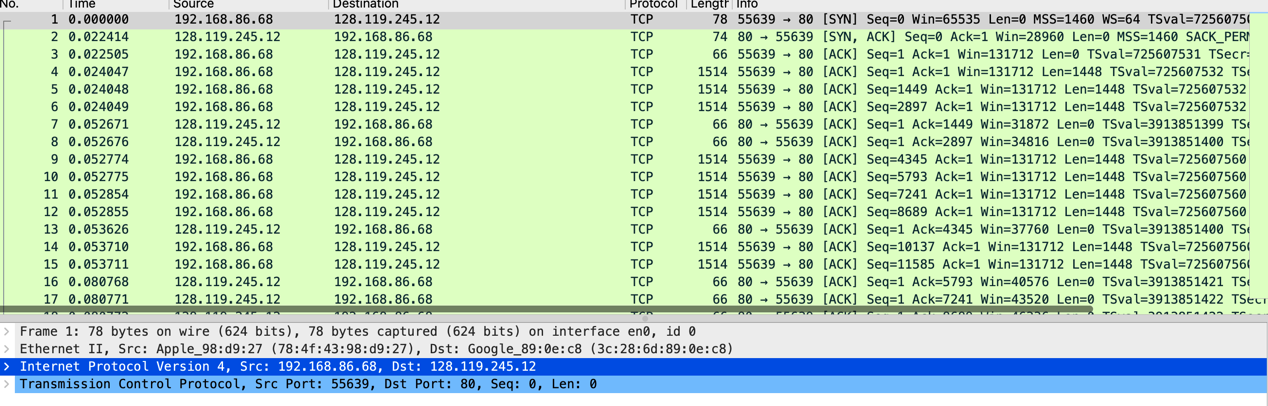
**Lab2实验报告**

**一、TCP**

**2. A first look at the captured trace**

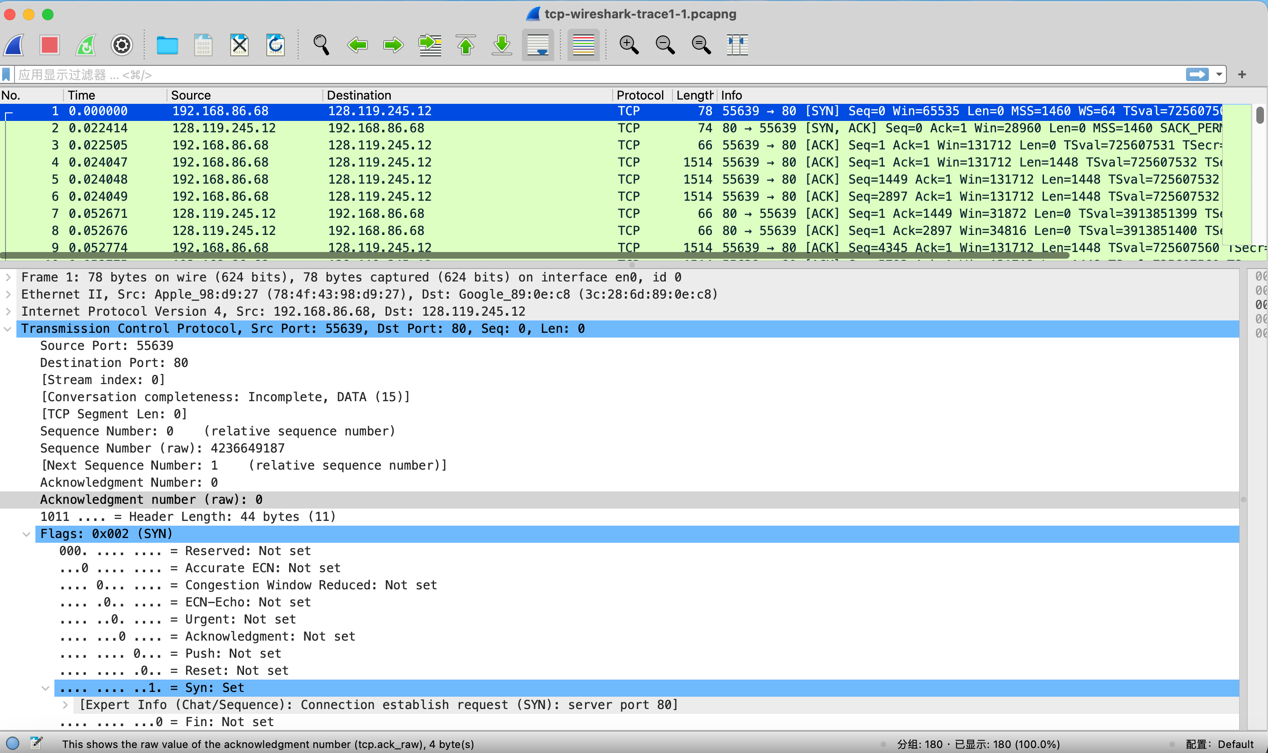
这里使用the Wireshark captured packet file tcp-wireshark-trace1-1 in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip>

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window”.

答案：客户端计算机（源）使用的IP地址是192.168.86.68，源TCP端口号是55639。

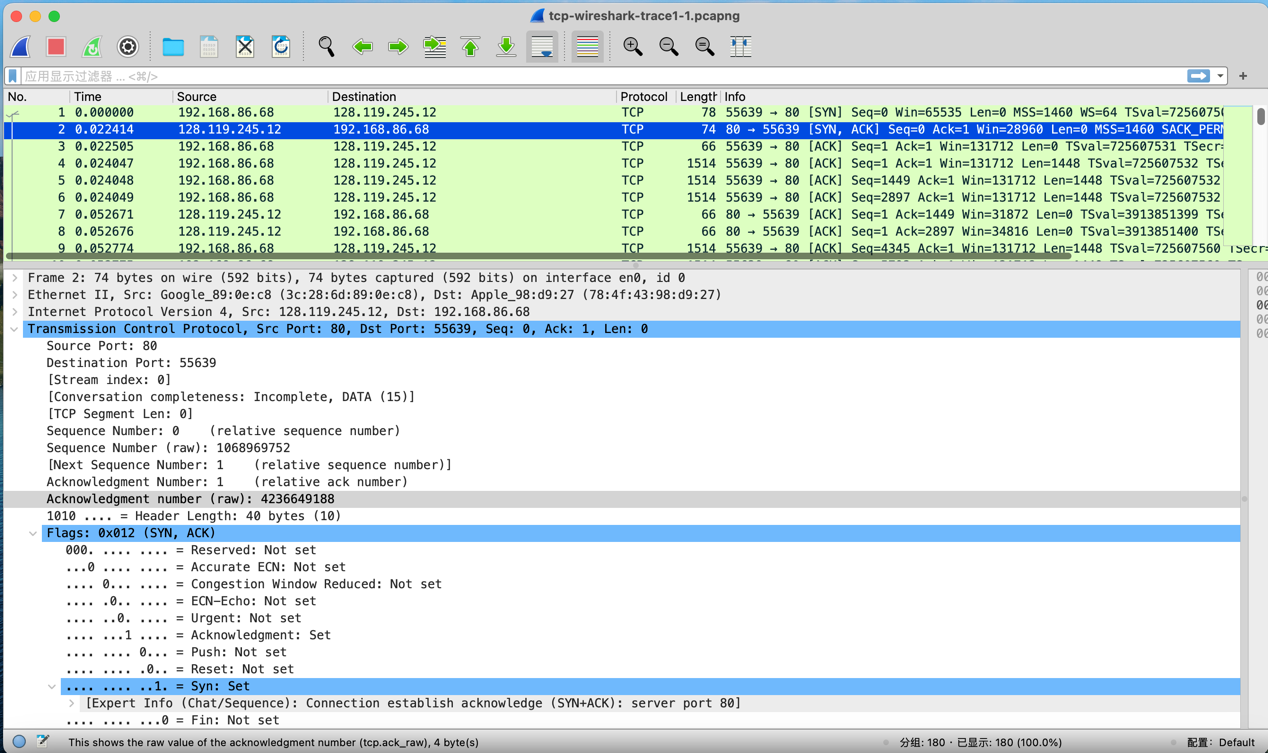
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

答案：gaia.cs.umass.edu的IP地址是128.119.245.12。它在该连接上发送和接收TCP段的端口号为80。

**3. TCP Basics**

1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? (Note: this is the “raw” sequence number carried in the TCP segment itself; it is NOT the packet # in the “No.” column in the Wireshark window. Remember there is no such thing as a “packet number” in TCP or UDP; as you know, there are sequence numbers in TCP and that’s what we’re after here. Also note that this is not the relative sequence number with respect to the starting sequence number of this TCP session.). What is it in this TCP segment that identifies the segment as a SYN segment?

答案：在提供的TCP段中，TCP SYN段的序列号（raw sequence number）是4236649187。这个TCP段被标识为SYN段的特征是"Flags"字段的数值为0x002，它的标志字段中的SYN标志被设置为1（SYN: Set）。这表示它是一个连接建立请求（SYN）段，用于初始化TCP连接。

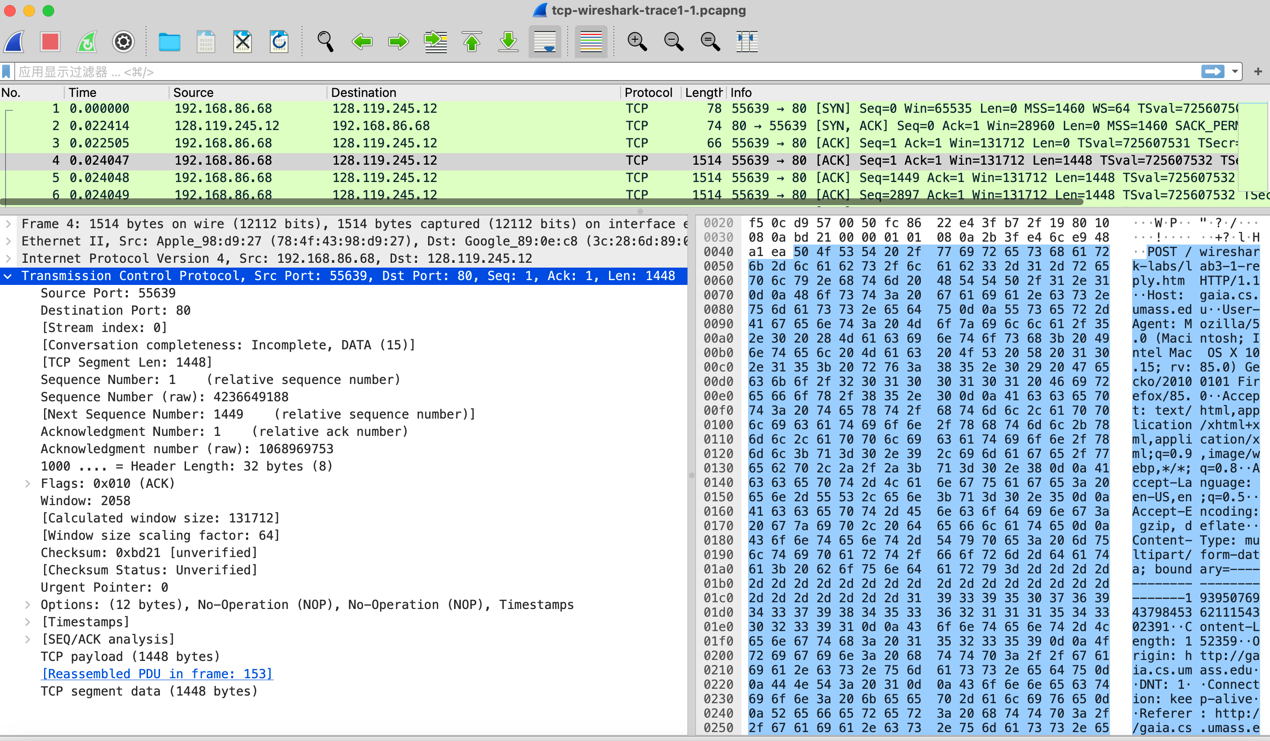


2. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is it in the segment that identifies the segment as a SYNACK segment? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?

答案：SYNACK段的序列号是：1068969752（在"Sequence Number (raw)"字段中）。这是服务器gaia.cs.umass.edu用来标识自己在TCP连接中的位置的唯一序列号。

SYNACK段被标识为SYNACK段的特征是TCP标志字段中的"Flags"。在这里，"Flags"字段的数值为0x012，表示同时设置了SYN和ACK标志。SYN标志表明服务器同意建立连接，而ACK标志表示已经收到了客户端发送的SYN段。

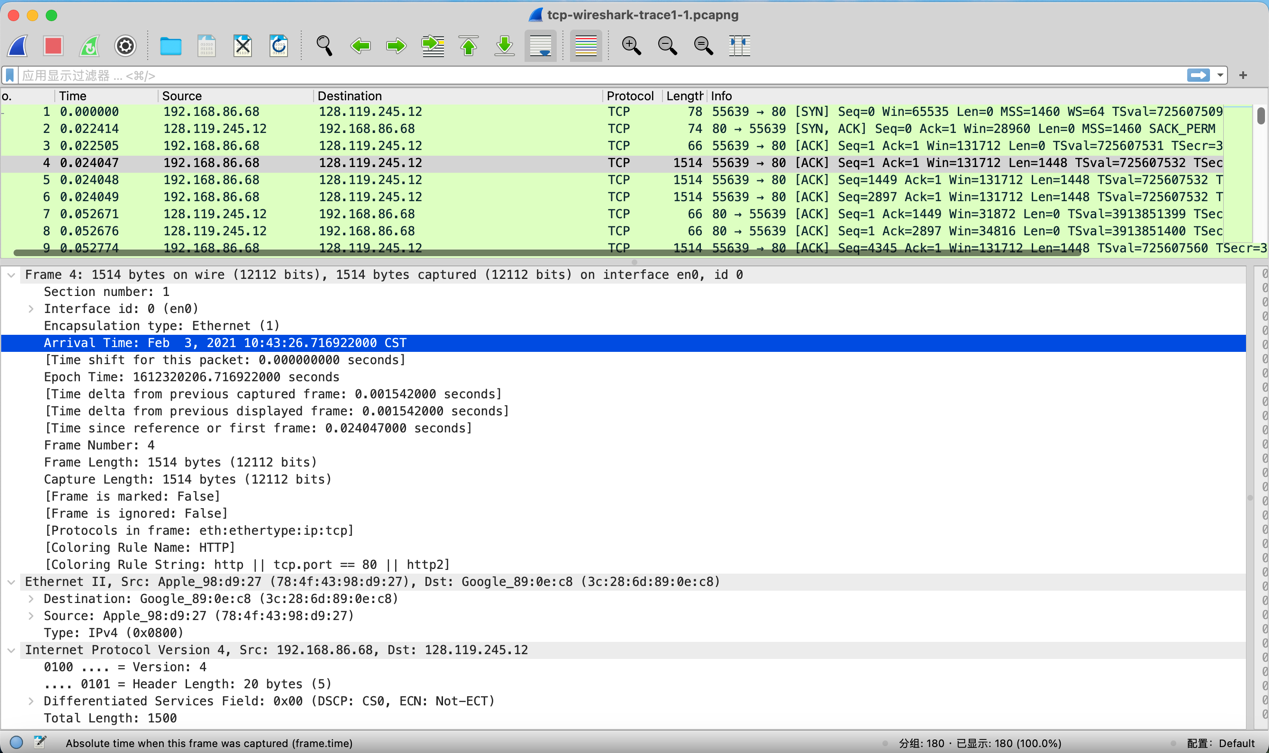
SYNACK段中的确认字段的值为4236649188（在"Acknowledgment Number(raw)"字段中）。gaia.cs.umass.edu确定这个值的方式是在客户端发送的SYN段的序列号的基础上加1。这表示服务器已经成功接收到了客户端的SYN段，并同意建立连接。



3. What is the sequence number of the TCP segment containing the header of the HTTP POST command? Note that in order to find the POST message header, you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text “POST” within its DATA field 1 2. How many bytes of data are contained in the payload (data) field of this TCP segment? Did all of the data in the transferred file alice.txt fit into this single segment?

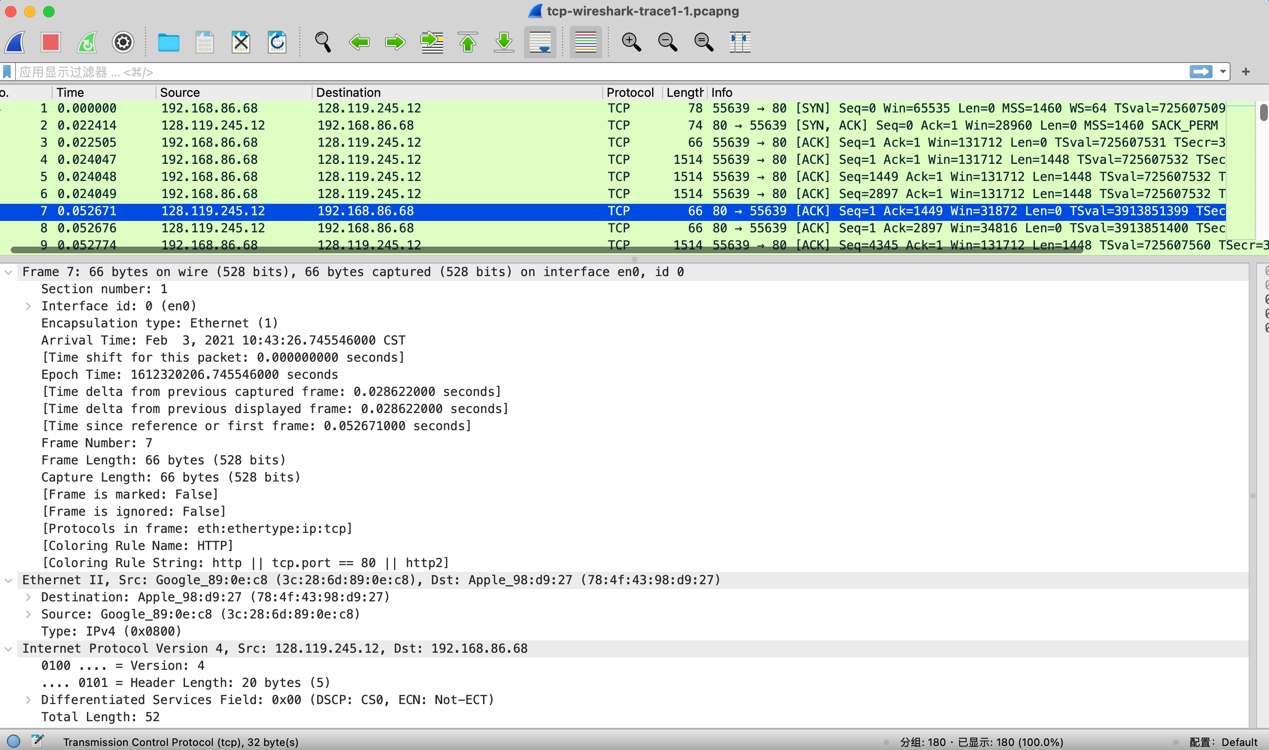
答案：HTTP POST命令头的TCP段的序列号是：4236649188（在"Sequence Number (raw)"字段中）。

该TCP段的有效载荷（数据）字段中包含了1448字节的数据（在"TCP Segment Len"字段中）。这是该段的数据大小。  
根据Wireshark数据包信息，alice.txt文件的所有数据并未完全适合这个单个TCP段中。alice.txt文件可能会被分成多个TCP段进行传输。这个段只包含了一部分数据，而不是整个文件。



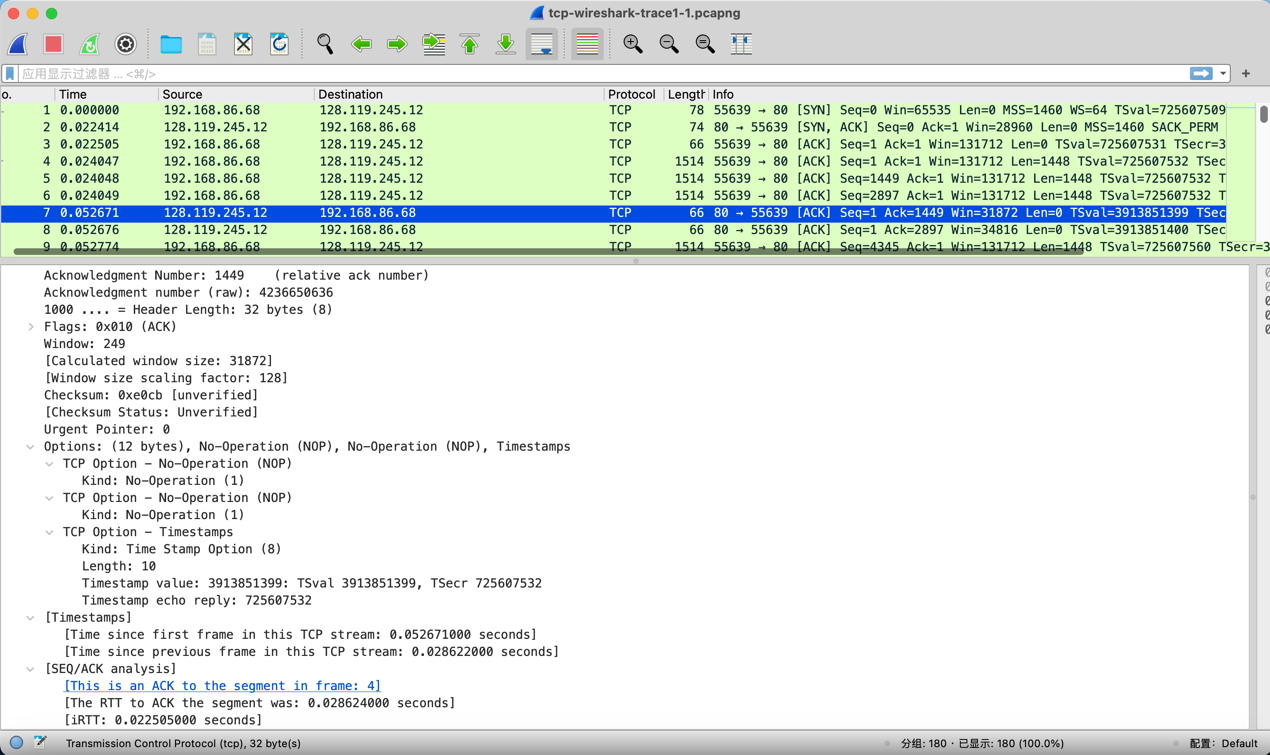
4. Consider the TCP segment containing the HTTP “POST” as the first segment in the data transfer part of the TCP connection.At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent?

答案：第一个数据包的发送时间是：Feb 3, 2021 10:43:26.716922000 CST。



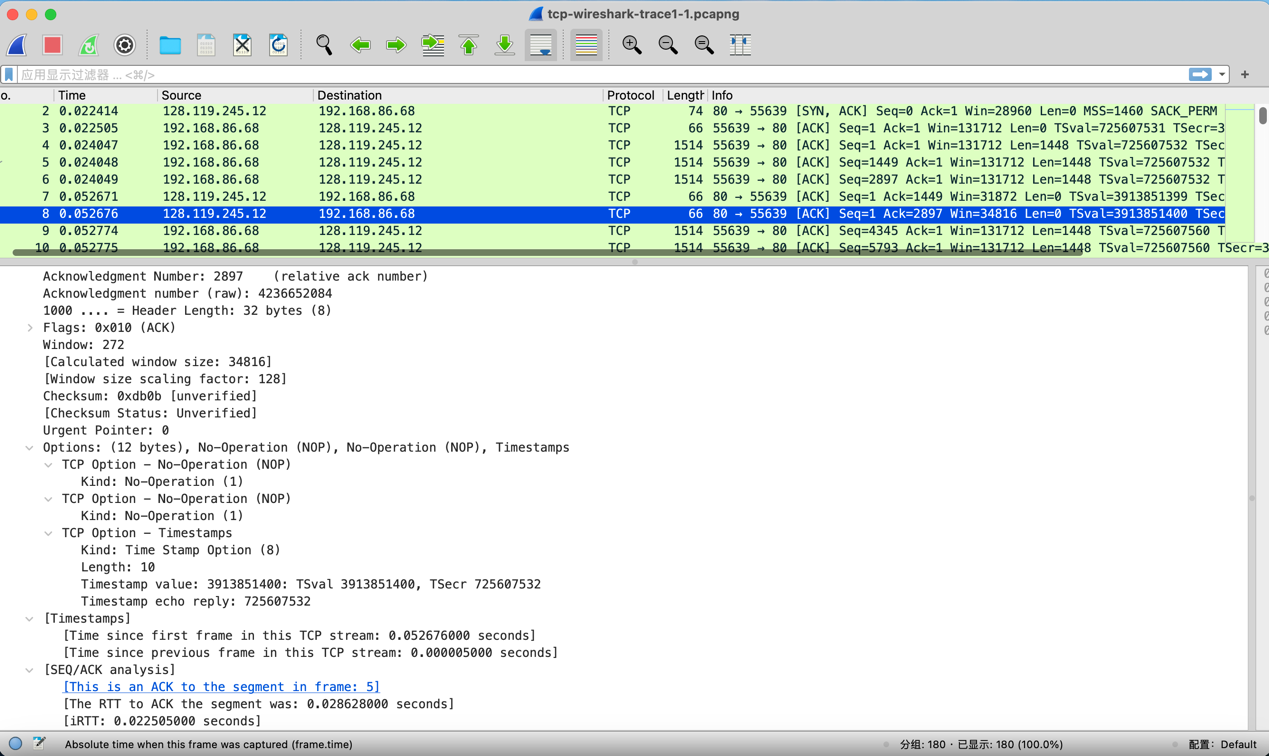
At what time was the ACK for this first data-containing segment received?

答案：第一个数据包的接收时间是：Feb 3, 2021 10:43:26.745546000 CST。



What is the RTT for this first data-containing segment?

答案：第一个数据包含的段的往返时延（RTT）是：0.028624000秒，即28.624毫秒。

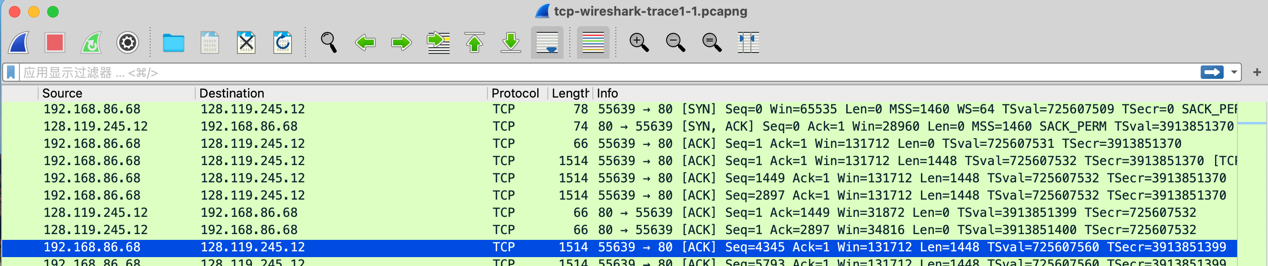


What is the RTT value the second data-carrying TCP segment and its ACK?

答案：第二个数据包含的段的往返时延（RTT）是：0.028628000秒，即28.628毫秒。

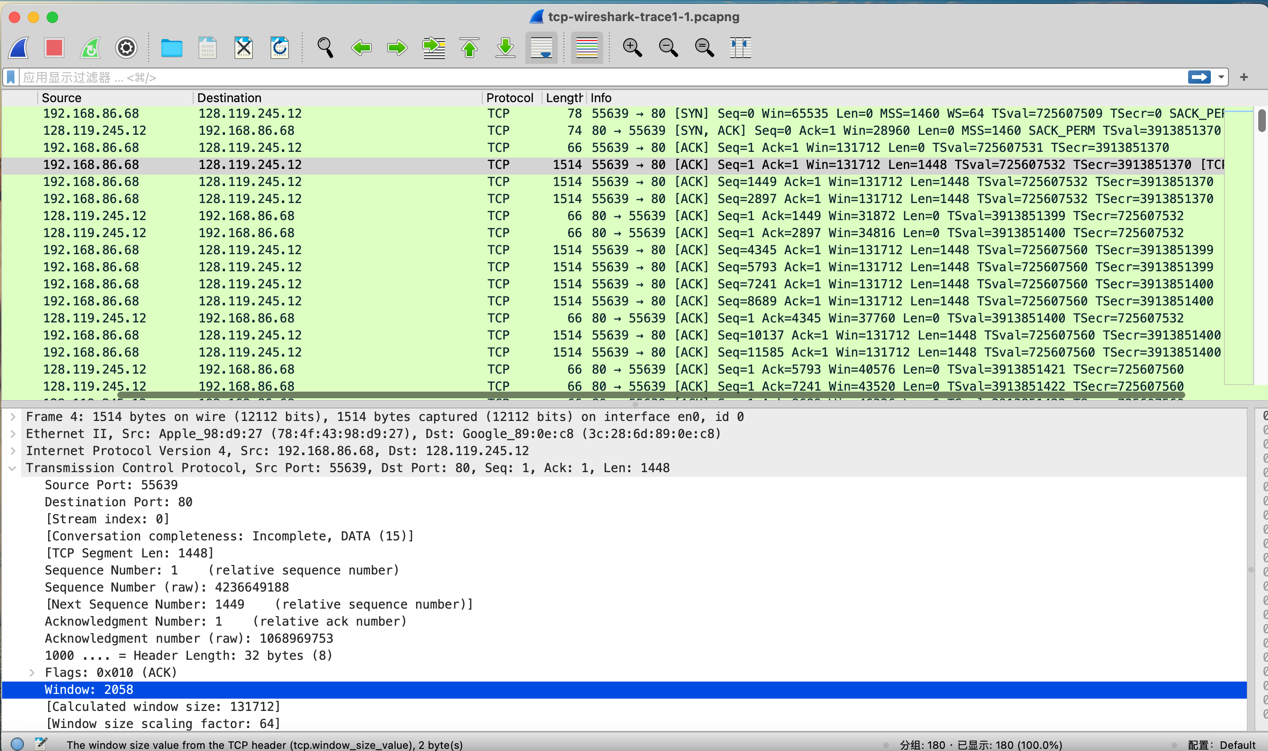
What is the EstimatedRTT value after the ACK for the second data-carrying segment is received? Assume that in making this calculation after the received of the ACK for the second segment, that the initial value of EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation, and a value of a = 0.125.

答案：EstimatedRTT = (1 - 0.125) \* 0.028624 + 0.125 \* 0.028628= 0.875 \* 0.028624 + 0.125 \* 0.028628= 0.0286245s，即28.6245毫秒



5. What is the length (header plus payload) of each of the first four data-carrying TCP segments?

答案：1514，1514，1514，1514



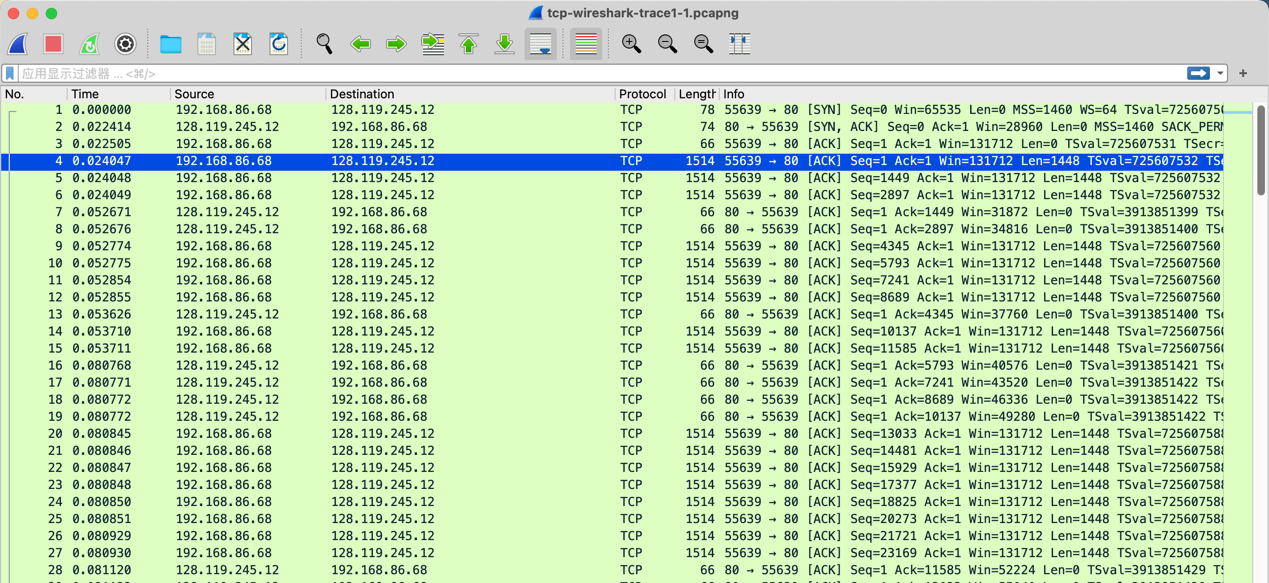
6. What is the minimum amount of available buffer space advertised to the client by gaia.cs.umass.edu among these first four data-carrying TCP segments ? Does the lack of receiver buffer space ever throttle the sender for these first four data-carrying segments?

答案：最小可用缓冲区空间为131712字节。

在这四个特定的TCP数据段中，没有触发接收方缓冲区溢出（receiver buffer overflow）的情况，因为窗口大小远大于即将到达的数据的大小，所以没有限制发送方的速度。

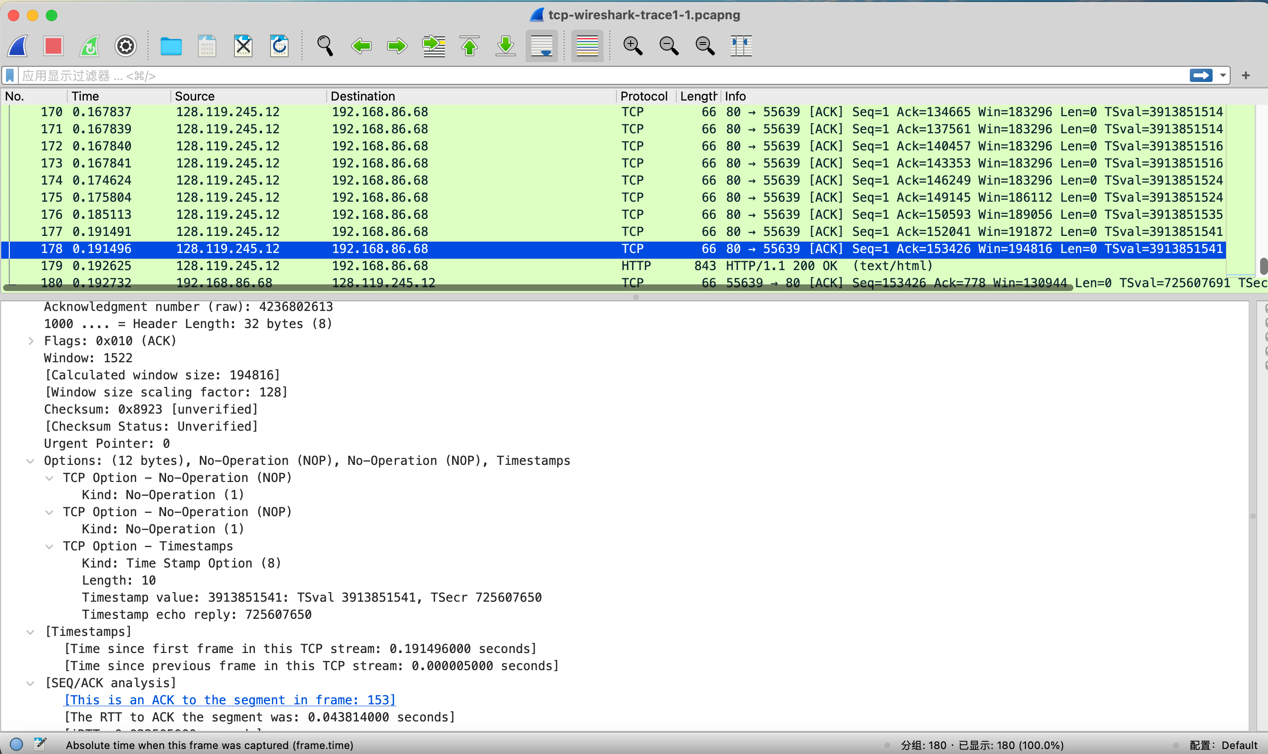
7. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

答案：跟踪文件中没有重新传输的数据段。我们可以通过检查跟踪文件中TCP数据段的序列号来验证这一点。在这个跟踪的时间-序列图（Stevens）中，从源（192.168.1.102）到目的地（128.119.245.12）的所有序列号都是随时间单调递增的。如果存在重新传输的数据段，那么这个重新传输数据段的序列号应该小于其相邻数据段的序列号。



8. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to gaia.cs.umass.edu?

答案：1480 \* 10 = 14800Bytes

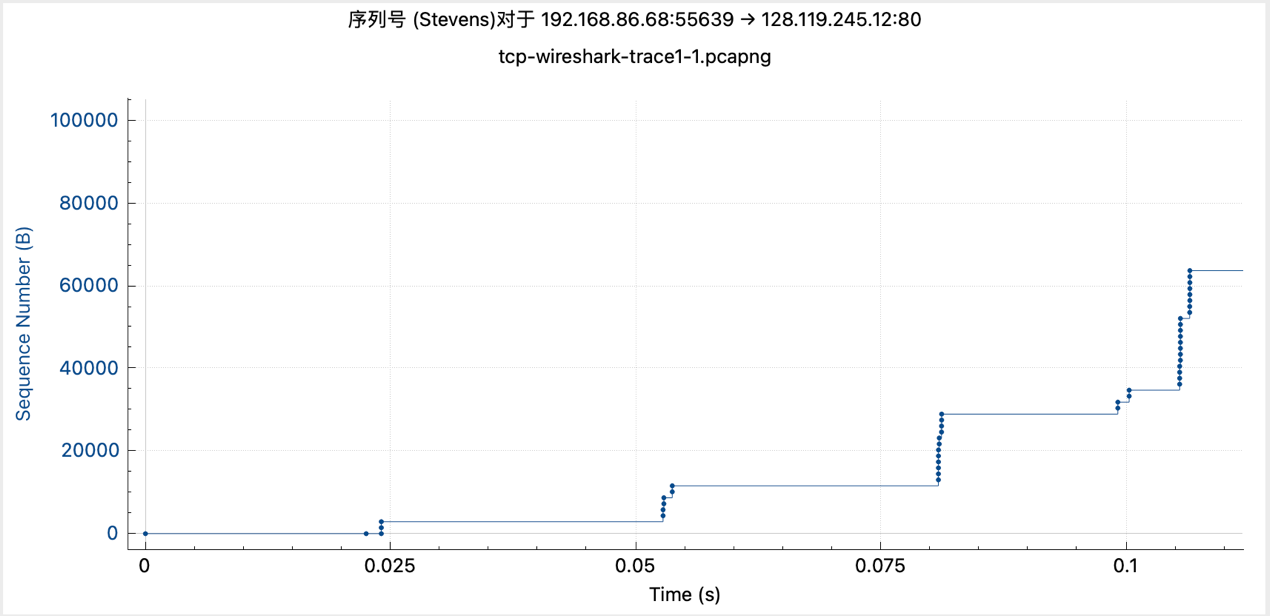
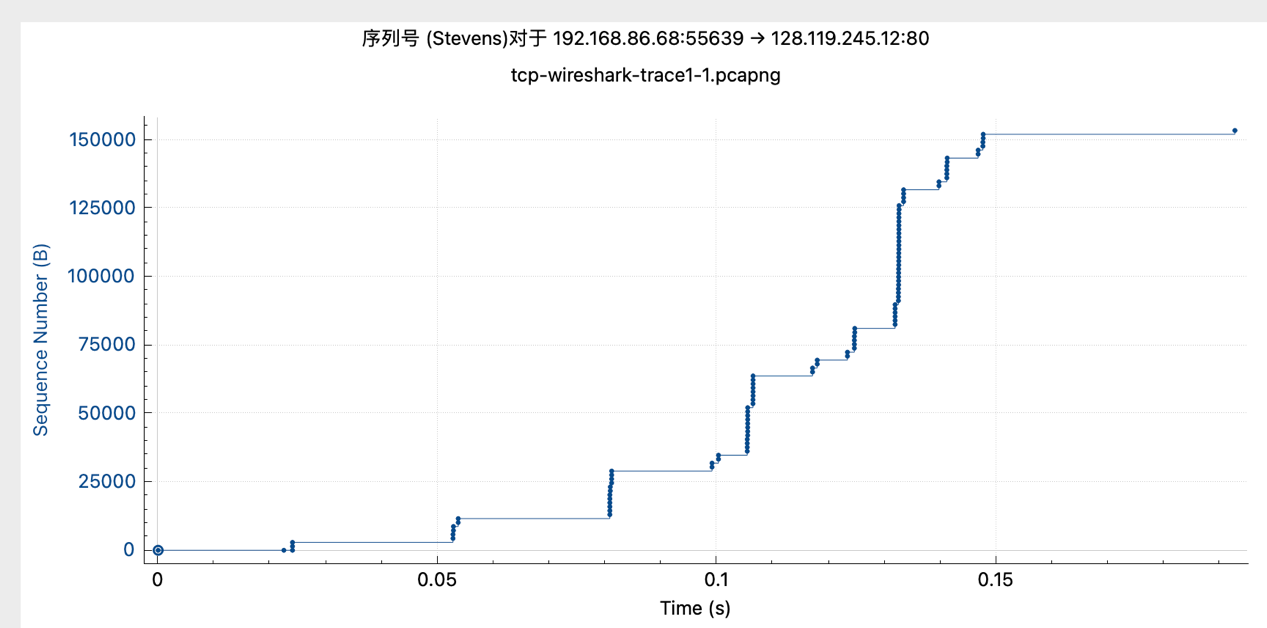


9. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

答案：首先，确定整个TCP连接的传输时间。通过查看[Time since first frame in this TCP stream: 0.191496000 seconds]得到传输时间为0.191496000s。

接下来，计算整个TCP连接期间传输的总数据量。这是通过计算第一个TCP段的序列号和最后一个ACK的确认序列号之间的差异来完成的。总数据量为153426字节 - 1字节 = 153425字节。

最后，通过将总数据量除以传输时间来计算吞吐量：153425字节 /0.191496000秒 = 801192Byte/秒。

**4. TCP congestion control in action**

1. Use the Time-Sequence-Graph (Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Consider the "fleets" of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase.

答案：在慢启动阶段，因为一直在加倍。

2. These "fleets" of segments appear to have some periodicity. What can you say about the period?

答案：周期是逐渐增加的，表示数据段的发送间隔逐渐变大，这种周期性变化受到TCP的拥塞控制算法的影响。

**二、UDP**

1. Select the first UDP segment in your trace. What is the packet number of this segment in the trace file? What type of application-layer payload or protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields there are in the UDP header? What are the names of these fields?

答案：第一个UDP分段在跟踪文件中的包号是15。这个UDP分段携带的是域名系统（DNS）应用层协议消息。

在UDP头部有以下字段：

源端口（Source Port）：58350

目标端口（Destination Port）：53

长度（Length）：43

校验和（Checksum）：0xc31d

这些是UDP头部的字段名称和值。这个UDP分段的源端口是58350，目标端口是53，长度为43字节，校验和为0xc31d。这个UDP分段携带了35字节的UDP有效载荷，是一个域名系统（DNS）查询。

2. By consulting the displayed information in Wireshark's packet content field for this packet, what is the length (in bytes) of each of the UDP header fields?

答案：源端口字段的长度为2字节。

目标端口字段的长度为2字节。

长度字段的长度为2字节。

校验和字段的长度为2字节。

因此，每个UDP头部字段的长度都是2字节

3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

答案：在UDP头部中的“Length”字段表示UDP数据报文的总长度，包括UDP头部和UDP有效载荷的长度。这个字段的值是16位，以字节为单位，包括UDP头部的8字节和UDP有效载荷的长度。这个字段的值可以通过捕获的UDP数据包来验证。根据数据包信息，UDP头部中的“Length”字段的值为43。这表示整个UDP数据包的长度为43字节，包括8字节的UDP头部和35字节的UDP有效载荷。因此，这个字段的值确实表示了UDP数据包的总长度，包括头部和有效载荷。

4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

答案：UDP负载中可以包含的最大字节数是2^16-1减去头部字节数，这将得到65535减去8等于65527字节。

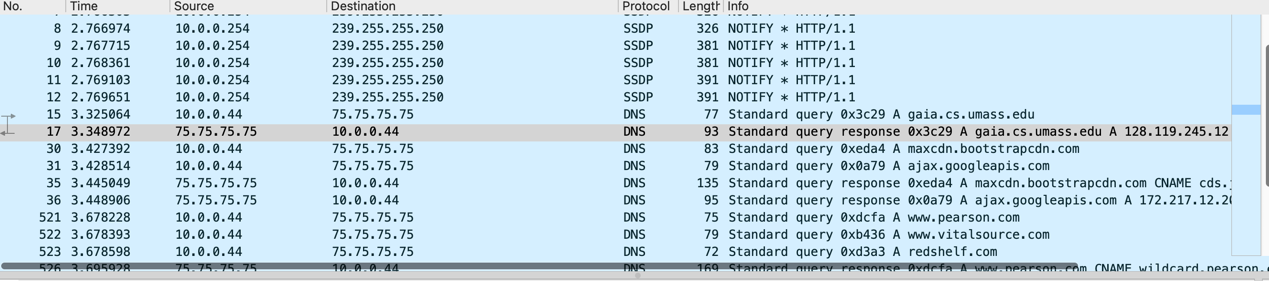
5. What is the largest possible source port number? (Hint: see the hint in 4.)

答案：最大可能的源端口号是65535。UDP头部中的源端口字段是一个16位字段，因此可以表示的端口号范围是从0到65535。所以，65535是最大可能的源端口号。

6. What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment.

答案：UDP的协议号是17。这可以从IP数据报中的协议字段（Protocol field）获得。在数据包中，IP数据报中的协议字段的值为*0x11 hex*

，表示这是一个UDP数据包。



7. Examine the pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). What is the packet number of the first of these two UDP segments in the trace file? What is the packet number of the second of these two UDP segments in the trace file? Describe the relationship between the port numbers in the two packets.

答案：第一个UDP分段在跟踪文件中的包号是15，第二个UDP分段在跟踪文件中的包号是17

对于这两个UDP分段，源端口和目标端口之间存在一种互换关系，这是标准的请求和响应通信模式。具体来说：

第一个UDP分段（发送方）的源端口是58350，目标端口是53。

第二个UDP分段（响应方）的源端口是53，目标端口是58350。

这种端口号的互换关系表示了通信的请求和响应关系，第一个UDP分段是请求，第二个UDP分段是对请求的响应。这是一个典型的客户端-服务器通信模式，其中客户端使用一个随机的源端口向服务器发送请求，服务器然后使用相同的端口号向客户端发送响应。