计网实验5

姓名：岳宇轩 学号：19020011038 指导老师：洪峰

1. **Capturing a bulk TCP transfer from your computer to a remote server**

打开http://gaia.cs.umass.edu/wiresharklabs/alice.txt，并将其中内容保存为alice.txt。

打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，选择刚刚保存的alice.txt文件

打开wireshark进行抓包，随后点击页面中的Upload alice.txt file

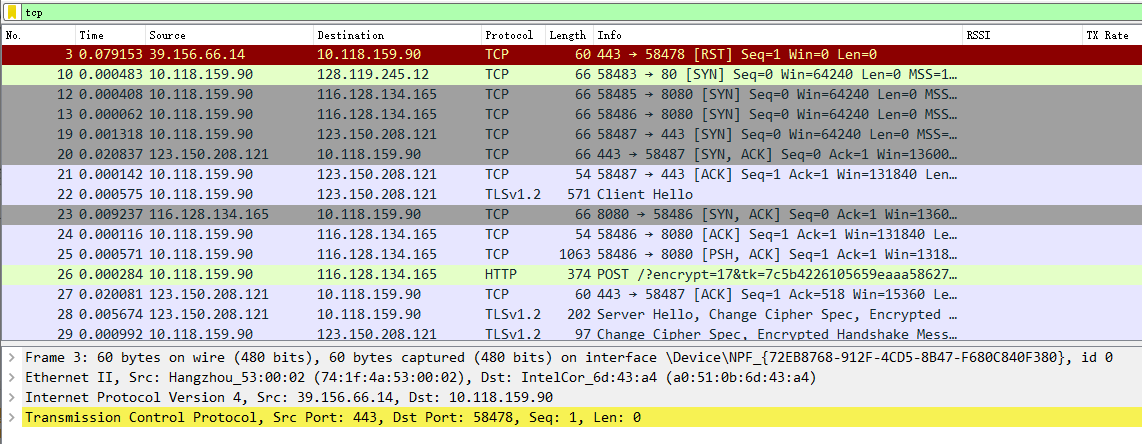
页面提示



后停止wireshark抓包

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

在筛选框中输入tcp得到下图所示结果



**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?**





**（1）IP address ： 10.118.159.90**

**（2）TCP port ： 58483**

**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?**





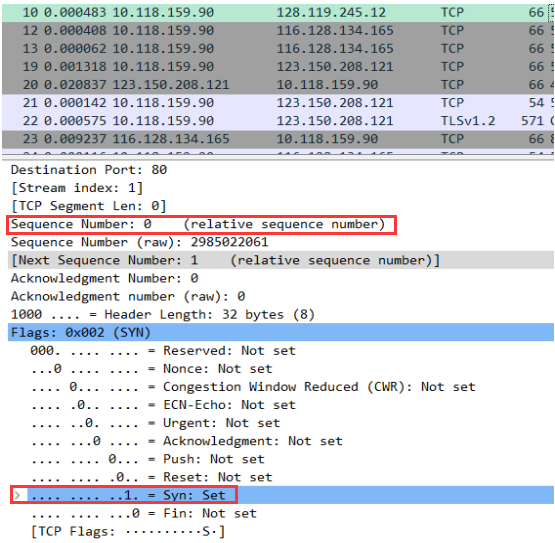
**（1）IP address ： 128.119.245.12**

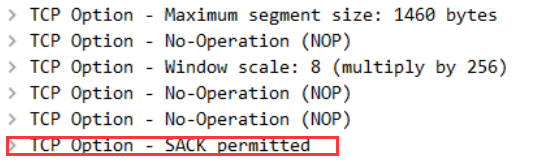
**（2）port number ： 80**

**3. TCP Basics**

**3. 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? What is it in this TCP segment that identifies the segment as aSYN segment? Will the TCP receiver in this session be able to use SelectiveAcknowledgments (allowing TCP to function a bit more like a "selective repeat”'receiver, see section 3.4.5 in the text)?**



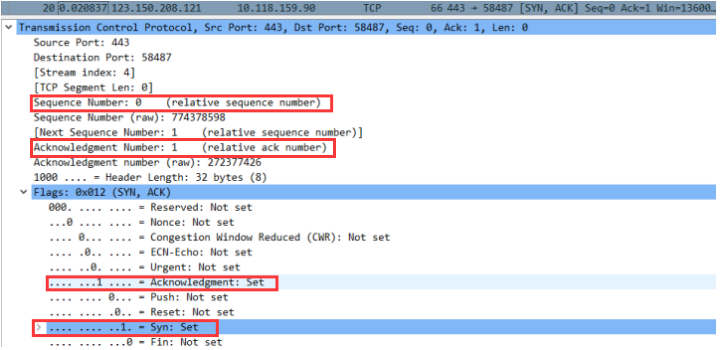


**（1）sequence number： 0**

**（2）Syn标志被置为1，表示这是一个Syn segment**

**（3）允许SelectiveAcknowledgments**

**4.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?**



**（1）sequence number：0**

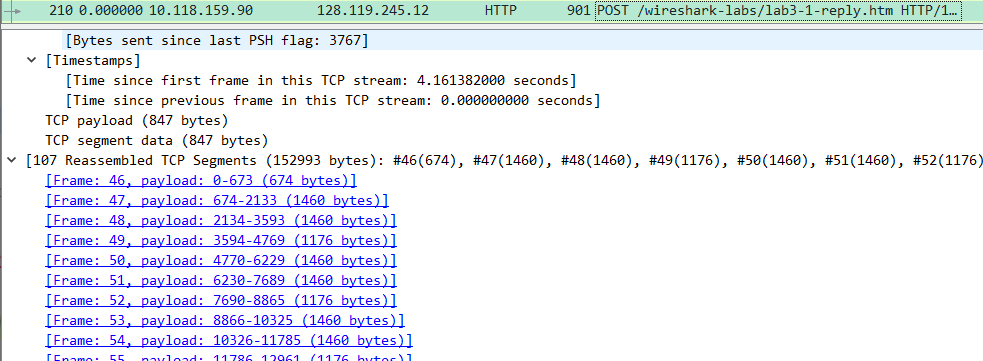
**（2）Acknowledgement和Syn标志都被置为1**

**（3）the value of the Acknowledgement field in the SYNACK segment ： 1**

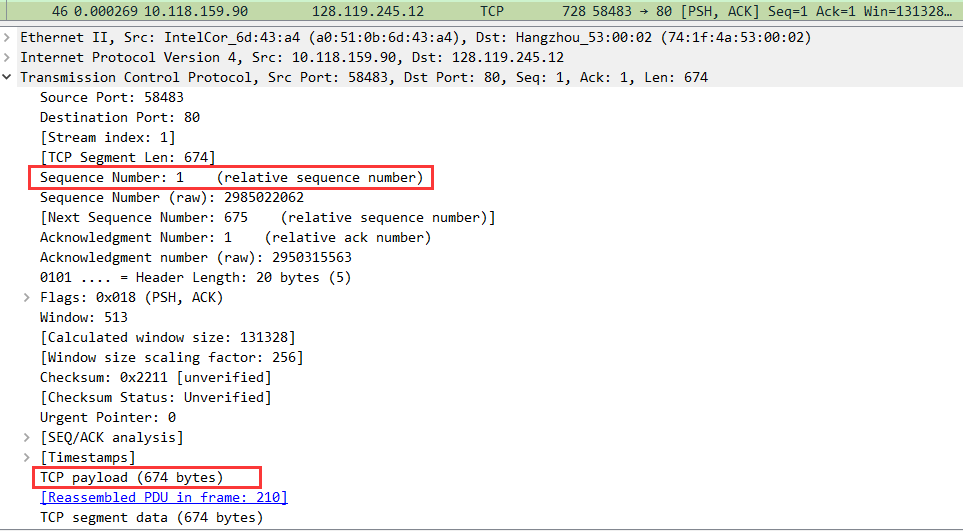
**（4）对来自client computer的initial sequence number of SYN 加一**

**5. 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 Wiresharkwindow, looking for a segment with the ASCl text "POST"within its DATAfield3+. How many bytes of data are contained in the payload (data) field of thisTCP segment? Did all of the data in the transferred file alice.txt fit into this single segment?**



找到http post请求，frame:46包含http post的tcp segment



根据下图可知



第一个TCP segment只携带了部分数据，并没有将alice.txt中的全部内容放入。

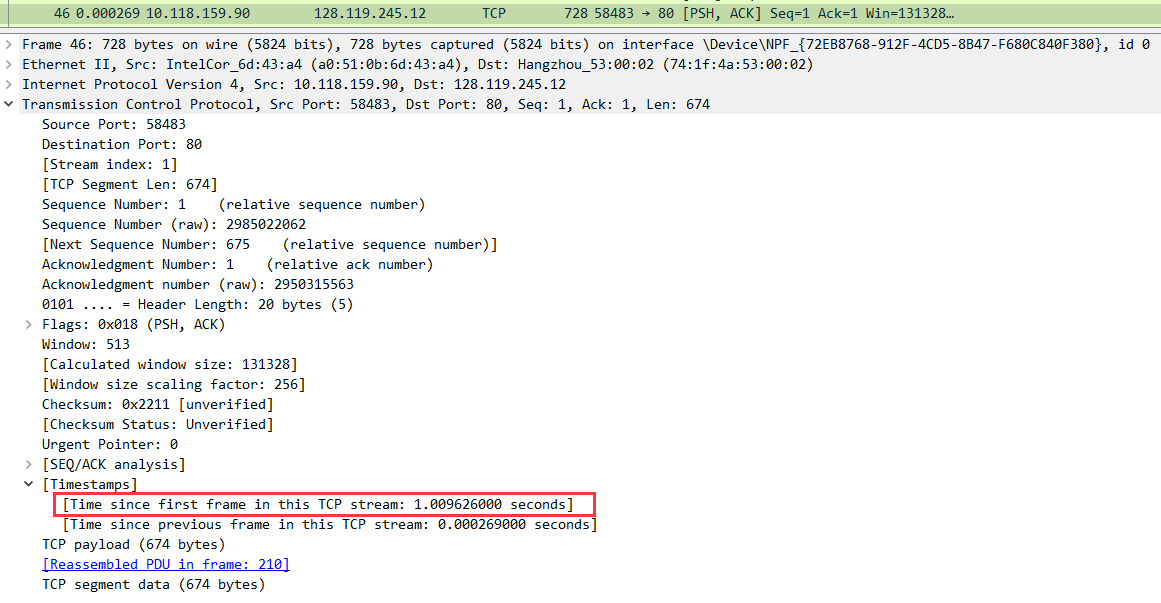
1. **sequence number : 1**
2. **674bytes**
3. **NO ，第一个TCP segment只携带了部分数据，并没有将alice.txt中的全部内容放入。**

**6. Consider the TCP segment containing the HTTP "POST"as the first segment in**

**the data transfer part of the TCP connection.**

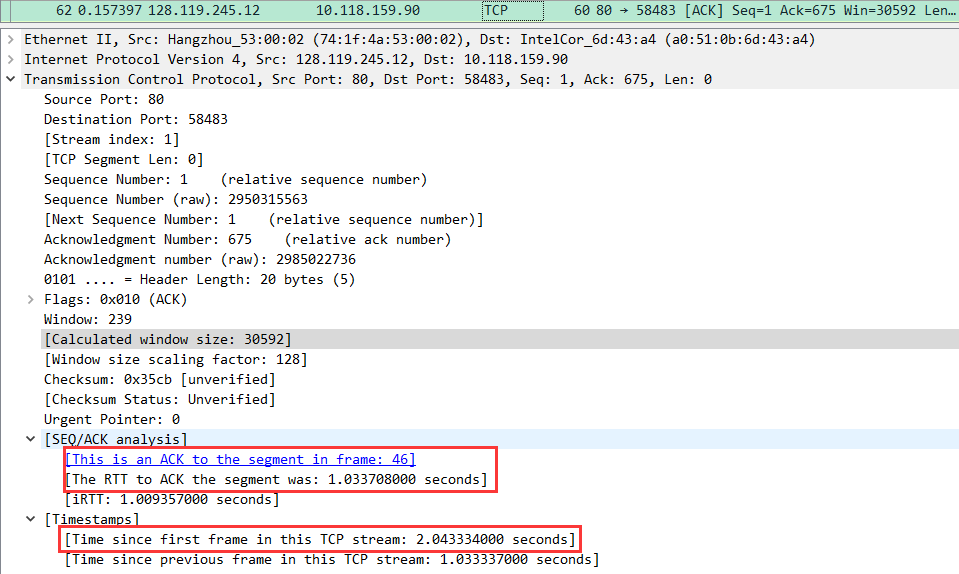
**根据第五问找到first segment编号是46，second segment编号是47**

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



46号包：**Time since first frame in this TCP stream : 1.009626seconds**

. At what time was the ACK for this first data-containing segment received?. What is the RTT for this first data-containing segment?

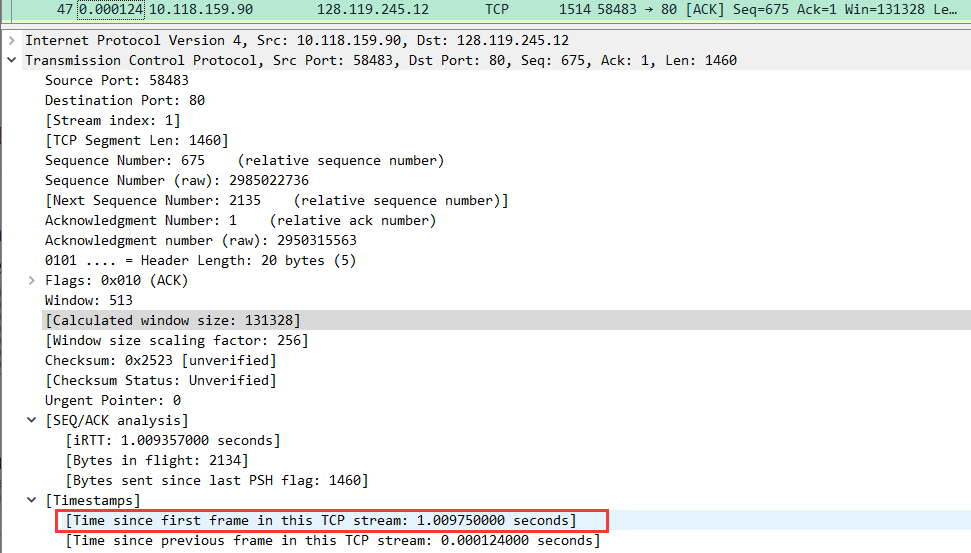


找到62号包是对46号包的ACK

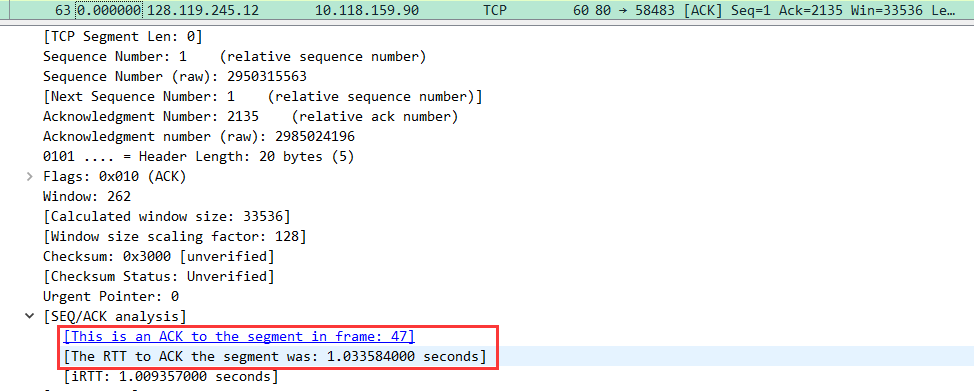
62号包：**Time since first frame in this TCP stream : 2.043334seconds**

**RTT：1.033708seconds**

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



47号包是 the second data-carrying TCP segment



63号包是对47号包的ACK，**RTT是1.033584seconds。**

. What is the Estimated RTT value(see Section 3.5.3, in the text) 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 Estimated RTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation onpage 242, and a value of a = 0.125.

Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets"window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph->Round Trip Time Graph.

EstimatedRTT = 0.875 \* EstimatedRTT + 0.125 \* SampleRTT

After the first segment received:

EstimatedRTT = 1.033708s

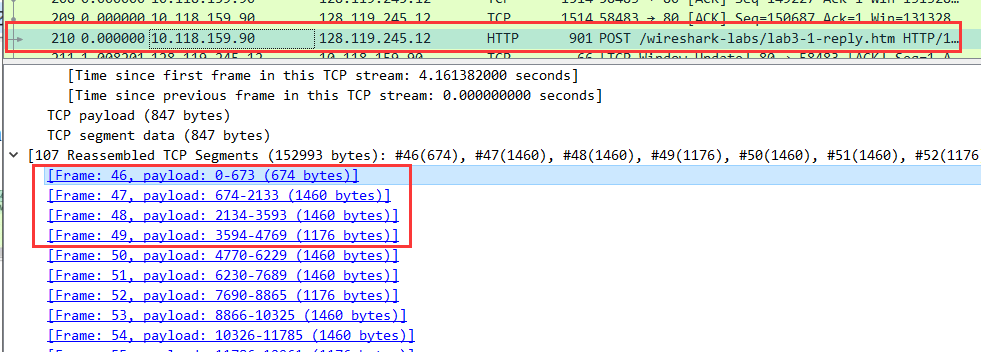
**After the second segment received:**

**EstimatedRTT = 0.875 \* 1.033708 + 0.125 \* 1.033584**

**= 1.0336925s**

**7. What is the length (header plus payload) of each of the first four data-carrying**

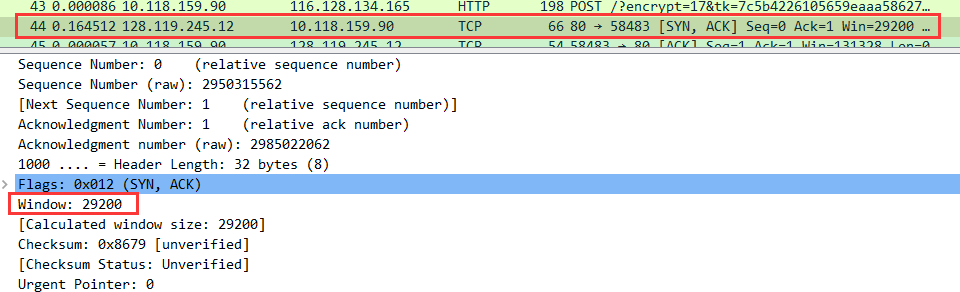
**TCP segments?**



前四个段长度分别为:**674bytes, 1460bytes, 1460bytes, 1176bytes**

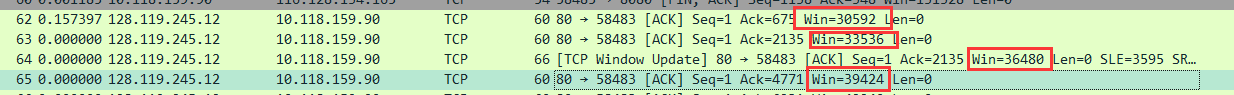
**8. What is the minimum amount of available buffer space advertised to the client by**

**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?**



（1）在44号分组传输完成后，46-47便是前四个tcp segment

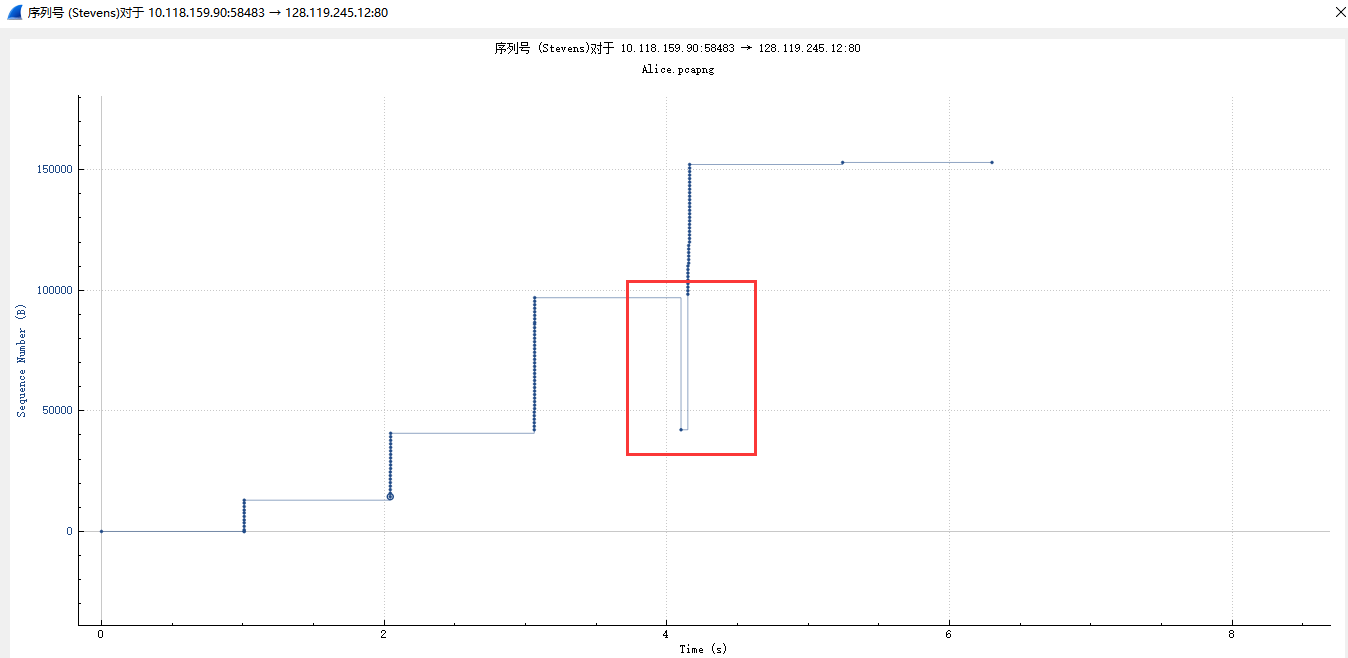
在传送前四个TCP segment之前服务器传回的的**窗口大小为29200**



（2）62是对第一个tcp segment 的ACK，65是对第四个tcp segment的ACK，可以看到在这期间窗口值稳步增长，说明**没有出现接收方窗口大小抑制发放传输速率**

**9. Are there any retransmitted segments in the trace file? What did you check for (in**

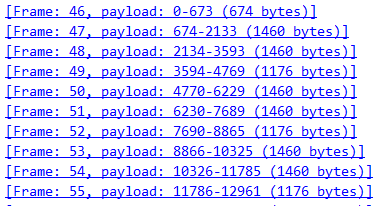
**the trace) in order to answer this question?**



**存在重传的分组，发送到服务器的sequence number并不是一直递增的，比如在图中t=4s左右发送的分组序号小于上一个的序号。**

**10.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?Can you identify cases where the receiver is ACKing every other received segment(see Table 3.2 in the text) among these first ten data-carrying segments?**



**（1）在前十个TCP segment 中接收方在一个ACK确定的最多的是1460bytes (6次），其次是1176字节 （3次），674bytes （1次）。**

观察前十个tcp segment 的ACK的sequence number 和payload之间的关系，得出下表

|  |  |  |
| --- | --- | --- |
| ACK的Frame | ACK的sequence number | receiver acking data |
| 46 | 1 | 674 |
| 47 | 675 | 1460 |
| 48 | 2135 | 1460 |
| 49 | 3595 | 1176 |
| 50 | 4771 | 1460 |
| 51 | 6231 | 1460 |
| 52 | 7691 | 1176 |
| 53 | 8867 | 1460 |
| 54 | 10327 | 1460 |
| 55 | 11787 | 1176 |

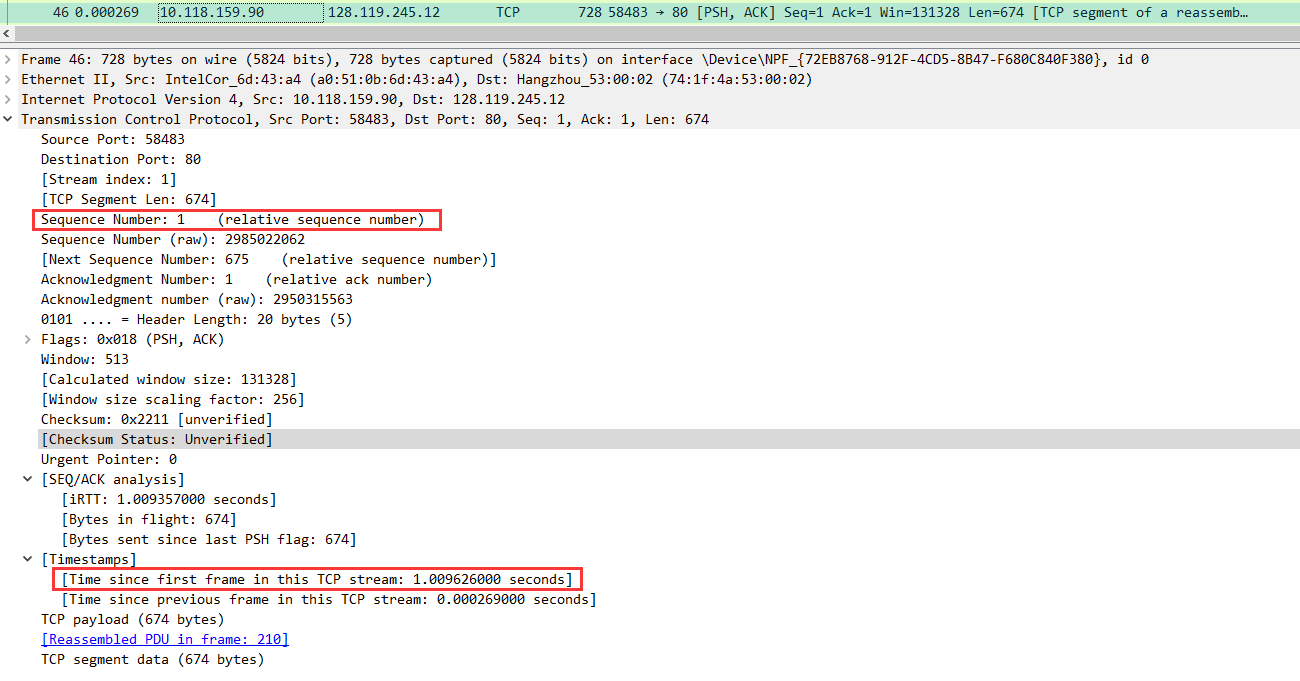
1. **观察上表可以看出：每次服务器ACK的tcp segment的sequence num增长的间隔就是前一个tcp segment 的 payload**

**11.What is the throughput (bytes transferred per unit time) for the TCP connection?**

**Explain how you calculated this value.**

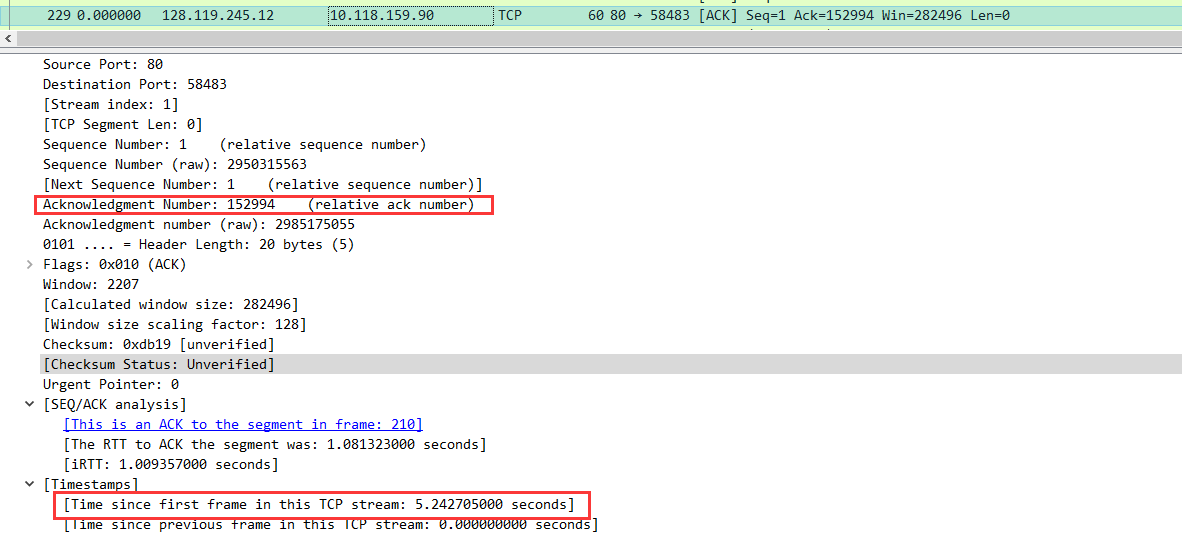
throughput = ammount of data transmitted / time

总传输数据量：首先寻找第一个tcp segment



seq为1，time为1.009626s

然后寻找最后一个ACK



ACK的tcp segment的sequence number 是152994，time是5.242705

**故throughput=(152994-1) / (5.242705-1.009626)=36142.25bytes/s**

4.TCP congestion control in action

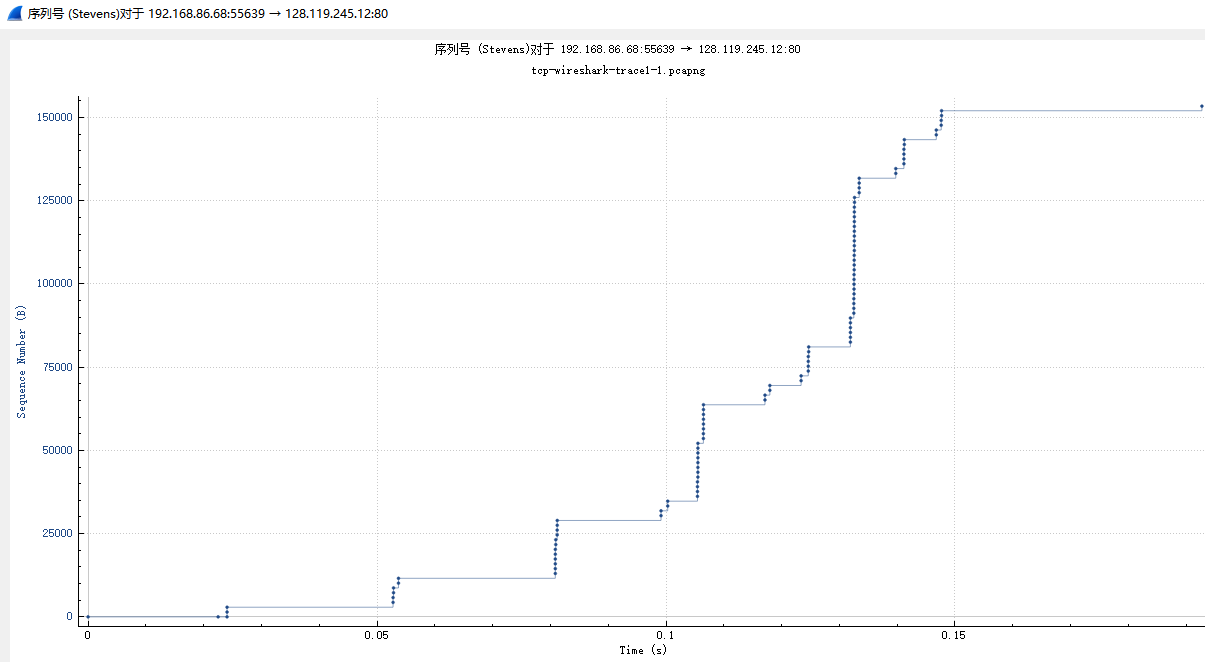
**12.Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Consider the "fleets”of packets sent around t= 0.025,t=0.053,t= 0.082 and t=0.1.Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase.Figure 6 showsa slightly different view of this data.**

首先访问

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip

下载tcp-wireshark-trace1-1

打开统计->TCP流图形->时间序列，得到下图



分析其中部分：

根据图中标出的线段：绿线，红线，橙线长度可知，在t=0.025，0.053,0.082时刻附近，sequence number成倍增长（红线长度差=2倍绿线长度，橙线长度=2倍红线长度）可知，**t=0.025，0.053,0.082时刻左右均处于慢开始阶段。**而t=1s时刻左右标出的黄线长度与开始时相近，说明在t=0.082-到t=0.1之间发生了超时，**所以在t=1时刻又回到了慢开始阶段。**

**13.These "fleets of segments appear to have some periodicity. What can you say**

**about the period?**

**总体来说：**

**tcp在开始发送报文段时先发送一个，试探网络的拥塞程度，然后成倍增加；**

**当发送数量超过了慢开始门限之后，就要执行拥塞避免，发送报文段数线性增加；**

**一旦发生超时，就要重新执行慢开始阶段；**

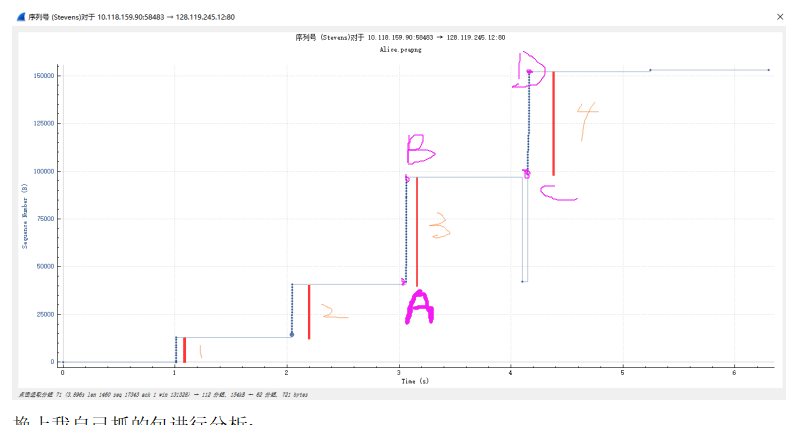
**连续收到3个重复确认，则乘法减小；**

**在发送数小于拥塞窗口时有特定发送报文段数的的加倍增大和加法增大，发送报文段数逐渐增多；而在超过拥塞窗口后又要退回去重新执行发送报文段数的增大；故呈现出一定的周期性。**

**在这张图中：**

**周期性主要表现在TCP报文段发送数小于慢开始门限时的倍增和发生超时后的退回到慢开始所表现出的周期性规律中。**

1. **Answer each of two questions above for the trace that you have gatheredwhen you transferred a file from your computer to gaia.cs.umass.edu**



**换上我自己抓的包进行分析：**

**（1）**

**1、2、3表示的线段长度逐渐倍增，可以判断在t=1s,t=2.05s,t=3.08s左右的时刻，均处于慢开始的阶段。计算A、B两点直接的sequence number之差为96911-49463=47488，C、D两点的sequence number之差为152147-99831=52316可以看出t=4.1s时刻左右，TCP发送报文段数执行加法增长，故处于拥塞避免阶段。**

**（2）**

**对周期性的分析同上题，不过我自己抓的包似乎没有周期性，只有从慢开始的倍增向拥塞避免的加法增大的变化阶段。**