

Preguntas Wireshark

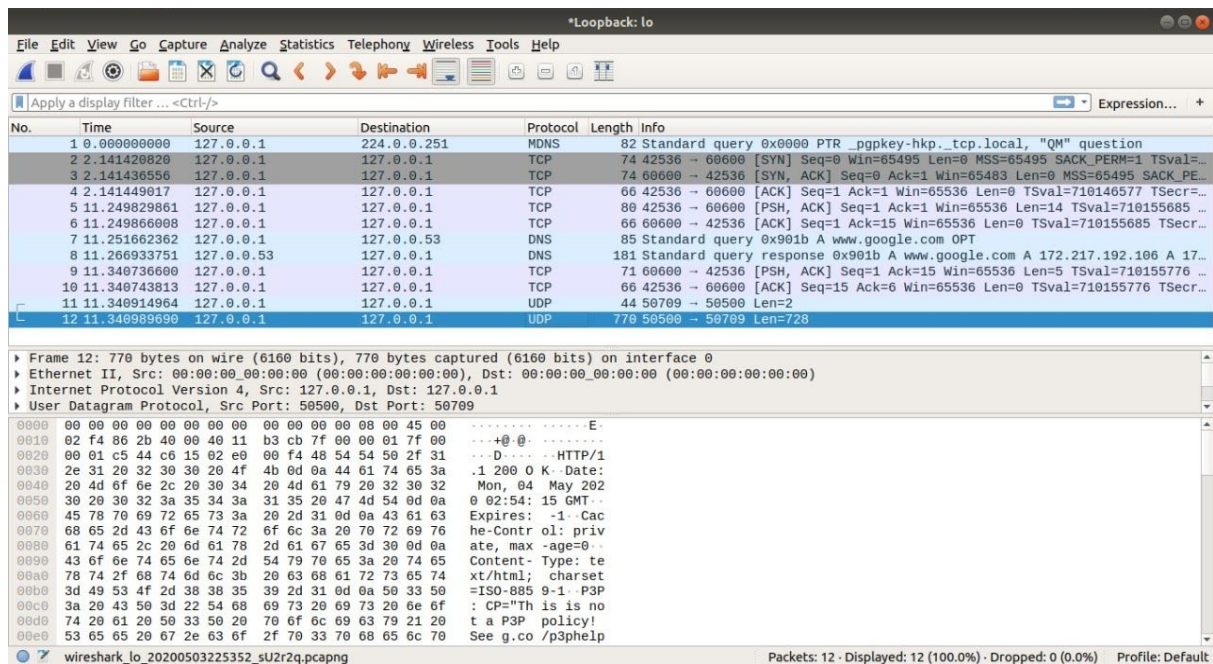
1.- En la ejecución del programa se esperaba ver mensajes con protocolo TCP, UDP entre el servidor y el cliente, se esperaba HTTP con respuesta TCP entre el servidor y la página web.

Por Wireshark se encontraron efectivamente conexiones TCP y UDP entre cliente y servidor. Por último entre servidor y página web se hace una solicitud HTTP y responde en TCP. Por lo cual cumple con lo esperado.

2.- Se esperaba que se usará siempre el mismo puerto, ya que lo definimos en el programa. Pero Wireshark nos mostró que no es así, ya que los puertos que definimos son del servidor y no del cliente, por lo cual los puertos de servidor se mantienen (siendo diferente entre TCP y UDP), pero los del cliente varían en cada ejecución.

3.- La verdad es que no es legible, pero Wireshark nos decodifica el mensaje, por lo cual en una parte está el mensaje codificado y en la otra está decodificado. Igual es importante notar que en la parte codificada hay una parte que no es legible, pero al final se muestra el mensaje que se envía.

4. Parte con una parte que es ilegible, pero luego es igual al almacenado por el cliente, con la única diferencia de que la respuesta a la consulta HTTP viene con el archivo HTML incluido.



Conexión Cliente-Servidor

Wireshark interface showing network traffic analysis. The main display area shows a list of captured packets, with packet 57 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
54	28.274587119	192.168.0.27	172.217.192.147	TCP	76	48094 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=...
55	28.302745236	172.217.192.147	192.168.0.27	TCP	76	80 → 48094 [SYN, ACK] Seq=0 Ack=1 Win=62392 Len=0 MSS=1430 SACK_...
56	28.302839943	192.168.0.27	172.217.192.147	TCP	68	48094 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3854225080 TS...
57	28.302983741	192.168.0.27	172.217.192.147	HTTP	86	GET / HTTP/1.1
58	28.378874425	172.217.192.147	192.168.0.27	TCP	68	80 → 48094 [ACK] Seq=1 Ack=19 Win=62464 Len=0 TSval=2494856449 T...
59	28.414417350	172.217.192.147	192.168.0.27	TCP	1486	80 → 48094 [ACK] Seq=1 Ack=19 Win=62464 Len=1418 TSval=249485648...
60	28.414451237	192.168.0.27	172.217.192.147	TCP	68	48094 → 80 [ACK] Seq=19 Ack=1419 Win=64128 Len=0 TSval=385422519...
61	28.414500814	172.217.192.147	192.168.0.27	TCP	1486	80 → 48094 [ACK] Seq=1419 Ack=19 Win=62464 Len=1418 TSval=249485...
62	28.414518749	192.168.0.27	172.217.192.147	TCP	68	48094 → 80 [ACK] Seq=19 Ack=2837 Win=62976 Len=0 TSval=385422519...
63	28.414540804	172.217.192.147	192.168.0.27	TCP	1486	80 → 48094 [ACK] Seq=2837 Ack=19 Win=62464 Len=1418 TSval=249485...
64	28.414551378	192.168.0.27	172.217.192.147	TCP	68	48094 → 80 [ACK] Seq=19 Ack=4255 Win=61824 Len=0 TSval=385422519...
65	28.414566989	172.217.192.147	192.168.0.27	TCP	1486	80 → 48094 [ACK] Seq=4255 Ack=19 Win=62464 Len=1418 TSval=249485...
66	28.414578951	192.168.0.27	172.217.192.147	TCP	68	48094 → 80 [ACK] Seq=19 Ack=5673 Win=60544 Len=0 TSval=385422519...

Frame 57: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.0.27, Dst: 172.217.192.147
Transmission Control Protocol, Src Port: 48094, Dst Port: 80, Seq: 1, Ack: 1, Len: 18

```

0000  00 04 00 01 00 06 24 0a 64 51 c6 f1 00 00 08 00  ....$.dQ.....
0010  45 00 00 46 12 57 40 00 40 06 fa 2a c0 a8 00 1b  E..F.W@.@.*....
0020  ac d9 c0 93 bb de 00 50 44 dd 40 2b 56 4e a9 98  ....P.D.@+VN...
0030  80 18 01 f6 60 e2 00 00 01 01 08 0a e5 ba ce b8  ....*.....
0040  94 b4 7c b3 47 45 54 20 2f 20 48 54 54 50 2f 31  ..|.GET / HTTP/1
0050  2e 31 0d 0a 0d 0a  ....1....

```

Wireshark interface showing network traffic analysis. The main display area shows a list of captured packets, with packet 57 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Conexión Servidor-Página Web