Redes de Comunicaciones I, Práctica 1: Introducción a Wireshark

Ana Calzada, Leandro García y Fabián Gutiérrez (Grupo 1302_08)

10 de octubre de 2020

Ejercicio 1

Ejecutamos Wireshark y seleccionamos la interfaz *ens33*, que representa una tarjeta de red Ethernet. Configuramos las opciones de visualización para facilitar el posterior análisis y comenzamos la captura de tráfico. Abrimos una consola y ejecutamos el comando `sudo hping3 -S -p 80 www.uam.es`. Al poco tiempo, detenemos la captura de trafico y analizamos los datos obtenidos. Guardamos la traza en un fichero con *Save*. A continuación, ordenamos los paquetes respecto a la columna PO, es decir, con respecto a su puerto de origen, con sentido desendente, y buscamos los paquetes para los que este campo tenga el valor 53. Como podemos observar en la figura 1, aparece un único paquete con este valor.

Ejercicio 2

1. Para visualizar únicamente los paquetes de tipo IP de tamaño mayor a 1000 B basta con utilizar el filtro visual `ip.len>1000`.

2. En lugar de hacer *Save* como en el ejercicio 1, es necesario utilizar *File >Export Specified Packets...* y seleccionar *Displayed*, como se indica en la figura 2.

3. De los primeros cuatro paquetes, el segundo y el tercero tienen una longitud de 3438 B, pero su campo *length* del protocolo IP reporta 3424 B. Similarmente, el primero, el cuarto y el quinto tienen una longitud de 3446 B, 2974 B y 1113 B, pero los protocolos IP reportan 3432 B, 2960 B y 1099 B, respectivamente. Es fácil ver que en todos estos casos la diferencia entre ambos valores es de 14 B, los correspondientes a la cabecera Ethernet.

No.	Time	Source	Destination	Protocol	Length	Interarrival	PO ▾	PD	Info
42	1601900233.088072	150.244.214.237	192.168.36.128	TCP	60	0.040737	80	1833	80 → 1833 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
39	1601900232.066524	150.244.214.237	192.168.36.128	TCP	60	0.022350	80	1832	80 → 1832 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
36	1601900231.070862	150.244.214.237	192.168.36.128	TCP	60	0.028431	80	1831	80 → 1831 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
33	1601900230.064100	150.244.214.237	192.168.36.128	TCP	60	0.024404	80	1830	80 → 1830 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
29	1601900229.061857	150.244.214.237	192.168.36.128	TCP	60	0.022951	80	1829	80 → 1829 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
23	1601900228.057896	150.244.214.237	192.168.36.128	TCP	60	0.021778	80	1828	80 → 1828 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
19	1601900227.058667	150.244.214.237	192.168.36.128	TCP	60	0.022985	80	1827	80 → 1827 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
15	1601900226.055051	150.244.214.237	192.168.36.128	TCP	60	0.022580	80	1826	80 → 1826 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
12	1601900225.119411	150.244.214.237	192.168.36.128	TCP	60	0.088009	80	1825	80 → 1825 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
9	1601900224.066421	150.244.214.237	192.168.36.128	TCP	60	0.037286	80	1824	80 → 1824 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
6	1601900223.050746	150.244.214.237	192.168.36.128	TCP	60	0.021717	80	1823	80 → 1823 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
4	1601900222.986574	192.168.36.2	192.168.36.128	DNS	97	0.000187	53	34067	Standard query response 0xa6dd A www.uam.es A 150.
31	1601900229.971831	192.168.36.1	239.255.255.250	SSDP	216	0.909921	52188	1900	M-SEARCH * HTTP/1.1
27	1601900228.967737	192.168.36.1	239.255.255.250	SSDP	216	0.800438	52188	1900	M-SEARCH * HTTP/1.1
21	1601900227.967737	192.168.36.1	239.255.255.250	SSDP	216	0.908995	52188	1900	M-SEARCH * HTTP/1.1
17	1601900226.964689	192.168.36.1	239.255.255.250	SSDP	216	0.909611	52188	1900	M-SEARCH * HTTP/1.1
1	1601900222.962622	192.168.36.128	192.168.36.2	DNS	81	0.000000	34067	53	Standard query 0xa6dd A www.uam.es OPT
43	1601900233.088125	192.168.36.128	150.244.214.237	TCP	54	0.000053	1833	80	1833 → 80 [RST] Seq=1 Win=0 Len=0
41	1601900233.047335	192.168.36.128	150.244.214.237	TCP	54	0.980750	1833	80	1833 → 80 [SYN] Seq=0 Win=512 Len=0
40	1601900232.066585	192.168.36.128	150.244.214.237	TCP	54	0.000061	1832	80	1832 → 80 [RST] Seq=1 Win=0 Len=0

Figura 1: Paquetes ordenados según su puerto de origen en el ejercicio 1

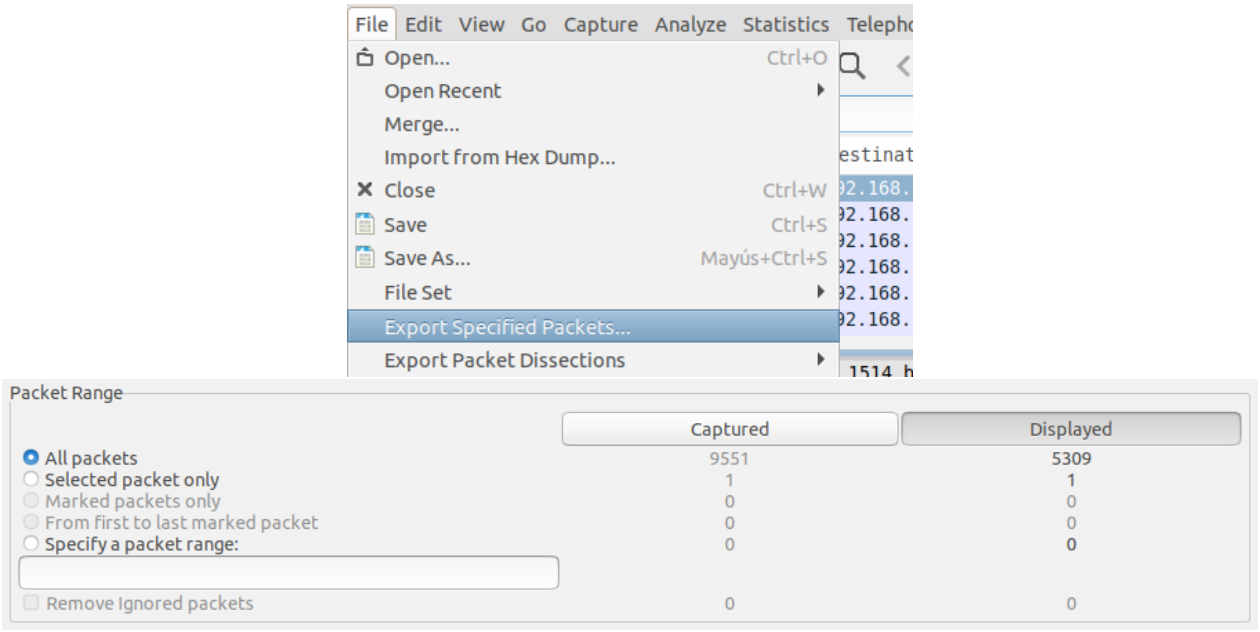
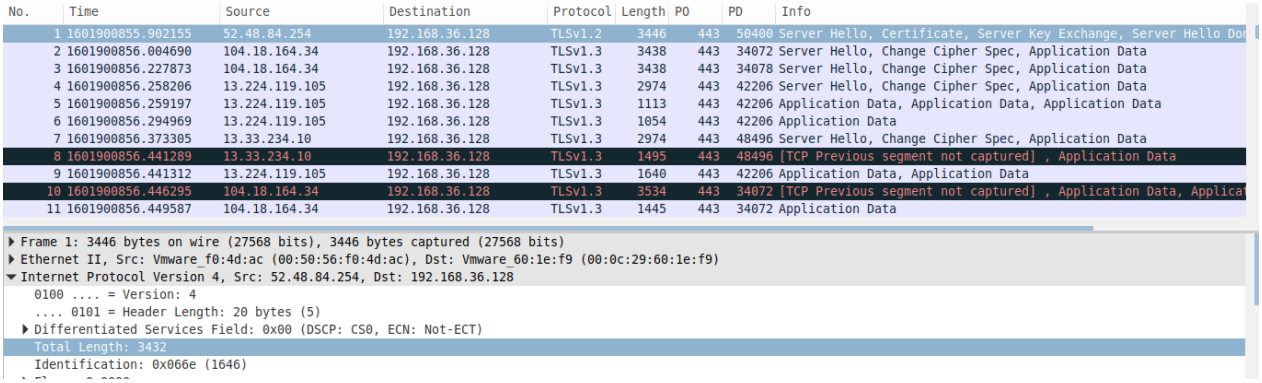
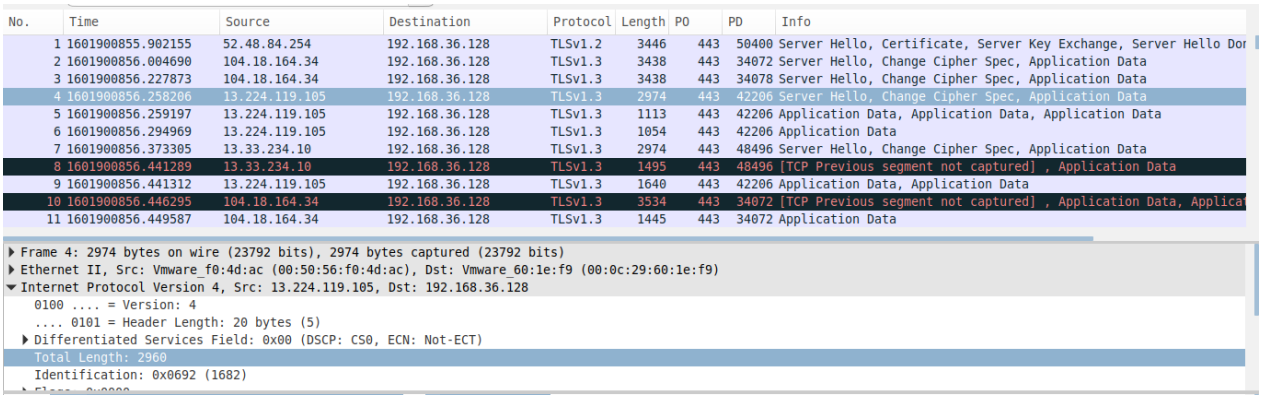


Figura 2: Pasos para guardar los paquetes filtrados en el ejercicio 2

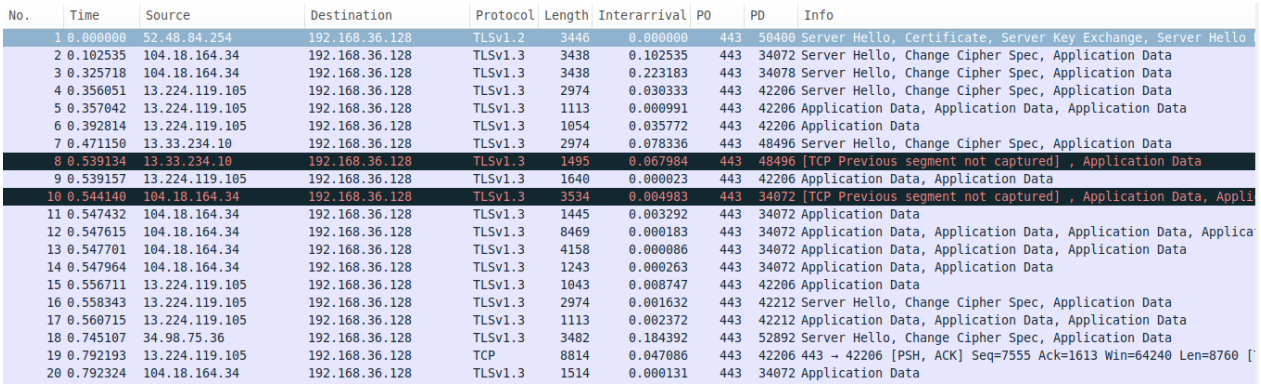


(a) Primer paquete



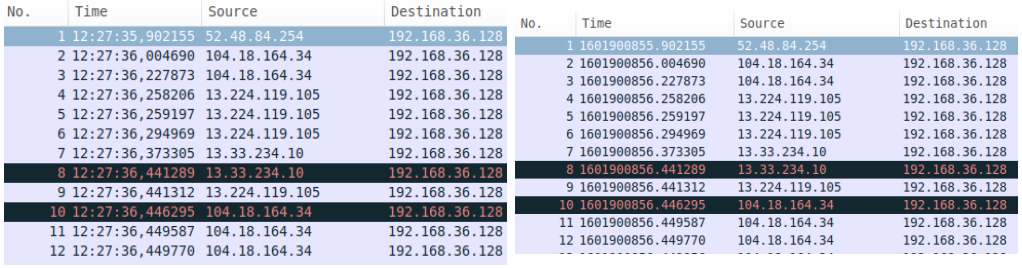
(b) Cuarto paquete

Figura 3: Paquetes capturados en el ejercicio 2, con su longitud y *length* del protocolo IP



No.	Time	Source	Destination	Protocol	Length	Interarrival	PO	PD	Info
1	0.000000	52.48.84.254	192.168.36.128	TLSv1.2	3446	0.000000	443	50400	Server Hello, Certificate, Server Key Exchange, Server Hello
2	0.102535	104.18.164.34	192.168.36.128	TLSv1.3	3438	0.102535	443	34072	Server Hello, Change Cipher Spec, Application Data
3	0.325718	104.18.164.34	192.168.36.128	TLSv1.3	3438	0.223183	443	34078	Server Hello, Change Cipher Spec, Application Data
4	0.356051	13.224.119.105	192.168.36.128	TLSv1.3	2974	0.030333	443	42206	Server Hello, Change Cipher Spec, Application Data
5	0.357042	13.224.119.105	192.168.36.128	TLSv1.3	1113	0.000991	443	42206	Application Data, Application Data, Application Data
6	0.392814	13.224.119.105	192.168.36.128	TLSv1.3	1054	0.035772	443	42206	Application Data
7	0.471150	13.33.234.10	192.168.36.128	TLSv1.3	2974	0.078336	443	48496	Server Hello, Change Cipher Spec, Application Data
8	0.539134	13.33.234.10	192.168.36.128	TLSv1.3	1495	0.067984	443	48496	[TCP Previous segment not captured] , Application Data
9	0.539157	13.224.119.105	192.168.36.128	TLSv1.3	1640	0.000023	443	42206	Application Data, Application Data
10	0.544140	104.18.164.34	192.168.36.128	TLSv1.3	3534	0.004983	443	34072	[TCP Previous segment not captured] , Application Data, Appli
11	0.547432	104.18.164.34	192.168.36.128	TLSv1.3	1445	0.003292	443	34072	Application Data
12	0.547615	104.18.164.34	192.168.36.128	TLSv1.3	8469	0.000183	443	34072	Application Data, Application Data, Application Data, Applica
13	0.547701	104.18.164.34	192.168.36.128	TLSv1.3	4158	0.000086	443	34072	Application Data, Application Data, Application Data
14	0.547964	104.18.164.34	192.168.36.128	TLSv1.3	1243	0.000263	443	34072	Application Data, Application Data
15	0.556711	13.224.119.105	192.168.36.128	TLSv1.3	1043	0.008747	443	42206	Application Data
16	0.558343	13.224.119.105	192.168.36.128	TLSv1.3	2974	0.001632	443	42212	Server Hello, Change Cipher Spec, Application Data
17	0.560715	13.224.119.105	192.168.36.128	TLSv1.3	1113	0.002372	443	42212	Application Data, Application Data, Application Data
18	0.745107	34.98.75.36	192.168.36.128	TLSv1.3	3482	0.184392	443	52892	Server Hello, Change Cipher Spec, Application Data
19	0.792193	13.224.119.105	192.168.36.128	TCP	8814	0.047086	443	42206	443 → 42206 [PSH, ACK] Seq=7555 Ack=1613 Win=64240 Len=8760 [
20	0.792324	104.18.164.34	192.168.36.128	TLSv1.3	1514	0.000131	443	34072	Application Data

Figura 4: Visualización de la captura tras añadir la columna *interarrival* para el ejercicio 3



No.	Time	Source	Destination
1	12:27:35,902155	52.48.84.254	192.168.36.128
2	12:27:36,004690	104.18.164.34	192.168.36.128
3	12:27:36,227873	104.18.164.34	192.168.36.128
4	12:27:36,258206	13.224.119.105	192.168.36.128
5	12:27:36,259197	13.224.119.105	192.168.36.128
6	12:27:36,294969	13.224.119.105	192.168.36.128
7	12:27:36,373305	13.33.234.10	192.168.36.128
8	12:27:36,441289	13.33.234.10	192.168.36.128
9	12:27:36,441312	13.224.119.105	192.168.36.128
10	12:27:36,446295	104.18.164.34	192.168.36.128
11	12:27:36,449587	104.18.164.34	192.168.36.128
12	12:27:36,449770	104.18.164.34	192.168.36.128

(a) Para humanos

No.	Time	Source	Destination
1	1601900855.902155	52.48.84.254	192.168.36.128
2	1601900856.004690	104.18.164.34	192.168.36.128
3	1601900856.227873	104.18.164.34	192.168.36.128
4	1601900856.258206	13.224.119.105	192.168.36.128
5	1601900856.259197	13.224.119.105	192.168.36.128
6	1601900856.294969	13.224.119.105	192.168.36.128
7	1601900856.373305	13.33.234.10	192.168.36.128
8	1601900856.441289	13.33.234.10	192.168.36.128
9	1601900856.441312	13.224.119.105	192.168.36.128
10	1601900856.446295	104.18.164.34	192.168.36.128
11	1601900856.449587	104.18.164.34	192.168.36.128
12	1601900856.449770	104.18.164.34	192.168.36.128

(b) UNIX en segundos

Figura 5: Tiempo en distintos formatos para el ejercicio 4

Ejercicio 3

Primero entramos en el menú *Edit >Preferences*, dentro del cual accedemos a la opción *User Interface >Columns*. Luego hacemos clic en el botón *Añadir* para introducir una nueva columna en la lista. Seleccionamos como tipo de campo *Delta time* para mostrar el tiempo entre la llegada de dos paquetes consecutivos (o *Delta time displayed* para hacerlo considerando exclusivamente los paquetes mostrados). Para cambiar el nombre basta con seleccionar la columna en la lista, hacer clic en el título y escribir *interarrival*. Finalmente, hacemos clic en *Aplicar* y en *Aceptar*, con lo que salimos del menú. Si no se muestra la nueva columna es recomendable volver a acceder en el menú y comprobar que la columna está marcada en la lista, porque suele no estarlo de primeras.

Una forma alternativa de hacerlo sería acceder en el panel central a la pestaña *Frame*, hacer clic derecho en el campo *Time delta from previous captured frame* (literalmente la información que queremos añadir) y seleccionar *Apply as Column*. Se creará una columna con el mismo nombre; para cambiarlo basta con hacer clic derecho en el título y seleccionar *Edit Column Details...*, con lo que aparece un menú donde podemos editar el título.

Ejercicio 4

Primero pulsamos en el menú *View >Time Display Format*, donde se despliega una lista con los distintos formatos en los que se puede mostrar el tiempo. Si queremos mostrarlo en formato para humanos, deberemos seleccionar *Time of Day* o bien *UTC Time of Day*. Si queremos mostrarlo en tiempo Unix con resolución de segundos, deberemos seleccionar *Seconds since Epoch*.

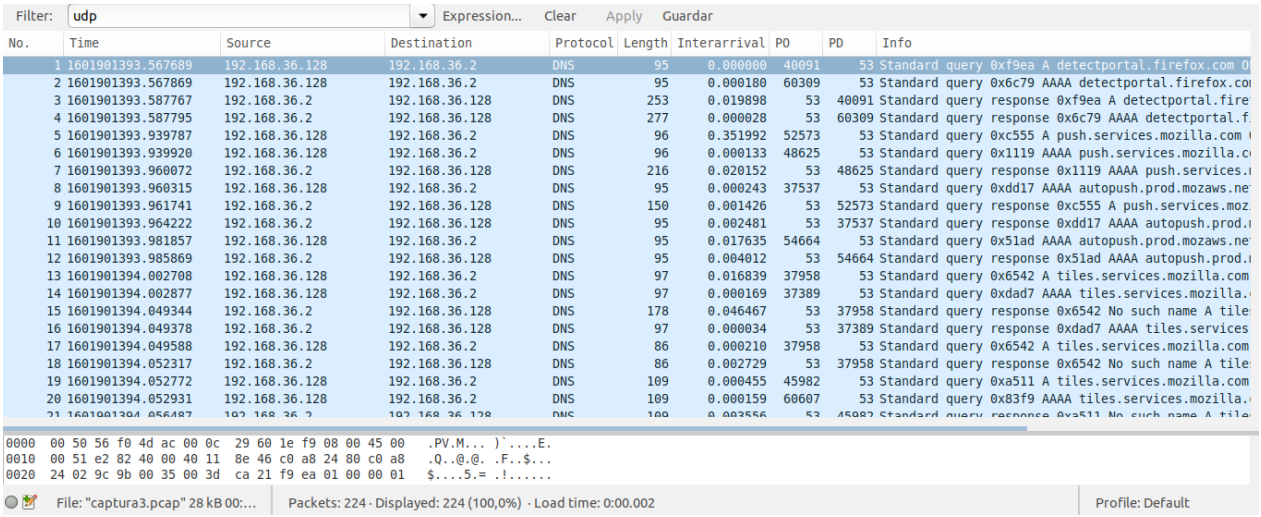


Figura 6: Paquetes UDP capturados en el ejercicio 5

Ejercicio 5

Antes de iniciar la captura de tráfico ha de configurarse el filtro de captura. En la ventana de configuración para la captura de tráfico, hacemos clic en el botón *Capture filter* y seleccionamos la opción *UDP only*. Una vez aplicado el filtro, iniciamos la captura y generamos tráfico con el comando de la terminal utilizado anteriormente y visualizando páginas web. Tras unos segundos detenemos la captura y procedemos a analizar el tráfico. Aplicando el filtro de visualización `udp` observamos en la parte inferior de Wireshark que el 100 % de los paquetes está siendo mostrado (como se observa en la figura 6), esto es, todos los paquetes capturados son UDP.