

Now, we will do a Wireshark analysis of an **HTTPS** server: <https://www.wikiversity.com>
Again, we set the host as **www.wikiversity.com** in the Capture Filters of Wireshark. HTTPS is an extension to HTTP, having better security features. HTTPS also uses TCP as the Transport Layer protocol, so there is a possibility of ECN support.

ECN Related Details: Inspecting the TCP SYN packet sent by our system, we see that the **ECE and CWR bits have been set to 1**, indicating that the client supports ECN.

Capturing from wlo1 (host www.wikiversity.com)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.71	103.102.166.224	TCP	74	42752 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 SA=192.168.43.71
2	0.249852414	192.168.43.71	103.102.166.224	TCP	74	42754 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 SA=192.168.43.71
3	0.266880040	103.102.166.224	192.168.43.71	TCP	74	80 → 42752 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
4	0.266943329	192.168.43.71	103.102.166.224	TCP	66	42752 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=134891928
5	0.267169578	192.168.43.71	103.102.166.224	HTTP	485	GET / HTTP/1.1
6	1.016470900	192.168.43.71	103.102.166.224	TCP	485	[TCP Retransmission] 42752 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
7	1.272468491	192.168.43.71	103.102.166.224	TCP	74	[TCP Retransmission] 42754 → 80 [SYN] Seq=0 Win=64240 Len=0
8	1.284278530	103.102.166.224	192.168.43.71	TCP	66	80 → 42752 [ACK] Seq=1 Ack=420 Win=30208 Len=0 TSval=1437614
9	1.533848102	103.102.166.224	192.168.43.71	HTTP	1219	HTTP/1.1 301 Moved Permanently (text/html)
10	1.533860892	192.168.43.71	103.102.166.224	TCP	66	42752 → 80 [ACK] Seq=420 Ack=1154 Win=63104 Len=0 TSval=1348
11	1.533863806	103.102.166.224	192.168.43.71	TCP	74	80 → 42754 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1310 S
12	1.533880582	192.168.43.71	103.102.166.224	TCP	66	42754 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=134892055
13	1.633581168	192.168.43.71	103.102.166.224	TCP	74	43286 → 443 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 S
14	1.789074760	192.168.43.71	103.102.166.224	TCP	74	43288 → 443 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 S
15	1.904903056	103.102.166.224	192.168.43.71	TCP	74	443 → 43286 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: IntelCor_b6:5c:47 (34:e1:2d:b6:5c:47), Dst: AsustekC_dc:af:fa (18:31:bf:dc:af:fa)
Internet Protocol Version 4, Src: 192.168.43.71, Dst: 103.102.166.224
Transmission Control Protocol, Src Port: 42752, Dst Port: 80, Seq: 0, Len: 0
Source Port: 42752
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1010 = Header Length: 40 bytes (10)
Flags: 0x0c2 (SYN, ECN, CWR)
000. = Reserved: Not set
...0 = Nonce: Not set
...1 = Congestion Window Reduced (CWR): Set
...1 = ECN-Echo: Set

Packets: 98 · Displayed: 98 (100.0%) Profile: Default

The Wikiversity server does support ECN, which is indicated by the **ECE bit being set** and **CWR bit being 0** in the SYN+ACK response.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.71	103.102.166.224	TCP	74	42752 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 SA=192.168.43.71
2	0.249852414	192.168.43.71	103.102.166.224	TCP	74	42754 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 SA=192.168.43.71
3	0.266880040	103.102.166.224	192.168.43.71	TCP	74	80 → 42752 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
4	0.266943329	192.168.43.71	103.102.166.224	TCP	66	42752 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=134891928
5	0.267169578	192.168.43.71	103.102.166.224	HTTP	485	GET / HTTP/1.1
6	1.016470900	192.168.43.71	103.102.166.224	TCP	485	[TCP Retransmission] 42752 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
7	1.272468491	192.168.43.71	103.102.166.224	TCP	74	[TCP Retransmission] 42754 → 80 [SYN] Seq=0 Win=64240 Len=0
8	1.284278530	103.102.166.224	192.168.43.71	TCP	66	80 → 42752 [ACK] Seq=1 Ack=420 Win=30208 Len=0 TSval=1437614
9	1.533848102	103.102.166.224	192.168.43.71	HTTP	1219	HTTP/1.1 301 Moved Permanently (text/html)
10	1.533860892	192.168.43.71	103.102.166.224	TCP	66	42752 → 80 [ACK] Seq=420 Ack=1154 Win=63104 Len=0 TSval=1348
11	1.533863806	103.102.166.224	192.168.43.71	TCP	74	80 → 42754 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1310 S
12	1.533880582	192.168.43.71	103.102.166.224	TCP	66	42754 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=134892055
13	1.633581168	192.168.43.71	103.102.166.224	TCP	74	43286 → 443 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 S
14	1.789074760	192.168.43.71	103.102.166.224	TCP	74	43288 → 443 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 S
15	1.904903056	103.102.166.224	192.168.43.71	TCP	74	443 → 43286 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: AsustekC_dc:af:fa (18:31:bf:dc:af:fa), Dst: IntelCor_b6:5c:47 (34:e1:2d:b6:5c:47)
Internet Protocol Version 4, Src: 103.102.166.224, Dst: 192.168.43.71
Transmission Control Protocol, Src Port: 80, Dst Port: 42752, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 42752
[Stream index: 0]
[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: 0x052 (SYN, ACK, ECN)
000. = Reserved: Not set
...0 = Nonce: Not set
...0 = Congestion Window Reduced (CWR): Not set
...1 = ECN-Echo: Set

Packets: 100 · Displayed: 100 (100.0%) Profile: Default

