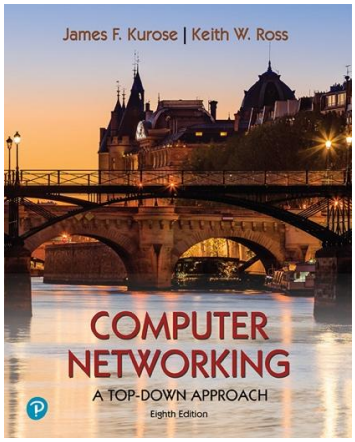
Wireshark 实验室：

传输控制协议v8.1

补充*计算机网络：自上而下的方法，8th编辑*，JF 黑濑和 KW 罗斯



*“告诉我，我就忘记了。给我看，我就记住了。让我参与，我就能理解。”*中国谚语

在本实验中，我们将详细研究著名的 TCP 协议的行为。我们将通过分析在传输 150KB 文件（包含 Lewis Carrol 的文本）时发送和接收的 TCP 段的踪迹来实现这一点。*爱丽丝梦游仙境*）从您的计算机到远程服务器。我们将研究 TCP 使用序列号和确认号来提供可靠的数据传输；我们将看到 TCP 的拥塞控制算法（慢启动和拥塞避免）的实际应用；我们将了解 TCP 的接收者通告流量控制机制。我们还将简要考虑 TCP 连接设置，并研究计算机和服务器之间 TCP 连接的性能（吞吐量和往返时间）。

在开始本实验之前，您可能需要回顾一下文本中的 3.5 和 3.7 节[1]。

1. 捕获从计算机到远程服务器的批量 TCP 传输

在开始探索 TCP 之前，我们需要使用 Wireshark 获取文件从计算机到远程服务器的 TCP 传输的数据包跟踪。您可以通过访问一个网页来完成此操作，该网页允许您输入计算机上存储的文件的名称（其中包含以下内容的 ASCII 文本）：*爱丽丝漫游仙境*），然后使用 HTTP POST 方法将文件传输到 Web 服务器（参见正文中的 2.2.3 节）。我们使用 POST 方法而不是 GET 方法，因为我们想要传输大量数据*从*您的计算机到另一台计算机。当然，我们将在此期间运行 Wireshark 来获取从您的计算机发送和接收的 TCP 段的跟踪信息。

请执行下列操作：

---

[1]对图和章节的引用适用于 8th我们文本的版本，*计算机网络，自上而下的方法，8th编辑，JF Kurose 和 KW Ross，Addison-Wesley/Pearson，2020*。我们这本书的网站是 http://gaia.cs.umass.edu/kurose_ross 您会在那里找到很多有趣的开放材料。

- 启动您的网络浏览器。去http://gaia.cs.umass.edu/wiresharklabs/alice.txt 并检索 ASCII 副本*爱丽丝漫游仙境。*将其作为 .txt 文件存储在计算机上的某个位置。
- 接下来前往http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-
- file1.html 。您应该看到如图 1 所示的屏幕。

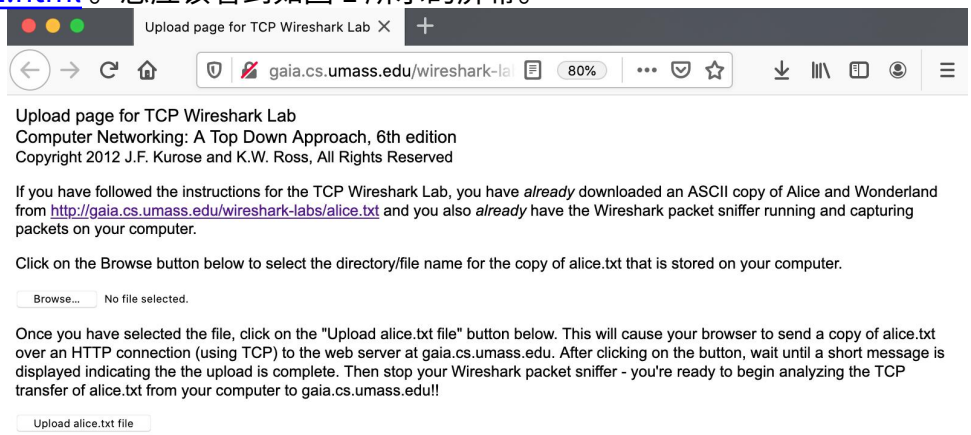


图1：用于将 alice.txt 文件从您的计算机上传到的页面 gaia.cs.umass.edu

- 使用*浏览*将此表单中的按钮添加到您刚刚创建的计算机上的文件中，其中包含*爱丽丝漫游仙境。*不要按“*上传 alice.txt 文件*”按钮还没有。

- 现在启动 Wireshark 并开始数据包捕获（如果您需要复习如何执行此操作，请参阅之前的 Wireshark 实验）。
- 返回浏览器，按“*上传 alice.txt 文件*”按钮将文件上传到 gaia.cs.umass.edu 服务器。文件上传后，浏览器窗口中将显示一条简短的祝贺消息。
- 停止 Wireshark 数据包捕获。您的 Wireshark 窗口应类似于图 2 中所示的窗口。

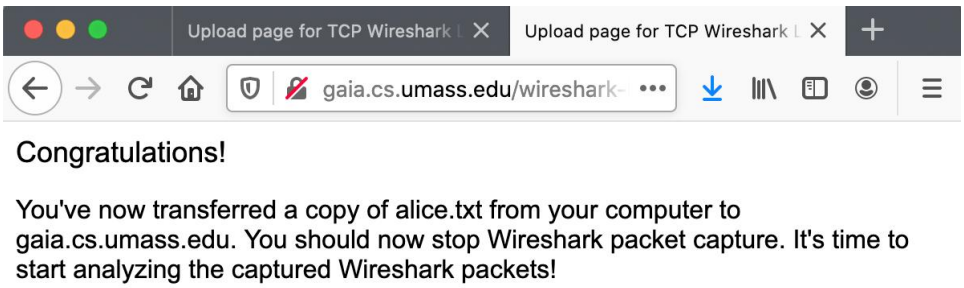


图2：成功！您已将文件上传到 gaia.cs.umass.edu 并已希望在此过程中捕获 Wireshark 数据包跟踪。

如果您无法在实时网络连接上运行 Wireshark，您可以下载在作者的一台计算机上执行上述步骤时捕获的数据包跟踪[2]。此外，您可能会发现下载此跟踪很有价值，即使您已捕获自己的跟踪并使用它，以及在探索以下问题时您自己的跟踪。

2. 首先查看捕获的轨迹

在详细分析 TCP 连接的行为之前，让我们对跟踪进行高级查看。

我们首先查看将 alice.txt 文件从计算机上传到 gaia.cs.umass.edu 的 HTTP POST 消息。在 Wireshark 跟踪中找到该文件，然后展开 HTTP 消息，以便我们可以更仔细地查看 HTTP POST 消息。您的 Wireshark 屏幕应类似于图 3。

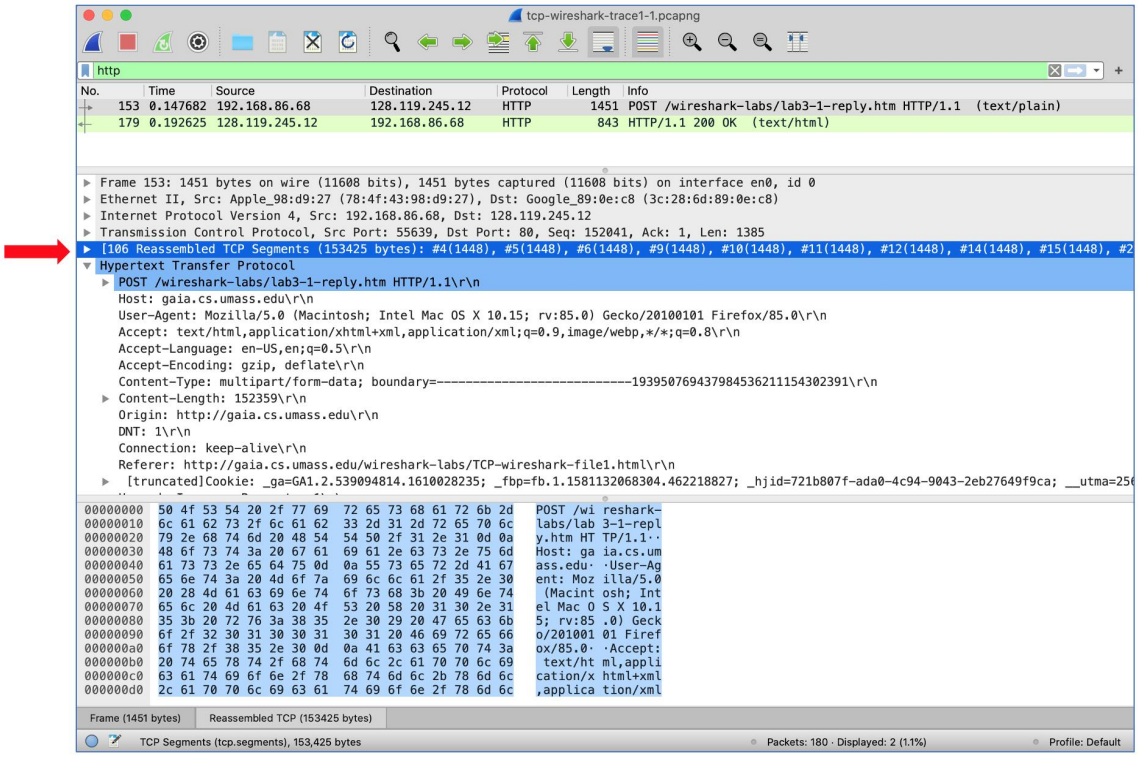


图3：展开从您的计算机上传 alice.txt 的 HTTP POST 消息
前往 gaia.cs.umass.edu

---

[2]您可以下载 zip 文件http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip 并提取跟踪文件*tcp-wireshark-trace1-1*。此跟踪文件可用于回答此 Wireshark 实验，而无需您自己实际捕获数据包。此跟踪是使用在作者的一台计算机上运行的 Wireshark 进行的，同时执行此 Wireshark 实验室中指示的步骤。下载跟踪文件后，您可以将其加载到 Wireshark 中并使用以下命令查看跟踪：*文件*下拉菜单，选择*打开*，然后选择跟踪文件名。

这里有几点需要注意：

- 应用程序层 HTTP POST 消息的正文包含文件 alice.txt 的内容，该文件是一个超过 152K 字节的大文件。好吧 – 不是*那*很大，但是对于仅包含在一个 TCP 段中的这一条 HTTP POST 消息来说太大了！

- 事实上，如图 3 中的 Wireshark 窗口所示，我们看到 HTTP POST 消息分布在 106 个 TCP 段上。这显示在图 3 中红色箭头所在的位置 [旁白：Wireshark 没有这样的红色箭头；我们将其添加到图中以提供帮助 -]。如果您更仔细地观察，您会发现 Wireshark 对您也非常有帮助，它告诉您包含 POST 消息开头的第一个 TCP 段是图 3 中示例的特定跟踪中的数据包 #4 ，这是痕迹 *tcp-wireshark-trace1-1*脚注 2 中注明。第二个 TCP 段包含跟踪中数据包 #5 中的 POST 消息，依此类推。

现在让我们“亲自动手”查看一些 TCP 段。

- 首先，通过在 Wireshark 窗口顶部的显示过滤器规范窗口中输入“tcp”（小写，无引号，不要忘记输入后按回车键！）来过滤 Wireshark 窗口中显示的数据包。您的 Wireshark 显示应类似于图 4。在图 4 中，我们注意到设置了 SYN 位的 TCP 段 – 这是三向握手中的第一个 TCP 消息，用于建立与 gaia.cs 的 TCP 连接.umass.edu 最终将携带 HTTP POST 消息和 alice.txt 文件。我们还注意到 SYNACK 段（TCP 三向握手中的第二步），以及携带 POST 消息的 TCP 段（数据包#4，如上所述）和 alice.txt 文件的开头。当然，如果您使用自己的跟踪文件，数据包编号将会不同，但您应该会看到与图 3 和图 4 中所示类似的行为。

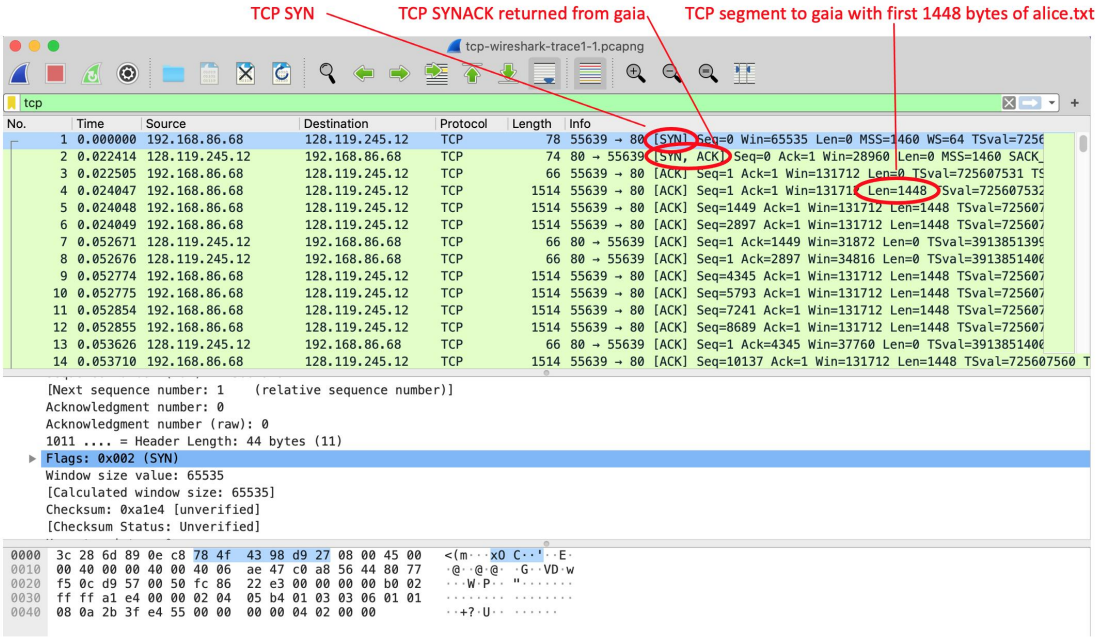


图4：发送 HTTP POST 消息所涉及的 TCP 段（包括文件 alice.txt) 到 gaia.cs.umass.edu

回答下列问题[3]，无论是来自您自己的实时跟踪，还是通过打开 Wireshark 捕获的数据包文件*tcp-wireshark-trace1-1*在 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip

1. 将 alice.txt 文件传输到 gaia.cs.umass.edu 的客户端计算机（源）使用的 IP 地址和 TCP 端口号是什么？要回答这个问题，最简单的方法可能是选择一条 HTTP 消息并探索该消息的详细信息
   用于携带此 HTTP 消息的 TCP 数据包，使用“所选数据包标头窗口的详细信息”（如果您不确定 Wireshark 窗口，请参阅“Wireshark 入门”实验室中的图 2）。
2. gaia.cs.umass.edu的IP地址是多少？它在哪个端口号上发送和接收此连接的 TCP 段？

由于本实验涉及 TCP 而不是 HTTP，因此现在更改 Wireshark 的“捕获的数据包列表”窗口，使其显示有关包含 HTTP 消息的 TCP 段的信息，而不是有关 HTTP 消息的信息，如图 4 所示

[3]对于作者的课程，当通过交作业回答以下问题时，学生有时需要打印出特定的数据包（有关如何执行此操作的说明，请参阅介绍性 Wireshark 实验室）并指出他们在数据包中找到了回答问题的信息。他们通过用笔标记纸质副本或用彩色字体的文本注释电子副本来做到这一点。还有供教师使用的学习管理系统 (LMS) 模块，允许学生在线回答这些问题，并为这些 Wireshark 实验室自动评分答案

http://gaia.cs.umass.edu/kurose_ross/lms.htm

多于。这就是我们正在寻找的——在您的计算机和 gaia.cs.umass.edu 之间发送的一系列 TCP 段！

3. TCP 基础知识

回答以下关于 TCP 段的问题：

3. 什么是*序列号*用于启动客户端计算机和 gaia.cs.umass.edu 之间 TCP 连接的 TCP SYN 段的长度？ （注意：这是 TCP 段本身携带的“原始”序列号；它是*不是*“No.”中的数据包# Wireshark 窗口中的列。请记住，TCP 或 UDP 中没有“数据包号”这样的东西；如你所知，那里*是*TCP 中的序列号，这就是我们所追求的。另请注意，这不是相对于该 TCP 会话的起始序列号的相对序列号。）。这个 TCP 报文段中的什么内容将该报文段标识为 SYN 报文段？此会话中的 TCP 接收方是否能够使用选择性确认（允许 TCP 的功能更像“选择性重复”接收方，请参阅文本中的第 3.4.5 节）？

4. 什么是*序列号*gaia.cs.umass.edu 发送到客户端计算机以回复 SYN 的 SYNACK 段的长度？段中是什么将段标识为 SYNACK 段？ SYNACK 段中的确认字段的值是多少？ gaia.cs.umass.edu 如何确定该值？

5. 包含HTTP POST 命令头的TCP 段的序列号是多少？请注意，为了找到 POST 消息标头，您需要深入了解 Wireshark 窗口底部的数据包内容字段，*查找其 DATA 字段中包含 ASCII 文本“POST”的段*[4,5]。该 TCP 报文段的有效负载（数据）字段中包含多少字节的数据？传输的文件 alice.txt 中的所有数据是否都适合这个单独的段？

6. 将包含 HTTP“POST”的 TCP 段视为 TCP 连接数据传输部分的第一个段。

   - TCP 连接数据传输部分中的第一个数据段（包含 HTTP POST 的数据段）何时发送？
   - 第一个包含数据的段的 ACK 是在什么时间收到的？第一个包含数据的分
   - 段的 RTT 是多少？
   - 第二个承载数据的 TCP 段及其 ACK 的 RTT 值是多少？是什么估计RTT收
   - 到第二个数据承载段的 ACK 后的值（参见正文中的第 3.5.3 节）？假设在收到第二段的 ACK 后进行此计算，

---

[4]*暗示：*在从服务器收到 SYNACK 段后，客户端很快（但并不总是立即）发送此 TCP 段。

[5]请注意，如果您过滤为仅显示“http”消息，您将看到 Wireshark 与 HTTP POST 消息关联的 TCP 段是*最后的*连接中的 TCP 段（其中包含位于*结尾*alice.txt：“THE END”）和*不是*连接中的第一个数据承载段。学生（和老师！）经常发现这出乎意料和/或令人困惑。

的初始值估计RTT等于第一段测量的 RTT，然后使用以下公式计算估计RTT第 242 页上的方程，值为 - = 0.125。

笔记： Wireshark 有一个很好的功能，允许您绘制每个发送的 TCP 段的 RTT。在“捕获的数据包列表”窗口中选择从客户端发送到 gaia.cs.umass.edu 服务器的 TCP 段。然后选择：*统计->TCP流图->往返时间图。*

7. 前四个承载数据的 TCP 段中每个段的长度（标头加有效负载）是多少？[6]

8. gaia.cs.umass.edu 在前四个数据承载 TCP 段中向客户端通告的最小可用缓冲区空间是多少[7]？接收方缓冲区空间的缺乏是否会限制前四个数据传输段的发送方？

9. 跟踪文件中是否有重传的段？为了回答这个问题，您（在跟踪中）检查了什么？
10. 在从客户端发送到 gaia.cs.umass.edu 的前 10 个数据承载段中，接收方通常会在 ACK 中确认多少数据？您能否识别出接收方在这前 10 个数据承载段中每隔一个接收到的段（参见正文中的表 3.2）进行 ACK 的情况？

11. TCP 连接的吞吐量（单位时间传输的字节数）是多少？解释一下你是如何计算这个值的。

4. TCP 拥塞控制的实际应用

现在让我们检查一下每单位时间从客户端发送到服务器的数据量。我们将使用 Wireshark 的 TCP 图形实用程序之一，而不是（乏味地！）从 Wireshark 窗口中的原始数据计算这一点 -*时序图（Stevens*)——绘制数据。

- 在 Wireshark 的“捕获数据包列表”窗口中选择客户端发送的 TCP 段，该窗口对应于从客户端到 gaia.cs.umass.edu 的 alice.txt 传输。然后选择菜单：*统计->TCP流图->时序图(Stevens*[8]）。您应该看到类似于图 5 中的图的图，该图是根据数据包跟踪中捕获的数据包创建的*tcpwireshark-trace1-1*。您可能需要扩大、缩小和调整轴中显示的间隔，才能使图表看起来如图 5 所示。

---

[6]tcp-wireshark-trace1-1 跟踪文件中的 TCP 段均小于 1480 字节。这是因为收集跟踪的计算机有一个接口卡，该接口卡将最大 IP 数据报的长度限制为 1500 字节，并且有一个*最低限度*40 字节的 TCP/IP 标头数据。对于 Internet IP 数据报来说，这个 1500 字节值是相当典型的最大长度。

[7]给出 Wireshark 报告的“窗口大小值”值，然后必须将该值乘以窗口缩放因子，以给出 gaia.cs.umass.edu 上用于此连接的实际可用缓冲区字节数。

[8]William Stevens 写了一本关于 TCP 的“圣经”书，被称为*TCP图解*。

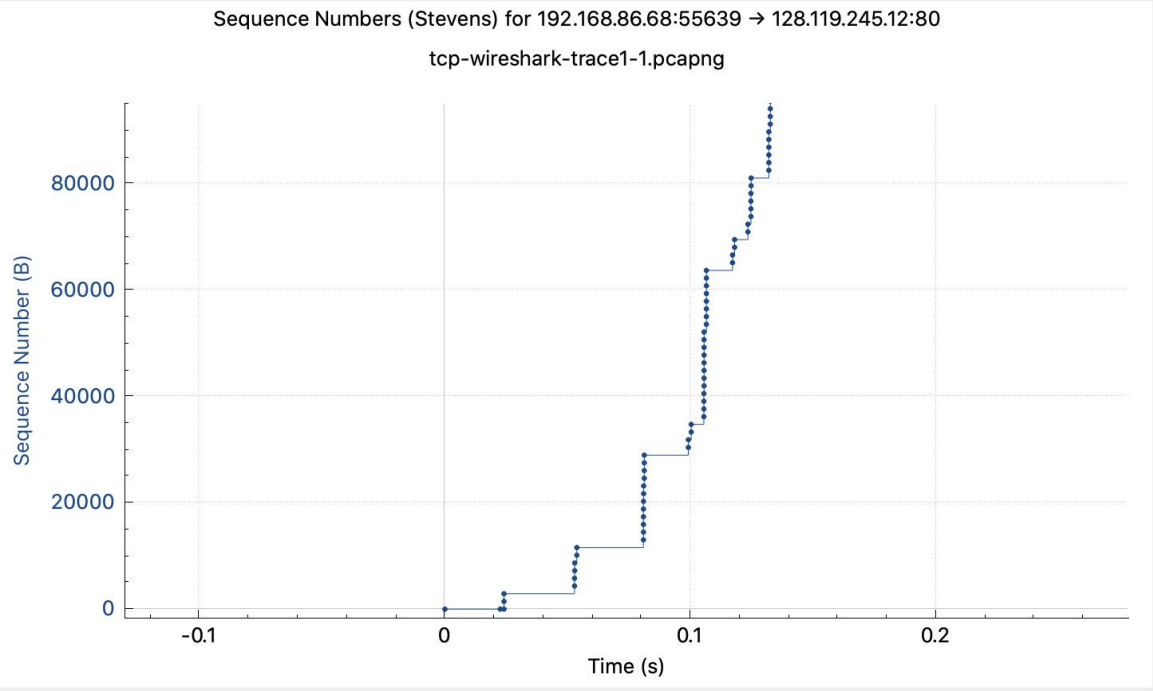


图 5：TCP 段的序列号与时间图（史蒂文斯格式）。

这里，每个点代表一个发送的 TCP 段，绘制该段的序列号与发送时间的关系。请注意，一组彼此堆叠的点表示由发送方连续发送的一系列数据包（有时称为数据包“队列”）。

针对数据包跟踪中的 TCP 段回答以下问题*tcp-wiresharktrace1-1*（见前面的脚注[2]）

12. 使用*时序图（Stevens*）绘图工具，用于查看从客户端发送到 gaia.cs.umass.edu 服务器的片段的序列号与时间图。考虑发送的数据包的“舰队” t=0.025, t = 0.053, t=0.082 和 t=0.1。评论一下这看起来 TCP 是否处于慢启动阶段、拥塞避免阶段或其他阶段。图 6 显示了该数据的略有不同的视图。

13. 这些分段“舰队”似乎具有一定的周期性。对于这段时期你有什么想说的吗?
14. 回答上述两个问题，了解您将文件从计算机传输到 gaia.cs.umass.edu 时收集的跟踪信息

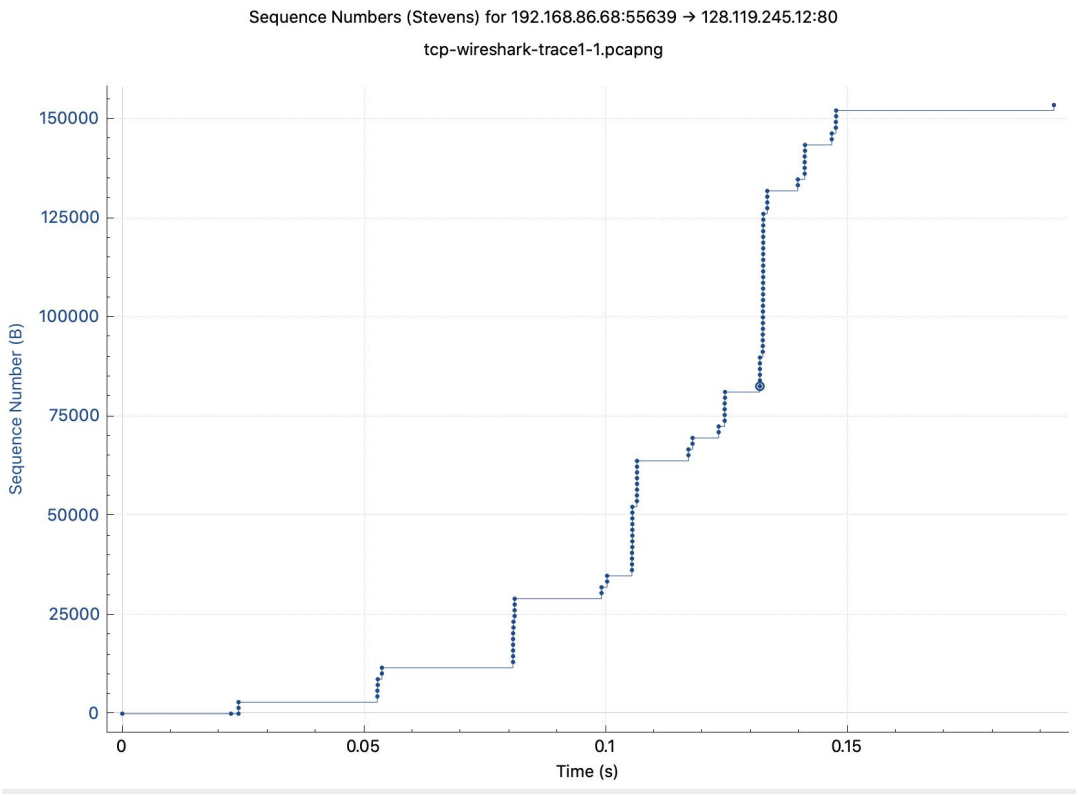


图 6：与图 5 中相同数据的另一个视图。