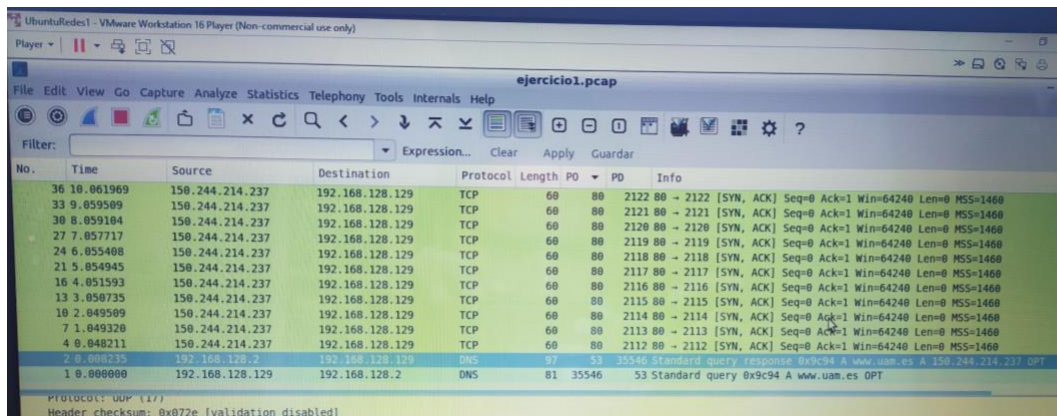


Práctica 1. Introducción a Wireshark para el análisis de trazas.

-Ejercicios de captura de tráfico

1-

Para realizar este ejercicio simplemente hemos seguido las instrucciones. Primeramente abrimos una shell en la que luego escribiríamos el comando solicitado. Después, abrimos otra; desde la cual ejecutamos *wireshark* para poder capturar señales en vivo. Seguimos las instrucciones y vemos como en *wireshark* nos han aparecido cierta cantidad de señales. Lo hemos examinado un poco (para quedarnos con algunos datos para así comprobar posteriormente que se guardaba bien) y hemos guardado el archivo con extensión .pcap. Hemos cerrado *wireshark*, y lo hemos abierto después nuevamente; pero esta vez desde el escritorio (ya que abriremos una traza ya almacenada). Abrimos el archivo que acabábamos de guardar y comprobamos que era igual. Después de ello, teníamos que filtrar la visualización de los paquetes capturados. No supimos cómo ordenar los paquetes basándonos en un campo, pero como realmente lo que necesitábamos saber era el número de paquetes con el campo PO con valor 53 aplicamos el siguiente filtro: **udp.srcport == 53**. Con el pudimos ver que paquetes tenían PO == 53, que era solamente uno.



2-

El filtro utilizado: **ip and frame.cap_len > 1000**

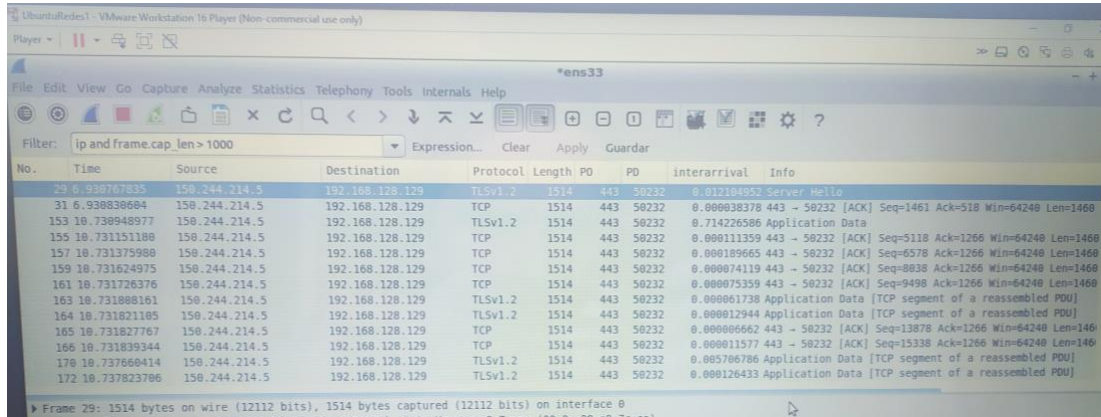
No hemos podido guardar los paquetes filtrados. Solamente podemos conseguir el archivo con los paquetes filtrados si utilizamos al capturar los paquetes un filtro de captura.

Hemos observado que el tamaño del paquete es mayor que el del campo length del protocolo ip. El tamaño total supera por 14 bytes al del protocolo. Estos 14 bytes son los que ocupan la cabecera.

3-

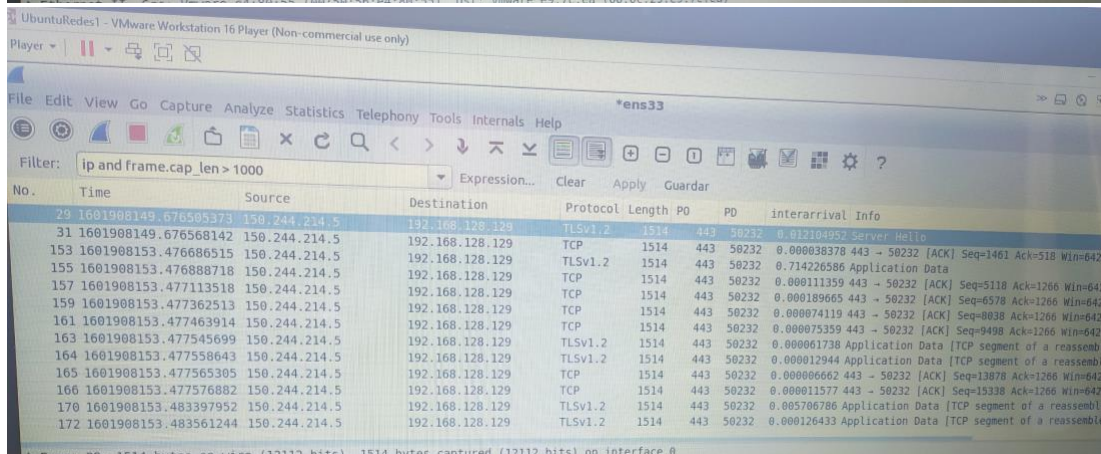
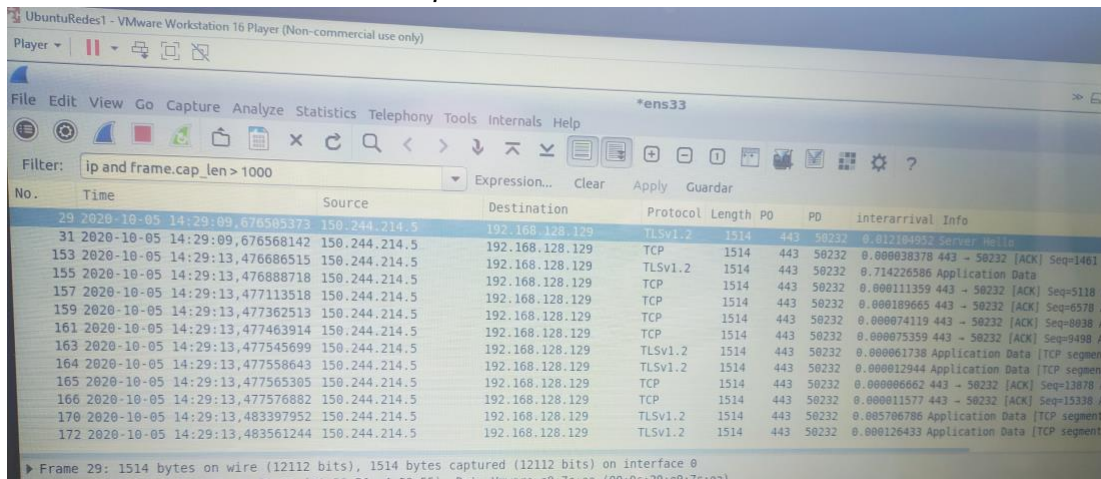
Para añadir el campo interarrival nos hemos ido arriba a la izquierda y hemos hecho click en *Edit*. Se ha desplegado un menú en el cual nos hemos ido abajo del todo para clickar en *Preferences*. Nos ha surgido una nueva ventana con varios apartados a la izquierda, donde

hemos hecho click en *Columns*. Hemos visto que a la derecha nos salen muchas opciones para elegir de qué tipo de dato queremos que sea nuestra nueva columna. Aquí hemos elegido *Delta Time*. Después hemos personalizado el nombre poniendo *Interarrival*. Aquí ha habido un problema porque nos ha dado un problema de permisos y no nos dejaba añadir la columna. Hemos pensado que ha sido por abrir *wireshark* desde el escritorio. Hemos abierto el programa desde la terminal con *sudo wireshark-gtk* y no hemos tenido problema para hacer lo descrito anteriormente.



4-

Para cambiar el formato del campo *Time*, arriba a la izquierda hacemos click en *View*. Tras esto, nos aparece un menú desplegable en el cual debemos seleccionar *Time Display Format*. Se nos desplegará otro menú anexo y veremos varias opciones. Para el tiempo en formato para humanos seleccionamos *Date and Time of Day*. Y para el tiempo Unix seleccionamos *Seconds Since Epoch*.



5-

Hemos hecho uso de un filtro de captura (**udp**) en las opciones de captura para solamente visualizar paquetes UDP. Hemos iniciado la captura, y hemos abierto el explorador web para hacer un par de consultas a la vez que en una shell ejecutábamos el comando `sudo hping3 -S -p 80 www.uam.es`. Tras esto, hemos comprobado que todos los paquetes capturados eran UDP, simplemente viéndolo, y también aplicando el filtro de visualización de udp y viendo que la entrada no cambiaba.

No.	Time	Source	Destination	Protocol	Length	PO	PD	Interarrival	Info
1	1601908894.631265764	192.168.128.129	192.168.128.2	DNS	86	47339	53	0.000000000	Standard query 0x128d A docs.google.com OPT
2	1601908894.631599462	192.168.128.129	192.168.128.2	DNS	86	52068	53	0.000233606	Standard query 0x351d AAAA docs.google.com OPT
3	1601908894.637986739	192.168.128.2	192.168.128.129	DNS	102	53	47339	0.006387277	Standard query response 0x128d A docs.google.com
4	1601908894.638046419	192.168.128.2	192.168.128.129	DNS	114	53	52068	0.000059680	Standard query response 0x351d AAAA docs.google.com
5	1601908896.767360531	192.168.128.129	192.168.128.2	DNS	86	53461	53	2.129314112	Standard query 0xc8f6 A play.google.com OPT
6	1601908896.767588587	192.168.128.129	192.168.128.2	DNS	86	56547	53	0.000228056	Standard query 0x8df7 AAAA play.google.com OPT
7	1601908896.772400175	192.168.128.2	192.168.128.129	DNS	102	53	53461	0.004811588	Standard query response 0xc8f6 A play.google.com
8	1601908896.774259738	192.168.128.2	192.168.128.129	DNS	114	53	56547	0.001859563	Standard query response 0x8df7 AAAA play.google.com
9	1601908897.289640484	192.168.128.129	192.168.128.2	DNS	86	41102	53	0.515380746	Standard query 0xc907 A www.mozilla.org OPT
10	1601908897.289760462	192.168.128.129	192.168.128.2	DNS	86	43176	53	0.000119978	Standard query 0xc376 AAAA www.mozilla.org OPT
11	1601908897.289949577	192.168.128.129	192.168.128.2	DNS	84	43166	53	0.000189115	Standard query 0x5da3 A moodle.uam.es OPT
12	1601908897.290062203	192.168.128.129	192.168.128.2	DNS	84	49529	53	0.000112626	Standard query 0x8dc9 AAAA moodle.uam.es OPT
13	1601908897.290180589	192.168.128.129	192.168.128.2	DNS	85	49367	53	0.000118386	Standard query 0x1100 A www.google.com OPT
14	1601908897.290306471	192.168.128.129	192.168.128.2	DNS	85	58386	53	0.000124152	Standard query 0x7f55 AAAA www.google.com OPT
15	1601908897.298714634	192.168.128.2	192.168.128.129	DNS	190	53	43176	0.008409893	Standard query response 0xc376 AAAA www.mozilla.org
16	1601908897.298744298	192.168.128.2	192.168.128.129	DNS	166	53	41102	0.000029664	Standard query response 0xc907 A www.mozilla.org

Encapsulation type: Ethernet (I)
 Arrival Time: Oct 5, 2020 14:41:34.631599462 UTC
 [Time shift for this packet: 0.000000000 seconds]