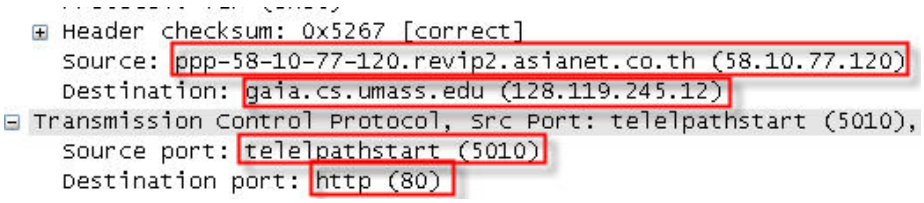
CNT IT51066406

Lab 4 Wireshark Lab : TCP

By it51066406

Capturing a bulk TCP transfer from your computer to a remote server

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).
answer source IP address is 58.10.77.120 , source TCP port is 5010 .



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?
answer IP address of gaia.cs.umass.edu is 128.119.245.12, port number of sending and receiving TCP segments is 80 . (From picture sequence 1)

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?
answer IP address is Local IP , TCP port is Local port .

TCP Basics

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?
answer 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 is 0 , SYS segment is 1 .

```
Destination port: http (80)
Sequence number: 0    (relative sequence number)
Header length: 28 bytes
Flags: 0x02 (SYN)
  0... .... = Congestion Window Reduced (CWR): Not set
  .0.. .... = ECN-Echo: Not set
  ..0. .... = Urgent: Not set
  ...0 .... = Acknowledgment: Not set
  .... 0... = Push: Not set
  .... .0.. = Reset: Not set
  .... ..1. = Syn: Set
  .... ...0 = Fin: Not set
Window size: 65535
```

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?

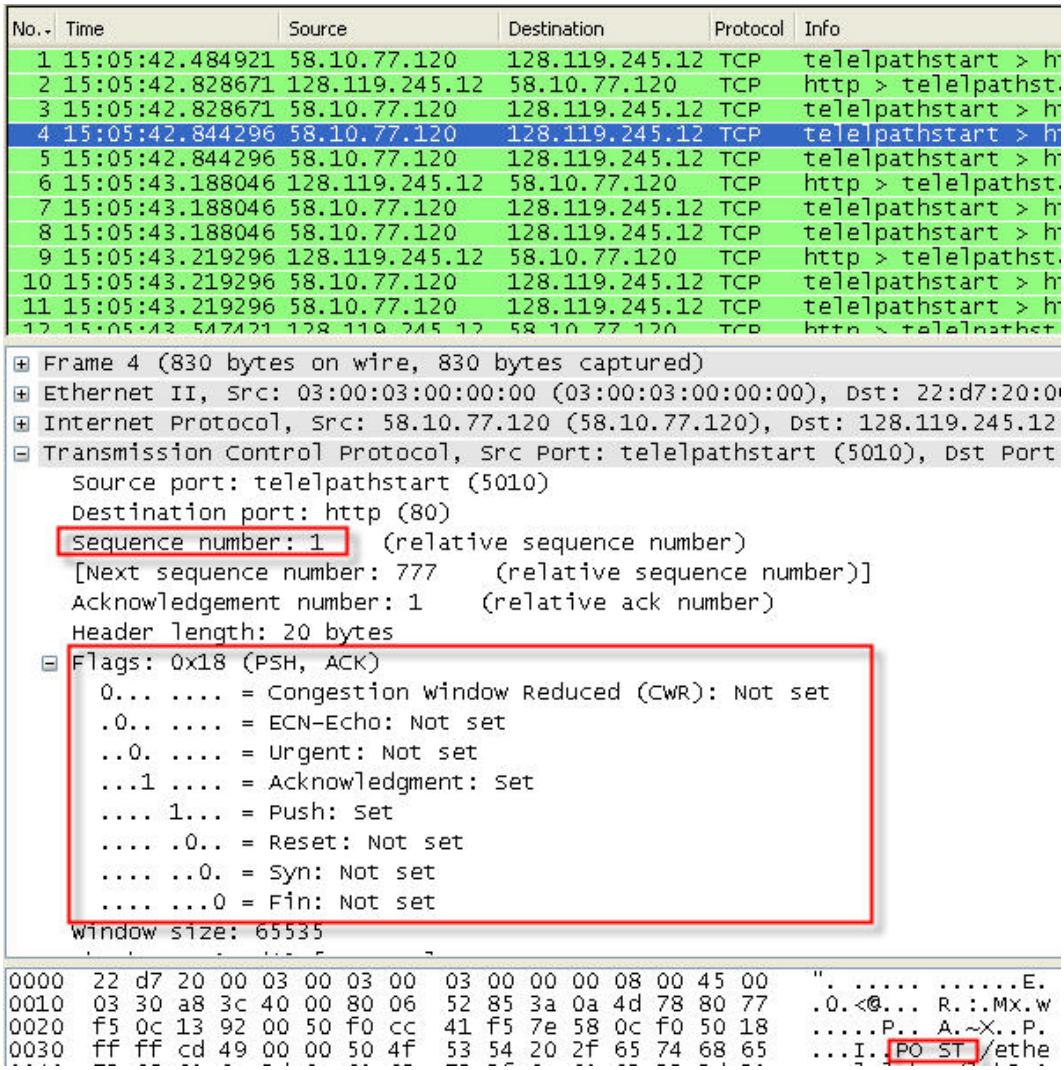
answer sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0 , value of the ACKnowledgement field in the SYNACK segment is 1 , SYNACK segment is 1.

No.	Time	Source	Destination	Protocol
1	15:05:42.484921	58.10.77.120	128.119.245.12	TCP
2	15:05:42.828671	128.119.245.12	58.10.77.120	TCP
3	15:05:42.828671	58.10.77.120	128.119.245.12	TCP
4	15:05:42.844296	58.10.77.120	128.119.245.12	TCP
5	15:05:42.844296	58.10.77.120	128.119.245.12	TCP
6	15:05:43.188046	128.119.245.12	58.10.77.120	TCP
7	15:05:43.188046	58.10.77.120	128.119.245.12	TCP
8	15:05:43.188046	58.10.77.120	128.119.245.12	TCP
9	15:05:43.219296	128.119.245.12	58.10.77.120	TCP
10	15:05:43.219296	58.10.77.120	128.119.245.12	TCP
11	15:05:43.219296	58.10.77.120	128.119.245.12	TCP
12	15:05:43.547421	128.119.245.12	58.10.77.120	TCP

```
Transmission Control Protocol, Src Port: http (80), Dst Por
  Source port: http (80)
  Destination port: telelpathstart (5010)
  Sequence number: 0    (relative sequence number)
  Acknowledgement number: 1    (relative ack number)
  Header length: 28 bytes
  Flags: 0x12 (SYN, ACK)
    0... .... = Congestion Window Reduced (CWR): 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
  Window size: 5840
  Checksum: 0x9d4d [correct]
  Options: (8 bytes)
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 1]
    [The RTT to ACK the segment was: 0.343750000 seconds]
```

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.

answer sequence number of the TCP segment containing the HTTP POST command is FRAME 4 .



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. Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph->Round Trip Time Graph.

answer HTTP POST segment is No. 4,5,7,8,10,11.

ACK segment is No. 6,9,12,14,15,16.

Segment 1 Sequence Number is 1

Segment 2 Sequence Number is 777

Segment 3 Sequence Number is 2203

Segment 4 Sequence Number is 3629

Segment 5 Sequence Number is 5055

Segment 6 Sequence Number is 6481

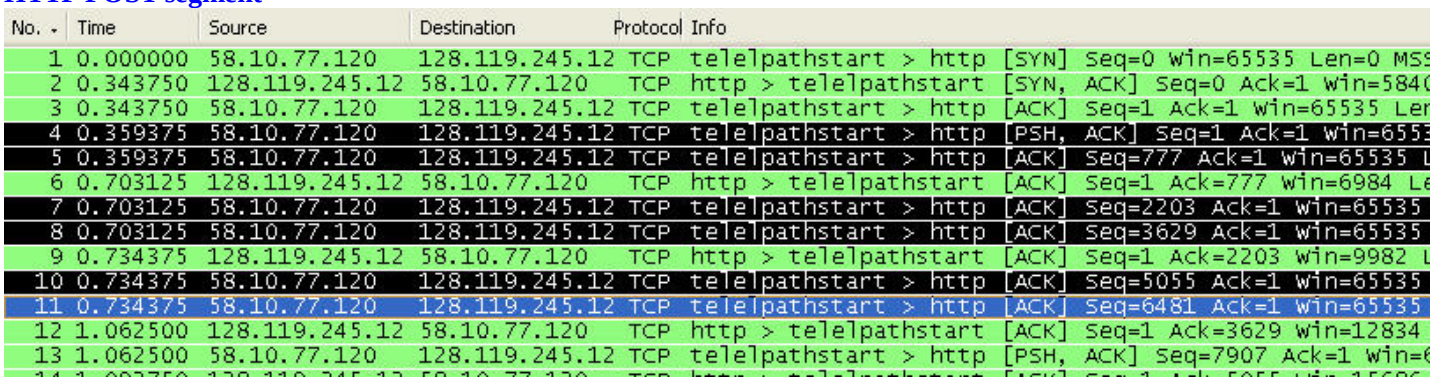
	send time	**ACK**	**RTT**
Segment 1	0.359375	0.703125	0.34375
Segment 2	0.359375	0.734375	0.375
Segment 3	0.703125	1.062500	0.359375
Segment 4	0.703125	1.093750	0.390625
Segment 5	0.734375	1.109375	0.375

Segment 6 0.734375 1.140625 0.40625

Calculated EstimatedRTT :

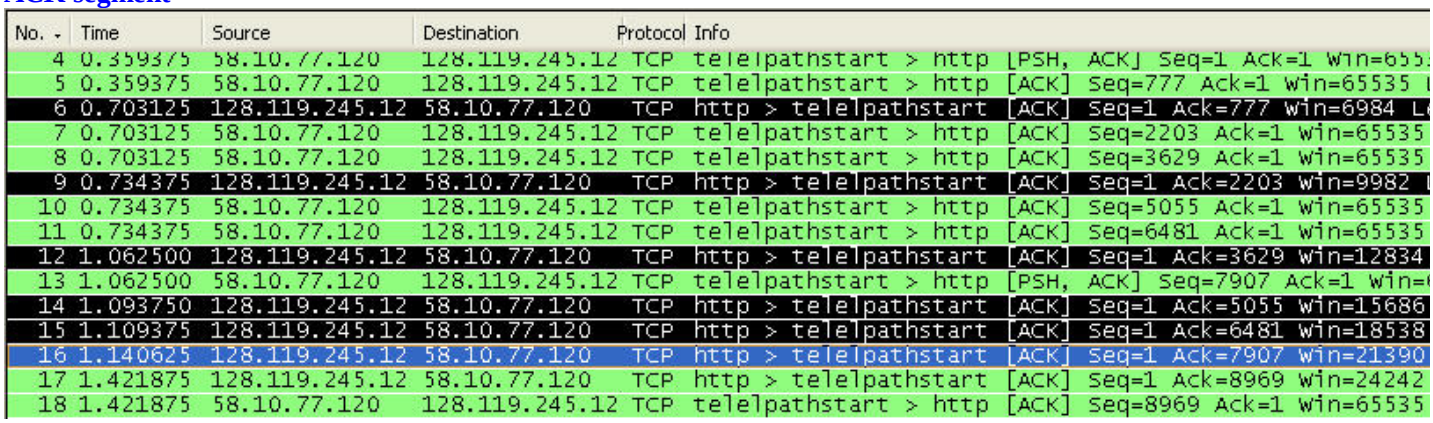
EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT
EstimatedRTT of Segment 1 = 0.34375
EstimatedRTT of Segment 2 = 0.875 * 0.34375 + 0.125 *0.375 = 0.3475
EstimatedRTT of Segment 3 = 0.875 * 0.3475 + 0.125 *0.359375 = 0.3489
EstimatedRTT of Segment 4 = 0.875 * 0.3489 + 0.125 *0.390625 = 0.3541
EstimatedRTT of Segment 5 = 0.875 * 0.3541 + 0.125 *0.375 = 0.3567
EstimatedRTT of Segment 6 = 0.875 * 0.3567 + 0.125 * 0.40625 = 0.3628

HTTP POST segment



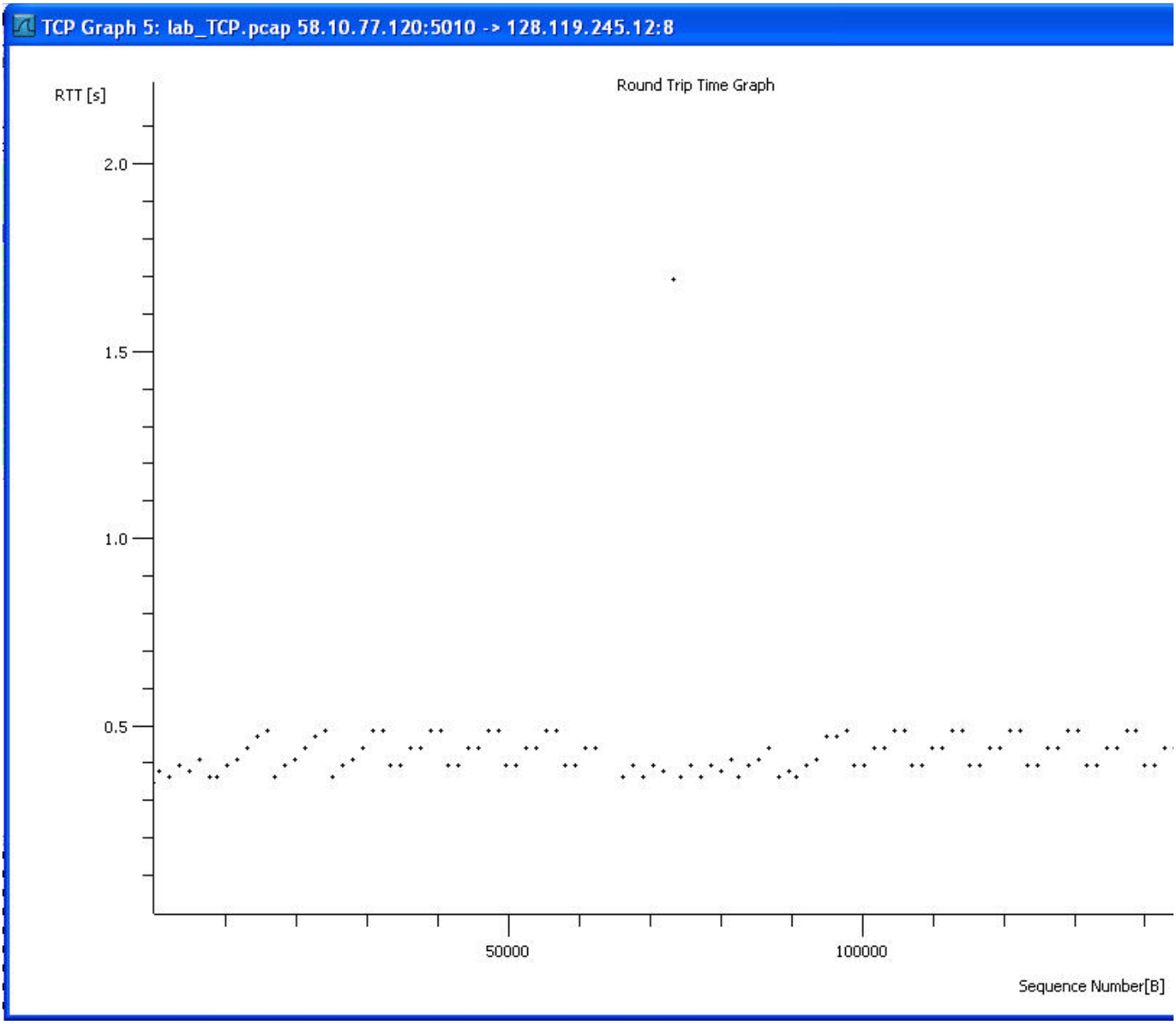
No.	Time	Source	Destination	Protocol	Info
1	0.000000	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [SYN] Seq=0 Win=65535 Len=0 MSS
2	0.343750	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [SYN, ACK] Seq=0 Ack=1 Win=584(
3	0.343750	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=1 Ack=1 Win=65535 Len
4	0.359375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [PSH, ACK] Seq=1 Ack=1 Win=6553
5	0.359375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=777 Ack=1 Win=65535 L
6	0.703125	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=777 Win=6984 Le
7	0.703125	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=2203 Ack=1 Win=65535
8	0.703125	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=3629 Ack=1 Win=65535
9	0.734375	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=2203 Win=9982 L
10	0.734375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=5055 Ack=1 Win=65535
11	0.734375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=6481 Ack=1 Win=65535
12	1.062500	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=3629 Win=12834
13	1.062500	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [PSH, ACK] Seq=7907 Ack=1 Win=6

ACK segment



No.	Time	Source	Destination	Protocol	Info
4	0.359375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [PSH, ACK] Seq=1 Ack=1 Win=655
5	0.359375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=777 Ack=1 Win=65535 L
6	0.703125	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=777 Win=6984 Le
7	0.703125	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=2203 Ack=1 Win=65535
8	0.703125	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=3629 Ack=1 Win=65535
9	0.734375	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=2203 Win=9982 L
10	0.734375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=5055 Ack=1 Win=65535
11	0.734375	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=6481 Ack=1 Win=65535
12	1.062500	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=3629 Win=12834
13	1.062500	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [PSH, ACK] Seq=7907 Ack=1 Win=6
14	1.093750	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=5055 Win=15686
15	1.109375	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=6481 Win=18538
16	1.140625	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=7907 Win=21390
17	1.421875	128.119.245.12	58.10.77.120	TCP	http > telelpathstart [ACK] Seq=1 Ack=8969 Win=24242
18	1.421875	58.10.77.120	128.119.245.12	TCP	telelpathstart > http [ACK] Seq=8969 Ack=1 Win=65535

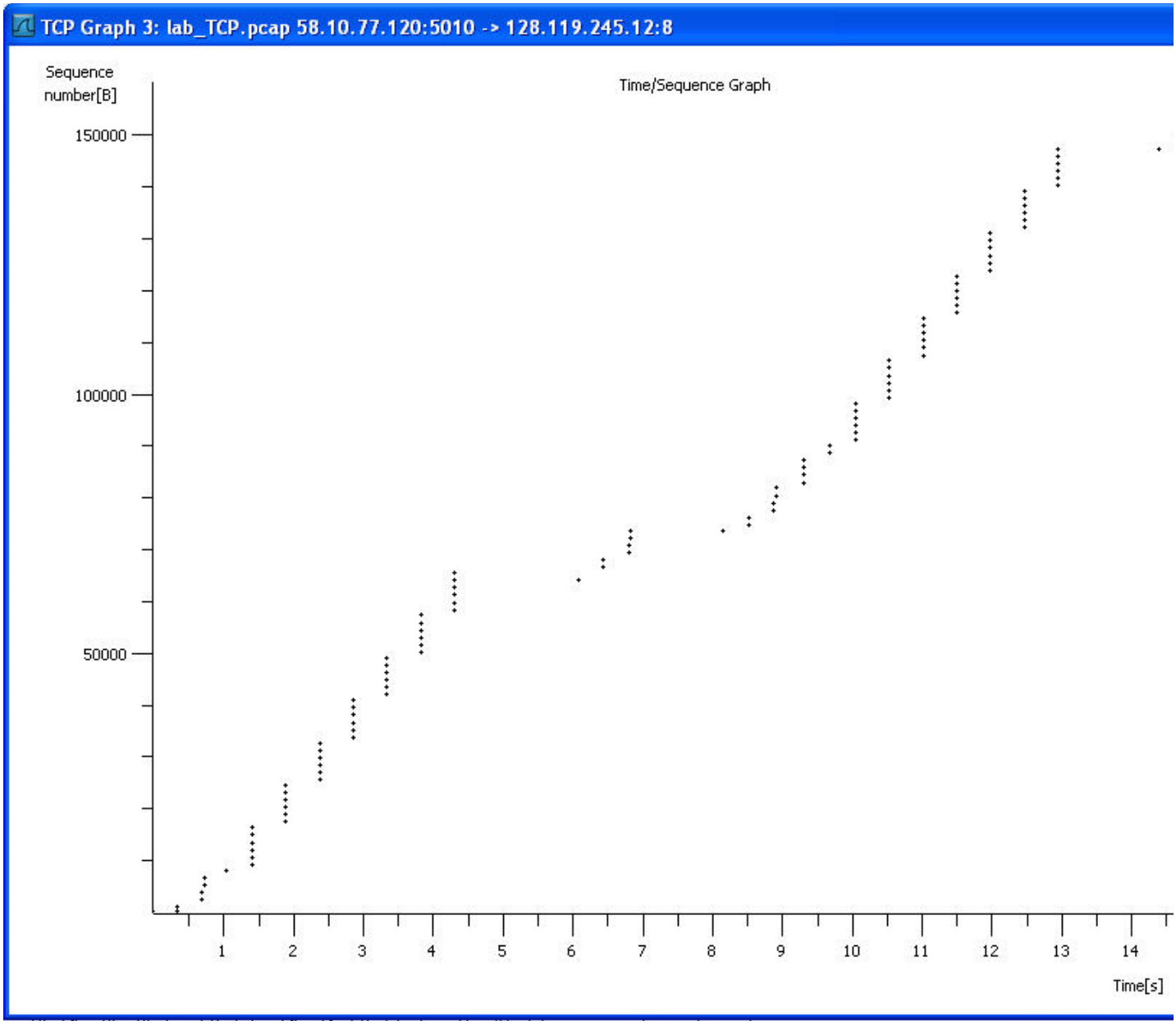
Round Trip Time Graph



8. What is the length of each of the first six TCP segments?
answer Length of first TCP segment is 776 bytes and Length of the other TCP segments(5 TCP segments) is 1426 bytes (From picture HTTP POST segment mention below).

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?
answer minimum amount of available buffer space advertised at the received for the entire trace is 5840 bytes (First Connention) . No, doesn't lack of receiver buffer space ever throttle the sender.

10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
answer No, aren't retransmitted segmensts in the trace file. I would check retransmitted segments from Time-Sequence Graph (Stevens).



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).

answer

	acknowledged sequence number	**acknowledged data**
ack1	1	776
ack2	777	1426
ack3	2203	1426
ack4	3629	1426
ack5	5505	1426
ack6	6481	1426
ack7	7907	1062
ack8	8969	1426
ack9	10395	1426
.	.	.
.	.	.
.	.	.

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

answer average throughput of a connection = (0.75*W)/RTT

W is window size (bytes)
RTT is the current round-trip time
Ex reference from 7 calculated first segment .
window size of first segment is 65535 .
RTT of first segment is 0.34375 .
average throughput of a connection = (0.75*65535)/0.34375
= 142,985.45 bytes/sec
= 142 Kbytes/sec

TCP congestion control in action

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 beginsand 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.
answer From picture sequence 10 becaue it may be traffic on network(bottleneck link). when TCP have connected between Sender and Receiver , it have a one value(it is a windows size) that used to fix value of Information can be to send to Receivers. so windows size is a value of deal between Sender and Receiver how many have in segment before sending.

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
answer when have a lot of traffic on network. TCP sender have used AIMD algorithm to reduce window size value.

---

1 Response to "Lab 4 Wireshark Lab : TCP"

Feed for this Entry Trackback Address

---

1. 1 » LAB 4 WIRESHARK TCP CNT IT51066406 Pingback on Jul 3rd, 2008 at 1:50 pm

Leave a Reply

Name

Mail (will not be published)

Website

Submit

Search

search blog archive GO

September 2010

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

« Sep

Blogroll

WordPress.com WordPress.org

Recent Entries

- LAB 10 WIRESHARK : SSL
- LAB 9 Wireshark Lab 802.11
- lab 8 wireshark Ethernet and ARP
- LAB 7 WIRESHARK ICMP
- LAB 6 WIRESHARK DHCP
- LAB 5 WIRESHARK IP
- Lab Assignment Skype
- LAB 4 WIRESHARK TCP
- LAB 3 WIRESHARK UDP
- LAB 2 WIRESHARK DNS

Months

- Septemb 2008
- August 2008
- July 2008
- June 2008
