**21级计算机科学与技术2班**

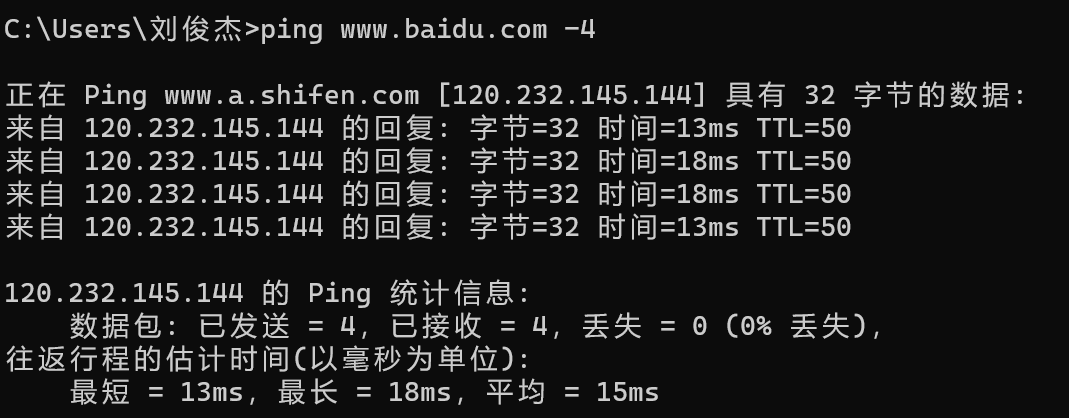
**计算机网络 实验七**

## **实验7.1TCP/IP 协议分析**

**(1)捕获一段IP数据包，分析报头的结构**

**打开wireshark进行抓包，同时在命令行输入ping [www.baidu.com](http://www.baidu.com) -4，**

**将其显示www.baidu.com的Ipv4地址**

****

**可以看到www.baidu.com的IP地址为120.232.145.144**

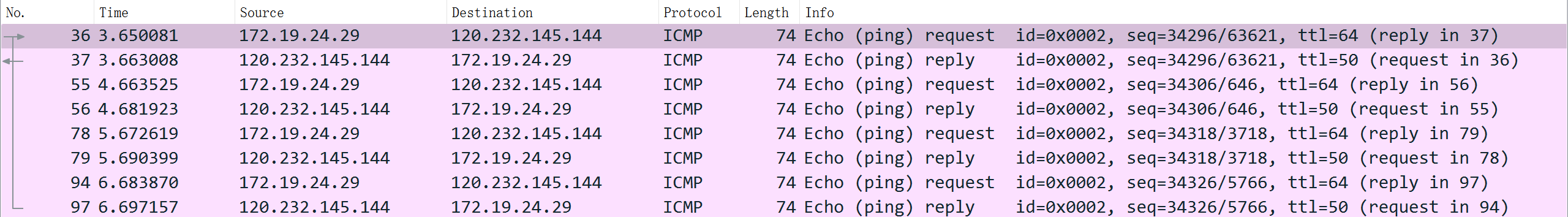
**停止wireshark抓包,将wireshark过滤选项设置为:**

****

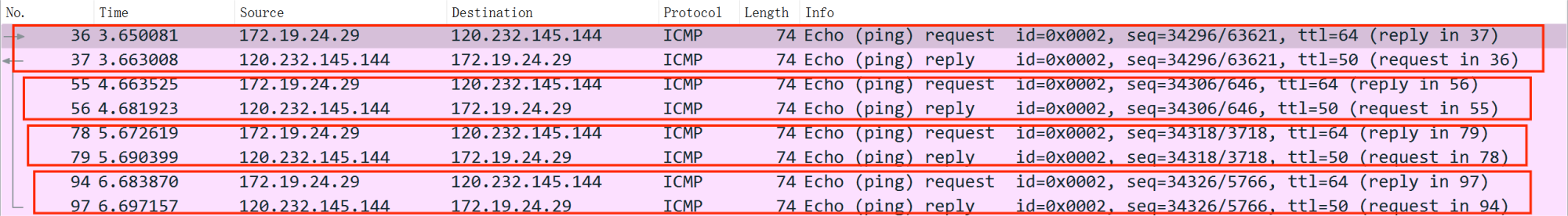
**或者:**

****

**抓取数据包的信息如下图所示:**

****

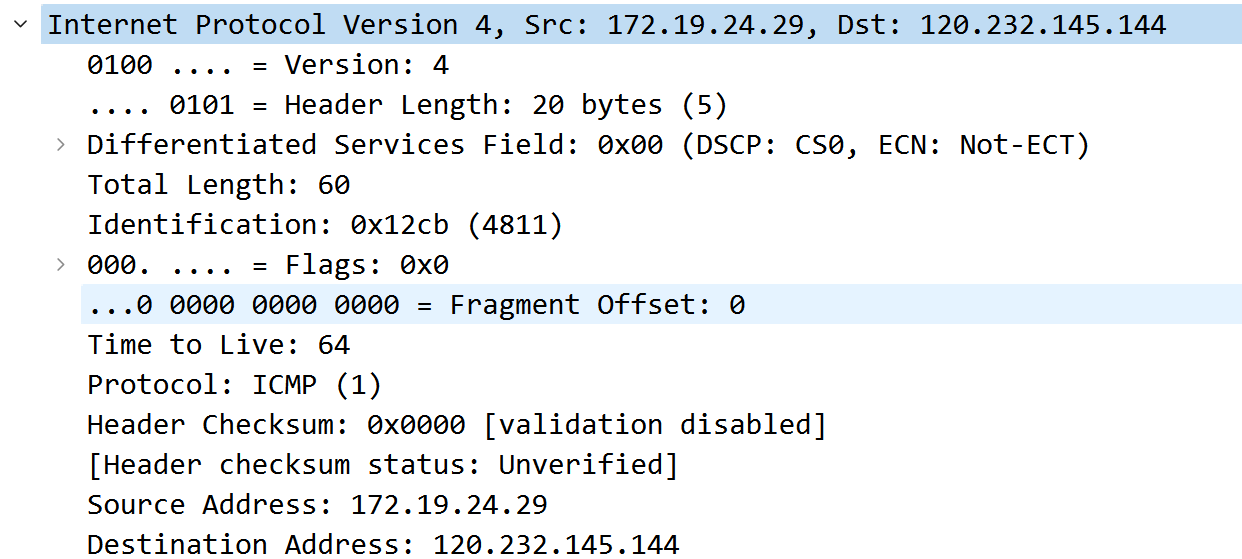
**可以看到一共有8条ICMP报文，有四对ICMP请求和回复报文：**

****

**截图可见ICMP 的请求(Echo)和回应(Echo reply)**

**分析序号为36的 Echo数据包:**

**展开数据包:**

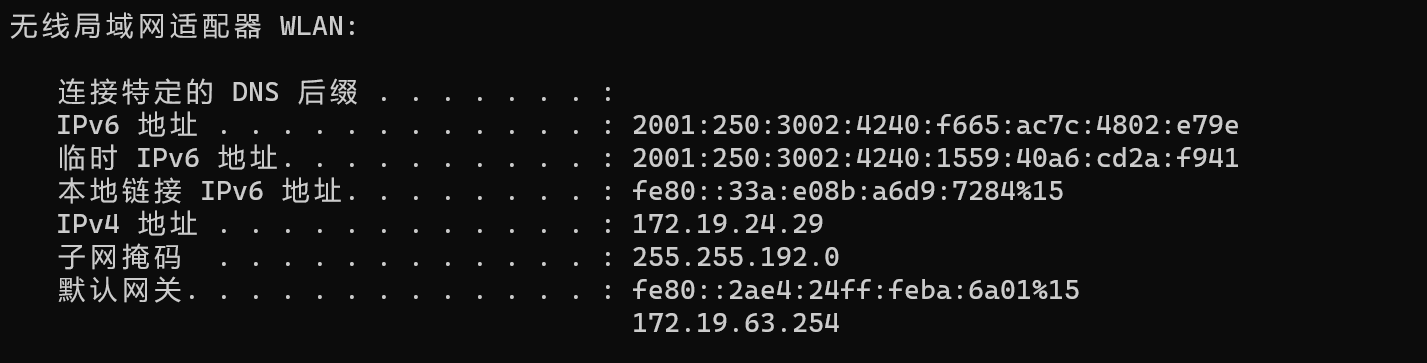
****

**分析:**

|  |  |  |
| --- | --- | --- |
| **报文结构** | **报文内容** | **作用** |
| **版本** | **0100** | **表示当前网络IP协议的版本是IPV4** |
| **首部结构** | **0101** | **表示IP报头长度,这里是20 bytes (5)。** |
| **区分服务** | **0x00** | **表示当前IP数据包中是否使用服务类型字段,表示0x00表示DSCP（差异化服务代码点）为CS0，ECN（拥塞通告）位没有设置。** |
| **总长度** | **60** | **表示该数据总长，该IP数据包总长度为60字节** |
| **标识** | **0x12cb(4811)** | **表示该数据标识，也是唯一标识** |
| **标志** | **0x0** | **表示该数据报能被分段，0x0表示没有设置标志** |
| **片偏移** | **0** | **表示该分段偏移量** |
| **生存时间** | **64** | **表示该数据报最多可以经过64个路由** |
| **协议** | **ICMP(1)** | **代表ICMP协议** |
| **检验和** | **0x000** | **表示该数据是完整的** |
| **源IP地址** | **172.19.24.29** | **本机IP地址** |
| **目的IP地址** | **120.232.145.144** | **目的机IP地址** |
| **选项** | **\** | **\** |

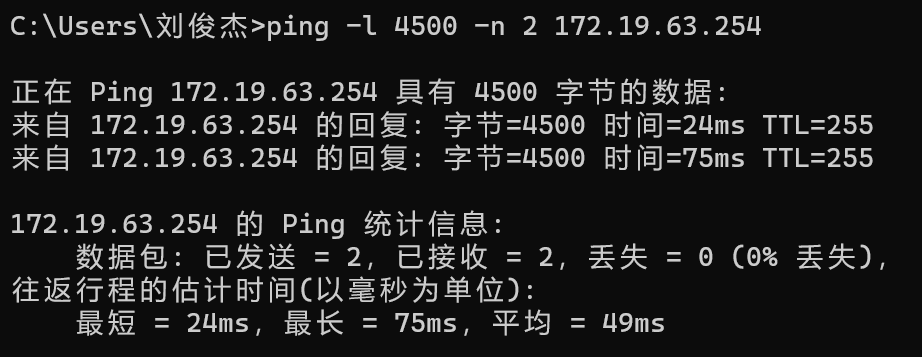
**(2)在命令窗口中 ping本地一个IP地址**

**通过ipconfig查询网关信息:**

****

**可以看到默认网关的IP地址为172.19.63.254**

**在命令行输入ping -l 4500 -n 2 172.19.63.254**

****

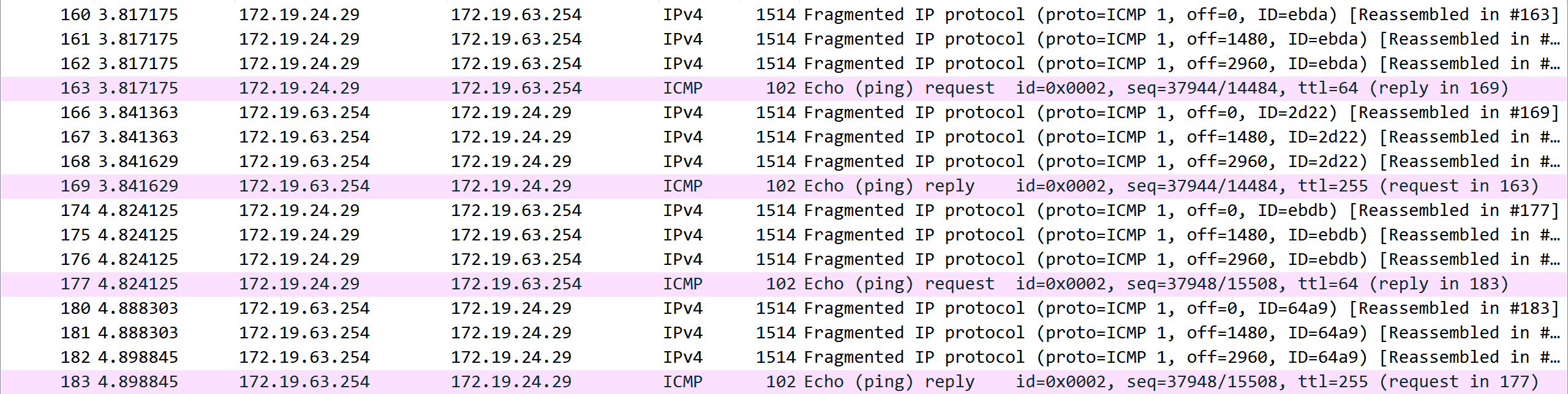
**Ping 的用法:**

**ping -n：跟无参数ping一个样。在默认情况下无参数ping一般都是只发送四个32字节数据包，-n的话可以指定发送多少数据包，通过这个命令从数据包返回的最短时间、最长时间、平均时间可以衡量网络速度、延迟，从丢失率可以衡量网络的稳定性。**

**ping -l：发送size指定大小的到目标主机的数据包。**

**ping -l 4500 -n 2 172.19.63.254 表示向默认网关发送2个size=4500的数据包**

**wireshark抓到的数据包为:**

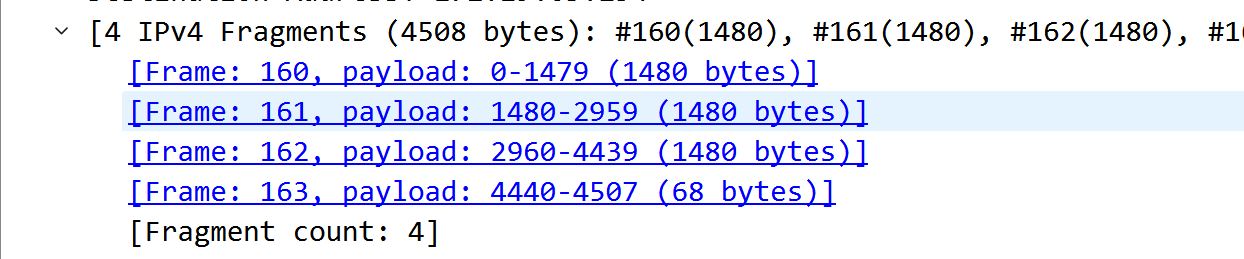
****

**可以看到两个请求的数据包和两个回复的数据报**

**回答:**

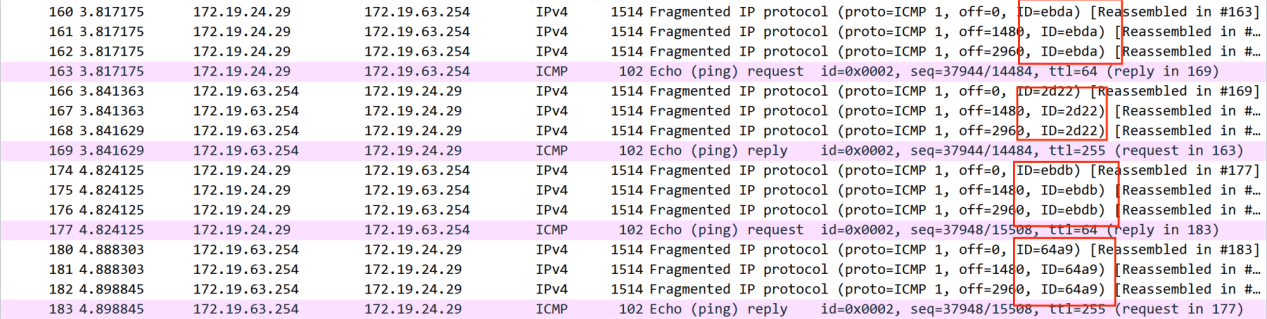
**①以太网的MTU是多少?**

**展开序号为163的ICMP数据报信息:**

****

**可以看到数据报被分为4段，分别为1480、1480、1480和68字节，所以可以看出以太网链路上一个报文最多可以经过的报文大小为1480字节，故以太网的MTU为1480字节。**

**②分析捕获的报文,找出属于同一ICMP 请求报文的分片,发起端发送的ICMP 请求报文分成了几个分片?**

****

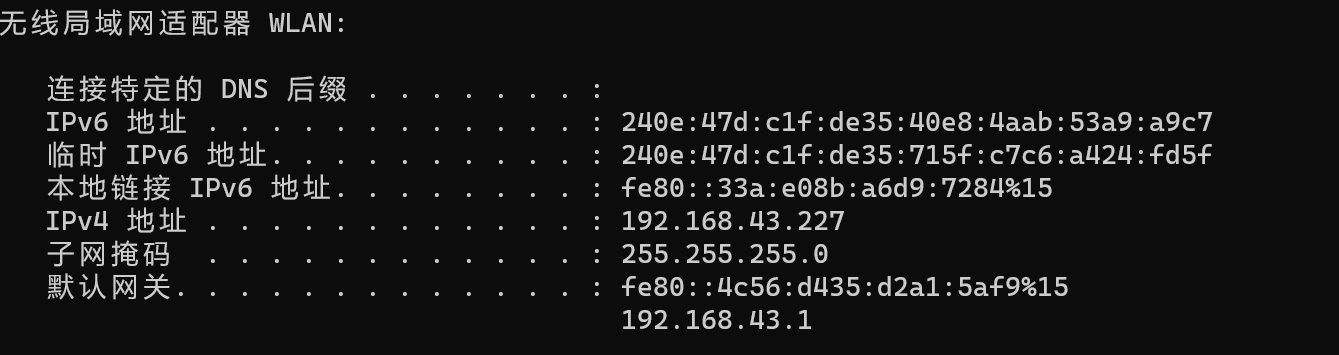
**ID号相同的IPv4报文属于一个ICMP请求的分段 ，所以发起端发送的ICMP 请求报文分成了4个分片。**

**③若要让 ping发起端发送的数据分为3个分片则 ping命令中的报文长度应为多大?**

**若想要ping发起端发送的数据分为3个分片，则ping命令中报文长度应该设置为2\*1480+1到3\*1480字节之间，即2961到4360字节之间。**

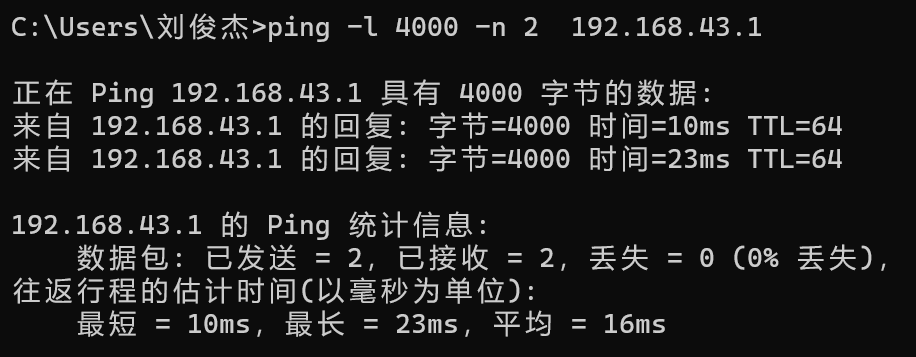
**现在ping发送的数据报的大小为4000字节，来实验是否是分成了3个分片:**

**重新查询网关IP:**

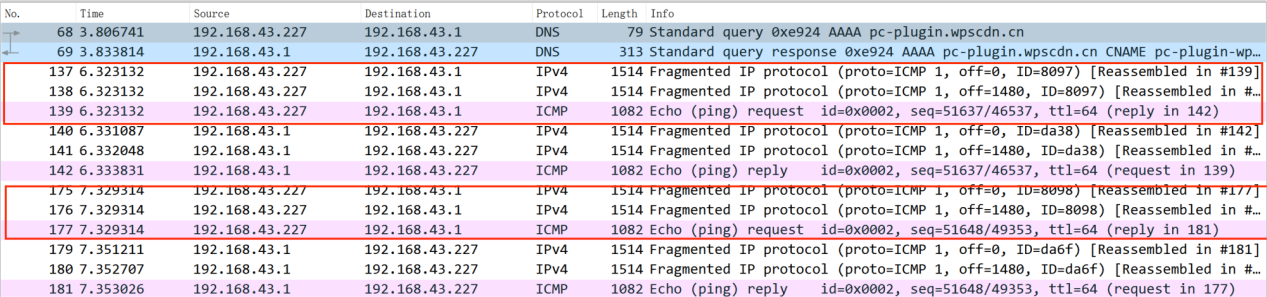
****

**网关IP:192.168.43.1**

**在命令行输入ping -l 4000 -n 2 192.168.43.1**

****

**抓取到的数据报文:**

****

**可以看到ping发起端发送的数据分为3个分片**

**实验7.2 UDP/IP 协议分析**

**【目的】 利用wireshark 分析 UDP的IP数据包服务；**

**【要求】**

**1）启动wireshark 抓包,设置过滤显示UDP相关的信息；**

**2） 运行命令 traceroute 命令（windows 的是 tracert）**

**Tracert www.ucdavis.edu**

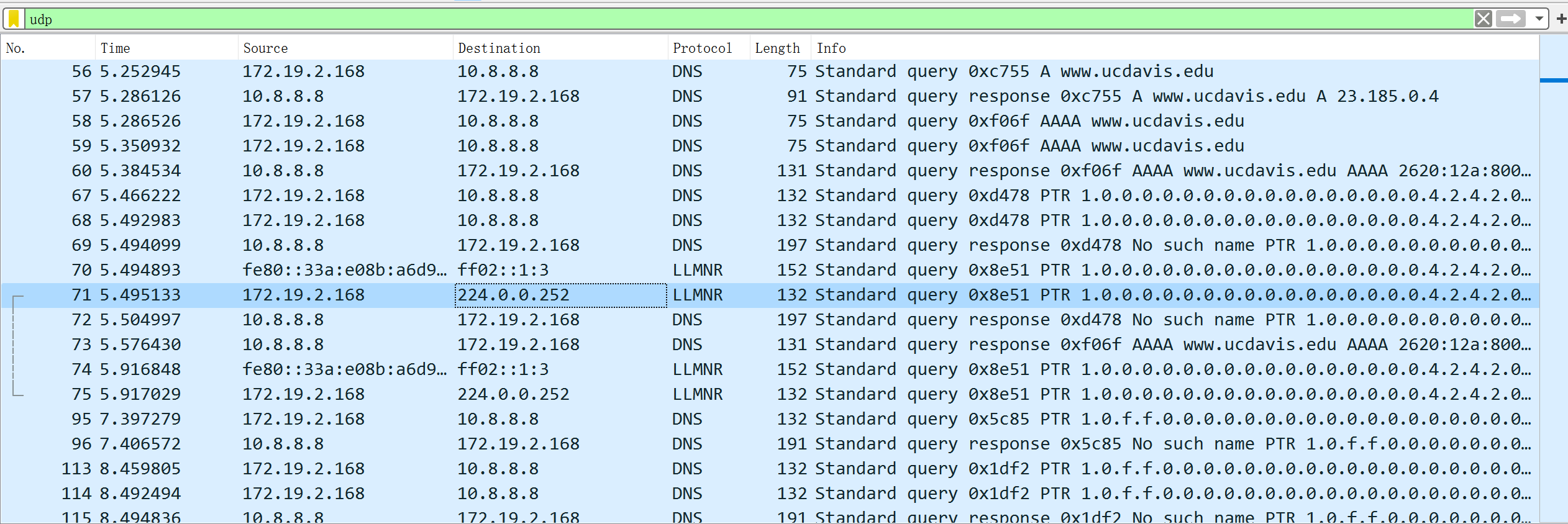
**3） 截图显示网络层（IP）、传输层及UDP 相关的信息；观察期间数据传输；**

**4） 分析并解释以上实验结果，分析IP数据包的内容。**

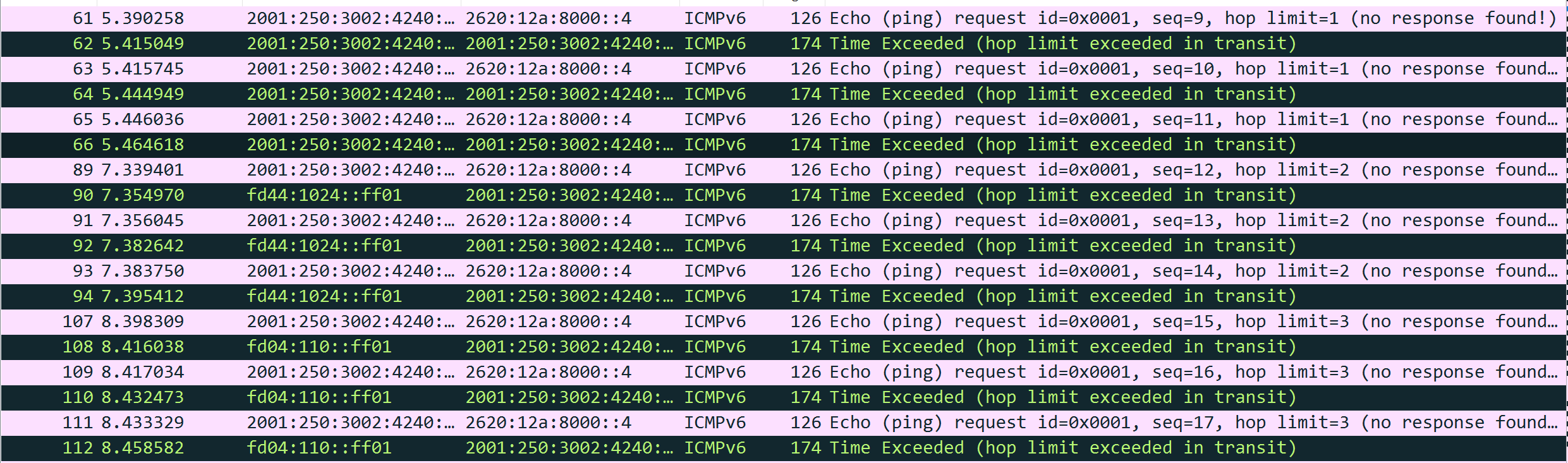
**在命令行运行Tracert www.ucdavis.edu**

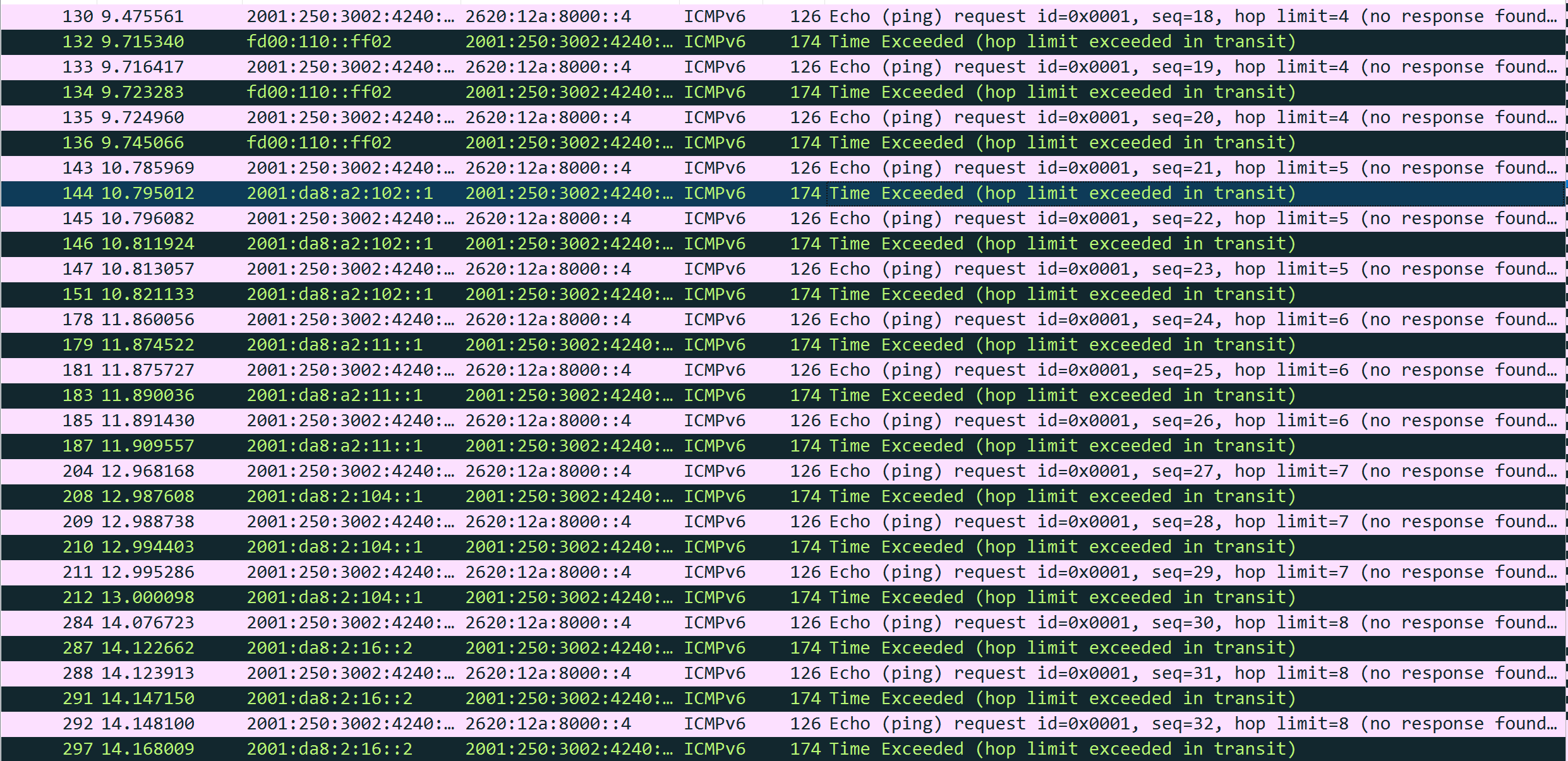
## 

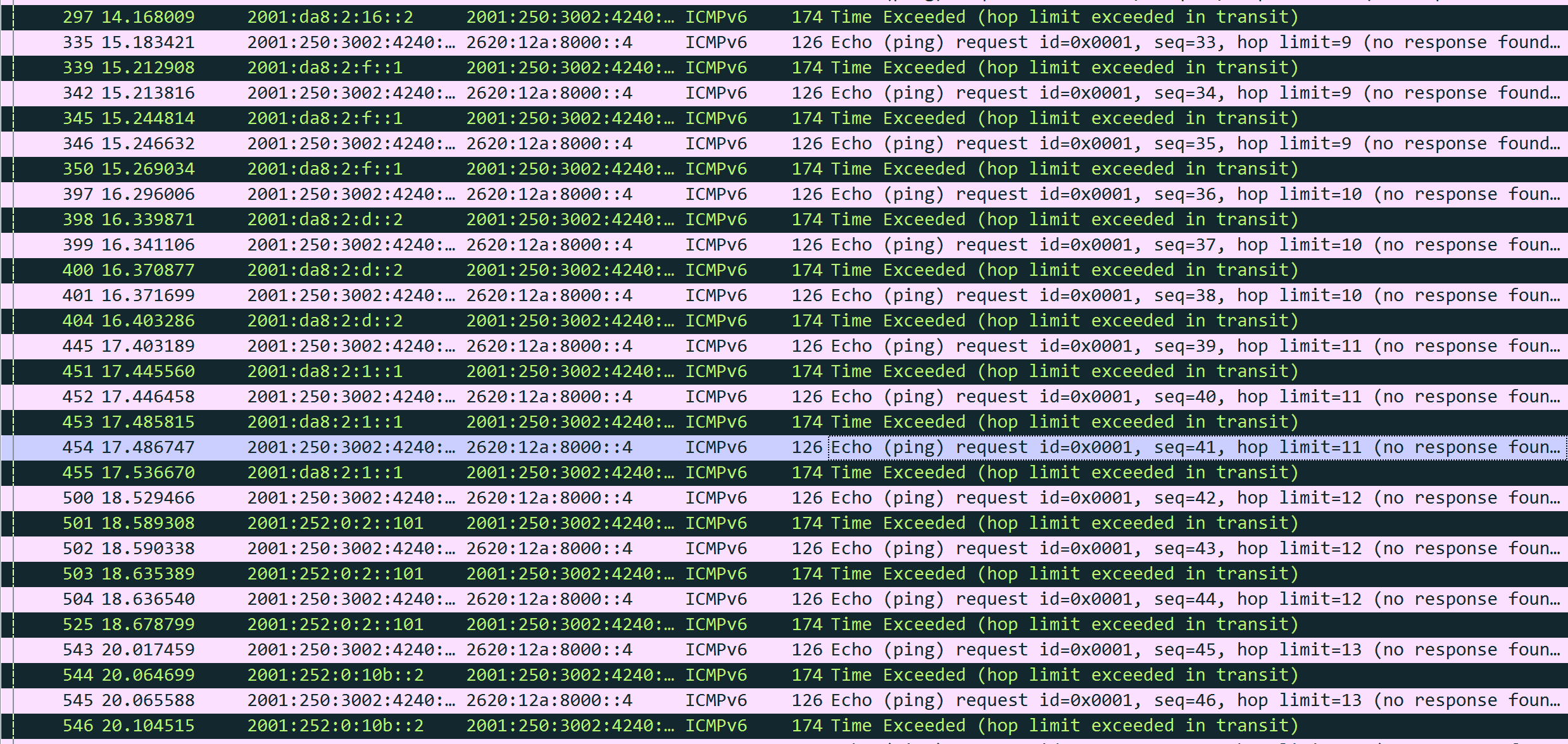
**查看wireshark抓到的数据包:**

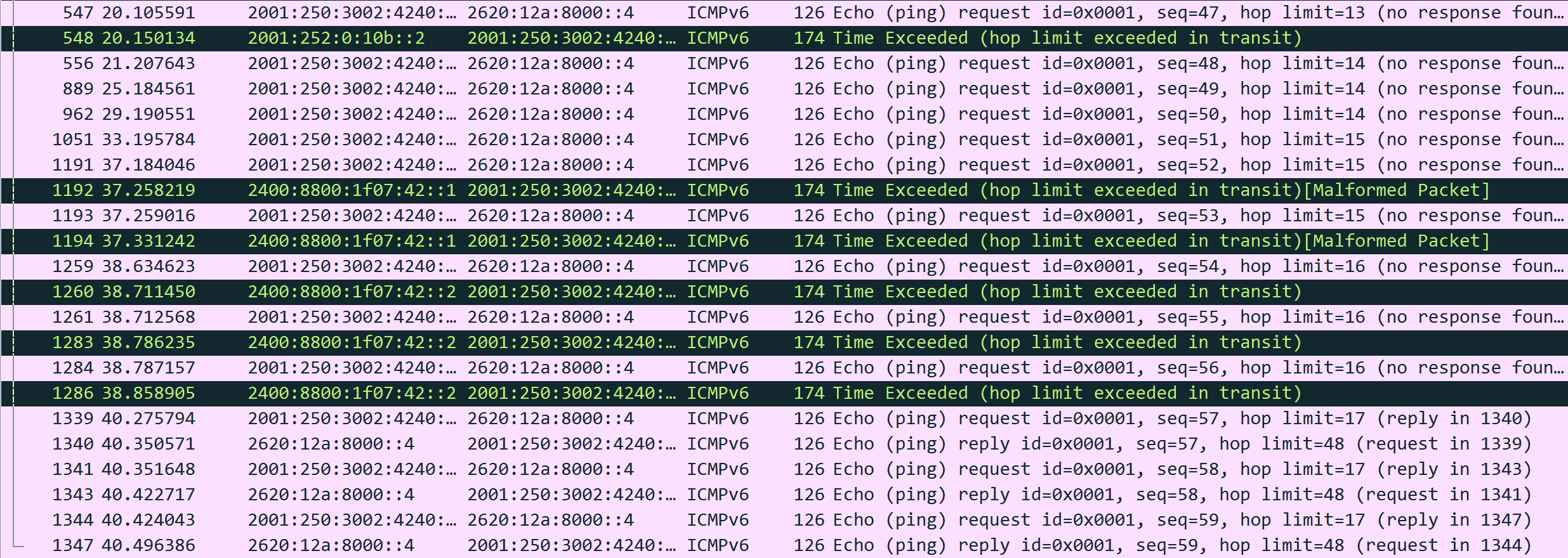
****

**可以看到没有IP数据包，这是因为windows的tracert使用的是icmp协议，所以我们将过滤信息改为ipv6.addr==2620:12a:8000::4，查看数据包:**

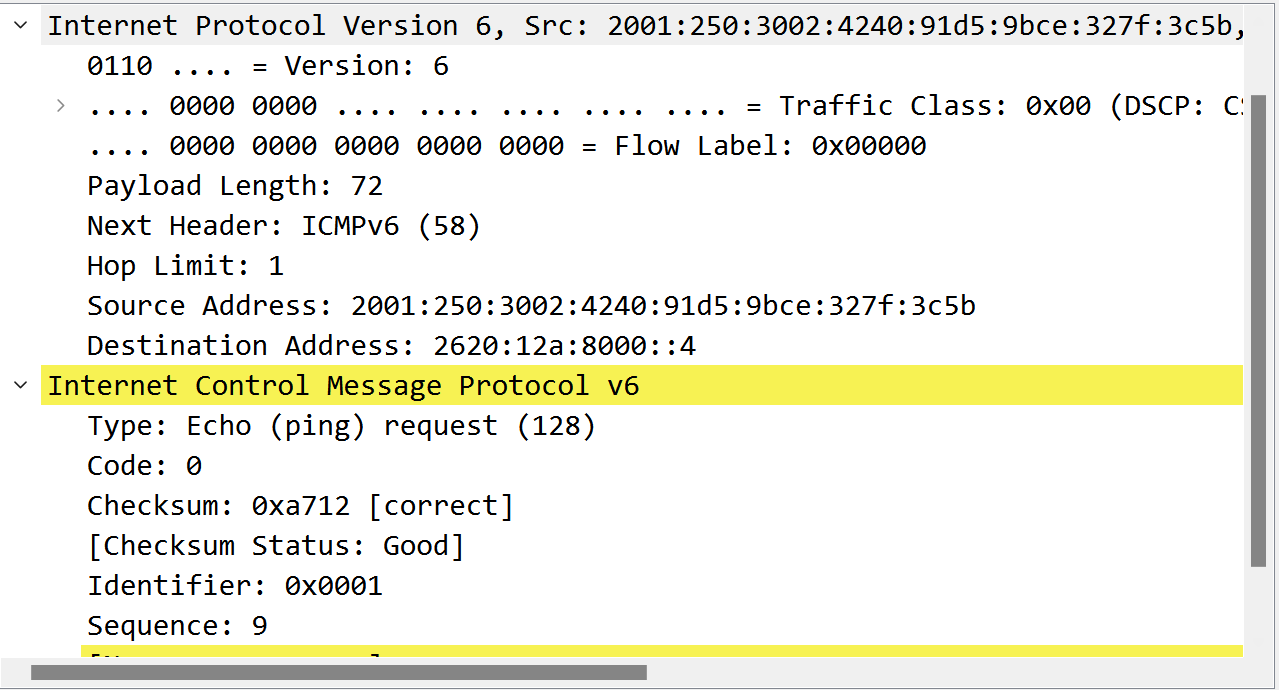
****

****

****

****

**分析序号为61的IP数据包:**

****

**这是一个捕获到的 ICMPv6 Echo 请求（ping）数据包:**

**协议（Protocol）: 数据包使用的协议类型，这里是 "ICMPv6"，表示IPv6的ICMP协议。**

**长度（Length）: 数据包的长度，这里是 "126" 字节。**

**ICMPv6类型（ICMPv6 Type）: 这是ICMPv6消息的类型字段，这里是 "Echo (ping) request"，表示这是一个Echo请求，用于测试网络连通性。**

**ID（id）: 这是Echo请求中的标识符字段，这里是 "0x0001"。**

**Sequence（seq）: 这是Echo请求中的序列号字段，这里是 "9"。**

**Hop Limit: 这是IPv6数据包的跳数限制（Hop Limit），也就是IPv4中的TTL（Time to Live）。在这个数据包中，跳数限制为 "1"，表示数据包只能在一跳内传播，因此在本例中没有找到响应（no response found!）。**

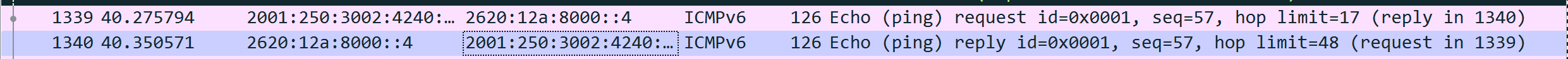
**所以有:**

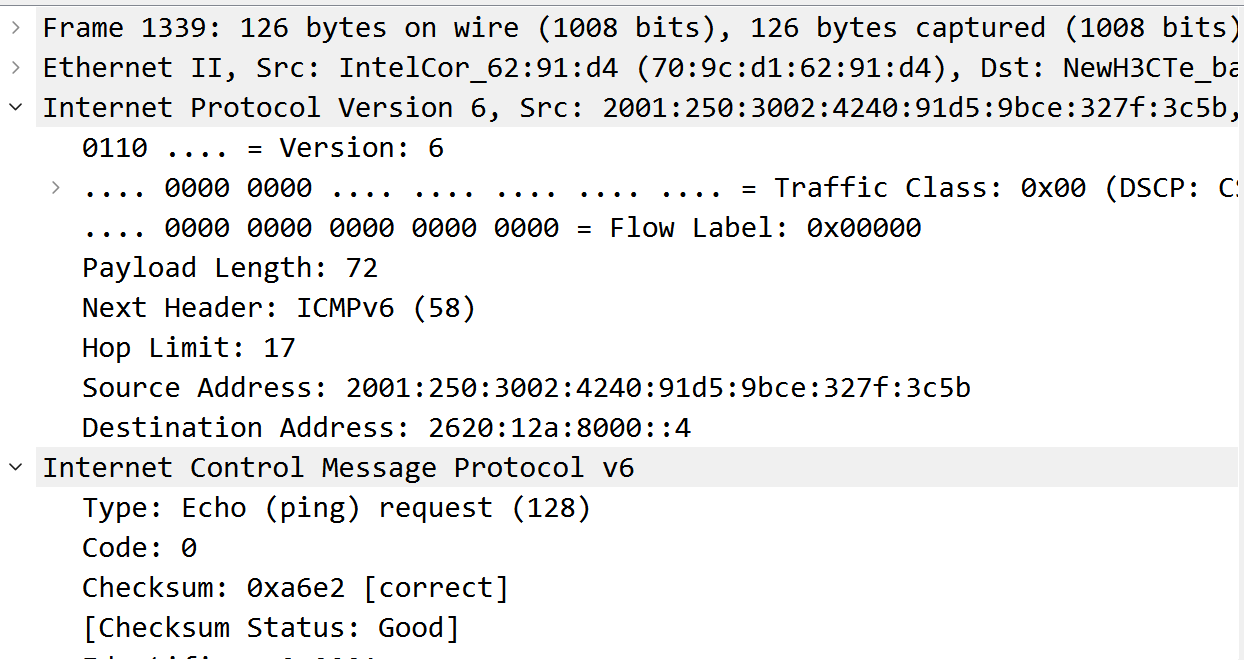
****

**跳数限制（Hop Limit）被超出。如果数据包在传输过程中经过了太多的路由跳数，跳数限制会被减小，当它达到0时，路由器将丢弃数据包并发送一个Time Exceeded错误消息。**

**这个数据包是一个IPv6网络中的ICMPv6 Echo请求，通常用于测试目标主机的可达性和响应时间。在这个示例中，数据包从源IPv6地址发送到目标IPv6地址，请求一个Echo回应。跳数限制为1，所以数据包未在网络中传播太远。如果网络中的目标主机能够响应，它将发送一个Echo回应以确认其可达性。**

**分析以下2个数据包:**

****

****

**1339数据包是一个捕获到的 ICMPv6 Echo 请求（ping）:**

**协议（Protocol）: 数据包使用的协议类型，这里是 "ICMPv6"，表示IPv6的ICMP协议。**

**长度（Length）: 数据包的长度，这里是 "126" 字节。**

**ICMPv6类型（ICMPv6 Type）: 这是ICMPv6消息的类型字段，这里是 "Echo (ping) request"，表示这是一个Echo请求，用于测试网络连通性。**

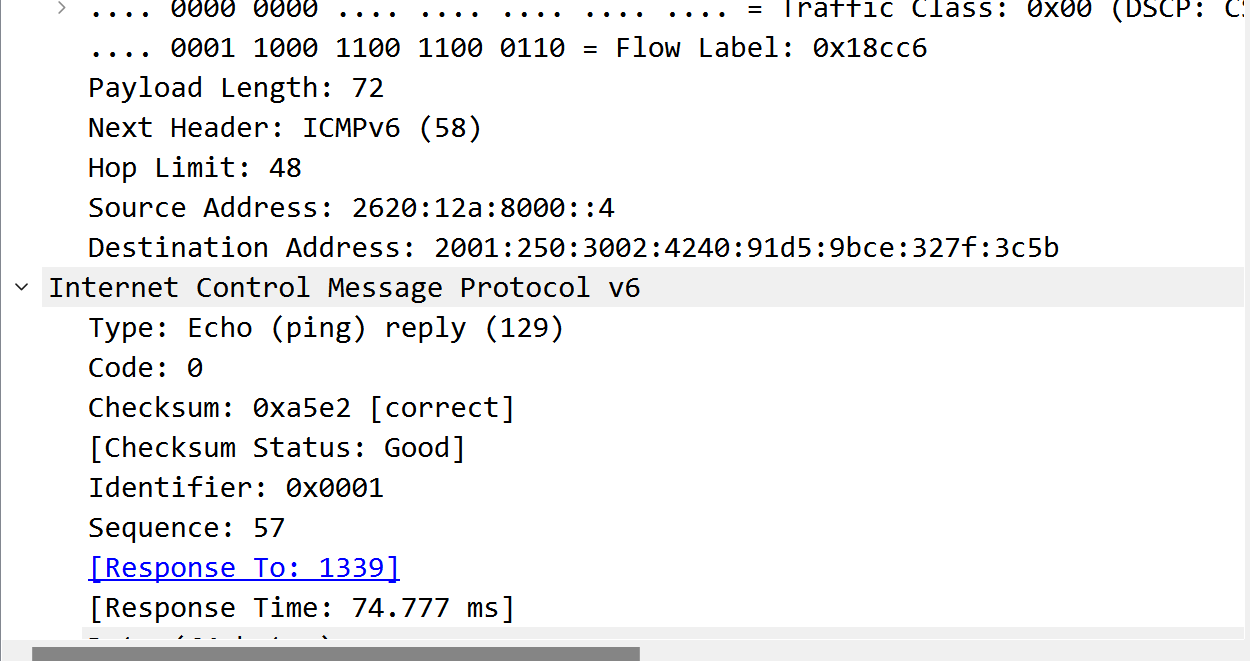
**ID（id）: 这是Echo请求中的标识符字段，这里是 "0x0001"。**

**Sequence（seq）: 这是Echo请求中的序列号字段，这里是 "57"。**

**Hop Limit: 这是IPv6数据包的跳数限制（Hop Limit），也就是IPv4中的TTL（Time to Live）。在这个数据包中，跳数限制为 "17"。**

**回复时间（reply in 1340）: 这是一个注释，指示在 1340 毫秒后可能会有Echo回应。它表示等待Echo回应的时间。**

**这个数据包是一个IPv6网络中的ICMPv6 Echo请求，通常用于测试目标主机的可达性和响应时间。数据包从源IPv6地址发送到目标IPv6地址，请求一个Echo回应。跳数限制为17，表示数据包可以在网络中传播到多达17个路由跳数的地方。**

****

**1340数据包是一个捕获到的 ICMPv6 Echo 回应（ping reply）数据包：**

**协议（Protocol）: 数据包使用的协议类型，这里是 "ICMPv6"，表示IPv6的ICMP协议。**

**长度（Length）: 数据包的长度，这里是 "126" 字节。**

**ICMPv6类型（ICMPv6 Type）: 这是ICMPv6消息的类型字段，这里是 "Echo (ping) reply"，表示这是Echo回应，用于确认网络连通性。**

**ID（id）: 这是Echo回应中的标识符字段，这里是 "0x0001"，与之前的Echo请求相匹配。**

**Sequence（seq）: 这是Echo回应中的序列号字段，这里是 "57"，与之前的Echo请求相匹配。**

**Hop Limit: 这是IPv6数据包的跳数限制（Hop Limit），也就是IPv4中的TTL（Time to Live）。在这个数据包中，跳数限制为 "48"，表示数据包可以在网络中传播到多达48个路由跳数的地方。**

**这个数据包是一个IPv6网络中的ICMPv6 Echo回应，它是对之前的Echo请求的响应。在Echo请求中，跳数限制为17，而在回应中，跳数限制为48，这表示数据包在网络中经过了更多的路由跳数。这个Echo回应确认了目标主机的可达性，并提供了响应时间等信息。这两个数据包一起构成了一次完整的Ping测试，用于测试网络的连通性和性能。**