



Wireshark 实验-TCP

专业班级： 智慧技术班信息安全专业

学号： 21307130076

姓名： 杨乙

（一） 捕获从计算机到远程服务器的批量 TCP 传输

访问网页 1，查看 ASCII 档案文件，右键选择“保存”，访问网页 2，使用“选择文件”按钮选择保存好的文件，先启动 Wireshark 开始数据包捕获，再点击“Upload alice.txt file”按钮将文件上传到服务器。浏览器窗口显示祝贺消息。停止 Wireshark 数据包捕获，Wireshark 视窗内容如下：

394	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=15228 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
395	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [PSH, ACK] Seq=16676 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
396	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=18124 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
397	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=19572 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
398	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=21020 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
399	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=22468 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
400	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=23916 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
401	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=25364 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
402	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=26812 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
403	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=28260 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
404	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=29708 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
405	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=31156 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
406	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [PSH, ACK] Seq=32604 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
407	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=34052 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
408	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=35500 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
409	42.808449	10.219.154.245	128.119.245.12	TCP	1514	57641 → 80 [ACK] Seq=36948 Ack=1 Win=131584 Len=1448 TSval=1320655506 TSecr=4033207182 [TCP segment of...
410	42.809072	128.119.245.12	10.219.154.245	TCP	66	80 → 57641 [ACK] Seq=1 Ack=13780 Win=56576 Len=0 TSval=4033207182 TSecr=1320655259

（二） 跟踪包的初步观察

可以发现跟踪包包含如下内容：

1. 包含 SYN 讯息的初始三次握手

TCP	74	52042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=1324771458 TSecr=0
TCP	74	80 → 52042 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=4037323389 TSecr=1324771458
TCP	66	52042 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1324771730 TSecr=4037323389

2. HTTP POST 消息

HTTP	347	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
------	-----	-------------------------------------------------------------

3. 重新组装的 PDU 的 TCP 段

35	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=90212 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
36	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=100660 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
37	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=102108 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
38	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=103556 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
39	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=105004 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
40	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=106452 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
41	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=107900 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
42	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=109348 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
43	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=110796 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
44	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=112244 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...
45	7.373913	10.219.154.245	128.119.245.12	TCP	1514	52042 → 80 [ACK] Seq=113692 Ack=1 Win=131584 Len=1448 TSval=1324773164 TSecr=4037324839 [TCP segment of...

4. 返回的 TCP ACK 区段

23	7.682668	128.119.245.12	10.219.154.245	TCP	78	80 → 52042 [ACK] Seq=1 Ack=146996 Win=235520 Len=0 TSval=4037325100 TSecr=1324773164 SLE=152788 SRE=15...
24	7.682668	128.119.245.12	10.219.154.245	TCP	78	80 → 52042 [ACK] Seq=1 Ack=148444 Win=237568 Len=0 TSval=4037325101 TSecr=1324773164 SLE=152788 SRE=15...
25	7.682668	128.119.245.12	10.219.154.245	TCP	78	80 → 52042 [ACK] Seq=1 Ack=149892 Win=237568 Len=0 TSval=4037325101 TSecr=1324773164 SLE=152788 SRE=15...
26	7.682668	128.119.245.12	10.219.154.245	TCP	78	80 → 52042 [ACK] Seq=1 Ack=151340 Win=237568 Len=0 TSval=4037325101 TSecr=1324773164 SLE=152788 SRE=15...

回答问题:

1. 将文件传输到 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？

86	7.374539	10.219.154.245	128.119.245.12	HTTP	347	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
<						
> Frame 586: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{84F30BE1-7874-473F-BB1D-9A7FAE3D946F}, id 0						
> Ethernet II, Src: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4), Dst: HuaweiTe_f2:be:11 (dc:99:14:f2:be:11)						
> Internet Protocol Version 4, Src: 10.219.154.245, Dst: 128.119.245.12						
> Transmission Control Protocol, Src Port: 52042, Dst Port: 80, Seq: 152788, Ack: 1, Len: 281						
> [107 Reassembled TCP Segments (153068 bytes): #391(747), #392(1448), #393(1448), #394(1448), #395(1448), #396(1448), #397(1448), #398(1448), #						
> Hypertext Transfer Protocol						
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "---WebKitFormBoundaryUvQIOFMXB4VJ89"						

如图，客户端计算机使用的 IP 地址：10.219.154.245

客户端计算机使用的 TCP 端口号：52042

2. gaia.cs.umass.edu 的 IP 地址是什么？在哪个端口号上发送和接收此连接的 TCP 区段？

如上图，分别是：

128.119.245.12

80

（三）TCP 基础

1. 用于在客户端计算机和 gaia.cs.umass.edu 之间启动 TCP 连接的 TCP SYN 区段的序列号是什么？将区段标识为 SYN 区段的区段有什么功能？

No.	Time	Source	Destination	Protocol	Length	Info
355	5.668026	10.219.154.245	128.119.245.12	TCP	74	52042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
<						
> Frame 355: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{84F30BE1-7874-473F-BB1D-9A7FAE3D946F}, id 0						
> Ethernet II, Src: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4), Dst: HuaweiTe_f2:be:11 (dc:99:14:f2:be:11)						
> Internet Protocol Version 4, Src: 10.219.154.245, Dst: 128.119.245.12						
> Transmission Control Protocol, Src Port: 52042, Dst Port: 80, Seq: 0, Len: 0						
Source Port: 52042						
Destination Port: 80						
[Stream index: 23]						
[Conversation completeness: Complete, WITH_DATA (31)]						
[TCP Segment Len: 0]						
Sequence Number: 0 (relative sequence number)						
Sequence Number (raw): 1777915152						

如图，序列号为 0

（注：相对序列号为 0，绝对序列号为 1777915152，以后为了方便统一使用相对序列号）

功能是开始三次握手，请求服务器建立连接，作为三次握手的第一次

2. gaia.cs.umass.edu 发送给客户端计算机以回复 SYN 的 SYNACK 区段的序列号是多少？

355	5.668026	10.219.154.245	128.119.245.12	TCP	74	52042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
368	5.940572	128.119.245.12	10.219.154.245	TCP	74	80 → 52042 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_F
<						
> Frame 368: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{84F30BE1-7874-473F-BB1D-9A7FAE3D946F}, id 0						
> Ethernet II, Src: HuaweiTe_f2:be:11 (dc:99:14:f2:be:11), Dst: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4)						
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.154.245						
> Transmission Control Protocol, Src Port: 80, Dst Port: 52042, Seq: 0, Ack: 1, Len: 0						
Source Port: 80						
Destination Port: 52042						
[Stream index: 23]						
[Conversation completeness: Complete, WITH_DATA (31)]						
[TCP Segment Len: 0]						
Sequence Number: 0 (relative sequence number)						
Sequence Number (raw): 1481470455						

如图，序列号为 0

SYN ACK 区段中的 Acknowledgment 栏位的值是多少？

```
▼ Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... 0... = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
[TCP Flags: .....A..S.]
```

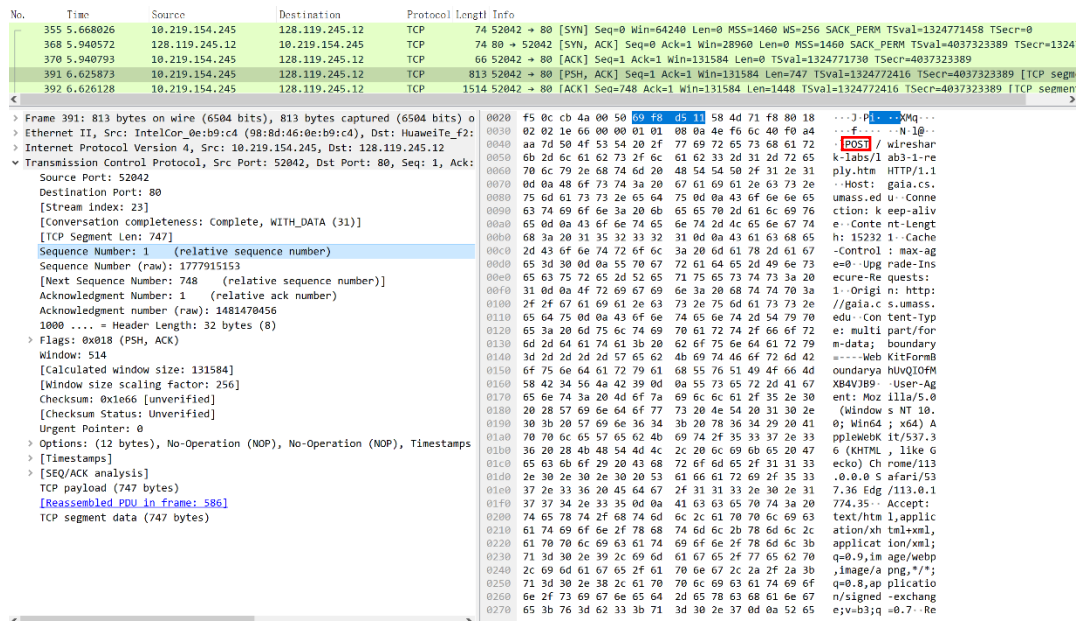
如图，SYN ACK 区段中的 Acknowledgment 栏位的相对值是 1

Gaia.cs.umass.edu 是如何确定此 Acknowledgment 的数值的？在将区段标识为 SYNACK 区段的区段在连线中有什么功能？

将第一次握手中客户端的序列号+1 后得到 Acknowledgment 值

功能是三次握手的第二次，告知客户端可以建立连接和接收请求，向客户端发送新序列号并和客户端确认原序列号

3. 包含 HTTP POST 命令的 TCP 区段的序列号是多少？请注意，为了找到 POST 命令，您需要深入了解 Wireshark 窗口底部的数据包内容字段，在其 DATA 栏位中查找带有“POST”的区段。



The image shows a Wireshark packet capture. The packet list pane displays a SYN-ACK segment from 10.219.154.245 to 10.219.154.128. The packet details pane shows the TCP segment with sequence number 1 and acknowledgment number 1. The packet bytes pane shows the raw data of the TCP segment, including the SYN and ACK flags, and the sequence and acknowledgment numbers.

如图，找到 DATA 栏位中带有“POST”的区段，对应的 TCP 区段的序列号为 1

注：因为退出 Wireshark，此时重新捕获分组，客户端的 IP 地址变更为 10.223.156.58
客户端的 TCP 端口号变更为 58544

4. 将包含 HTTP POST 的 TCP 区段视为 TCP 连接中的第一个区段。前六个 TCP 区段的长度是多少？在这个 TCP 连线中前 6 个 TCP 区段的序列号是什么（包括包含 HTTP POST 的区段）？每区段发送的时间是什么时候？收到的每个区段的 ACK 是什么时候？鉴于发送每个 TCP 区段的时间与收到确认的时间之间的差异，六个区段中每个区段的 RTT 值是多少？收到每个 ACK 后，Estimated RTT 值是什么？假设第一个 Estimated RTT 的值等于第一个区段的测量 RTT。

通过追踪 TCP 流，提取从第一个 TCP 区段开始的前六个 TCP 区段：

33	4.825564	10.223.156.58	128.119.245.12	TCP	875 62173 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=809 TSval=1363198326 TSecr=4075746861 [TCP segment of
34	4.825773	10.223.156.58	128.119.245.12	TCP	1514 62173 → 80 [ACK] Seq=810 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
35	4.825773	10.223.156.58	128.119.245.12	TCP	1514 62173 → 80 [ACK] Seq=2258 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
36	4.825773	10.223.156.58	128.119.245.12	TCP	1514 62173 → 80 [ACK] Seq=3706 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
37	4.825773	10.223.156.58	128.119.245.12	TCP	1514 62173 → 80 [ACK] Seq=5154 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
38	4.825773	10.223.156.58	128.119.245.12	TCP	1514 62173 → 80 [ACK] Seq=6602 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of

提取这六个 TCP 区段的回复：

47	5.223823	128.119.245.12	10.223.156.58	TCP	66 80 → 62173 [ACK] Seq=1 Ack=810 Win=30592 Len=0 TSval=4075747152 TSecr=1363198326
48	5.223823	128.119.245.12	10.223.156.58	TCP	66 80 → 62173 [ACK] Seq=1 Ack=2258 Win=33536 Len=0 TSval=4075747152 TSecr=1363198326
49	5.223823	128.119.245.12	10.223.156.58	TCP	66 80 → 62173 [ACK] Seq=1 Ack=3706 Win=36480 Len=0 TSval=4075747152 TSecr=1363198326
50	5.223823	128.119.245.12	10.223.156.58	TCP	66 80 → 62173 [ACK] Seq=1 Ack=5154 Win=39296 Len=0 TSval=4075747152 TSecr=1363198326
51	5.223823	128.119.245.12	10.223.156.58	TCP	66 80 → 62173 [ACK] Seq=1 Ack=6602 Win=42240 Len=0 TSval=4075747152 TSecr=1363198326
52	5.223823	128.119.245.12	10.223.156.58	TCP	66 80 → 62173 [ACK] Seq=1 Ack=8090 Win=45184 Len=0 TSval=4075747152 TSecr=1363198326

可以看到，前六个 TCP 区段的长度分别为 809、1448、1448、1448、1448、1448

这六个 TCP 区段的序列号分别为 1、810、2258、3706、5154、6602

这六个 TCP 区段的发送时间分别为

4.825564、4.825773、4.825773、4.825773、4.825773、4.825773

收到这六个 TCP 区段的时间分别为

5.223823、5.223823、5.223823、5.223823、5.223823、5.223823

根据发送和接收确认时间的差异，六个 TCP 区段的 RTT 分别为

0.398259、0.398050、0.398050、0.398050、0.398050、0.398050

（在 Wireshark 中输入 tcp.analysis.ack_rtt 可以直接查看 TCP 段的 RTT，如下图）

```
▼ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 33]
  [The RTT to ACK the segment was: 0.398259000 seconds]
  [iRTT: 0.289230000 seconds]
```

根据 Estimated RTT 计算公式，收到每个 ACK 后，Estimated RTT 值分别为

0.398259

$0.875 * 0.398259 + 0.125 * 0.398050 = 0.398233$

$0.875 * 0.398233 + 0.125 * 0.398050 = 0.398210$

$0.875 * 0.398210 + 0.125 * 0.398050 = 0.398190$

$0.875 * 0.398210 + 0.125 * 0.398050 = 0.398172$

$0.875 * 0.398172 + 0.125 * 0.398050 = 0.398157$

5. 前六个 TCP 区段的长度是多少？

根据上一题，前六个 TCP 区段的长度分别为 809、1448、1448、1448、1448、1448

6. 对于整个跟踪包，收到的最小可用缓冲区空间量是多少？缺少接收器缓冲区空间是否会限制发送方传送 TCP 区段？

28	4.535795	10.223.156.58	128.119.245.12	TCP	74	62173 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=1363198036 TSecr=0
31	4.824903	128.119.245.12	10.223.156.58	TCP	74	80 → 62173 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=4075746861 TSecr=1363198036
32	4.825025	10.223.156.58	128.119.245.12	TCP	66	62173 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1363198325 TSecr=4075746861

通过比较，得到收到的最小可用缓冲区空间量是 28960，缺少接收器缓冲区空间会限制发送方传送 TCP 区段。根据 TCP 的流量控制服务，缓冲区空间能消除发送方便接收方缓存溢出的可能性。因此缺少接收器缓冲区空间会限制发送方传送 TCP 区段

10. 在跟踪文件中是否有重传的区段？

没有。观察序列号与时间，可见随着时间的增加，序列号一直是增大的，且没有出现重复的序列号。说明没有重传的区段

11. 接收器通常在 ACK 中确认多少数据？是否可以识别接收方每隔一个接收到的区段才发送确认的情况？

34	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=810 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
35	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=2258 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
36	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=3706 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
37	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=5154 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
38	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=6602 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
39	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=8050 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
40	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=9498 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
41	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=10946 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of
42	4.825773	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=12394 Ack=1 Win=131584 Len=1448 TSval=1363198326 TSecr=4075746861 [TCP segment of

如图，接收器通常在 ACK 中确认 1448 bit 的数据

57	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=13842 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
58	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=15290 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
59	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=16738 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
60	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=18186 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
61	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=19634 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
62	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [PSH, ACK] Seq=21082 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segm
63	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=22530 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
64	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=23978 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
65	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=25426 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
66	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=26874 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
67	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=28322 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
68	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=29770 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
69	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=31218 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
70	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [PSH, ACK] Seq=32666 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segm
71	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=34114 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
72	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=35562 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
73	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=37010 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
74	5.223986	10.223.156.58	128.119.245.12	TCP	1514	62173 → 80 [ACK] Seq=38458 Ack=1 Win=131584 Len=1448 TSval=1363198724 TSecr=4075747152 [TCP segment c
79	5.524573	128.119.245.12	10.223.156.58	TCP	66	80 → 62173 [ACK] Seq=1 Ack=16738 Win=62464 Len=0 TSval=4075747551 TSecr=1363198724

如图，79 号是对 57 和 58 号两个区段的确认

12. TCP 连接的吞吐量（每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数值的。

71	4.506800	10.223.156.58	128.119.245.12	TCP	789	51225 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66560 Len=723 TSval=1367148492 TSecr=4079697053 [TCP segmer
241	5.742484	128.119.245.12	10.223.156.58	TCP	66	80 → 51225 [ACK] Seq=1 Ack=153045 Win=215040 Len=0 TSval=4079698260 TSecr=1367149425

如上图，由吞吐量计算公式：

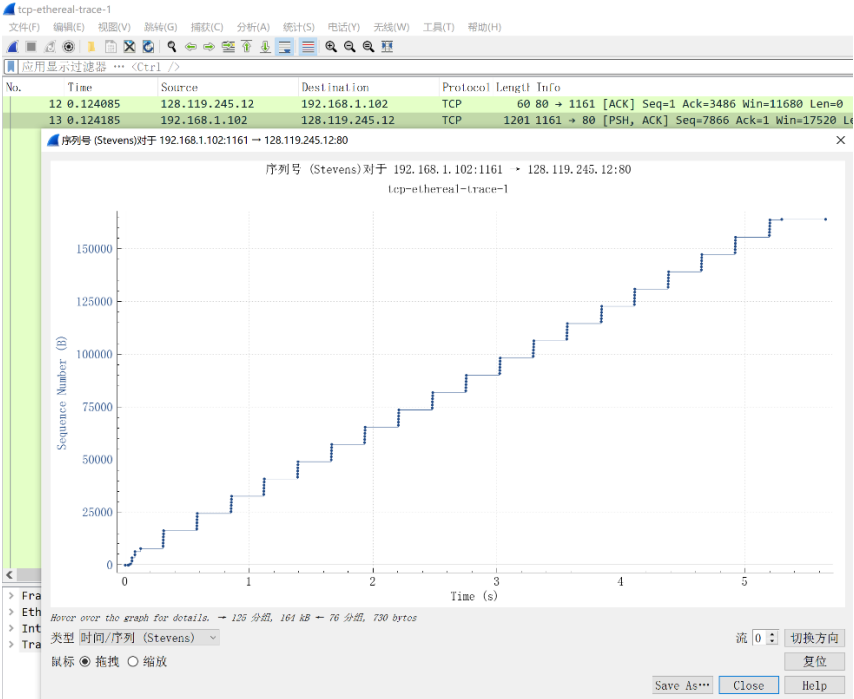
TCP 连接吞吐量 = 总数据量 / 总传输时间

总数据量 = 153045 - 1 = 153044

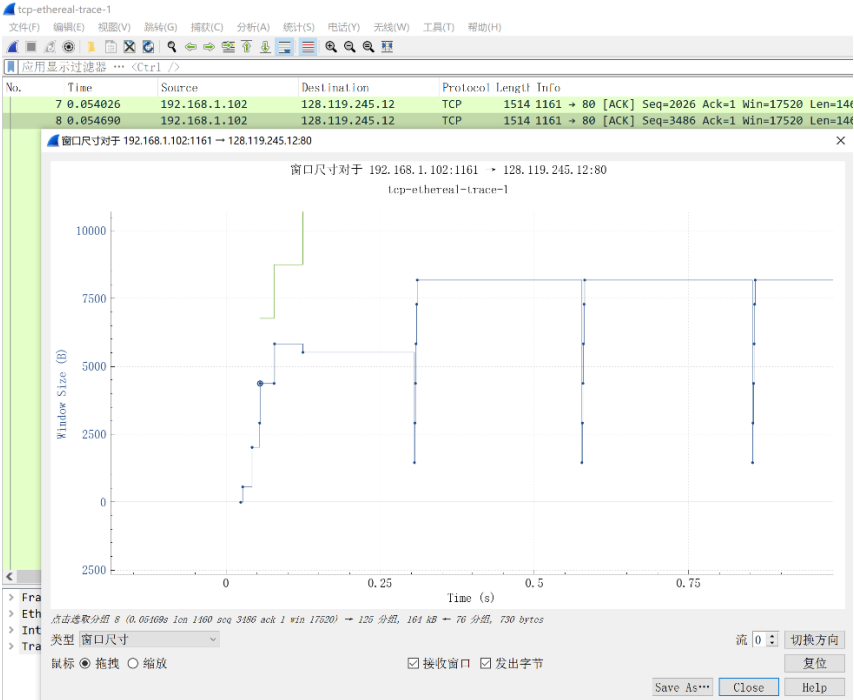
总传输时间 = 5.742484 - 4.506800 = 1.235684

TCP 连接吞吐量 = 153044 / 1.235684 = 123853 b/s = 123.853 kb/s

13. 使用时序图（Stevens）查看从客户端发送到 gaia.cs.umass.edu 服务器的区段的序列号与时间关系图。您能否确定 TCP 的慢启动阶段的开始和结束位置，以及拥塞避免接管的位置？



使用时序图可以确定 TCP 的慢启动阶段的开始位置是最开始的时刻，但不能确定结束位置以及拥塞避免接管的位置。但可以通过“窗口尺寸-时间”图来确定上述信息。



如图，从一开始到区段 8 窗口尺寸呈指数增加，可以确定慢启动的结束位置是区段 8 在 13 区段到 18 区段、23 区段到 30 区段等之间窗口尺寸突然减小，这些位置是拥塞避免接管的位置

14. 评论测量数据与我们在文本中研究的 TCP 的理想化行为的不同之处。

如果要发送的文件数据量较少且网络畅通，发送速度很快，就可能在慢启动结束之前发送完毕，不会出现拥塞控制阶段