

## The segments exchanged in the 3-way handshake

### First 3-way handshake segment.

It can be identified by the SYN flag as well as the fact that it is the first segment which comes from the client (the process of establishing communication).

```
▶ Frame 38: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{02AAA61F-F837-4BA5-9...}
▶ Ethernet II, Src: ASUSTekCOMPU_b0:49:5b (18:31:bf:b0:49:5b), Dst: Intel_84:04:45 (c8:8a:9a:84:04:45)
▶ Internet Protocol Version 4, Src: 192.168.87.112, Dst: 192.168.87.181
▼ Transmission Control Protocol, Src Port: 53766, Dst Port: 1235, Seq: 0, Len: 0
  Source Port: 53766
  Destination Port: 1235
  [Stream index: 2]
  [Stream Packet Number: 1]
  ▶ [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 473755703
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x002 (SYN)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0x5b4c [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (
  ▶ [Timestamps]
```

### Second 3-way handshake segment.

The second segment in the process has a SYN, ACK flag and comes from the server (source port is 1235).

```
▶ Frame 40: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{02AAA61F-F837-4BA5-9...}
▶ Ethernet II, Src: Intel_84:04:45 (c8:8a:9a:84:04:45), Dst: ASUSTekCOMPU_b0:49:5b (18:31:bf:b0:49:5b)
▶ Internet Protocol Version 4, Src: 192.168.87.181, Dst: 192.168.87.112
▼ Transmission Control Protocol, Src Port: 1235, Dst Port: 53766, Seq: 0, Ack: 1, Len: 0
  Source Port: 1235
  Destination Port: 53766
  [Stream index: 2]
  [Stream Packet Number: 2]
  ▶ [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 293795432
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 473755704
  1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x012 (SYN, ACK)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0x309d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
```

### Third 3-way handshake segment (the last one).

The 3<sup>rd</sup> segment in the process has ACK flag and comes from the client.

```
▶ Frame 42: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{02AAA61F-F837-4BA5-9E76-718EAA8776FC}, id 0
▶ Ethernet II, Src: ASUSTekCOMPU_b0:49:5b (18:31:bf:b0:49:5b), Dst: Intel_84:04:45 (c8:8a:9a:84:04:45)
▶ Internet Protocol Version 4, Src: 192.168.87.112, Dst: 192.168.87.181
▼ Transmission Control Protocol, Src Port: 53766, Dst Port: 1235, Seq: 1, Ack: 1, Len: 0
  Source Port: 53766
  Destination Port: 1235
  [Stream index: 2]
  [Stream Packet Number: 3]
  ▶ [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 473755704
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 293795433
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x010 (ACK)
  Window: 255
  [Calculated window size: 65280]
  [Window size scaling factor: 256]
  Checksum: 0x9324 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
```

## IP addresses and port numbers associated with the TCP socket established between client and server

Internet Protocol Version 4 section the source and the destination IP addresses are different as well as the ports in the Transmission Control Protocol section.

```
Wireshark - Packet 45 - Wi-Fi
▶ Frame 45: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{02AAA61F-F837-4BA5-9E76-718EAA8776FC}, id 0
▶ Ethernet II, Src: Intel_84:04:45 (c8:8a:9a:84:04:45), Dst: ASUSTekCOMPU_b0:49:5b (18:31:bf:b0:49:5b)
▼ Internet Protocol Version 4, Src: 192.168.87.181, Dst: 192.168.87.112
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 44
  Identification: 0xc528 (50472)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.87.181
  Destination Address: 192.168.87.112
  [Stream index: 3]
▼ Transmission Control Protocol, Src Port: 1235, Dst Port: 53766, Seq: 1, Ack: 5, Len: 4
  Source Port: 1235
  Destination Port: 53766
  [Sequence Number: 1]
  [Acknowledgment Number: 5]
  [Window Size: 255]
  [Length: 4]
  [Checksum: 0x0000]
  [Urgent Pointer: 0]
  [Flags: 0x0000]
  [Timestamps: 0, 0]
  [SEQ/ACK analysis]
```

## Application layer “borrow” request message from client and response message from server

Inside the data section, it can be seen that this is the request message sent by the client (source IP address and port number).

100	19.903239	192.168.87.112	192.168.87.181	TCP	145 53766 → 1235 [PSH, ACK] Seq=5 Ack=703 Win=64768 Len=91
101	19.951661	192.168.87.181	192.168.87.112	TCP	54 1235 → 53766 [ACK] Seq=703 Ack=96 Win=65280 Len=0
102	19.964658	192.168.87.112	192.168.87.181	TCP	272 53766 → 1235 [PSH, ACK] Seq=96 Ack=703 Win=64768 Len=218
103	19.978005	192.168.87.181	192.168.87.112	TCP	55 1235 → 53766 [PSH, ACK] Seq=703 Ack=314 Win=65024 Len=1
104	20.039704	192.168.87.112	192.168.87.181	TCP	60 53766 → 1235 [ACK] Seq=314 Ack=704 Win=64768 Len=0
105	20.039833	192.168.87.181	192.168.87.112	TCP	830 1235 → 53766 [PSH, ACK] Seq=704 Ack=314 Win=65024 Len=776
106	20.102494	192.168.87.112	192.168.87.181	TCP	60 53766 → 1235 [ACK] Seq=314 Ack=1480 Win=65280 Len=0

  

▶ Frame 100: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{02AAA61F-F837-4-80-00-00-00} 0000 c8 8a 9a 84 04 45 18 31 bf b0 49 5b 08 00 45 00 .....E 1 I[. E	0010 00 83 58 c8 40 00 80 06 71 36 c0 a8 57 70 c0 a8 ..X @... q6 Wp .
▶ Ethernet II, Src: ASUSTekCOMPU_b0:49:5b (18:31:bf:b0:49:5b), Dst: Intel_84:04:45 (c8:8a:9a:84:04:45) 0020 57 b5 d2 06 04 d3 1c 3c f0 3c 11 82 f9 27 50 18 W .....< <...P	0030 00 fd e8 54 00 00 73 72 00 0d 4d 6f 64 65 6c 2e ...T .sr .Model.
▶ Internet Protocol Version 4, Src: 192.168.87.112, Dst: 192.168.87.181 0040 52 65 71 75 65 73 74 13 59 7b 1f 98 8c 9a 26 02 Request Y{...&	0050 00 03 49 00 06 75 73 65 72 49 44 4c 00 06 61 63 ..I .use rIDL .ac
▶ Transmission Control Protocol, Src Port: 53766, Dst Port: 1235, Seq: 5, Ack: 703, Len: 91 0060 74 69 6f 6e 74 00 12 4c 6a 61 76 61 2f 6c 61 6e tiont..L java/lan	0070 67 2f 53 74 72 69 6e 67 3b 4c 00 05 76 69 6e 79 g/String ;L viny
▶ Data (91 bytes) 0080 6c 74 00 0d 4c 4d 6f 64 65 6c 2f 56 69 6e 79 6c it LMod el/Vinyl	0090 3b ;
Data: 7372000d4d6f64656c2e5265717565737413597b1f988c9a260200034900067573657249444c0006616374696f6e7400124c6a617 [Length: 91]	

The same situation for the server response.

105	20.039833	192.168.87.181	192.168.87.112	TCP	830 1235 → 53766 [PSH, ACK] Seq=704 Ack=314 Win=65024 Len=776
106	20.102494	192.168.87.112	192.168.87.181	TCP	60 53766 → 1235 [ACK] Seq=314 Ack=1480 Win=65280 Len=0

  

▶ Frame 105: 830 bytes on wire (6640 bits), 830 bytes captured (6640 bits) on interface \Device\NPF_{02AAA61F-F837-4-80-00-00-00} 0000 18 31 bf b0 49 5b c8 8a 9a 84 04 45 00 00 45 00 1 I[... E E	0010 03 30 c5 2d 40 00 80 06 00 00 c0 a8 57 b5 c0 a8 ..0 -0 .....W .
▶ Ethernet II, Src: Intel_84:04:45 (c8:8a:9a:84:04:45), Dst: ASUSTekCOMPU_b0:49:5b (18:31:bf:b0:49:5b) 0020 57 70 04 d3 d2 06 11 82 f9 28 1c 3c f1 71 50 18 Wp .....(< qP	0030 00 fe 33 99 00 00 73 72 00 10 4e 65 74 77 6f 72 ..3 .sr .Networ
▶ Internet Protocol Version 4, Src: 192.168.87.181, Dst: 192.168.87.112 0040 6b 2e 52 65 73 70 6f 6e 73 65 82 92 ab bf df 05 k.Respon se .....	0050 eb 8e 02 00 02 4c 00 07 6d 65 73 73 61 67 65 74 .....L .messaget
▶ Transmission Control Protocol, Src Port: 1235, Dst Port: 53766, Seq: 704, Ack: 314, Len: 776 0060 00 12 4c 6a 61 76 61 2f 6c 61 6e 67 2f 53 74 72 ..Ljava/ lang/Str	0070 69 6e 67 3b 4c 00 06 76 69 6e 79 6c 73 74 00 10 ing;L v inylst .
▶ Data (776 bytes) 0080 4c 6a 61 76 61 2f 75 74 69 6c 2f 4c 69 73 74 3b Ljava/ut il/List;	0090 70 70 74 00 1e 52 65 71 75 65 73 74 20 70 72 6f xpt .Req uest pro
Data [..]: 737200104e6574776f726b2e526573706f6e73658292abbfd05eb8e0200024c00076d6573736167657400124c6a6176612f6 [Length: 776]	0100 63 65 73 73 65 64 20 73 75 63 65 73 73 66 75 cesssed s uccessfu
	0110 6c 6c 79 73 72 00 13 6a 61 76 61 2e 75 74 69 6c llysr .j ava.util
	0120 2e 41 72 72 61 79 4c 69 73 74 78 81 d2 14 99 c7 .ArrayLi stx ...
	0130 61 9d 03 00 01 49 00 04 73 69 7a 65 78 70 00 00 a .....I .sizexp
	0140 00 08 77 04 00 00 00 08 73 72 00 0b 4d 6f 64 65 ..w .....sr .Mode
	0150 6c 2e 56 69 6e 79 6c c2 76 d1 5a 16 a7 10 8b 02 1.Vinyl v Z .....
	0160 00 05 5a 00 0c 69 73 6f 6f 72 52 65 6d 6f 6e 61 ..Z .isF orRemova
	0170 6c 49 00 0b 72 65 6c 65 61 73 65 59 65 61 72 4c lI .rele aseYearL
	0180 00 06 61 72 74 69 73 74 71 00 7e 00 01 4c 00 0c ..artist q...L .
	0190 63 75 72 72 65 6e 74 53 74 61 74 65 74 00 12 4c currentS tater .L
	01a0 4d 6f 64 65 6c 2f 56 69 6e 79 6c 53 74 61 74 65 Model/Va nylstate
	01b0 3b 4c 00 05 74 69 74 6c 65 71 00 7e 00 01 70 70 jL .titl eq...xp
	01c0 00 00 00 07 b5 74 00 0a 50 69 6e 6b 20 46 6c 6f .....t .Pink Flo
	01d0 79 64 73 72 00 14 4d 6f 64 65 6c 2e 41 76 61 69 ydsr .Mo del.Avai
	01e0 6c 61 62 6c 65 53 74 61 74 65 99 dd 3f c9 37 72 lableSta te ? 7r
	01f0 34 8a 02 00 01 5b 00 05 75 73 65 72 73 74 00 02 4 ....[ .userst .
	0200 5b 49 78 70 70 74 00 19 54 68 65 20 44 61 72 6b [Ixptt : The Dark
	0210 20 53 69 64 65 20 6f 6e 20 74 68 65 20 44 6f 6f Side of the Moo
	0220 6e 73 71 00 7e 00 07 00 00 00 07 b1 74 00 0b 54 nsg .....t .T