EJERCICIOS DE CAPTURA DE TRÁFICO

Junco de las Heras y Marta Vaquerizo

Índice

1. Apartado 1

Abrimos una consola y ejecutamos sudo wireshark-gtk.
Se abre Wireshark y empezamos a capturar tráfico con el interfaz ens33.
Luego en la terminal lanzamos el comando sudo hping3 -S -p 80 www.uam.es con Wireshark capturando los paquetes.

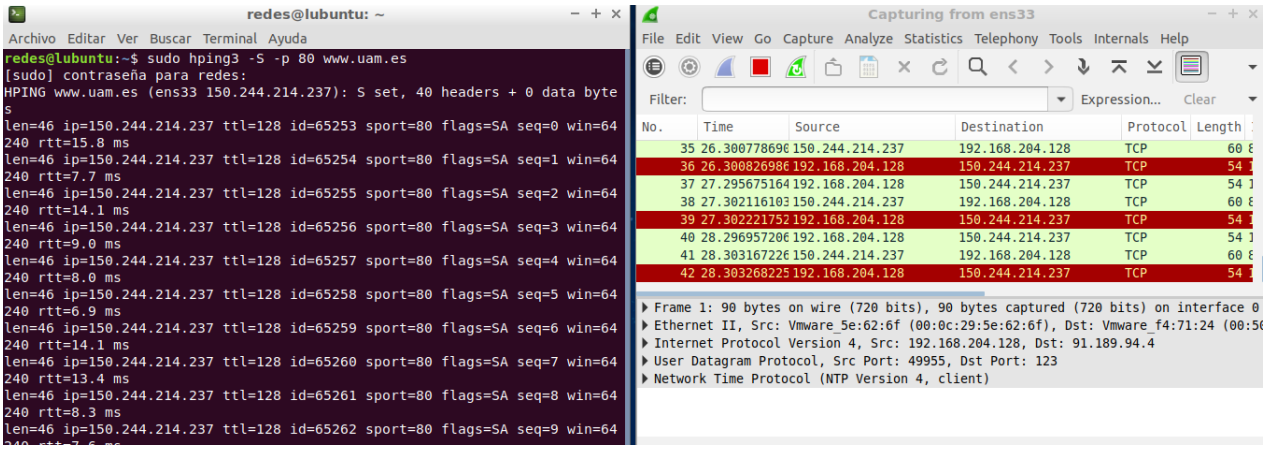


Figura 1: Ordenando por la columna PO.

Guardamos los paquetes en un fichero y reiniciamos Wireshark.
Añadimos las columnas PO (Src port (unresolved)) y PD (Dst port (unresolved)), y ordenamos las entradas por PO. Nótese que compara los datos de PO como si fueran cadenas de texto, y no como si fueran números, así que el resultado 45 iría antes que el 5.

No.	Time	Source	Destination	Protocol	Length	Info	PO	PD
37	27.295675164	192.168.204.128	150.244.214.237	TCP	54	1560 → 80 [SYN] Seq=0 Win=512 Len=0	1560	80
39	27.302221752	192.168.204.128	150.244.214.237	TCP	54	1560 → 80 [RST] Seq=1 Win=0 Len=0	1560	80
40	28.296957206	192.168.204.128	150.244.214.237	TCP	54	1561 → 80 [SYN] Seq=0 Win=512 Len=0	1561	80
42	28.303268225	192.168.204.128	150.244.214.237	TCP	54	1561 → 80 [RST] Seq=1 Win=0 Len=0	1561	80
43	64.249838367	192.168.204.128	91.189.94.4	NTP	90	NTP Version 4, client	36555	123
5	17.240313013	192.168.204.128	192.168.204.2	DNS	81	Standard query 0x8db3 A www.uam.es OPT	43091	53
1	0.000000000	192.168.204.128	91.189.94.4	NTP	90	NTP Version 4, client	49955	123
6	17.244715674	192.168.204.2	192.168.204.128	DNS	97	Standard query response 0x8db3 A www.uam.es A 150.244.214.237 OF	53	43091
8	17.294376334	150.244.214.237	192.168.204.128	TCP	60	80 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1550
11	18.293732369	150.244.214.237	192.168.204.128	TCP	60	80 → 1551 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1551
14	19.294743501	150.244.214.237	192.168.204.128	TCP	60	80 → 1552 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1552
17	20.295350573	150.244.214.237	192.168.204.128	TCP	60	80 → 1553 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1553
20	21.296863448	150.244.214.237	192.168.204.128	TCP	60	80 → 1554 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1554
23	22.297368925	150.244.214.237	192.168.204.128	TCP	60	80 → 1555 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1555
26	23.298422105	150.244.214.237	192.168.204.128	TCP	60	80 → 1556 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1556
29	24.299599816	150.244.214.237	192.168.204.128	TCP	60	80 → 1557 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1557
32	25.300226299	150.244.214.237	192.168.204.128	TCP	60	80 → 1558 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1558
35	26.300778690	150.244.214.237	192.168.204.128	TCP	60	80 → 1559 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	80	1559

Figura 2: Capturando paquetes creados por el comando hping3.

2. Apartado 2

2.1.

El filtro que se ha realizado para que se muestren los paquetes tipo IP con una longitud de paquete mayor que 1000 B es:

$$ip\ and\ ip.len > 1000$$

Guardamos la captura en practica1.pcap.

2.2.

Para guardar los paquetes filtrados se exportan en formato pcap.

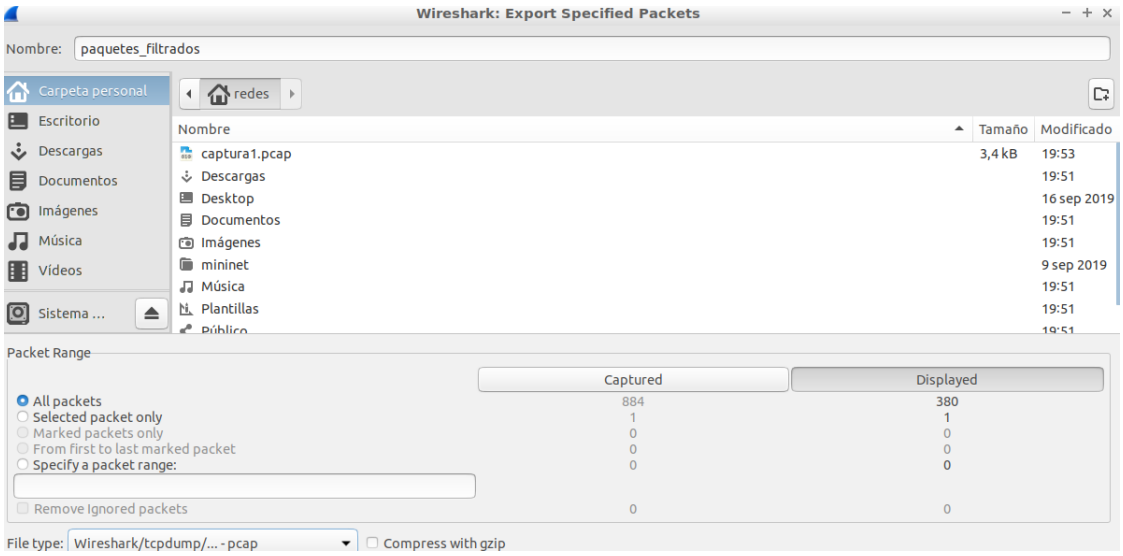


Figura 3: Exportar los paquetes mostrados.

2.3.

La length del paquete IP primero es de 1514, mientras que la length del protocolo IP primero es de 1500, lo que nos dice que hay unos 14 bits de más en el paquete, los que le corresponden a la cabecera del protocolo Ethernet.

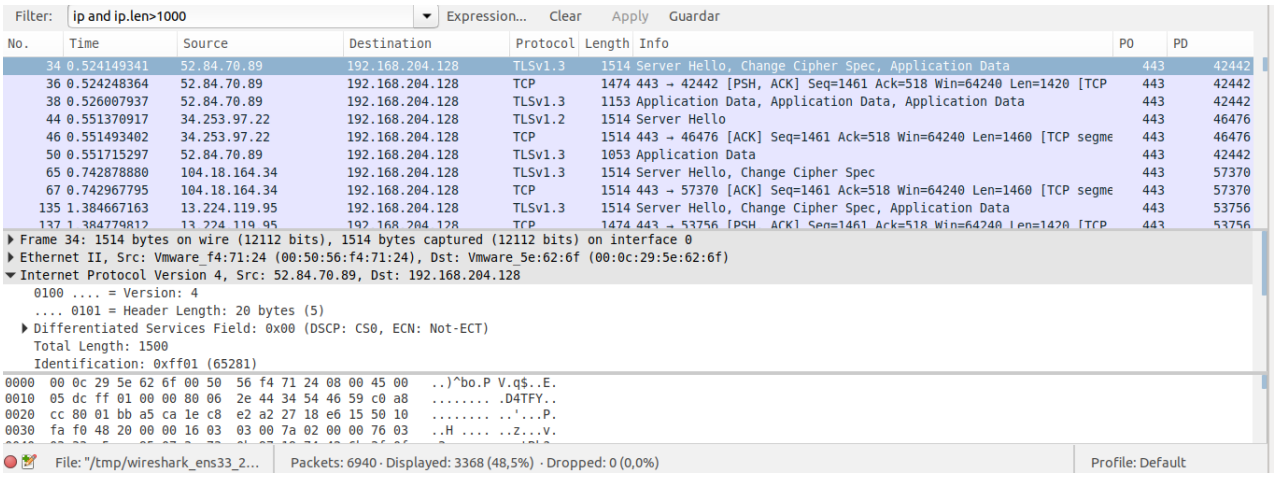


Figura 4: Paquetes filtrados.

3. Apartado 3

Para añadir la columna interarrival se han seguido los siguientes pasos: primero vamos al menú *'Edit→Preferences'*, y en la ventana que aparece se selecciona la opción de *'User Interface→ Columns'*. En la parte inferior de esta ventana, apretamos al botón de *'+Añadir'* y en el campo *'Field Type'* se pone **'delta time'**.

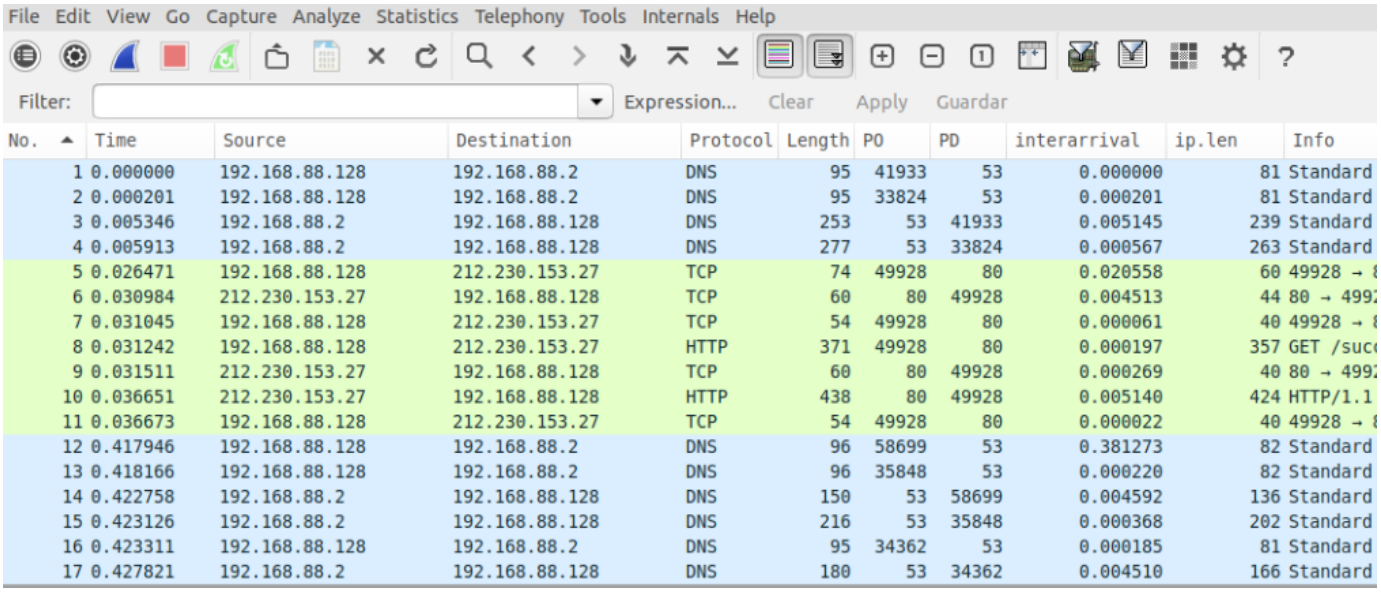
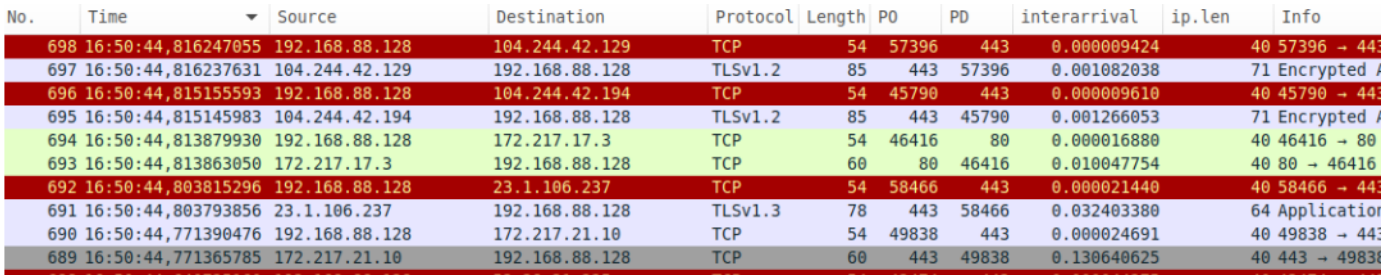


Figura 5: Captura con la columna 'interarrival'.

4. Apartado 4

Para cambiar el formato de los datos de la columna Time, hay que realizar los pasos del apartado anterior hasta la selección de *'User Interface→ Columns'*. Una vez en esta ventana, pinchamos sobre la fila de *'Time'* y cambiamos el *'Field Type'* de **'time'** a **'absolute time'**.

Este último formato contiene la hora y la resolución en segundos, como se puede ver en la siguiente imagen.

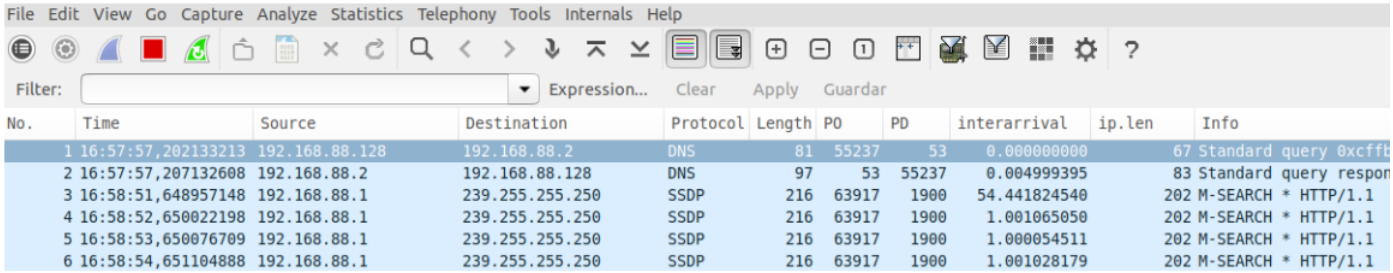


No.	Time	Source	Destination	Protocol	Length	PO	PD	interarrival	ip.len	Info
698	16:50:44,816247055	192.168.88.128	104.244.42.129	TCP	54	57396	443	0.000009424	40	57396 → 443
697	16:50:44,816237631	104.244.42.129	192.168.88.128	TLSv1.2	85	443	57396	0.001082038	71	Encrypted A
696	16:50:44,815155593	192.168.88.128	104.244.42.194	TCP	54	45790	443	0.000009610	40	45790 → 443
695	16:50:44,815145983	104.244.42.194	192.168.88.128	TLSv1.2	85	443	45790	0.001266053	71	Encrypted A
694	16:50:44,813879930	192.168.88.128	172.217.17.3	TCP	54	46416	80	0.000016880	40	46416 → 80
693	16:50:44,813863050	172.217.17.3	192.168.88.128	TCP	60	80	46416	0.010047754	40	80 → 46416
692	16:50:44,803815296	192.168.88.128	23.1.106.237	TCP	54	58466	443	0.000021440	40	58466 → 443
691	16:50:44,803793856	23.1.106.237	192.168.88.128	TLSv1.3	78	443	58466	0.032403380	64	Application
690	16:50:44,771390476	192.168.88.128	172.217.21.10	TCP	54	49838	443	0.000024691	40	49838 → 443
689	16:50:44,771365785	172.217.21.10	192.168.88.128	TCP	60	443	49838	0.130640625	40	443 → 49838

Figura 6: Captura con la fecha y la resolución en segundos.

5. Apartado 5

Para que le tráfico de solo capture los paquetes de tipo UDP, antes de darle a 'Start', en el menú *'Capture Options'*, en el campo de *'Capture Filter'* ponemos 'UDP only'.
La siguiente captura refleja el resultado de este apartado.



No.	Time	Source	Destination	Protocol	Length	PO	PD	interarrival	ip.len	Info
1	16:57:57,202133213	192.168.88.128	192.168.88.2	DNS	81	55237	53	0.000000000	67	Standard query 0xcffb
2	16:57:57,207132608	192.168.88.2	192.168.88.128	DNS	97	53	55237	0.004999395	83	Standard query respon
3	16:58:51,648957148	192.168.88.1	239.255.255.250	SSDP	216	63917	1900	54.441824540	202	M-SEARCH * HTTP/1.1
4	16:58:52,650022198	192.168.88.1	239.255.255.250	SSDP	216	63917	1900	1.001065050	202	M-SEARCH * HTTP/1.1
5	16:58:53,650076709	192.168.88.1	239.255.255.250	SSDP	216	63917	1900	1.000054511	202	M-SEARCH * HTTP/1.1
6	16:58:54,651104888	192.168.88.1	239.255.255.250	SSDP	216	63917	1900	1.001028179	202	M-SEARCH * HTTP/1.1

Figura 7: Captura con paquetes de tipo UDP.