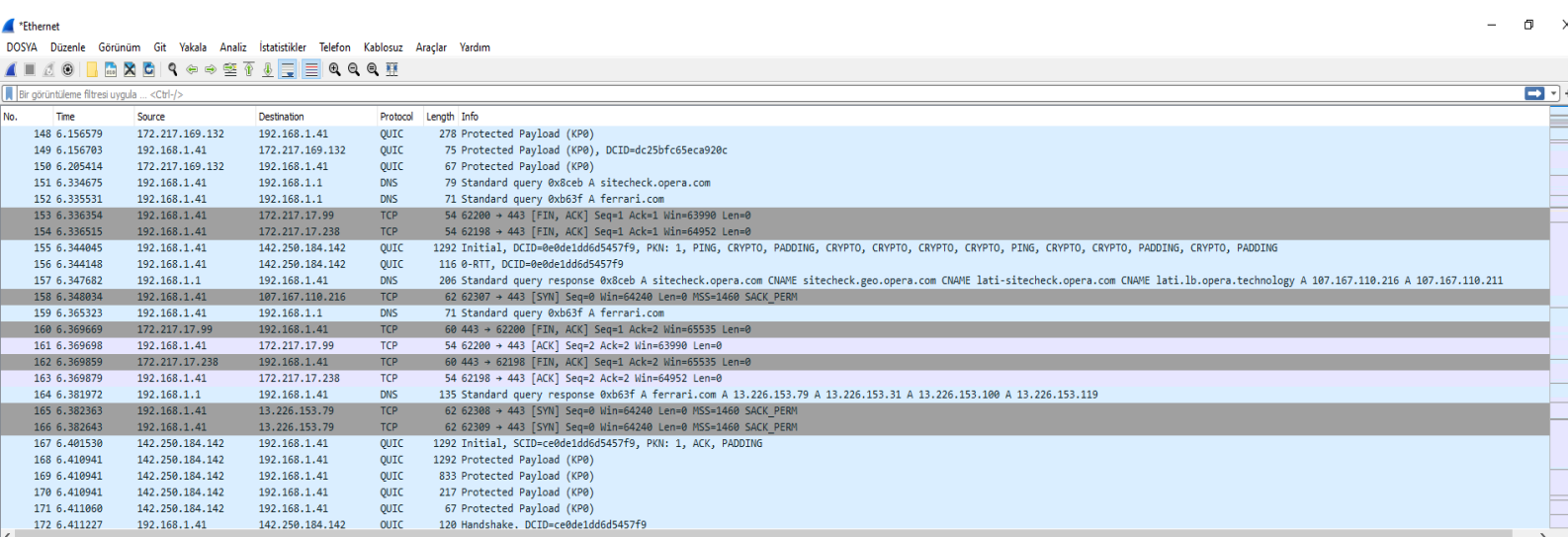


1)What happens in the background when you visit a web page?

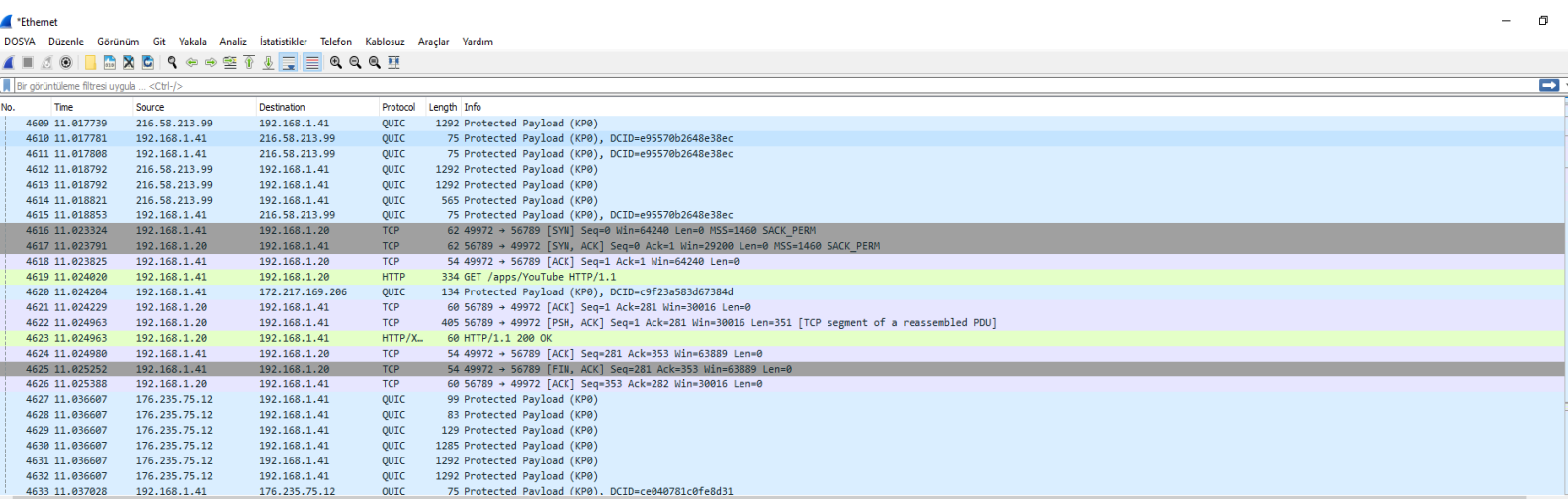
First, your browser checks whether the user has previously visited this site. If so, the browser will simply retrieve the IP address from the user's history. If the site has not been visited, the browser calls a software module called DNS resolver that is configured to your computer, and asks for the IP address that corresponds to the URL you entered. DNS transforms Domain names into IP addresses. Your browser, then, starts a connection to that IP address, using port 80 or 443(HTTP or HTTPS). The IP address signifies the server, while the port number refers to the service you want to connect to. All web servers run by default on port 80, while port 443 is used for secure web connections. The web server processes the URL you entered and gives the control to the back-end. The back-end code generates the HTML page and hands it over to the web server. The web server, then, finally sends the HTML page to the browser, via the HTTP channel.



The image shows a Wireshark packet capture for the first time visiting www.ferrari.com. The capture starts with a DNS query from 192.168.1.41 to 192.168.1.1 for the domain sitecheck.opera.com. This is followed by a TCP connection establishment (SYN, ACK) between 192.168.1.41 and 107.167.110.216 on port 443. The connection is then used to send a standard query response for the domain. The capture ends with a handshake (DCID=ce0de1dd6d5457f9).

No.	Time	Source	Destination	Protocol	Length	Info
148	6.156579	172.217.169.132	192.168.1.41	QUIC	278	Protected Payload (KP0)
149	6.156703	192.168.1.41	172.217.169.132	QUIC	75	Protected Payload (KP0), DCID=dc25bfc65eca920c
150	6.205414	172.217.169.132	192.168.1.41	QUIC	67	Protected Payload (KP0)
151	6.334675	192.168.1.41	192.168.1.1	DNS	79	Standard query 0x8ceb A sitecheck.opera.com
152	6.335531	192.168.1.41	192.168.1.1	DNS	71	Standard query 0xb63f A ferrari.com
153	6.336354	192.168.1.41	172.217.17.99	TCP	54	62200 → 443 [FIN, ACK] Seq=1 Ack=1 Win=63990 Len=0
154	6.336515	192.168.1.41	172.217.17.238	TCP	54	62198 → 443 [FIN, ACK] Seq=1 Ack=1 Win=64952 Len=0
155	6.344045	192.168.1.41	142.250.184.142	QUIC	1292	Initial, DCID=0e0de1dd6d5457f9, PKN: 1, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING
156	6.344148	192.168.1.41	142.250.184.142	QUIC	116	0-RTT, DCID=0e0de1dd6d5457f9
157	6.347682	192.168.1.1	192.168.1.41	DNS	206	Standard query response 0x8ceb A sitecheck.opera.com CNAME sitecheck.geo.opera.com CNAME lati-sitecheck.opera.com CNAME lati.lb.opera.technology A 107.167.110.216 A 107.167.110.211
158	6.348034	192.168.1.41	107.167.110.216	TCP	62	62307 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
159	6.365323	192.168.1.41	192.168.1.1	DNS	71	Standard query 0xb63f A ferrari.com
160	6.369669	172.217.17.99	192.168.1.41	TCP	60	443 → 62200 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
161	6.369698	192.168.1.41	172.217.17.99	TCP	54	62200 → 443 [ACK] Seq=2 Ack=2 Win=63990 Len=0
162	6.369859	172.217.17.238	192.168.1.41	TCP	60	443 → 62198 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
163	6.369879	192.168.1.41	172.217.17.238	TCP	54	62198 → 443 [ACK] Seq=2 Ack=2 Win=64952 Len=0
164	6.381972	192.168.1.1	192.168.1.41	DNS	135	Standard query response 0xb63f A ferrari.com A 13.226.153.79 A 13.226.153.31 A 13.226.153.100 A 13.226.153.119
165	6.382363	192.168.1.41	13.226.153.79	TCP	62	62308 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
166	6.382643	192.168.1.41	13.226.153.79	TCP	62	62309 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
167	6.401530	142.250.184.142	192.168.1.41	QUIC	1292	Initial, SCID=ce0de1dd6d5457f9, PKN: 1, ACK, PADDING
168	6.410941	142.250.184.142	192.168.1.41	QUIC	1292	Protected Payload (KP0)
169	6.410941	142.250.184.142	192.168.1.41	QUIC	833	Protected Payload (KP0)
170	6.410941	142.250.184.142	192.168.1.41	QUIC	217	Protected Payload (KP0)
171	6.411060	142.250.184.142	192.168.1.41	QUIC	67	Protected Payload (KP0)
172	6.411227	192.168.1.41	142.250.184.142	QUIC	120	Handshake. DCID=ce0de1dd6d5457f9

This image shows what happens when you visit www.ferrari.com first time.



The image shows a Wireshark packet capture for visiting www.youtube.com after having visited the site before. The capture shows a series of QUIC packets (Protected Payload) from 192.168.1.41 to 176.235.75.12. This is followed by a TCP connection establishment (SYN, ACK) between 192.168.1.41 and 176.235.75.12 on port 443. The connection is then used to send a standard query response for the domain. The capture ends with a handshake (DCID=ce040781c0fe8d31).

No.	Time	Source	Destination	Protocol	Length	Info
4609	11.017739	216.58.213.99	192.168.1.41	QUIC	1292	Protected Payload (KP0)
4610	11.017781	192.168.1.41	216.58.213.99	QUIC	75	Protected Payload (KP0), DCID=e95570b2648e38ec
4611	11.017808	192.168.1.41	216.58.213.99	QUIC	75	Protected Payload (KP0), DCID=e95570b2648e38ec
4612	11.018792	216.58.213.99	192.168.1.41	QUIC	1292	Protected Payload (KP0)
4613	11.018792	216.58.213.99	192.168.1.41	QUIC	1292	Protected Payload (KP0)
4614	11.018821	216.58.213.99	192.168.1.41	QUIC	565	Protected Payload (KP0)
4615	11.018853	192.168.1.41	216.58.213.99	QUIC	75	Protected Payload (KP0), DCID=e95570b2648e38ec
4616	11.023324	192.168.1.41	192.168.1.20	TCP	62	49972 → 56789 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4617	11.023791	192.168.1.20	192.168.1.41	TCP	62	56789 → 49972 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
4618	11.023825	192.168.1.41	192.168.1.20	TCP	54	49972 → 56789 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4619	11.024020	192.168.1.41	192.168.1.20	HTTP	334	GET /apps/YouTube HTTP/1.1
4620	11.024204	192.168.1.41	172.217.169.206	QUIC	134	Protected Payload (KP0), DCID=c9f23a583d67384d
4621	11.024229	192.168.1.20	192.168.1.41	TCP	60	56789 → 49972 [ACK] Seq=1 Ack=281 Win=30016 Len=0
4622	11.024963	192.168.1.20	192.168.1.41	TCP	405	56789 → 49972 [PSH, ACK] Seq=1 Ack=281 Win=30016 Len=351 [TCP segment of a reassembled PDU]
4623	11.024963	192.168.1.20	192.168.1.41	HTTP/X.	60	HTTP/1.1 200 OK
4624	11.024980	192.168.1.41	192.168.1.20	TCP	54	49972 → 56789 [ACK] Seq=281 Ack=353 Win=63889 Len=0
4625	11.025252	192.168.1.41	192.168.1.20	TCP	54	49972 → 56789 [FIN, ACK] Seq=281 Ack=353 Win=63889 Len=0
4626	11.025388	192.168.1.20	192.168.1.41	TCP	60	56789 → 49972 [ACK] Seq=353 Ack=282 Win=30016 Len=0
4627	11.036607	176.235.75.12	192.168.1.41	QUIC	99	Protected Payload (KP0)
4628	11.036607	176.235.75.12	192.168.1.41	QUIC	83	Protected Payload (KP0)
4629	11.036607	176.235.75.12	192.168.1.41	QUIC	129	Protected Payload (KP0)
4630	11.036607	176.235.75.12	192.168.1.41	QUIC	1285	Protected Payload (KP0)
4631	11.036607	176.235.75.12	192.168.1.41	QUIC	1292	Protected Payload (KP0)
4632	11.036607	176.235.75.12	192.168.1.41	QUIC	1292	Protected Payload (KP0)
4633	11.037028	192.168.1.41	176.235.75.12	QUIC	75	Protected Payload (KP0). DCID=ce040781c0fe8d31

This image shows what happens when you visit www.youtube.com if you have visited the site before.