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

一．　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。

二．　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

三．　实验条件

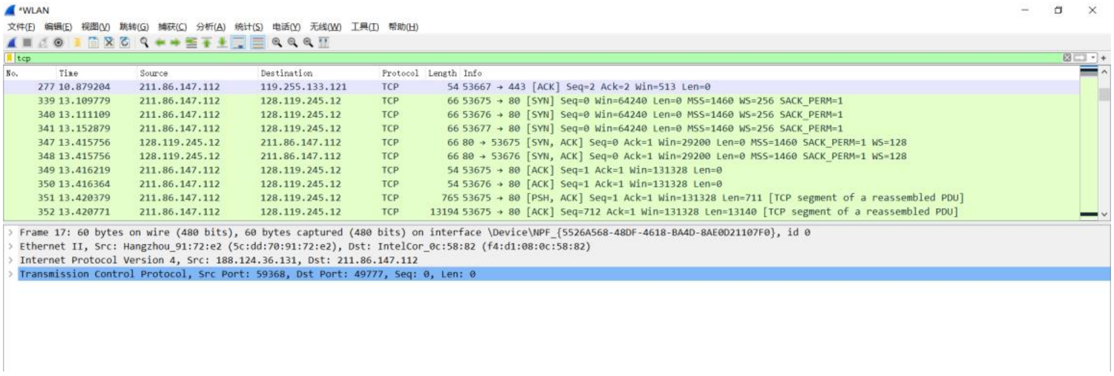
1、 硬件条件：一台 PC 机
2、 软件条件：win10, wireshark 软件

四．　实验过程

1. 访问 http://gaia.cs.umass.edu/wiresharklabs/alice.txt 下载 alice.txt，存在本地：

alice.txt　2020/11/15 9:18　文本文档　149 KB

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


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

tcp

```
No.   Time        Source          Destination      Protocol Length Info
  277 10.879204   211.86.147.112  119.255.133.121  TCP         54 53667 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0
  339 13.109779   211.86.147.112  128.119.245.12   TCP         66 53675 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  340 13.111109   211.86.147.112  128.119.245.12   TCP         66 53676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  341 13.152879   211.86.147.112  128.119.245.12   TCP         66 53677 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  347 13.415756   128.119.245.12  211.86.147.112   TCP         66 80 → 53675 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  348 13.415756   128.119.245.12  211.86.147.112   TCP         66 80 → 53676 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  349 13.416219   211.86.147.112  128.119.245.12   TCP         54 53675 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  350 13.416364   211.86.147.112  128.119.245.12   TCP         54 53676 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  351 13.420379   211.86.147.112  128.119.245.12   TCP        765 53675 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=711 [TCP segment of a reassembled PDU]
  352 13.420771   211.86.147.112  128.119.245.12   TCP      13194 53675 → 80 [ACK] Seq=712 Ack=1 Win=131328 Len=13140 [TCP segment of a reassembled PDU]
```

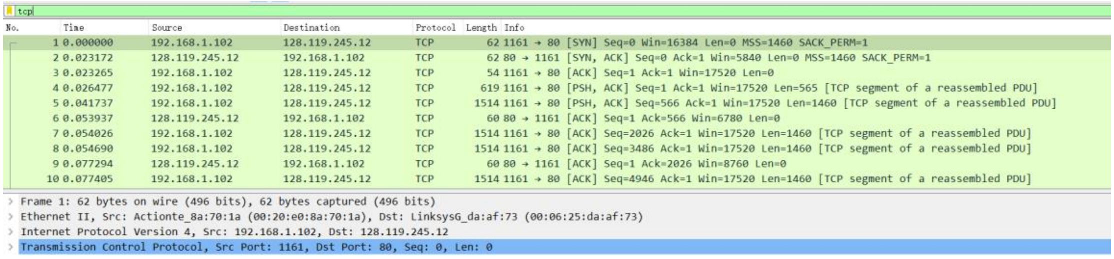
```
> Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_0c:58:82 (f4:d1:08:0c:58:82)
> Internet Protocol Version 4, Src: 188.124.36.131, Dst: 211.86.147.112
> Transmission Control Protocol, Src Port: 59368, Dst Port: 49777, Seq: 0, Len: 0
```

五．　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。



tcp

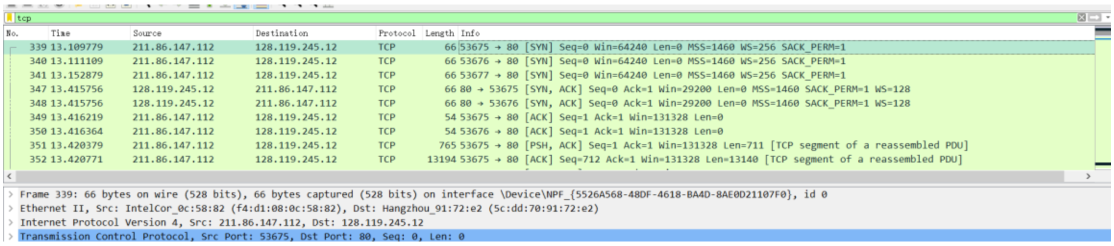
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
```

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。



tcp

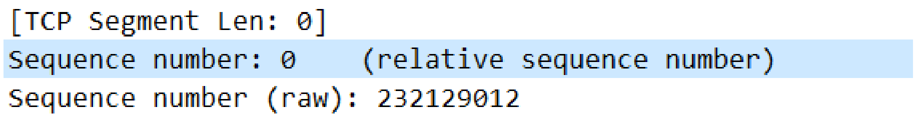
No.	Time	Source	Destination	Protocol	Length	Info
339	13.109779	211.86.147.112	128.119.245.12	TCP	66	53675 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
340	13.111109	211.86.147.112	128.119.245.12	TCP	66	53676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
341	13.152879	211.86.147.112	128.119.245.12	TCP	66	53677 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
347	13.415756	128.119.245.12	211.86.147.112	TCP	66	80 → 53675 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
348	13.415756	128.119.245.12	211.86.147.112	TCP	66	80 → 53676 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
349	13.416219	211.86.147.112	128.119.245.12	TCP	54	53675 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
350	13.416364	211.86.147.112	128.119.245.12	TCP	54	53676 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
351	13.420379	211.86.147.112	128.119.245.12	TCP	765	53675 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=711 [TCP segment of a reassembled PDU]
352	13.420771	211.86.147.112	128.119.245.12	TCP	13194	53675 → 80 [ACK] Seq=712 Ack=1 Win=131328 Len=13140 [TCP segment of a reassembled PDU]

```
> Frame 339: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 211.86.147.112, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53675, Dst Port: 80, Seq: 0, Len: 0
```

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：

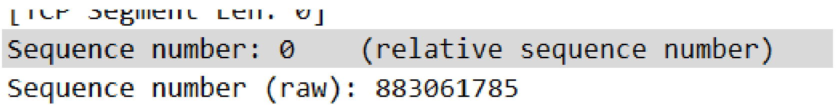


```
[TCP Segment Len: 0]
Sequence number: 0    (relative sequence number)
Sequence number (raw): 232129012
```

序号为 0；
报文中的 flag 中会把 SYN 置为 1.

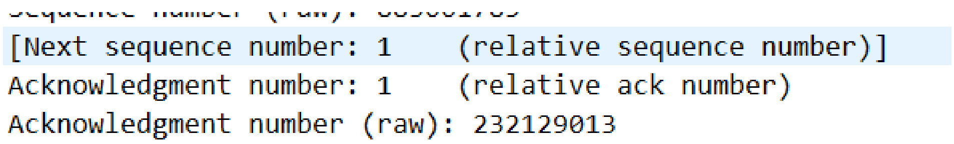
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu
to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a
SYNACK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

答：



```
[TCP Segment Len: 0]
Sequence number: 0    (relative sequence number)
Sequence number (raw): 883061785
```

序号为 0.

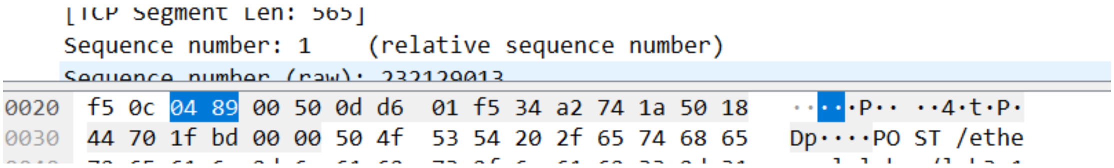


```
Sequence number (raw): 883061785
[Next sequence number: 1    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
Acknowledgment number (raw): 232129013
```

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：



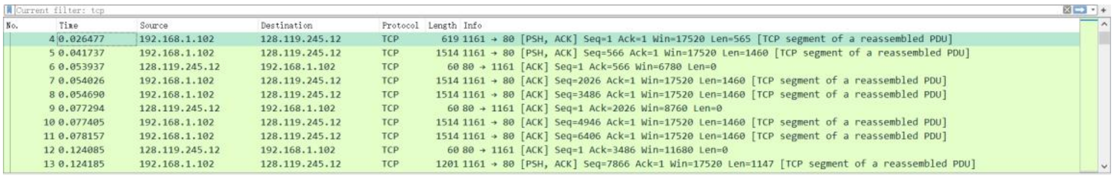
```
[TCP Segment Len: 565]
Sequence number: 1    (relative sequence number)
Sequence number (raw): 232129013

0020  f5 0c 04 89 00 50 0d d6  01 f5 34 a2 74 1a 50 18   ·····P·· ··4·t·P·
0030  44 70 1f bd 00 00 50 4f  53 54 20 2f 65 74 68 65   Dp····PO ST /ethe
```

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



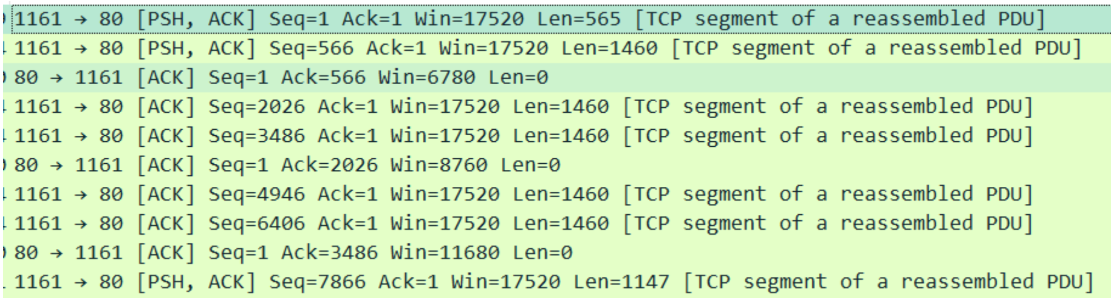
```
Current filter: tcp
No.   Time       Source          Destination     Protocol Length Info
    4 0.026477   192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
    5 0.041737   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
    6 0.053937   128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
    7 0.054026   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
    8 0.054690   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
    9 0.077294   128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
   10 0.077405   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
   11 0.078157   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
   12 0.124085   128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
   13 0.124185   192.168.1.102   128.119.245.12  TCP      1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
```

针对这个题绘了一个表如下：

编号	seq	发出时间	ack时间	RTT	EstimatedRTT
1	1	0.026477	0.053937	0.02746	0.02746
2	566	0.041737	0.077294	0.035557	0.0285
3	2026	0.054026	0.124085	0.070059	0.0337
4	3486	0.05469	0.169118	0.11443	0.0438
5	4946	0.077405	0.217299	0.13989	0.0558
6	6406	0.078157	0.267802	0.18964	0.0725

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

答：如下图：



```
1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
```

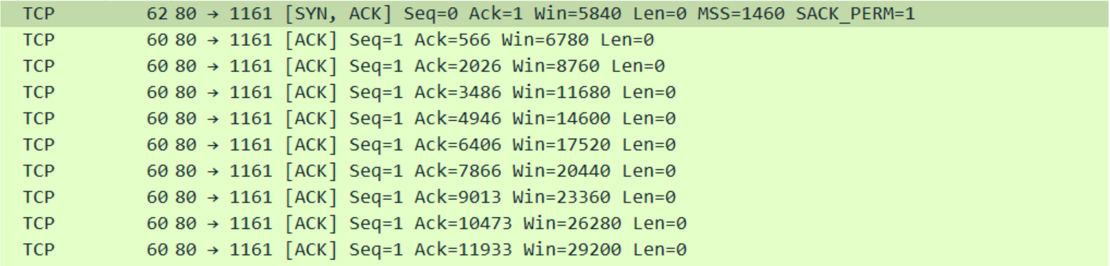
分别是：565,1460,1460,1460,1460,1460

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。

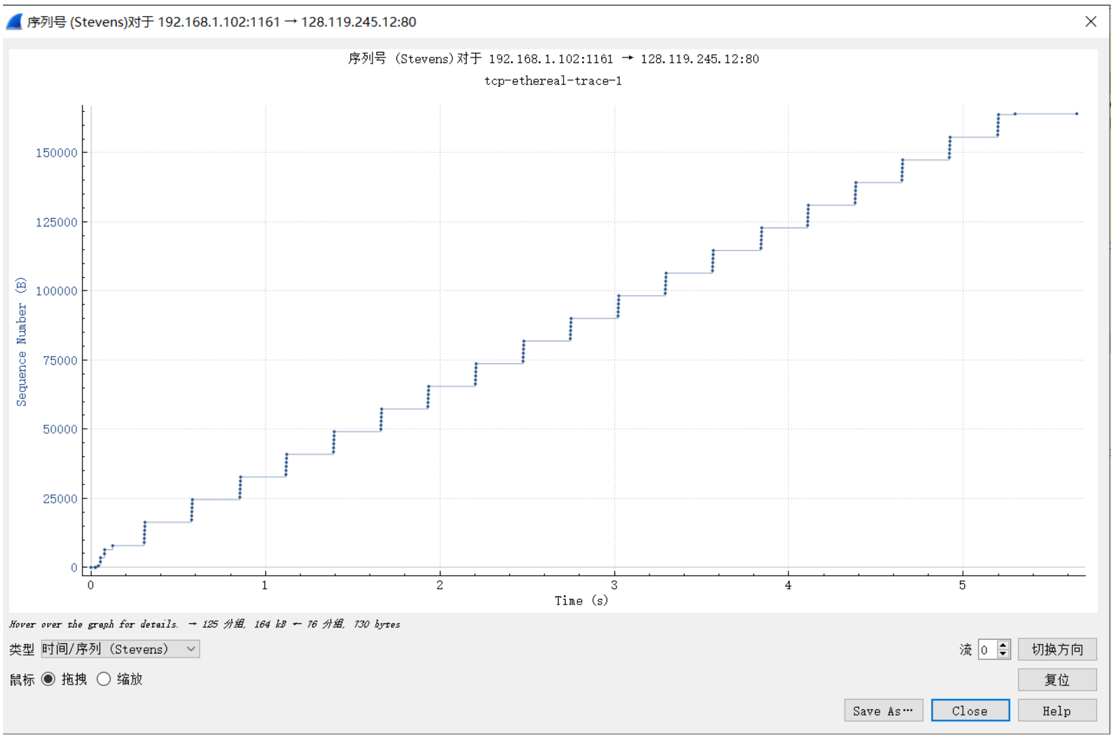


```
TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=10473 Win=26280 Len=0
TCP        60 80 → 1161 [ACK] Seq=1 Ack=11933 Win=29200 Len=0
```

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.



序列号 (Stevens)对于 192.168.1.102:1161 → 128.119.245.12:80

序列号 (Stevens) 对于 192.168.1.102:1161 → 128.119.245.12:80

tcp-ethereal-trace-1

Hover over the graph for details. → 125 分组, 164 kB ← 76 分组, 730 bytes

类型 时间/序列 (Stevens)

鼠标 ● 拖拽 ○ 缩放

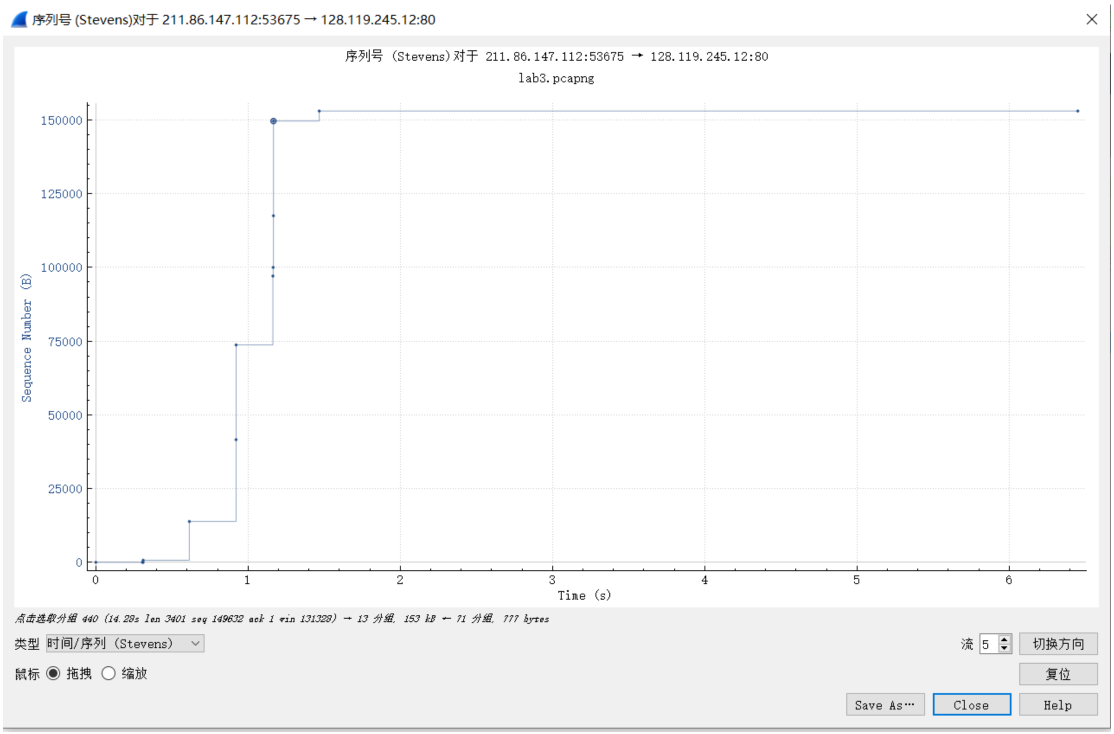
流 0

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：



序列号 (Stevens)对于 211.86.147.112:53675 → 128.119.245.12:80

序列号 (Stevens) 对于 211.86.147.112:53675 → 128.119.245.12:80

lab3.pcapng

点击选取分组 440 (14.28s len 3401 seq 149632 ack 1 win 131328) → 13 分组, 153 kB ← 71 分组, 777 bytes

类型 时间/序列 (Stevens)

鼠标 ● 拖拽 ○ 缩放

流 5

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。

六. 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