

1

a)

IP Address: 192.168.1.102

TCP Port: 1161

The image shows a Wireshark packet capture analysis of a TCP connection. The packet list on the left shows a series of packets, with packet 4 (Frame 4) selected. The packet details pane on the right shows the structure of the selected packet, which is a TCP Reset (RST) packet. The packet is 619 bytes on wire (4952 bits) and 619 bytes captured (4952 bits). It is an Ethernet II frame with source MAC address 00:20:e0:8a:70:1a and destination MAC address 00:06:25:da:af:73. The IP header shows source IP 192.168.1.102 and destination IP 128.119.245.12. The TCP header shows source port 1161 and destination port 80. The TCP flags are RST (0x02) and the reset sequence number is 1. The packet data is 565 bytes long.

Filter: 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	0.023477	192.168.1.102	128.119.245.12	TCP	619	1161->80 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=565
5	0.041257	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460
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
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460
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
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460
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
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=9013 Ack=1 win=17520 Len=1460
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=10473 Ack=1 win=17520 Len=1460

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_6da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 605

Identification: 0x1e21 (7713)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0xa2e7 [validation disabled]

Good: False

Bad: False

Source: 192.168.1.102 (192.168.1.102)

Destination: 128.119.245.12 (128.119.245.12)

[Source GeoIP: unknown]

[Destination GeoIP: unknown]

Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 565

Source Port: 1161 (1161)

Destination Port: 80 (80)

[Stream index: 0]

[TCP Segment Len: 565]

Sequence number: 1 (relative sequence number)

[Next sequence number: 566 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 20 bytes

... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)

Window size value: 17520

[calculated window size: 17520]

[window size scaling factor: -2 (no window scaling used)]

Checksum: 0x1fbd [validation disabled]

urgent pointer: 0

[SEQ/ACK analysis]

Data (565 bytes)

Data: 504f5354202f657468657265616c2d6c6162732f6c616233...

[Length: 565]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p...f.

0010 02 5d 1e 21 40 00 80 06 a2 e7 c0 a8 01 66 80 77 .].@... ..f.w

0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18P...4.t.p

0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 Dp...PO ST /ethe

0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 real-lab s/lab3-1

0050 74 77 45 70 6c 70 7a e8 74 e4 70 a9 54 54 50 7fb .m .vrrn /

File: "C:\Users\josephkramer\Desktop\wires..." Packets: 213 · Displayed: 202 (94.8%) · Load time: 0:00.046

Profile: Default

b)
IP Address: 128.119.245.12
TCP Port: 80

The image shows a Wireshark packet capture analysis of a TCP connection. The top pane displays a list of 19 packets. The selected packet (No. 4) is a TCP segment from 192.168.1.102 to 128.119.245.12, Seq=1, Ack=1, Win=17520, Len=565. The middle pane shows the packet details, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Filter: 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
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
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
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460
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
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=3486 win=11880 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
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=9013 Ack=1 win=17520 Len=1460
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514	1161->80 [ACK] Seq=10473 Ack=1 win=17520 Len=1460

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface 0
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 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
Total Length: 605
Identification: 0x1e21 (7713)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xa2e7 [validation disabled]
[Good: False]
[Bad: False]
Source: 192.168.1.102 (192.168.1.102)
Destination: 128.119.245.12 (128.119.245.12)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 565
Source Port: 1161 (1161)
Destination Port: 80 (80)
[Stream index: 0]
[TCP Segment Len: 565]
Sequence number: 1 (relative sequence number)
[Next sequence number: 566 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
Window size value: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1fbd [validation disabled]
Urgent pointer: 0
[SEQ/ACK analysis]
Data (565 bytes)
Data: 504f5354202f657468657265616c2d6c6162732f6c616233...
[Length: 565]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 .%.s. .P...E.
0010 02 5d 1e 21 40 00 80 06 a2 e7 c0 a8 01 66 80 77 .j.!@... .f.w
0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18P... .t.P.
0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 Dp...PO ST/ethe
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 real-lab s/lab3-1
0050 24 72 65 70 6c 70 70 68 74 64 20 19 54 54 50 2f only b r mto/

File: C:\Users\josephkramen\Desktop\wires... Packets: 213 - Displayed: 202 (94.8%) - Load time: 0:00.046
Profile: Default

c)
IP Address: 10.211.55.3
TCP Port: 2374

Wireshark packet capture showing a TCP connection from 10.211.55.3 to 128.119.245.12 on port 2374. The capture includes a SYN packet (No. 6) and subsequent ACK packets (Nos. 7-24). The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.2762270	10.211.55.3	128.119.245.12	TCP	66	2374→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	0.3357910	10.211.55.3	128.119.245.12	TCP	66	2375→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	0.3681450	128.119.245.12	10.211.55.3	TCP	62	80→2374 [SYN, ACK] Seq=0 Ack=1 win=32768 Len=0 MSS=1460 WS=2
9	0.3681990	10.211.55.3	128.119.245.12	TCP	54	2374→80 [ACK] Seq=1 Ack=1 win=65536 Len=0
10	0.3688460	10.211.55.3	128.119.245.12	TCP	668	2374→80 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=614
11	0.3689570	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=615 win=32768 Len=0
12	0.3691250	10.211.55.3	128.119.245.12	TCP	2974	2374→80 [ACK] Seq=615 Ack=1 win=65536 Len=2920
13	0.3692570	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=2075 win=32768 Len=0
14	0.3692570	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=3535 win=32768 Len=0
15	0.3692670	10.211.55.3	128.119.245.12	TCP	5894	2374→80 [ACK] Seq=3535 Ack=1 win=65536 Len=5840
16	0.3693510	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=4995 win=32768 Len=0
17	0.3693510	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=6455 win=32768 Len=0
18	0.3693520	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=7915 win=32768 Len=0
19	0.3693520	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=9375 win=32768 Len=0
20	0.3693610	10.211.55.3	128.119.245.12	TCP	11734	2374→80 [PSH, ACK] Seq=9375 Ack=1 win=65536 Len=11680
21	0.3694380	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=10835 win=32768 Len=0
22	0.3694380	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=12295 win=32768 Len=0
23	0.3694380	128.119.245.12	10.211.55.3	TCP	60	80→2374 [ACK] Seq=1 Ack=13755 win=32768 Len=0
24	0.3694460	10.211.55.3	128.119.245.12	TCP	8814	2374→80 [ACK] Seq=21055 Ack=1 win=65536 Len=8760

Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Parallel_ze:d2:0f (00:1c:42:2e:d2:0f), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
Internet Protocol Version 4, Src: 10.211.55.3 (10.211.55.3), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 2374 (2374), Dst Port: 80 (80), Seq: 0, Len: 0

0000 00 1c 42 00 00 18 00 1c 42 2e d2 0f 08 00 45 00 ..B.... B....E.
0010 00 34 4a 59 40 00 80 06 00 00 0a d3 37 03 80 77 .4jY@...7..w
0020 f5 0c 09 46 00 50 d7 a5 9c 07 00 00 00 80 02 ...F.P.
0030 20 00 b7 80 00 02 04 05 b4 01 03 03 08 01 01 ..
0040 04 02 ..

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?

The image displays the Wireshark 1.12.6 interface with a packet capture of a TCP connection. The packet list shows a SYN packet (Seq=0, Win=16384) and an ACK packet (Seq=1, Win=17520). The packet details pane shows the structure of the TCP segment, including the header and options. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Packet List:

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
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
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
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161-80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
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
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161-80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
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
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80-1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80-1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80-1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80-1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161-80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514	1161-80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460

Packet Details:

- Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: Actionet_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_Gda:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
- Total Length: 48
- Identification: 0x1ed (7709)
- Flags: 0x02 (Don't Fragment)
 - 0..... = Reserved bit: Not set
 - 1..... = Don't fragment: Set
 -0.. = More fragments: Not set
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0xa518 [validation disabled]
- Source: 192.168.1.102 (192.168.1.102)
- Destination: 128.119.245.12 (128.119.245.12)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 0, Len: 0
- Source Port: 1161 (1161)
- Destination Port: 80 (80)
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 0
- Header Length: 28 bytes
- Window size value: 16384
 - 0000 0000 0000 0000 = Flags: 0x002 (SYN)
 - [calculated window size: 16384]
- Checksum: 0xf6e9 [validation disabled]
- Urgent pointer: 0
- Options: (8 bytes), Maximum segment size, No-operation (NOP), No-operation (NOP), SACK permitted

Packet Bytes:

```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  ..%.S.  ..p..E.
0010 00 30 1e 1d 40 00 80 06 a5 18 c0 a8 01 66 80 77  .0..@...f.w
0020 f5 0c 04 89 00 30 00 06 01 74 00 00 00 70 02  ....P....p.
0030 40 00 f6 e9 00 00 02 04 05 d4 01 01 04 02      @.....
  
```

Sequence number (tcp.seq), 4 bytes **Packets: 213 - Displayed: 213 (100.0%) - Load time: 0:00:015** **Profile: Default**

3.

What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?

The sequence number of the SYNACK segment is: HEX->0H34A27419 or 883061785.

What is the value of the Acknowledgement field in the SYNACK segment?

Acknowledgment number of the SYNACK segment is: HEX->DD601F5 or 232129013

How did gaia.cs.umass.edu determine that value?

The TCP receiver incremented increments the previous Sequence Number by 1, then it copies it into the acknowledgement field.

What is it in the segment that identifies the segment as a SYNACK segment?

The SYN and ACK flag bits are both set to 1, this indicates that it's a SYNACK packet.

The image shows a Wireshark packet capture of a TCP SYNACK segment. The packet list shows a SYNACK segment from 192.168.1.102 to 128.119.245.12. The packet details show the following information:

- Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
- Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 48
- Identification: 0x0000 (0)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 55
- Protocol: TCP (6)
- Header checksum: 0x0c36 [validation disabled]
- [Good: False]
- [Bad: False]
- Source: 128.119.245.12 (128.119.245.12)
- Destination: 192.168.1.102 (192.168.1.102)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1161 (1161), Seq: 0, Ack: 1, Len: 0
- Source Port: 80 (80)
- Destination Port: 1161 (1161)
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Header Length: 28 bytes
- ... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
- Window size value: 5840
- [calculated window size: 5840]
- Checksum: 0x774d [validation disabled]
- Urgent pointer: 0
- Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
- [SEQ/ACK analysis]

The packet bytes pane shows the raw data of the packet, including the flags and sequence/acknowledgment numbers.

4.

What is the sequence number of the TCP segment containing the HTTP POST command?

Sequence number is: HEX 0H0DD601F5 or 232129013.

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of captured packets. Packet 4 is selected, showing details of an Ethernet II frame, an Internet Protocol Version 4 packet, and a Transmission Control Protocol (TCP) segment. The TCP segment details show the source port as 1161 and the destination port as 80. The sequence number is 1 (relative sequence number), and the acknowledgment number is 1 (relative ack number). The window size is 17520. The data field shows the start of an HTTP POST request.

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

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_gd:a:f73 (00:06:25:da:f7:3)

Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)

Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
Total Length: 605
Identification: 0xe121 (7713)
Flags: 0x02 (Don't fragment)
0... .. = Reserved bit: Not set
... .. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xa2e7 [validation disabled]
Source: 192.168.1.102 (192.168.1.102)
Destination: 128.119.245.12 (128.119.245.12)
[Source geoIP: Unknown]
[Destination geoIP: Unknown]

Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 565
Source Port: 1161 (1161)
Destination Port: 80 (80)
[Stream index: 0]
[TCP segment Len: 565]

Sequence number: 1 (relative sequence number)
[Next sequence number: 566 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
window size value: 17520
[calculated window size: 17520]
[window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1fbd [validation disabled]
urgent pointer: 0
[SEQ/ACK analysis]
Data (565 bytes)

0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18P.....4.T.P.
0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 dp....PO ST / ethe
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 real-lab s/lab3-1
0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f -reply.h tm HTTP/
0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 1..Hos t: gaia.
0070 62 72 3c 75 6d 61 72 72 2a 65 64 75 0d 0a 55 72 cc.unacc edly uc

Sequence number (tcp.seq), 4 bytes | Packets: 213 - Displayed: 213 (100.0%) - Load time: 0:00:015 | Profile: Default

5.

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?

	Sequence #	Sent Time	ACK Received Time	RTT in Seconds
Segment 1	1	0.026477	0.053937	0.027460
Segment 2	566	0.041737	0.077294	0.035557
Segment 3	2026	0.054026	0.124085	0.070059
Segment 4	3486	0.054690	0.169118	0.114428
Segment 5	4946	0.077405	0.217299	0.139894
Segment 6	6406	0.078157	0.267802	0.189645

What is the EstimatedRTT value (see Section 3.5.3, page 239 in text) after the receipt of each ACK?

EstimatedRTT = $(1 - 1/8) * \text{EstimatedRTT} + 1/8 * \text{sampleRTT}$

EstimatedRTT = 0.02746 second

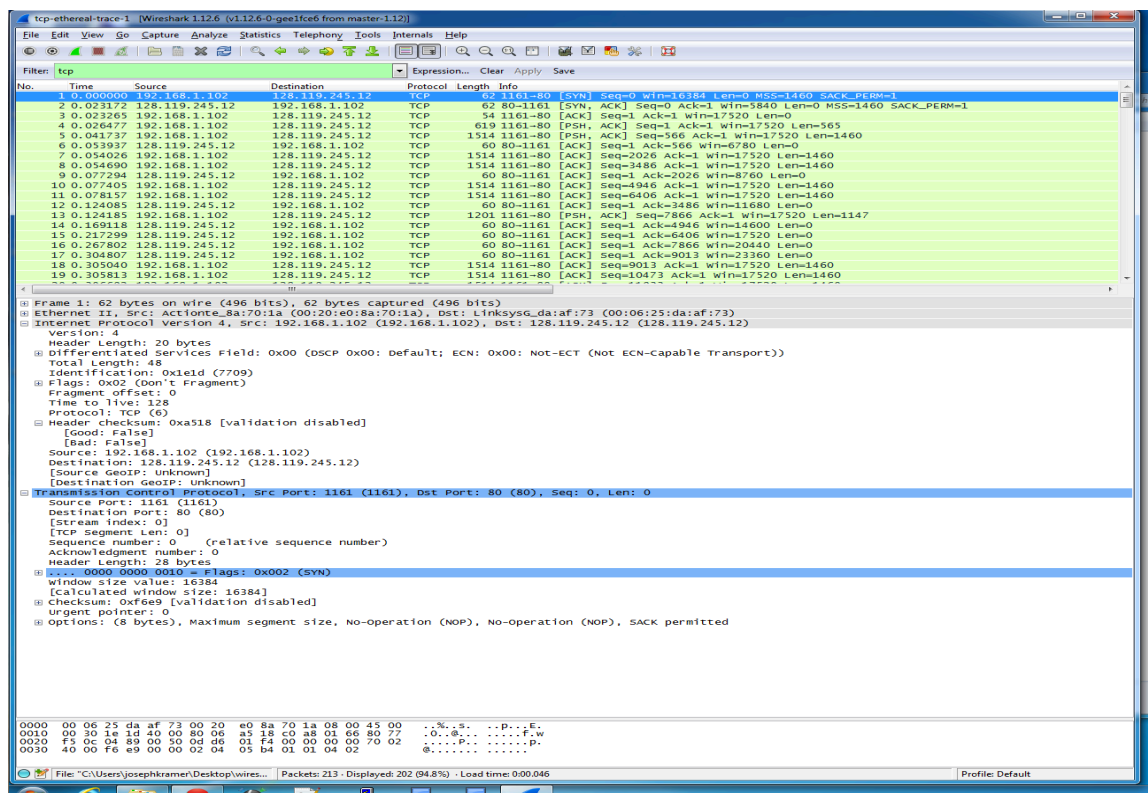
EstimatedRTT = $(1 - 1/8) * 0.02746 + 1/8 * 0.035557 = 0.0285$

EstimatedRTT = $(1 - 1/8) * 0.0285 + 1/8 * 0.070059 = 0.0337$

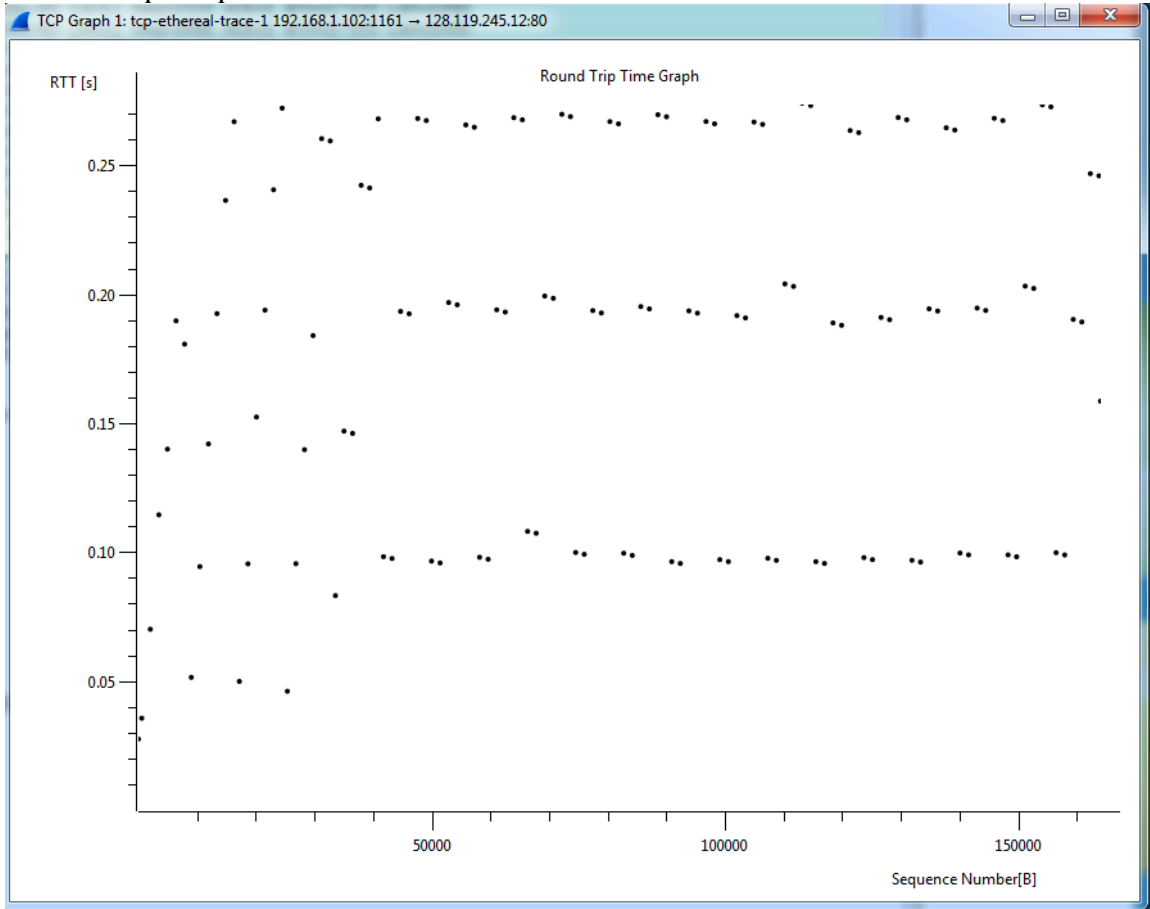
EstimatedRTT = $(1 - 1/8) * 0.0337 + 1/8 * 0.114428 = 0.0438$

EstimatedRTT = $(1 - 1/8) * 0.0438 + 1/8 * 0.139894 = 0.0558$

EstimatedRTT = $(1 - 1/8) * 0.0558 + 1/8 * 0.189645 = 0.0725$



Round Trip Graph



6.

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

565, 1460, 1460, 1460, 1460, 1460

The image shows a Wireshark packet capture of a TCP connection. The packet list at the top shows the first six TCP segments with their lengths. The packet details pane for packet 4 shows the TCP header and data fields, confirming the segment length of 565 bytes.

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
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
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80->1161 [ACK] Seq=1 Ack=566 win=6780 Len=0

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface 0
Ethernet II, Src: Actiontec_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_Gd_a:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
Total Length: 605
Identification: 0x1e21 (7713)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xa2e7 [validation disabled]
[Good: False]
[Bad: False]
Source: 192.168.1.102 (192.168.1.102)
Destination: 128.119.245.12 (128.119.245.12)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 565
Source Port: 1161 (1161)
Destination Port: 80 (80)
[Stream index: 0]
[TCP Segment Len: 565]
Sequence number: 1 (relative sequence number)
[Next sequence number: 566 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
Window size value: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1fbd [validation disabled]
Urgent pointer: 0
[SEQ/ACK analysis]
Data (565 bytes)
Data: 504f5354202f657468657265616c62d6c6162732f6c616233...
[Length: 565]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 .%.s. .P...E.
0010 02 5d 1e 21 40 00 80 06 a2 e7 c0 a8 01 66 80 77 .j.!@...f.w
0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18P.. ..t.P.
0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 Dp...P ST /ethe
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 24 31 real-lab s/lab3-1
0050 24 72 65 70 6c 70 70 68 74 64 20 19 54 54 50 2f conly b t= HTTP/

7.

What is the minimum amount of available buffer space advertised at the received for the entire trace?

Buffer: Win=5840

Does the lack of receiver buffer space ever throttle the sender?

The sender is never throttled back due to lack of receiver buffer space, because the size reaches 62780; which is 43 MSS segments. It does not appear that the lack of receiver buffer space is an issue. The sender may be more constrained by congestion then flow control.

The image shows a Wireshark packet capture analysis of a TCP connection. The packet list at the top shows 19 packets. Packet 4 is selected, showing details for the TCP segment. The details pane shows the following information:

- Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 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 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 605
- Identification: 0x1e21 (7713)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0xa2e7 [validation disabled]
- [Good: False]
- [Bad: False]
- Source: 192.168.1.102 (192.168.1.102)
- Destination: 128.119.245.12 (128.119.245.12)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 565
- Source Port: 1161 (1161)
- Destination Port: 80 (80)
- [Stream index: 0]
- [TCP Segment Len: 565]
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 566 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Header Length: 20 bytes
- 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
- Window size value: 17520
- [Calculated window size: 17520]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0x1fbd [validation disabled]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- Data (565 bytes)
- Data: 504f5354202f657468657265616c2d6c6162732f6c616233...
- [Length: 565]

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII part shows the string "GET / HTTP/1.1" followed by some control characters and a carriage return.

8.

Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

There are no retransmitted segments, because all sequence numbers from the source to the destination are increasing. There would need to be a repeat entry for a retransmitted segment with the same sequence number.

9.

How much data does the receiver typically acknowledge in an ACK?

1460 is the typical acknowledged data.

Can you identify cases where the receiver is ACKing every other received segment.

Yes, cases can be identified because there are times where ACK is more than usual. For example, there are several instances past segment number 60, where the receiver will send an ACK for every other received segment. At this point the receiver is sending a combined ACK for two segments. The textbook indicates that TCP's will use "delayed ACK's," this is when the receiver will wait 500ms for the arrival of another segment and then send them both back. Always look for if the data is double, because then it is ACKing every other.

10.

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

First we need to take the total data sent; which is number 2 through number 202. Now at 202 the total data sent is 164091. Then we need to subtract 1. Therefore we are left with 164090.

Now we do the same with time. We start at 4 and go to 202. The time at 2 is 0.026477 and at 202 it is 5.455830. Therefore we have $5.455830 - 0.026477 = 5.429353$

Now to calculate the throughput. $164090 / 5.429353 = 30222.75$ bytes

11.

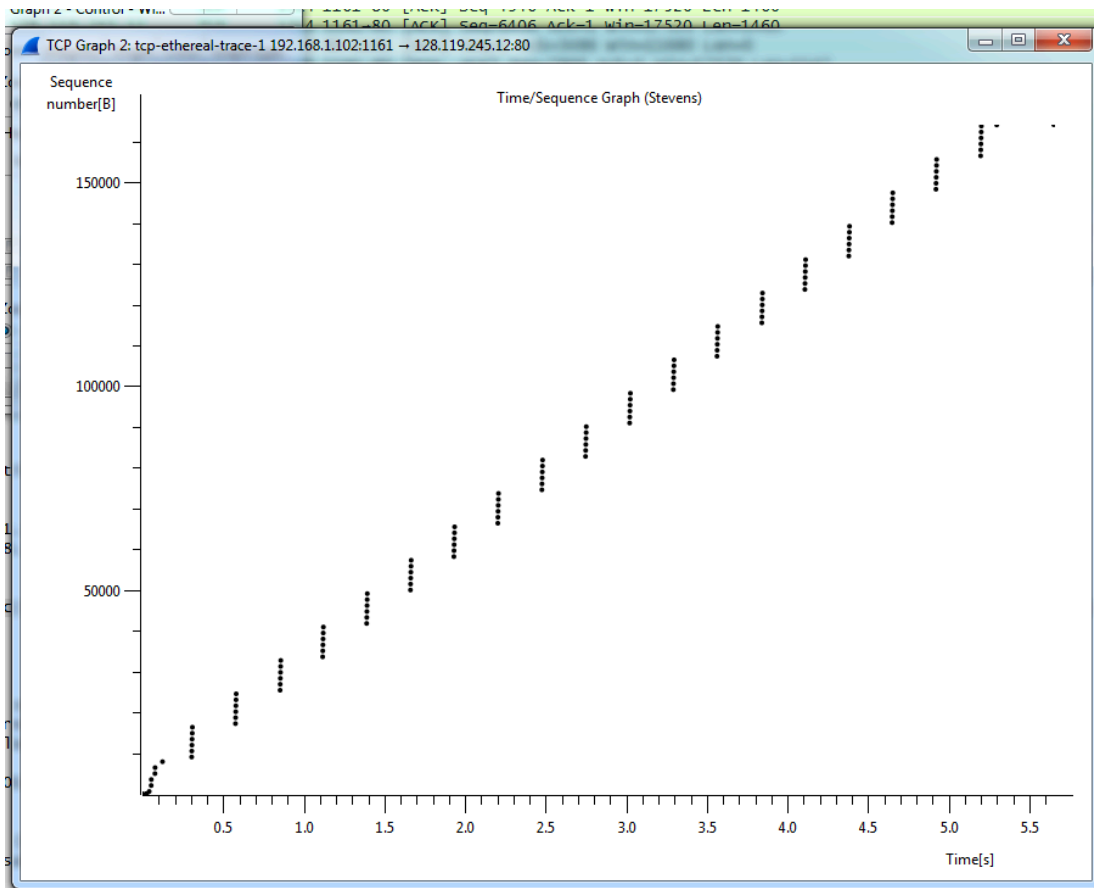
Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.

It appears that TCP slowstart begins when the HTTP POST is sent out. The congestion window size is based on the TCP congestion avoidance and slow start phase. It does not appear that the congestion window size can be retrieved from the Time Sequence Graph. After review the graph it appears that the slow start phase last for 0.1 seconds and after that it is always operating in congestion avoidance. I cannot see that the buffer is an issue, because the WIN is 5840 and that is not reached.

It does not appear the TCP is sending data at a state that would engage congestion avoidance. The largest data block the application sends out is 8192 bytes, before it receives and ACK for the bytes, it will not send anymore. Therefore the application will temporally stops transmission and this happens before the end of a slow start phase. It does not seem possible to precisely determine the slow start phase or the congestion avoidance phase. According to the graph it does appear to transmit packets in batches of 5; however this is not a flow control issue, because the receiver window is larger than 5 packets

How does this data differ from the book?

In this lab the file was small and it never got out of the slow start phase. The text would indicate that senders send out data as fast as possible all the time and that does not appear to be the case. I also think the TCP behavior depends on that type of application it is being used for. Since this was a small program, handling congestion was not a concern; however sending an HD movie would face congestion issues.



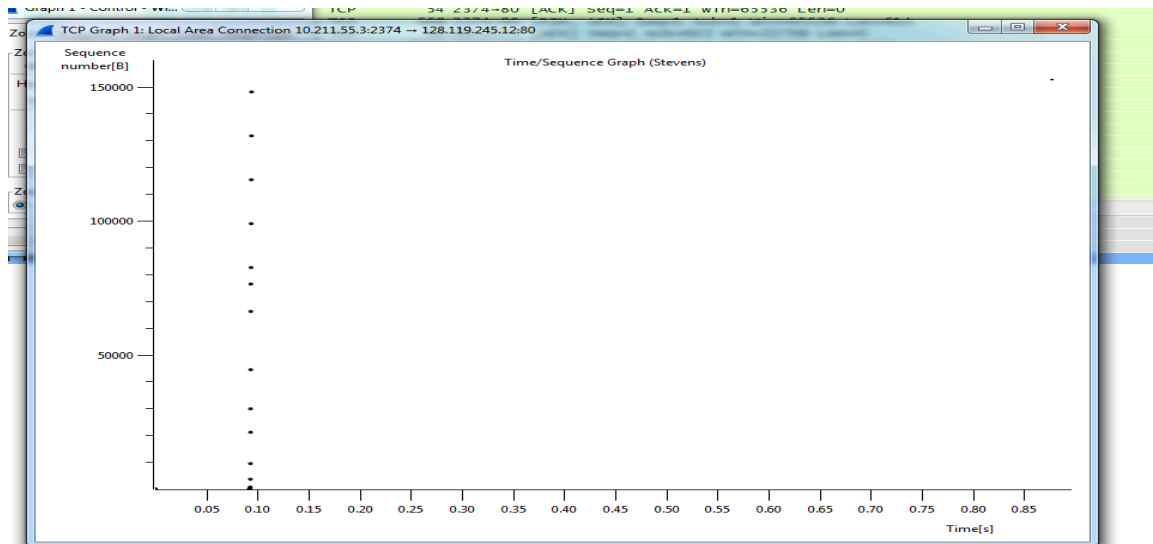
16r7d6c6162727f6c616232

12.

Answer each of two questions in Question 11 for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

The Time Sequence Graph is much different. (I followed the direction exactly, however I'm running this on Parallels and maybe that makes a difference.) However it does not seem like the congestion window size can be determined by this graph either. Here it does not appear that the buffer become an issue, because the WIN is 65536 and that is not reached. Also congestion avoidance did not become an issue, because the data plots are in a verticle line. Same as question 11, I cannot get the exact slow start or congestion avoidance phase.

It differs from the book the same as question 11. The textbook seems to deal with scenarios where the sender sends out data, as fast as possible, and in this lab the data does not appear to operate like that.



Local Area Connection [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6	0.276227000	10.211.55.3	128.119.245.12	TCP	66	2374->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	0.335791000	10.211.55.3	128.119.245.12	TCP	66	2375->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	0.368145000	128.119.245.12	10.211.55.3	TCP	62	80->2374 [SYN, ACK] Seq=0 Ack=1 win=32768 Len=0 MSS=1460 WS=2
9	0.368199000	10.211.55.3	128.119.245.12	TCP	54	2374->80 [ACK] Seq=1 Ack=1 win=65536 Len=0
10	0.368846000	10.211.55.3	128.119.245.12	TCP	66	2374->80 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=614
11	0.368957000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=615 win=32768 Len=0
12	0.369125000	10.211.55.3	128.119.245.12	TCP	2974	2374->80 [ACK] Seq=615 Ack=1 win=65536 Len=2920
13	0.369257000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=2075 win=32768 Len=0
14	0.369257000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=3535 win=32768 Len=0
15	0.369267000	10.211.55.3	128.119.245.12	TCP	5894	2374->80 [ACK] Seq=3535 Ack=1 win=65536 Len=5840
16	0.369351000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=4995 win=32768 Len=0
17	0.369351000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=6455 win=32768 Len=0
18	0.369352000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=7915 win=32768 Len=0
19	0.369352000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=9375 win=32768 Len=0
20	0.369361000	10.211.55.3	128.119.245.12	TCP	11734	2374->80 [PSH, ACK] Seq=9375 Ack=1 win=65536 Len=11680
21	0.369438000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=10835 win=32768 Len=0
22	0.369438000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=12295 win=32768 Len=0
23	0.369438000	128.119.245.12	10.211.55.3	TCP	60	80->2374 [ACK] Seq=1 Ack=13755 win=32768 Len=0
24	0.369446000	10.211.55.3	128.119.245.12	TCP	8814	2374->80 [ACK] Seq=21055 Ack=1 win=65536 Len=8760

Frame 12: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface 0

Ethernet II, Src: Parallel_2e:d2:0f (00:1c:42:2e:d2:0f), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)

Internet Protocol Version 4, Src: 10.211.55.3 (10.211.55.3), Dst: 128.119.245.12 (128.119.245.12)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))

Total Length: 2960

Identification: 0x4a5d (19037)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

Source: 10.211.55.3 (10.211.55.3)

Destination: 128.119.245.12 (128.119.245.12)

[Source GeoIP: unknown]

[Destination GeoIP: unknown]

Transmission Control Protocol, Src Port: 2374 (2374), Dst Port: 80 (80), Seq: 615, Ack: 1, Len: 2920

Source Port: 2374 (2374)

Destination Port: 80 (80)

[Stream index: 0]

[TCP segment Len: 2920]

Sequence number: 615 (relative sequence number)

[Next sequence number: 3535 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 20 bytes

... 0000 0001 0000 = Flags: 0x010 (ACK)

Window size value: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

Checksum: 0xb760 [validation disabled]

Urgent pointer: 0

[SEQ/ACK analysis]

Data (2920 bytes)

0000 00 1c 42 00 00 18 00 1c 42 2e d2 0f 08 00 45 00 ..B.... B....E.

0010 0b 90 4a 5d 40 00 80 06 00 00 0a d3 37 03 80 77 ...J]@....7..w

0020 f5 0c 09 46 00 50 d7 a5 9e 6e 78 d1 c3 d3 50 10 ...F.P...nx...P.

0030 01 00 b7 60 00 00 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ...---webK

0040 69 74 46 6f 72 6d 42 6f 75 6e 64 61 72 79 37 55 ltrFormBo undary7U

0050 25 2d 67 44 56 42 6d 4d 66 70 59 6f 62 46 0d 02 54b070M fux03F

File: "C:\Users\JOSEPH-1\AppData\Local\T... Packets: 150 - Displayed: 138 (92.0%) - Dropped: 0 (0.0%) Profile: Default