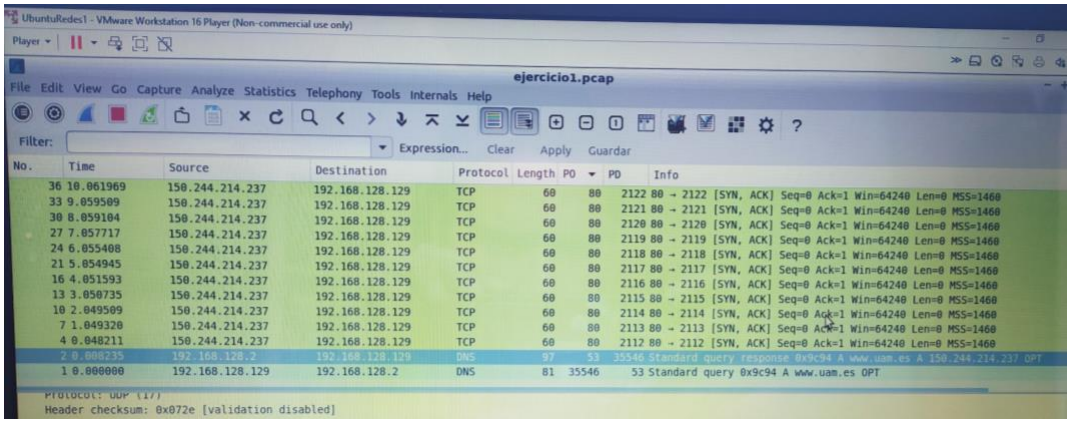
Práctica 1. Introducción a Wireshark para el análisis de trazas.

-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.

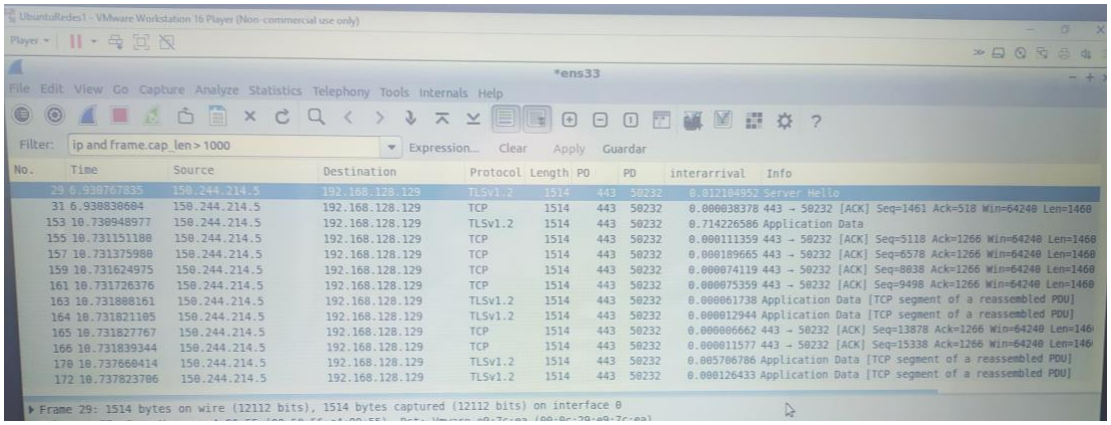


2-
El filtro utilizado: **ip and frame.cap_len > 1000**

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.

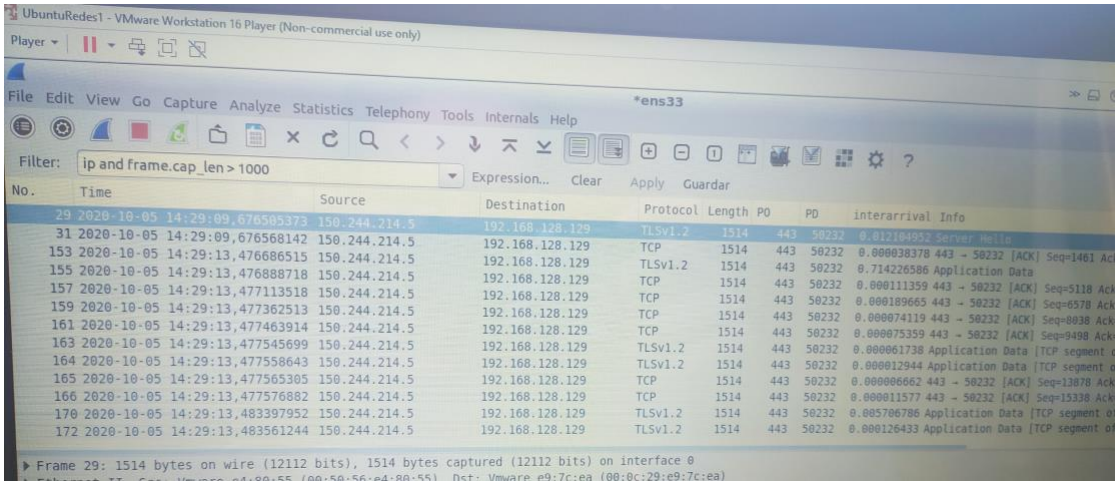
Hemos observado que el tamaño del paquete es mayor que el del campo lenght del protocolo ip. El tamaño total supera por 14 bytes al del protocolo. Estos 14 bytes son los que ocupan la cabecera.
3-
Para añadir el campo interarrival nos hemos ido arriba a la izquierda y hemos hecho click en *Edit*. Se 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

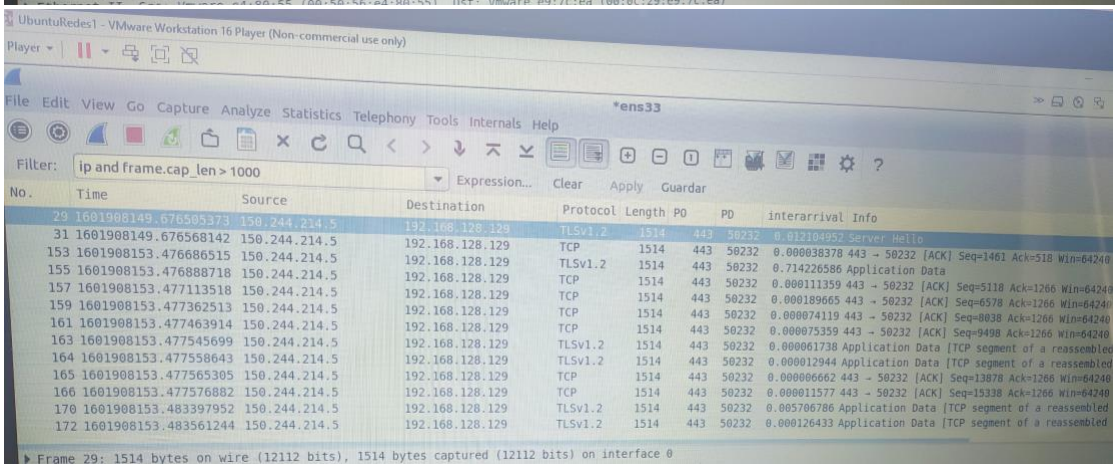
hemos hecho click en *Columns.* Hemos visto que a la derecha nos salen muchas opciones para elegir de qué tipo de dato queremos que sea nuestra nueva columna. Aquí hemos elegido *Delta Time.* Después hemos personalizado el nombre poniendo *Interarrival.* Aquí ha habido un problema porque nos ha dado 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.