HY-335a Computer Networks
Χρηστος Παπασταμος csd4569
Assignment 3

Part 1

Question 1

1) **Checksum** is a mechanism TCP uses to confirm that the received packet is correct and that no distortions happened to it during its transmission. Therefore, it is not reliable for the transformation of the packet.
2) This statement is **false**. The value of the **ssthresh** (after a timeout) is set to **half of cwnd** (right before the timeout)
3) This statement is **true**. During the slow start phase cwnd is increasing exponentially, until it reaches the value of ssthresh
4) A **triple duplicate ACK** can possibly mean a high congestion in the network, as it reflects on a packet loss
5) This statement is **true.**
6) TCP does not support broadcast, therefore it is only possible to send packets to a single host per socket.
7) TCP's flow control is responsible to inform the sender about the free space in the receiver's window
8) If the receiver is reading data from its buffer faster than the sender is sending to it, then the flow control has no use in that connection
9) TCP and UDP can be used together in streaming services, such as YouTube, Spotify and Netflix
10) When using plain UDP, you cannot have guarantees for the data delivery since UDP has no congestion avoidance or flow control mechanisms, unlike TCP

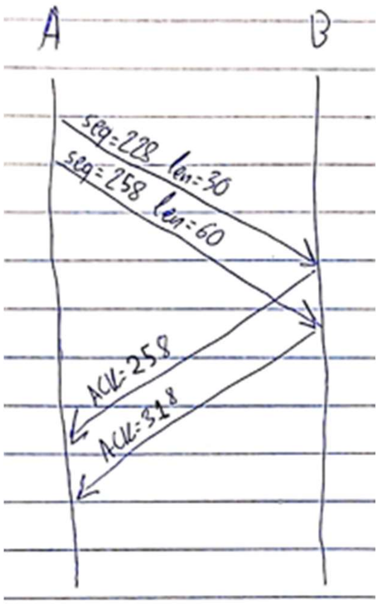
Question 2

1) Flow control is responsible for informing the sender of each packet about the remaining size on the receiver's buffer, unlike congestion control, which is responsible for avoiding overloading the network with packets. Also flow control is achieved through a communication between the two participants through the ACK packets (which contain the remaining buffer size), unlike congestion control which is computed locally by each node
2) Unlike TCP, UDP is a much faster protocol which is useful in applications like games and streaming services where lost packets don't matter that much.
3) Duplicate ACKs mean that a previous section is lost and the receiver needs it to continue reading the next packets. Timeout occurs when the connection faulty and no acknowledgment is received for a packet. Due to the above, fast retransition is not considered complimentary to the timeout timer.

Part 2

Question 1

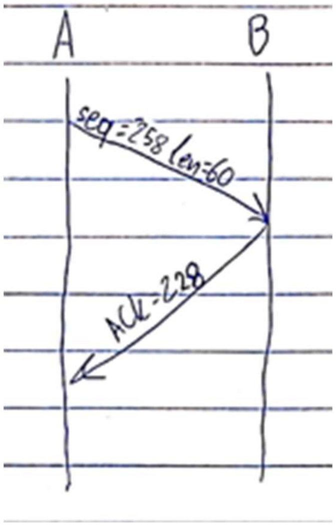
1)



The sequence number of the second packet is 258 since the seq. number of the previous packet was 228 and had length 30bytes. The sequence number is calculated by adding the previous length to the previous sequence number

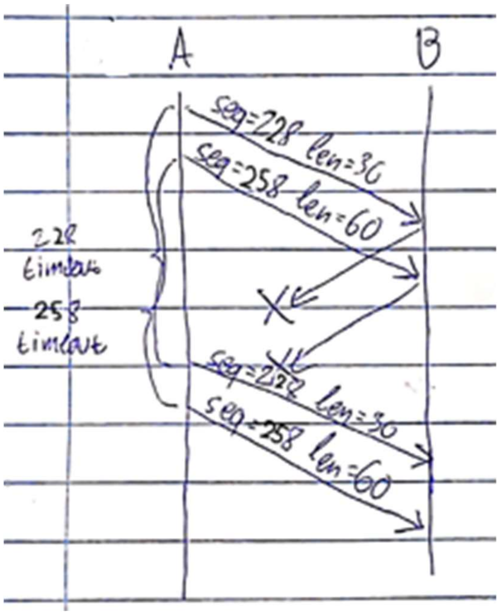
2) The source port of the ACKs is 80 and the destination port is 306

3)



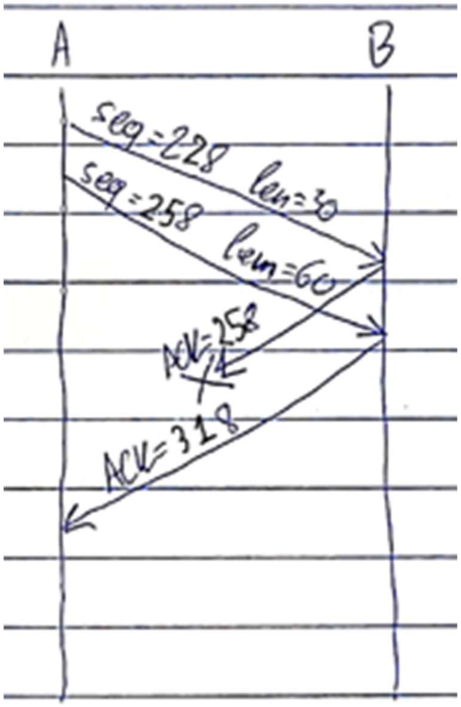
Host b sends a ACK for the last (valid) packet he received. Therefore after receiving 258 without receiving 228, it answers that it needs 228 first by ACKing it

4)



When the timer of each packet runs out, the fast recovery mechanism will try and resend the packets that were not acknowledged by the receiver. Host A cannot be certain if the packets reached the destination!

5)



In this case, there is no need to retransmit the packets, because by acknowledging the second packet (258), the sender can be certain that the first one (228) was received too.

Question 2

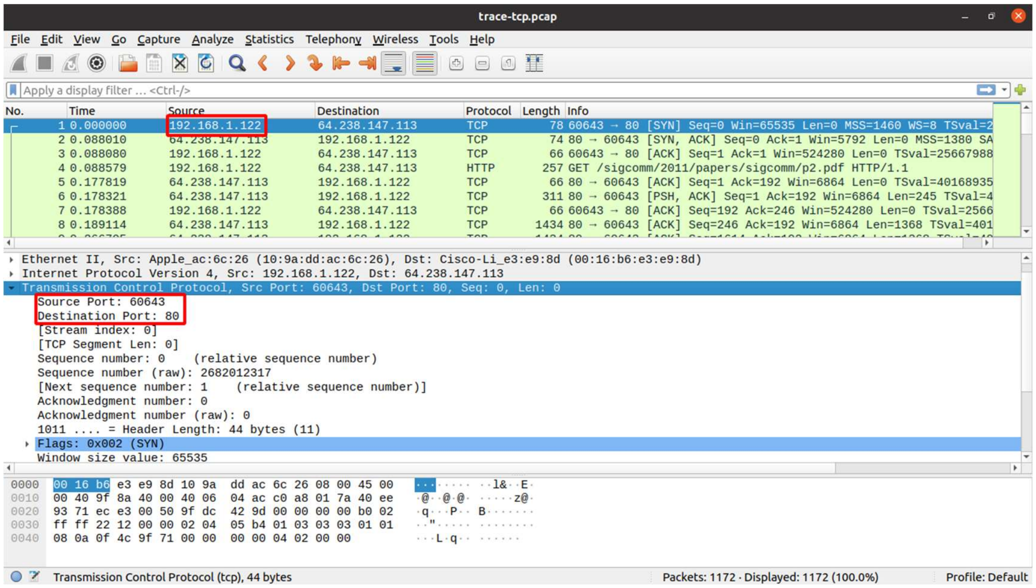
1) **TCP slow start** operates from 0 to 6 and from 23 to 26
2) **TCP congestion avoidance** operates from 6 to 16 and from 17 to 22. This can be distinguished by the linear graph seen on these segments. (On slow start the graph is exponential)
3) Considering that the drop was to about the half of the cwnd (which is also the ssthresh), there was a triple duplicate ACK detected. This probably means the network is overloaded and the packet was lost somewhere

4) The sudden drop got cwnd to 1 MSS, which means there was a packet timeout. A timeout indicates a faulty connection where neither the packet nor its acknowledgment made it across
5) The 89th segment was sent at the 6th transmission. This can be seen when you calculate which was the first packet sent at each transmission (#1:1, #2:3, #3:7, #4:15, #5:37, #6:69, #7:102)
6) The cwnd at the 17th transmission is 24. Before the drop cwnd was at 42, after the drop ssthresh=cwnd/2=21 and cwnd=ssthresh+3=24
7) ssthresh at the 24th transmission is 15. This can be calculated by looking at the last cwnd drop. It went from 29 to 1, so ssthresh was set to cwnd/2=29/2=15

Part 3

For short, let's call 192.168.1.122 Host A, and 64.238.1.122 Host B

1) The host that initiates the connection (sends a SYN packet) is 193.168.1.122 and uses source port 60643 and destination port 80


trace-tcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

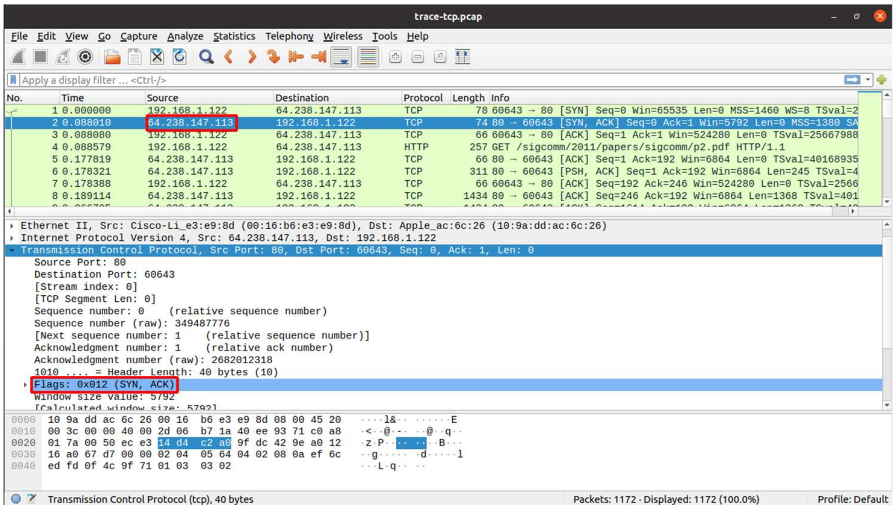
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.122   64.238.147.113  TCP        78 60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=2
   2 0.088010  64.238.147.113  192.168.1.122   TCP        74 80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SA
   3 0.088080  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=25667988
   4 0.088579  192.168.1.122   64.238.147.113  HTTP      257 GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
   5 0.177819  64.238.147.113  192.168.1.122   TCP        66 80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 TSval=40168935
   6 0.178321  64.238.147.113  192.168.1.122   TCP       311 80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=245 TSval=4
   7 0.178388  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0 TSval=2566
   8 0.189114  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1368 TSval=401
```

```
▸ Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
▸ Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
▾ Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 60643
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 2682012317
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1011 .... = Header Length: 44 bytes (11)
  ▸ Flags: 0x002 (SYN)
    Window size value: 65535
```

```
0000  00 16 b6 e3 e9 8d 10 9a  dd ac 6c 26 08 00 45 00   ········ ··l&··E·
0010  00 40 9f 8a 40 00 40 06  04 ac c0 a8 01 7a 40 ee   ·@··@·@· ·····z@·
0020  93 71 ec e3 00 50 9f dc  42 9d 00 00 00 00 b0 02   ·q···P·· B·······
0030  ff ff 22 12 00 00 02 04  05 b4 01 03 03 03 01 01   ··"····· ········
0040  08 0a 0f 4c 9f 71 00 00  00 00 04 02 00 00         ···L·q·· ······
```

Transmission Control Protocol (tcp), 44 bytes   Packets: 1172 · Displayed: 1172 (100.0%)   Profile: Default

2) The SYN packet can be seen in the screenshot above. It is obviously the first packet on the connection. The second packet is sent from B to A and it is a SYN-ACK packet. The third packet is the final step of the 3-way handshake and it is a ACK packet sent from A to B

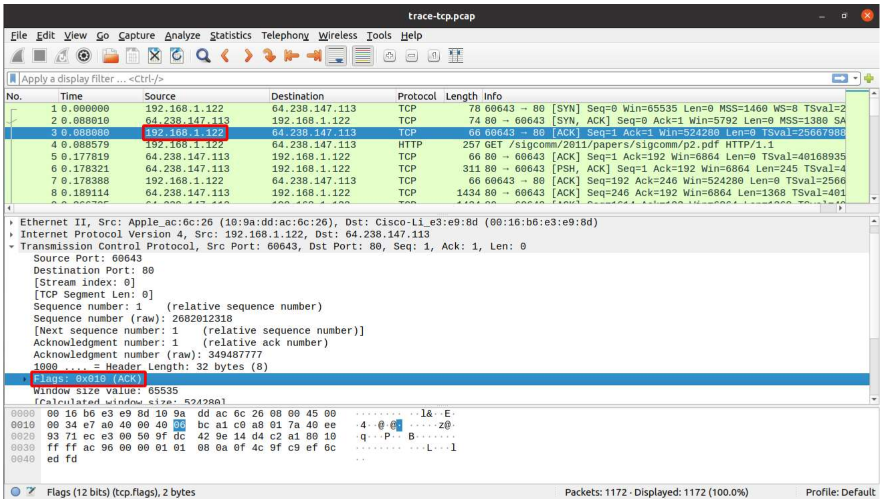

trace-tcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.122   64.238.147.113  TCP        78 60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=2
   2 0.088010  64.238.147.113  192.168.1.122   TCP        74 80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SA
   3 0.088080  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=25667988
   4 0.088579  192.168.1.122   64.238.147.113  HTTP      257 GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
   5 0.177819  64.238.147.113  192.168.1.122   TCP        66 80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 TSval=40168935
   6 0.178321  64.238.147.113  192.168.1.122   TCP       311 80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=245 TSval=4
   7 0.178388  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0 TSval=2566
   8 0.189114  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1368 TSval=401
```

```
▸ Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_ac:6c:26 (10:9a:dd:ac:6c:26)
▸ Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 60643
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 349487776
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 2682012318
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x012 (SYN, ACK)
    Window size value: 5792
    [Calculated window size: 5792]
```

```
0000  10 9a dd ac 6c 26 00 16  b6 e3 e9 8d 08 00 45 20   ····l&·· ······E
0010  00 3c 00 00 40 00 2d 06  b7 1a 40 ee 93 71 c0 a8   ·<··@·-· ··@··q··
0020  01 7a 00 50 ec e3 14 d4  c2 a0 9f dc 42 9e a0 12   ·z·P···· ····B···
0030  16 a0 67 d7 00 00 02 04  05 64 04 02 08 0a ef 6c   ··g····· ·d·····l
0040  ed fd 0f 4c 9f 71 01 03  03 02                     ···L·q·· ··
```

Transmission Control Protocol (tcp), 40 bytes   Packets: 1172 · Displayed: 1172 (100.0%)   Profile: Default


trace-tcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

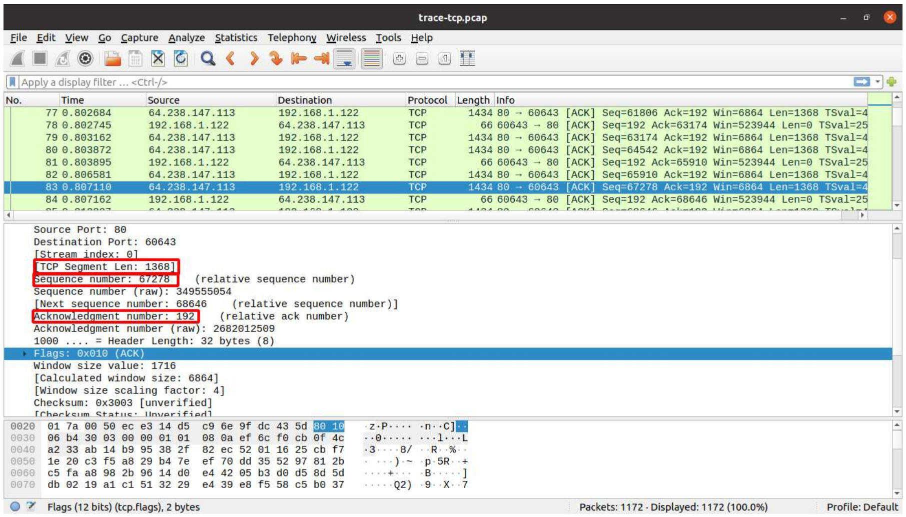
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.122   64.238.147.113  TCP        78 60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=2
   2 0.088010  64.238.147.113  192.168.1.122   TCP        74 80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SA
   3 0.088080  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=25667988
   4 0.088579  192.168.1.122   64.238.147.113  HTTP      257 GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
   5 0.177819  64.238.147.113  192.168.1.122   TCP        66 80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 TSval=40168935
   6 0.178321  64.238.147.113  192.168.1.122   TCP       311 80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=245 TSval=4
   7 0.178388  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0 TSval=2566
   8 0.189114  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1368 TSval=401
```

```
▸ Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
▸ Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
▾ Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 60643
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 2682012318
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 349487777
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 65535
    [Calculated window size: 524280]
```

```
0000  00 16 b6 e3 e9 8d 10 9a  dd ac 6c 26 08 00 45 00   ········ ··l&··E·
0010  00 34 e7 a0 40 00 40 06  bc a1 c0 a8 01 7a 40 ee   ·4··@·@· ·····z@·
0020  93 71 ec e3 00 50 9f dc  42 9e 14 d4 c2 a1 80 10   ·q···P·· B·······
0030  ff ff ac 96 00 00 01 01  08 0a 0f 4c 9f c9 ef 6c   ········ ···L···l
0040  ed fd                                              ··
```

Flags (12 bits) (tcp.flags), 2 bytes   Packets: 1172 · Displayed: 1172 (100.0%)   Profile: Default

3) The selected packet has a sequence number of 67278 and has length of 1368.
   Therefore the acknowledgment for this packet has to be 68646


trace-tcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

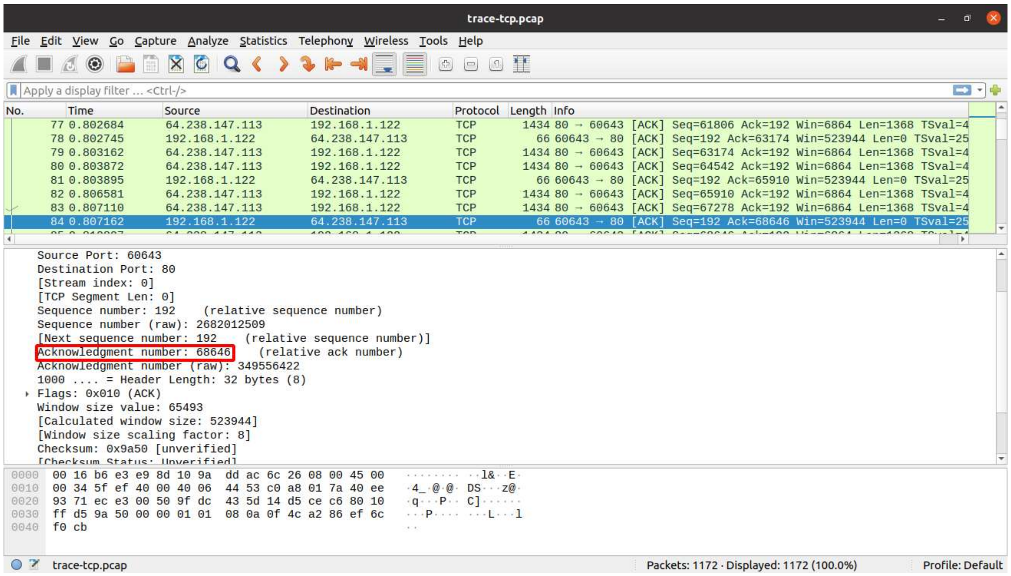
```
No.  Time      Source          Destination     Protocol Length Info
  77 0.802684  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=61806 Ack=192 Win=6864 Len=1368 TSval=4
  78 0.802745  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=63174 Win=523944 Len=0 TSval=25
  79 0.803162  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=63174 Ack=192 Win=6864 Len=1368 TSval=4
  80 0.803872  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=64542 Ack=192 Win=6864 Len=1368 TSval=4
  81 0.803895  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=65910 Win=523944 Len=0 TSval=25
  82 0.806581  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=65910 Ack=192 Win=6864 Len=1368 TSval=4
  83 0.807110  64.238.147.113  192.168.1.122   TCP      1434 80 → 60643 [ACK] Seq=67278 Ack=192 Win=6864 Len=1368 TSval=4
  84 0.807162  192.168.1.122   64.238.147.113  TCP        66 60643 → 80 [ACK] Seq=192 Ack=68646 Win=523944 Len=0 TSval=25
```

```
    Source Port: 80
    Destination Port: 60643
    [Stream index: 0]
    [TCP Segment Len: 1368]
    Sequence number: 67278    (relative sequence number)
    Sequence number (raw): 349555054
    [Next sequence number: 68646    (relative sequence number)]
    Acknowledgment number: 192    (relative ack number)
    Acknowledgment number (raw): 2682012509
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 1716
    [Calculated window size: 6864]
    [Window size scaling factor: 4]
    Checksum: 0x3003 [unverified]
    [Checksum Status: Unverified]
```

```
0020  01 7a 00 50 ec e3 14 d5  c9 6e 9f dc 43 5d 80 10   ·z·P···· ·n··C]··
0030  06 b4 30 03 00 00 01 01  08 0a ef 6c f0 cb 0f 4c   ··0····· ···l···L
0040  a2 33 ab 14 b9 95 38 2f  82 ec 52 01 16 25 cb f7   ·3····8/ ··R··%··
0050  1e 20 c3 f5 a8 29 b4 7e  ef 70 dd 35 52 97 81 2b   · ···)·~ ·p·5R··+
0060  c5 fa a8 98 2b 96 14 d0  e4 42 05 b3 d0 d5 8d 5d   ····+··· ·B·····]
0070  db 02 19 a1 c1 51 32 29  e4 39 e8 f5 58 c5 b0 37   ·····Q2) ·9··X··7
```

Flags (12 bits) (tcp.flags), 2 bytes   Packets: 1172 · Displayed: 1172 (100.0%)   Profile: Default

The ACK to the previous packet:



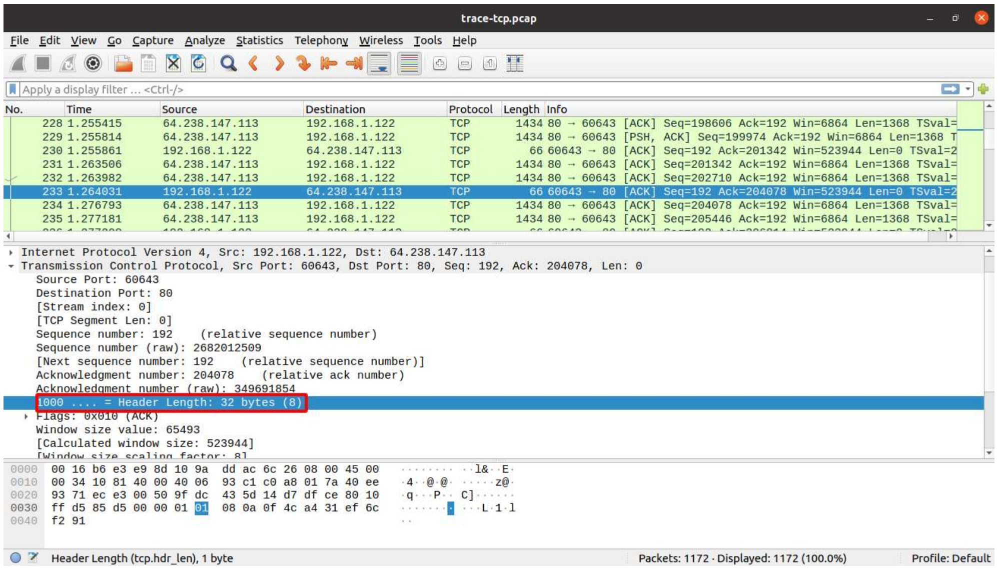
```
No.   Time        Source           Destination      Protocol Length Info
   77 0.802684    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=61806 Ack=192 Win=6864 Len=1368 TSval=4
   78 0.802745    192.168.1.122    64.238.147.113   TCP        66 60643 → 80 [ACK] Seq=192 Ack=63174 Win=523944 Len=0 TSval=25
   79 0.803162    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=63174 Ack=192 Win=6864 Len=1368 TSval=4
   80 0.803872    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=64542 Ack=192 Win=6864 Len=1368 TSval=4
   81 0.803895    192.168.1.122    64.238.147.113   TCP        66 60643 → 80 [ACK] Seq=192 Ack=65910 Win=523944 Len=0 TSval=25
   82 0.806581    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=65910 Ack=192 Win=6864 Len=1368 TSval=4
   83 0.807110    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=67278 Ack=192 Win=6864 Len=1368 TSval=4
   84 0.807162    192.168.1.122    64.238.147.113   TCP        66 60643 → 80 [ACK] Seq=192 Ack=68646 Win=523944 Len=0 TSval=25
```

```
    Source Port: 60643
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 192    (relative sequence number)
    Sequence number (raw): 2682012509
    [Next sequence number: 192    (relative sequence number)]
    Acknowledgment number: 68646    (relative ack number)
    Acknowledgment number (raw): 349556422
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 65493
    [Calculated window size: 523944]
    [Window size scaling factor: 8]
    Checksum: 0x9a50 [unverified]
```

```
0000  00 16 b6 e3 e9 8d 10 9a  dd ac 6c 26 08 00 45 00   ········ ··l&··E·
0010  00 34 5f ef 40 00 40 06  44 53 c0 a8 01 7a 40 ee   ·4_·@·@· DS···z@·
0020  93 71 ec e3 00 50 9f dc  43 5d 14 d5 ce c6 80 10   ·q···P·· C]······
0030  ff d5 9a 50 00 00 01 01  08 0a 0f 4c a2 86 ef 6c   ···P···· ···L···l
0040  f0 cb                                              ··
```

trace-tcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
trace-tcp.pcap
Packets: 1172 · Displayed: 1172 (100.0%)
Profile: Default

4) The length in bytes of all the header fields is 32 bytes, as seen in the header length field:



```
No.   Time        Source           Destination      Protocol Length Info
  228 1.255415    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=198606 Ack=192 Win=6864 Len=1368 TSval=
  229 1.255814    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [PSH, ACK] Seq=199974 Ack=192 Win=6864 Len=1368 T
  230 1.255861    192.168.1.122    64.238.147.113   TCP        66 60643 → 80 [ACK] Seq=192 Ack=201342 Win=523944 Len=0 TSval=2
  231 1.263506    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=201342 Ack=192 Win=6864 Len=1368 TSval=
  232 1.263982    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=202710 Ack=192 Win=6864 Len=1368 TSval=
  233 1.264031    192.168.1.122    64.238.147.113   TCP        66 60643 → 80 [ACK] Seq=192 Ack=204078 Win=523944 Len=0 TSval=2
  234 1.276793    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=204078 Ack=192 Win=6864 Len=1368 TSval=
  235 1.277181    64.238.147.113   192.168.1.122    TCP      1434 80 → 60643 [ACK] Seq=205446 Ack=192 Win=6864 Len=1368 TSval=
```

```
▸ Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
▾ Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack: 204078, Len: 0
    Source Port: 60643
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 192    (relative sequence number)
    Sequence number (raw): 2682012509
    [Next sequence number: 192    (relative sequence number)]
    Acknowledgment number: 204078    (relative ack number)
    Acknowledgment number (raw): 349691854
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 65493
    [Calculated window size: 523944]
```

```
0000  00 16 b6 e3 e9 8d 10 9a  dd ac 6c 26 08 00 45 00   ········ ··l&··E·
0010  00 34 10 81 40 00 40 06  93 c1 c0 a8 01 7a 40 ee   ·4··@·@· ·····z@·
0020  93 71 ec e3 00 50 9f dc  43 5d 14 d7 df ce 80 10   ·q···P·· C]······
0030  ff d5 85 d5 00 00 01 01  08 0a 0f 4c a4 31 ef 6c   ········ ···L·1·l
0040  f2 91                                              ··
```

trace-tcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Header Length (tcp.hdr_len), 1 byte
Packets: 1172 · Displayed: 1172 (100.0%)
Profile: Default