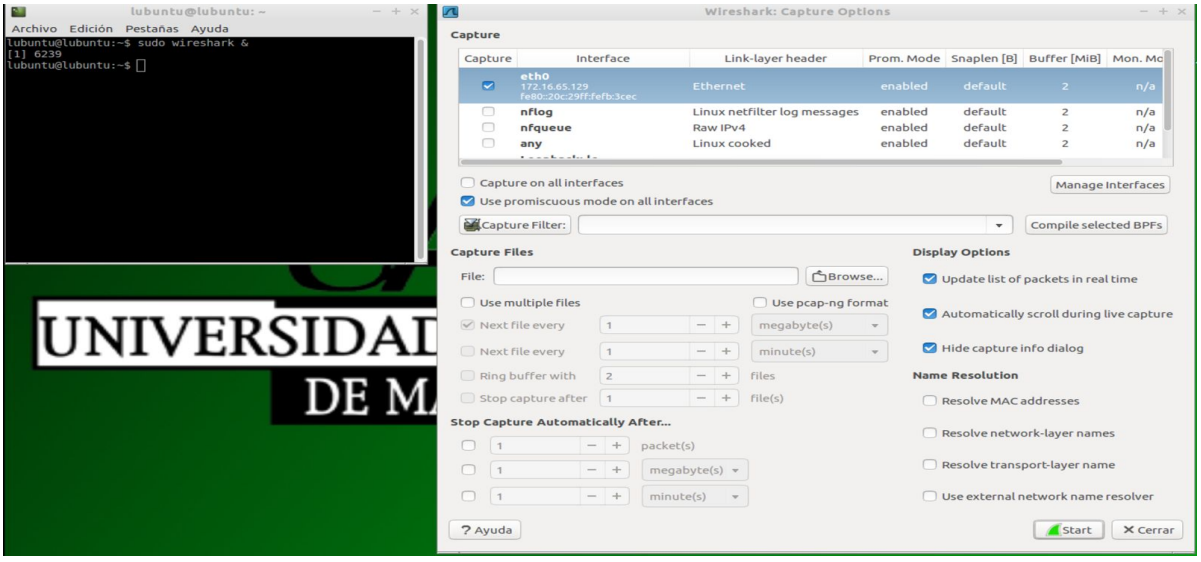
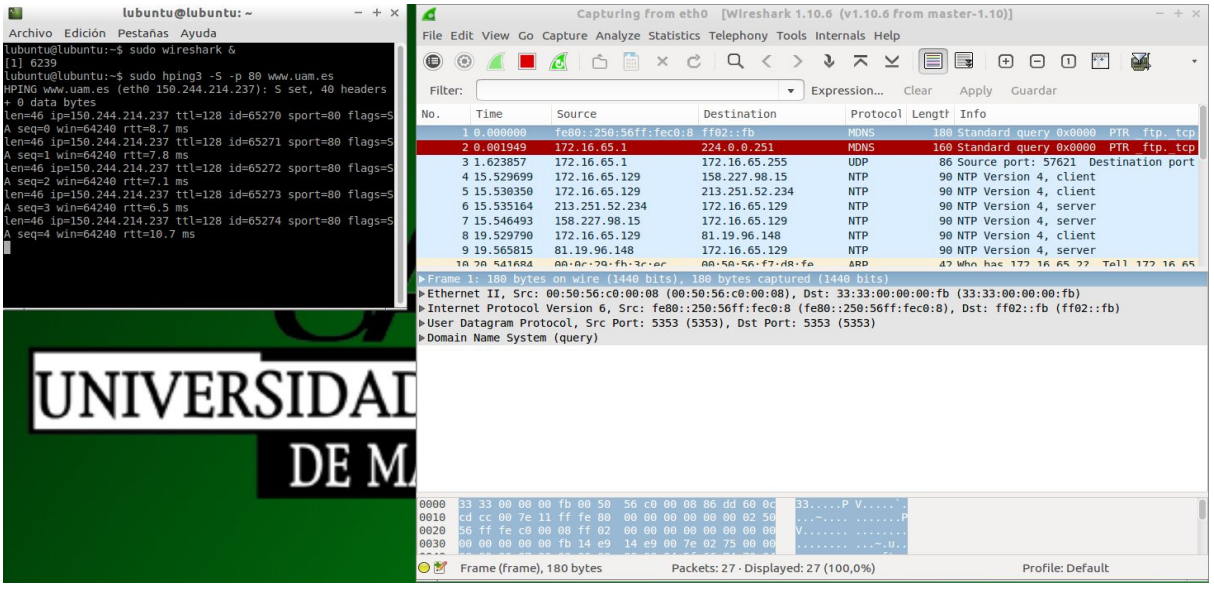
Práctica 1 - Ejercicios captura de tráfico

Ejercicio 1.-

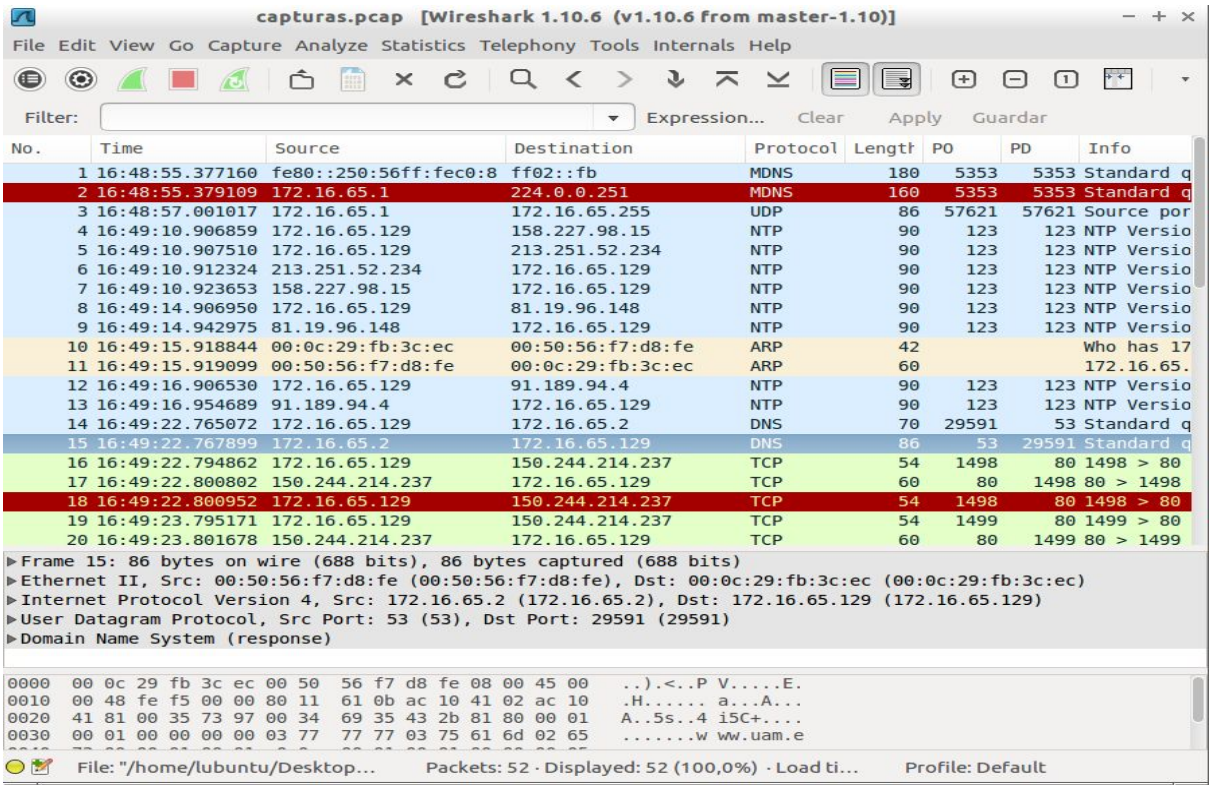
Tras haber conseguido instalar correctamente la máquina virtual necesaria nos disponemos a iniciar esta primera práctica de la asignatura. En primer lugar, abrimos la terminal para ejecutar wireshark en segundo plano con permisos de superusuario para después proceder a capturar el tráfico generado por el comando especificado en el punto 4. Una vez hayamos seleccionado los ajustes oportunos en la ventana “opciones de captura” (activamos solo modo promiscuo y todas las opciones del display).



Una vez que se ha capturado varios paquetes detenemos el proceso y observamos los distintos frames que han sido capturados, apreciando el desglose de cada uno en sus correspondientes protocolos en el panel intermedio; mientras que con el panel inferior vemos los valores hexadecimales de los campos seleccionados.



A continuación, guardamos la traza realizada y comprobamos que se vuelve a abrir sin problema. Finalmente, una vez hemos añadido las columnas PO y PD, nos disponemos a ordenar los paquetes como se especifica y como resultado vemos que tan solo existe un paquete cuyo campo PO sea 53. Este es el 15 que fue capturado y se corresponde con el protocolo Domain Name System (DNS).



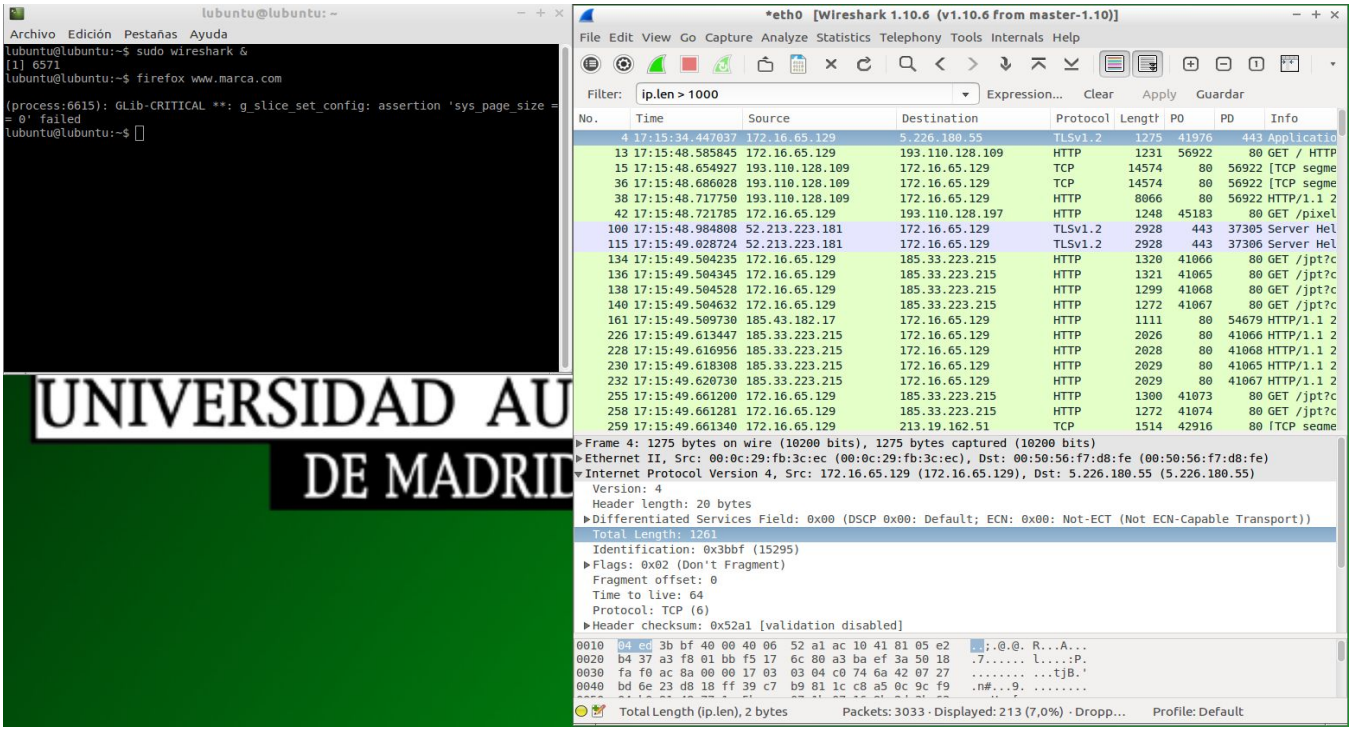
Ejercicio 2.-

En este segundo ejercicio repetimos el proceso inicial del anterior pero esta vez generando tráfico arbitrario desde el navegador.

1. Una vez capturado, usamos el filtro de interfaz abajo descrito para cumplir que solo se visualicen los paquetes que sean de tipo IP y que tengan un tamaño de paquete mayor a 1000 Bytes:

$$ip.len > 1000$$

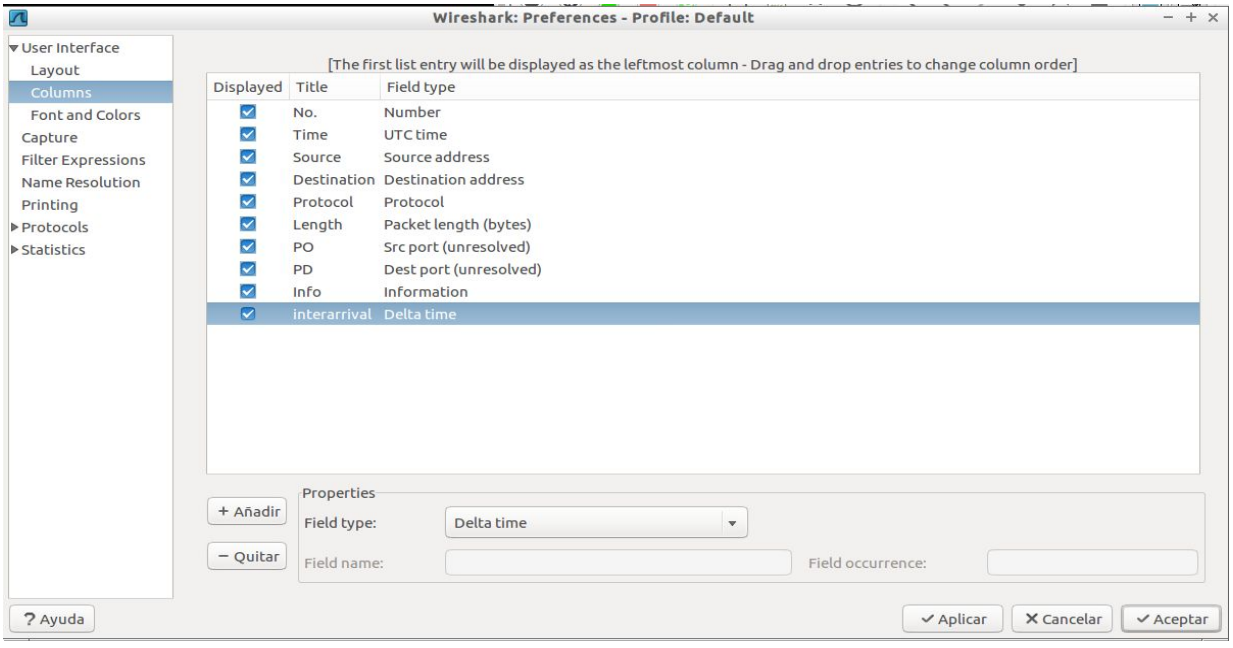
2. Al ser paquetes filtrados tras haberse hecho la captura y no al revés, se han capturado todos los paquetes. Entonces, a la hora de guardar la captura, Wireshark nos da la opción de guardar todos los paquetes o solo los filtrados, seleccionando esta última opción, obtenemos los paquetes que queremos.
3. Para responder a esta pregunta, hemos realizado ciertos cálculos triviales: en la columna tamaño que sale de cada paquete, se encuentra el tamaño total, pulsando sobre cada uno de los cinco primeros paquetes y después en el panel intermedio abriendo la información relacionada con el IP, nos encontramos con un tamaño del IP que siempre es 14 bytes más pequeño que el paquete total. Esto es debido a que el IP es un protocolo que se encuentra dentro de los demás y estos incorporan su propia cabecera que ocupa esos 14 bytes.



En la imagen se aprecia en la terminal la búsqueda en firefox de una página web y a su derecha el resultado de la captura tras aplicar el filtro de interfaz pedido, además se selecciona el primero de los paquetes y en el panel central de Wireshark se remarca el tamaño del Internet Protocol (IP) que es 1261 frente a los 1275 del paquete.

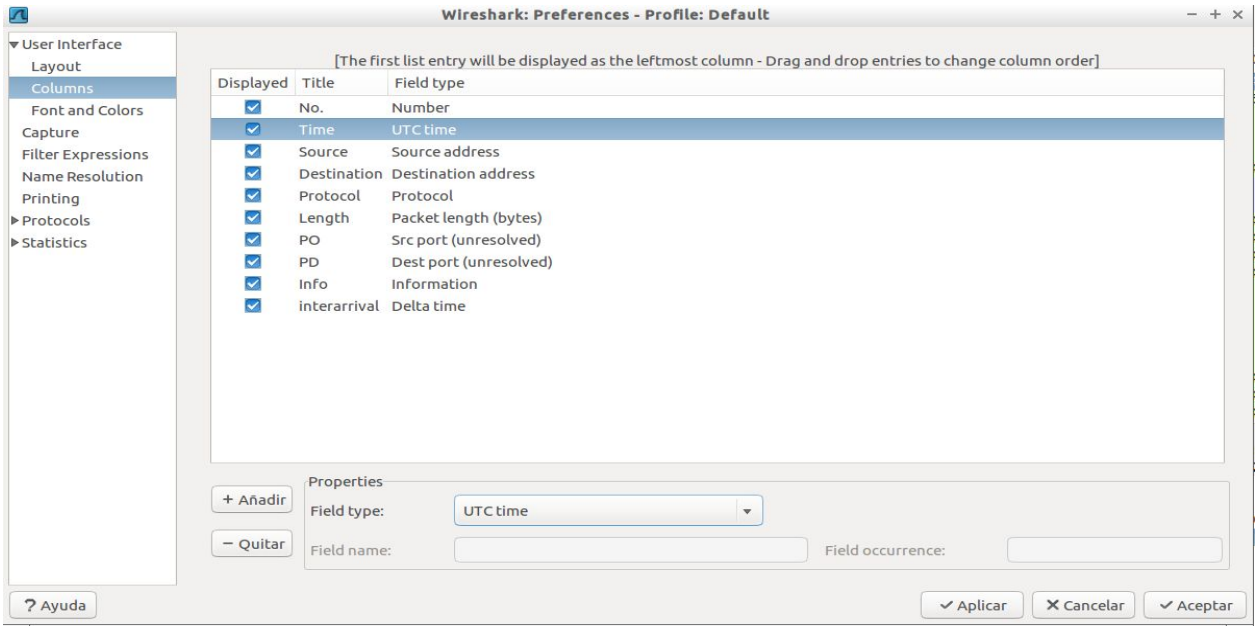
Ejercicio 3.-

Para este apartado simplemente añadimos una columna correspondiente al *interarrival* especificado, que será de tipo “Delta Time”. El proceso seguido es pinchar en Edit -> Preferences y seleccionar dentro del grupo User Interface el grupo Columns y ahí ya añadir una nueva columna con el nombre pedido y las unidades antes mencionadas.

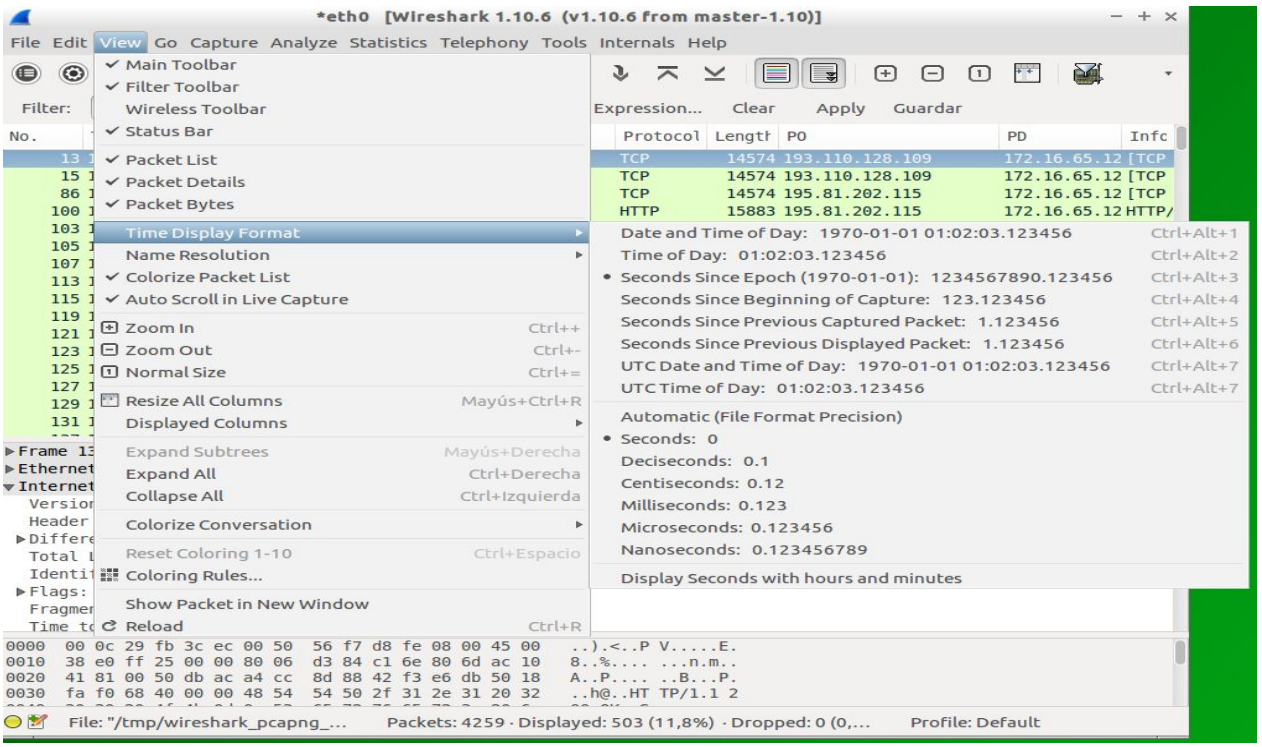


Ejercicio 4.-

En este caso nos disponemos a modificar el tipo de la columna “Time” en preferencias dentro del desplegable de “edit”. De este modo podemos escoger unas unidades adecuadas para ser leídas por humanos como es el tipo “UTC Time”.

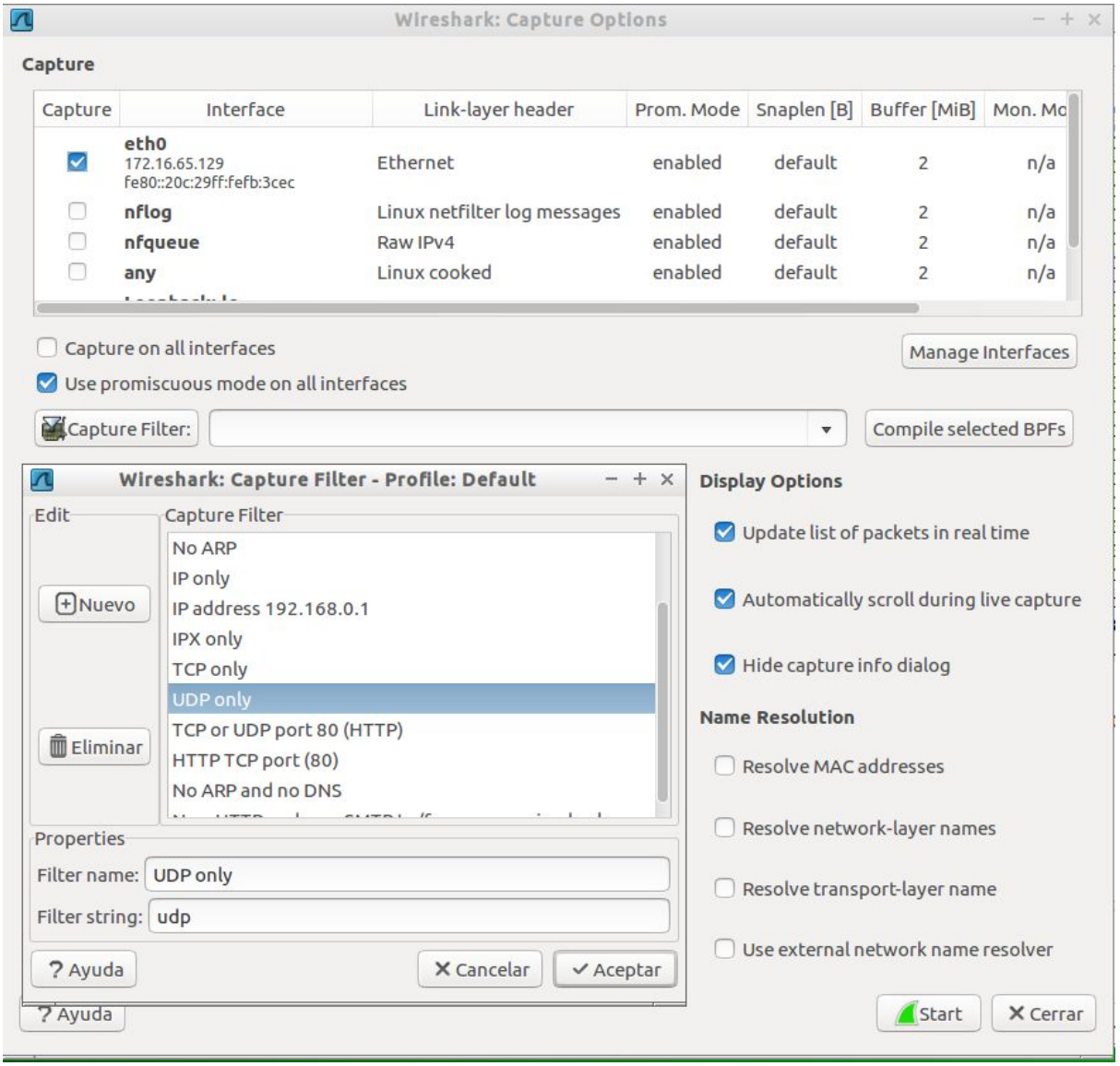


Para hacerlo en modo UNIX es algo más complejo, primero nos desplegamos por los menús principales y al pulsar sobre view, pinchamos en el desplegable en “Time Display Format” y dentro seleccionamos “Seconds since Epoch” y “Seconds”. Una vez hecho esto, solo debemos acceder de nuevo a la columna de tiempo igual que antes y seleccionar esta vez el tipo “Time (format as specified)”.



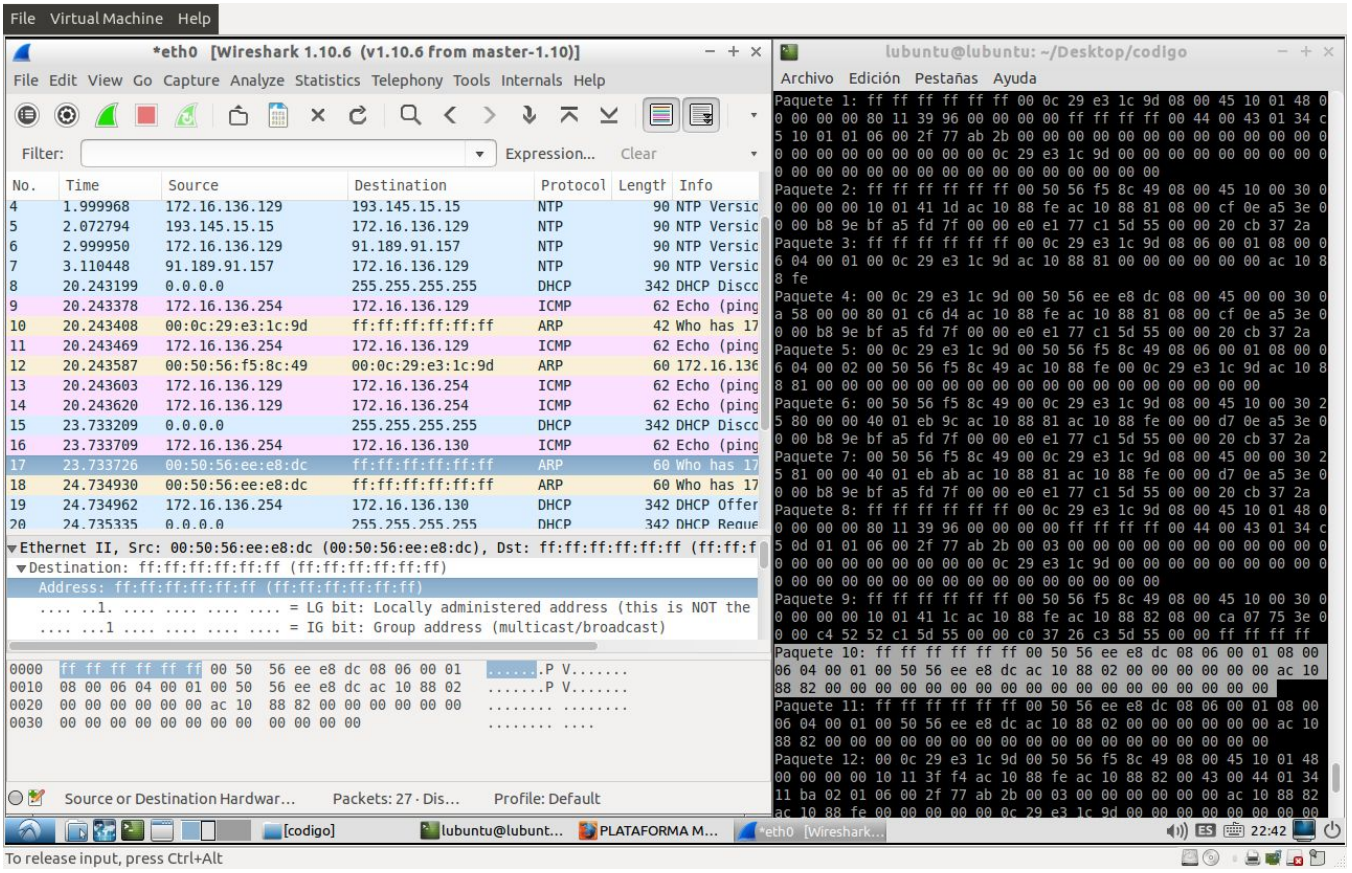
Ejercicio 5.-

El objetivo de este ejercicio es que entendamos la diferencia con respecto al anterior ejercicio 2. En este se nos pide capturar paquetes siguiendo un cierto filtro mientras que en el anterior se pedía que una vez capturados los paquetes desde la interfaz se filtrasen una serie de paquetes. El proceso a seguir para la captura es la misma que en el ejercicio uno pero con una salvedad en el campo Capture Filter pinchar sobre el botón y seleccionar el filtro UDP only. Todos los pasos a partir de ahí siguen siendo los mismos, se capturan muchos menos paquetes al actuar el filtro en la captura y se corresponden con paquetes del protocolo UDP como era esperado.



NOTA:

Tal y como se comenta en la parte de codifiación del enunciado adjunto se encuentra una captura de pantalla con la captura de nuestro programa y la de Wireshark en paralelo donde se aprecia que ambas son iguales, la diferencia en cuanto a la posición se debe a que no se pudo iniciar ambas capturas en el mismo instante de tiempo.



Andrés Salas Peña y Francisco Vicente Lana