计算机网络TCP实验报告

PB19071535徐昊天

一.实验目的

- 学习并了解TCP协议的行为与原理。
- 利用wireshark捕获TCP数据包，并通过数据包分析进一步掌握TCP的报文段结构。

二.实验环境与工具

- windows操作系统
- wireshark数据嗅探器
- Microsoft Edge浏览器

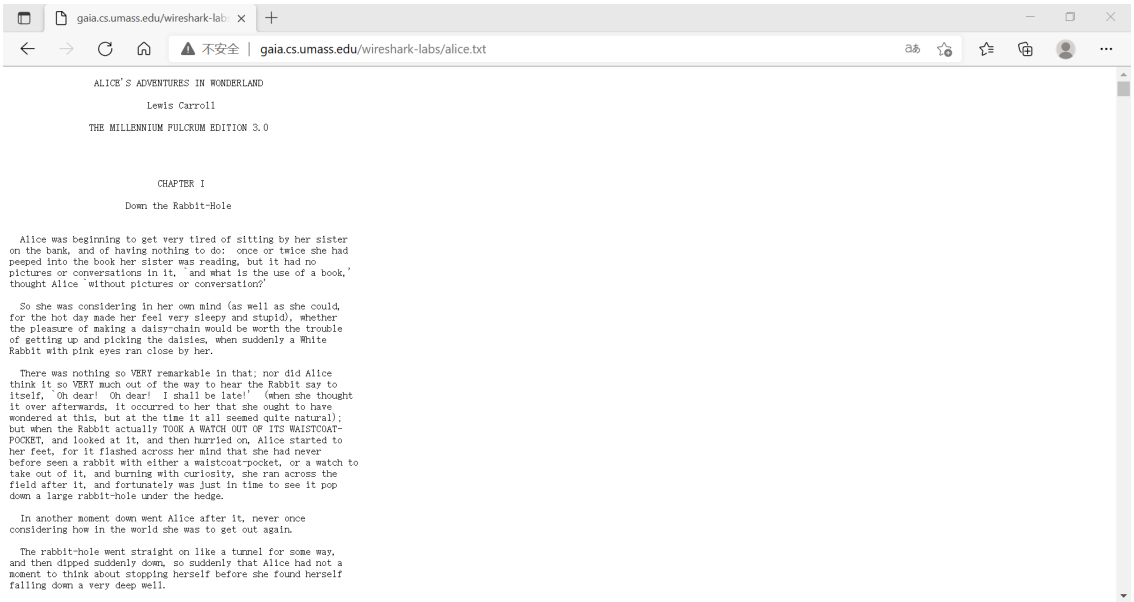
三.实验步骤

1.捕获从计算机到远程服务器的批量 TCP 传输

通过访问一个网页并在网页输入计算机存储的文件名称，将文件传输到web服务器，使用wireshark以获取计算机发送和接收的TCP区段的内容。

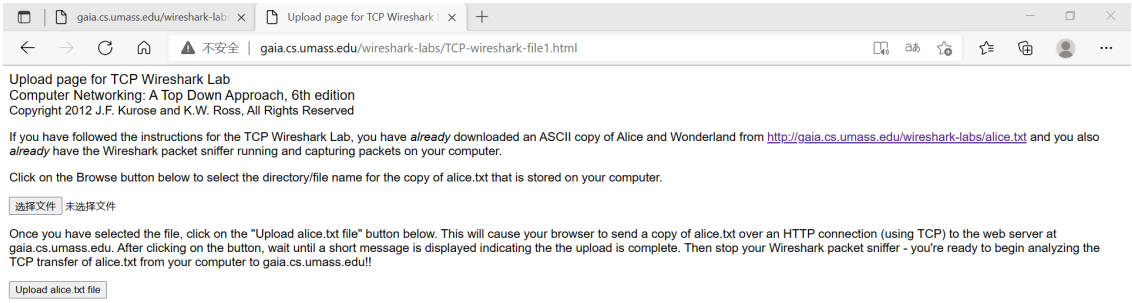
1. 启动 Web 浏览器。 在 http://gaia.cs.umass.edu/wireshark-labs/alice.txt 查看 *Alice in Wonderland* 的 ASCII 档案文件。 将此文件存储在计算机上的某个位置。

   打开http://gaia.cs.umass.edu/wireshark-labs/alice.txt后得到界面如下图所示：



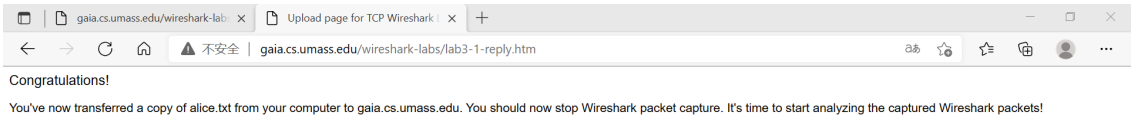
2. 打开 http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html。

   得到界面如下图所示：



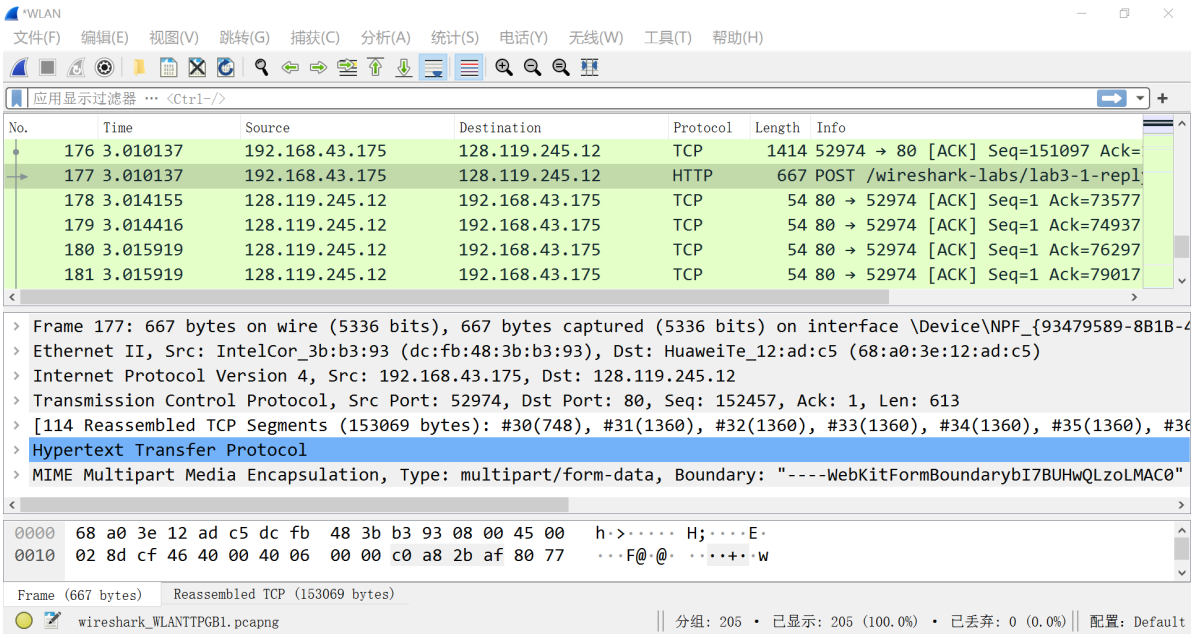
3. 点击 `选择文件` 并输入包含 *Alice in Wonderland* 的文件名。
4. 打开wireshark进行抓包。
5. 返回浏览器，点击 `Upload alice.txt file` 按钮将文件上传到 gaia.cs.umass.edu 服务器。

   得到界面如下图所示：



6. 停止抓包。

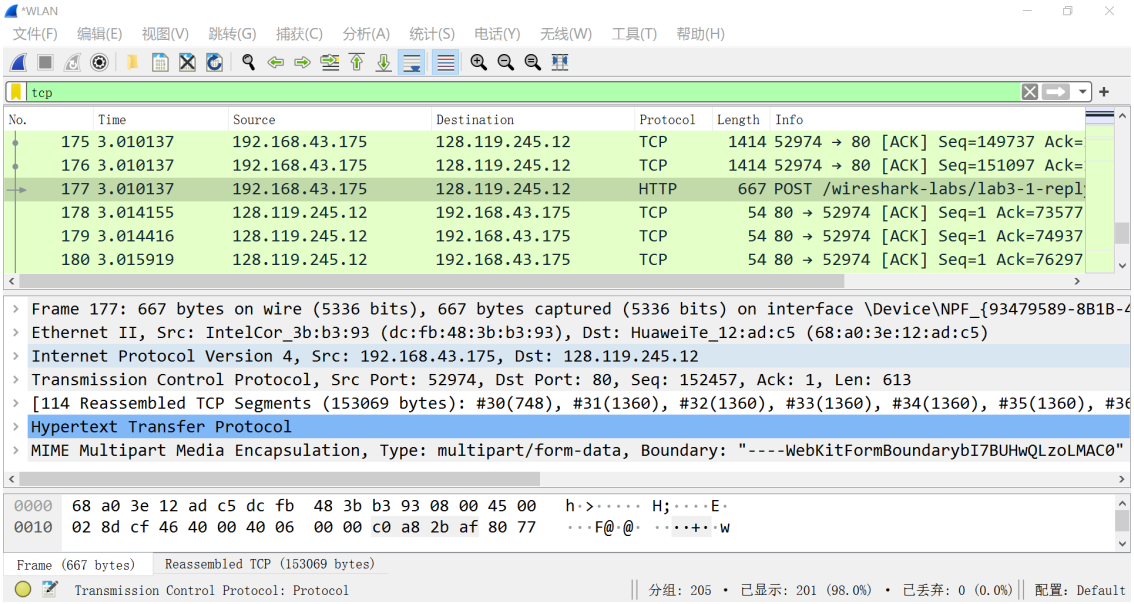
抓包结束后wireshark界面如下图所示：



2.跟踪包的初步观察

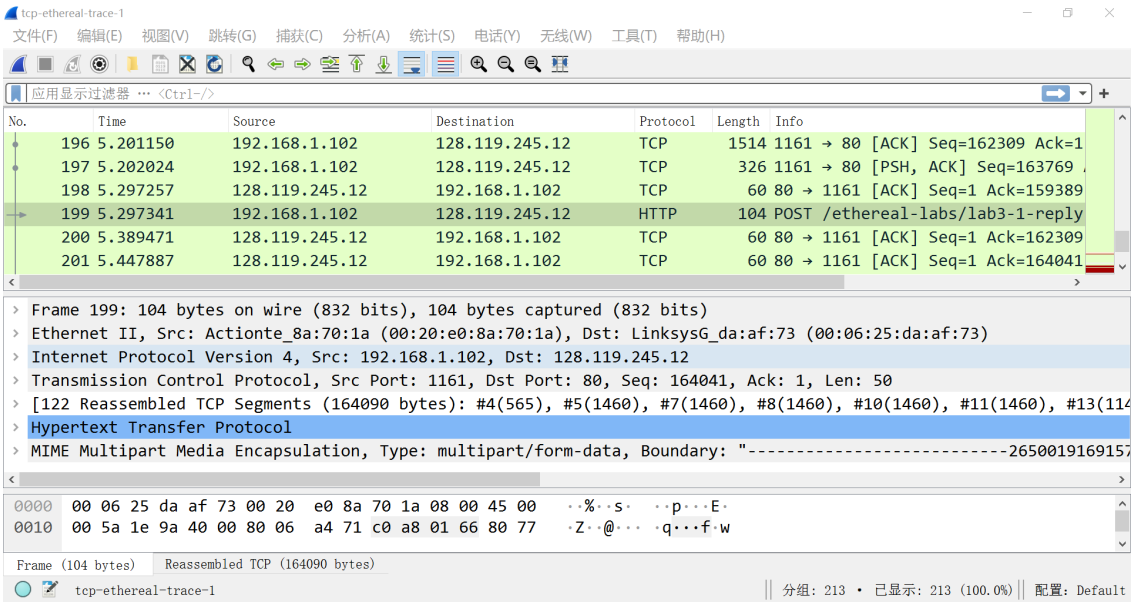
1. 在wireshark的过滤窗口输入“tcp”，对数据包进行过滤。

   得到wireshark界面如下图所示：



2. 打开http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip 中的 数据包文件 `tcp-ethereal-trace-1` 。

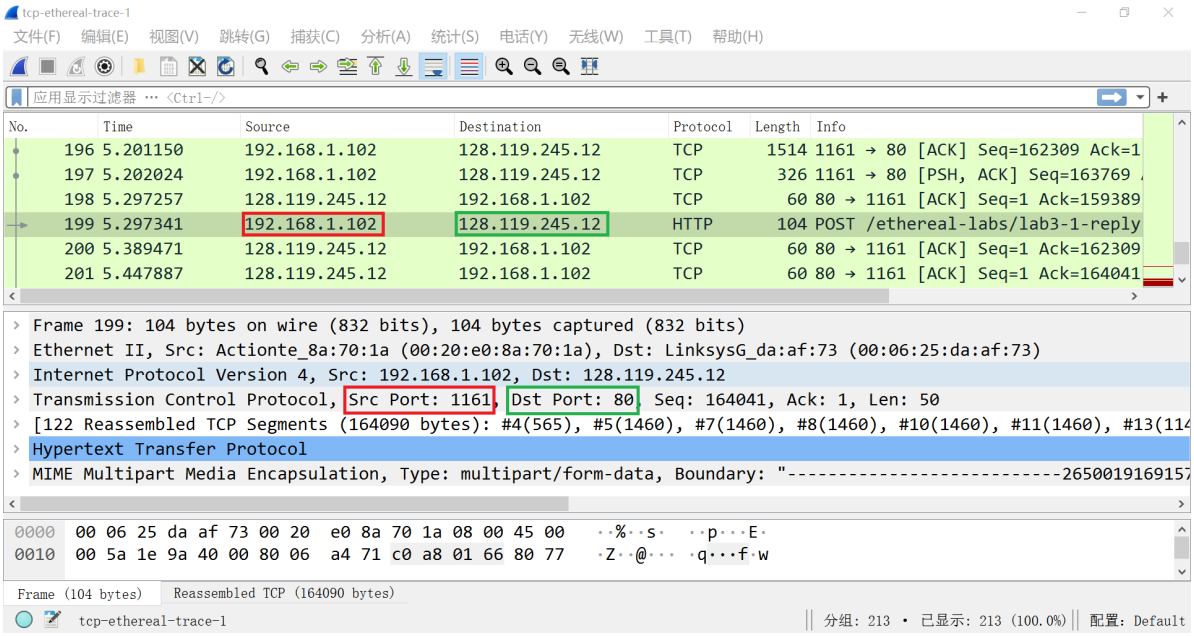
   打开此数据包文件后wireshark界面如下图所示：



回答以下问题：

> 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：HTTP POST讯息如下图所示：



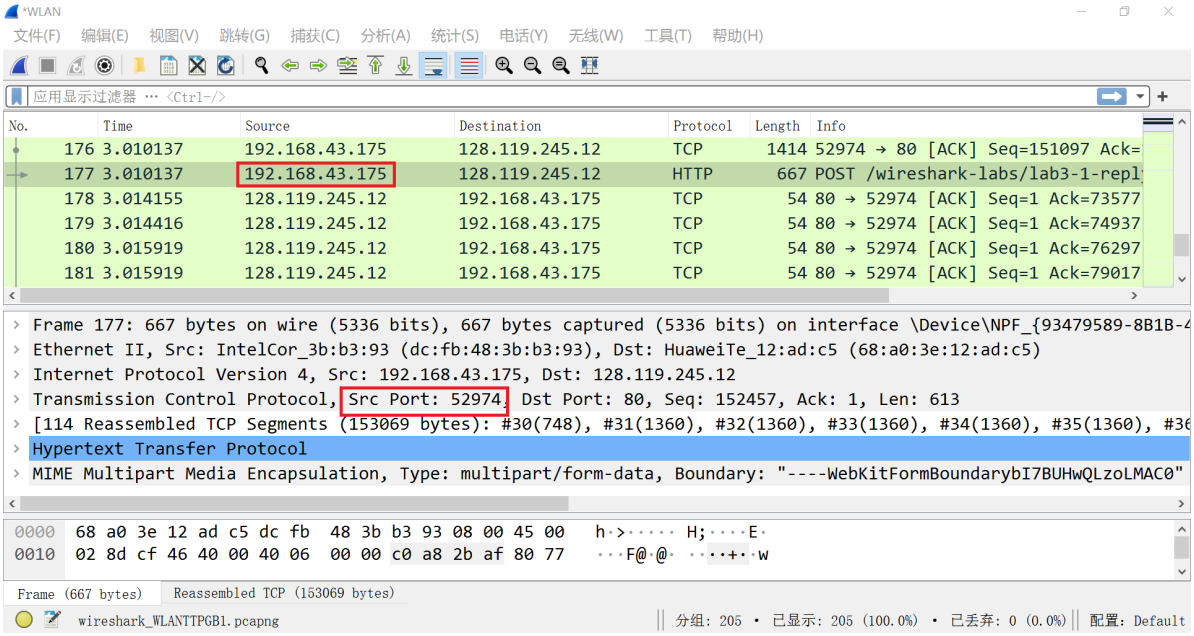
根据红色框中内容可知，源IP地址为**192.168.1.102**，源TCP端口号为**1161**。

> 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：根据上图中绿色框中内容可知，`gaia.cs.umass.edu`的IP地址为**128.119.245.12**，接收端口号为**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：本机HTTP POST讯息如下图所示：



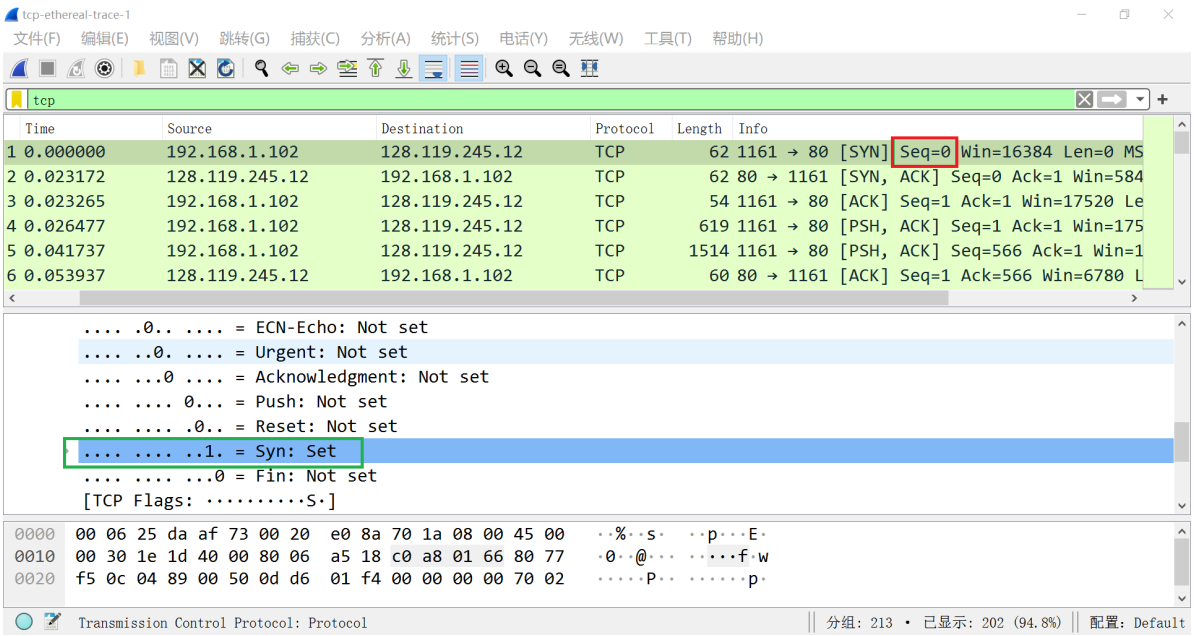
根据红色框中内容，本机源IP地址为**192.168.43.175**，源TCP端口号为**52974**。

3.TCP基础

通过读取`tcp-ethereal-trace-1`文件回答如下问题：

> 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?

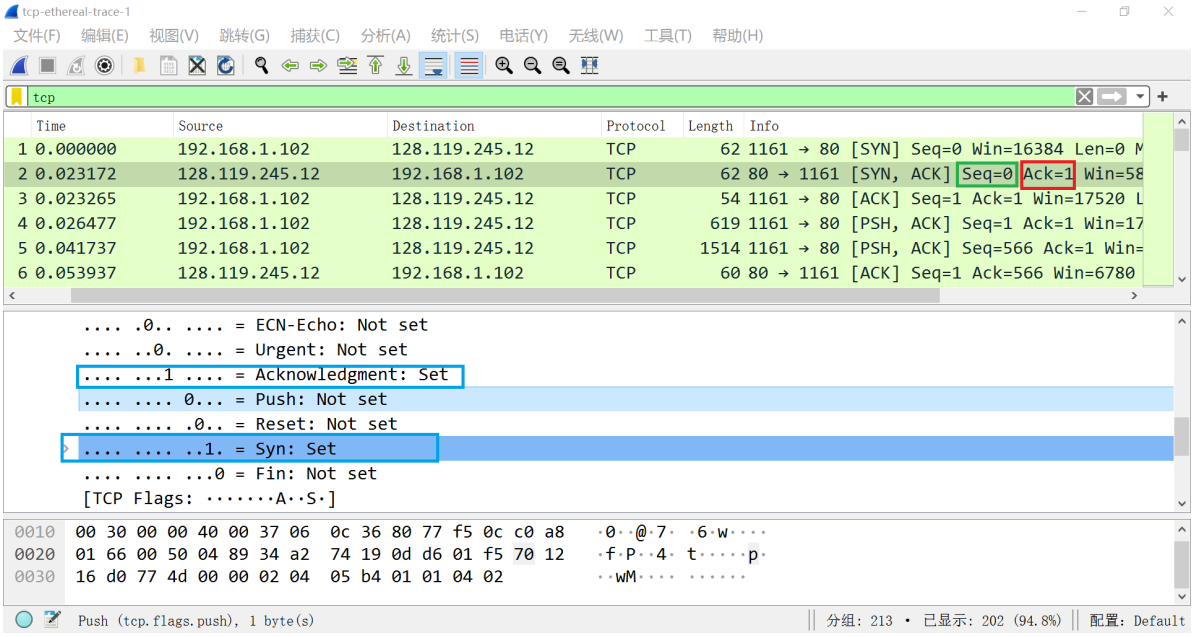
答：TCP SYN数据包信息如下图所示：



根据红色框中内容可知：`sequence number`为**0**；根据绿色框中内容，SYN标志为**1**，表示这一区段为SYN段，这是三次握手的第一步。

> 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：SYN ACK数据包信息如下图所示：



根据绿色框中内容，SYNACK区段的`sequence number`为**0**；

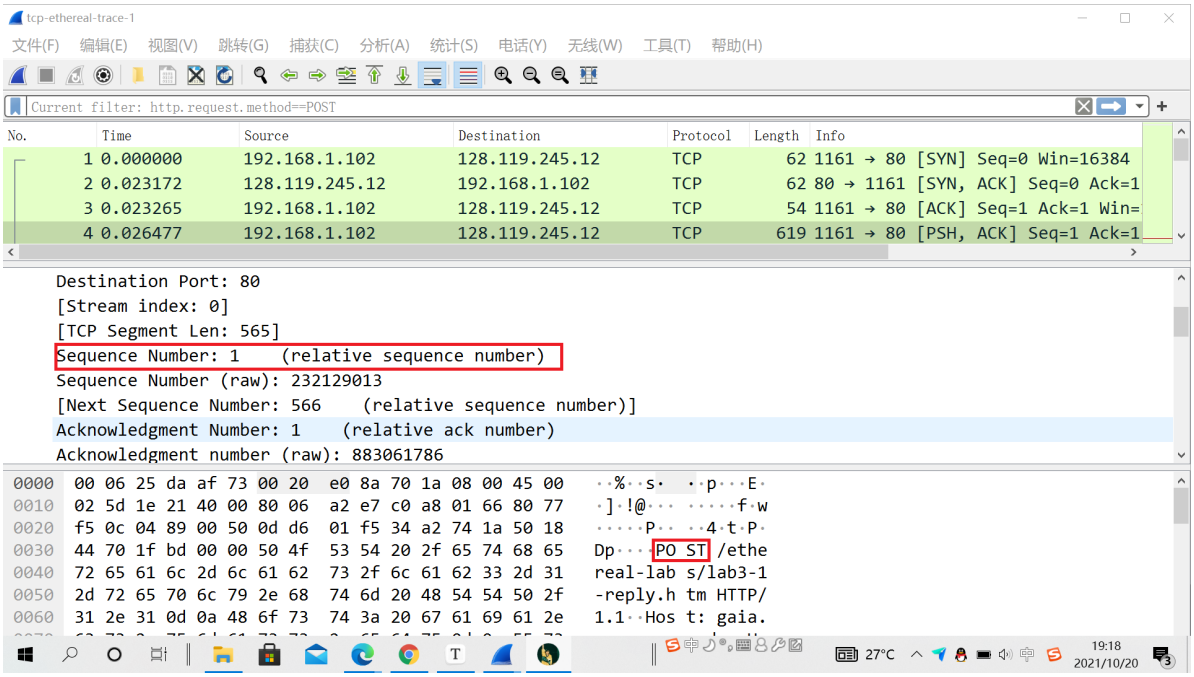
根据红色框中内容，SYNACK区段的`Acknowledgement field`为**1**；

Acknowledgement field = sequence number（SYN） + 1；

根据蓝色框中内容，SYN与Acknowledgment标志皆为**1**，表示这一区段为SYNACK区段，这是三次握手的第二步。

> 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.

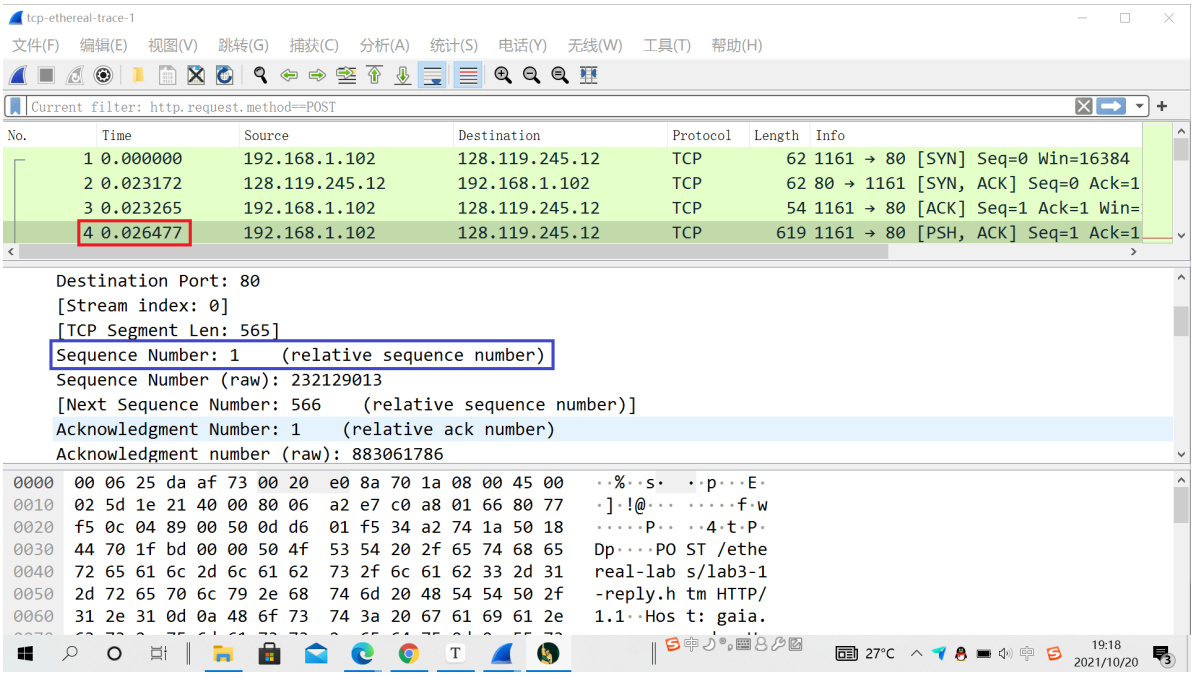
答：所求TCP区段如下图所示：

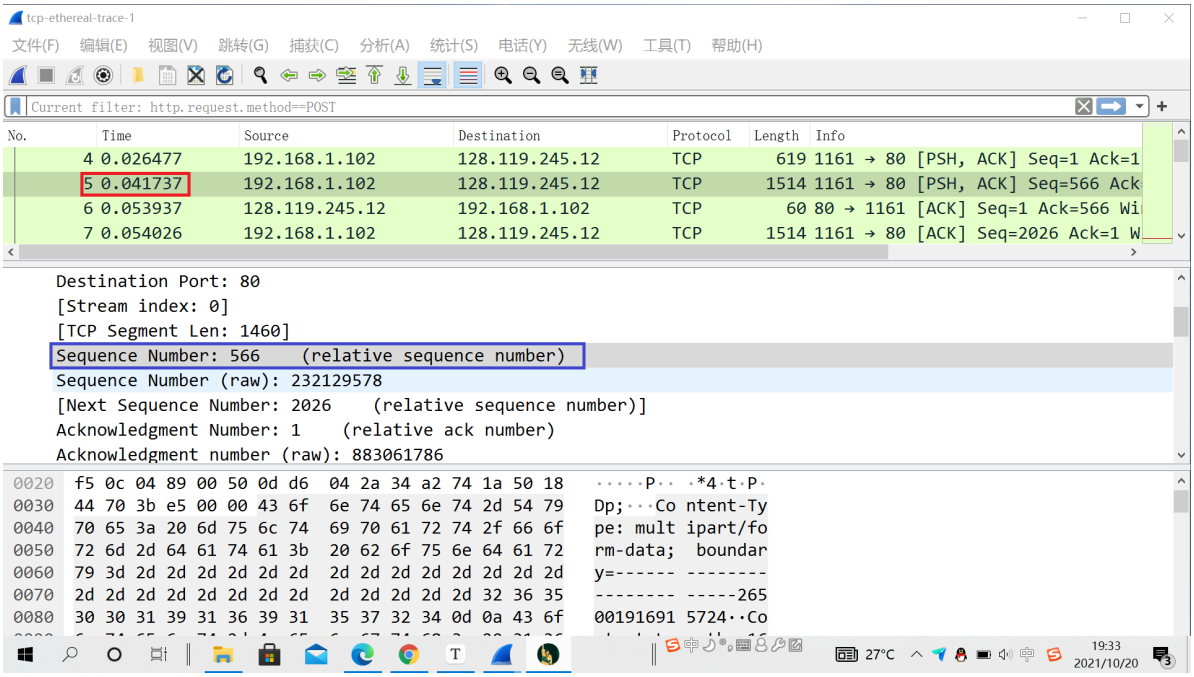


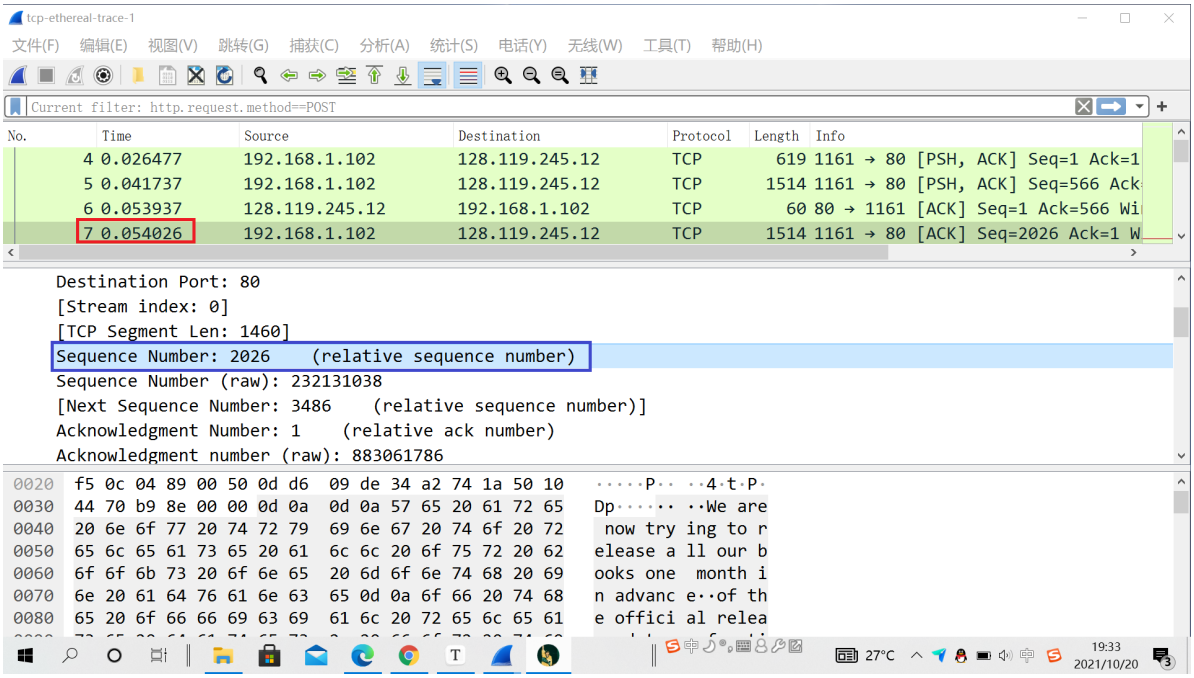
如上图红色框中所示，数据栏中**4**号数据包带有“POST”字段且`sequence number`为**1**。

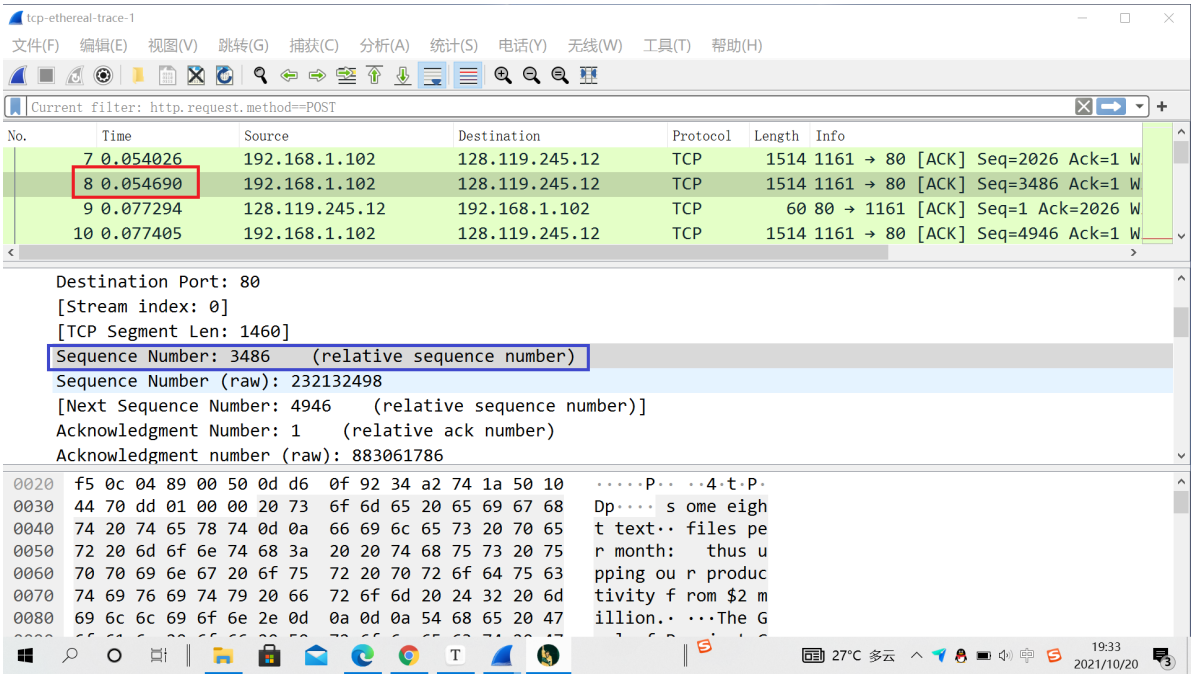
> 7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? 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 Section 3.5.3, page 242 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 242 for all subsequent segments.

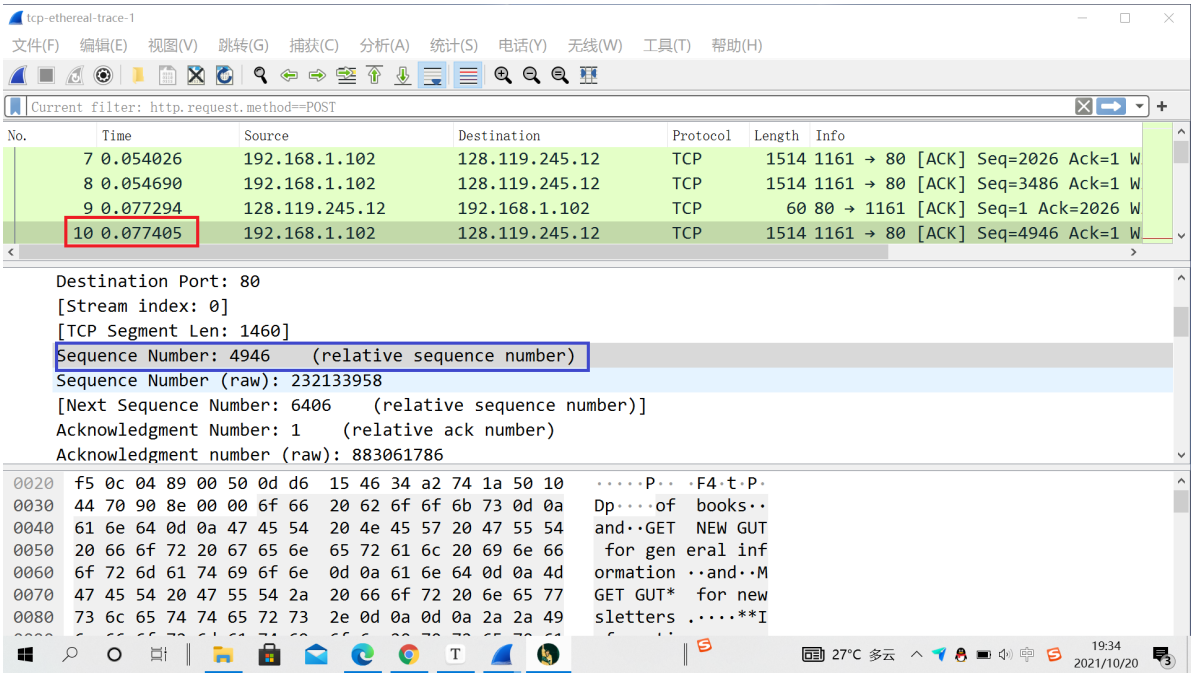
答：前六个TCP区段信息分别如下图所示：

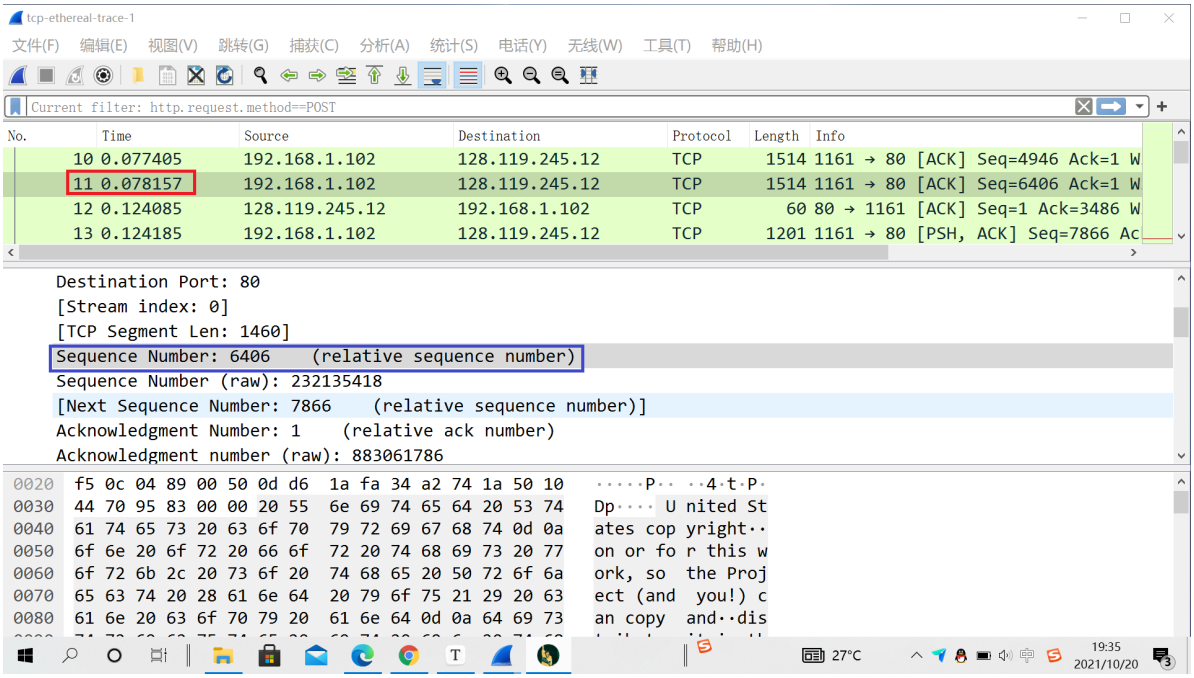



tcp-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: http.request.method==POST
No. Time Source Destination Protocol Length Info
4 0.026477 192.168.1.102 128.119.245.12 TCP 619 1161 → 80 [PSH, ACK] Seq=1 Ack=1
5 0.041737 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [PSH, ACK] Seq=566 Ack
6 0.053937 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=566 Wi
7 0.054026 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=2026 Ack=1 W
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence Number: 566 (relative sequence number)
Sequence Number (raw): 232129578
[Next Sequence Number: 2026 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0020 f5 0c 04 89 00 50 0d d6 04 2a 34 a2 74 1a 50 18 ·····P·· ·*4·t·P·
0030 44 70 3b e5 00 00 43 6f 6e 74 65 6e 74 2d 54 79 Dp;···Co ntent-Ty
0040 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f pe: mult ipart/fo
0050 72 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 rm-data; boundar
0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d y=------ --------
0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 36 35 -------- -----265
0080 30 30 31 39 31 36 39 31 35 37 32 34 0d 0a 43 6f 00191691 5724··Co
27°C
19:33
2021/10/20


tcp-ethereal-trace-1
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)
Current filter: http.request.method==POST
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
5 0.041737 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [PSH, ACK] Seq=566 Ack
6 0.053937 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=566 Wi
7 0.054026 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=2026 Ack=1 W
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence Number: 2026 (relative sequence number)
Sequence Number (raw): 232131038
[Next Sequence Number: 3486 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0020 f5 0c 04 89 00 50 0d d6 09 de 34 a2 74 1a 50 10 ·····P·· ··4·t·P·
0030 44 70 b9 8e 00 00 0d 0a 0d 0a 57 65 20 61 72 65 Dp····· ··We are
0040 20 6e 6f 77 20 74 72 79 69 6e 67 20 74 6f 20 72 now try ing to r
0050 65 6c 65 61 73 65 20 61 6c 6c 20 6f 75 72 20 62 elease a ll our b
0060 6f 6f 6b 73 20 6f 6e 65 20 6d 6f 6e 74 68 20 69 ooks one month i
0070 6e 20 61 64 76 61 6e 63 65 0d 0a 6f 66 20 74 68 n advanc e··of th
0080 65 20 6f 66 66 69 63 69 61 6c 20 72 65 6c 65 61 e offici al relea
27°C
19:33
2021/10/20


tcp-ethereal-trace-1
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)
Current filter: http.request.method==POST
No. Time Source Destination Protocol Length Info
7 0.054026 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=2026 Ack=1 W
8 0.054690 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=3486 Ack=1 W
9 0.077294 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=2026 W
10 0.077405 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=4946 Ack=1 W
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence Number: 3486 (relative sequence number)
Sequence Number (raw): 232132498
[Next Sequence Number: 4946 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0020 f5 0c 04 89 00 50 0d d6 0f 92 34 a2 74 1a 50 10 ·····P·· ··4·t·P·
0030 44 70 dd 01 00 00 20 73 6f 6d 65 20 65 69 67 68 Dp···· s ome eigh
0040 74 20 74 65 78 74 0d 0a 66 69 6c 65 73 20 70 65 t text·· files pe
0050 72 20 6d 6f 6e 74 68 3a 20 20 74 68 75 73 20 75 r month: thus u
0060 70 70 69 6e 67 20 6f 75 72 20 70 72 6f 64 75 63 pping ou r produc
0070 74 69 76 69 74 79 20 66 72 6f 6d 20 24 32 20 6d tivity f rom $2 m
0080 69 6c 6c 69 6f 6e 2e 0d 0a 0d 0a 54 68 65 20 47 illion.· ···The G
27°C 多云
19:33
2021/10/20





根据以上图中蓝色框中内容，前六个TCP区段序列号分别为：1,566,2026,3486,4946,6406；

根据以上图中红色框中内容，前六个TCP区段发送时间分别为：0.026477s,0.041737s,0.054026s,0.054690s,0.077405s,0.078157s。

收到ACK时间分别为：0.053937s,0.077294s,0.124085s,0.169118s,0.217299s,0.267802s。

两者相减得RTT分别为：0.02746s,0.035557s,0.070059s,0.114428s,0.139894s,0.189645s。

EstimatedRTT(1)=RTT(1)=0.02746s

EstimatedRTT(2)=0.875×EstimatedRTT+0.125×SampleRTT=0.875×0.02746+0.125×0.035557s≈0.028472s

EstimatedRTT(3)=0.875×EstimatedRTT+0.125×SampleRTT=0.875×0.028472+0.125×0.070059s≈0.03367s

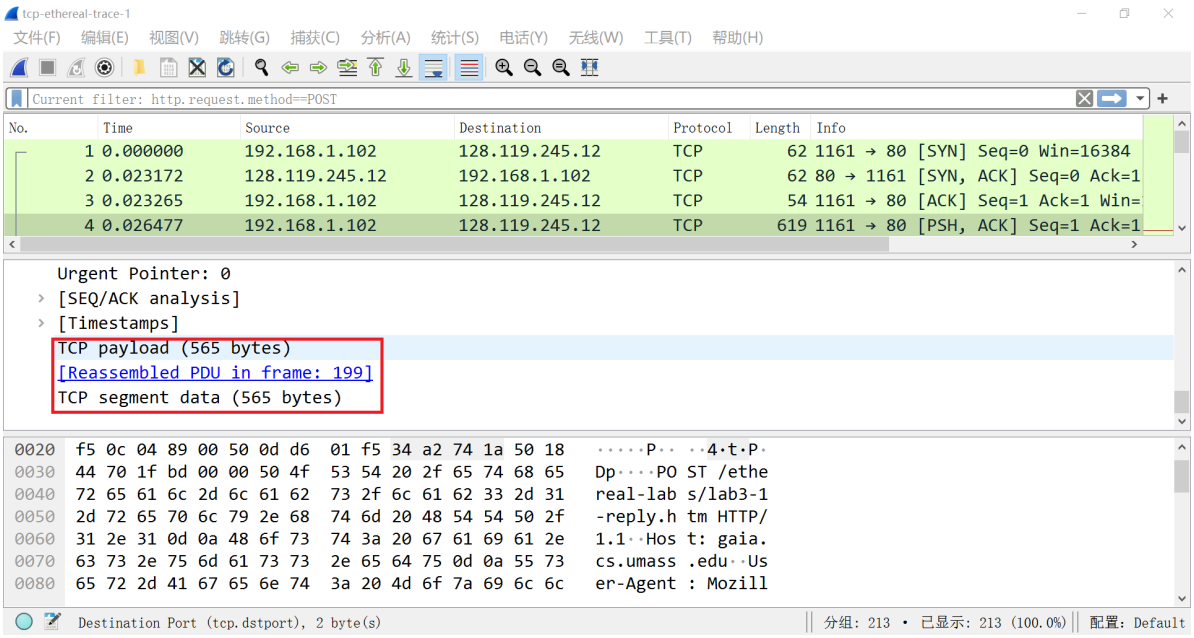
EstimatedRTT(4)=0.875×EstimatedRTT+0.125×SampleRTT=0.875×0.03367+0.125×0.114428s≈0.043765s

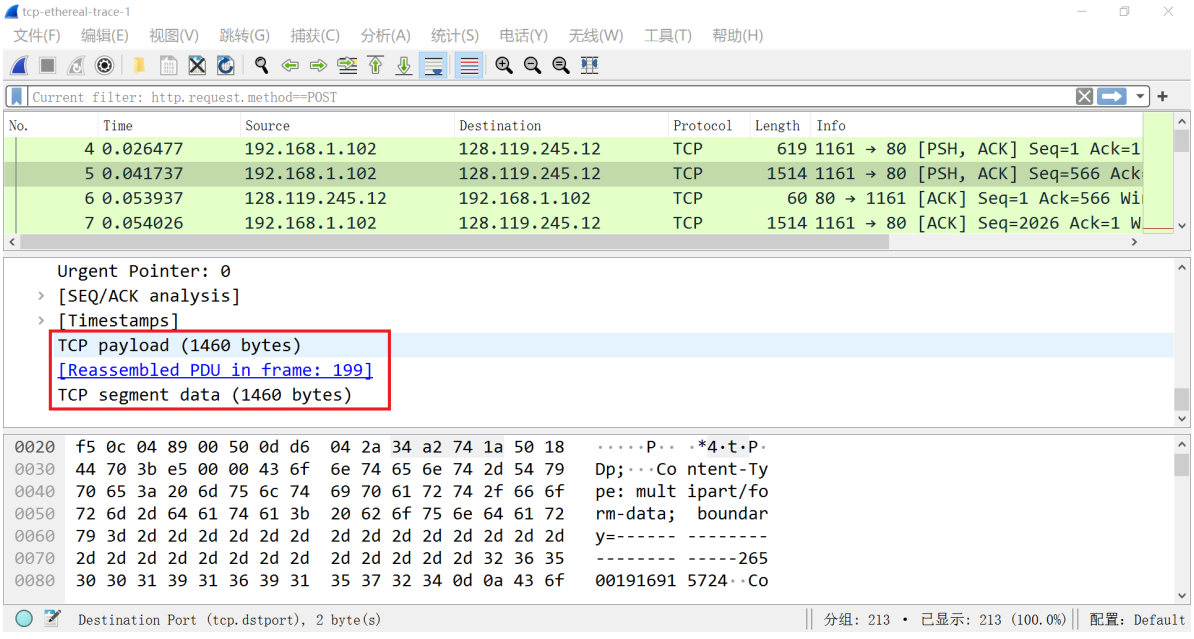
EstimatedRTT(5)=0.875×EstimatedRTT+0.125×SampleRTT=0.875×0.043765+0.125×0.139894s≈0.055781s

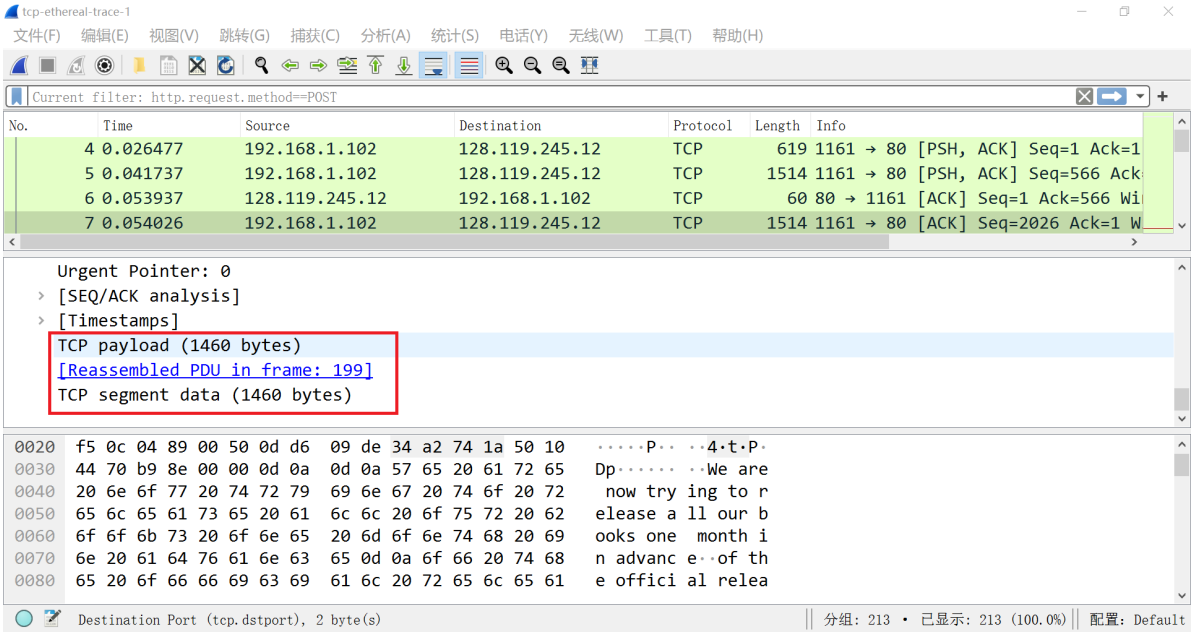
EstimatedRTT(6)=0.875×EstimatedRTT+0.125×SampleRTT=0.875×0.055781+0.125×0.189645s≈0.072514s

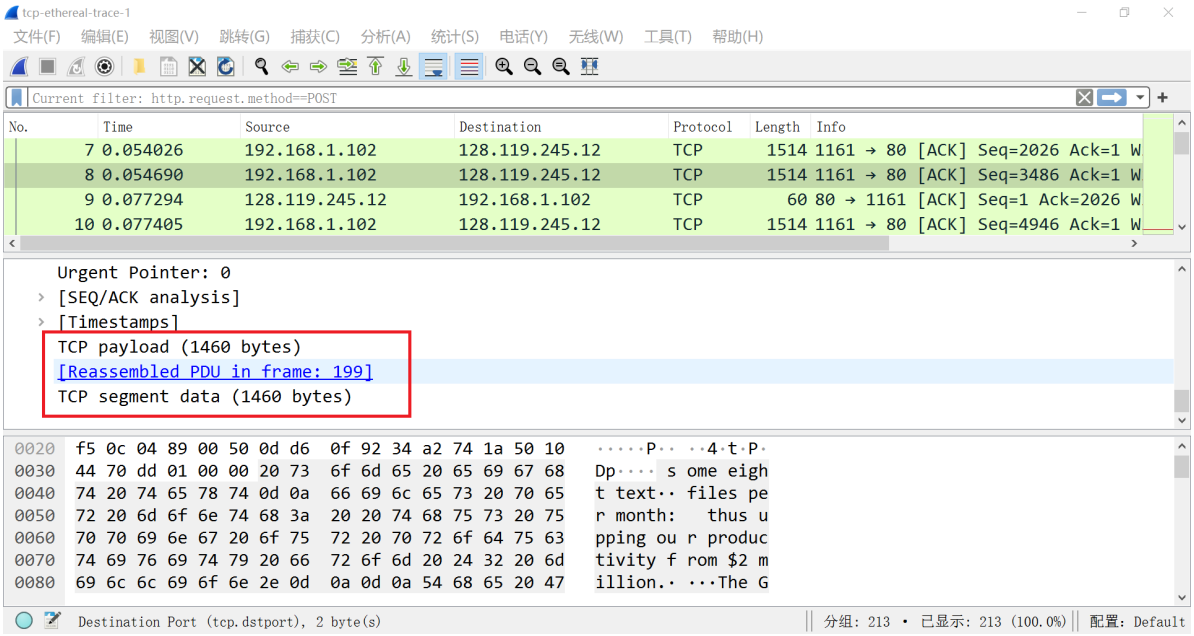
> 8. What is the length of each of the first six TCP segments?

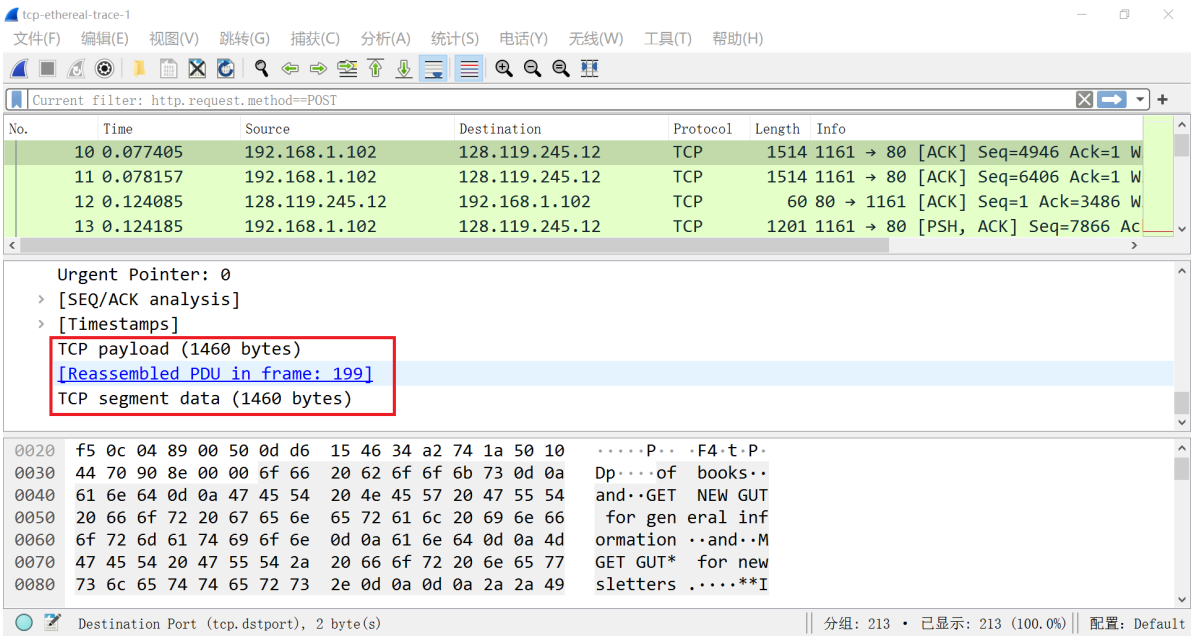
答：前六个TCP区段信息分别如下图所示：

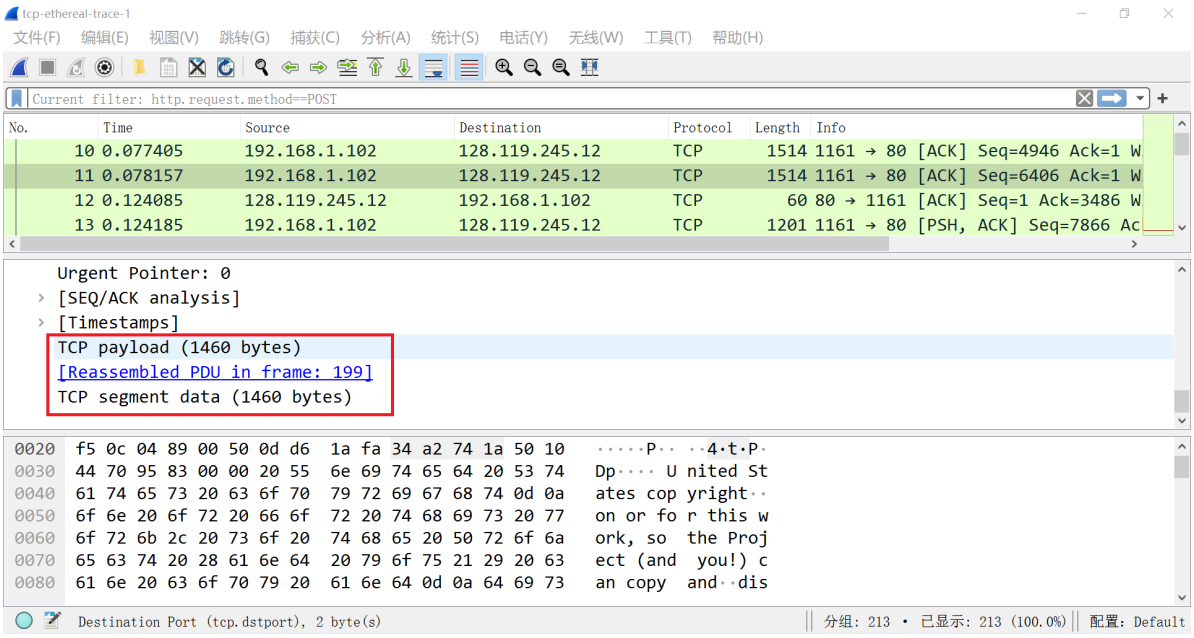





tcp-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: http.request.method==POST
No. Time Source Destination Protocol Length Info
4 0.026477 192.168.1.102 128.119.245.12 TCP 619 1161 → 80 [PSH, ACK] Seq=1 Ack=1
5 0.041737 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [PSH, ACK] Seq=566 Ack
6 0.053937 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=566 Wi
7 0.054026 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=2026 Ack=1 W
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1460 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (1460 bytes)
0020 f5 0c 04 89 00 50 0d d6 09 de 34 a2 74 1a 50 10 ·····P·· ··4·t·P·
0030 44 70 b9 8e 00 00 0d 0a 0d 0a 57 65 20 61 72 65 Dp····· ··We are
0040 20 6e 6f 77 20 74 72 79 69 6e 67 20 74 6f 20 72 now try ing to r
0050 65 6c 65 61 73 65 20 61 6c 6c 20 6f 75 72 20 62 elease a ll our b
0060 6f 6f 6b 73 20 6f 6e 65 20 6d 6f 6e 74 68 20 69 ooks one month i
0070 6e 20 61 64 76 61 6e 63 65 0d 0a 6f 66 20 74 68 n advanc e··of th
0080 65 20 6f 66 66 69 63 69 61 6c 20 72 65 6c 65 61 e offici al relea
Destination Port (tcp.dstport), 2 byte(s)
分组: 213 · 已显示: 213 (100.0%)
配置: Default


tcp-ethereal-trace-1
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)
Current filter: http.request.method==POST
No. Time Source Destination Protocol Length Info
7 0.054026 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=2026 Ack=1 W
8 0.054690 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=3486 Ack=1 W
9 0.077294 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=2026 W
10 0.077405 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=4946 Ack=1 W
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1460 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (1460 bytes)
0020 f5 0c 04 89 00 50 0d d6 0f 92 34 a2 74 1a 50 10 ·····P·· ··4·t·P·
0030 44 70 dd 01 00 00 20 73 6f 6d 65 20 65 69 67 68 Dp···· s ome eigh
0040 74 20 74 65 78 74 0d 0a 66 69 6c 65 73 20 70 65 t text·· files pe
0050 72 20 6d 6f 6e 74 68 3a 20 20 74 68 75 73 20 75 r month: thus u
0060 70 70 69 6e 67 20 6f 75 72 20 70 72 6f 64 75 63 pping ou r produc
0070 74 69 76 69 74 79 20 66 72 6f 6d 20 24 32 20 6d tivity f rom $2 m
0080 69 6c 6c 69 6f 6e 2e 0d 0a 0d 0a 54 68 65 20 47 illion.· ···The G
Destination Port (tcp.dstport), 2 byte(s)
分组: 213 · 已显示: 213 (100.0%)
配置: Default

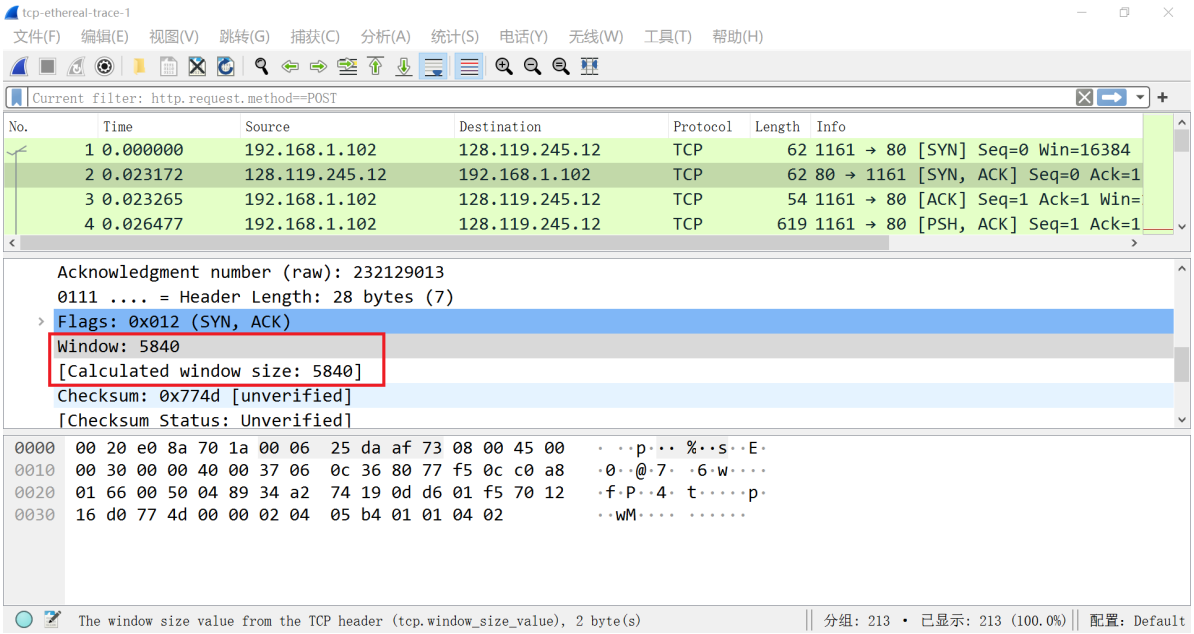

tcp-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: http.request.method==POST
No. Time Source Destination Protocol Length Info
10 0.077405 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=4946 Ack=1 W
11 0.078157 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=6406 Ack=1 W
12 0.124085 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=3486 W
13 0.124185 192.168.1.102 128.119.245.12 TCP 1201 1161 → 80 [PSH, ACK] Seq=7866 Ac
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1460 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (1460 bytes)
0020 f5 0c 04 89 00 50 0d d6 15 46 34 a2 74 1a 50 10 ·····P·· ·F4·t·P·
0030 44 70 90 8e 00 00 6f 66 20 62 6f 6f 6b 73 0d 0a Dp····of books··
0040 61 6e 64 0d 0a 47 45 54 20 4e 45 57 20 47 55 54 and··GET NEW GUT
0050 20 66 6f 72 20 67 65 6e 65 72 61 6c 20 69 6e 66 for gen eral inf
0060 6f 72 6d 61 74 69 6f 6e 0d 0a 61 6e 64 0d 0a 4d ormation ··and··M
0070 47 45 54 20 47 55 54 2a 20 66 6f 72 20 6e 65 77 GET GUT* for new
0080 73 6c 65 74 74 65 72 73 2e 0d 0a 0d 0a 2a 2a 49 sletters .····**I
Destination Port (tcp.dstport), 2 byte(s)
分组: 213 · 已显示: 213 (100.0%)
配置: Default



由上图红色框中可知，第一个TCP区段长度为565bytes，后五个TCP区段长度为1460bytes。

> 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：关于数据包最小可用缓冲区空间量的信息如下图所示：



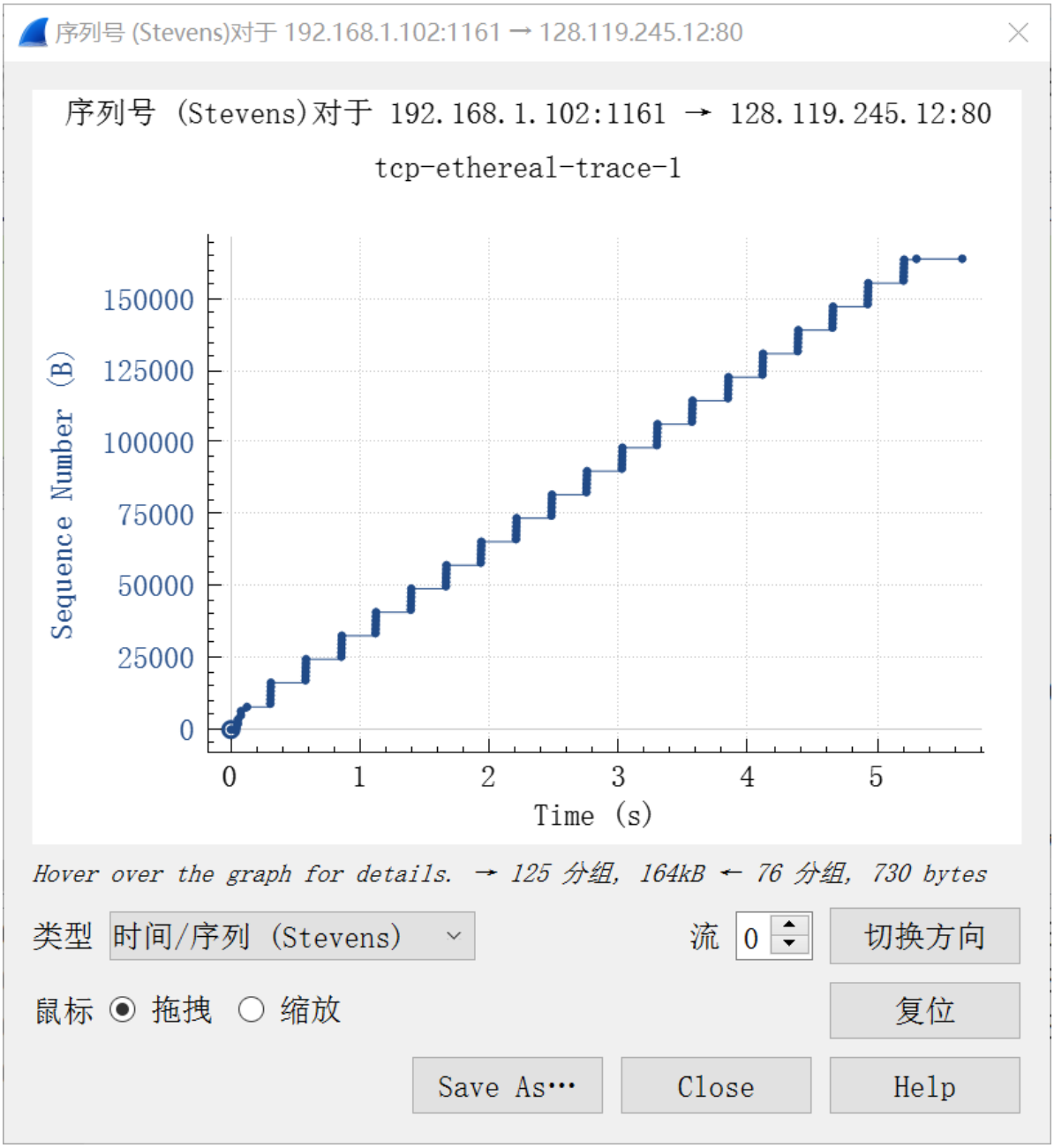
故数据包的最小可用缓冲区空间量为5840bytes。

若缺少接收器缓冲区空间，则接收器将能不断接收TCP区段，发送方将不会被限制。

> 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：**没有重传的区段。**

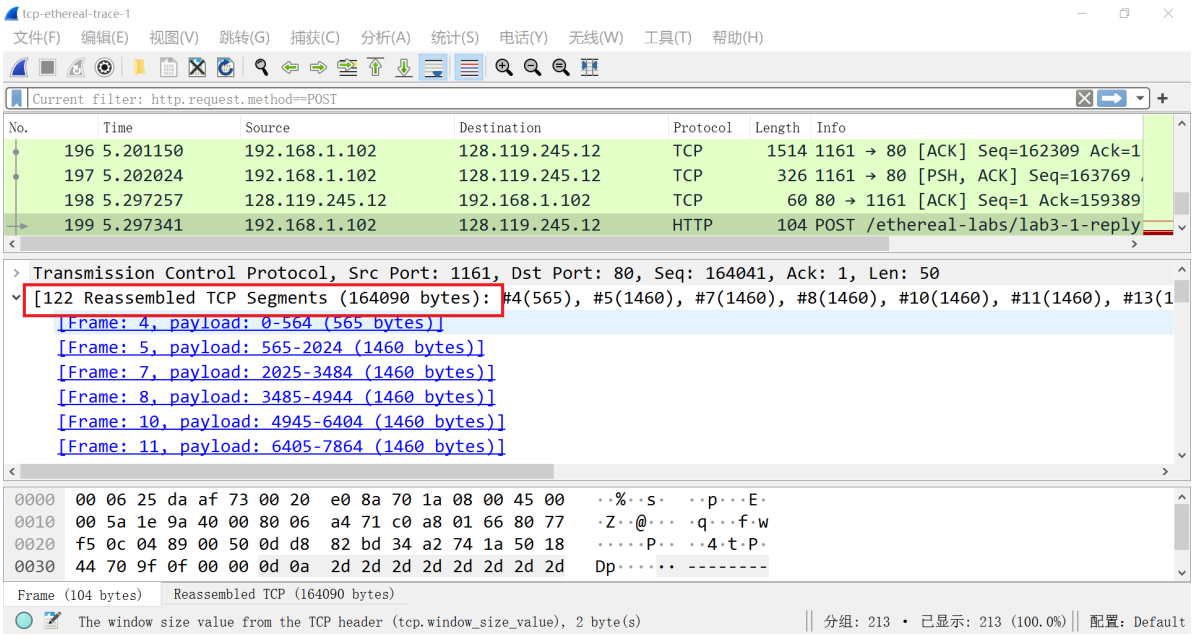
通过检查wireshark中的`Time-Sequence-Graph(Stevens)`观察时序图如下：



如上图所示，随着时间推移，不存在重传的`sequence number`，故没有重传的区段。

> 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 250 in the text).

答：通过观察HTTP POST数据包信息如下图所示：



根据上图红色框中内容可知：接收器确认数据为164090bytes。

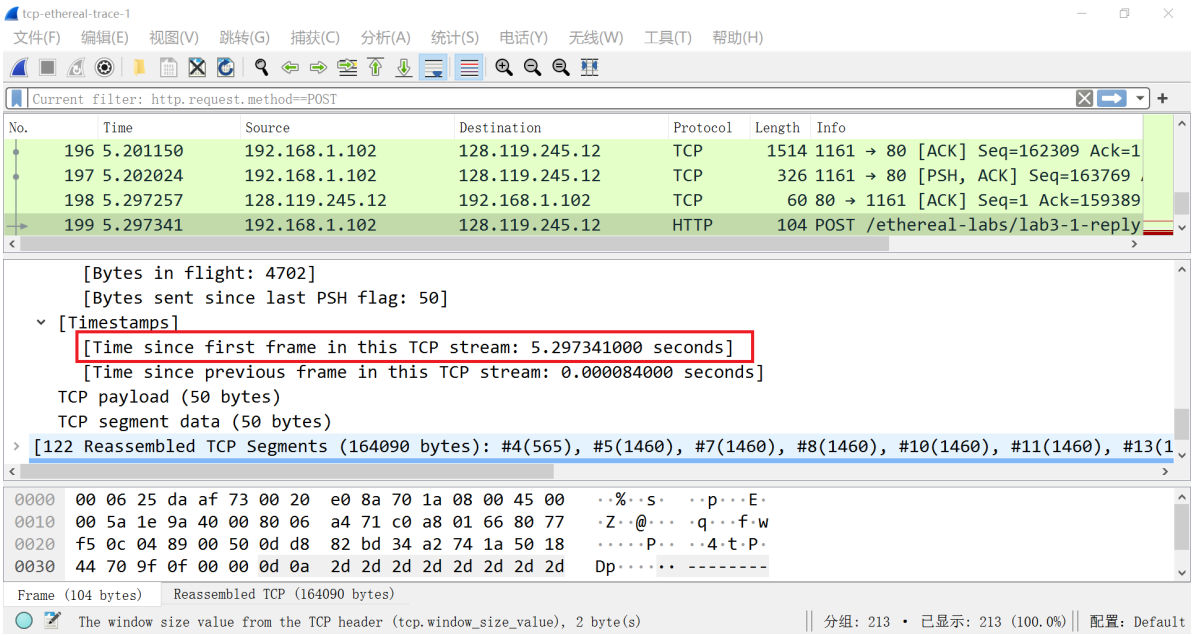
能够识别接收方每隔一个区段才发送的情况，由于连续两个 ACK 的确认序列号之间的差异表示服务器在这两个 ACK 之间接收的数据，可以根据ACK序列号的顺序来识别。

> 12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

答：吞吐量=数据大小/时间

由11题可知，数据大小为164090bytes；

有关时间信息如下图所示：



根据红色框中内容，时间为5.297341s

故吞吐量=164090/5.297341 bytes/s = 30975.91792 bytes/s = 30.976Kb/s

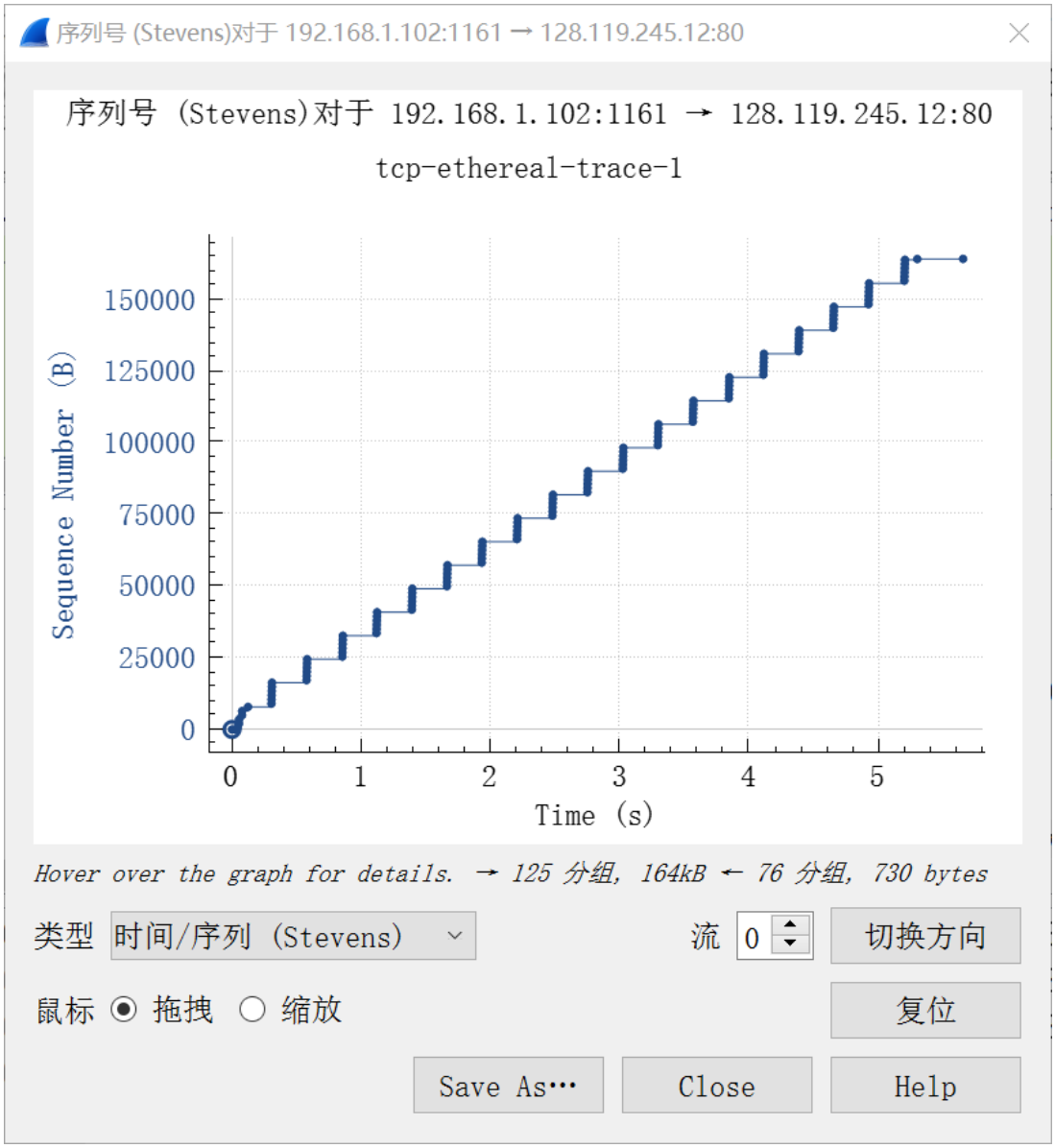
4.TCP拥塞控制

检查从客户端服务器的每单位时间发送的数据量，利用wireshark的时序图绘制数据。

回答如下问题：

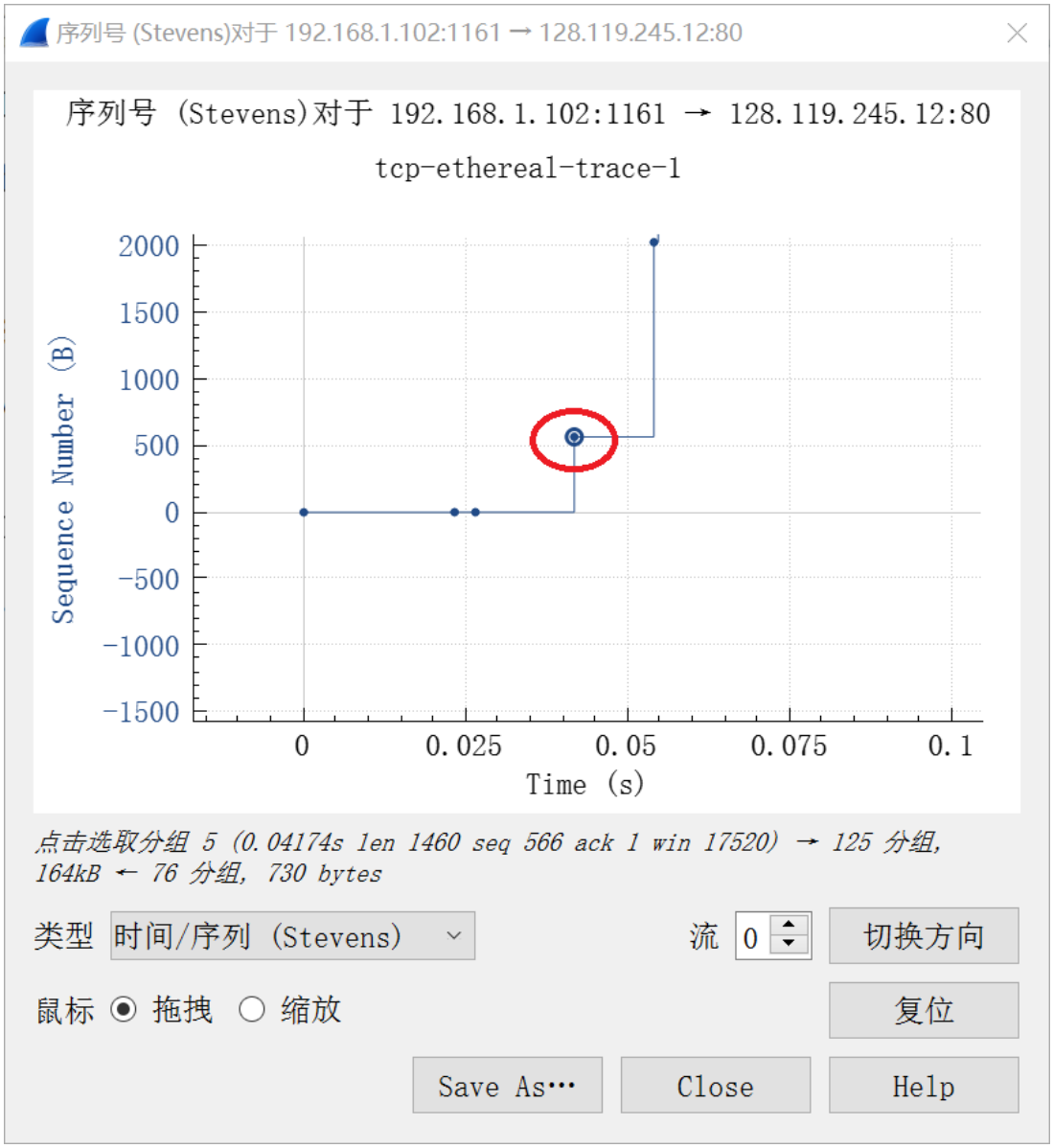
> 13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.

答：使用绘图工具获得的时序图如下图所示：

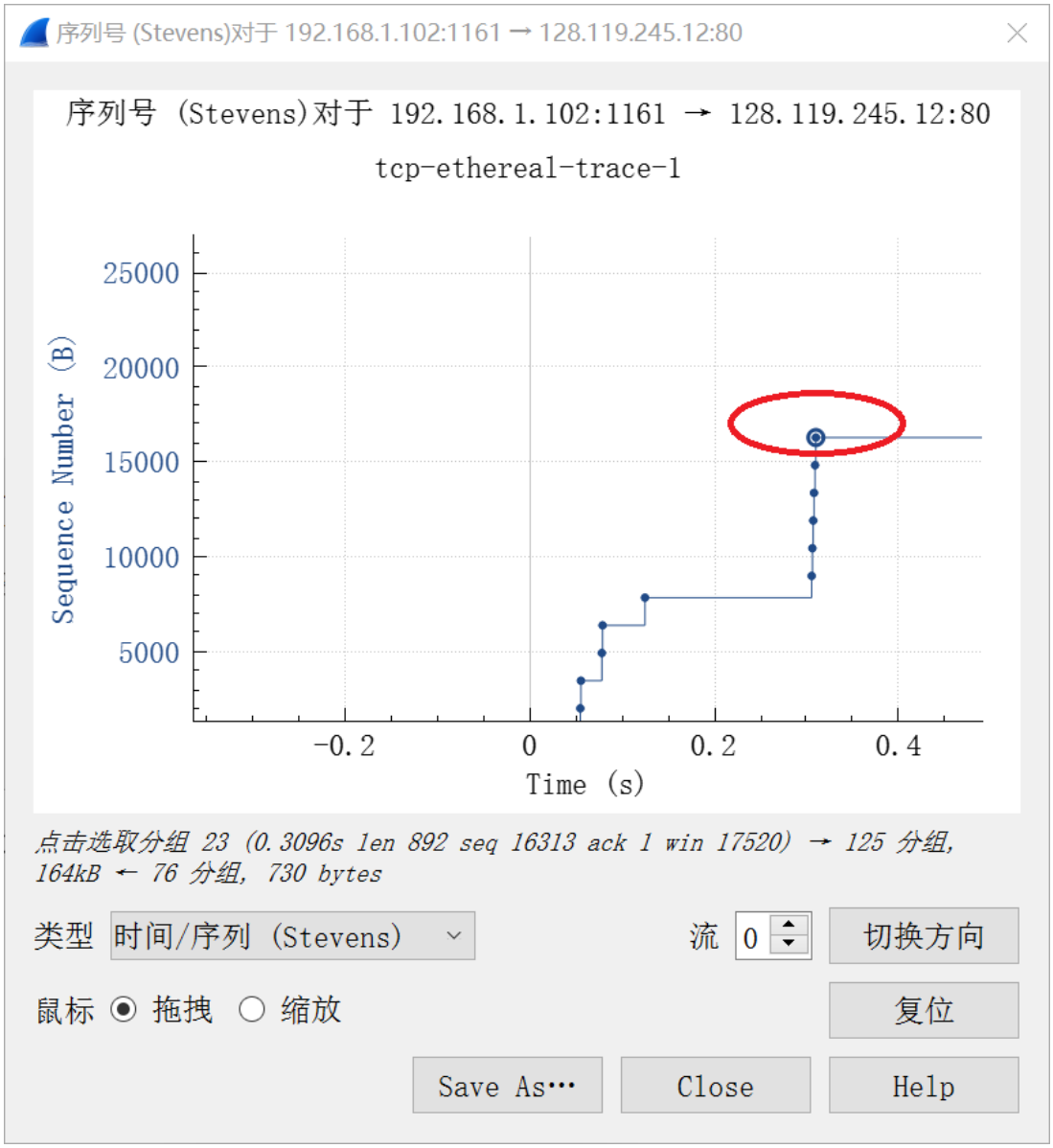


通过放大时序图中的信息，观察发送速率的变化；

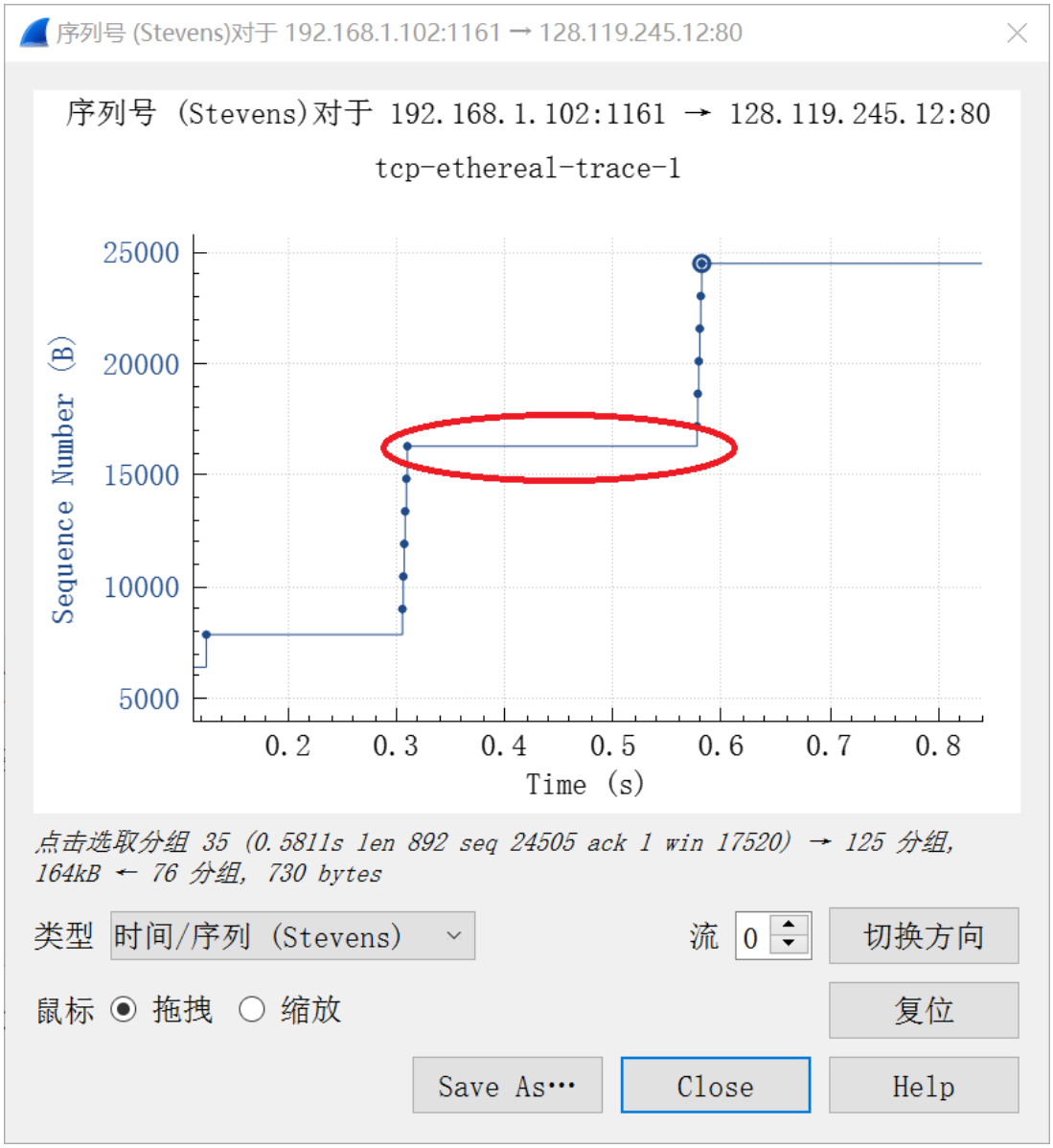
已知：慢启动表示发送速率呈指数型增长。



根据上图红色框，慢启动开始于第一个TCP区段发送的时候，即为分组 5 发送的时候；



根据上图红色框，慢启动结束于指数型增长中断的时候，即为分组`23`发送的时候；



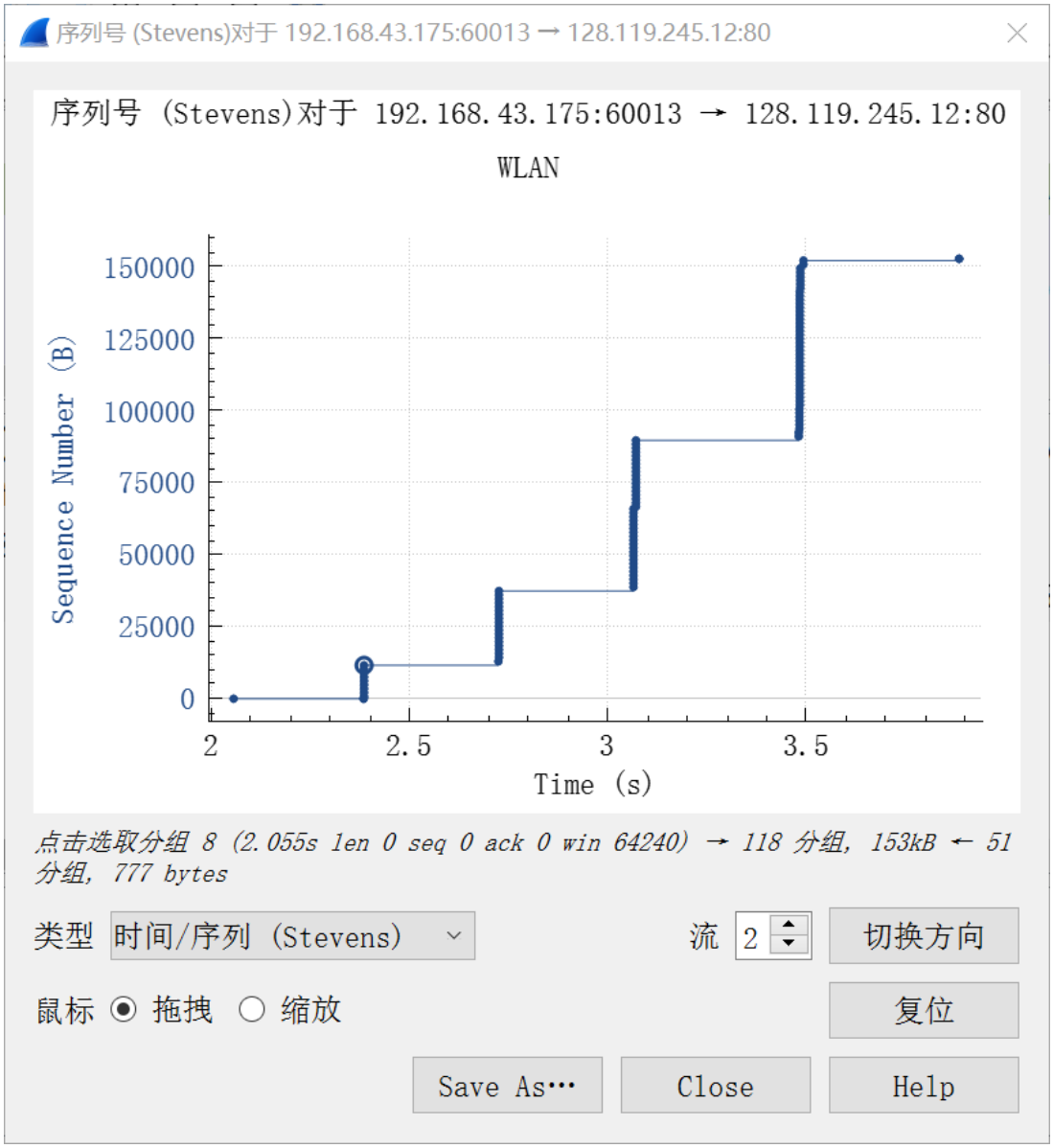
上图红色框中部分即为拥塞避免部分。

不同之处：

对于一些数据量较小的文件，在网络状况良好的前提下发送较快，甚至在慢启动结束之前便已发送完毕——故此时慢启动反而限制了小文件的发送，导致了传输的低效。进而可知慢启动并非适用于所有的传输情况。

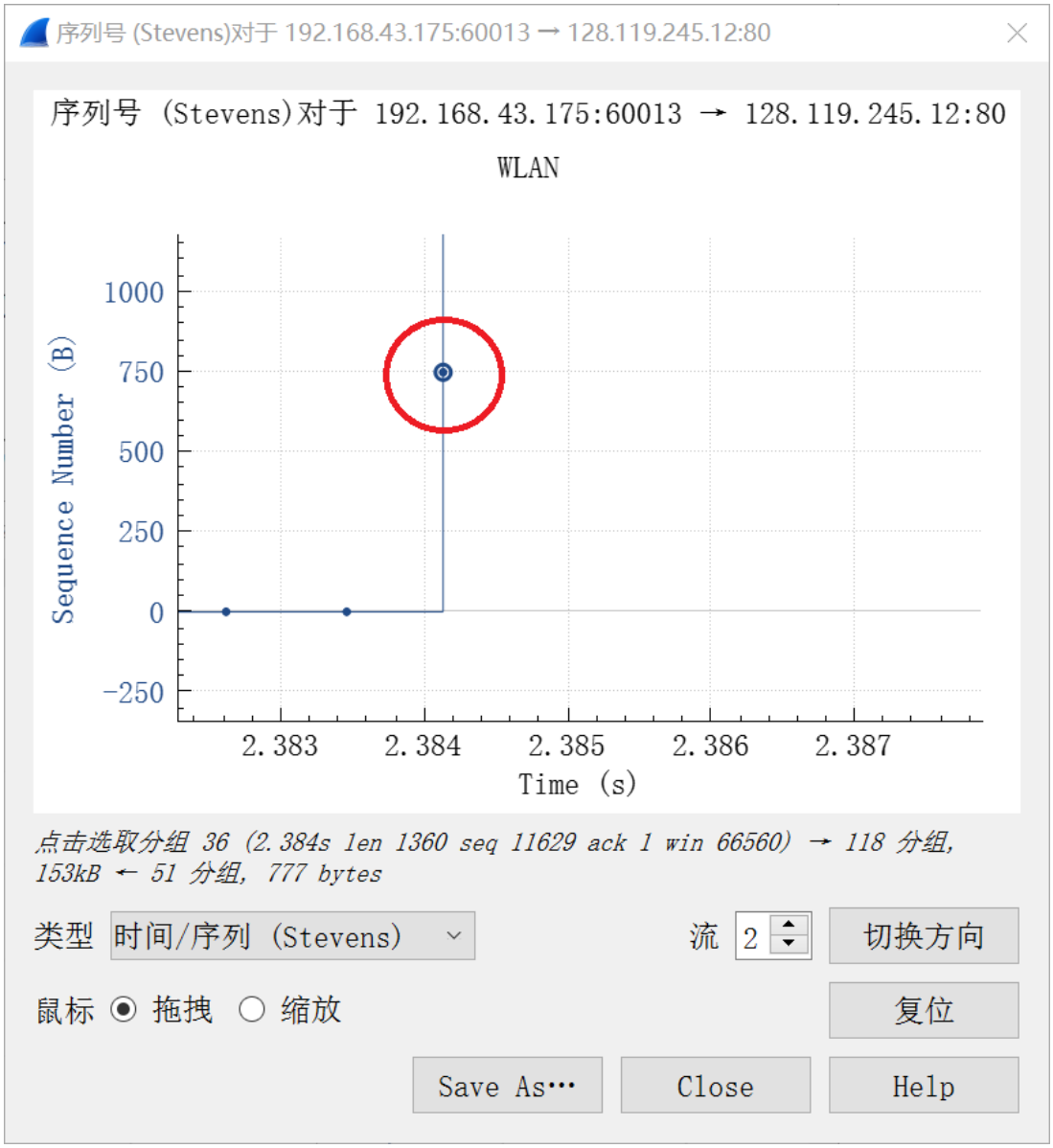
> 14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu.

答：使用绘图工具获得的时序图如下图所示：

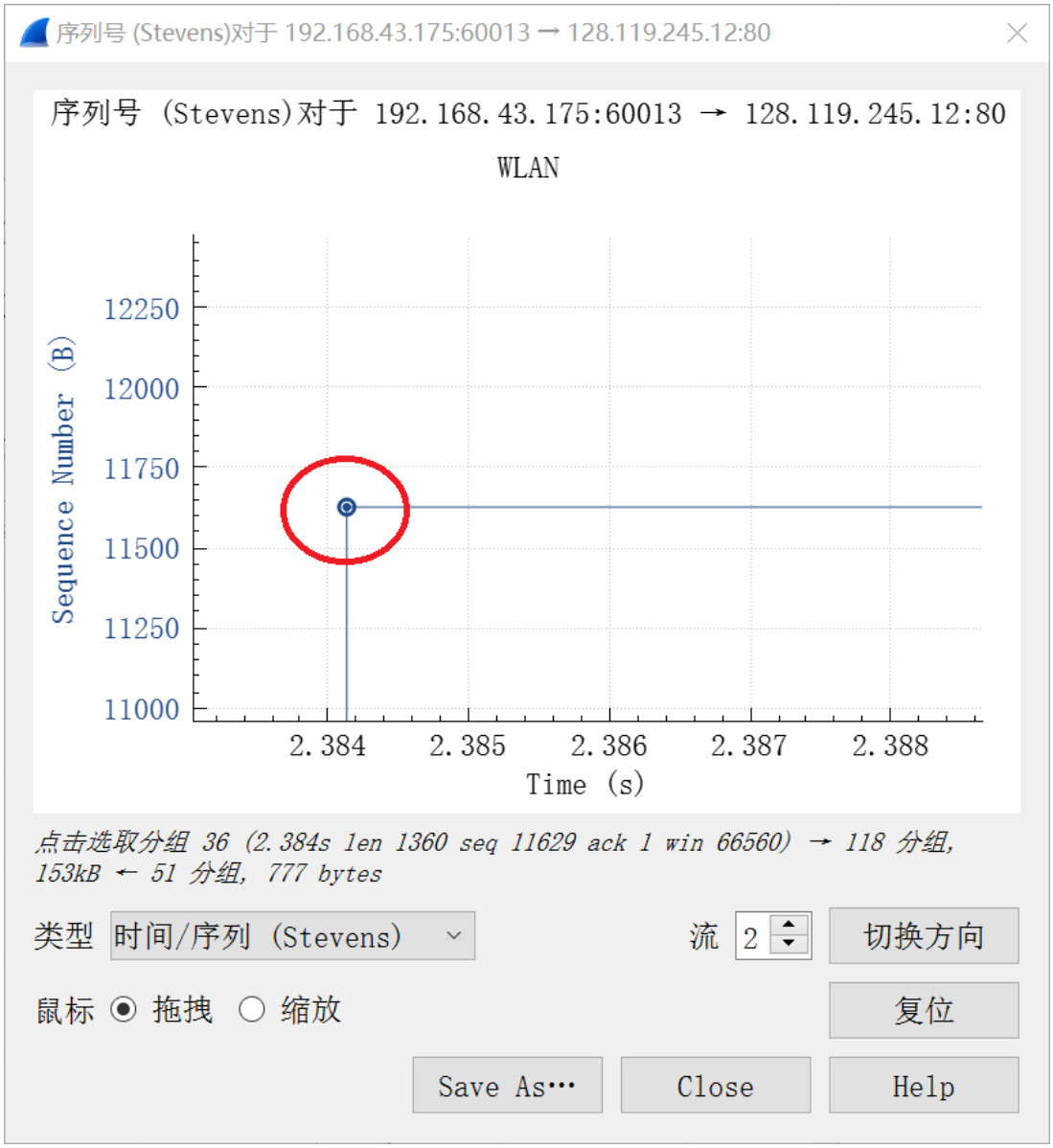


通过放大时序图中的信息，观察发送速率的变化；

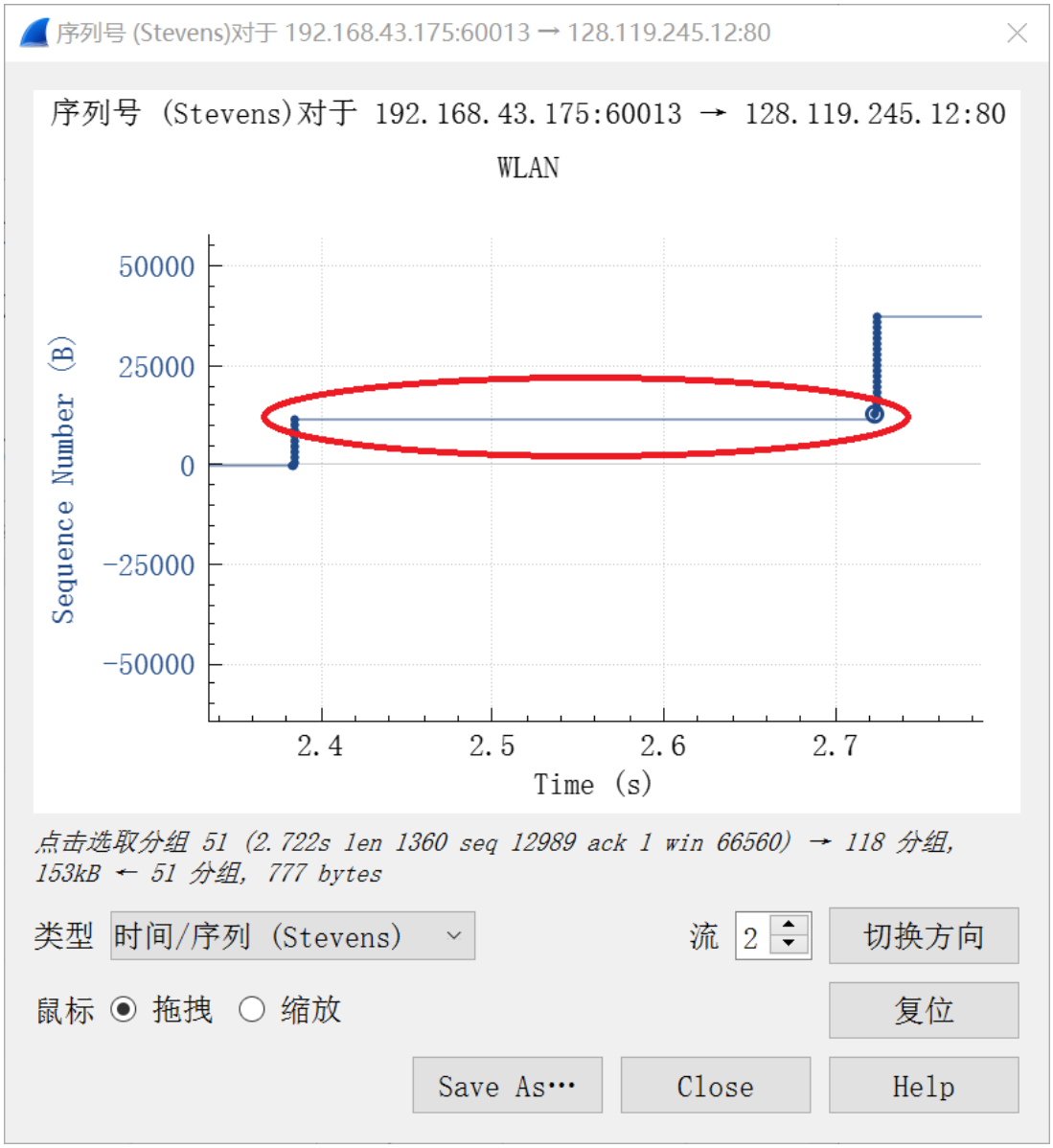
已知：慢启动表示发送速率呈指数型增长。



根据上图红色框，慢启动开始于第一个TCP区段发送的时候，即为分组 36 发送的时候；



根据上图红色框，慢启动结束于指数型增长中断的时候，即为分组`36`发送结束的时候；



上图红色框中部分即为拥塞避免部分。

不同之处：同`13`问。

四.实验收获与感想

1. 深入理解了TCP的SEQ与ACK序列号和确认号在TCP协议的作用。
2. 深入理解了TCP三次握手的过程。
3. 深入理解了TCP的拥塞控制。
4. 学习了有关TCP协议的数据的抓取和计算。
5. 进一步理解了TCP报文段的结构。
6. 加强了对wireshark的了解和运用，了解了更多数据的抓取位置和时序图的使用与观察。