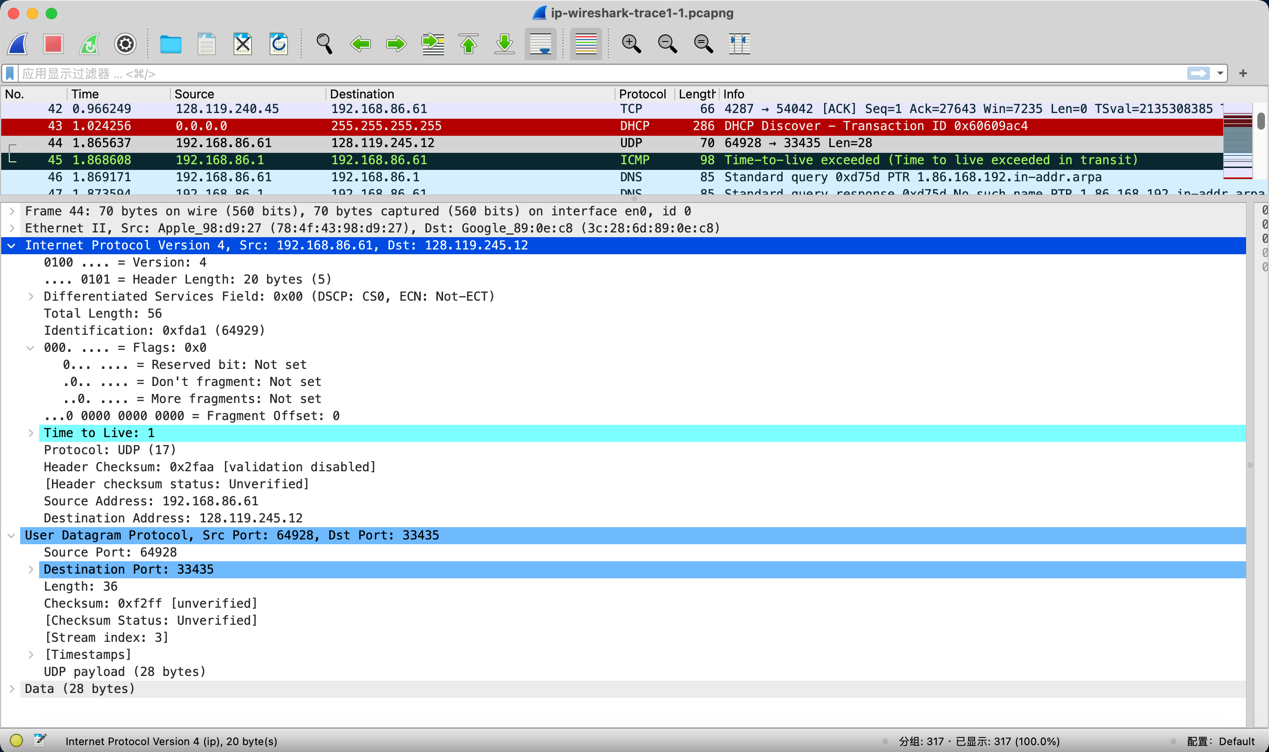
**Lab3实验报告**

**本次lab均使用官方提供的数据包**

**一、IP**

**Part1：Basic IPv4**

****

**1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. (Hint: this is 44th packet in the trace file in the ipwireshark-trace1-1.pcapng file in footnote 2). Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?**

**答案：计算机的IP地址是192.168.86.61。**

**2. What is the value in the time-to-live (TTL) field in this IPv4 datagram’s header?**

**答案：TTL字段的值是1。**

**3. What is the value in the upper layer protocol field in this IPv4 datagram’s header?[Note: the answers for Linux/MacOS differ from Windows here].**

**答案：上层协议字段的值是UDP，对应协议号17。**

**4. How many bytes are in the IP header?**

**答案：IP头部有20字节。**

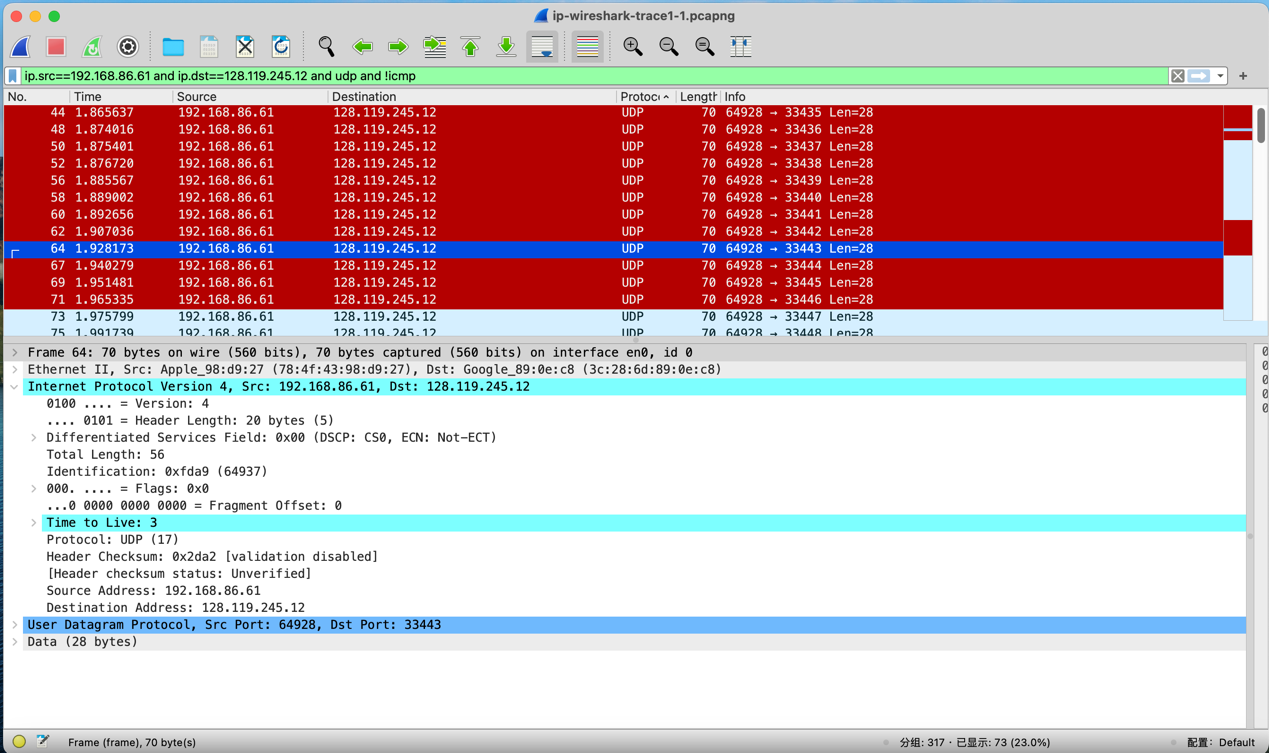
**5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.**

**答案：IP数据报的有效载荷有28字节。这是通过直接查看UDP payload或是UDP段的长度字段（36字节）并减去UDP头部长度（8字节）得到的。**

**6. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**

**答案：IP数据报的标志字段中的"不分段"标志位被设置为未设置（0），表示这个IP数据报没有被分段。**

**（就截一张，其他类似的滑动查看）**

****

**7. Which fields in the IP datagram always change from one datagram to the next within this series of UDP segments sent by your computer destined to 128.119.245.12, via traceroute? Why?**

**答案：UDP包中, TTL每三个增长一次； Identification顺序增长, 因为Identification相同的报文表示同一报文的拷贝或不同分片, 因此需要增长来区分；校验和Header Checksum也一直在变，因为每个UDP段都不同。**

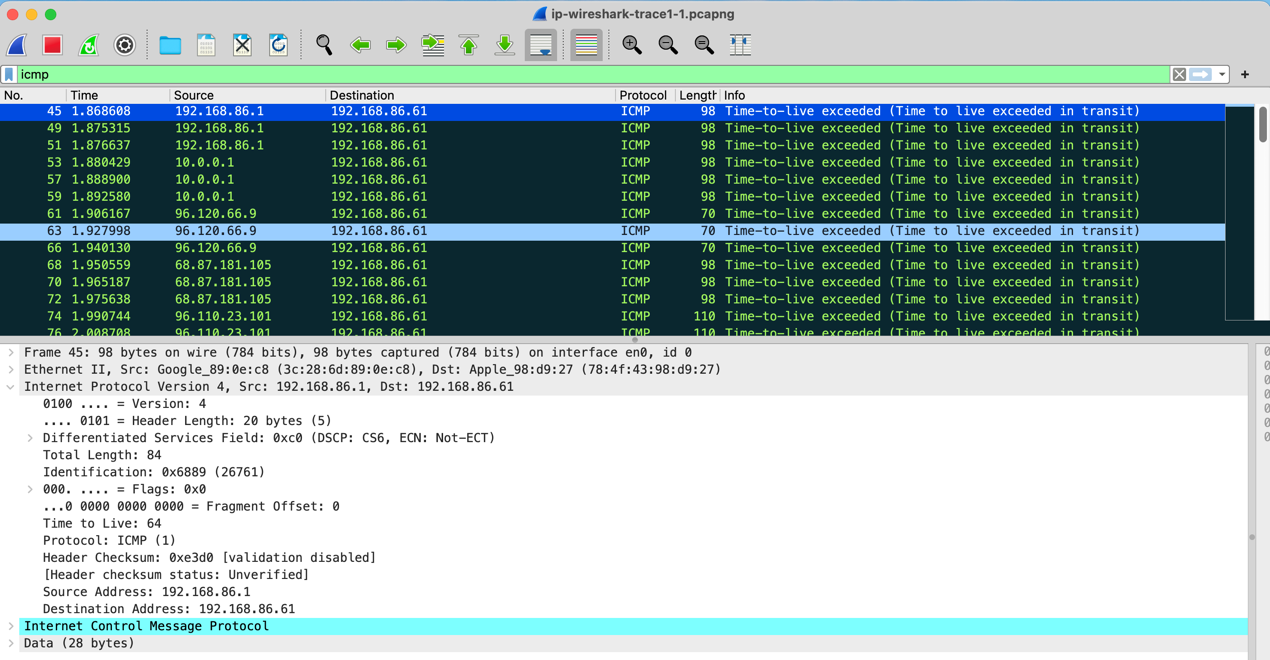
**8. Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?**

**答案：版本字段（因为所有数据包都使用IPv4）、头部长度字段（因为这些是UDP数据包）、源IP地址（因为我们从相同的源发送）以及目标IP地址（因为我们发送到相同的目标）。**

**9. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.**

**答案：Identification顺序增长，每个加1。**

**（就截一张，其他类似的滑动查看）**

****

**10. What is the upper layer protocol specified in the IP datagrams returned from the routers? [Note: the answers for Linux/MacOS differ from Windows here].**

**答案：在返回的IP数据报中, 协议字段是 ICMP(1)**

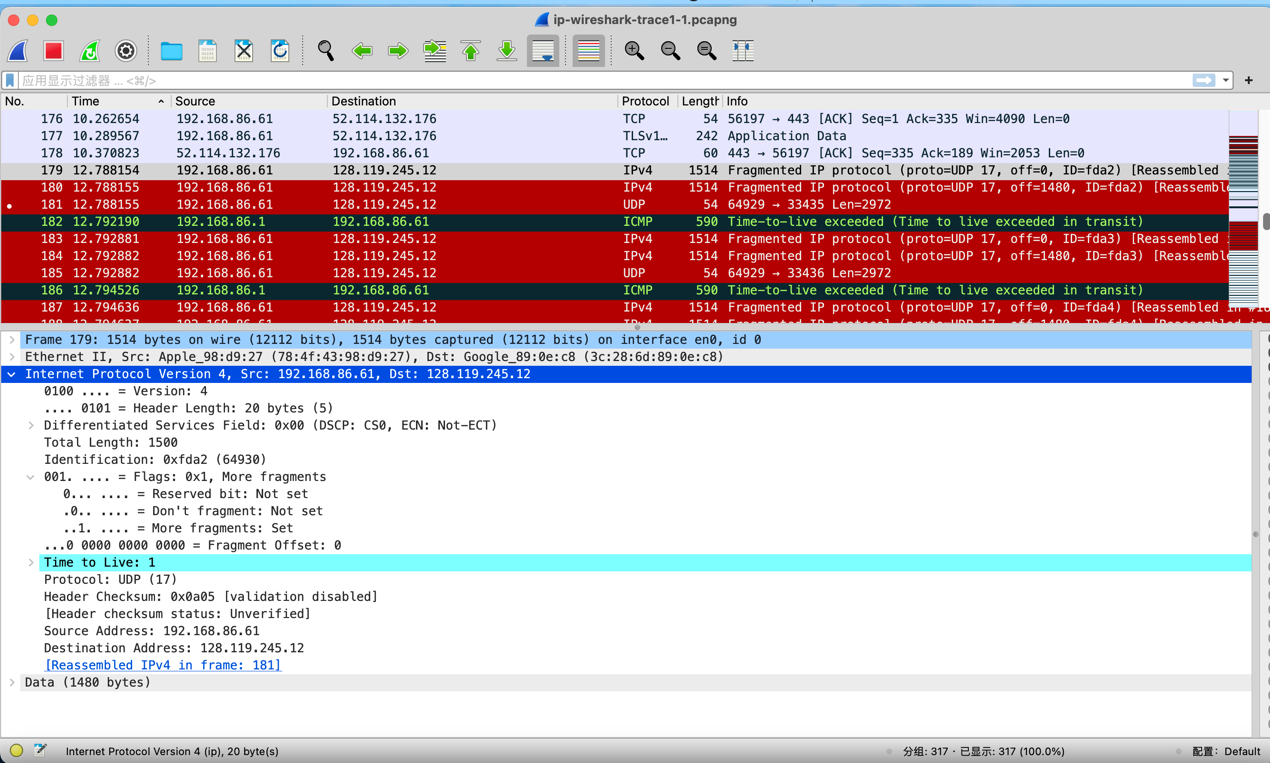
**11. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?**

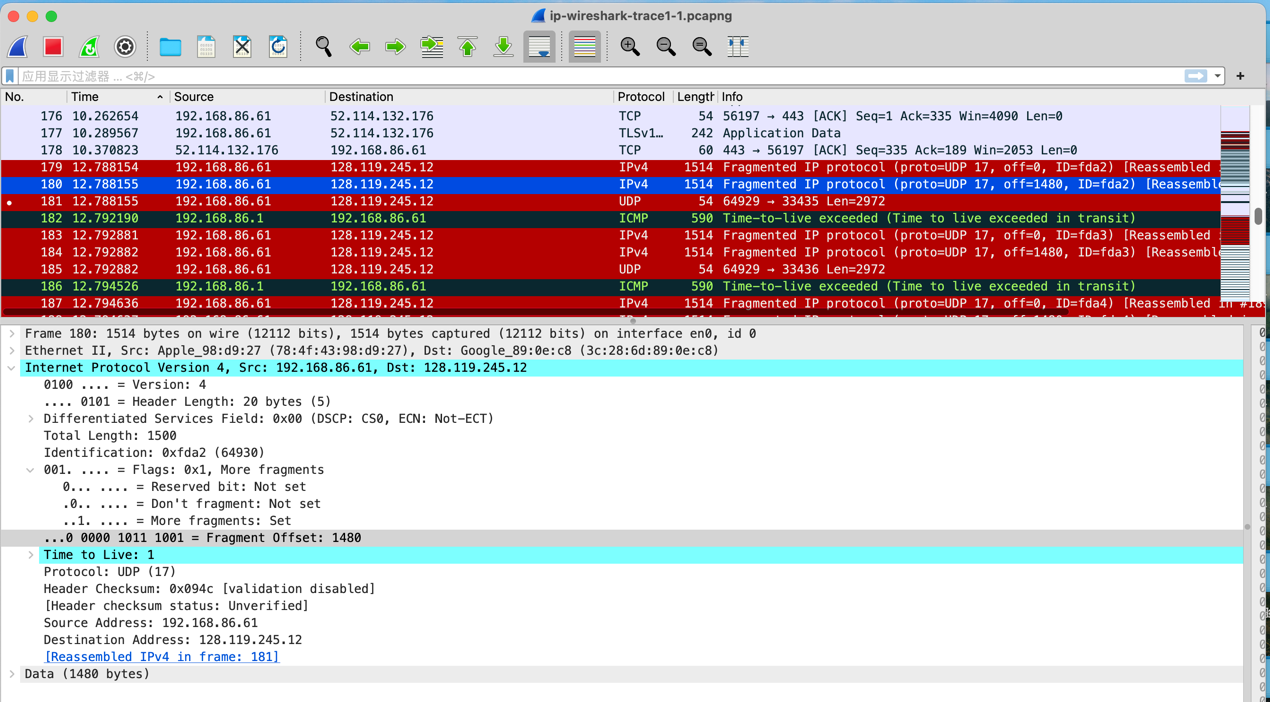
**答案：Identification 字段的值无法确定, 假如对连续三条请求作出响应的是同一个路由器, 则 Identification 字段顺序增长, 否则无法保证其关系。**

**12. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?**

**答案：TTL也跟作出响应的路由器有关**

**Part 2: Fragmentation**

****

****

****

**13. Find the first IP datagram containing the first part of the segment sent to 128.119.245.12 sent by your computer via the traceroute command to gaia.cs.umass.edu, after you specified that the traceroute packet length should be 3000. Has that segment been fragmented across more than one IP datagram?**

**答案：被分片。**

**14. What information in the IP header indicates that this datagram been fragmented?**

**答案：IP头中的“Flags”字段中的“More fragments”标志表明该数据报已经被分片。**

**15. What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?**

**答案：在IP头中，通过“Flags”字段中的“More fragments”标志为1和“Fragment Offset”为0，可以确定这是UDP段的第一个分片。**

**16. How many bytes are there in is this IP datagram (header plus payload)?**

**答案：该IP数据报的总长度为1500字节，包括头部（20）和负载（1480）。**

**17. Now inspect the datagram containing the second fragment of the fragmented UDP segment. What information in the IP header indicates that this is not the first datagram fragment?**

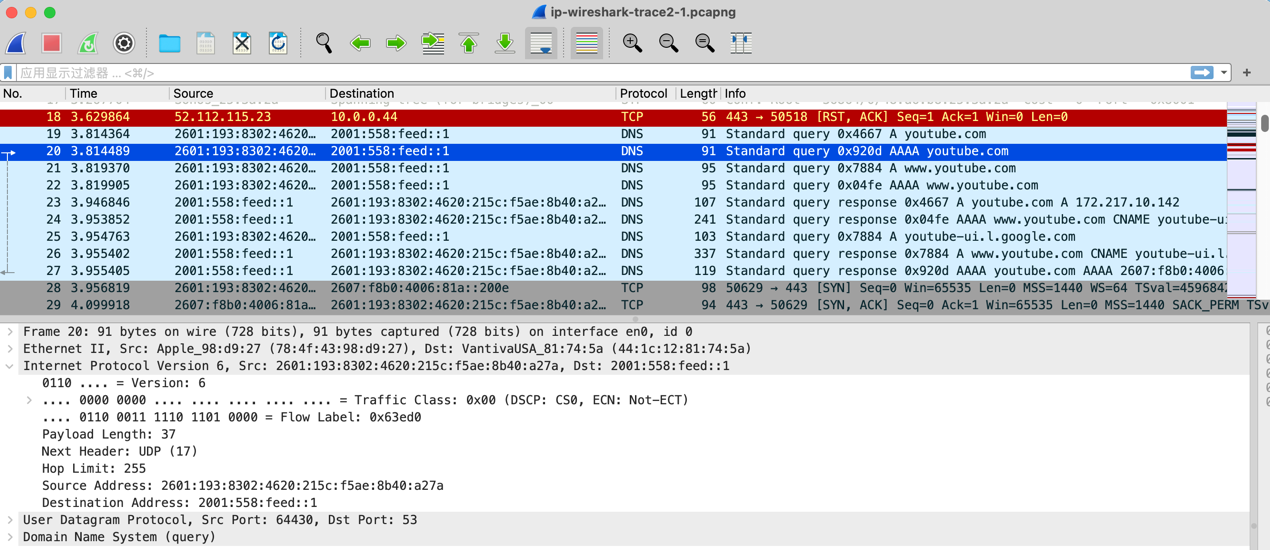
**答案：“More fragments”标志为1，并且“Fragment Offset”字段的值为1480，表明这不是第一个数据报分片。**

**18. What fields change in the IP header between the first and second fragment?**

**答案：在第一个和第二个分片之间，“Fragment Offset”字段的值发生了变化，从第一个分片的0变为第二个分片的1480。**

**19. Now find the IP datagram containing the third fragment of the original UDP segment. What information in the IP header indicates that this is the last fragment of that segment?**

**答案： “More fragments”标志为0，且“Fragment Offset”字段的值为2960，表明这是最后一个分片。**

**Part 3: IPv6**

**20. What is the IPv6 address of the computer making the DNS AAAA request? This is the source address of the 20th packet in the trace. Give the IPv6 source address for this datagram in the exact same form as displayed in the Wireshark**

**window.**

**答案：进行DNS AAAA请求的计算机的IPv6地址是2601:193:8302:4620:215c:f5ae:8b40:a27a。**

**21. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window.**

**答案：此数据报的IPv6目标地址是2001:558:feed::1。**

**22. What is the value of the flow label for this datagram?**

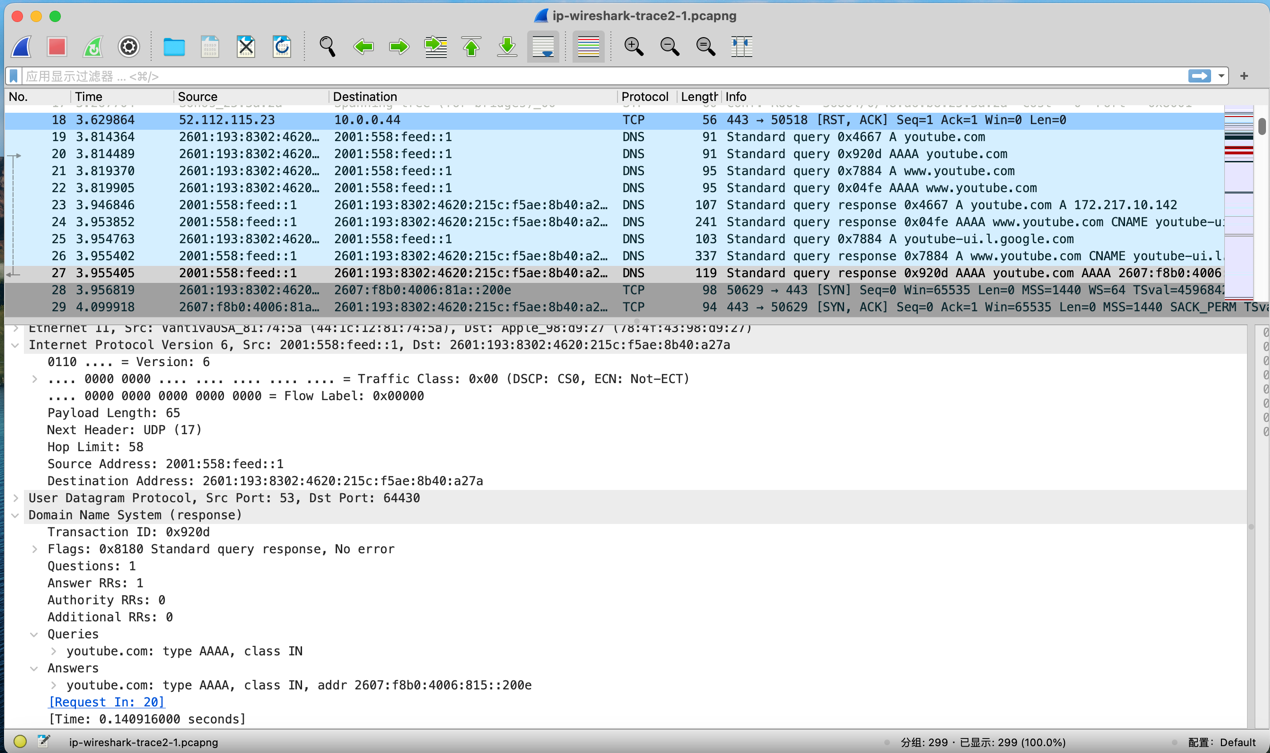
**答案：此数据报的流标签(flow label)的值是0x63ed0。**

**23. How much payload data is carried in this datagram?**

**答案：此数据报携带了37个字节的有效负载数据。**

**24. What is the upper layer protocol to which this datagram’s payload will be delivered at the destination?**

**答案：此数据报的有效负载将在目标地点交付到UDP协议。**

****

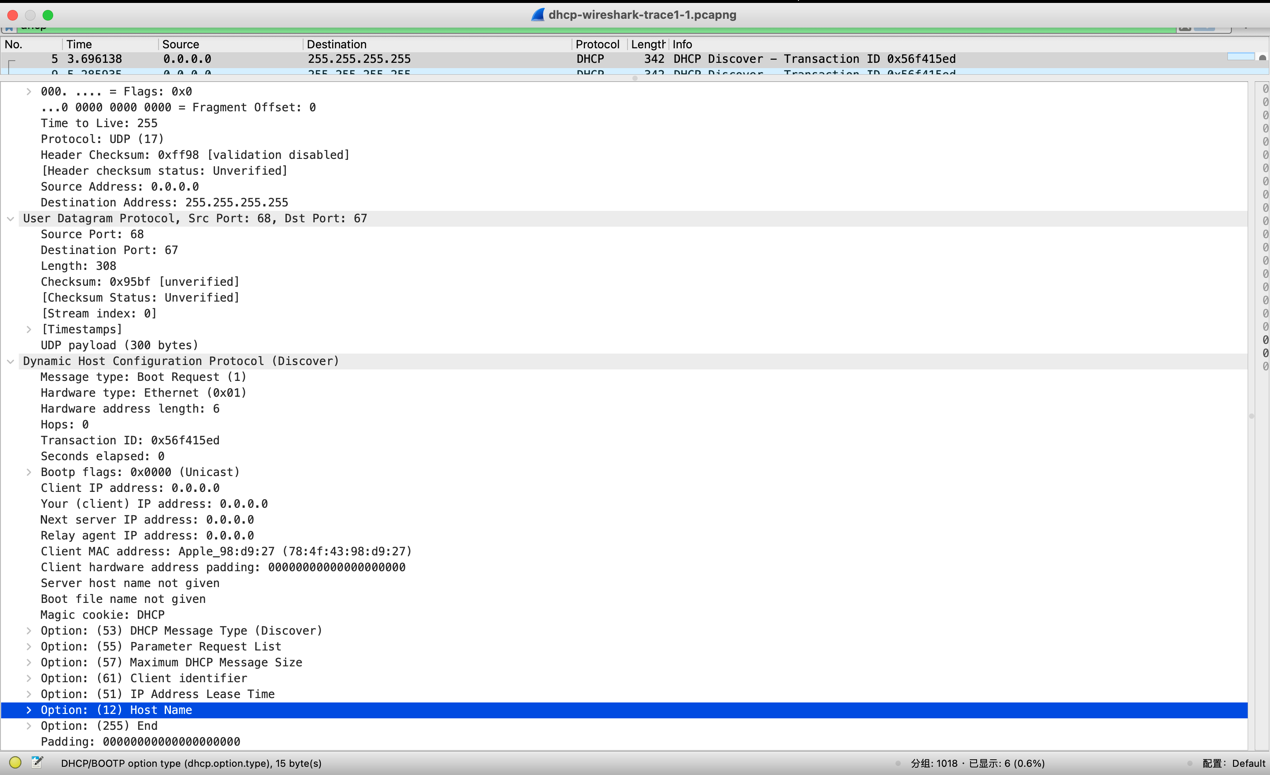
**25. How many IPv6 addresses are returned in the response to this AAAA request?**

**答案：在AAAA请求的响应中返回了一个IPv6地址。**

**26. What is the first of the IPv6 addresses returned by the DNS for youtube.com? Give this IPv6 address in the exact same shorthand form as displayed in the Wireshark window.**

**答案：youtube.com的第一个IPv6地址是2607:f8b0:4006:815::200e。**

**二、DHCP**

****

**1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?**

**答案：UDP。**

**2. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.**

**答案：源IP地址为0.0.0.0。这是一个特殊的地址，表示客户端尚未分配到IP地址，正处于发现阶段。**

**3. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.**

**答案：包含Discover消息的数据报的目标IP地址为255.255.255.255。这是广播地址，表示客户端希望将Discover消息发送到网络上的所有设备，以便寻找可用的DHCP服务器。**

**4. What is the value in the transaction ID field of this DHCP Discover message?**

**答案：DHCP Discover消息中的事务ID字段的值为0x56f415ed。**

**5. Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?**

**答案：DHCP Discover消息中的选项字段提供了客户端建议或请求DHCP服务器的五个信息（除了IP地址之外）：**

**1）DHCP消息类型（Option 53）：这里是Discover。**

**2）参数请求列表（Option 55）：客户端请求的参数包括子网掩码、静态路由、路由器、DNS服务器、域名、域搜索、私有/代理自动发现、LDAP等。**

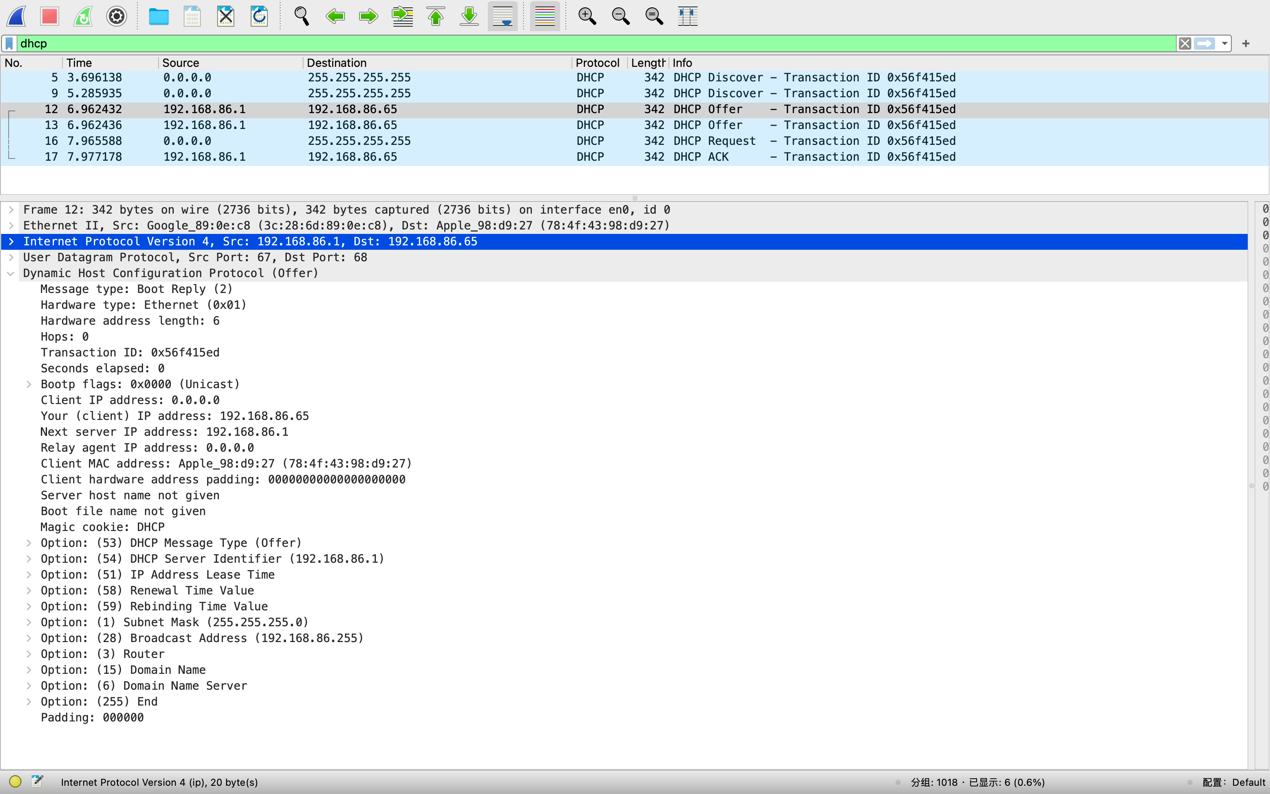
**3）最大DHCP消息大小（Option 57）：客户端建议的最大消息大小为1500字节。**

**4）客户端标识符（Option 61）：这里包含了以太网类型的客户端MAC地址。**

**5）IP地址租约时间****（Option 51）：客户端请求的租约时间为90天（7776000秒）。**

**6）主机名（Option 12）：客户端提供的主机名是"MacBook-Pro-6"。**

**7）选项结束标志（Option 255）：表示选项字段的结束。**

****

**6. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?**

**答案：事务ID（Transaction ID）字段的值（0x56f415ed）与前面的DHCP Discover消息相同。**

**7. What is the source IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.**

**答案：包含Offer消息的IP数据报的源IP地址是192.168.86.1。这是DHCP服务器的IP地址，特殊之处在于它是为客户端分配IP地址的服务器。**

**8. What is the destination IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain.**

**答案：Offer消息的数据报目标IP地址是192.168.86.65。这是DHCP客户端的IP地址，表明DHCP服务器向特定的客户端发送了这个Offer消息。**

**9. Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?**

**答案：DHCP Offer消息中的选项字段提供了DHCP服务器为DHCP客户端提供的信息：**

**1）DHCP消息类型（Option 53）：这里是Offer。**

**2）DHCP服务器标识符（Option 54）：指定了提供IP地址的DHCP服务器的IP地址（192.168.86.1）。**

**3）IP地址租约时间（Option 51）：指定了客户端分配的IP地址的租约时间为1天（86400秒）。**

**4）续约时间值（Option 58）：指定了续约的时间。**

**5）重新绑定时间值（Option 59）：指定了重新绑定的时间。**

**6）子网掩码（Option 1）：指定了客户端分配的IP地址所在的子网掩码（255.255.255.0）。**

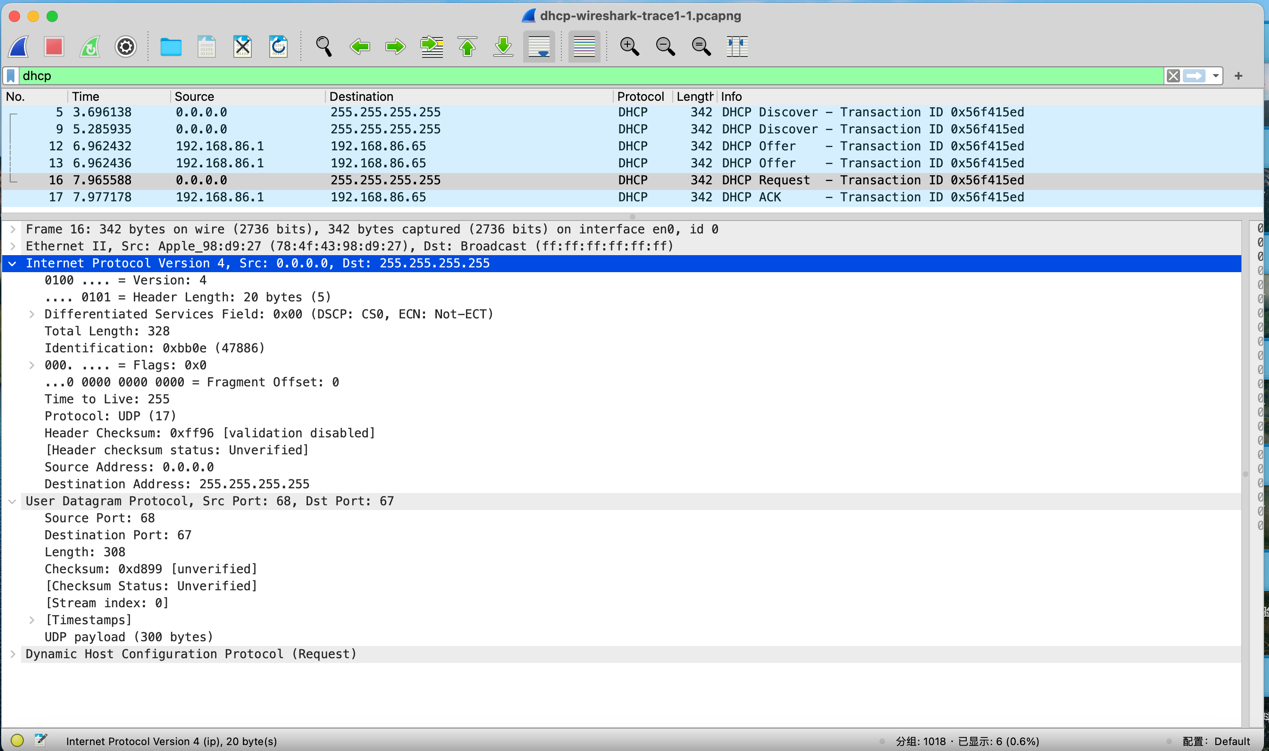
**7）广播地址（Option 28）：指定了子网的广播地址（192.168.86.255）。**

**8）路由器（Option 3）：指定了客户端要使用的默认网关的IP地址（192.168.86.1）。**

**9）域名（Option 15）：指定了客户端所在域的名称（lan）。**

**10）域名服务器（Option 6）：指定了用于DNS解析的域名服务器的IP地址（192.168.86.1）。**

**11）结束选项（Option 255）：标志DHCP选项字段的结束。**

****

**10. What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?**

**答案：包含第一个DHCP Request消息的IP数据报中，UDP源端口号是68，UDP目标端口号是67。**

**11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.**

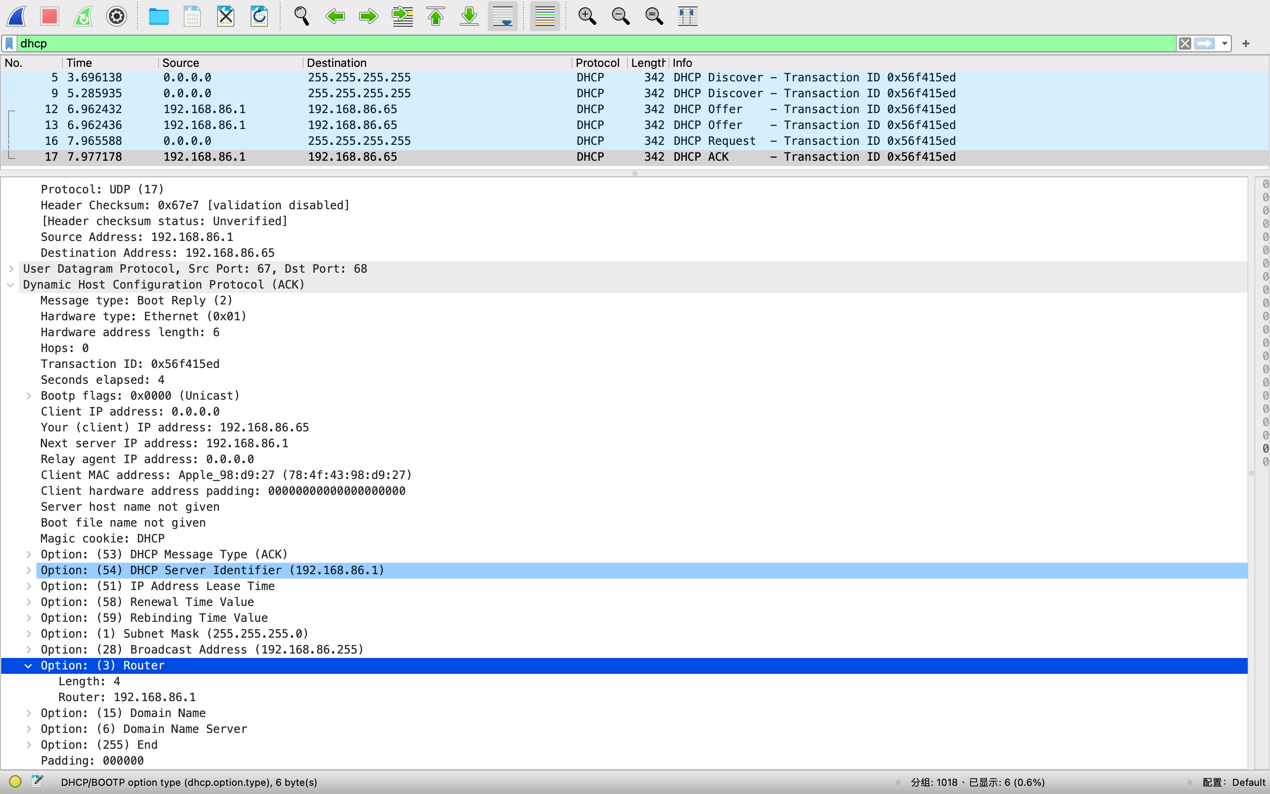
**答案：Request消息的数据报中，源IP地址是0.0.0.0。这表示客户端正在请求分配一个IP地址，但在此时还未被分配。**

**12. What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.**

**答案：Request消息的数据报中，目标IP地址是255.255.255.255。这是广播地址，表示客户端正在向网络上的所有设备发送Request消息，以寻找提供所请求IP地址的DHCP服务器。**

**13. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?**

**答案：DHCP Request消息中的事务ID字段的值是0x56f415ed。是的，这个事务ID的值与之前的Discover和Offer消息中的事务ID相匹配。DHCP事务ID用于关联DHCP交互的各个阶段，确保正确的响应与相应的请求匹配。**

****

**14. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.**

**答案：源IP地址是192.168.86.1。这是DHCP服务器的IP地址，特殊之处在于它是为客户端分配IP地址的服务器。**

**15. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.**

**答案：目标IP地址是****192.168.86.65。这是DHCP客户端的IP地址，表示DHCP服务器向特定的客户端发送了这个ACK消息。**

**16. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?**

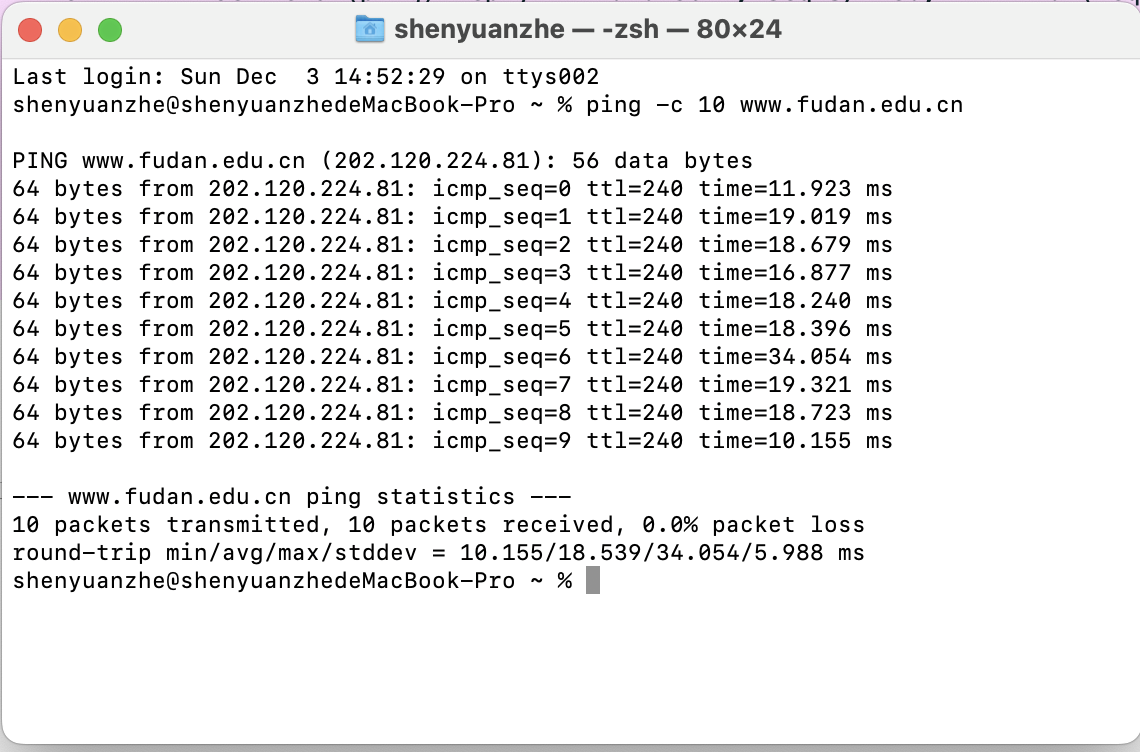
**答案：DHCP ACK消息中包含了分配给客户端的IP地址的字段名称是"Your (client) IP address"。**

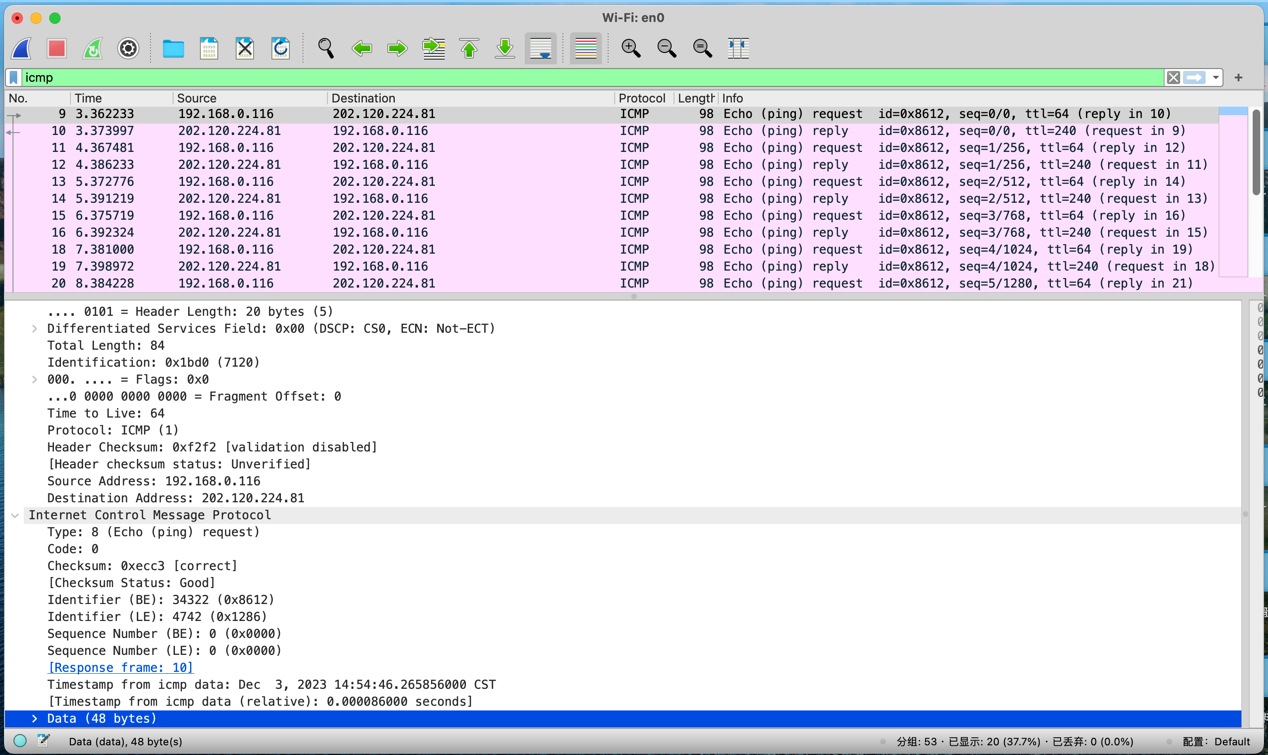
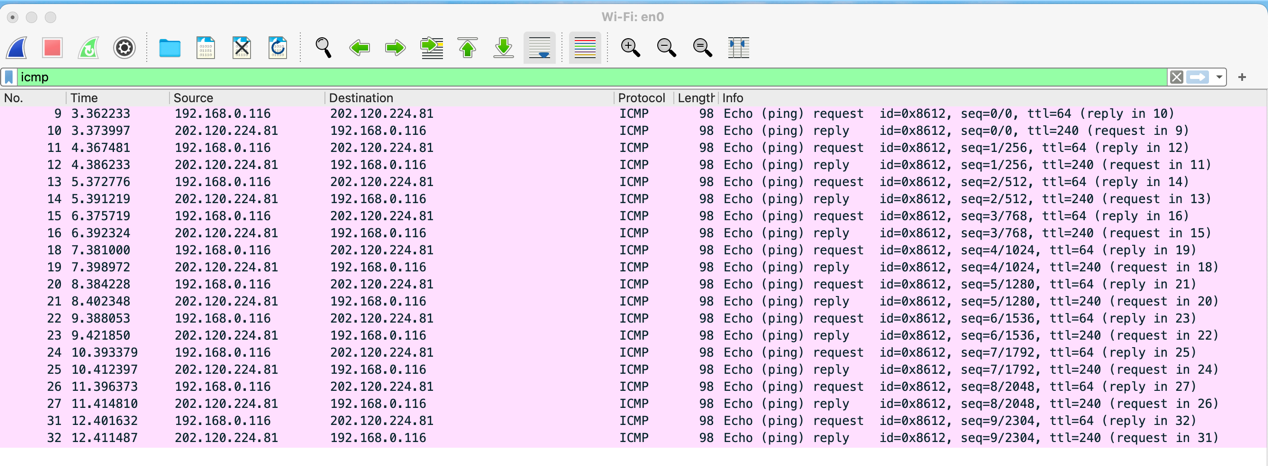
**17. For how long a time (the so-called “lease time”) has the DHPC server assigned this IP address to the client?**

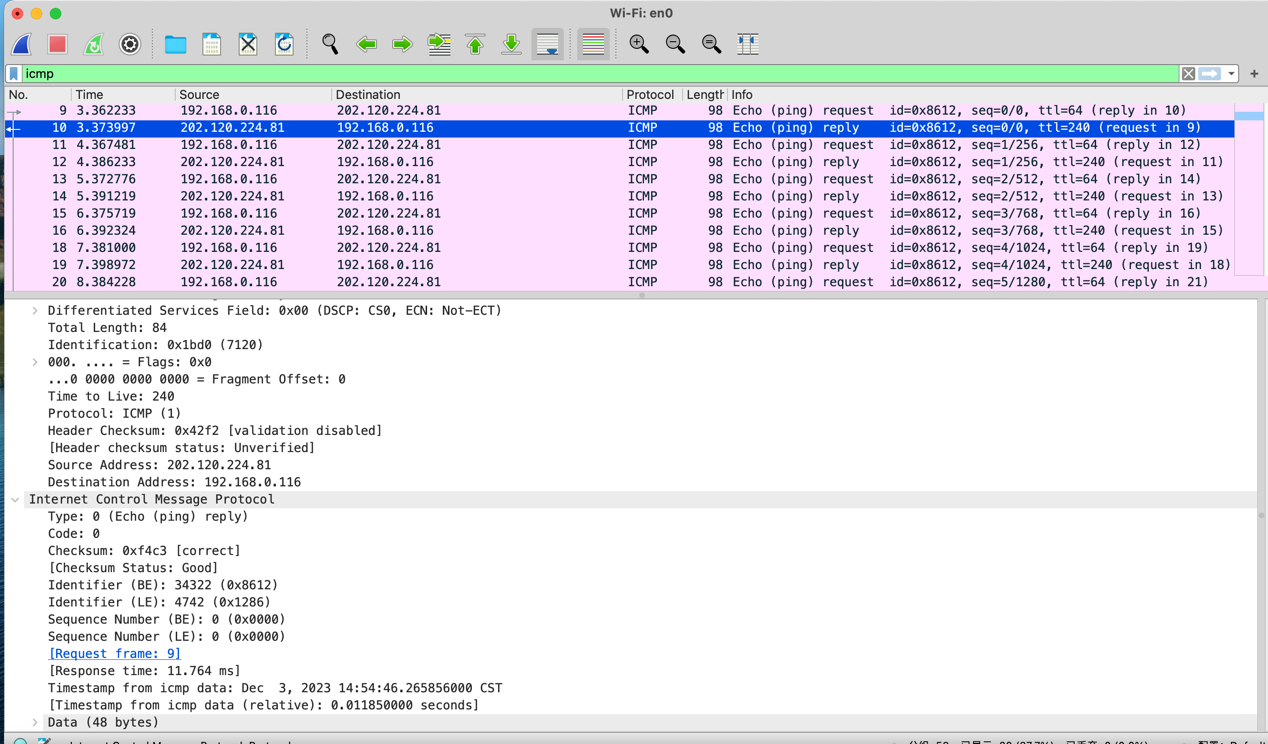
**答案：DHCP服务器分配给客户端的IP地址的租约时间是在DHCP ACK消息的选项字段中的"Option: (51) IP Address Lease Time"中指定的。租约时间是1天（86400秒）。**

**18. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?**

**答案：DHCP ACK消息中，DHCP服务器返回给客户端的IP地址的默认网关（第一跳路由器）是在选项字段中的"Option: (3) Router"中指定的。第一跳路由器的IP地址是192.168.86.1。**

**三、ICMP**

****

****

**1. What is the IP address of your host? What is the IP address of the destination host?**

**答案：源主机的IP地址是192.168.0.116，目标主机的IP地址是202.120.224.81。**

**2. Why is it that an ICMP packet does not have source and destination port numbers?**

**答案：ICMP 数据包没有源和目标端口号是因为它被设计用于在主机和路由器之间传递网络层信息，而不是在应用层进程之间传递信息。每个 ICMP 数据包都有一个“类型”和一个“代码”。类型/代码组合标识接收到的特定消息。由于网络软件本身解释所有 ICMP 消息，因此不需要端口号将 ICMP 消息定向到应用层进程。**

**3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have?** **How many bytes are the checksum, sequence number and identifier fields?**

**答案：检查ping请求数据包：**

**ICMP类型：8（回显请求）**

**ICMP代码：0**

**校验和：0xecc3**

**标识符：34322**

**序列号：0**

**数据字段长度：48字节**

**校验和：2字节，序列号：2字节，标识符：2字节**

**4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

**答案：检查相应的ping响应数据包：**

**ICMP类型：0（回显响应）**

**ICMP代码：0**

**校验和：0xf4c3**

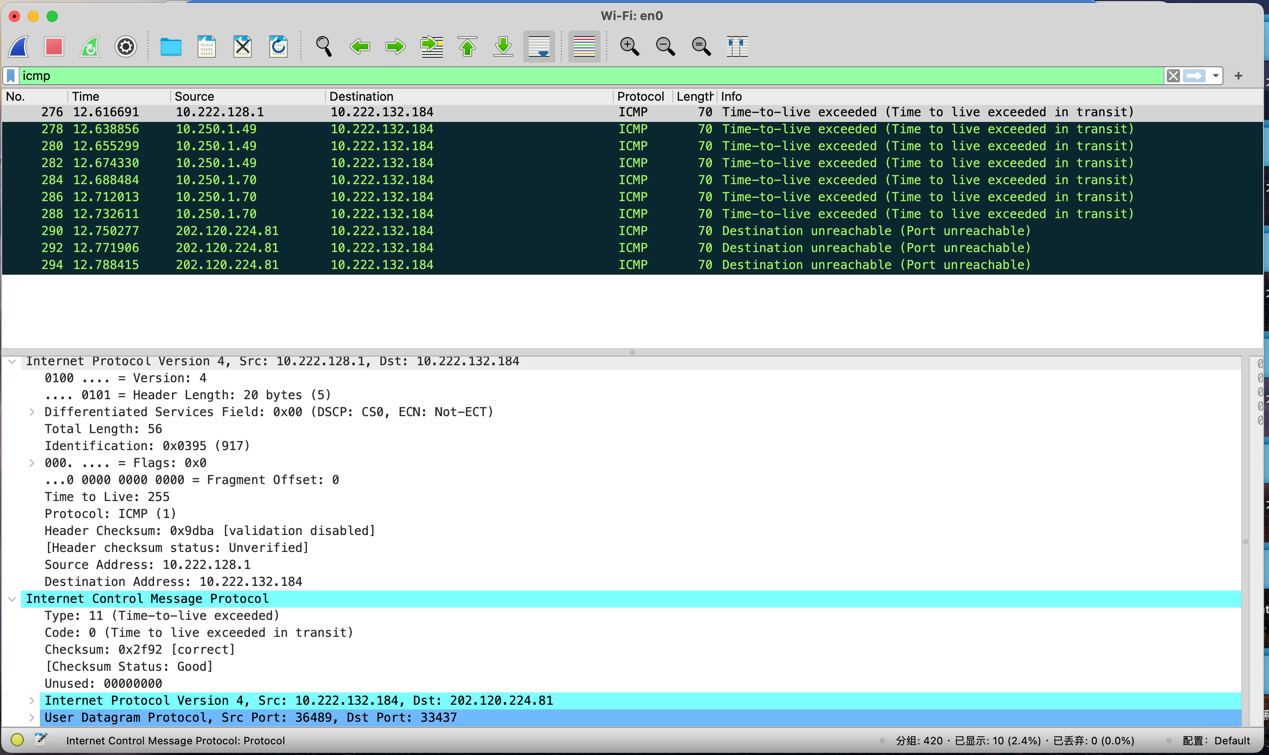
**标识符：34322**

**序列号：0**

**响应时间：11.764毫秒**

**数据字段长度：48字节**

**校验和：2字节，序列号：2字节，标识符：2字节**

****

**5. What is the IP address of your host? What is the IP address of the target**

**destination host?**

**答案：主机IP地址10.222.128.1，目的IP地址10.222.132.184**

**6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?**

**答案：不同的协议有不同的协议号。ICMP使用的是IP协议号1，而UDP使用的是IP协议号17。因此，如果ICMP发送UDP数据包，IP协议号将是17而不是01。**

**7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?**

**答案：ICMP回显数据包具有与ping查询数据包相同的字段。**

**8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?**

**答案：ICMP错误数据包与ping查询数据包不同。它包含了IP头部以及引起错误的原始ICMP数据包的前8个字节。**

**9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?**

**答案：最后三个ICMP数据包的消息类型是0（回显应答），而不是11（TTL过期）。它们之间的区别在于，在TTL（生存时间）过期之前，数据报已经成功到达目标主机。**