**计算机网络实验报告（实验3）**

  班级21计科留学生（1） 学号2021529620004 姓名 LOW REN HONG

实验时间： 18/12/2023

|  |  |  |
| --- | --- | --- |
| **课程目标2** | **课程目标3** | **报告成绩** |
|  |  |  |

1. 实验名称：

**Wireshark 软件使用与 ARP 协议分析，IP 与 ICMP 分析**

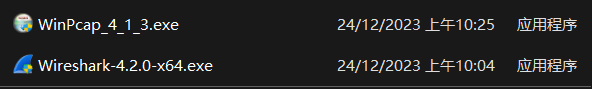
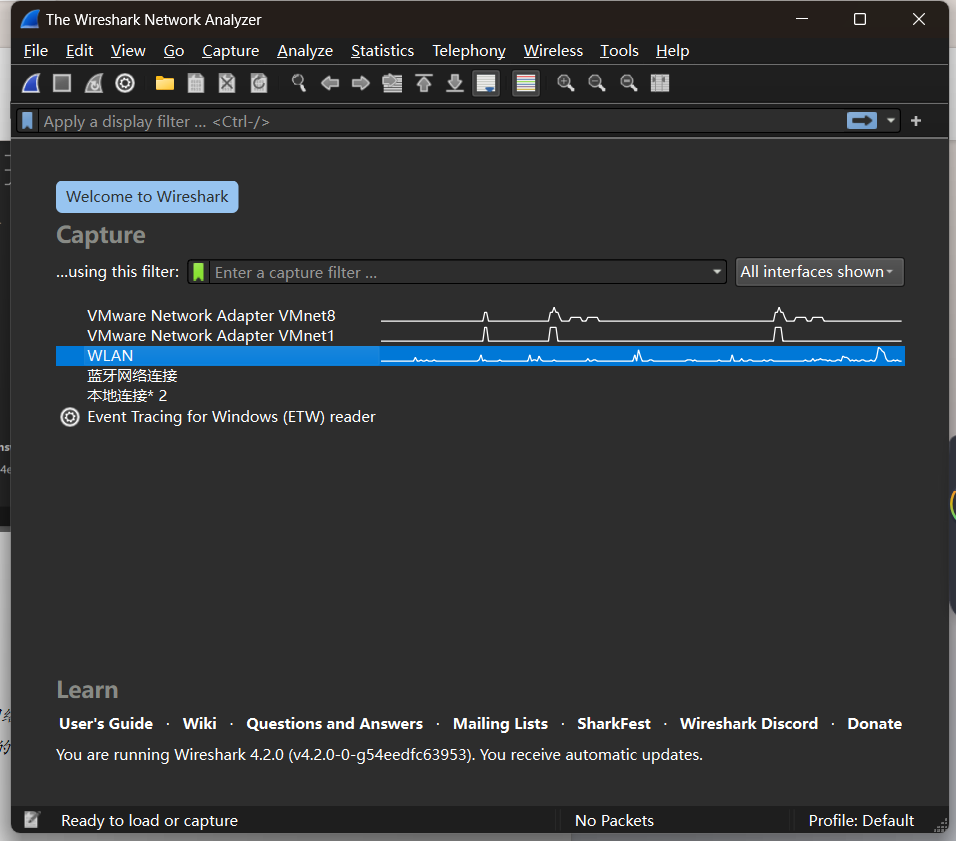
1. 实验目的：
   * 1. 学习 Wireshark 基本操作：重点掌握捕获过滤器和显示过滤器。
     2. 观察 MAC 地址：了解 MAC 地址的组成，辨识 MAC 地址类型。
     3. 分析以太网帧结构：观察以太网帧的首部和尾部，了解数据封装成帧的原理。
     4. 分析 ARP 协议：抓取 ARP 请求和应答报文，分析其工作过程。
     5. 使用 Wireshark 软件，观察 IP数据报的基本结构，分析数据报的分片；掌握基于 ICMP 协议的 ping 和 traceroute 命令及其工作原理。
2. 实验方案：

WireShark:4.2.0 和 WinPcap4.1.4

Ping工具：CMD

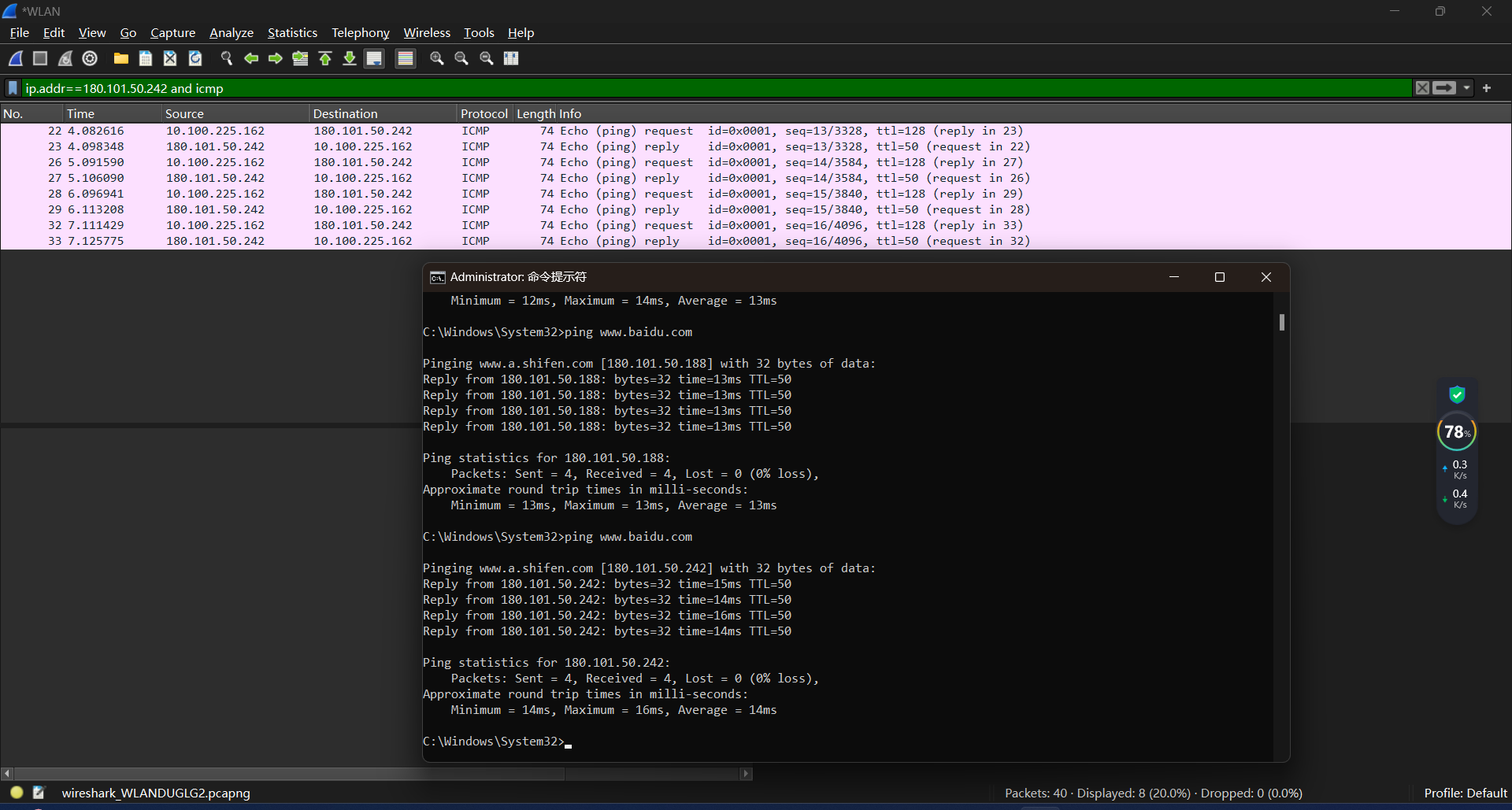
**1.1安装WireShark**

这里选择的是WireShark的最新版然后使用的是WinPcap是因为在安装WireShark的时候默认安装了Npcap但是安装不了，报错了。发现是没用管理员运行但是运行了还是一样不行还是报错了就删除了Npcap然后运动了WinPcap来代替Npcap。WireShark的安装可以在官网安装和WinPcap也可以在官网上安装。

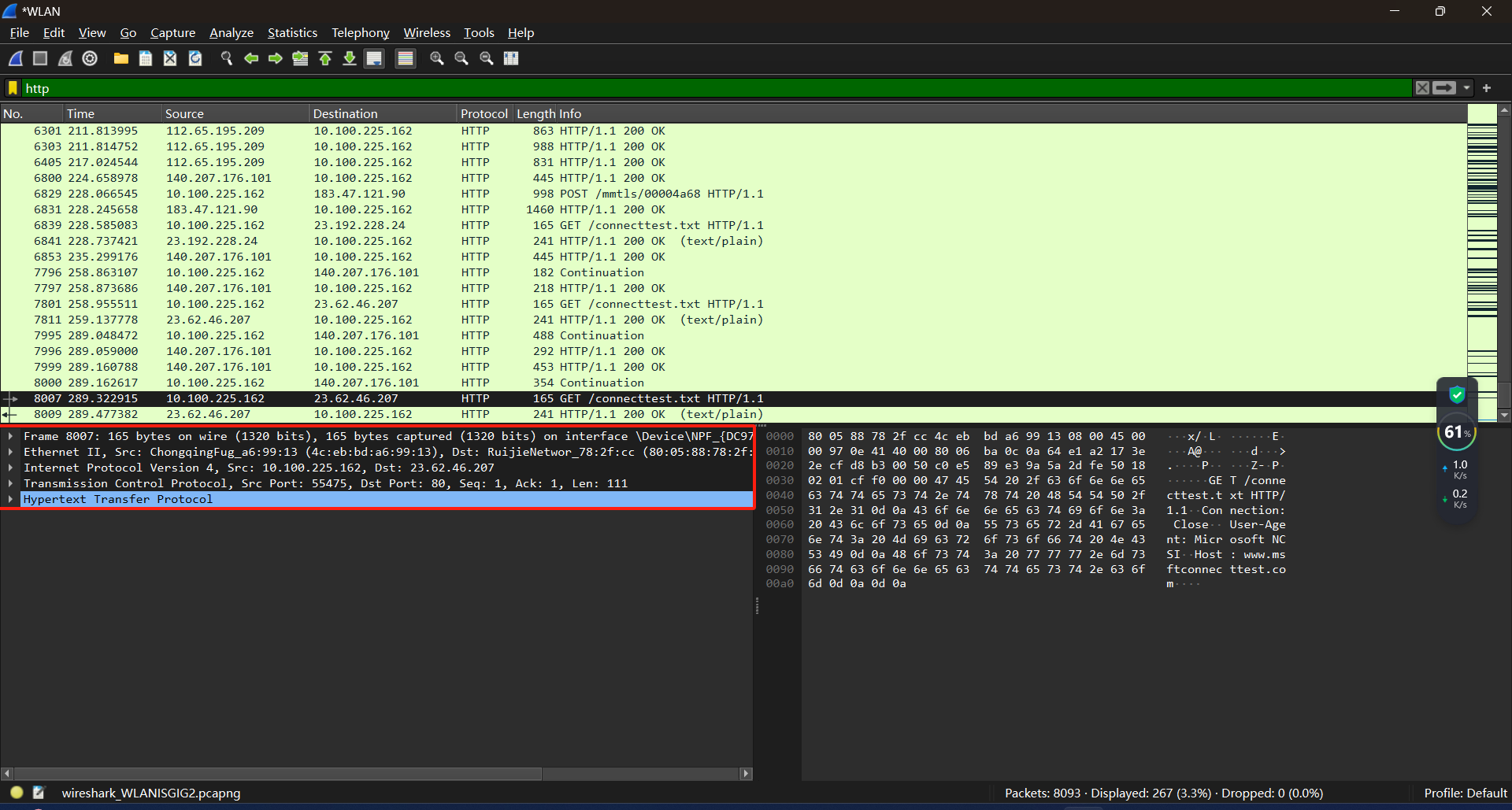
WireShark

**1.2 实现网络协议分析软件在网络环境中进行数据包捕获**



WireShark数据包捕获

这里我们尝试使用CMD里的ping [www.baidu.com](http://www.baidu.com) 为了避免不必要的数据包影响分析，这里使用了WireShark里的Filter ip.addr==180.101.50.242 and icmp。Icmp只是表示显示协议且源主机IP或者目标主机Ip为10.100.50.242的数据包。ip.addr 180.101.50.242是www.baidu.com的ip而我们自己的ip是10.100.50.242。我们可以使用ipconfig里来查找自己的ip。



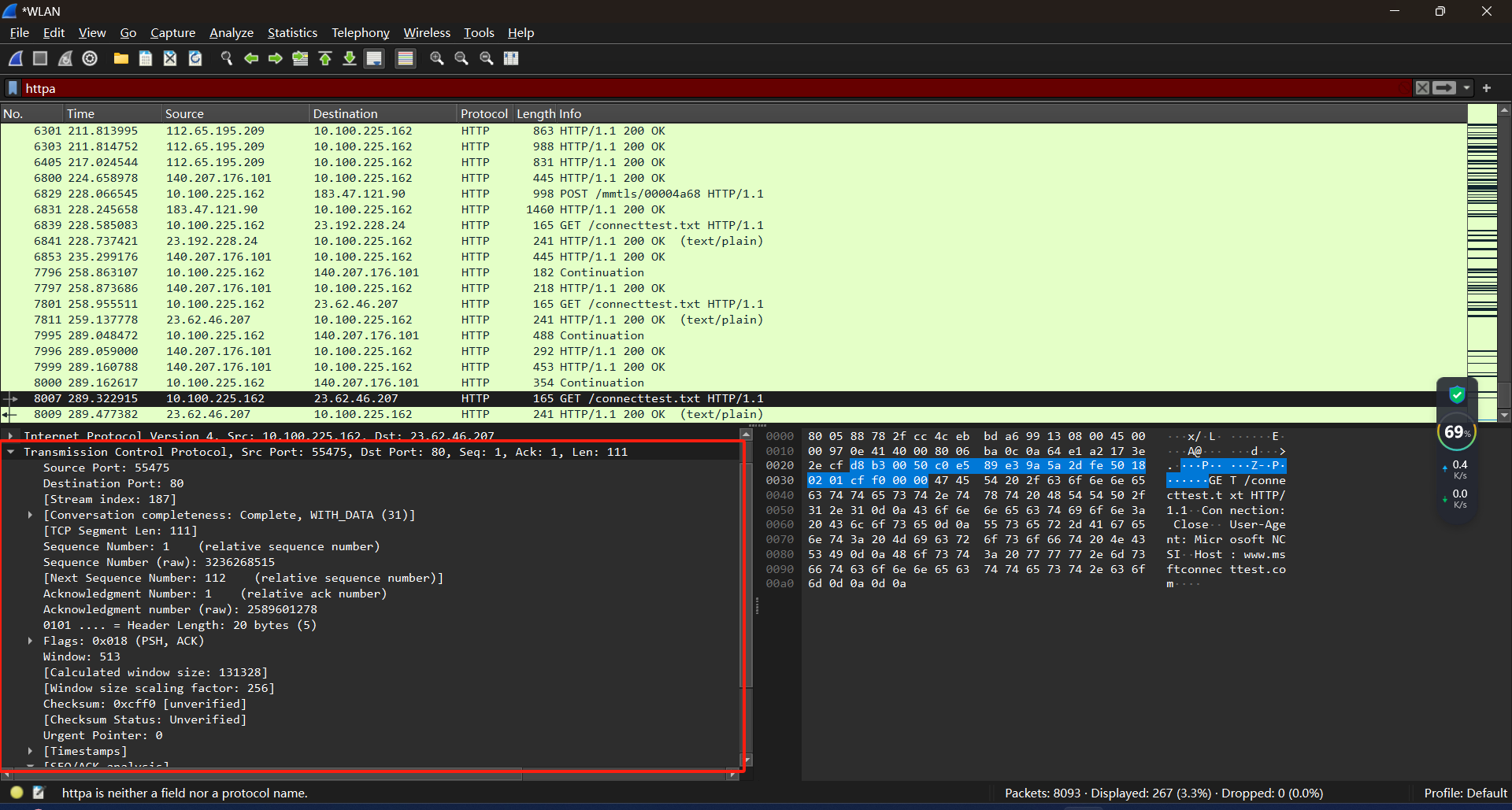
Frame对应的是物理层

Ethernet对应的是数据链路曾

Internet Protocol 对应的是网络层,也就是IP

Transmission Control Protocol对应的是传输层,TCP

Hypertext Transfer Protocol 对应的应用层



TCP的从Wireshark里捕获到的每个字段

SourcePort对应的是TCP里的端口号

DestinationPort 对应的是目的端口号

Sequence number 对应的是序号

Acknowledgment number是确认号

Header length是报头长度

Flags 是标志位

Window size是窗口

Checksum 是检验和

实验数据及数据的解释与对比分析：

*【考察1）是否能收集和记录有效数据。2） 是否能对数据进行解释和对比分析。】*

**1.3 观察 MAC 地址**

分别ping了www.huawei.com和ping自己的ip

**重点观察以太网帧的 Destination 和 Source 的 MAC 地址， 辨识 MAC 地址类型，解读 OUI 信息、I/G 和 G/L 位。**

1. Destination Address: 78:2f:cc (80:05:88:78:2f:cc)

OUI信息：80:05:88

I/G位：I (Individual，因为最左边的十六进制数的最右侧位是0)

G/L位：G (Global，因为最左边的十六进制数的次右侧位是0)

解释：

目标MAC地址的OUI信息是80:05:88，表示这个地址属于某个特定制造商。

I/G位为I，表明这是一个单播地址。

G/L位为G，表明这是一个全局地址。

1. Source Address: a6:99:13 (4c:eb:bd:a6:99:13)

OUI信息：4c:eb:bd

I/G位：I (Individual，因为最左边的十六进制数的最右侧位是0)

G/L位：G (Global，因为最左边的十六进制数的次右侧位是0)

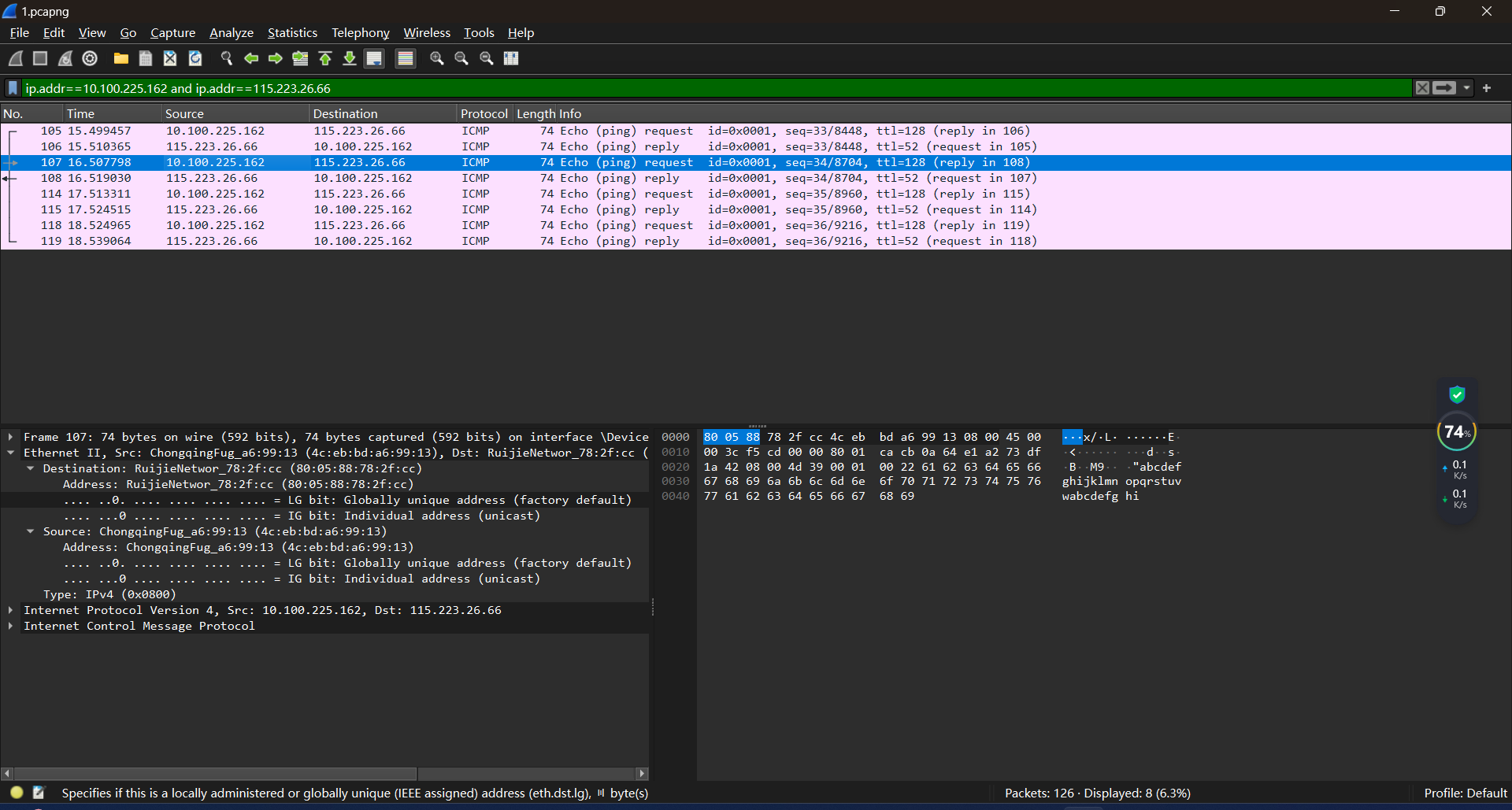
解释：

源MAC地址的OUI信息是4c:eb:bd，表示这个地址属于某个特定制造商。

I/G位为I，表明这是一个单播地址。

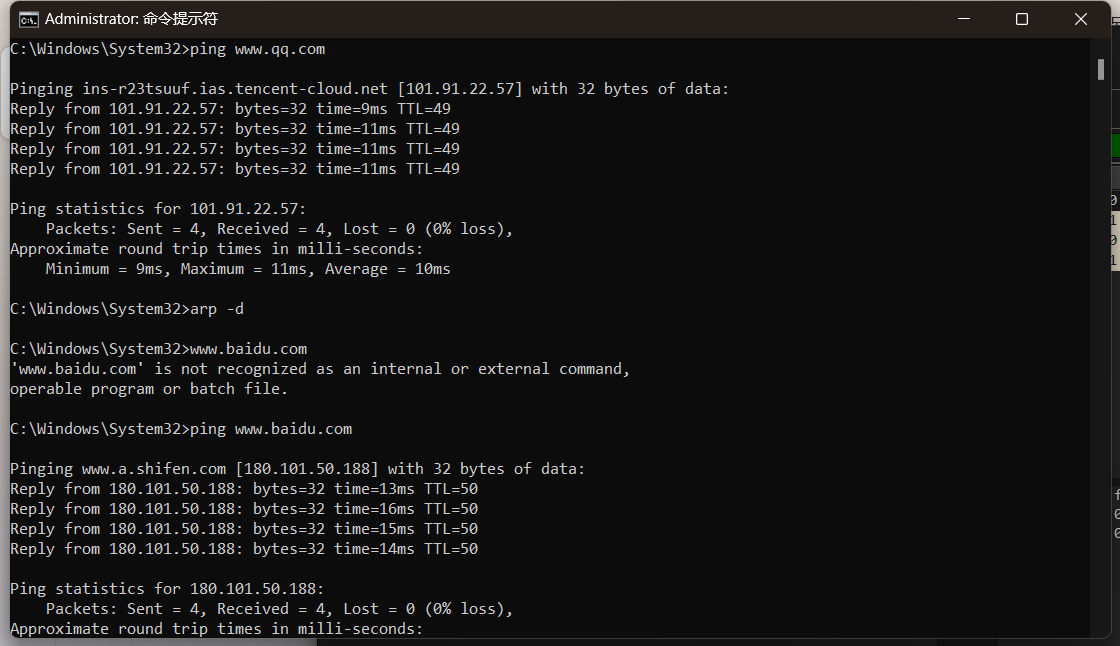
G/L位为G，表明这是一个全局地址。

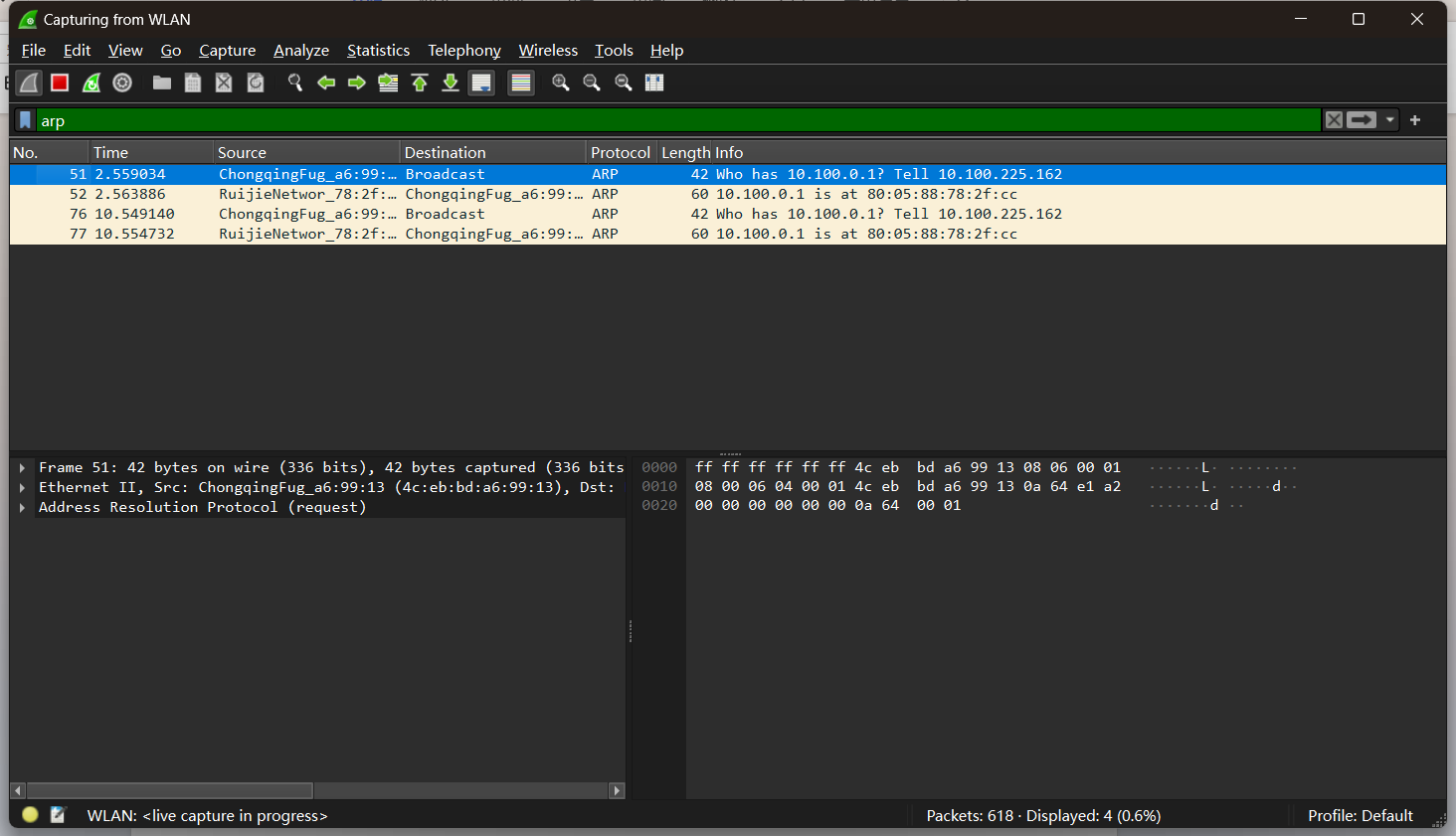
**1.4 分析以太网的帧结构**



这两个MAC地址都是单播地址，属于全局范围，分别对应于某个特定制造商。这些信息有助于识别设备制造商和MAC地址的类型。

**1.5 ARP 协议分析**



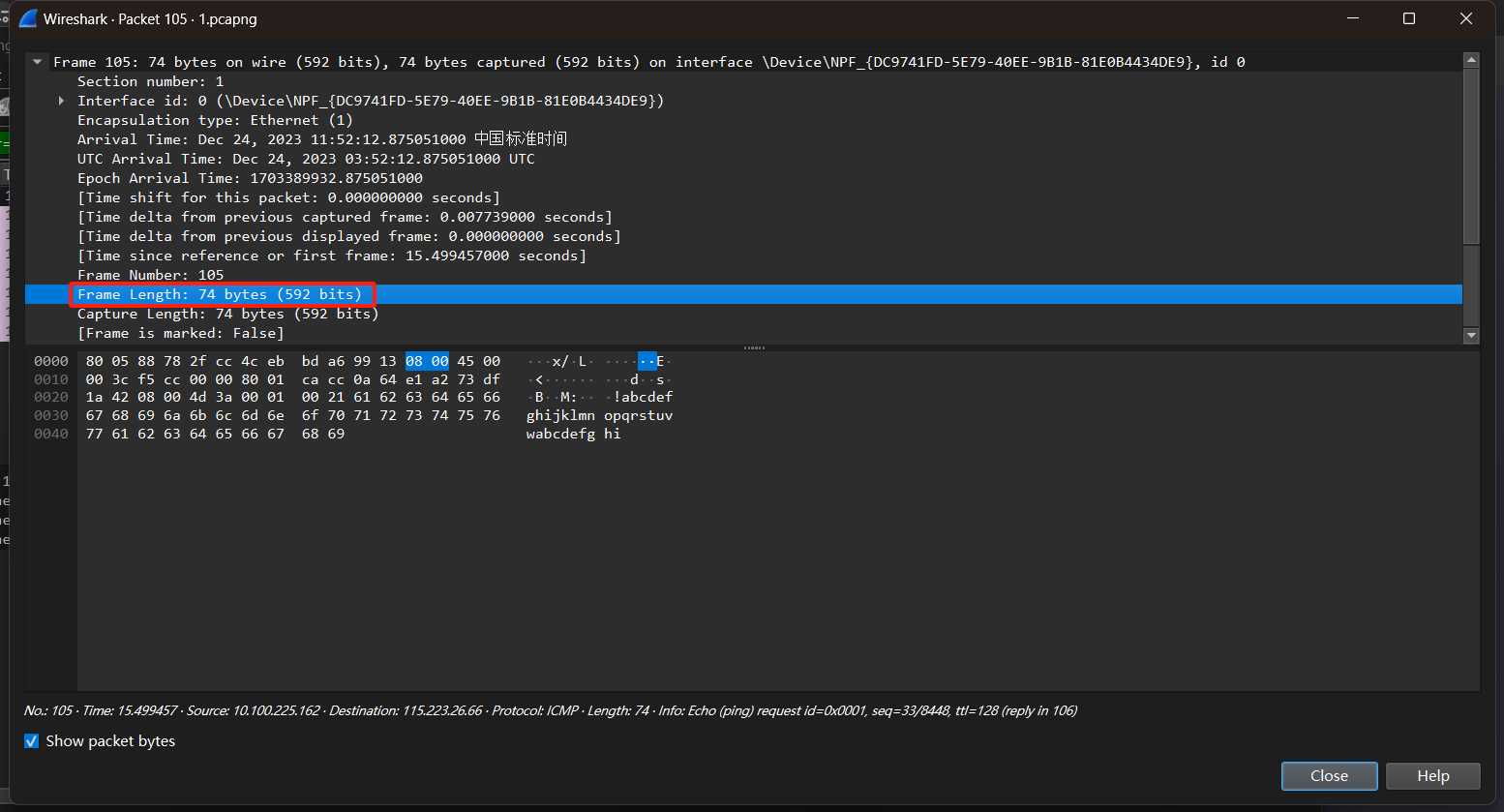


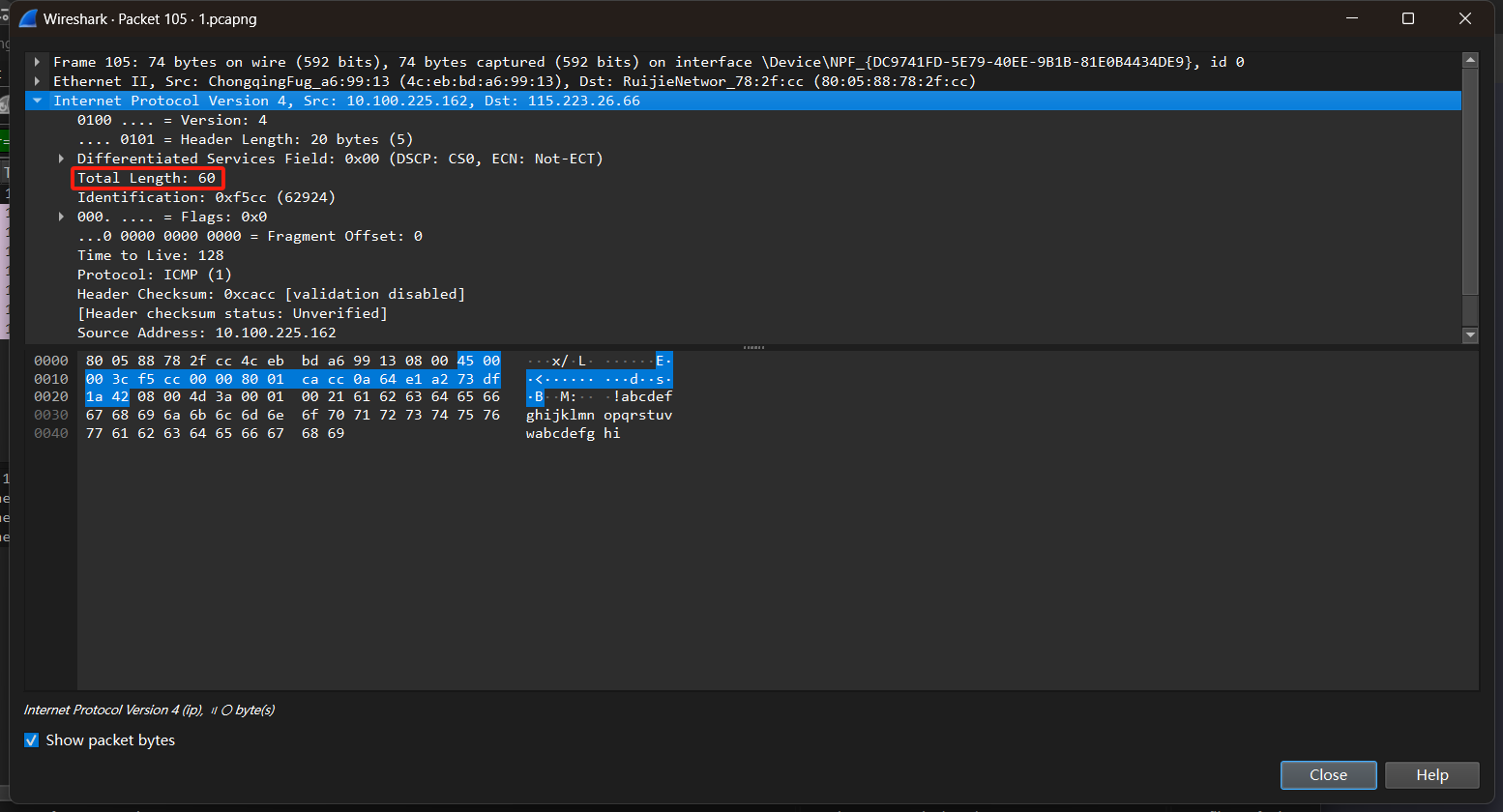
**1.6 思考题**

1. **使用了显示过滤器后，Wireshark 的抓包工作量会减少吗？**

不会，显示过滤器只是用于方便用户来查看数据包

1. **MAC 帧的长度和 IP 数据报的长度有怎样的关系？请用你的数据记录进行验证。**





Frame length 表示整个 MAC 帧的长度，而 Total length 表示 IP 数据报的总长度。MAC 帧的数据字段包含了整个 IP 数据报，包括 IP 头、TCP/UDP 头和应用层数据。

1. ping 同一局域网内的主机和局域网外的主机，都会产生 ARP 报文么？所产生的ARP 报文有何不同，为什么？

**Ping 同一局域网内的主机：** 当你ping同一局域网内的主机时，如果目标主机的MAC地址不在发送主机的ARP缓存中，发送主机会发送ARP请求以获取目标主机的MAC地址。

**Ping 局域网外的主机：** 当你ping局域网外的主机时，如果目标主机的IP地址不在发送主机的ARP缓存中，发送主机会发送ARP请求以获取默认网关（路由器）的MAC地址。这是因为在跨子网通信时，通信需要经过默认网关。

**不同之处：**

1. **ARP请求的目标IP地址不同：**

对于局域网内的主机，ARP请求的目标IP地址是所要访问的主机的IP地址。

对于局域网外的主机，ARP请求的目标IP地址是默认网关（路由器）的IP地址。

1. **ARP请求的回应可能不同：**

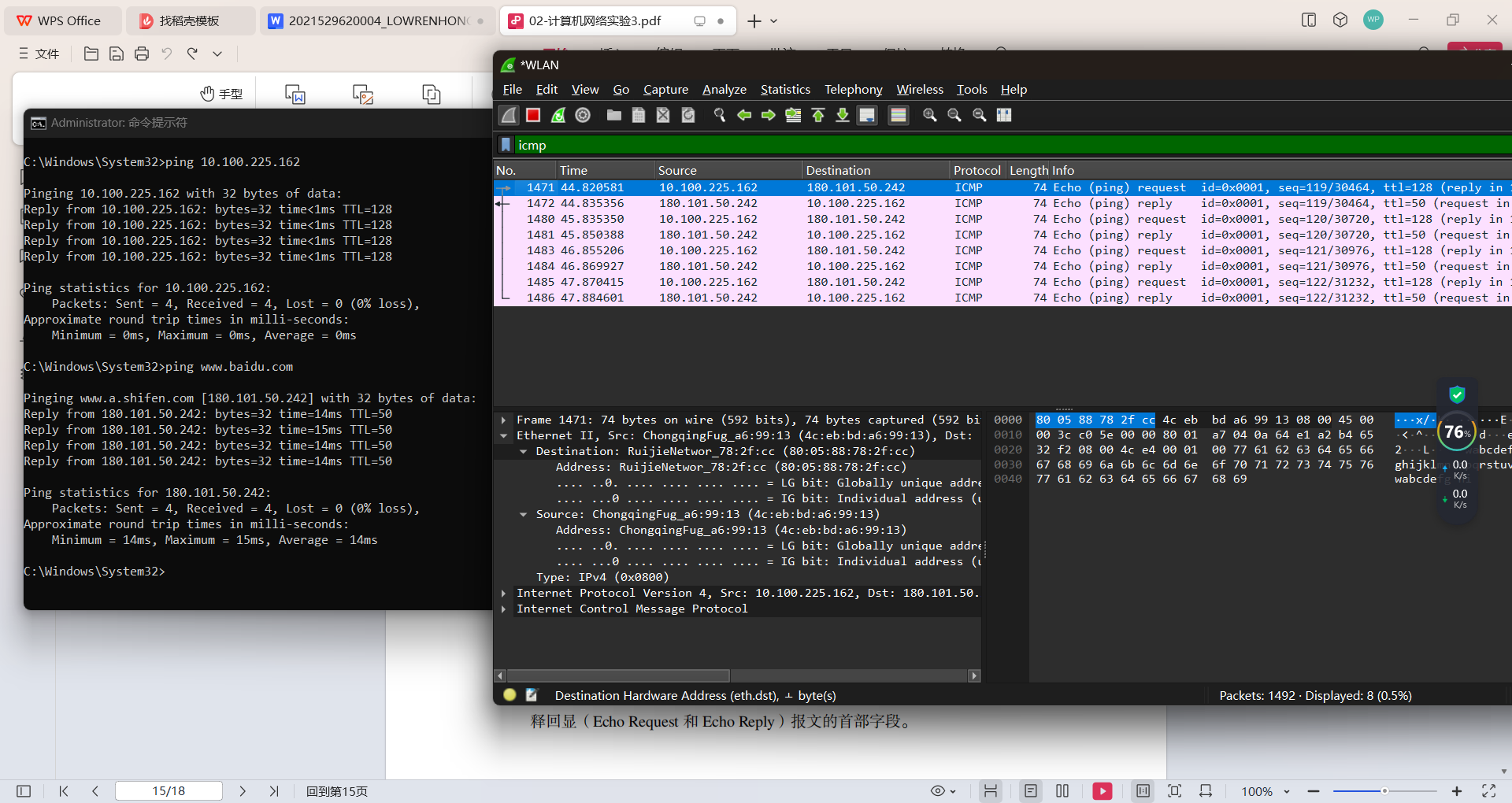
在局域网内，如果目标主机在线且可达，它将回应ARP请求，提供自己的MAC地址。在局域网外，如果默认网关在线且可达，它将回应ARP请求，提供默认网关的MAC地址。这是为了确保跨子网通信经过正确的网关。

**为什么不同：**

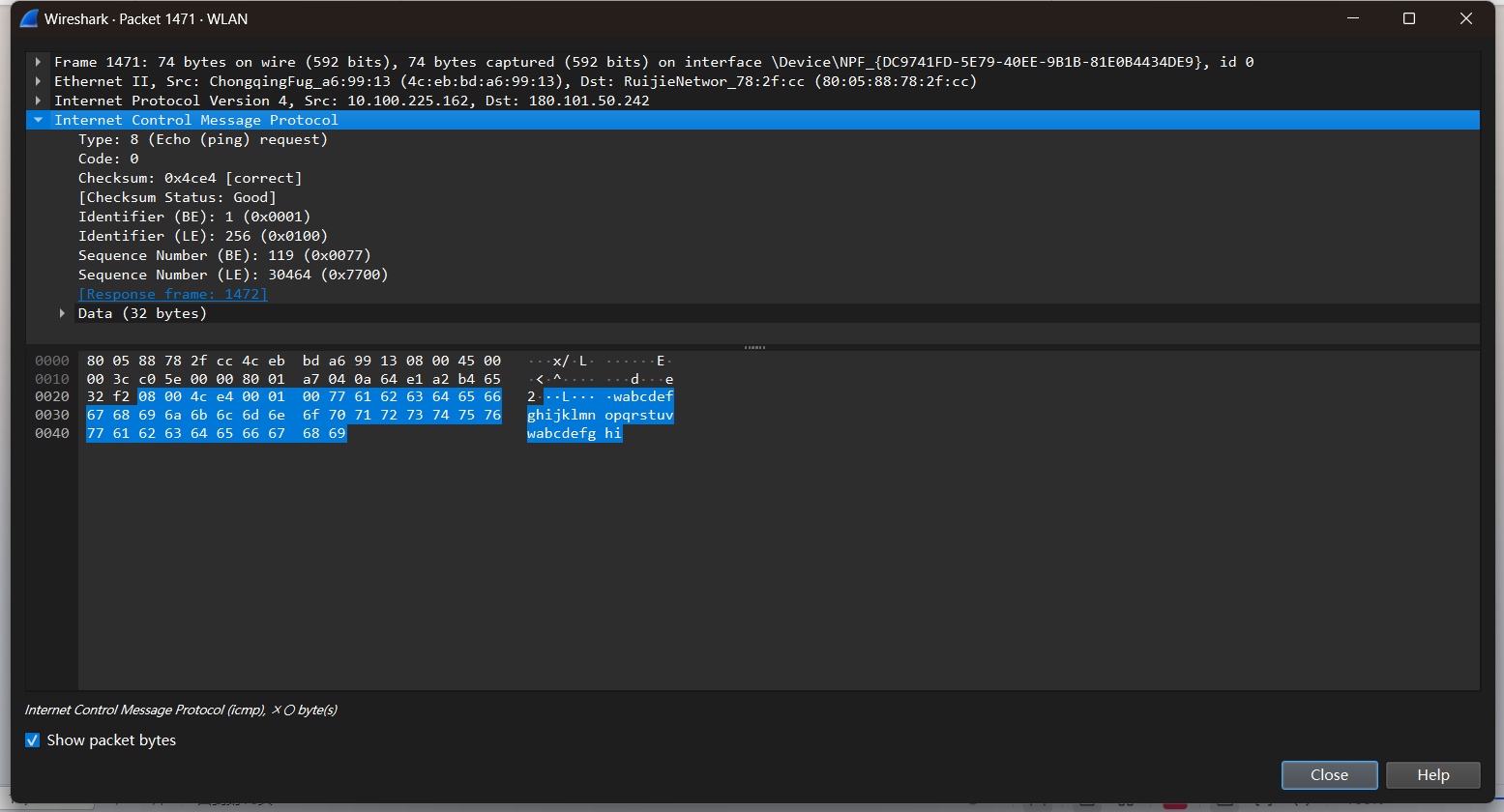
**在局域网内：** 通信直接发生在同一子网上，因此ARP请求的目标直接是目标主机的IP地址，以获取其MAC地址。

**在局域网外：** 通信需要通过路由器（默认网关），因此ARP请求的目标是默认网关的IP地址，以获取默认网关的MAC地址。默认网关将负责将数据包转发到目标主机所在的子网。

* 1. **Ping命令**



Wireshark 监视器



Echo request 示例

**解释回显（Echo Request 和 Echo Reply）报文的首部字段**

**类型字段（Type）：** 占一个字节，用于指示 ICMP 消息的类型。回显请求的类型值通常是 8，而回显回复的类型值通常是 0。

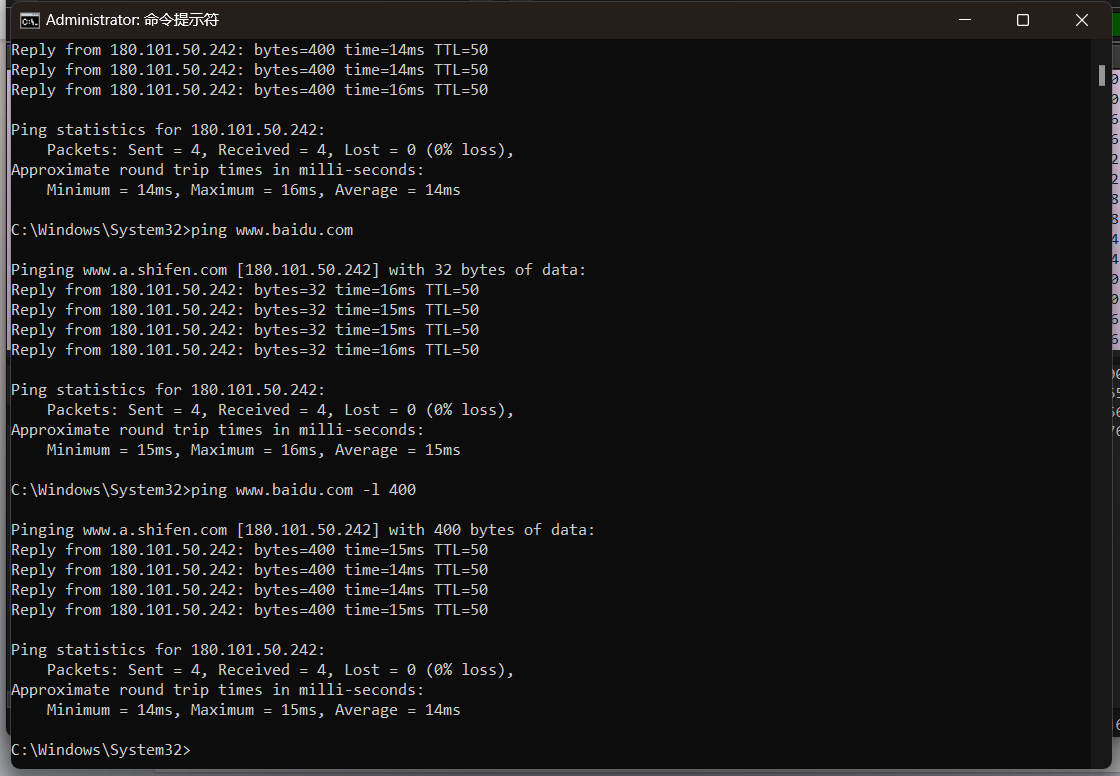
**代码字段（Code）：** 也占一个字节，用于提供关于 ICMP 消息的更多信息。对于回显请求和回显回复，通常是 0。

**校验和字段（Checksum）：** 占两个字节，用于检测 ICMP 报文的错误。校验和字段涵盖了整个 ICMP 报文。

**标识符字段（Identifier）：** 占两个字节，用于在请求和响应之间唯一标识一个 ICMP 会话。

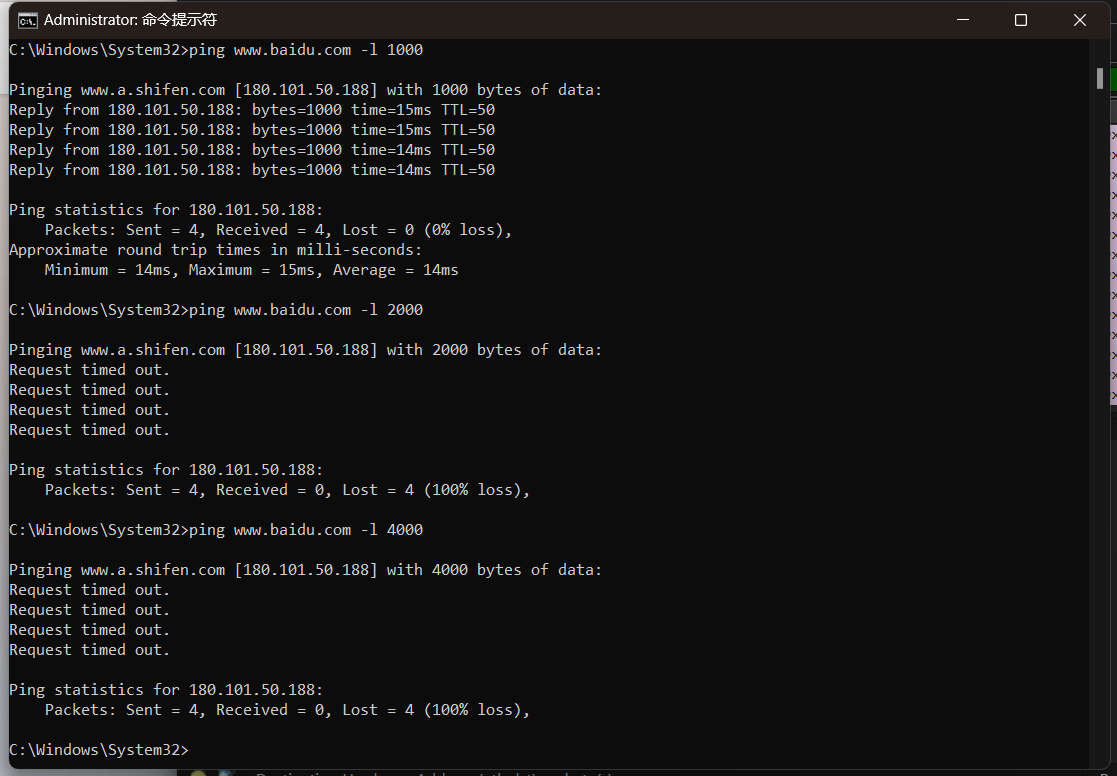
**序列号字段（Sequence Number）：** 占两个字节，表示特定回显请求或回显回复的顺序。

**数据字段（Data）：** ICMP 报文可能包含可变长度的数据字段，其中包括回显请求中的原始数据，以及回显回复中的回显请求的副本。

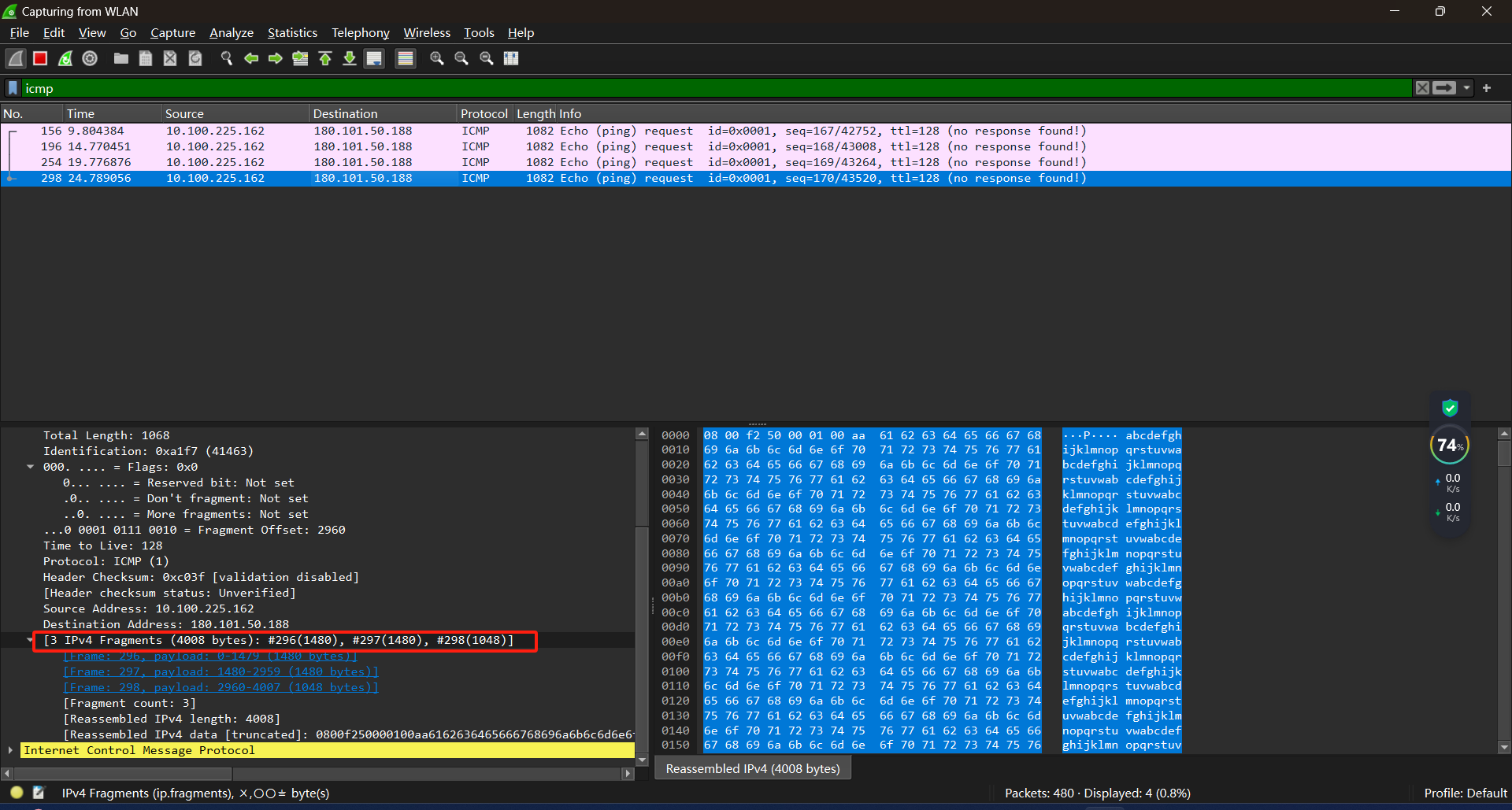


ping IP 地址/域名–l #length

在第一次执行 ping 命令时，使用默认的 32 字节的数据包大小。通常，这是标准的 ICMP Echo Request 数据包大小。在第二次执行 ping 命令时，通过 -l 400 参数指定了更大的数据包大小（400 字节）。这样可以测试网络对较大数据包的响应情况。在两次执行中，网络的可达性都良好，都成功收到了回复。往返时间的差异可能是由于网络状况的轻微波动引起的。



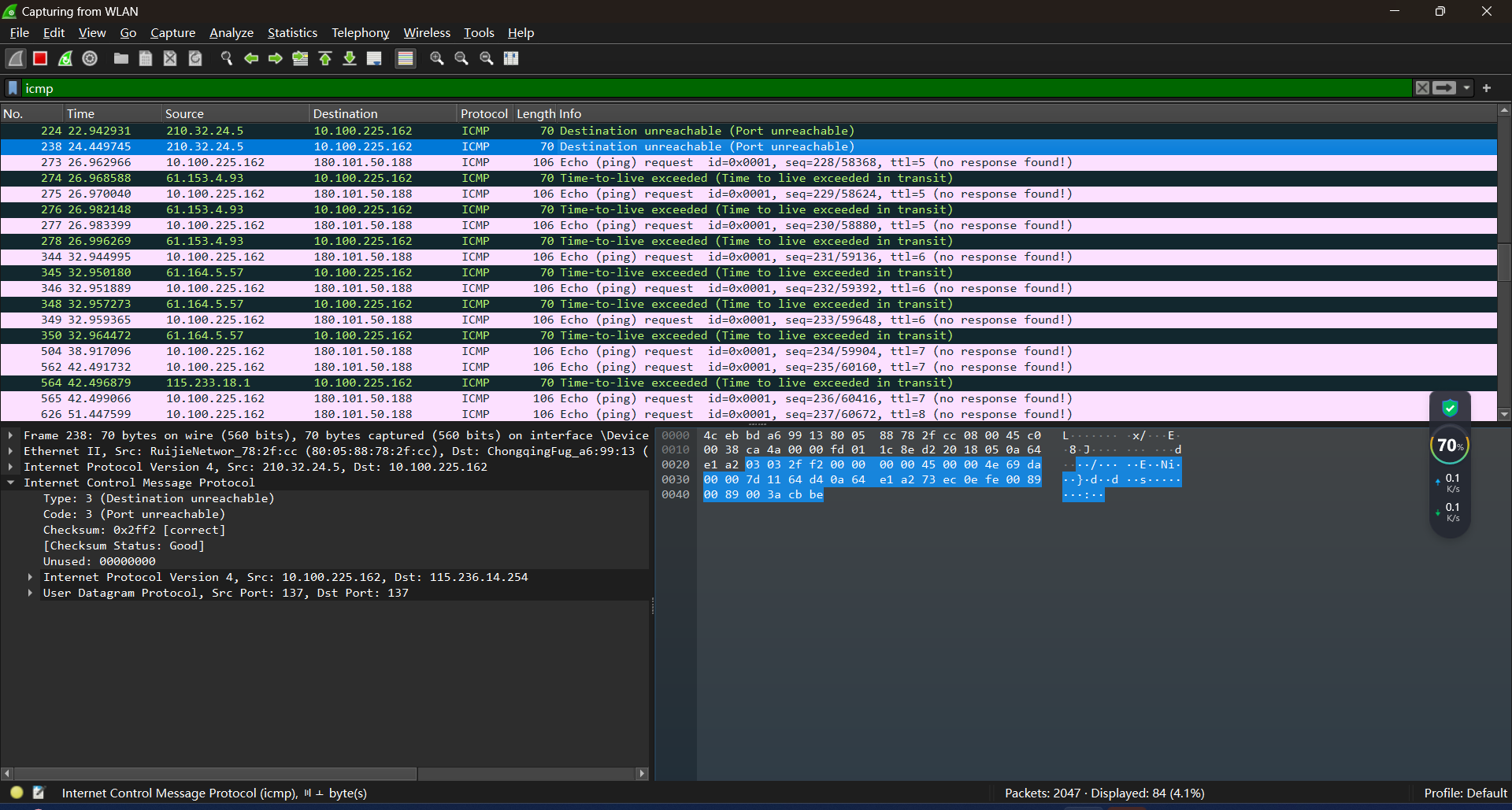
多次改变 #length 的大小



原因： IP 数据报分片的主要原因是为了适应不同网络链路上的 MTU 差异。如果 IP 数据报大小超过某个网络链路的 MTU，就需要分片以确保传输。最后一个分片到4007，因为片位移8字节倍数，4000相当于第4001字节，所以最后一片4007才能分片。以太网的 最大传送单元 MTU 是 1500 字节 ,超过则自动分片，减去IP首部20字节，所以IP数据部 能发1480字节。片位移计算=起点位置/8

具体情况： 数据报何时会分片取决于发送主机到目标主机之间经过的网络链路的 MTU。如果链路上的 MTU 足够大，数据报就不会被分片。如果 MTU 较小，数据报可能会被分片成多个较小的片段。

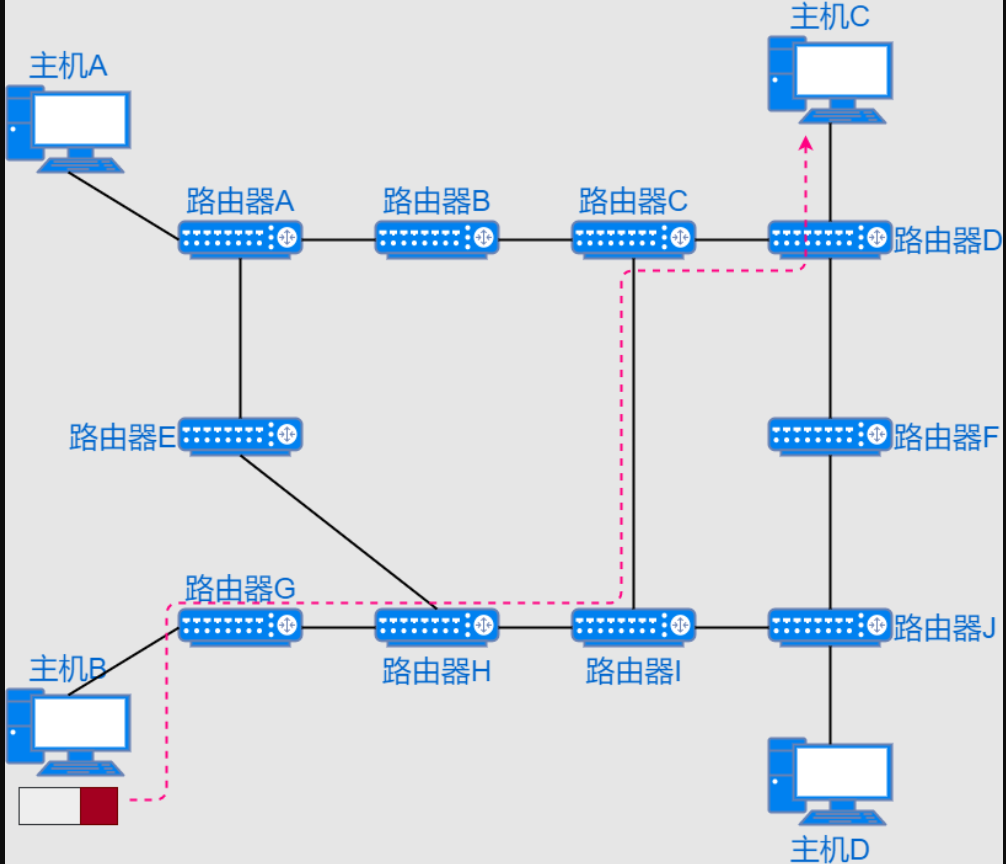
MTU即允许发送不需要分段的最大IP单包字节数。Data-length=MTU-IP头-iCMP头使用ping IP地址/域名–l#length，命令，当length+IP头+ICMP头<=MTU时，包不会被分片否则会被分片发送。



Tracert

这是终点不可达错误类型，代码标号是0 - 15，表示引发终点不可达错误类型的具体错误原因有16种可能，其中标识符和序列号全都用0来填充。

tracert工作原理：首先源主机发起一个 TTL=1 的 ICMP 报文。第一个路由器收到该报文后，TTL减 1 变为 0 并丢弃此报文，返回一个 [ICMP time exceeded] 的消息。源主机通过这个消息获知 IP 数据报转发路径上的第一个路由器信息。然后，依次增加发送ICMP 报文的 TTL 值，可以获取路径上的后续路由器的信息。当到达目的地时，目标主机返回一个 [ICMP port unreachable] 的消息，使发起者确认 IP 数据报已经正常到达。

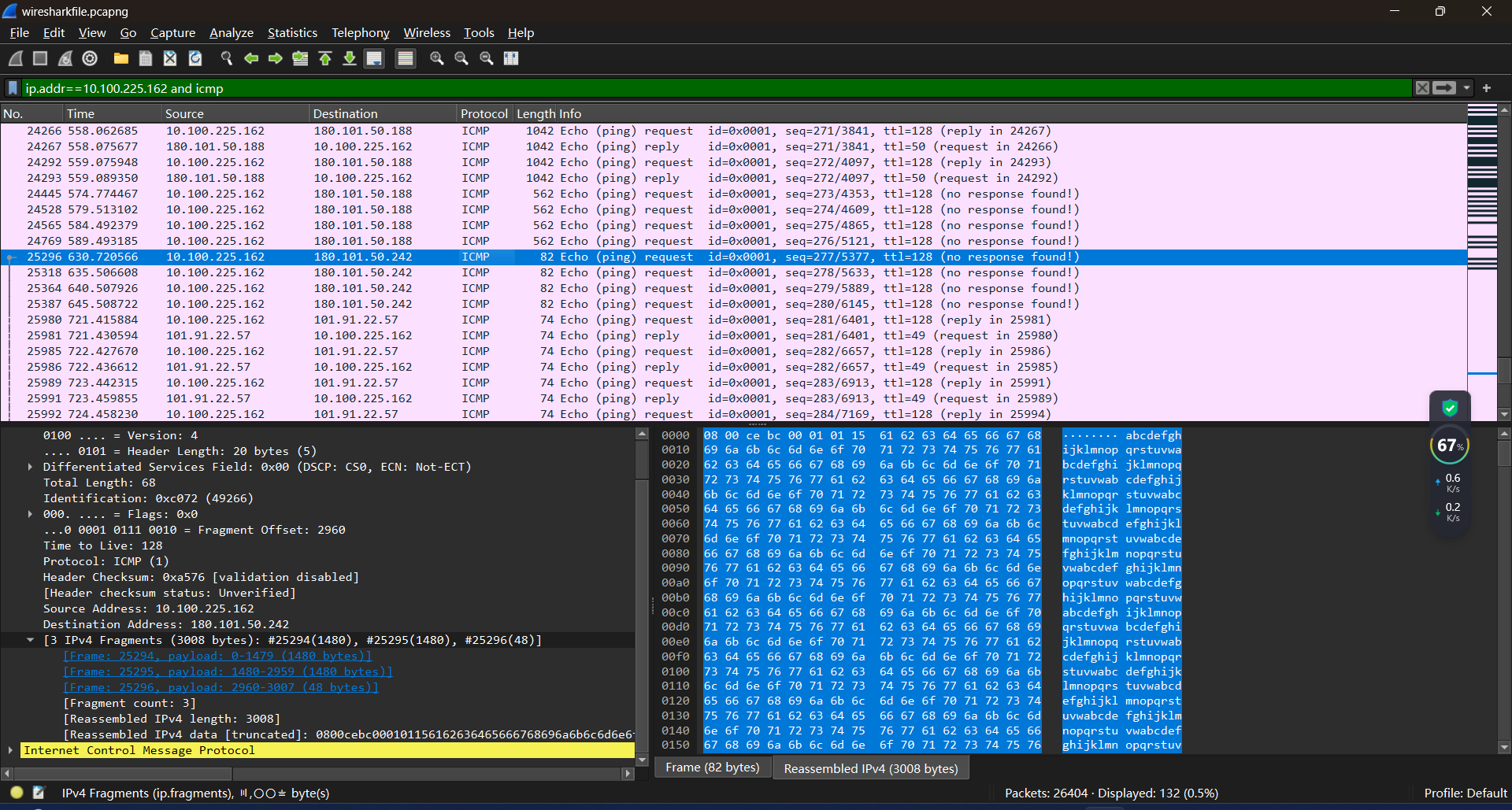


使用 tracert 命令时，源设备的 tracert 逐跳发送数据包，并等待每一个响应报文。发送第一个数据包时，TTL 值设为 1 。第一个路由器收到数据包后 TTL 值减 1 ，随即丢弃数据包，并返回一个 Time Exceeded 消息。源设备的 tracert 收到响应报文后，取出源 IP 地址，即路径上的第一个路由器地址。然后 tracert 发送一个 TTL 值为 2 的数据包。第一个路由器将 TTL 值减 1 ，并转发数据包。第二个路由器再将 TTL 值减 1 ，丢弃数据包并返回一个 Time Exceeded 消息。tracert 收到响应报文后，取出源 IP 地址，即路径上的第二个路由器地址。类似步骤，tracert 逐跳获得每一个路由器的地址，并探测到目的设备的可达性。

1. 实验结论：

*【应给出有效的实验结论，并需含对“网络行为进行分析、模拟和验证，提高解决工程问题的能力和效率”的体会和评价】*

该实验通过Wireshark软件使用进行ARP和IP与ICMP协议分析。通过本次实验对与网络层的协议有了进一步的学习，进行抓包以及分析，使得更理解网络中的各个协议。本次实验，收获颇多，对今后的学习有了较大的帮助。



从该界面可以很清楚看到，和前面捕获到的数据包不同。在该界面的Protocol列，显示了IPv4协议的包。这是因为发送数据包过大，所有是经过了分片后发送。

1480=1514-14-20(以太网侦大小-数据链路层头部-IP头部)

48=88-14-25-1(帧尾）