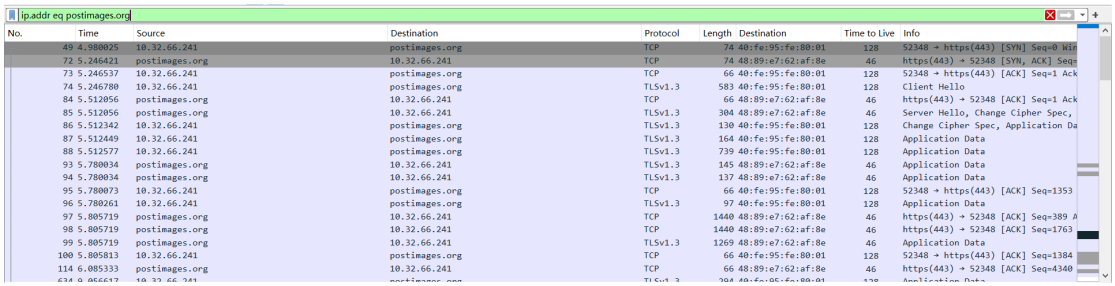
先登录一个免费的图床，我们这里以“postimage”为例，其域名为“postimages.org”

将 Wireshark 的显示过滤器设置为“ip.addr eq postimages.org”，如下图所示：

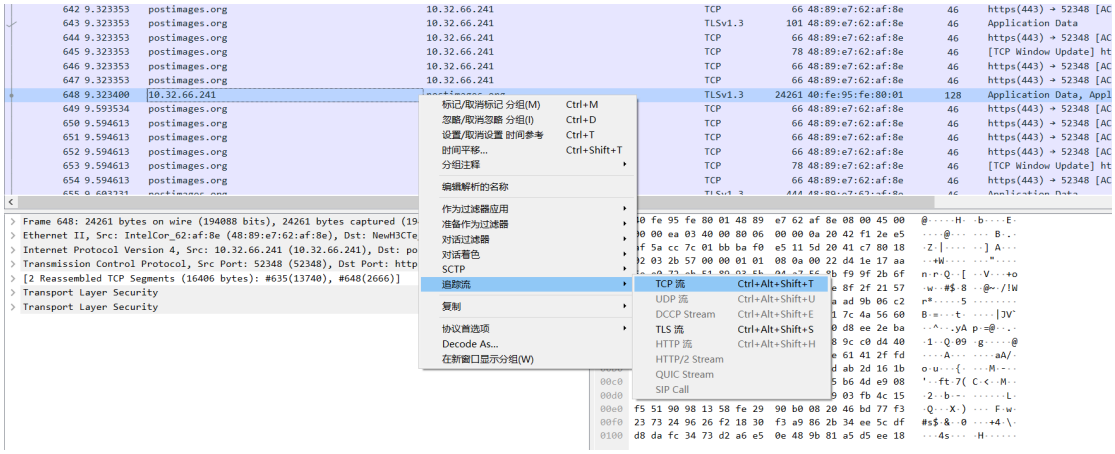
我们选择一张图片上传，如下图：



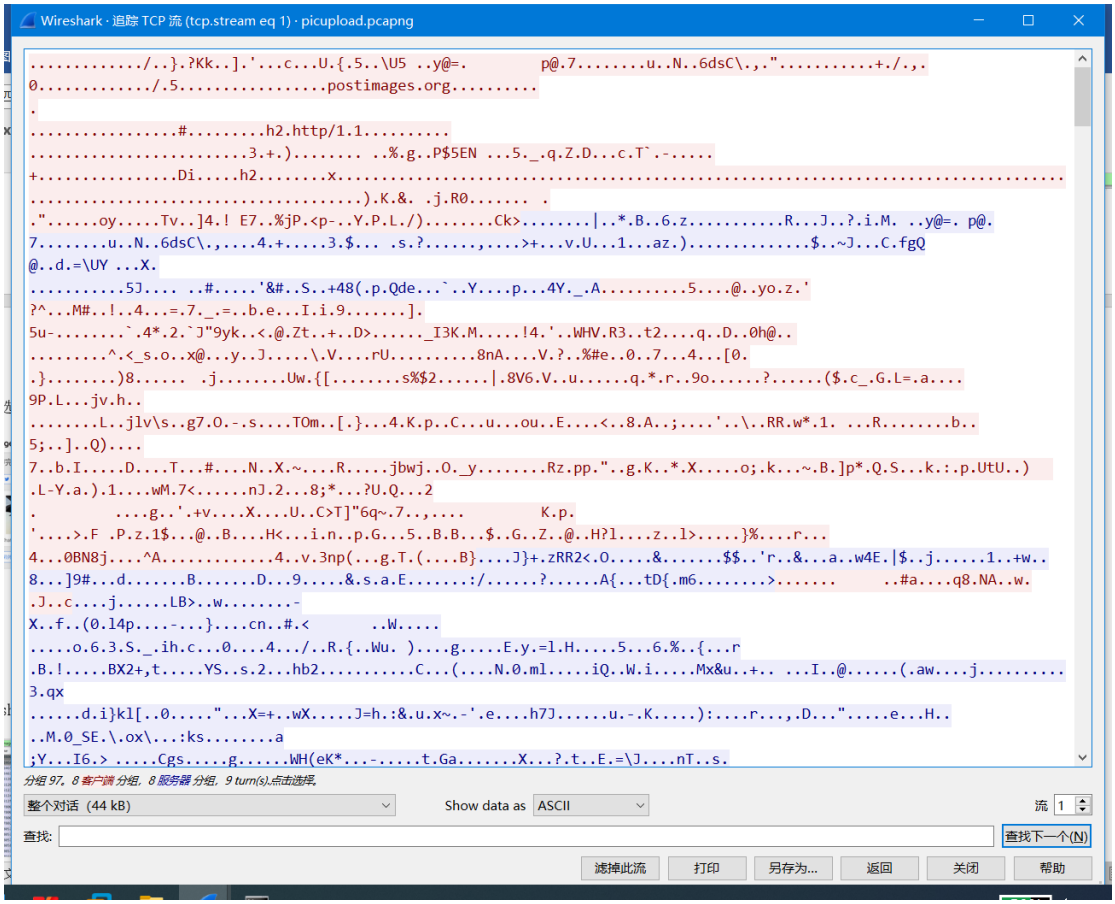
Wireshark 抓包结果如下图所示：



这里我们尝试追踪 TCP 流，如下图所示：

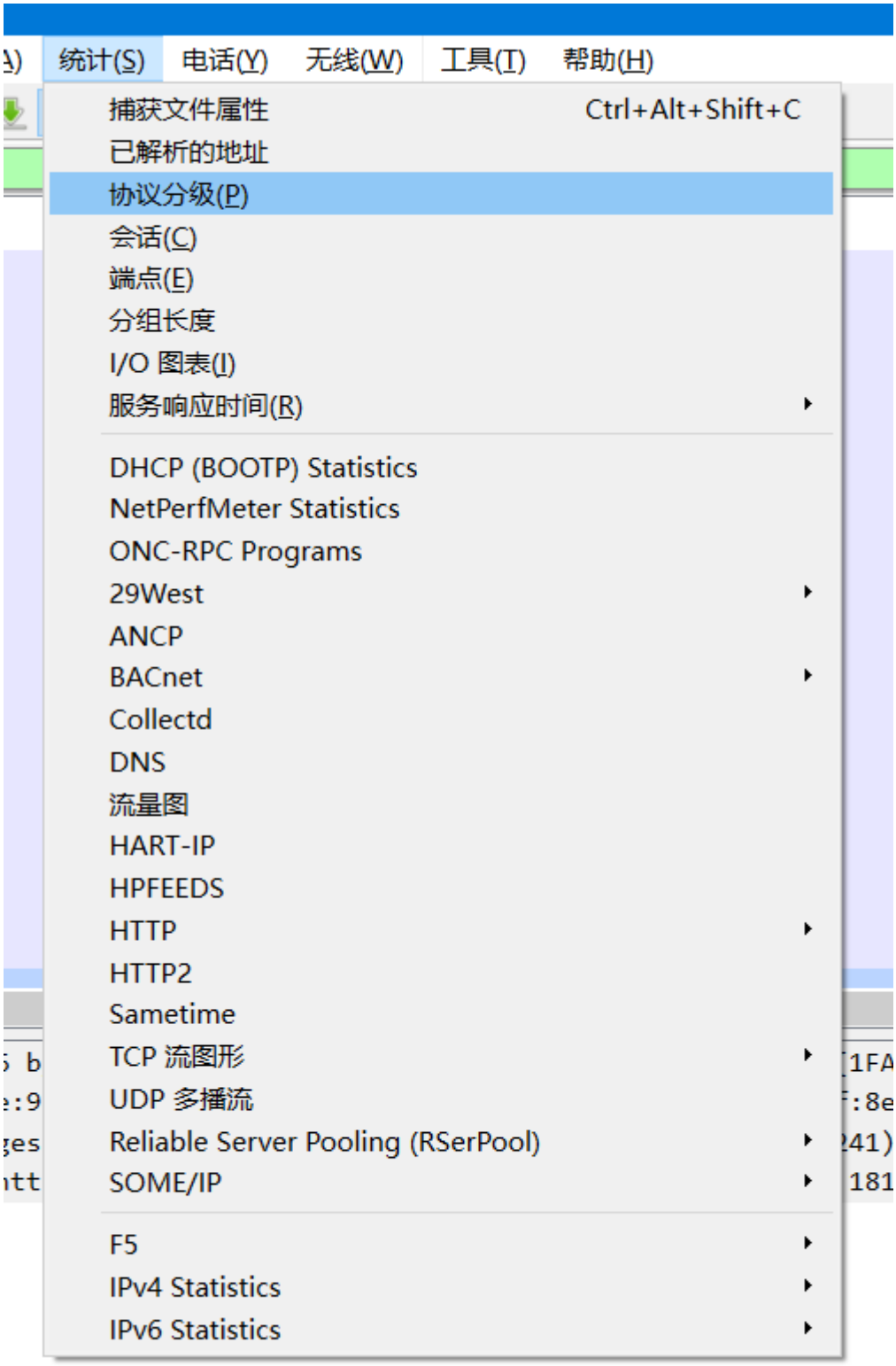


如下图，红色流为源到目的地址，蓝色为目的地址到源：

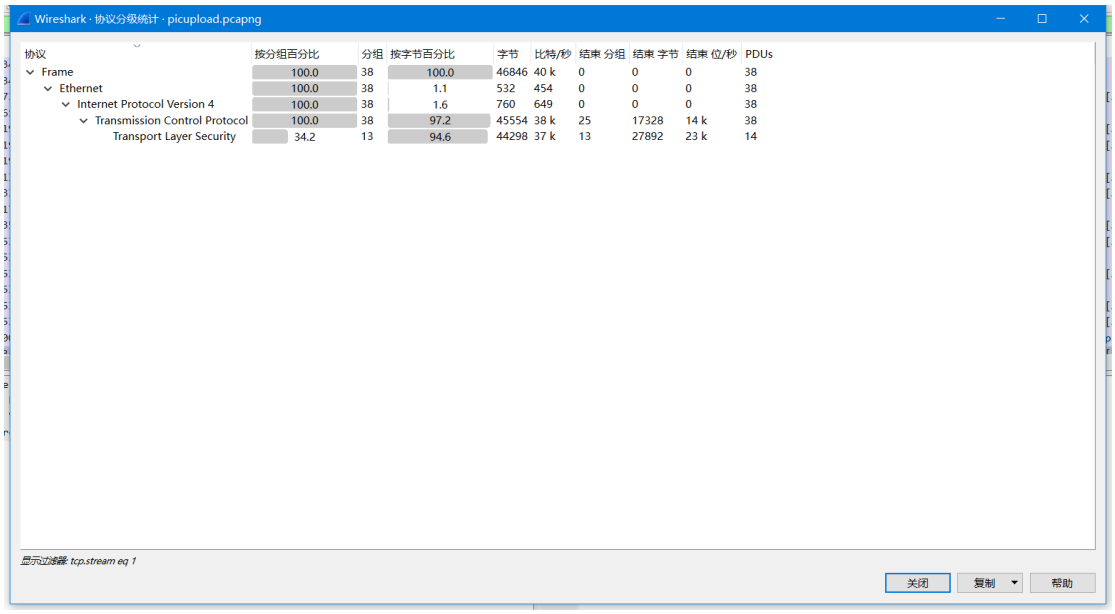


但是我的这里显示乱码，仍未解决……

(2)　协议分层统计

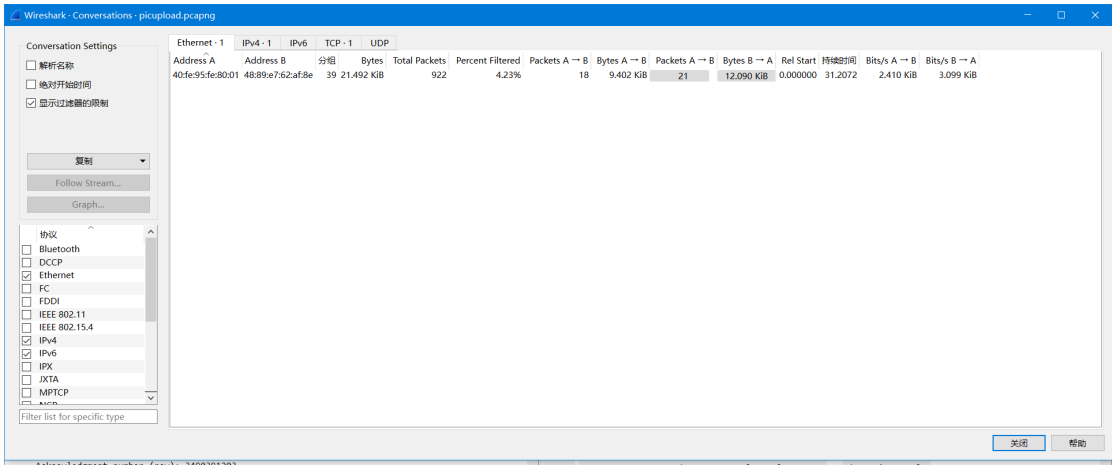


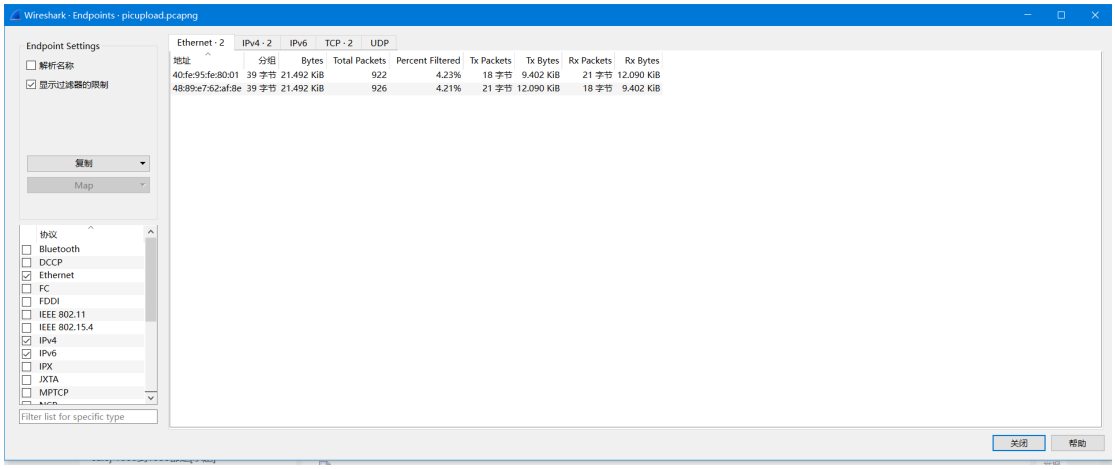
协议分级统计如下图所示：



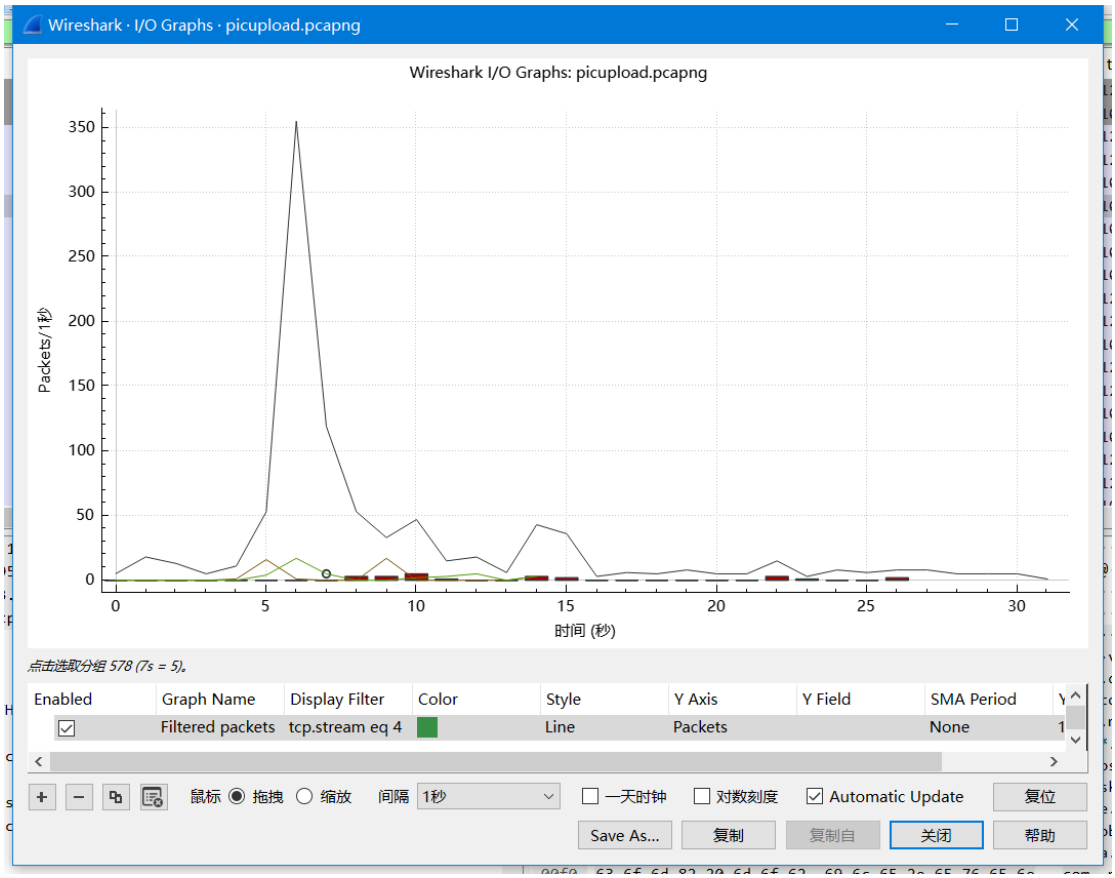
可以看到按分组百分比有 34.2%的数据包是 TSL 协议。

(3) 网络节点和会话统计功能

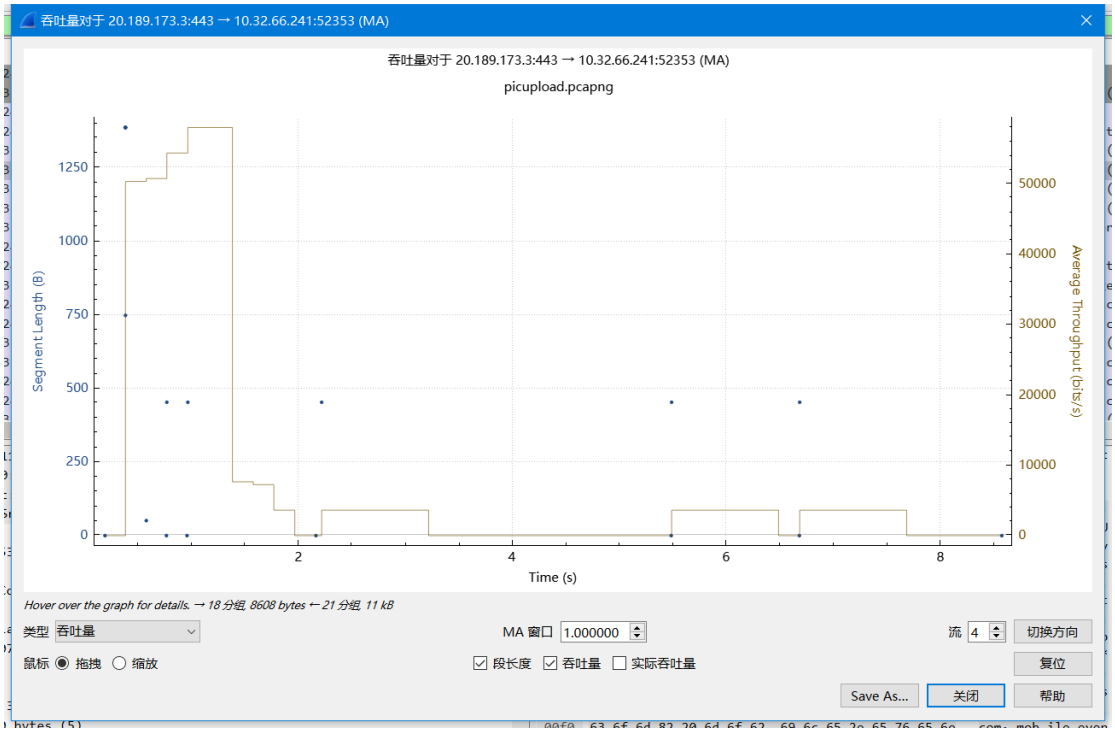




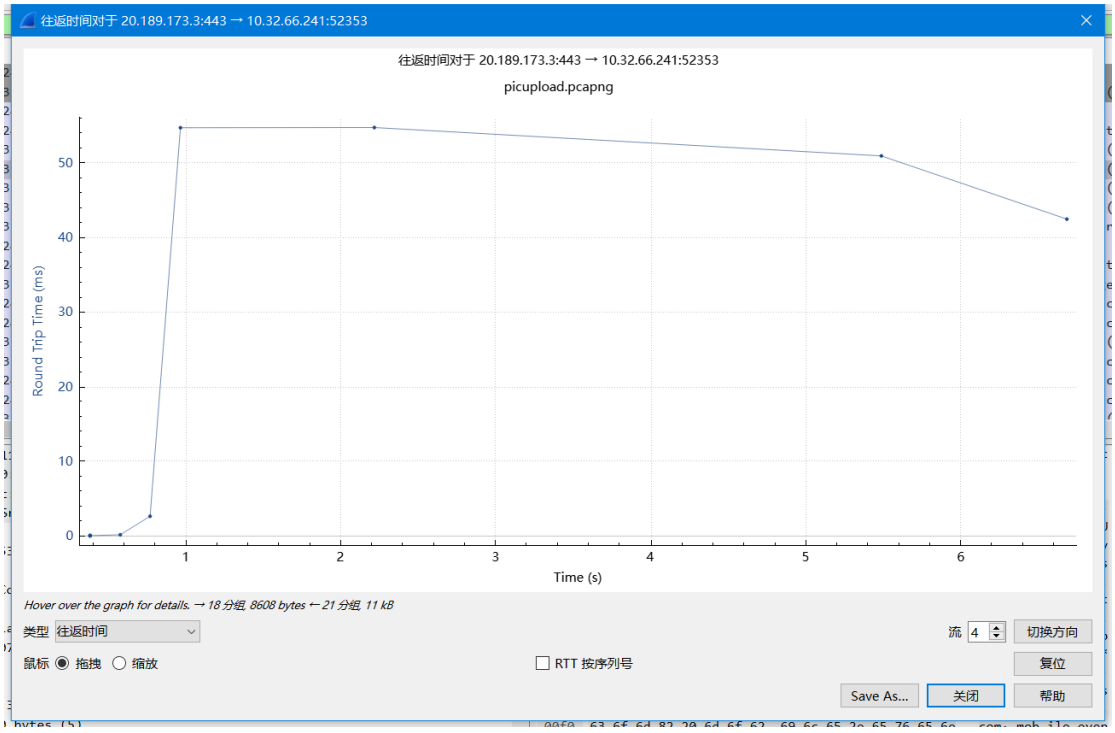
(4) IO 图表


Wireshark · I/O Graphs · picupload.pcapng
Wireshark I/O Graphs: picupload.pcapng
Packets/1秒
时间 (秒)
点击选取分组 578 (7s = 5)。
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Filtered packets
tcp.stream eq 4
Line
Packets
None
鼠标
拖拽
缩放
间隔
1秒
一天时钟
对数刻度
Automatic Update
复位
Save As...
复制
复制自
关闭
帮助

(5) 吞吐量


吞吐量对于 20.189.173.3:443 → 10.32.66.241:52353 (MA)
picupload.pcapng
Segment Length (B)
Average Throughput (bits/s)
Time (s)
Hover over the graph for details. → 18 分组, 8608 bytes ← 21 分组, 11 kB
类型
吞吐量
MA 窗口
1.000000
流
4
切换方向
鼠标
拖拽
缩放
段长度
吞吐量
实际吞吐量
复位
Save As...
关闭
帮助

(6) 往返时间



三、 实验小结

通过本次实验，我学会了一些使用 wireshark 抓包的基本操作，并自行探索了 wireshark 更强大的功能。对一些报文如 IPv4、IPv6、ARP 等有了更深层、更直观的理解。