

Redes de comunicaciones

I

Práctica I

Emilio Cuesta Fernández

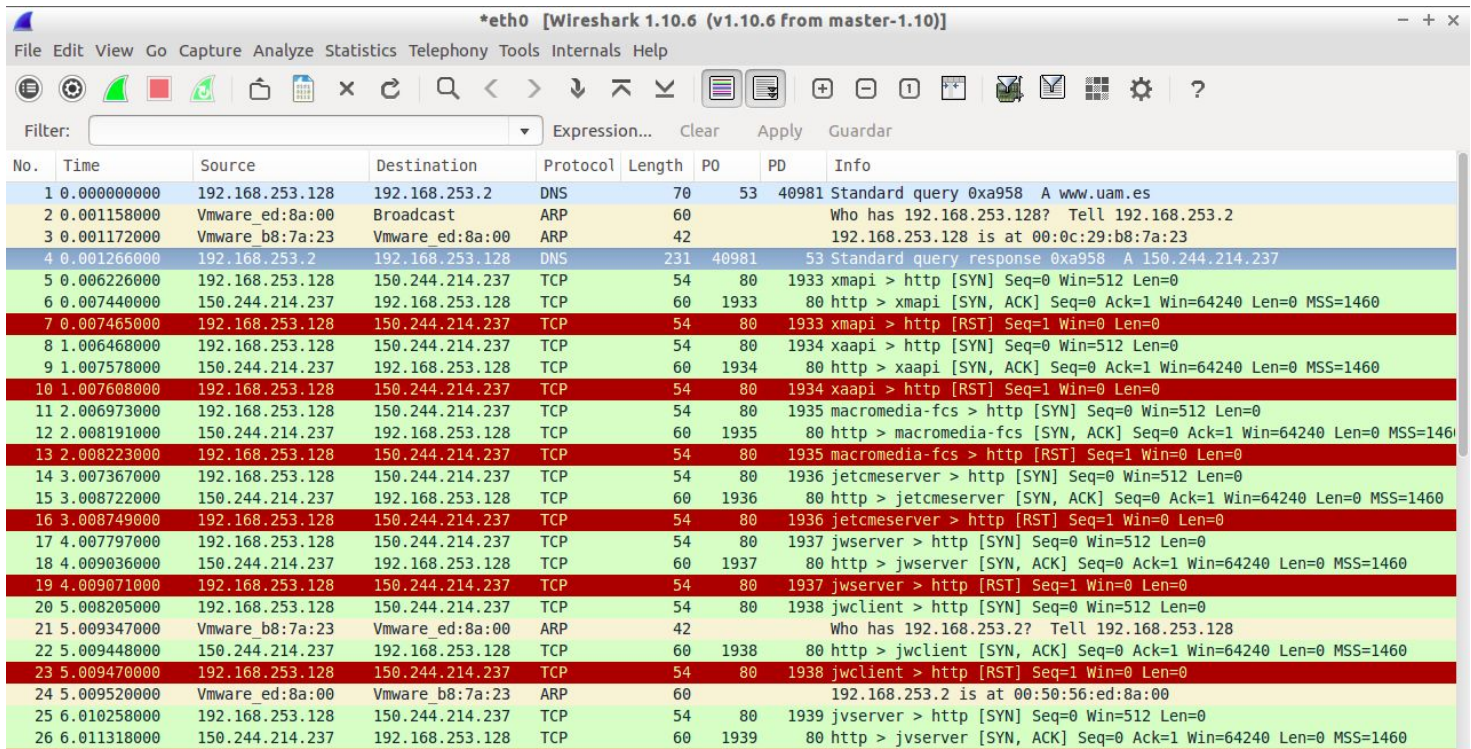
Pablo Alejo Polanía Bernárdez

Grupo 1302. Pareja 6

EJERCICIOS DE CAPTURA DE TRÁFICO

EJERCICIO 1:

Captura de la interfaz “eth0” tras ejecutar el comando “sudo hping3 -S -p 80 www.uam.es”:



No.	Time	Source	Destination	Protocol	Length	PO	PD	Info
1	0.000000000	192.168.253.128	192.168.253.2	DNS	70	53	40981	Standard query 0xa958 A www.uam.es
2	0.001158000	Vmware_ed:8a:00	Broadcast	ARP	60			Who has 192.168.253.128? Tell 192.168.253.2
3	0.001172000	Vmware_b8:7a:23	Vmware_ed:8a:00	ARP	42			192.168.253.128 is at 00:0c:29:b8:7a:23
4	0.001266000	192.168.253.2	192.168.253.128	DNS	231	40981	53	Standard query response 0xa958 A 150.244.214.237
5	0.006226000	192.168.253.128	150.244.214.237	TCP	54	80	1933	xmapi > http [SYN] Seq=0 Win=512 Len=0
6	0.007440000	150.244.214.237	192.168.253.128	TCP	60	1933	80	http > xmapi [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7	0.007465000	192.168.253.128	150.244.214.237	TCP	54	80	1933	xmapi > http [RST] Seq=1 Win=0 Len=0
8	1.006468000	192.168.253.128	150.244.214.237	TCP	54	80	1934	xaapi > http [SYN] Seq=0 Win=512 Len=0
9	1.007578000	150.244.214.237	192.168.253.128	TCP	60	1934	80	http > xaapi [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10	1.007608000	192.168.253.128	150.244.214.237	TCP	54	80	1934	xaapi > http [RST] Seq=1 Win=0 Len=0
11	2.006973000	192.168.253.128	150.244.214.237	TCP	54	80	1935	macromedia-fcs > http [SYN] Seq=0 Win=512 Len=0
12	2.008191000	150.244.214.237	192.168.253.128	TCP	60	1935	80	http > macromedia-fcs [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
13	2.008223000	192.168.253.128	150.244.214.237	TCP	54	80	1935	macromedia-fcs > http [RST] Seq=1 Win=0 Len=0
14	3.007367000	192.168.253.128	150.244.214.237	TCP	54	80	1936	jetcmseserver > http [SYN] Seq=0 Win=512 Len=0
15	3.008722000	150.244.214.237	192.168.253.128	TCP	60	1936	80	http > jetcmseserver [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	3.008749000	192.168.253.128	150.244.214.237	TCP	54	80	1936	jetcmseserver > http [RST] Seq=1 Win=0 Len=0
17	4.007797000	192.168.253.128	150.244.214.237	TCP	54	80	1937	jwserver > http [SYN] Seq=0 Win=512 Len=0
18	4.009036000	150.244.214.237	192.168.253.128	TCP	60	1937	80	http > jwserver [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
19	4.009071000	192.168.253.128	150.244.214.237	TCP	54	80	1937	jwserver > http [RST] Seq=1 Win=0 Len=0
20	5.008205000	192.168.253.128	150.244.214.237	TCP	54	80	1938	jwclient > http [SYN] Seq=0 Win=512 Len=0
21	5.009347000	Vmware_b8:7a:23	Vmware_ed:8a:00	ARP	42			Who has 192.168.253.2? Tell 192.168.253.128
22	5.009448000	150.244.214.237	192.168.253.128	TCP	60	1938	80	http > jwclient [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
23	5.009470000	192.168.253.128	150.244.214.237	TCP	54	80	1938	jwclient > http [RST] Seq=1 Win=0 Len=0
24	5.009520000	Vmware_ed:8a:00	Vmware_b8:7a:23	ARP	60			192.168.253.2 is at 00:50:56:ed:8a:00
25	6.010258000	192.168.253.128	150.244.214.237	TCP	54	80	1939	jvserver > http [SYN] Seq=0 Win=512 Len=0
26	6.011318000	150.244.214.237	192.168.253.128	TCP	60	1939	80	http > jvserver [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

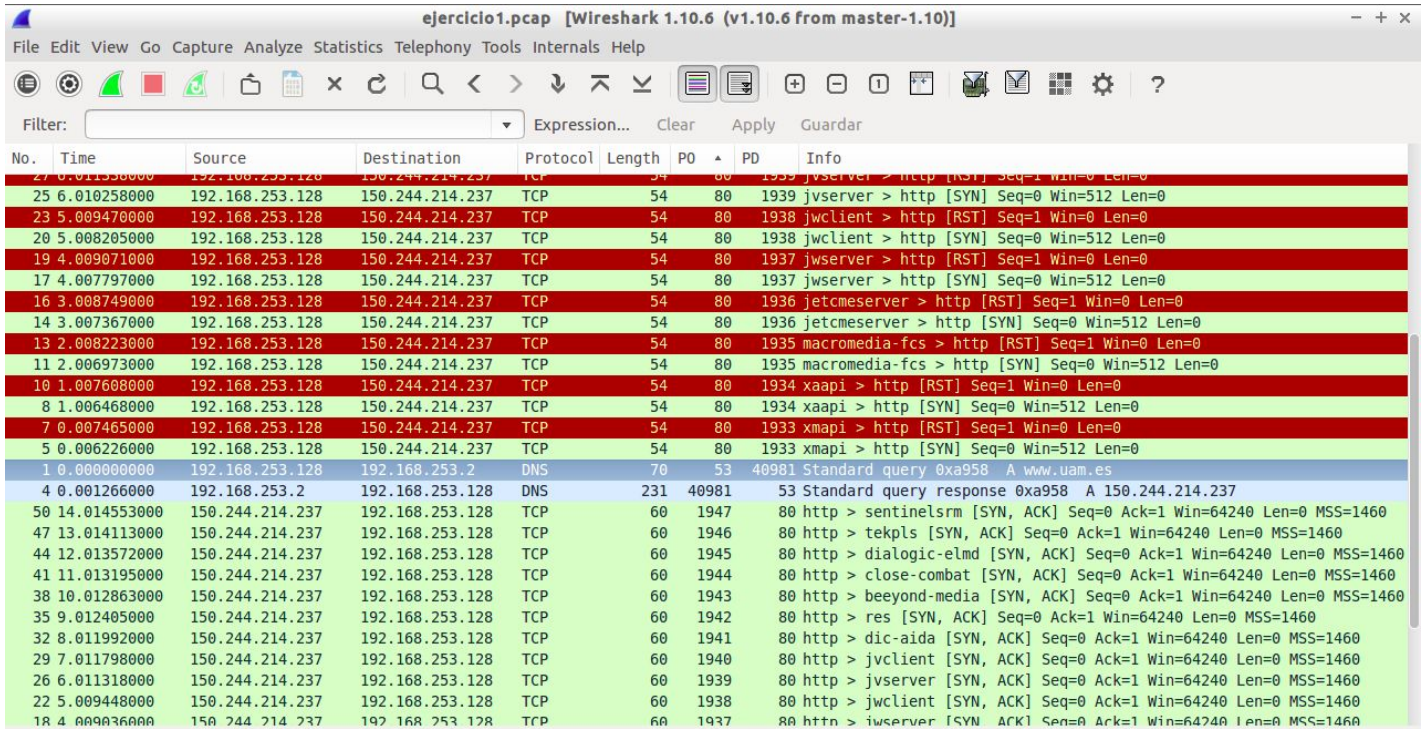
La traza capturada en este ejercicio se entrega en el fichero “ejercicio1.pcap”.

6. Analice el tráfico capturado (aunque no lo entienda en detalle)

La aplicación WireShark ordena los paquetes según se van capturando y muestra por pantalla distinta información (IP, length, Source, etc...) sobre el paquete en forma de columnas. El usuario puede seleccionar un paquete y acceder a los distintos niveles de la estructura del paquete. Con ello se ve, por ejemplo, el espacio que ocupa cada protocolo y su contenido.

10. Utilizando las columnas que se han añadido durante el tutorial, ordene con respecto al campo 'PO' en sentido descendente y contabilice el número de paquetes en el que este campo tiene valor 53.

Como se puede ver en la captura de pantalla tras ordenar las filas según la columna 'PO' (basta con hacer doble click en la columna para ordenar) solo hay un Puerto Origen 53.



No.	Time	Source	Destination	Protocol	Length	PO	PD	Info
27	0.001338000	192.168.253.128	150.244.214.237	TCP	54	80	80	1939 jwserver > http [RST] Seq=1 Win=0 Len=0
25	6.010258000	192.168.253.128	150.244.214.237	TCP	54	80	80	1939 jwserver > http [SYN] Seq=0 Win=512 Len=0
23	5.009470000	192.168.253.128	150.244.214.237	TCP	54	80	80	1938 jwclient > http [RST] Seq=1 Win=0 Len=0
20	5.008205000	192.168.253.128	150.244.214.237	TCP	54	80	80	1938 jwclient > http [SYN] Seq=0 Win=512 Len=0
19	4.009071000	192.168.253.128	150.244.214.237	TCP	54	80	80	1937 jwserver > http [RST] Seq=1 Win=0 Len=0
17	4.007797000	192.168.253.128	150.244.214.237	TCP	54	80	80	1937 jwserver > http [SYN] Seq=0 Win=512 Len=0
16	3.008749000	192.168.253.128	150.244.214.237	TCP	54	80	80	1936 jetcmeserver > http [RST] Seq=1 Win=0 Len=0
14	3.007367000	192.168.253.128	150.244.214.237	TCP	54	80	80	1936 jetcmeserver > http [SYN] Seq=0 Win=512 Len=0
13	2.008223000	192.168.253.128	150.244.214.237	TCP	54	80	80	1935 macromedia-fcs > http [RST] Seq=1 Win=0 Len=0
11	2.006973000	192.168.253.128	150.244.214.237	TCP	54	80	80	1935 macromedia-fcs > http [SYN] Seq=0 Win=512 Len=0
10	1.007608000	192.168.253.128	150.244.214.237	TCP	54	80	80	1934 xaapi > http [RST] Seq=1 Win=0 Len=0
8	1.006468000	192.168.253.128	150.244.214.237	TCP	54	80	80	1934 xaapi > http [SYN] Seq=0 Win=512 Len=0
7	0.007465000	192.168.253.128	150.244.214.237	TCP	54	80	80	1933 xmapl > http [RST] Seq=1 Win=0 Len=0
5	0.006226000	192.168.253.128	150.244.214.237	TCP	54	80	80	1933 xmapl > http [SYN] Seq=0 Win=512 Len=0
1	0.000000000	192.168.253.128	192.168.253.2	DNS	70	53	40981	Standard query 0xa958 A www.uam.es
4	0.001266000	192.168.253.2	192.168.253.128	DNS	231	40981	53	Standard query response 0xa958 A 150.244.214.237
50	14.014553000	150.244.214.237	192.168.253.128	TCP	60	1947	80	http > sentinelsrm [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
47	13.014113000	150.244.214.237	192.168.253.128	TCP	60	1946	80	http > tekpls [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
44	12.013572000	150.244.214.237	192.168.253.128	TCP	60	1945	80	http > dialogic-elmd [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
41	11.013195000	150.244.214.237	192.168.253.128	TCP	60	1944	80	http > close-combat [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
38	10.012863000	150.244.214.237	192.168.253.128	TCP	60	1943	80	http > beeyond-media [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35	9.012405000	150.244.214.237	192.168.253.128	TCP	60	1942	80	http > res [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
32	8.011992000	150.244.214.237	192.168.253.128	TCP	60	1941	80	http > dic-aida [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
29	7.011798000	150.244.214.237	192.168.253.128	TCP	60	1940	80	http > jwclient [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
26	6.011318000	150.244.214.237	192.168.253.128	TCP	60	1939	80	http > jwserver [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
22	5.009448000	150.244.214.237	192.168.253.128	TCP	60	1938	80	http > jwclient [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
18	4.008036000	150.244.214.237	192.168.253.128	TCP	60	1937	80	http > jwserver [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Curiosamente, también parece haber solo un puerto 53 en la columna PD.

Descripción y dificultades

Se ha capturado el tráfico según las especificaciones del enunciado pero al ordenar de manera descendente según la columna 'PO' el resultado no fue el esperado. A pesar de ser un número "bajo", el puerto 53 estaba por encima de otros como el 1946. Esto se debe a que el criterio de ordenación utilizado por Wireshark no es numérico, sino que los ordena como si fuesen cadenas de caracteres.

Por otro lado, la primera vez no había ningún paquete con el PO = 53, seguramente debido a una mala coordinación entre el inicio de captura y la ejecución del comando.

EJERCICIO 2:

La traza sobre la que se trabaja en este ejercicio se adjunta en el fichero “*ejercicio2.pcap*”.

1. Copie el filtro realizado

Para visualizar los paquetes de tipo IP y de un tamaño superior a los 1000 Bytes hemos ejecutado el siguiente comando de filtro: *ip && frame.len > 1000*

2. ¿Cómo almacenaría en una captura solo los paquetes mostrados?

Para almacenar en una captura solamente los paquetes que se muestran por pantalla, una vez ejecutado el filtro, simplemente se debe exportar (Export Specified Packets) y seleccionar la opción de guardar solo los que se estén mostrando por pantalla en ese momento, es decir, los que han superado el filtro. No es válido guardar el documento después de aplicar el filtro, porque eso tiene como resultado la traza sobre la que se trabajaba originalmente.

Se adjunta una traza con los elementos filtrados en el archivo “*ejercicio2filtrado.pcap*”

3. Compare el tamaño del primer paquete IP, y el campo 'length' del protocolo IP del mismo.

Repita para los primeros 5 paquetes, ¿qué relación encuentra?

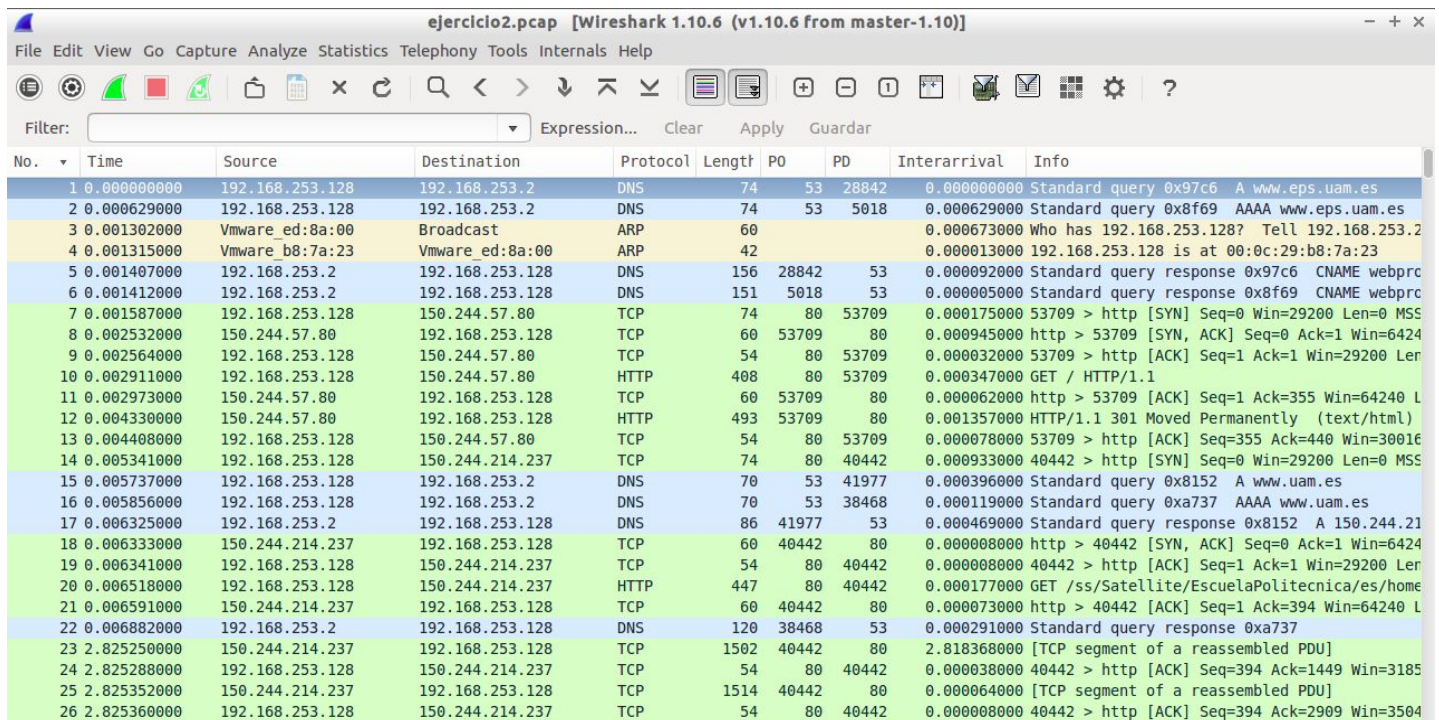
	Tamaño de IP (Bytes)	Tamaño total del paquete (Bytes)
Paquete 1	1488	1502
Paquete 2	1500	1514
Paquete 3	1500	1514
Paquete 4	1500	1514
Paquete 5	1500	1514

Se puede apreciar que la diferencia entre el tamaño de Internet Protocol y la del tamaño total del paquete es de 14 Bytes. También parece que el tamaño de los paquetes nunca supera los 1514 Bytes.

EJERCICIO 3:

Se debe acceder a “Column Preferences” y añadir una nueva columna del tipo “Delta time” denominándola *interarrival*. Luego hay que hacerla visible desde la opción “Columns Display”.

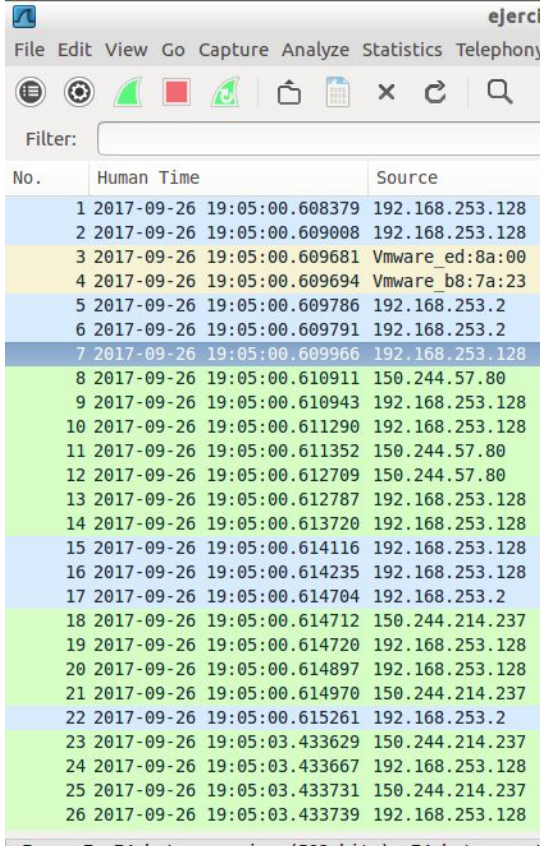
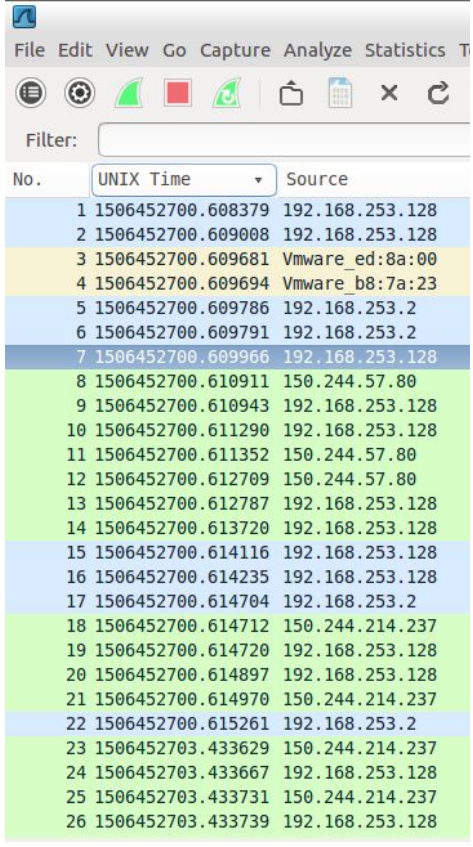
Como se puede apreciar en la siguiente imagen, el tiempo entre la llegada de dos paquetes consecutivos es muy pequeño, tan solo en una vez supera el segundo, pero eso no es algo común.



No.	Time	Source	Destination	Protocol	Length	PO	PD	Interarrival	Info
1	0.000000000	192.168.253.128	192.168.253.2	DNS	74	53	28842	0.000000000	Standard query 0x97c6 A www.eps.uam.es
2	0.000629000	192.168.253.128	192.168.253.2	DNS	74	53	5018	0.000629000	Standard query 0x8f69 AAAA www.eps.uam.es
3	0.001302000	Vmware_ed:8a:00	Broadcast	ARP	60			0.000673000	Who has 192.168.253.128? Tell 192.168.253.2
4	0.001315000	Vmware_b8:7a:23	Vmware_ed:8a:00	ARP	42			0.000013000	192.168.253.128 is at 00:0c:29:b8:7a:23
5	0.001407000	192.168.253.2	192.168.253.128	DNS	156	28842	53	0.000092000	Standard query response 0x97c6 CNAME webprc
6	0.001412000	192.168.253.2	192.168.253.128	DNS	151	5018	53	0.000005000	Standard query response 0x8f69 CNAME webprc
7	0.001587000	192.168.253.128	150.244.57.80	TCP	74	80	53709	0.000175000	53709 > http [SYN] Seq=0 Win=29200 Len=0 MSS
8	0.002532000	150.244.57.80	192.168.253.128	TCP	60	53709	80	0.000945000	http > 53709 [SYN, ACK] Seq=0 Ack=1 Win=6424
9	0.002564000	192.168.253.128	150.244.57.80	TCP	54	80	53709	0.000032000	53709 > http [ACK] Seq=1 Ack=1 Win=29200 Ler
10	0.002911000	192.168.253.128	150.244.57.80	HTTP	408	80	53709	0.000347000	GET / HTTP/1.1
11	0.002973000	150.244.57.80	192.168.253.128	TCP	60	53709	80	0.000062000	http > 53709 [ACK] Seq=1 Ack=355 Win=64240 L
12	0.004330000	150.244.57.80	192.168.253.128	HTTP	493	53709	80	0.001357000	HTTP/1.1 301 Moved Permanently (text/html)
13	0.004408000	192.168.253.128	150.244.57.80	TCP	54	80	53709	0.000078000	53709 > http [ACK] Seq=355 Ack=440 Win=30016
14	0.005341000	192.168.253.128	150.244.214.237	TCP	74	80	40442	0.000933000	40442 > http [SYN] Seq=0 Win=29200 Len=0 MSS
15	0.005737000	192.168.253.128	192.168.253.2	DNS	70	53	41977	0.000396000	Standard query 0x8152 A www.uam.es
16	0.005856000	192.168.253.128	192.168.253.2	DNS	70	53	38468	0.000119000	Standard query 0xa737 AAAA www.uam.es
17	0.006325000	192.168.253.2	192.168.253.128	DNS	86	41977	53	0.000469000	Standard query response 0x8152 A 150.244.21
18	0.006333000	150.244.214.237	192.168.253.128	TCP	60	40442	80	0.000008000	http > 40442 [SYN, ACK] Seq=0 Ack=1 Win=6424
19	0.006341000	192.168.253.128	150.244.214.237	TCP	54	80	40442	0.000008000	40442 > http [ACK] Seq=1 Ack=1 Win=29200 Ler
20	0.006518000	192.168.253.128	150.244.214.237	HTTP	447	80	40442	0.000177000	GET /ss/Satellite/EscuelaPolitecnica/es/home
21	0.006591000	150.244.214.237	192.168.253.128	TCP	60	40442	80	0.000073000	http > 40442 [ACK] Seq=1 Ack=394 Win=64240 L
22	0.006882000	192.168.253.2	192.168.253.128	DNS	120	38468	53	0.000291000	Standard query response 0xa737
23	2.825250000	150.244.214.237	192.168.253.128	TCP	1502	40442	80	2.818368000	[TCP segment of a reassembled PDU]
24	2.825288000	192.168.253.128	150.244.214.237	TCP	54	80	40442	0.000038000	40442 > http [ACK] Seq=394 Ack=1449 Win=3185
25	2.825352000	150.244.214.237	192.168.253.128	TCP	1514	40442	80	0.000064000	[TCP segment of a reassembled PDU]
26	2.825360000	192.168.253.128	150.244.214.237	TCP	54	80	40442	0.000008000	40442 > http [ACK] Seq=394 Ack=2909 Win=3504

EJERCICIO 4:

Para mostrar el tiempo “humano” se accede al menú “View/Time Display Format” y se selecciona “Date and Time of Day”. Análogamente, para mostrar el tiempo Unix (en segundos) se accede al mismo menú seleccionando la opción “Seconds Since Epoch”.

	
Tiempo humano	Tiempo UNIX(s)

EJERCICIO 5:

Para decidir los filtros de captura, en la pantalla de inicio de WireShark, se debe hacer doble click sobre la interfaz “eth0” de la “Interface List” mostrada en la primera pantalla del programa, aunque también se puede configurar posteriormente. En el pop-up se selecciona “Capture Filter” y finalmente “UDP only”.

El resultado de aplicar el filtro de captura es el siguiente:

No.	UNIX Time	Source	Destination	Protocol	Length	PO	PD	Interarrival
1	1506455934.9455296	192.168.253.128	192.168.253.2	DNS	70	53	13856	0.000000000
2	1506455934.9469476	192.168.253.2	192.168.253.128	DNS	231	13856	53	0.001418000
3	1506455938.5968276	192.168.253.128	192.168.253.2	DNS	79	53	48523	3.649880000
4	1506455938.5969996	192.168.253.128	192.168.253.2	DNS	79	53	6276	0.000172000
5	1506455938.6429076	192.168.253.2	192.168.253.128	DNS	79	48523	53	0.045908000
6	1506455938.6429396	192.168.253.2	192.168.253.128	DNS	79	6276	53	0.000032000
7	1506455938.6432436	192.168.253.128	192.168.253.2	DNS	67	53	56105	0.000304000
8	1506455938.6435006	192.168.253.128	192.168.253.2	DNS	67	53	12458	0.000257000
9	1506455938.6438226	192.168.253.2	192.168.253.128	DNS	67	56105	53	0.000322000
10	1506455938.6438316	192.168.253.2	192.168.253.128	DNS	67	12458	53	0.000009000
11	1506455938.6443386	192.168.253.128	192.168.253.2	DNS	79	53	56330	0.000507000
12	1506455938.6446206	192.168.253.2	192.168.253.128	DNS	79	56330	53	0.000282000
13	1506455938.6448006	192.168.253.128	192.168.253.2	DNS	79	53	24842	0.000180000
14	1506455938.6449476	192.168.253.2	192.168.253.128	DNS	79	24842	53	0.000147000
15	1506455938.6452696	192.168.253.128	192.168.253.2	DNS	67	53	61525	0.000322000
16	1506455938.6454966	192.168.253.128	192.168.253.2	DNS	67	53	62283	0.000227000
17	1506455938.6456416	192.168.253.2	192.168.253.128	DNS	67	61525	53	0.000145000
18	1506455938.6457966	192.168.253.2	192.168.253.128	DNS	67	62283	53	0.000155000
19	1506455938.6474086	192.168.253.128	192.168.253.2	DNS	79	53	48106	0.001612000
20	1506455938.6475786	192.168.253.2	192.168.253.128	DNS	79	48106	53	0.000170000
21	1506455938.6478806	192.168.253.128	192.168.253.2	DNS	79	53	28411	0.000302000
22	1506455938.6480276	192.168.253.2	192.168.253.128	DNS	79	28411	53	0.000147000
23	1506455938.6494026	192.168.253.128	192.168.253.2	DNS	67	53	58747	0.001375000
24	1506455938.6496296	192.168.253.128	192.168.253.2	DNS	67	53	15943	0.000227000
25	1506455938.6497746	192.168.253.2	192.168.253.128	DNS	67	58747	53	0.000145000
26	1506455938.6507716	192.168.253.2	192.168.253.128	DNS	67	15943	53	0.000997000

Como se puede apreciar, ahora solo se han capturado paquetes que tienen en la columna el campo DNS, que no es UDP. Sin embargo, haciendo click en cada paquete, podemos ver que en otras capas de estos paquetes está presente el protocolo “User Datagram Protocol”, que es el que se estaba filtrando. Es decir, los filtros de captura no sólo se fijan en el protocolo exterior, por así llamarlo, si no que también comprueban los demás.

Cabe destacar la diferencia entre los filtros de captura y los filtros de representación, que solo ocultan de la traza mostrada por pantalla los paquetes que no cumplen una serie de condiciones, pero estos siguen siendo parte de la traza. Mediante un filtro de captura, en la traza sólo se almacenan los paquetes que satisfacen las condiciones fijadas.

Por otro lado, que todos los paquetes filtrados (incluso los que no se muestran en la captura) sean DNS, parece indicar que existe una fuerte relación entre el protocolo UDP y el DNS.

EJERCICIO DE CODIFICACIÓN

Se puede apreciar que, al ejecutar `practical.c` pasando “*prueba.pcap*” como argumento, la salida de la información del primer paquete coincide con la recogida por WireShark en su totalidad (en el ejemplo se imprimen por pantalla tan solos los 25 primeros bytes).

```

lubuntu@lubuntu:~/Desktop/redes1/pl$ sudo ./practical 25 prueba.pcap
Nuevo paquete capturado a las Tue Sep 26 19:58:54 2017
Contenido:
00 50 56 ED 8A 00 00 0C 29 B8 7A 23 08 00 45 00 00 38 FE 0A 40 00 40 11 C0
Nuevo paquete capturado a las Tue Sep 26 19:58:54 2017

```

No.	Time	Source	Destination
1	0.000000	192.168.253.128	192.168.253.2
2	0.001418	192.168.253.2	192.168.253.128
3	3.651298	192.168.253.128	192.168.253.2

```

▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560
▼ Ethernet II, Src: Vmware_b8:7a:23 (00:0c:29:b8:7a:23), Dst: V
  ▼ Destination: Vmware_ed:8a:00 (00:50:56:ed:8a:00)
    Address: Vmware_ed:8a:00 (00:50:56:ed:8a:00)
      .... 0. .... = LG bit: Globally unique address
      .... 0 .... = IG bit: Individual address
    Source: Vmware_b8:7a:23 (00:0c:29:b8:7a:23)

```

```

0000  00 50 56 ed 8a 00 00 0c 29 b8 7a 23 08 00 45 00  .PV..
0010  00 38 fe 0a 40 00 40 11 c0 d5 c0 a8 fd 80 c0 a8  .8..@
0020  fd 02 36 20 00 35 00 24 69 3b 8e 07 01 00 00 01  ..6 .
0030  00 00 00 00 00 00 03 77 77 77 03 75 61 6d 02 65  ....
0040  73 00 00 01 00 01                                S....

```

No es viable adjuntar fotos de cada uno de los paquetes, pero los datos coinciden. Se puede comprobar ejecutando el programa con el fichero anteriormente mencionado.