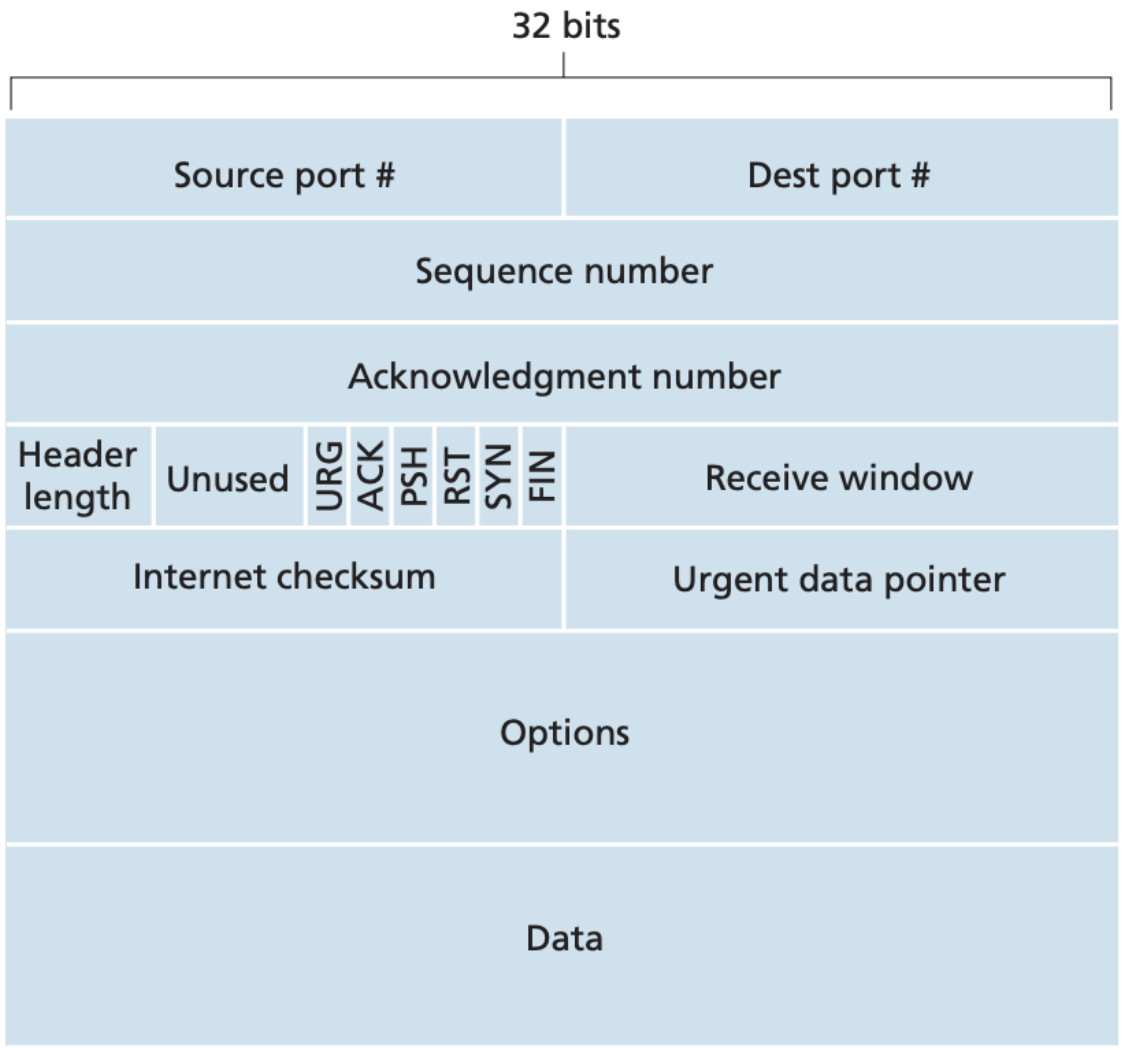
TCP 3-WAY HANDSHAKE PROCESS

(Check video link in the comment section)

INTRODUCTION

- TCP is a connection oriented protocol
- Client and server has to establish a connection before they can start exchanging data
- The process of establishing a TCP connection is called TCP 3-way handshake
- Many TCP variables are initialized on both sided during handshake process. Buffers are allocated on both the sides.
- Duplex connection

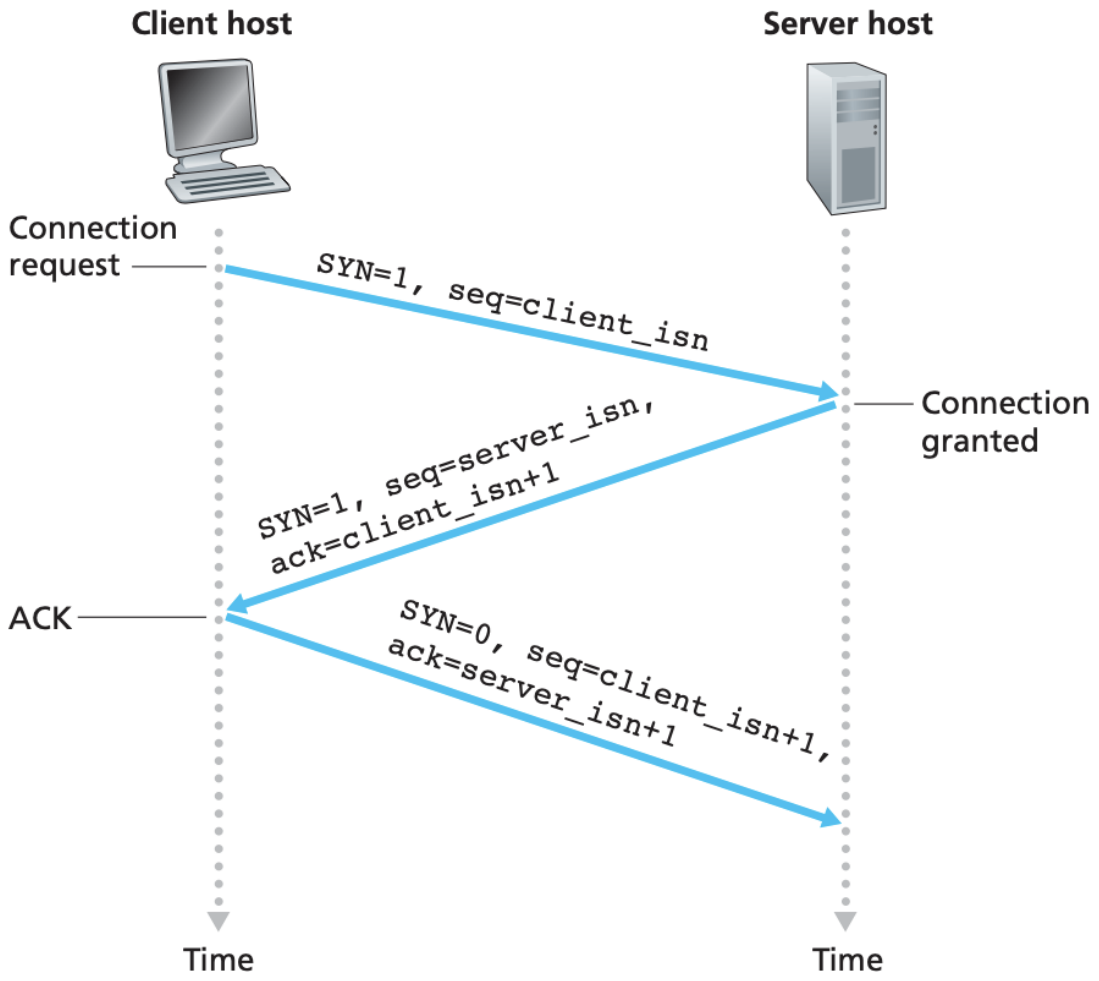
TCP SEGMENT STRUCTURE



SEQUENCE NUMBER AND ACKNOWLEDGEMENT NUMBER

- Sequence number – the byte number of first byte of data that the host is going to send in the segment
- Acknowledgement number – the next byte of data one host is expecting from the other host.
- These state variables are maintained on both client and server

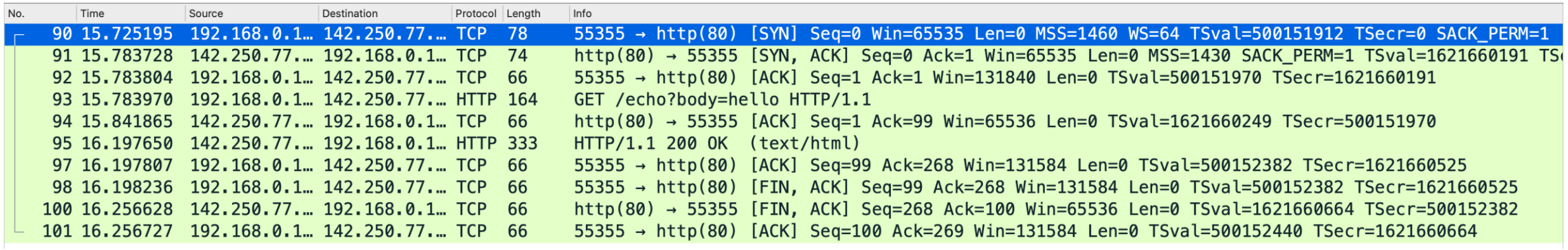
TCP 3-WAY HANDSHAKE PROCESS



WIRESHARK EXAMPLE

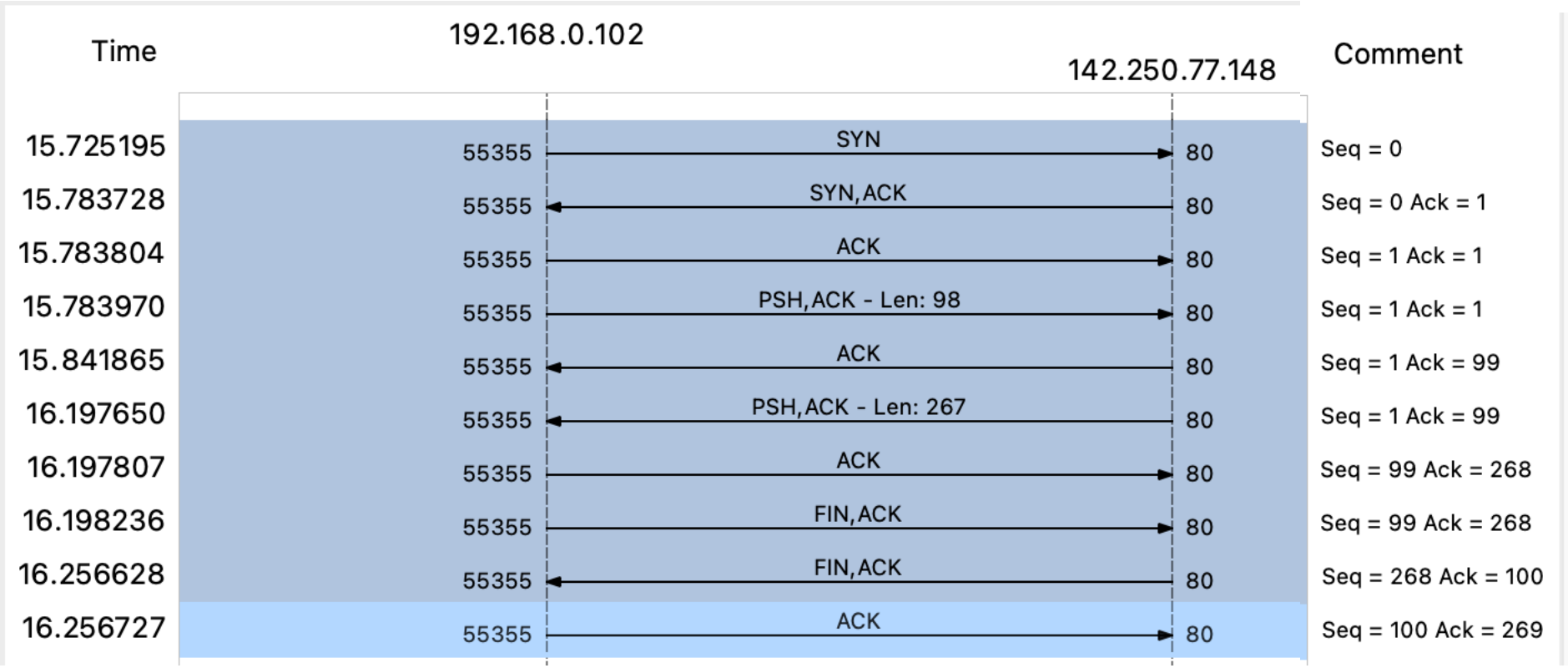
http://urlecho.appspot.com/echo?body=hello

WIRESHARK CAPTURE



No.	Time	Source	Destination	Protocol	Length	Info
90	15.725195	192.168.0.1…	142.250.77.…	TCP	78	55355 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=500151912 TSecr=0 SACK_PERM=1
91	15.783728	142.250.77.…	192.168.0.1…	TCP	74	http(80) → 55355 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 TSval=1621660191 TS
92	15.783804	192.168.0.1…	142.250.77.…	TCP	66	55355 → http(80) [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=500151970 TSecr=1621660191
93	15.783970	192.168.0.1…	142.250.77.…	HTTP	164	GET /echo?body=hello HTTP/1.1
94	15.841865	142.250.77.…	192.168.0.1…	TCP	66	http(80) → 55355 [ACK] Seq=1 Ack=99 Win=65536 Len=0 TSval=1621660249 TSecr=500151970
95	16.197650	142.250.77.…	192.168.0.1…	HTTP	333	HTTP/1.1 200 OK (text/html)
97	16.197807	192.168.0.1…	142.250.77.…	TCP	66	55355 → http(80) [ACK] Seq=99 Ack=268 Win=131584 Len=0 TSval=500152382 TSecr=1621660525
98	16.198236	192.168.0.1…	142.250.77.…	TCP	66	55355 → http(80) [FIN, ACK] Seq=99 Ack=268 Win=131584 Len=0 TSval=500152382 TSecr=1621660525
100	16.256628	142.250.77.…	192.168.0.1…	TCP	66	http(80) → 55355 [FIN, ACK] Seq=268 Ack=100 Win=65536 Len=0 TSval=1621660664 TSecr=500152382
101	16.256727	192.168.0.1…	142.250.77.…	TCP	66	55355 → http(80) [ACK] Seq=100 Ack=269 Win=131584 Len=0 TSval=500152440 TSecr=1621660664

FLOW GRAPH


Time
192.168.0.102
142.250.77.148
Comment
15.725195
55355
SYN
80
Seq = 0
15.783728
55355
SYN,ACK
80
Seq = 0 Ack = 1
15.783804
55355
ACK
80
Seq = 1 Ack = 1
15.783970
55355
PSH,ACK - Len: 98
80
Seq = 1 Ack = 1
15.841865
55355
ACK
80
Seq = 1 Ack = 99
16.197650
55355
PSH,ACK - Len: 267
80
Seq = 1 Ack = 99
16.197807
55355
ACK
80
Seq = 99 Ack = 268
16.198236
55355
FIN,ACK
80
Seq = 99 Ack = 268
16.256628
55355
FIN,ACK
80
Seq = 268 Ack = 100
16.256727
55355
ACK
80
Seq = 100 Ack = 269

SYN PACKET – START OF 3 WAY HANDSHAKE PROCESS

```
Frame 90: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: Apple_6a:ba:75 (88:e9:fe:6a:ba:75), Dst: d8:47:32:01:47:74 (d8:47:32:01:47:74)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 142.250.77.148
Transmission Control Protocol, Src Port: 55355 (55355), Dst Port: http (80), Seq: 0, Len: 0
  Source Port: 55355 (55355)
  Destination Port: http (80)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 0    (relative sequence number)
  [Next sequence number: 0    (relative sequence number)]
  Acknowledgment number: 0
  1011 .... = Header Length: 44 bytes (11)
  Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 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
    [TCP Flags: ··········S·]
  Window size value: 65535
```

SYN ACK PACKET

```
Frame 91: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: d8:47:32:01:47:74 (d8:47:32:01:47:74), Dst: Apple_6a:ba:75 (88:e9:fe:6a:ba:75)
Internet Protocol Version 4, Src: 142.250.77.148, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: http (80), Dst Port: 55355 (55355), Seq: 0, Ack: 1, Len: 0
  Source Port: http (80)
  Destination Port: 55355 (55355)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 0    (relative sequence number)
  [Next sequence number: 0    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  1010 .... = Header Length: 40 bytes (10)
  Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 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
    [TCP Flags: ·······A··S·]
  Window size value: 65535
```

ACK PACKET – 3 WAY HANDSHAKE IS COMPLETED

```
Frame 92: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Apple_6a:ba:75 (88:e9:fe:6a:ba:75), Dst: d8:47:32:01:47:74 (d8:47:32:01:47:74)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 142.250.77.148
Transmission Control Protocol, Src Port: 55355 (55355), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
  Source Port: 55355 (55355)
  Destination Port: http (80)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 1    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 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
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A····]
  Window size value: 2060
```

HTTP GET REQUEST FROM CLIENT

```
Frame 93: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
Ethernet II, Src: Apple_6a:ba:75 (88:e9:fe:6a:ba:75), Dst: d8:47:32:01:47:74 (d8:47:32:01:47:74)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 142.250.77.148
Transmission Control Protocol, Src Port: 55355 (55355), Dst Port: http (80), Seq: 1, Ack: 1, Len: 98
  Source Port: 55355 (55355)
  Destination Port: http (80)
  [Stream index: 7]
  [TCP Segment Len: 98]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 99    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
› Flags: 0x018 (PSH, ACK)
  Window size value: 2060
  [Calculated window size: 131840]
  [Window size scaling factor: 64]
  Checksum: 0xad14 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
› Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
› [SEQ/ACK analysis]
› [Timestamps]
  TCP payload (98 bytes)
Hypertext Transfer Protocol
```

HTTP REQUEST HEADERS

```
Hypertext Transfer Protocol
  GET /echo?body=hello HTTP/1.1\r\n
  Host: urlecho.appspot.com\r\n
  User-Agent: curl/7.64.1\r\n
  Accept: */*\r\n
  \r\n
  [Full request URI: http://urlecho.appspot.com/echo?body=hello]
  [HTTP request 1/1]
  [Response in frame: 95]
```

HTTP REQUEST RECEIVED - ACK FROM SERVER

```
Frame 94: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: d8:47:32:01:47:74 (d8:47:32:01:47:74), Dst: Apple_6a:ba:75 (88:e9:fe:6a:ba:75)
Internet Protocol Version 4, Src: 142.250.77.148, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: http (80), Dst Port: 55355 (55355), Seq: 1, Ack: 99, Len: 0
  Source Port: http (80)
  Destination Port: 55355 (55355)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 1    (relative sequence number)]
  Acknowledgment number: 99    (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x010 (ACK)
  Window size value: 256
  [Calculated window size: 65536]
  [Window size scaling factor: 256]
  Checksum: 0x0b34 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
```

HTTP RESPONSE FROM SERVER

```
Frame 95: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface 0
Ethernet II, Src: d8:47:32:01:47:74 (d8:47:32:01:47:74), Dst: Apple_6a:ba:75 (88:e9:fe:6a:ba:75)
Internet Protocol Version 4, Src: 142.250.77.148, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: http (80), Dst Port: 55355 (55355), Seq: 1, Ack: 99, Len: 267
  Source Port: http (80)
  Destination Port: 55355 (55355)
  [Stream index: 7]
  [TCP Segment Len: 267]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 268    (relative sequence number)]
  Acknowledgment number: 99    (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
› Flags: 0x018 (PSH, ACK)
  Window size value: 256
  [Calculated window size: 65536]
  [Window size scaling factor: 256]
  Checksum: 0x0f22 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
› Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
› [SEQ/ACK analysis]
› [Timestamps]
  TCP payload (267 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
```

HTTP RESPONSE HEADERS

```
Hypertext Transfer Protocol
› HTTP/1.1 200 OK\r\n
  Content-Type: text/html; charset=utf-8\r\n
  Cache-Control: max-age=3600\r\n
  Access-Control-Allow-Origin: *\r\n
  X-Cloud-Trace-Context: 84926b6ee3e9853041b71a2a1cad281c;o=1\r\n
  Date: Sun, 15 Aug 2021 20:17:25 GMT\r\n
  Server: Google Frontend\r\n
› Content-Length: 5\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.413680000 seconds]
  [Request in frame: 93]
  [Request URI: http://urlecho.appspot.com/echo?body=hello]
  File Data: 5 bytes
```

RESPONSE RECEIVED - ACK FROM CLIENT

```
Frame 97: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Apple_6a:ba:75 (88:e9:fe:6a:ba:75), Dst: d8:47:32:01:47:74 (d8:47:32:01:47:74)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 142.250.77.148
Transmission Control Protocol, Src Port: 55355 (55355), Dst Port: http (80), Seq: 99, Ack: 268, Len: 0
  Source Port: 55355 (55355)
  Destination Port: http (80)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 99    (relative sequence number)
  [Next sequence number: 99    (relative sequence number)]
  Acknowledgment number: 268    (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
› Flags: 0x010 (ACK)
  Window size value: 2056
  [Calculated window size: 131584]
  [Window size scaling factor: 64]
  Checksum: 0x0071 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
› Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
```