

Actividad 18/1. Investigación protocolos

1. Escucha con Wireshark el tráfico e identifica el protocolo utilizado.

ip.dst == 192.173.31.59 ip.src == 192.173.31.59						
No.	Time	Source	Destination	Protocol	Length	Info
87	0.666222	10.0.2.15	192.173.31.59	TCP	66	58992 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
88	0.697541	192.173.31.59	10.0.2.15	TCP	66	443 → 58992 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
89	0.697711	10.0.2.15	192.173.31.59	TCP	54	58992 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
90	0.698156	10.0.2.15	192.173.31.59	TLSv1.3	571	Client Hello
91	0.698828	192.173.31.59	10.0.2.15	TCP	66	443 → 58992 [ACK] Seq=1 Ack=518 Win=65535 Len=0
92	1.032254	192.173.31.59	10.0.2.15	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
93	1.032254	192.173.31.59	10.0.2.15	TCP	1514	443 → 58992 [ACK] Seq=1461 Ack=518 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
94	1.032298	10.0.2.15	192.173.31.59	TCP	54	58992 → 443 [ACK] Seq=518 Ack=2921 Win=64240 Len=0
95	1.032820	192.173.31.59	10.0.2.15	TCP	1230	443 → 58992 [PSH, ACK] Seq=2921 Ack=518 Win=65535 Len=1176 [TCP segment of a reassembled PDU]
96	1.039106	192.173.31.59	10.0.2.15	TLSv1.3	1434	Application Data
97	1.039147	10.0.2.15	192.173.31.59	TCP	54	58992 → 443 [ACK] Seq=518 Ack=5477 Win=64240 Len=0
98	1.057882	192.173.31.59	10.0.2.15	TLSv1.3	283	Application Data, Application Data
99	1.065959	10.0.2.15	192.173.31.59	TLSv1.3	134	Change Cipher Spec, Application Data
100	1.066483	192.173.31.59	10.0.2.15	TCP	66	443 → 58992 [ACK] Seq=5706 Ack=598 Win=65535 Len=0
101	1.067337	10.0.2.15	192.173.31.59	TLSv1.3	911	Application Data
102	1.075999	192.173.31.59	10.0.2.15	TCP	66	443 → 58992 [ACK] Seq=5706 Ack=1455 Win=65535 Len=0
103	1.163031	192.173.31.59	10.0.2.15	TLSv1.3	293	Application Data
104	1.218226	10.0.2.15	192.173.31.59	TCP	54	58992 → 443 [ACK] Seq=1455 Ack=5945 Win=63772 Len=0
105	1.229165	192.173.31.59	10.0.2.15	TLSv1.3	293	Application Data
106	1.280950	10.0.2.15	192.173.31.59	TCP	54	58992 → 443 [ACK] Seq=1455 Ack=6184 Win=63533 Len=0
107	1.458132	192.173.31.59	10.0.2.15	TLSv1.3	1514	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
108	1.458133	192.173.31.59	10.0.2.15	TLSv1.3	281	Application Data, Application Data, Application Data

RADIO

ip.dst == 185.43.181.49 ip.src == 185.43.181.49						
No.	Time	Source	Destination	Protocol	Length	Info
12	0.431807	10.0.2.15	185.43.181.49	TLSv1.2	909	Application Data
13	0.432526	185.43.181.49	10.0.2.15	TCP	66	443 → 58065 [ACK] Seq=1 Ack=856 Win=65535 Len=0
15	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=1 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
16	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=1461 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
17	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=2921 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
18	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=4381 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
19	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=5841 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
20	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=7301 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
21	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=8761 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
22	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=10221 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
23	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=11681 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
24	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=13141 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
25	0.445528	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=14601 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
26	0.445528	185.43.181.49	10.0.2.15	TCP	399	Application Data
27	0.445590	10.0.2.15	185.43.181.49	TCP	54	58065 → 443 [ACK] Seq=856 Ack=16406 Win=64240 Len=0
28	0.445992	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=16406 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
29	0.445992	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=17866 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
30	0.445992	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=19326 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
31	0.445992	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=20786 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
32	0.445992	185.43.181.49	10.0.2.15	TCP	1114	443 → 58065 [PSH, ACK] Seq=22246 Ack=856 Win=65535 Len=1060 [TCP segment of a reassembled PDU]
33	0.446014	10.0.2.15	185.43.181.49	TCP	54	58065 → 443 [ACK] Seq=856 Ack=23306 Win=64240 Len=0
34	0.449046	185.43.181.49	10.0.2.15	TCP	1514	443 → 58065 [ACK] Seq=23306 Ack=856 Win=65535 Len=1460 [TCP segment of a reassembled PDU]

VIMEO

ip.dst == 173.194.139.170 ip.src == 173.194.139.170						
No.	Time	Source	Destination	Protocol	Length	Info
97	0.454472	10.0.2.15	173.194.139.170	QUIC	1292	Initial, DCID=e5c3e9d69425df72, PKN: 1, PADDING, CRYPTO, PADDING, PING, PING
98	0.471510	173.194.139.170	10.0.2.15	QUIC	1292	Handshake, SCID=e5c3e9d69425df72
99	0.472005	173.194.139.170	10.0.2.15	QUIC	1292	Handshake, SCID=e5c3e9d69425df72
100	0.472331	10.0.2.15	173.194.139.170	QUIC	83	Handshake, DCID=e5c3e9d69425df72
101	0.473926	173.194.139.170	10.0.2.15	QUIC	1292	Handshake, SCID=e5c3e9d69425df72
102	0.473926	173.194.139.170	10.0.2.15	QUIC	1292	Handshake, SCID=e5c3e9d69425df72
103	0.473926	173.194.139.170	10.0.2.15	QUIC	640	Protected Payload (KP0)
104	0.474334	10.0.2.15	173.194.139.170	QUIC	83	Handshake, DCID=e5c3e9d69425df72
105	0.476945	10.0.2.15	173.194.139.170	QUIC	83	Handshake, DCID=e5c3e9d69425df72
106	0.483989	10.0.2.15	173.194.139.170	QUIC	125	Handshake, DCID=e5c3e9d69425df72
107	0.485450	10.0.2.15	173.194.139.170	QUIC	112	Protected Payload (KP0), DCID=e5c3e9d69425df72
108	0.488300	10.0.2.15	173.194.139.170	QUIC	1288	Protected Payload (KP0), DCID=e5c3e9d69425df72
109	0.488472	10.0.2.15	173.194.139.170	QUIC	127	Protected Payload (KP0), DCID=e5c3e9d69425df72
110	0.489699	10.0.2.15	173.194.139.170	QUIC	1064	Protected Payload (KP0), DCID=e5c3e9d69425df72
111	0.495027	173.194.139.170	10.0.2.15	QUIC	573	Protected Payload (KP0)
112	0.495878	173.194.139.170	10.0.2.15	QUIC	158	Protected Payload (KP0)
113	0.496458	10.0.2.15	173.194.139.170	QUIC	76	Protected Payload (KP0), DCID=e5c3e9d69425df72
114	0.503666	173.194.139.170	10.0.2.15	QUIC	67	Protected Payload (KP0)
118	0.505225	173.194.139.170	10.0.2.15	QUIC	71	Protected Payload (KP0)
119	0.505225	173.194.139.170	10.0.2.15	QUIC	1292	Protected Payload (KP0)
120	0.505225	173.194.139.170	10.0.2.15	QUIC	1292	Protected Payload (KP0)
121	0.505225	173.194.139.170	10.0.2.15	QUIC	602	Protected Payload (KP0)

YOUTUBE

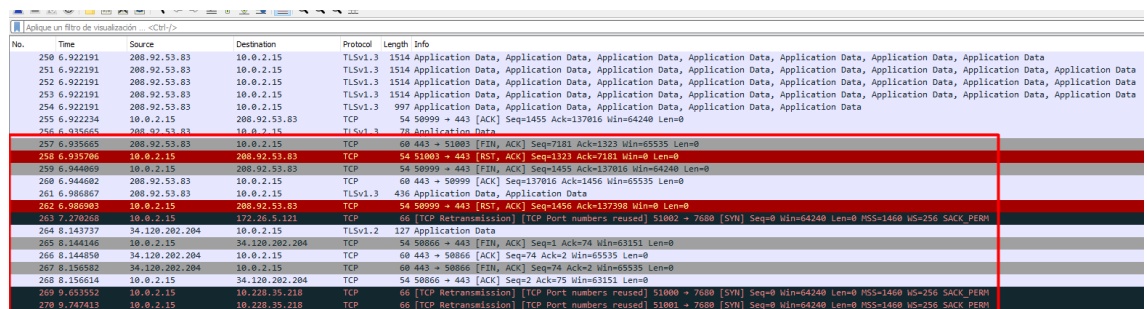
- Busca ese protocolo y resume su funcionamiento. Busca en Wireshark los campos que debe tener e identifica los que puedas.
 - Protocolo QUIC:** QUIC es el nombre de un protocolo experimental de conexión UDP rápida a Internet. El protocolo admite una serie de conexiones multiplexadas a través de UDP y se diseñó para proporcionar

una protección equivalente a TLS/SSL con una menor latencia de conexión y de transporte. Utiliza UDP denajo

- **Protocolo TCP:** Es un protocolo ubicado en la capa de transporte del modelo OSI. El objetivo del protocolo TCP es crear conexiones dentro de una red de datos compuesta por redes de computadoras para intercambiar datos.
- **Protocolo UDP:** se encarga de proporcionar un servicio de comunicación punto a punto no orientado a conexión, sino a transacciones en la capa de transporte, permitiendo la transmisión sin conexión de datagramas en redes que estén basadas en IP

3. Pausa la reproducción y observa qué pasa.

RADIO:



No.	Time	Source	Destination	Protocol	Length	Info
258	6.922191	208.92.53.83	10.0.2.15	TLSv1.3	1514	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
259	6.922191	208.92.53.83	10.0.2.15	TLSv1.3	1514	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
260	6.922191	208.92.53.83	10.0.2.15	TLSv1.3	1514	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
261	6.922191	208.92.53.83	10.0.2.15	TLSv1.3	1514	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
262	6.922234	10.0.2.15	208.92.53.83	TCP	54	58999 → 443 [ACK] Seq=1455 Ack=137816 Win=64240 Len=0
263	6.935605	208.92.53.83	10.0.2.15	TLSv1.3	78	Application Data
264	6.935706	10.0.2.15	208.92.53.83	TCP	60	443 → 51002 [RST, ACK] Seq=1323 Ack=51002 Win=0 Len=0
265	6.944089	10.0.2.15	208.92.53.83	TCP	54	58999 → 443 [FIN, ACK] Seq=1455 Ack=137816 Win=64240 Len=0
266	6.944602	208.92.53.83	10.0.2.15	TCP	60	443 → 58999 [ACK] Seq=137816 Ack=1456 Win=65535 Len=0
267	6.986867	208.92.53.83	10.0.2.15	TLSv1.3	436	Application Data, Application Data
268	6.986983	10.0.2.15	208.92.53.83	TCP	54	58999 → 443 [RST, ACK] Seq=1456 Ack=137398 Win=0 Len=0
269	7.270268	10.0.2.15	172.26.5.121	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 51002 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
270	8.143737	34.120.202.204	10.0.2.15	TLSv1.2	127	Application Data
271	8.144146	10.0.2.15	34.120.202.204	TCP	54	58999 → 443 [FIN, ACK] Seq=1 Ack=74 Win=63151 Len=0
272	8.144598	34.120.202.204	10.0.2.15	TCP	60	443 → 58999 [ACK] Seq=74 Ack=2 Win=65535 Len=0
273	8.156582	34.120.202.204	10.0.2.15	TCP	60	443 → 58999 [FIN, ACK] Seq=74 Ack=2 Win=65535 Len=0
274	8.156614	10.0.2.15	34.120.202.204	TCP	54	58999 → 443 [ACK] Seq=2 Ack=75 Win=63151 Len=0
275	8.633552	10.0.2.15	10.228.35.218	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 51002 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
276	9.747415	10.0.2.15	10.228.35.218	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 51002 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Lo que ocurre es que aparece un paquete FYN ACK y luego un paquete FYN RST que indica el final de la reproducción.

VIMEO:

Cambia los TCP por UDP

YOUTUBE:

Deja de enviar Quic