

Filter TCP packets:

The screenshot shows the Wireshark interface with the filter 'tcp.stream eq 24' applied. The packet list on the left shows several packets, with packet 183 selected. The packet details pane on the right shows the structure of the selected packet, including the HTTP 1.1 status line '200 OK' and the response body. The packet bytes pane at the bottom shows the raw data of the selected packet.

Wireshark - Follow TCP Stream (tcp.stream eq 24) - Wi-Fi

Filter: tcp.stream eq 24

Packet List:

No.	Time	Source
154	20.990454	172.20.10.5
175	21.998047	172.20.10.5
181	22.278488	34.223.124.45
182	22.278566	172.20.10.5
183	22.278878	172.20.10.5
187	22.554301	34.223.124.45
191	22.736267	34.223.124.45
192	22.736343	34.223.124.45
193	22.736369	172.20.10.5

Packet Details (Packet 183):

- Frame 183: 537 bytes on wire (4296 bits) captured (4296 bits) on interface 0
- Ethernet II, Src: Realtek, Dst: 172.20.10.5
- Internet Protocol Version 4, Src: 172.20.10.5, Dst: 34.223.124.45
- Transmission Control Protocol, Src Port: 54704, Dst Port: 80
- Hypertext Transfer Protocol
- GET /online/ HTTP/1.1
- Request Method: GET
- Request URI: /online/
- Request Version: HTTP/1.1
- Host: shiningholeclearlight.neverssl.com
- Connection: keep-alive
- Cache-Control: max-age=0
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK

Date: Fri, 12 Sep 2025 17:42:28 GMT

Server: Apache/2.4.62 (Ubuntu)

Upgrade: h2,h2c

Connection: Upgrade, Keep-Alive

Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT

ETag: "8be-5e20b29291e10-gzip"

Accept-Ranges: bytes

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 1173

Keep-Alive: timeout=5, max=100

Content-Type: text/html; charset=UTF-8

Stream 24

TCP handshake

The screenshot shows the Wireshark interface with the filter 'tcp.flags.reset' applied. The packet list on the left shows several packets, with packet 62 selected. The packet details pane on the right shows the structure of the selected packet, including the TCP header and the HTTP 1.1 status line '200 OK'. The packet bytes pane at the bottom shows the raw data of the selected packet.

Wireshark - Filtered Packets (tcp.flags.reset) - Wi-Fi

Filter: tcp.flags.reset

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
50	7.080421	172.20.10.5	34.223.124.45	TCP	66	54704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53	7.376047	34.223.124.45	172.20.10.5	TCP	66	80 → 54704 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 SACK_PERM WS=128
54	7.376148	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
55	7.376466	172.20.10.5	34.223.124.45	HTTP	628	GET /online/ HTTP/1.1
56	7.660744	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [FIN, ACK] Seq=575 Ack=1 Win=131584 Len=0
59	7.696170	34.223.124.45	172.20.10.5	TCP	54	80 → 54704 [ACK] Seq=1 Ack=575 Win=28032 Len=0
61	7.699544	34.223.124.45	172.20.10.5	TCP	1454	80 → 54704 [ACK] Seq=1 Ack=575 Win=28032 Len=1400 [TCP PDU reassembled in 63]
62	7.699588	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [RST, ACK] Seq=576 Ack=1401 Win=0 Len=0
63	7.699633	34.223.124.45	172.20.10.5	HTTP	200	HTTP/1.1 200 OK (text/html)
69	7.954582	34.223.124.45	172.20.10.5	TCP	54	80 → 54704 [FIN, ACK] Seq=1547 Ack=576 Win=28032 Len=0
77	8.564713	34.223.124.45	172.20.10.5	TCP	54	[TCP Retransmission] 80 → 54704 [FIN, ACK] Seq=1547 Ack=576 Win=28032 Len=0

Packet Details (Packet 62):

- Frame 62: 54 bytes on wire (432 bits) captured (432 bits) on interface 0
- Ethernet II, Src: Realtek, Dst: 172.20.10.5
- Internet Protocol Version 4, Src: 172.20.10.5, Dst: 34.223.124.45
- Transmission Control Protocol, Src Port: 54704, Dst Port: 80
- Flags: 0x0002 (SYN)
- Sequence Number: 576
- Acknowledgment Number: 0
- Window: 0
- Length: 0
- Checksum: 0x0000
- Options: None
- HTTP
- 200 OK (text/html)

Stream 24

SYN-ACK: Acknowledges and responds to the SYN

The screenshot shows a Wireshark capture of a TCP connection establishment. The packet list pane displays several packets, with packet 62 highlighted in red. The details pane shows the structure of the SYN-ACK packet, including the acknowledgment number, flags, and window size.

No.	Time	Source	Destination	Protocol	Length	Info
50	7.080421	172.20.10.5	34.223.124.45	TCP	66	54704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53	7.376047	34.223.124.45	172.20.10.5	TCP	66	80 → 54704 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 SACK_PERM WS=128
54	7.376140	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
55	7.376466	172.20.10.5	34.223.124.45	HTTP	628	GET /online/ HTTP/1.1
56	7.660744	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [FIN, ACK] Seq=575 Ack=1 Win=131584 Len=0
59	7.696170	34.223.124.45	172.20.10.5	TCP	54	80 → 54704 [ACK] Seq=1 Ack=575 Win=28032 Len=0
61	7.699544	34.223.124.45	172.20.10.5	TCP	1454	80 → 54704 [ACK] Seq=1 Ack=575 Win=28032 Len=1400 [TCP PDU reassembled in 63]
62	7.699588	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [RST, ACK] Seq=576 Ack=1401 Win=0 Len=0
63	7.699633	34.223.124.45	172.20.10.5	HTTP	200	HTTP/1.1 200 OK (text/html)
69	7.954582	34.223.124.45	172.20.10.5	TCP	54	80 → 54704 [FIN, ACK] Seq=1547 Ack=576 Win=28032 Len=0
77	8.564713	34.223.124.45	172.20.10.5	TCP	54	[TCP Retransmission] 80 → 54704 [FIN, ACK] Seq=1547 Ack=576 Win=28032 Len=0

Packet 62 Details:

- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3738327550
- 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
-0... = Syn: Set
-0... = Fin: Not set
- [TCP Flags:A..S]
- Window: 26883
- [Calculated window size: 26883]

Packets: 222 - Displayed: 11 (5.0%) - Dropped: 0 (0.0%) Profile: Default

ACK: Acknowledges the SYN-ACK and establishes the connection:

The screenshot shows the same Wireshark capture as before, but with packet 54 highlighted in blue. The details pane shows the structure of the ACK packet, including the acknowledgment number, flags, and window size.

No.	Time	Source	Destination	Protocol	Length	Info
50	7.080421	172.20.10.5	34.223.124.45	TCP	66	54704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53	7.376047	34.223.124.45	172.20.10.5	TCP	66	80 → 54704 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 SACK_PERM WS=128
54	7.376140	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
55	7.376466	172.20.10.5	34.223.124.45	HTTP	628	GET /online/ HTTP/1.1
56	7.660744	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [FIN, ACK] Seq=575 Ack=1 Win=131584 Len=0
59	7.696170	34.223.124.45	172.20.10.5	TCP	54	80 → 54704 [ACK] Seq=1 Ack=575 Win=28032 Len=0
61	7.699544	34.223.124.45	172.20.10.5	TCP	1454	80 → 54704 [ACK] Seq=1 Ack=575 Win=28032 Len=1400 [TCP PDU reassembled in 63]
62	7.699588	172.20.10.5	34.223.124.45	TCP	54	54704 → 80 [RST, ACK] Seq=576 Ack=1401 Win=0 Len=0
63	7.699633	34.223.124.45	172.20.10.5	HTTP	200	HTTP/1.1 200 OK (text/html)
69	7.954582	34.223.124.45	172.20.10.5	TCP	54	80 → 54704 [FIN, ACK] Seq=1547 Ack=576 Win=28032 Len=0
77	8.564713	34.223.124.45	172.20.10.5	TCP	54	[TCP Retransmission] 80 → 54704 [FIN, ACK] Seq=1547 Ack=576 Win=28032 Len=0

Packet 54 Details:

- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3602339061
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x010 (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
-0... = Syn: Not set
-0... = Fin: Not set
- [TCP Flags:A....]
- Window: 514
- [Calculated window size: 131584]

Packets: 222 - Displayed: 11 (5.0%) - Dropped: 0 (0.0%) Profile: Default

Observe the data packets exchanged between the client and server

The image shows a Wireshark packet capture of an HTTP GET request and response. The packet list on the left shows a sequence of packets, with packet 62 (HTTP GET) and packet 63 (HTTP 200 OK) highlighted. The packet details pane on the right shows the structure of the HTTP GET request, including the Host, User-Agent, Accept, and Accept-Encoding headers. The packet bytes pane at the bottom shows the raw data of the request.

GET /online/ HTTP/1.1
Host: shiningwholeclearlight.neverssl.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.0
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "8be-5e28b29291e10-gzip"
If-Modified-Since: Wed, 29 Jun 2022 00:23:22 GMT

HTTP/1.1 200 OK
Date: Fri, 12 Sep 2025 17:42:12 GMT
Server: Apache/2.4.62 ()
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT
ETag: "8be-5e28b29291e10-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1173
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8

Look at the TCP termination process (FIN, ACK packets).

The image shows a Wireshark packet capture of the TCP termination process. The packet list on the left shows a sequence of packets, with packet 62 (HTTP GET), packet 63 (HTTP 200 OK), and packet 64 (TCP FIN) highlighted. The packet details pane on the right shows the structure of the TCP FIN packet, including the Sequence Number, Acknowledgment Number, and Flags. The packet bytes pane at the bottom shows the raw data of the FIN packet.

Sequence Number (raw): 3602340607
[Next Sequence Number: 1548 (relative sequence number)]
Acknowledgment Number: 576 (relative ack number)
Acknowledgment number (raw): 3788328125
0101 = Header Length: 20 bytes (5)
▼ Flags: 0x011 (FIN, ACK)
..... = Reserved: Not set
..... = Accurate ECN: Not set
..... = Congestion Window Reduced: Not set
..... = ECHO: Not set
..... = Urgent: Not set
..... = Acknowledgment: Set
..... = Push: Not set
..... = Reset: Not set
..... = Syn: Not set
..... = Fin: Set
TCP Flags:A..F..

Task 1: Fill in the following table and provide reasons.

	TCP or UDP	Reasons
Reliability and Connection Establishment	TCP	TCP is connection-oriented and uses a handshake to establish a reliable connection.
Reliability and Connection Establishment	UDP	TCP guarantees data integrity using checksums and ensures packets are delivered in the correct order using sequence numbers.

Task 2: Identify the use Cases and Performance of TCP and UDP. ask 2: Identify the use Cases and Performance of TCP and UDP.

	TCP	UDP
Use cases	Web browsing (HTTP/HTTPS), Email, File transfer (FTP)	Video streaming, Online gaming, VoIP, Live broadcasts
Performance	Slower but reliable due to error checking, acknowledgments, and retransmissions	Faster with low latency because there is no connection setup or retransmission