

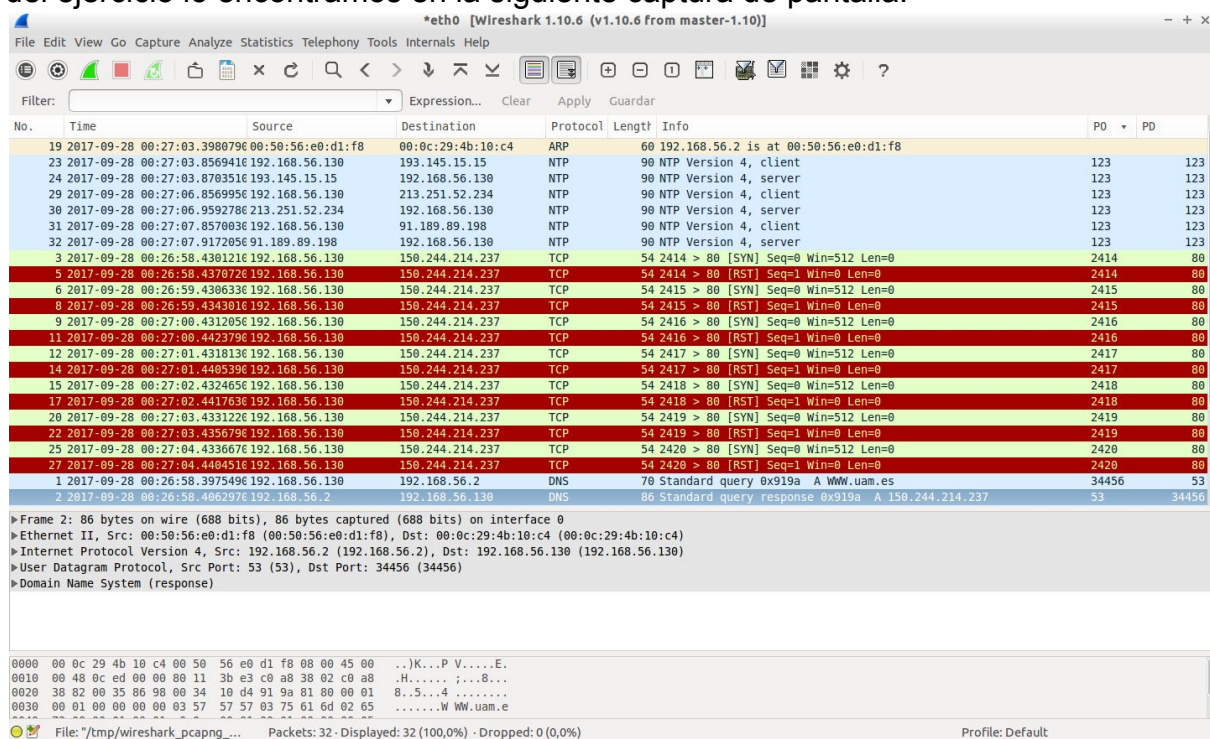
Practica 1:

Parte 0:

- Ejercicio 1:

Para añadir las columnas PO y PD seguimos las instrucciones dadas en la práctica: Edit→Preferences→Columns y en el menú seleccionamos añadir columna tomando los campos deseados. Al organizar los paquetes y ver su valor en el campo 'PO' solo encontramos un paquete con el valor 53 (seleccionado en la imagen inferior).

No se encontró inconveniente en la realización de este ejercicio. El resultado del ejercicio lo encontramos en la siguiente captura de pantalla.



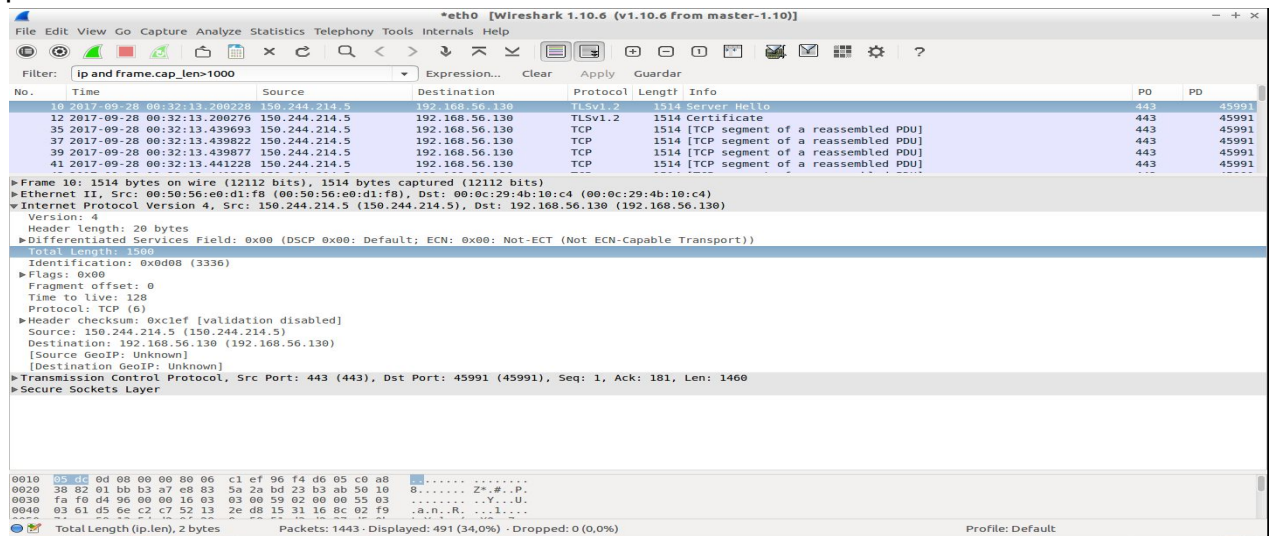
- Ejercicio 2:

Una vez terminada la captura, introducimos el filtro "ip and frame.cap_len > 1000" para obtener los paquetes solicitados por el enunciado.

Para guardar el filtro, basta con clicar en la esquina superior izquierda "File" y luego "Export specified packets".

Al revisar las longitudes de los cinco primeros paquetes (después del filtrado) todos eran de 1514 bytes, como se puede observar en la imagen inferior. Además, su longitud de protocolo IP era solo de 1500 bytes (fila seleccionada en la imagen

inferior), por ello inferimos que los otros 14 bytes corresponden a la cabecera del protocolo IP en la trama.



- Ejercicio 3:

Para añadir la columna con información referente al tiempo de llegada entre paquetes utilizamos el mismo menú que en el ejercicio 1 y seleccionamos 'Delta Time' que muestra la información requerida.

En la siguiente captura de pantalla observamos la columna de "Interarrival" añadida al principio.

Interarrival.	Time	Source	Destination	Protocol	Length	Info	PO	PD
0.000000	0.000000	192.168.56.128	150.244.214.237	TCP	54	1890 > 80 [SYN] Seq=0 Win=512 Len=0	1890	80
0.003166	0.003166	150.244.214.237	192.168.56.128	TCP	60	80 > 1890 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1890
0.000135	0.000135	192.168.56.128	150.244.214.237	TCP	54	1890 > 80 [RST] Seq=1 Win=0 Len=0	1890	80
0.997229	1.000530	192.168.56.128	150.244.214.237	TCP	54	1891 > 80 [SYN] Seq=0 Win=512 Len=0	1891	80
0.004908	1.005438	150.244.214.237	192.168.56.128	TCP	60	80 > 1891 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1891
0.000037	1.005475	192.168.56.128	150.244.214.237	TCP	54	1891 > 80 [RST] Seq=1 Win=0 Len=0	1891	80
0.995597	2.001072	192.168.56.128	150.244.214.237	TCP	54	1892 > 80 [SYN] Seq=0 Win=512 Len=0	1892	80
0.004821	2.005893	150.244.214.237	192.168.56.128	TCP	60	80 > 1892 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1892
0.000038	2.005931	192.168.56.128	150.244.214.237	TCP	54	1892 > 80 [RST] Seq=1 Win=0 Len=0	1892	80
0.995547	3.001478	192.168.56.128	150.244.214.237	TCP	54	1893 > 80 [SYN] Seq=0 Win=512 Len=0	1893	80
0.004175	3.005653	150.244.214.237	192.168.56.128	TCP	60	80 > 1893 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1893
0.000037	3.005690	192.168.56.128	150.244.214.237	TCP	54	1893 > 80 [RST] Seq=1 Win=0 Len=0	1893	80
0.008844	3.014534	00:0c:29:38:c7:61	00:50:56:e0:d1:f8	ARP	42	Who has 192.168.56.2? Tell 192.168.56.128		
0.000205	3.014739	00:50:56:e0:d1:f8	00:0c:29:38:c7:61	ARP	60	192.168.56.2 is at 00:50:56:e0:d1:f8		
0.150309	3.165048	192.168.56.128	213.251.52.234	NTP	90	NTP Version 4, client	123	123
0.039098	3.204146	213.251.52.234	192.168.56.128	NTP	90	NTP Version 4, server	123	123
0.797682	4.001828	150.244.214.237	192.168.56.128	TCP	54	1894 > 80 [SYN] Seq=0 Win=512 Len=0	1894	80
0.003270	4.005098	150.244.214.237	192.168.56.128	TCP	60	80 > 1894 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1894
0.000043	4.005141	192.168.56.128	150.244.214.237	TCP	54	1894 > 80 [RST] Seq=1 Win=0 Len=0	1894	80
0.997177	5.002318	192.168.56.128	150.244.214.237	TCP	54	1895 > 80 [SYN] Seq=0 Win=512 Len=0	1895	80
0.001665	5.003983	150.244.214.237	192.168.56.128	TCP	60	80 > 1895 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1895
0.000035	5.004018	192.168.56.128	150.244.214.237	TCP	54	1895 > 80 [RST] Seq=1 Win=0 Len=0	1895	80
0.998820	6.002838	192.168.56.128	150.244.214.237	TCP	54	1896 > 80 [SYN] Seq=0 Win=512 Len=0	1896	80
0.004386	6.007224	150.244.214.237	192.168.56.128	TCP	60	80 > 1896 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1896
0.000044	6.007260	192.168.56.128	150.244.214.237	TCP	54	1896 > 80 [RST] Seq=1 Win=0 Len=0	1896	80
0.996128	7.003396	192.168.56.128	150.244.214.237	TCP	54	1897 > 80 [SYN] Seq=0 Win=512 Len=0	1897	80
0.007849	7.011245	150.244.214.237	192.168.56.128	TCP	60	80 > 1897 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1897
0.000038	7.011283	192.168.56.128	150.244.214.237	TCP	54	1897 > 80 [RST] Seq=1 Win=0 Len=0	1897	80
0.153752	7.165035	192.168.56.128	193.145.15.15	NTP	90	NTP Version 4, client	123	123
0.004268	7.169303	193.145.15.15	192.168.56.128	NTP	90	NTP Version 4, server	123	123

- Ejercicio 4:

Para el primer cambio, hemos clicado en la columna “Time”, hemos pulsado “Edit column”, y nos ha aparecido sobre las columnas un menú como el siguiente, donde en “Type”, eligiendo “UTC date” y clicando OK, obtenemos el tiempo en formato “humano”, como observamos a continuación (segunda columna):

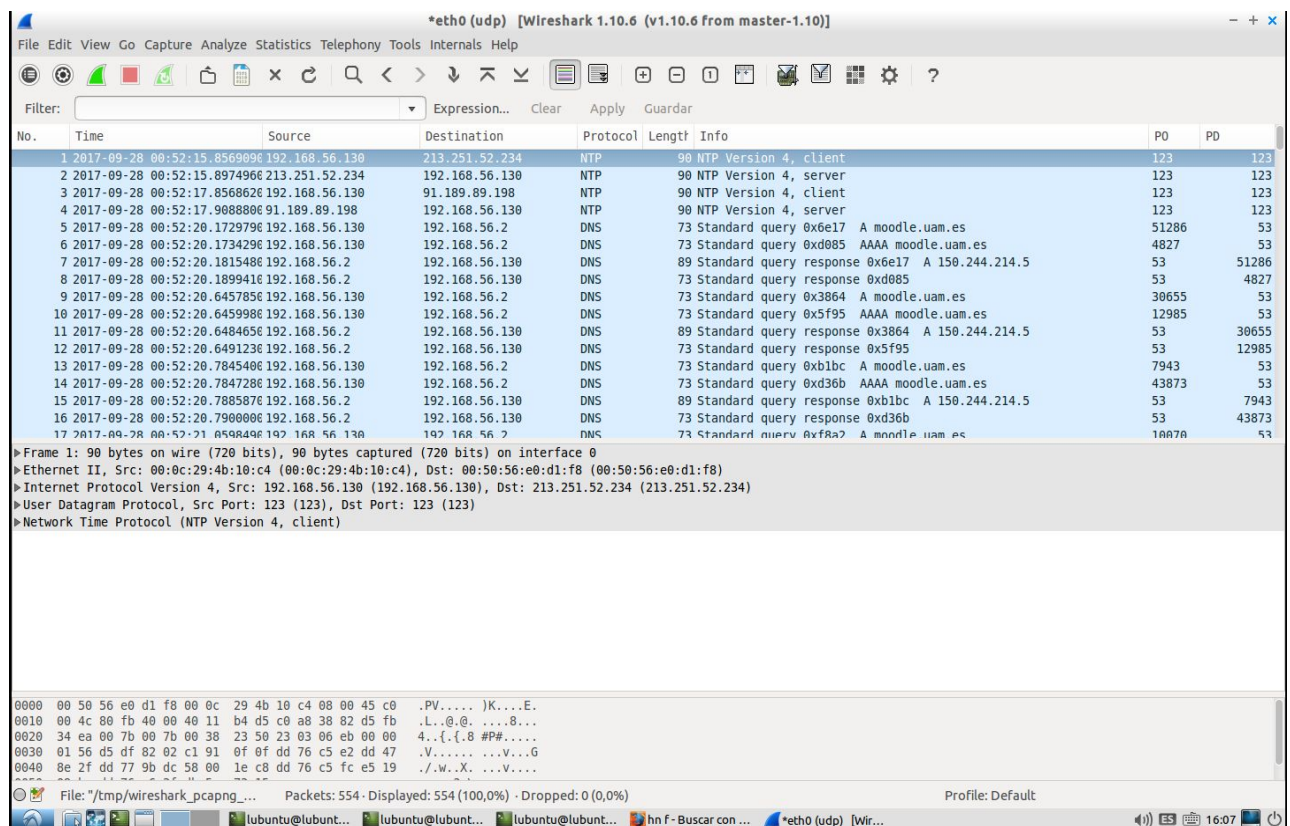
Title: Time		Type: UTC date, as YYYY-MM-DD, and time	Fields:	Occurrence:	OK	Cancel
No.	Time	Source	Destination	Protocol	Length	Info
1	2017-09-27 22:11:45	192.168.1.46	93.184.228.29	TCP	66	53708 → 80 [ACK] Seq=1 Ack=1 Win=266 Len=0 TSval=899184 TSecr=1254078092
2	2017-09-27 22:11:45	93.184.228.29	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 80 → 53708 [ACK] Seq=1 Ack=2 Win=290 Len=0 TSval=1254080596 TSecr=788877 [ETHERNET FRAME CH
3	2017-09-27 22:11:46	192.168.1.46	35.161.203.124	TCP	66	36612 → 443 [ACK] Seq=1 Ack=1 Win=427 Len=0 TSval=809392 TSecr=289189827
4	2017-09-27 22:11:46	35.161.203.124	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 443 → 36612 [ACK] Seq=1 Ack=2 Win=136 Len=0 TSval=289192466 TSecr=788704 [ETHERNET FRAME CH
5	2017-09-27 22:11:47	84:ef:18:db:97:9b	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.1.1? Tell 192.168.1.49
6	2017-09-27 22:11:53	192.168.1.46	52.85.50.181	TCP	66	44898 → 443 [ACK] Seq=1 Ack=1 Win=382 Len=0 TSval=811256 TSecr=3496138879
7	2017-09-27 22:11:53	52.85.50.181	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 443 → 44898 [ACK] Seq=1 Ack=2 Win=128 Len=0 TSval=3496139881 TSecr=788720 [ETHERNET FRAME CH
8	2017-09-27 22:11:53	192.168.1.46	93.184.228.29	TCP	66	53734 → 80 [ACK] Seq=1 Ack=1 Win=241 Len=0 TSval=811352 TSecr=1136799478
9	2017-09-27 22:11:53	93.184.228.29	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 80 → 53734 [ACK] Seq=1 Ack=2 Win=285 Len=0 TSval=1136801981 TSecr=788797 [ETHERNET FRAME CH
10	2017-09-27 22:11:54	192.168.1.46	80.58.61.250	DNS	74	Standard query 0x64b0 A duckduckgo.com
11	2017-09-27 22:11:54	192.168.1.46	80.58.61.254	DNS	74	Standard query 0x64b0 A duckduckgo.com
12	2017-09-27 22:11:54	192.168.1.46	80.58.61.250	DNS	81	Standard query 0xaa97 A images.duckduckgo.com
13	2017-09-27 22:11:54	192.168.1.46	80.58.61.250	DNS	81	Standard query 0xe71f AAAA images.duckduckgo.com
14	2017-09-27 22:11:54	192.168.1.46	80.58.61.250	DNS	80	Standard query 0xa06b A icons.duckduckgo.com
15	2017-09-27 22:11:54	80.58.61.250	192.168.1.46	DNS	272	Standard query response 0x64b0 A duckduckgo.com A 176.34.135.167 A 176.34.155.20 A 54.229.105.203 A 176.34.131.233 A 54.229.110.205
16	2017-09-27 22:11:54	192.168.1.46	176.34.135.167	TCP	74	49542 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=811442 TSecr=0 WS=128
17	2017-09-27 22:11:54	80.58.61.254	192.168.1.46	DNS	170	Standard query response 0x64b0 A duckduckgo.com A 54.229.105.203 A 176.34.135.167 A 46.51.197.89 A 176.34.155.20 A 54.229.110.205
18	2017-09-27 22:11:54	80.58.61.250	192.168.1.46	DNS	198	Standard query response 0xa06b A icons.duckduckgo.com A 54.229.110.205 NS ns0.dnsmadeeasy.com NS ns1.dnsmadeeasy.com NS ns2.dnsmadeeasy.com
19	2017-09-27 22:11:54	192.168.1.46	54.229.110.205	TCP	74	46898 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=811444 TSecr=0 WS=128
20	2017-09-27 22:11:54	192.168.1.46	80.58.61.250	DNS	74	Standard query 0x9456 A duckduckgo.com
21	2017-09-27 22:11:54	192.168.1.46	80.58.61.250	DNS	74	Standard query 0xd9ec AAAA duckduckgo.com
22	2017-09-27 22:11:54	80.58.61.250	192.168.1.46	DNS	272	Standard query response 0x9456 A duckduckgo.com A 54.229.105.203 A 176.34.155.20 A 176.34.135.167 A 54.229.105.92 A 176.34.131.233

Para poner el tiempo en formato Unix hemos tenido que clicar en “View” en el menú superior, luego en “Time Display Format”, y seleccionar “Seconds since 1970-01-01” y obtenemos un escenario como el siguiente (segunda columna):

No.	Time	Source	Destination	Protocol	Length	Info
1	1506550305	192.168.1.46	93.184.228.29	TCP	66	53708 → 80 [ACK] Seq=1 Ack=1 Win=266 Len=0 TSval=899184 TSecr=1254078092
2	1506550305	93.184.228.29	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 80 → 53708 [ACK] Seq=1 Ack=2 Win=290 Len=0 TSval=1254080596 TSecr=788877 [ETHERNET FRAME CH
3	1506550306	192.168.1.46	35.161.203.124	TCP	66	36612 → 443 [ACK] Seq=1 Ack=1 Win=427 Len=0 TSval=809392 TSecr=289189827
4	1506550306	35.161.203.124	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 443 → 36612 [ACK] Seq=1 Ack=2 Win=136 Len=0 TSval=289192466 TSecr=788704 [ETHERNET FRAME CH
5	1506550307	84:ef:18:db:97:9b	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.1.1? Tell 192.168.1.49
6	1506550313	192.168.1.46	52.85.50.181	TCP	66	44898 → 443 [ACK] Seq=1 Ack=1 Win=382 Len=0 TSval=811256 TSecr=3496138879
7	1506550313	52.85.50.181	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 443 → 44898 [ACK] Seq=1 Ack=2 Win=128 Len=0 TSval=3496139881 TSecr=788720 [ETHERNET FRAME CH
8	1506550313	192.168.1.46	93.184.228.29	TCP	66	53734 → 80 [ACK] Seq=1 Ack=1 Win=241 Len=0 TSval=811352 TSecr=1136799478
9	1506550313	93.184.228.29	192.168.1.46	TCP	84	[TCP ACKed unseen segment] 80 → 53734 [ACK] Seq=1 Ack=2 Win=285 Len=0 TSval=1136801981 TSecr=788797 [ETHERNET FRAME CH
10	1506550314	192.168.1.46	80.58.61.250	DNS	74	Standard query 0x64b0 A duckduckgo.com
11	1506550314	192.168.1.46	80.58.61.254	DNS	74	Standard query 0x64b0 A duckduckgo.com
12	1506550314	192.168.1.46	80.58.61.250	DNS	81	Standard query 0xaa97 A images.duckduckgo.com
13	1506550314	192.168.1.46	80.58.61.250	DNS	81	Standard query 0xe71f AAAA images.duckduckgo.com
14	1506550314	192.168.1.46	80.58.61.250	DNS	80	Standard query 0xa06b A icons.duckduckgo.com
15	1506550314	80.58.61.250	192.168.1.46	DNS	272	Standard query response 0x64b0 A duckduckgo.com A 176.34.135.167 A 176.34.155.20 A 54.229.105.203 A 176.34.131.233 A 54.229.110.205
16	1506550314	192.168.1.46	176.34.135.167	TCP	74	49542 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=811442 TSecr=0 WS=128
17	1506550314	80.58.61.254	192.168.1.46	DNS	170	Standard query response 0x64b0 A duckduckgo.com A 54.229.105.203 A 176.34.135.167 A 46.51.197.89 A 176.34.155.20 A 54.229.110.205
18	1506550314	80.58.61.250	192.168.1.46	DNS	198	Standard query response 0xa06b A icons.duckduckgo.com A 54.229.110.205 NS ns0.dnsmadeeasy.com NS ns1.dnsmadeeasy.com NS ns2.dnsmadeeasy.com
19	1506550314	192.168.1.46	54.229.110.205	TCP	74	46898 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=811444 TSecr=0 WS=128
20	1506550314	192.168.1.46	80.58.61.250	DNS	74	Standard query 0x9456 A duckduckgo.com
21	1506550314	192.168.1.46	80.58.61.250	DNS	74	Standard query 0xd9ec AAAA duckduckgo.com
22	1506550314	80.58.61.250	192.168.1.46	DNS	272	Standard query response 0x9456 A duckduckgo.com A 54.229.105.203 A 176.34.155.20 A 176.34.135.167 A 54.229.105.92 A 176.34.131.233
23	1506550314	80.58.61.250	192.168.1.46	DNS	130	Standard query response 0xd9ec AAAA duckduckgo.com SOA ns0.dnsmadeeasy.com
24	1506550314	80.58.61.250	192.168.1.46	DNS	219	Standard query response 0xaa97 A images.duckduckgo.com CNAME icons.duckduckgo.com A 54.229.110.205 NS ns4.dnsmadeeasy.com
25	1506550314	80.58.61.250	192.168.1.46	DNS	157	Standard query response 0xe71f AAAA images.duckduckgo.com CNAME icons.duckduckgo.com SOA ns0.dnsmadeeasy.com
26	1506550314	54.229.110.205	192.168.1.46	TCP	74	443 → 46898 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1452 SACK_PERM=1 TSval=1189312994 TSecr=811444 WS=128
27	1506550314	192.168.1.46	54.229.110.205	TCP	66	46898 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=811453 TSecr=1189312994
28	1506550314	192.168.1.46	54.229.110.205	TLSv1.2	583	Client Hello

- Ejercicio 5:

La captura la iniciamos con la configuración Capture Filter a “udp”, dejando pasar solo paquetes del protocolo “User Data Protocol”. Con esta configuración no se capturaban los paquetes generados por el comando hping3. A continuación vemos el resultado:



Parte 1:

El programa de la práctica fue probado tanto con Valgrind como comprobando las salidas con Wireshark.

A continuación adjuntamos capturas de pantalla en las que mostramos el correcto funcionamiento del programa implementado.

Autores: Lucía Asencio, Rodrigo De Pool

Solicitamos que se mostraran por pantalla 10 bytes.

Observamos que, en efecto, los 10 primeros bytes del paquete 2410 coinciden en la salida del programa con Wireshark.

[illegible]

Generando un archivo .pcap a través de la captura de paquetes en Wireshark, hemos podido comprobar el funcionamiento de nuestro programa al introducir 2 argumentos (siendo este fichero pcap el segundo).

Efectivamente, el número de paquetes analizados coincide con el de Wireshark, así como los 10 primeros Bytes de cada uno. En la imagen adjunta se puede apreciar como esto ocurre con el último paquete capturado.

The image shows a Wireshark window titled 'eth0.ejemplo.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]' and a terminal window titled 'lubuntu@lubuntu: ~/redes1/practica1/partel/codigo'.

The Wireshark window displays a list of captured packets. The 'Filter' field is empty. The packet list shows various protocols including DNS, HTTP, and TCP. The packet details pane on the right shows the selected packet (496) and its corresponding hex and ASCII data.

The terminal window shows the output of a program, displaying the hex and ASCII data for the selected packet (496) from the Wireshark packet list.

No.	Time	Source	Destination	Protocol	Length
469	2017-09-28 16:40:41.336286	192.168.56.2	192.168.56.130	DNS	90
470	2017-09-28 16:40:41.336930	192.168.56.2	192.168.56.130	DNS	90
471	2017-09-28 16:40:41.337108	192.168.56.130	192.168.56.2	DNS	102
472	2017-09-28 16:40:41.337273	192.168.56.130	192.168.56.2	DNS	102
473	2017-09-28 16:40:41.358029	150.244.214.237	192.168.56.130	HTTP	448
474	2017-09-28 16:40:41.358045	192.168.56.130	150.244.214.237	TCP	54
475	2017-09-28 16:40:41.360510	192.168.56.130	192.168.56.2	DNS	70
476	2017-09-28 16:40:41.360621	192.168.56.130	192.168.56.2	DNS	70
477	2017-09-28 16:40:41.361166	192.168.56.130	150.244.214.237	HTTP	856
478	2017-09-28 16:40:41.361279	150.244.214.237	192.168.56.130	TCP	60
479	2017-09-28 16:40:41.361372	192.168.56.130	150.244.214.237	HTTP	856
480	2017-09-28 16:40:41.361476	150.244.214.237	192.168.56.130	TCP	60
481	2017-09-28 16:40:41.364108	192.168.56.2	192.168.56.130	DNS	86
482	2017-09-28 16:40:41.372082	192.168.56.2	192.168.56.130	DNS	102
483	2017-09-28 16:40:41.372098	192.168.56.2	192.168.56.130	DNS	102
484	2017-09-28 16:40:41.372381	192.168.56.130	192.168.56.2	DNS	90
485	2017-09-28 16:40:41.372456	192.168.56.130	192.168.56.2	DNS	90
486	2017-09-28 16:40:41.379561	192.168.56.2	192.168.56.130	DNS	70
487	2017-09-28 16:40:41.382020	192.168.56.2	192.168.56.130	DNS	90
488	2017-09-28 16:40:41.382031	192.168.56.2	192.168.56.130	DNS	90
489	2017-09-28 16:40:41.382169	192.168.56.130	192.168.56.2	DNS	102
490	2017-09-28 16:40:41.382293	192.168.56.130	192.168.56.2	DNS	102
491	2017-09-28 16:40:41.382653	150.244.214.237	192.168.56.130	HTTP	244
492	2017-09-28 16:40:41.382664	192.168.56.130	150.244.214.237	TCP	54
493	2017-09-28 16:40:41.383449	150.244.214.237	192.168.56.130	HTTP	244
494	2017-09-28 16:40:41.391271	192.168.56.2	192.168.56.130	DNS	102
495	2017-09-28 16:40:41.391284	192.168.56.2	192.168.56.130	DNS	102
496	2017-09-28 16:40:41.421018	192.168.56.130	150.244.214.237	TCP	54

Packet 496 details:

- Ethernet II, Src: 00:0c:29:4b:10:c4 (00:0c:29:4b:10:c4), Dst: 00:50:56:e0:d1:f8 (00:50:56:e0:d1:f8)
- Internet Protocol Version 4, Src: 192.168.56.130 (192.168.56.130), Dst: 150.244.214.237 (150.244.214.237)
- Transmission Control Protocol, Src Port: 55736 (55736), Dst Port: 80 (80), Seq: 0, Len: 0

Packet 496 hex data:

```
0000 00 50 56 e0 d1 f8 00 0c 29 4b 10 c4 08 00 45 00 .PV.... )K....E.  
0010 00 3c ca 5b 40 00 40 06 09 54 c0 a8 38 82 96 f4 .<.[@. .T..8...  
0020 d6 ed d9 b8 00 50 1c c9 7b cd 00 00 00 00 a0 02 ....P.. {.....  
0030 72 10 4a 9e 00 00 02 04 05 b4 04 02 08 0a 00 0f r.J.....
```

Terminal output:

```
496 paquetes fueron leídos.  
lubuntu@lubuntu:~/redes1/practical/partel/codigo$
```