**中国科学技术大学计算机学院**

**计算机网络实验报告**

**实验三**

**利用Wireshark观察TCP报文**

**学 号：JL19110004**

**姓 名：徐语林**

**专 业：计算机科学与技术**

**指导老师：张信明**

**中国科学技术大学计算机学院**

**2020 年 11 月 15 日**

1. 实验目的

通过捕获以及观察分析TCP报文，更加深入的理解TCP的细节，例如：TCP的报文结构，TCP的三次握手过程，TCP的流量控制机制以及TCP的拥塞控制算法慢启动和拥塞避免。

1. 实验原理

Wireshark是一种非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的各种详细信息。Wireshark使用Npcap作为接口，直接与网卡进行数据报文交换，监听共享网络上传送的数据包

1. 实验条件

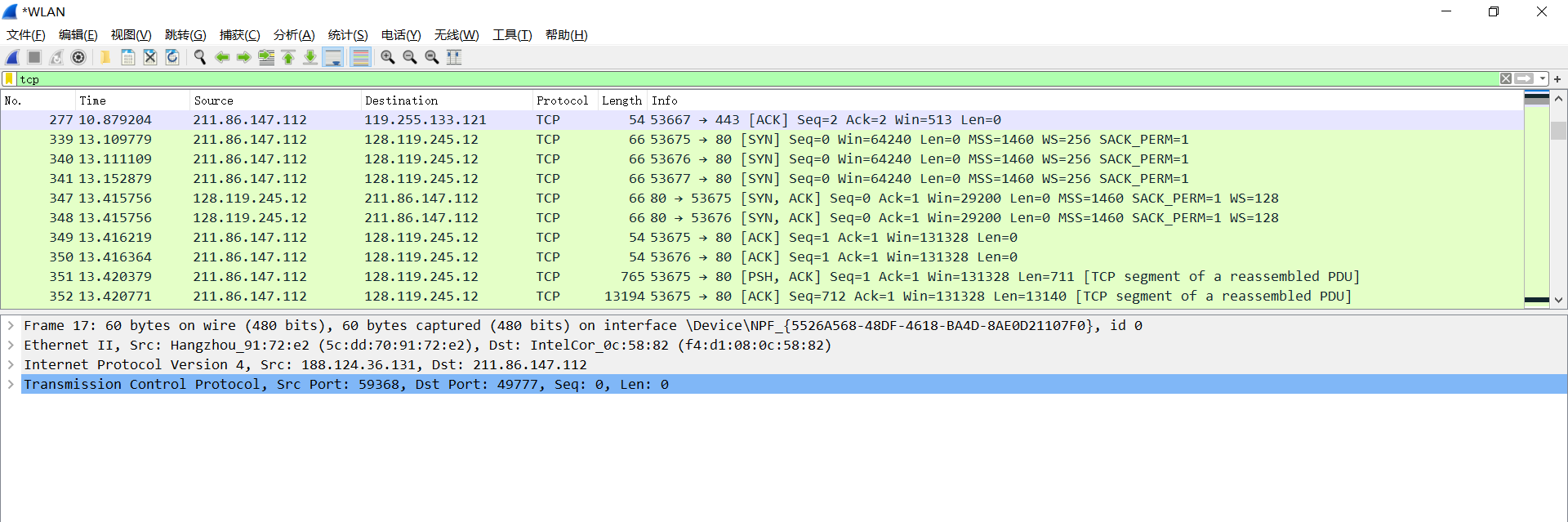
1、 硬件条件：一台PC机

2、 软件条件：win10, wireshark软件

1. 实验过程
2. 访问[http://gaia.cs.umass.edu/wiresharklabs/alice.txt](http://gaia.cs.umass.edu/wiresharklabs/alice.txt ) 下载alice.txt，存在本地：



1. 访问<http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，选择文件alice.txt>；
2. 打开wireshark开始捕获
3. 切回浏览器开始上传
4. 停止wireshark捕获，如下：



1. 回答问题

1.What is the IP address and TCP port number used by the client computer (source)

that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s

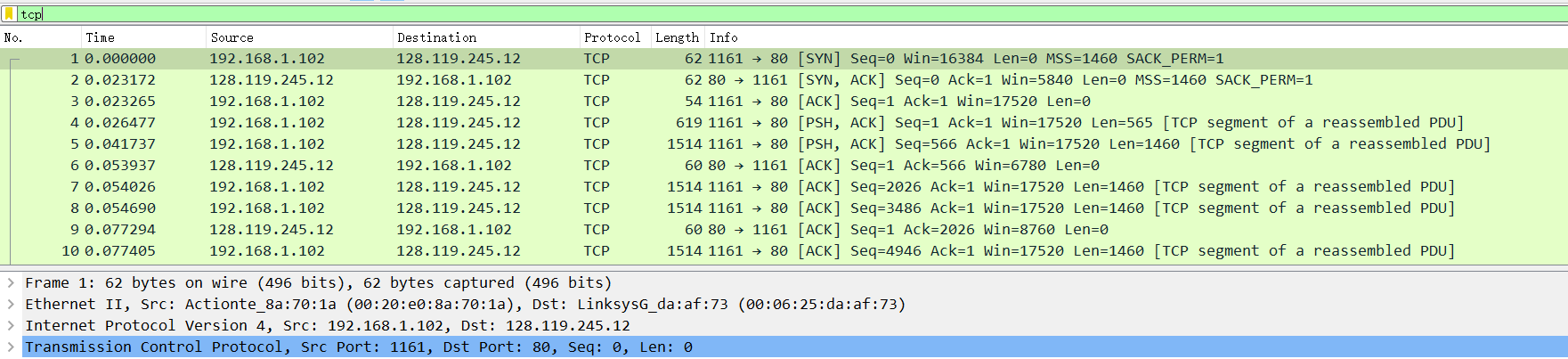
probably easiest to select an HTTP message and explore the details of the TCP

packet used to carry this HTTP message, using the “details of the selected packet

header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if

you’re uncertain about the Wireshark windows).

答：通过下载的trace文件回答。



其中IP地址为192.168.1.102；TCP的端口号为1161

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending

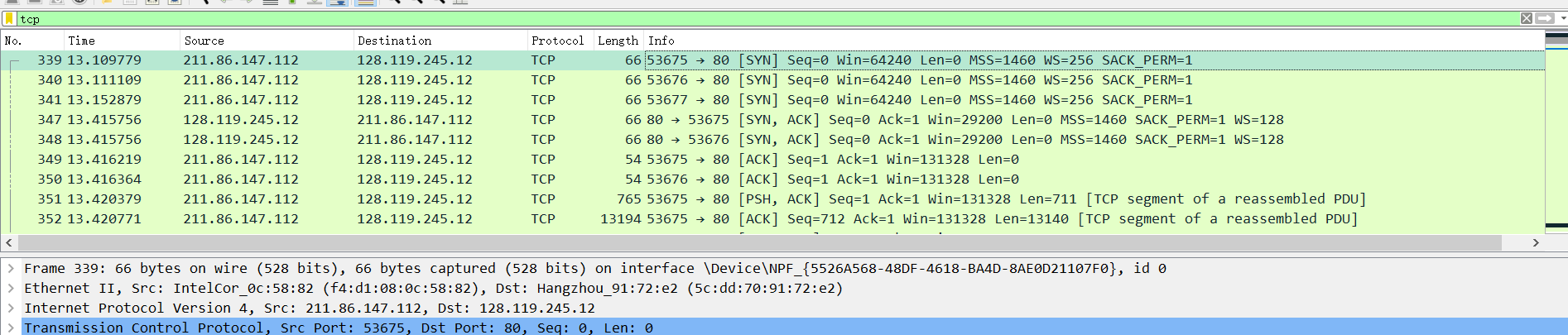
and receiving TCP segments for this connection?

答：IP地址为：128.119.245.12；端口号为：80

3. What is the IP address and TCP port number used by your client computer

(source) to transfer the file to gaia.cs.umass.edu?

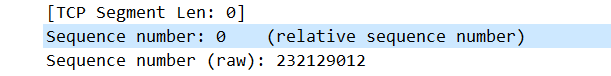
答：用自己的电脑得到的trace文件。

 IP地址为：211.86.147.112；端口号为：53675

4. 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 the segment that identifies the segment as a SYN segment?

答：

序号为0；

报文中的flag中会把SYN置为1.

5. 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 the value of the

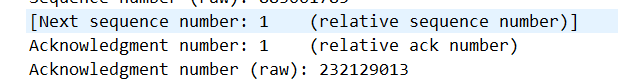
ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu

determine that value? What is it in the segment that identifies the segment as a

SYNACK segment?

答：

序号为0.



ACKnowledgement会被置为1.

Gaia.cs.umass.edu会将该值设置为所期望的下一个报文的序号。

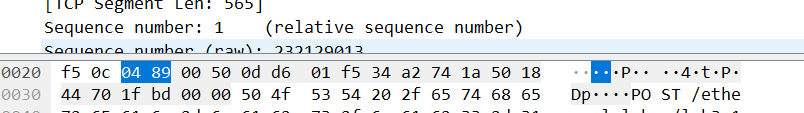
在flag中ACK以及SYN位将被置为1.

6. What is the sequence number of the TCP segment containing the HTTP POST

command? Note that in order to find the POST command, you’ll need to dig into

the packet content field at the bottom of the Wireshark window, looking for a

segment with a “POST” within its DATA field.

答：

序号为：1

7. Consider the TCP segment containing the HTTP POST as the first segment in the

TCP connection. What are the sequence numbers of the first six segments in the

TCP connection (including the segment containing the HTTP POST)? At what

time was each segment sent? When was the ACK for each segment received?

Given the difference between when each TCP segment was sent, and when its

acknowledgement was received, what is the RTT value for each of the six

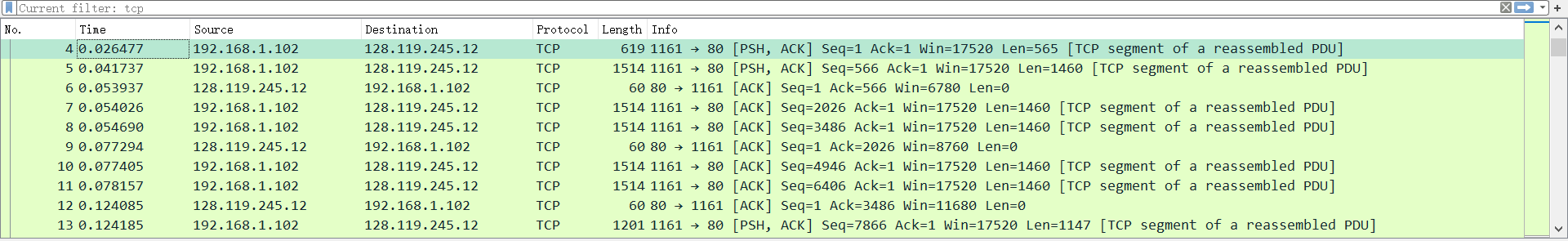
segments? What is the EstimatedRTT value (see page 249 in text) after the

receipt of each ACK? Assume that the value of the EstimatedRTT is equal to

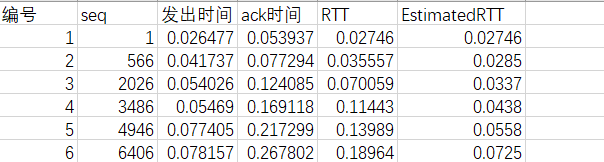
the measured RTT for the first segment, and then is computed using the

EstimatedRTT equation on page 249 for all subsequent segments.

答：如下图

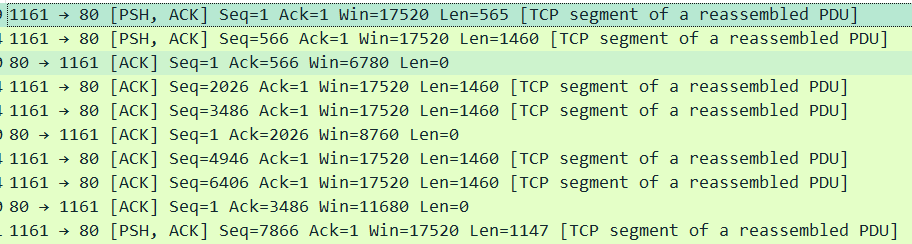


针对这个题绘了一个表如下：



8. What is the length of each of the first six TCP segments?

答：如下图：



分别是：565,1460,1460,1460,1460,1460

9. What is the minimum amount of available buffer space advertised at the received

for the entire trace? Does the lack of receiver buffer space ever throttle the

sender?

答：最小的缓冲空间为5840；没有限制过发送端

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

the trace) in order to answer this question?

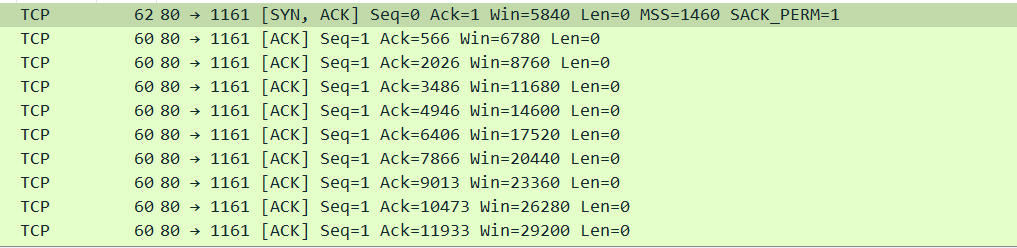
答：没有。检查了发送端发送的报文序号，发现并没有两个完全一样序号的报文，所以可以确定没有重传的报文。

11. How much data does the receiver typically acknowledge in an ACK? Can you

identify cases where the receiver is ACKing every other received segment (see

Table 3.2 on page 257 in the text).

答：如下图截取了部分接收端收到的报文。



典型的有1460；就直接使用后一个接收到的ack值减去前一个ack值就可以得到一次ack的字节数。

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

Explain how you calculated this value.

答：第一次发送post的时间为：0.026477

收到最后一个ack的时间为：5.455830

时间差为：5.429353

字节数为：164090

吞吐量为：164090/5.429353=30222.754Bps

13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence

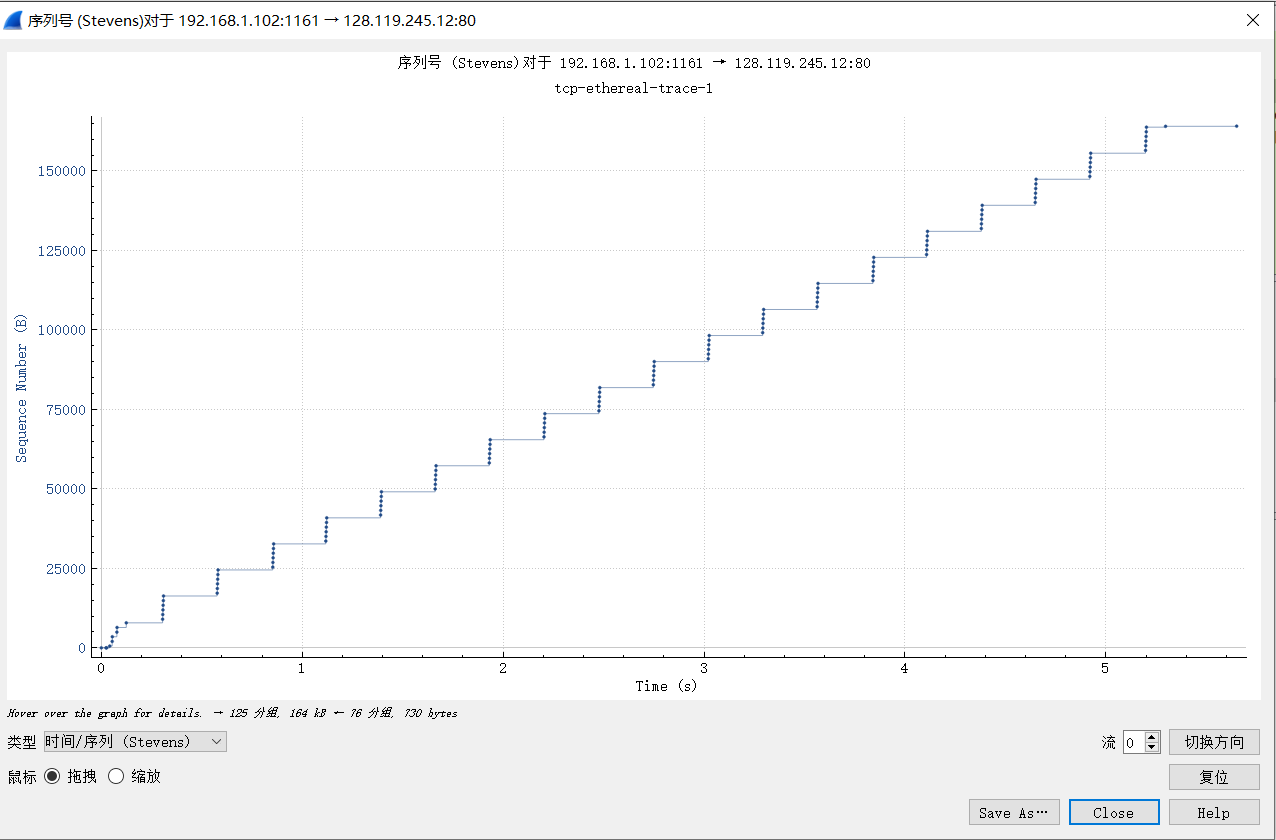
number versus time plot of segments being sent from the client to the

gaia.cs.umass.edu server. Can you identify where TCP’s slowstart phase begins

and ends, and where congestion avoidance takes over? Comment on ways in

which the measured data differs from the idealized behavior of TCP that we’ve

studied in the text.



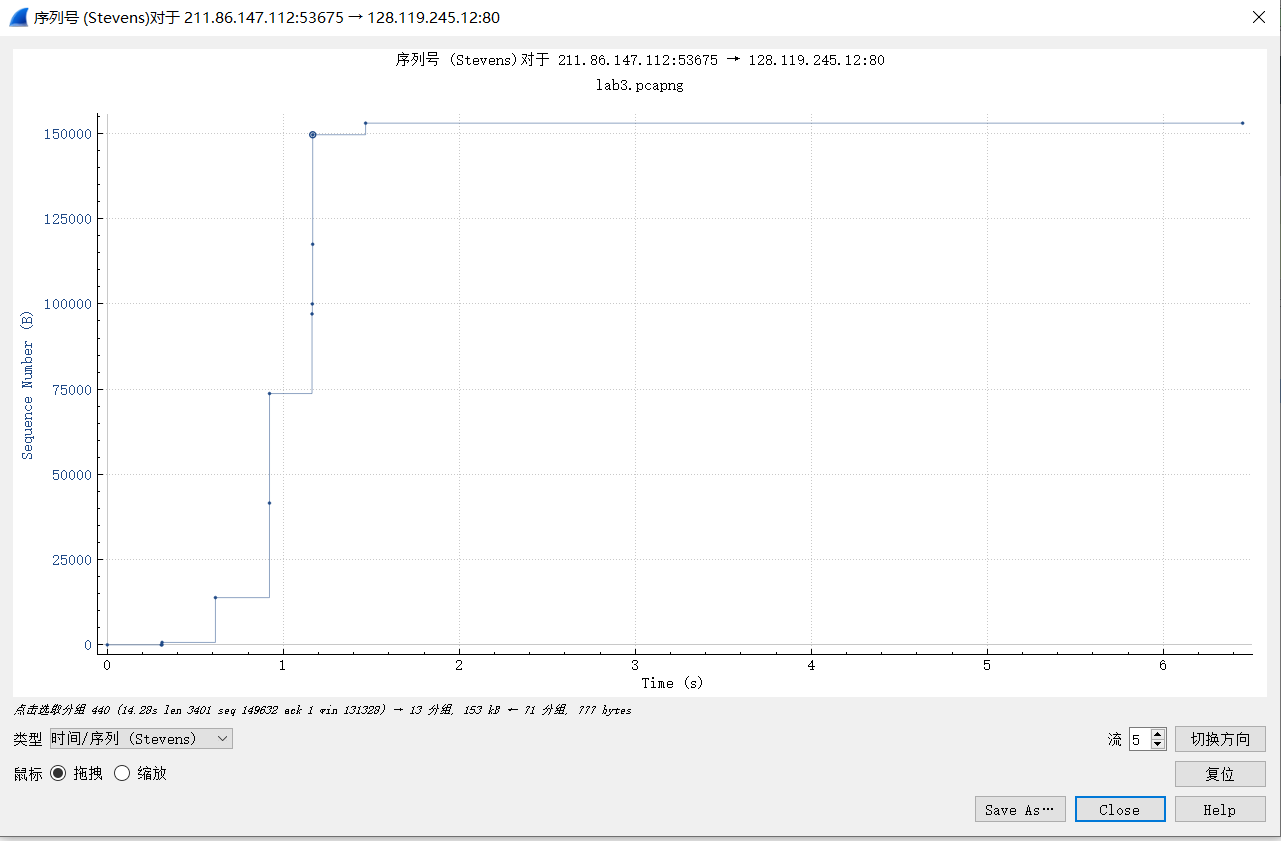
答：只有最开始一小部分处于慢启动状态，之后进入拥塞避免的状态。

和书本上的出入主要在于，慢启动结束之后，便一直在以一个恒定的发送速率来发送，因此也不会出现课本上的过一个轮次加一这种情形。

14. Answer each of two questions above for the trace that you have gathered when

you transferred a file from your computer to gaia.cs.umass.edu

答：如图所示：



答：我这里的情况是慢启动还没完成就已经结束了文件的发送，看不出拥塞避免的状态。慢启动阶段和书本上的比较一致。

1. 实验总结

通过对于tcp的分析，进一步熟悉了tcp的报文以及tcp的整个工作的流程，同时也对书上的理想情形下的tcp的状况和真实的状况有了更加深刻的认识