实验二

TCP

**实验目的**

在这个实验室里，我们将详细探究著名的TCP协议的细节行为。通过分析对你的计算机向远程服务器传输150KB文件（包含Lewis Carrol的著作Alice’s Adventures in Wonderland 的文本）时发送和接收到的TCP报文段的跟踪来做到这一点。我们研究TCP如何使用序号和确认号来提供可靠的数据传输；亦将看到运行中的TCP拥塞控制算法“慢启动和拥塞避免”；也将粗略考察TCP连接的建立并探究在你的计算机和服务器之间TCP连接的性能（吞吐量和往返时间）。

在开始实验之前，请先复习课本中的第3.5节和第3.7节。

**实验步骤**

1. 捕获到远程服务器的批量TCP传输

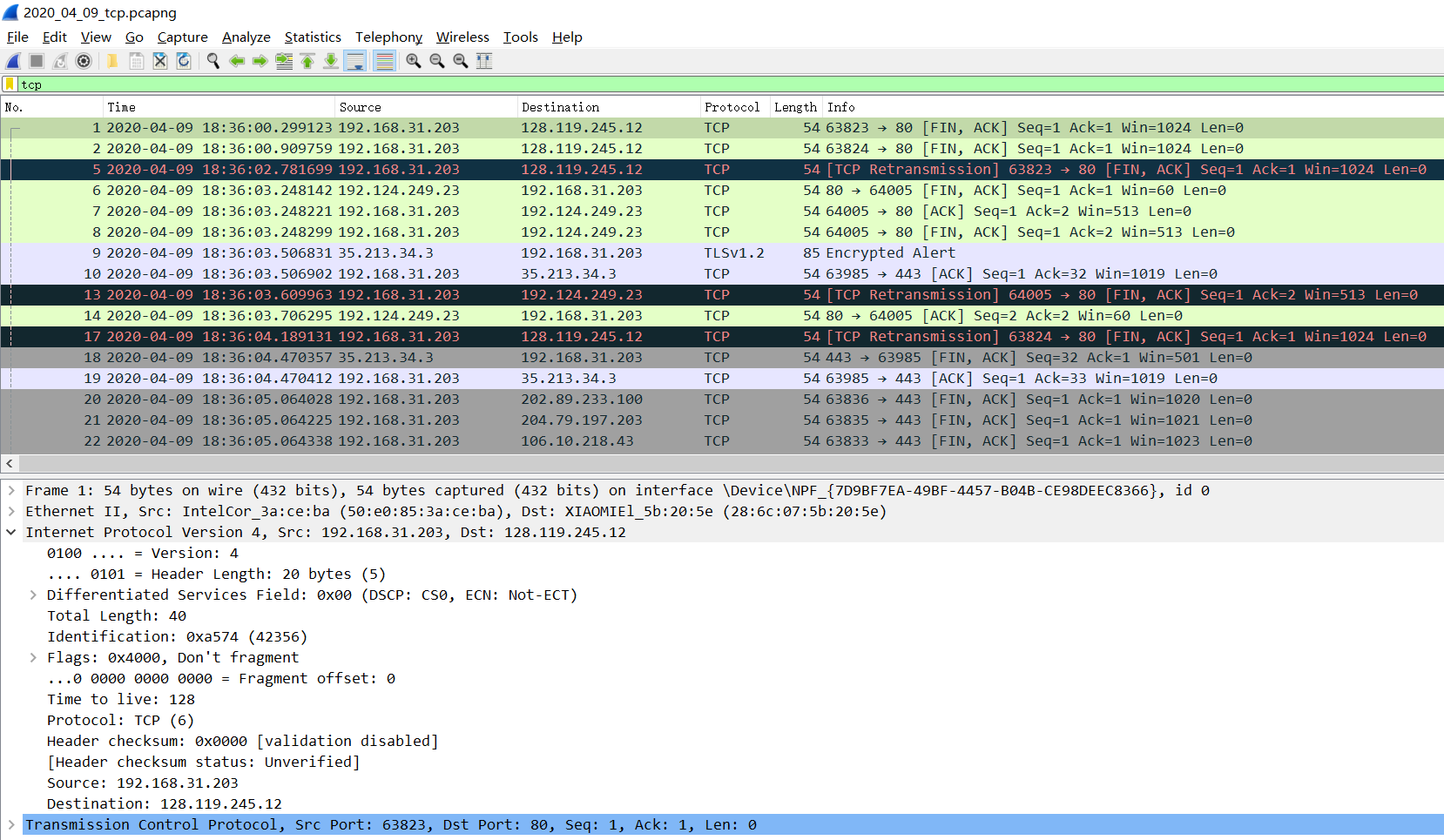
开始探究TCP之前需首先要使用Wireshark来对通过TCP上传文件到远程服务器的传输分组进行跟踪捕获。这可以通过一个网页来访问存储在电脑上的文件（爱丽丝梦游仙境的ASCII文本），然后使用HTTP POST方法将该文件传输到Web服务器（参见教材中的第2.2.3节）。使用POST方法而不是GET方法是因为希望将大量数据从你的电脑传输到另一台计算机。此间将运行Wireshark来获取对发送和接收的TCP报文段的跟踪捕获。

执行以下操作:

* 在github.com/network-distributed的lab仓库中下载附加的txt文件alice.txt，这是爱丽丝梦游仙境的ASCII文本文件, 将此文件保存到计算机
* 下一步转到 <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.
* 将看到类似下面的屏幕显示:



* 使用表单中“*Browse*”这个按钮来输入包含《爱丽丝梦游仙境》的本地电脑上的文件（含完整路径名），此时请不要点击“*Upload alice.txt file*”按钮
* 现在启动Wireshark并开始分组捕获（捕获->启动），然后在Wireshark分组捕获选项屏幕上按OK（此处不需要选择任何选项）
* 返回使用浏览器。点击 “*Upload alice.txt file*” 按钮，将该文件上传到“gaia.cs.umass.edu”服务器。一矣文件上载完后，浏览器窗口中将显示一条简短的祝贺消息
* 停止Wireshark分组捕获，此时的Wireshark窗口应该类似下面的截屏



将此捕获跟踪保存到pcapng文件中，你可能在探寻下面问题的答案时需要使用它。

1. 捕获跟踪的粗略观察

在详细分析TCP连接的行为之前，让我们先从更高的层次观察捕获跟踪的数据。

* 首先输入“tcp”（小写无引号，输入后不要忘记按回车键）到位于Wireshark窗口顶部的显示过滤规则窗口来过滤Wireshark窗口中显示的分组

现在可以观察到在你的电脑和gaia.cs.umass.edu服务器之间一系列的TCP及HTTP消息。应该能看到包含SYN消息的初始三次握手。还可以观察到一条HTTP POST消息。根据所使用的Wireshark的版本的不同，可能会看到一系列从你的电脑发送到gaia.cs.umass.edu的“HTTP Continuation”消息。回想一下之前在Wireshark HTTP实验中的讨论，并没有一个这样的HTTP Continuation消息——这里只是Wireshark表示有多个TCP报文段被用于承载同一HTTP消息的方式。在Wireshark的最新版本中，则是在Wireshark显示的Info列中看到“[TCP segment of a reassembled PDU]”（重组PDU的TCP报文段），以指示该TCP段包含属于上层协议消息（在这里是HTTP）的数据。还应该观察到TCP ACK报文段从gaia.cs.umass.edu返回到你的计算机。

通过打开第一步中保存的Wireshark捕获的分组pcapng文件，进行观察后回答以下问题。如果可能的话，当你回答一个问题时，请在你的实验报告中包含用来回答所问问题的相关分组捕获记录的打印件。要打印分组捕获记录，请点击“文件”->“打印”->“打印到pdf文件”，选择“仅选定分组”，其后选“分组摘要行”，且选择回答问题所需的分组最少详细信息量。

1. 将文件传输到gaia.cs.umass.edu的客户端计算机（源端）所使用的IP地址及TCP端口号是多少？要回答这个问题，最简单的方法是选择一条HTTP消息，并通过“details of the selected packet header window” （请参阅第一次实验课中的图2）浏览所选分组的首部详细信息并观察承载该HTTP消息的TCP分组的详细信息。
2. gaia.cs.umass.edu的IP地址是什么？使用哪个端口发送和接收此连接的TCP报文段？
3. 客户端计算机（源端）用于将文件传输到gaia.cs.umass.edu的IP地址和TCP端口号各是多少?

由于这个实验是关于TCP而不是HTTP的，改变Wireshark的“listing of captured packets”窗口，使之显示包含HTTP消息的相关TCP报文段的信息，而不是HTTP消息的信息。要让Wireshark执行此操作，请选择“分析”->“启用的协议”。然后取消选中“HTTP”框并“确定”。现在看到的Wireshark窗口看起来应该类似下面截屏:



这正是我们所寻找的 —— 在你的计算机和gaia.cs.umass.edu.之间传送的一系列TCP报文段。我们将使用所捕获的分组跟踪来研究本实验其余部分的TCP行为。

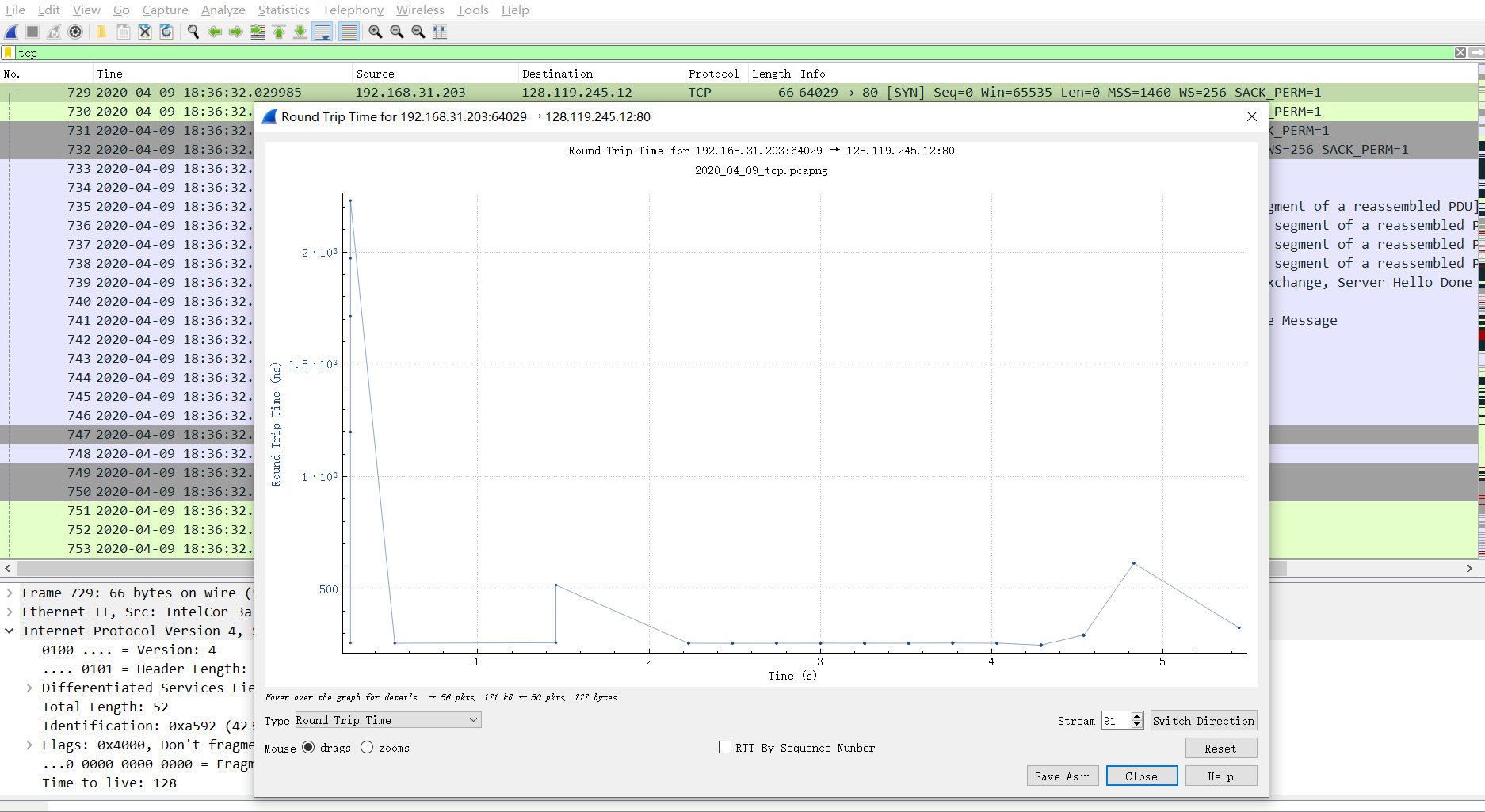
1. TCP 基础

回答关于TCP报文段的以下问题:

1. 客户端计算机与gaia.cs.umass.edu之间TCP连接的TCP SYN报文段的初始序号是多少？在报文段中是什么将其标识为SYN报文段？
2. gaia.cs.umass.edu发送给客户端计算机的SYNACK报文段的序号是多少？在SYNACK报文段中，确认号字段的值是多少？gaia.cs.umass.edu是如何确定这个值的？将该报文段中标识为SYNACK报文段的标记是什么？
3. 包含HTTP POST命令的TCP报文段的序号是多少？请注意，要找到POST命令需要深入Wireshark窗口底部的packet content字段，寻找在数据字段中带有“POST”的报文段。
4. 将包含HTTP POST的TCP报文段视为TCP连接中的第一个报文段。TCP连接的前六个报文段（包括包含HTTP POST的报文段）的序号是多少？每个报文段是何时发送的？每个报文段的确认是何时收到的？给出每个TCP报文段的发送的时间与接收到其确认的时间之差，六个报文段中的每个报文段的RTT值各是多少？收到每个ACK后的EstimatedRTT值是多少（见教材第3.5.3节）？·假设EstimatedRTT的值等于第一个报文段的RTT测量值，然后使用教材中的公式计算所有后续报文段的EstimatedRTT。

*注：*Wireshark有一个很友好的功能，允许为发送的每个TCP段绘制RTT图。在“listing of captured packets”窗口中选择一个TCP报文段，该TCP报文段正在从客户端发送到gaia.cs.umass.edu服务器。然后选择：统计信息->TCP流图->RTT图（*Statistics->TCP Stream Graph->Round Trip Time Graph*）。

1. 前六个TCP报文段每个的长度是多少?[[1]](#footnote-1)
2. 整个跟踪捕获过程中所接收到的最小可用缓冲空间是多少？接收缓冲空间的缺乏是否会限制发送者？
3. 是否有重传的报文段？为回答这个问题你查询了什么？
4. 接收端通常在ACK中确认多少数据？能识别出接收端每收到一个报文段后都进行了确认的情况吗（参见教材表3.2）
5. TCP连接的吞吐量（单位时间传输的字节数）是多少？解释是如何计算到这个值的。



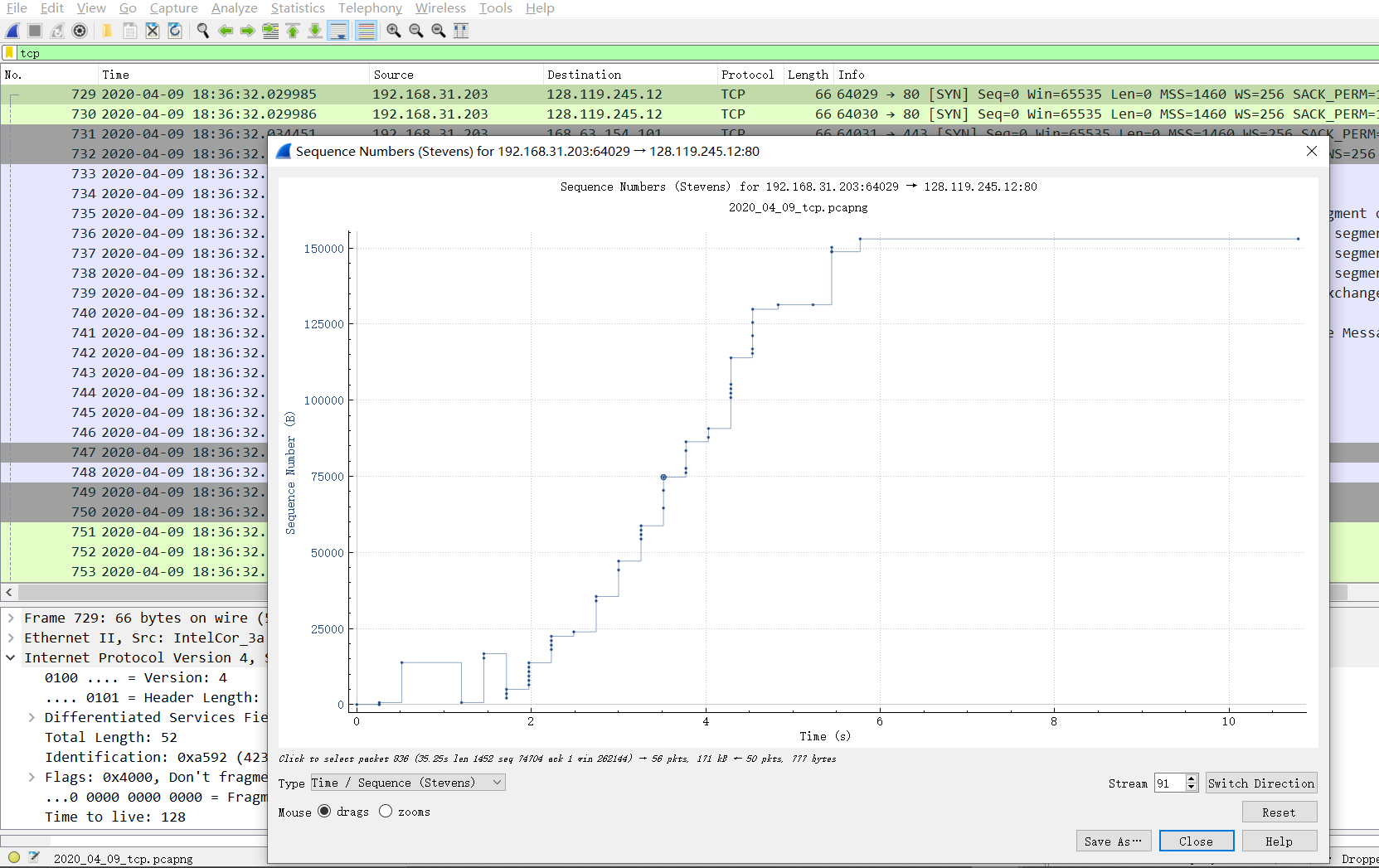
1. 运行中的TCP 拥塞控制

现在来检查每单位时间从客户端发送到服务器的数据量。我们将不是根据Wireshark窗口中的原始数据来计算，而是使用Wireshark的TCP绘图工具之一的时间序列图*Time-Sequence-Graph*（Stevens）来绘制数据。

* 在Wireshark “listing of captured-packets” 窗口中选择一TCP报文段。点击菜单:*Statistics->TCP Stream Graph-> Time-Sequence-Graph(Stevens*)：会看到类似于下图的绘图，它是从http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip中捕获的分组跟踪*tcp-ethereal-trace-1*中的分组创建的：



这里，每个点代表一个发出的TCP报文段，绘制了报文段的序号与发出的时间。请注意，堆叠在一起的一组点表示发送者盲发的一列分组。



请使用http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip中的分组跟踪*tcp-ethereal-trace-1*来回答以下有关TCP报文段的问题，

1. 使用*Time-Sequence-Graph ( Stevens* )绘图工具查看从客户端发送到gaia.cs.umass.edu服务器的报文段的序号与时间曲线。你能确定TCP的慢启动阶段开始和结束的位置，以及拥塞避免接续的位置吗？也请对测量数据与我们在教材中学到的TCP理想行为的不同之处进行评论。
2. 使用你所获取从计算机向gaia.cs.umass.edu传输文件时捕获到的跟踪信息来回答以上每个问题。

1. 如果你的跟踪显示TCP长度大于1500字节（40字节的TCP/IP首部数据和1460字节的TCP负载），并且你的计算机使用的是以太网连接，则Wireshark有可能报告错误的TCP报文段长度；它可能只显示一个大的TCP报文段，而不是多个小的报文段。你的计算机可能确实发送了多个小的报文段，正如它收到的ACK所示。报告的段长度不一致是由于以太网驱动程序和Wireshark软件之间的交互所致。 [↑](#footnote-ref-1)