

COMP2322 Computer Networking

Lab 6 Report: TCP

ZHOU Siyu

1.

5747	75.589276	172.16.166.214	128.119.245.12	HTTP	533	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
5782	75.891162	128.119.245.12	172.16.166.214	HTTP	831	HTTP/1.1 200 OK (text/html)

> Frame 5747: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{93EBE42A-}	0000	04 27 58 0b 71 e8 8e fc 0b c4
> Ethernet II, Src: 8e:fc:0b:c4:e9:70 (8e:fc:0b:c4:e9:70), Dst: HuaweiTe_0b:71:e8 (04:27:58:0b:71:e8)	0010	02 07 4a f9 40 00 00 06 00 00
> Internet Protocol Version 4, Src: 172.16.166.214, Dst: 128.119.245.12	0020	f5 0c ef ea 00 50 02 62 f2 10
> Transmission Control Protocol, Src Port: 61418, Dst Port: 80, Seq: 152588, Ack: 1, Len: 479	0030	01 00 ca 64 00 00 61 72 73 2c
Source Port: 61418	0040	69 6d 70 6c 65 20 61 6e 64 0d
Destination Port: 80	0050	67 20 68 65 61 72 74 20 6f 66
[Stream index: 83]	0060	68 69 6c 64 68 6f 6f 64 3a 20
[Conversation completeness: Complete, WITH_DATA (31)]	0070	6f 77 20 73 68 65 20 77 6f 75
TCP Segment Len: 479]	0080	68 65 72 20 61 62 6f 75 74 0d
	0090	74 68 6c 73 70 6f 6a 74 74 0d

According to above figure, client computer's IP address is 172.16.166.214, TCP port number is 61418.

5.

4	0.004737	120.232.23.208	172.16.166.214	TCP	66	443 → 61708 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1424 SACK_PERM WS=1
5	0.004776	172.16.166.214	120.232.23.208	TCP	54	61708 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=0
6	0.004987	172.16.166.214	120.232.23.208	SSL	195	Continuation Data
11	0.105166	120.232.23.208	172.16.166.214	TCP	56	80 → 61707 [ACK] Seq=1 Ack=142 Win=31979 Len=0
12	0.111578	157.148.41.188	172.16.166.214	TCP	74	36688 → 61705 [PSH, ACK] Seq=1 Ack=1 Win=195 Len=20
13	0.112193	172.16.166.214	157.148.41.188	TCP	339	61705 → 36688 [PSH, ACK] Seq=1 Ack=21 Win=32448 Len=285
14	0.116877	120.232.23.208	172.16.166.214	TCP	56	443 → 61708 [ACK] Seq=1 Ack=142 Win=31979 Len=0

> Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{93EBE42A-F837-4581-A7C7-17CF5550BAE1}, id 0	0000	8e fc 0b c4 e9 70 04 27 58 0b
> Ethernet II, Src: HuaweiTe_0b:71:e8 (04:27:58:0b:71:e8), Dst: 8e:fc:0b:c4:e9:70 (8e:fc:0b:c4:e9:70)	0010	00 34 00 00 40 00 2e 06 00 00
> Internet Protocol Version 4, Src: 120.232.23.208, Dst: 172.16.166.214	0020	a6 d6 01 bb f1 0c 23 ab 7d 7b
> Transmission Control Protocol, Src Port: 443, Dst Port: 61708, Seq: 0, Ack: 1, Len: 0	0030	7d 7b 3c 77 00 00 02 04 03 00
Source Port: 443	0040	
Destination Port: 61708		
[Stream index: 1]		
[Conversation completeness: Incomplete (30)]		
TCP Segment Len: 0]		
Sequence Number: 0 (relative sequence number)		
Sequence Number (raw): 598426783		
[Next Sequence Number: 1 (relative sequence number)]		
Acknowledgment Number: 1 (relative ack number)		
Acknowledgment number (raw): 1453334507		
1000 = Header Length: 32 bytes (8)		
> Flags: 0x012 (SYN, ACK)		
0000 = 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.]		

Sequence number of SYNACK segment in reply to SYN is 0. Value of acknowledgement file in SYNACK segment is 1. Server add 1 to initial sequence number value of SYN segment 0. If acknowledgement number is 1, and SYN number is 1, then it can be identified as a SYNACK segment.

9.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	120.232.23.208	172.16.166.214	TCP	66	80 → 61707 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1424 SACK_PERM WS=1
2	0.000162	172.16.166.214	120.232.23.208	TCP	54	61707 → 80 [ACK] Seq=1 Ack=1 Win=517 Len=0
3	0.000344	172.16.166.214	120.232.23.208	TCP	195	61707 → 80 [PSH, ACK] Seq=1 Ack=1 Win=517 Len=141
4	0.004737	120.232.23.208	172.16.166.214	TCP	66	80 → 61708 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1424 SACK_PERM WS=1
5	0.004776	172.16.166.214	120.232.23.208	TCP	54	61708 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=0
6	0.004987	172.16.166.214	120.232.23.208	SSL	195	Continuation Data
11	0.105166	120.232.23.208	172.16.166.214	TCP	56	80 → 61707 [ACK] Seq=1 Ack=142 Win=31979 Len=0

Type: IP4 (0x0800)		
> Internet Protocol Version 4, Src: 120.232.23.208, Dst: 172.16.166.214		
0100 = Version: 4		
....0101 = Header Length: 20 bytes (5)		
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 52		
Identification: 0x0000 (0)		
> 010 = Flags: 0x2, Don't fragment		
...0 0000 0000 0000 = Fragment Offset: 0		
Time to Live: 46		
Protocol: TCP (6)		
Header Checksum: 0x6925 [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 120.232.23.208		
Destination Address: 172.16.166.214		
> Transmission Control Protocol, Src Port: 443, Dst Port: 61708, Seq: 0, Ack: 1, Len: 0		
Source Port: 443		
Destination Port: 61708		
[Stream index: 1]		
[Conversation completeness: Incomplete (30)]		
TCP Segment Len: 0]		
Sequence Number: 0 (relative sequence number)		
Sequence Number (raw): 598426783		
[Next Sequence Number: 1 (relative sequence number)]		
Acknowledgment Number: 1 (relative ack number)		
Acknowledgment number (raw): 1453334507		
1000 = Header Length: 32 bytes (8)		
> Flags: 0x012 (SYN, ACK)		
Window: 32120		
[Calculated window size: 32120]		

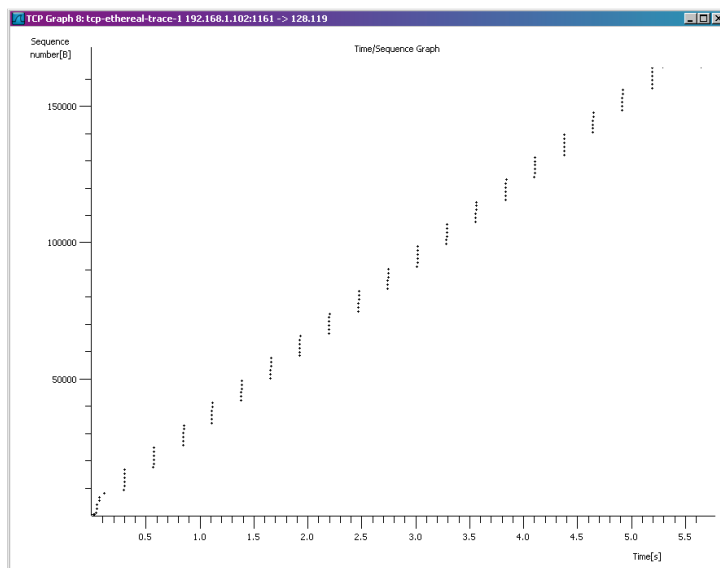
Minimum amount of available buffer space is 32120. The receiver buffer size is 62780 byte, so sender will not throttled because of lack of space.

11.

The image shows a Wireshark packet capture of a TCP connection. The top pane displays a list of packets, with several TCP segments highlighted. The bottom pane shows the details of a selected packet (Sequence Number: 3668, Acknowledgment Number: 1460). The details pane includes fields for Destination, Source, Internet Protocol Version 4, and Transmission Control Protocol. The TCP segment length is 1460 bytes, and the acknowledgment number is 1460. The status bar at the bottom indicates 906 packets displayed, with 335 (37.0%) displayed and 0 (0.0%) dropped.

Typically, receiver acknowledge 1460 bytes in an ACK. With the number of ACK, we can find receiver is ACKing every other received segment.

13.



TCP's slowstart phase begins at 0s, and ends at 0.1s. Congestion avoidance takes over after 0.1s.

We studied that the TCP should behave as a linear increasing line in the graph. Maybe HTTP server limit the rate of sending segments.