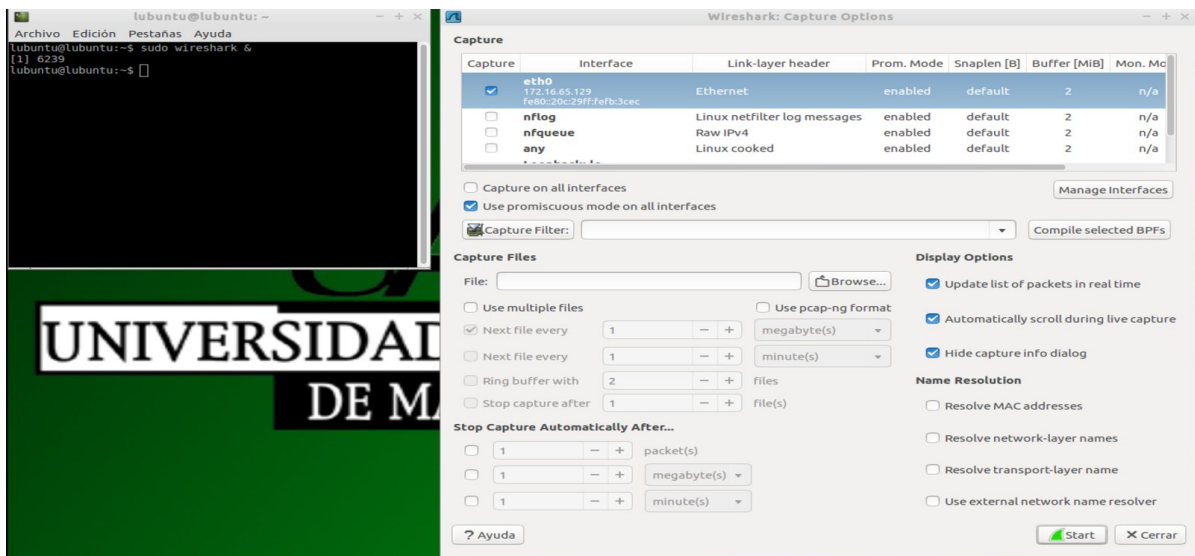


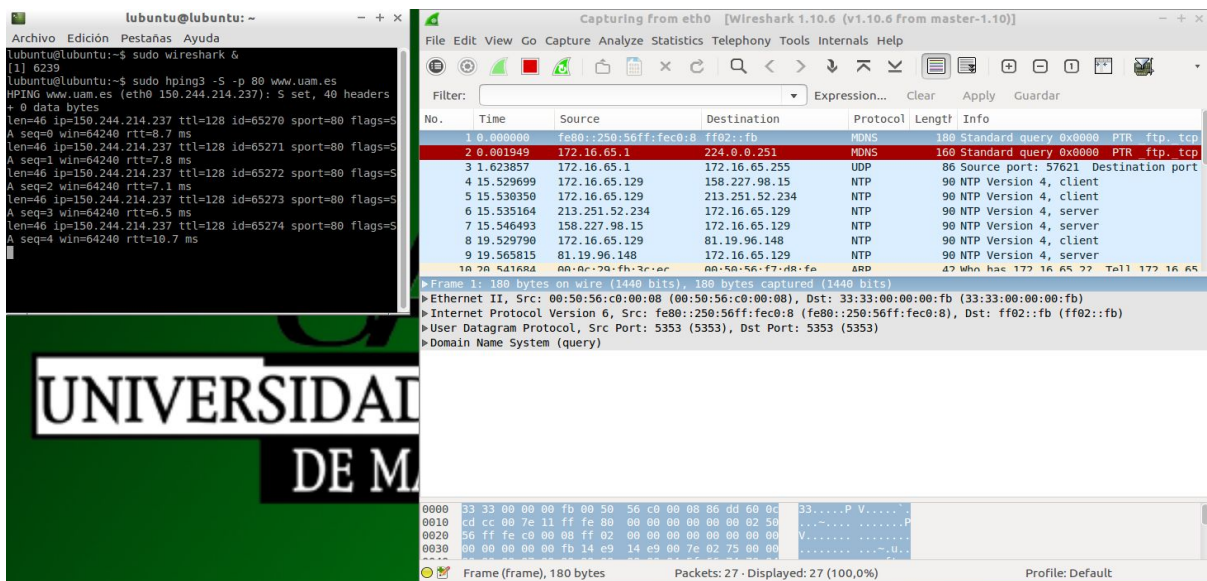
# Práctica 1 - Ejercicios captura de tráfico

## 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).

No.	Time	Source	Destination	Protocol	Length	PO	PD	Info
1	16:48:55.377160	fe80::250:56ff:fec0:8	ff02::fb	MDNS	180	5353	5353	Standard q
2	16:48:55.379109	172.16.65.1	224.0.0.251	MDNS	160	5353	5353	Standard q
3	16:48:57.001017	172.16.65.1	172.16.65.255	UDP	86	57621	57621	Source por
4	16:49:10.906859	172.16.65.129	158.227.98.15	NTP	90	123	123	NTP Versio
5	16:49:10.907510	172.16.65.129	213.251.52.234	NTP	90	123	123	NTP Versio
6	16:49:10.912324	213.251.52.234	172.16.65.129	NTP	90	123	123	NTP Versio
7	16:49:10.923653	158.227.98.15	172.16.65.129	NTP	90	123	123	NTP Versio
8	16:49:14.906950	172.16.65.129	81.19.96.148	NTP	90	123	123	NTP Versio
9	16:49:14.942975	81.19.96.148	172.16.65.129	NTP	90	123	123	NTP Versio
10	16:49:15.918844	00:0c:29:fb:3c:ec	00:50:56:f7:d8:fe	ARP	42			Who has 17
11	16:49:15.919099	00:50:56:f7:d8:fe	00:0c:29:fb:3c:ec	ARP	60			172.16.65.
12	16:49:16.906530	172.16.65.129	91.189.94.4	NTP	90	123	123	NTP Versio
13	16:49:16.954689	91.189.94.4	172.16.65.129	NTP	90	123	123	NTP Versio
14	16:49:22.765072	172.16.65.129	172.16.65.2	DNS	70	29591	53	Standard q
15	16:49:22.767899	172.16.65.2	172.16.65.129	DNS	86	53	29591	Standard q
16	16:49:22.794862	172.16.65.129	150.244.214.237	TCP	54	1498	80	1498 > 80
17	16:49:22.800802	150.244.214.237	172.16.65.129	TCP	60	80	1498	80 > 1498
18	16:49:22.800952	172.16.65.129	150.244.214.237	TCP	54	1498	80	1498 > 80
19	16:49:23.795171	172.16.65.129	150.244.214.237	TCP	54	1499	80	1499 > 80
20	16:49:23.801678	150.244.214.237	172.16.65.129	TCP	60	80	1499	80 > 1499

Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: 00:50:56:f7:d8:fe (00:50:56:f7:d8:fe), Dst: 00:0c:29:fb:3c:ec (00:0c:29:fb:3c:ec)

Internet Protocol Version 4, Src: 172.16.65.2 (172.16.65.2), Dst: 172.16.65.129 (172.16.65.129)

User Datagram Protocol, Src Port: 53 (53), Dst Port: 29591 (29591)

Domain Name System (response)

0000 00 0c 29 fb 3c ec 00 50 56 f7 d8 fe 08 00 45 00 ..).<..P V....E.

0010 00 48 fe f5 00 00 80 11 61 0b ac 10 41 02 ac 10 .H.....a...A...

0020 41 81 00 35 73 97 00 34 69 35 43 2b 81 80 00 01 A..5s..4 i5C+....

0030 00 01 00 00 00 00 03 77 77 77 03 75 61 6d 02 65 .....W ww.uam.e

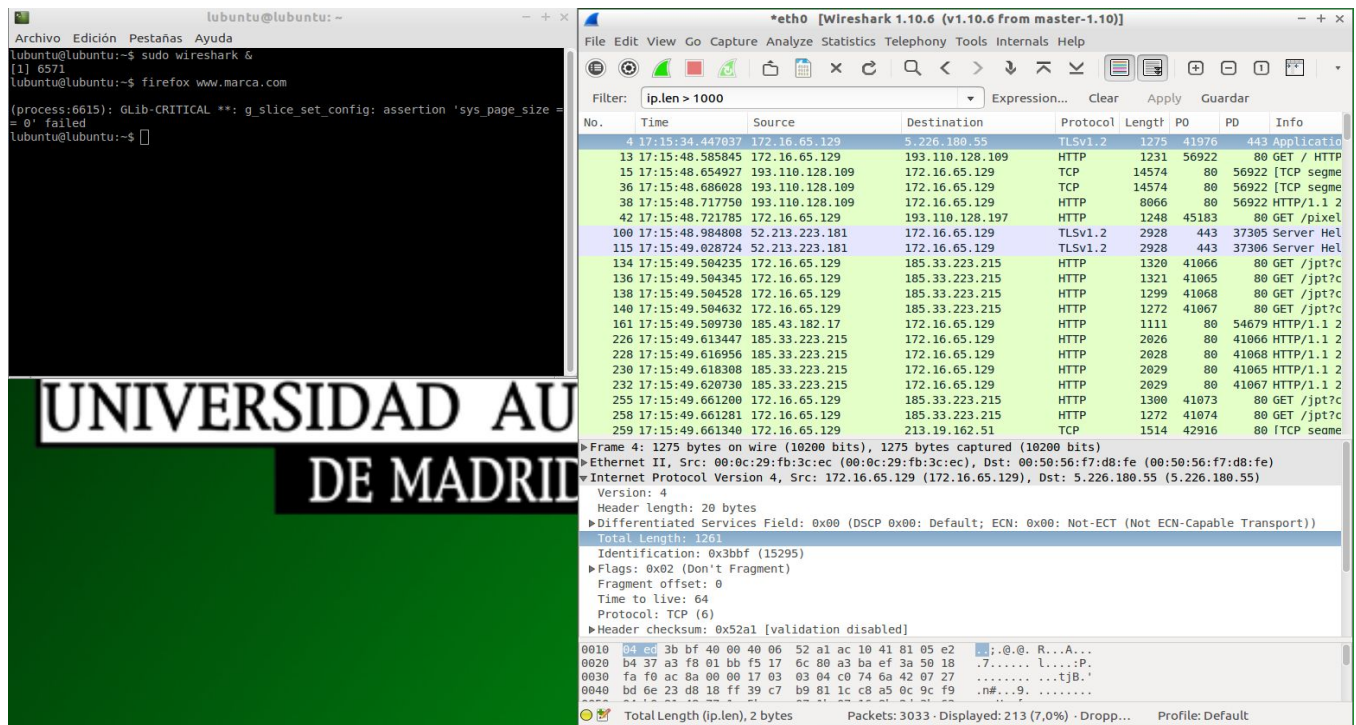
## Ejercicio 2.-

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:

$ip.len > 1000$

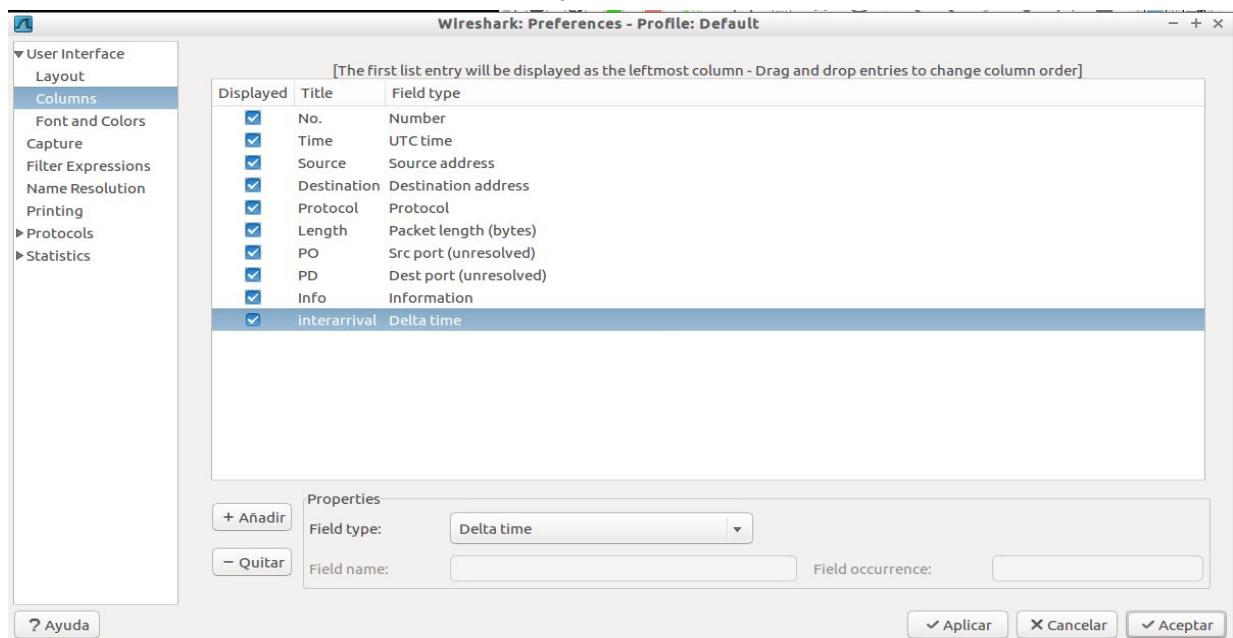
2. Al ser paquetes filtrados tras haberse hecho la captura y no al revés, se han capturado todos los paquetes. Entonces, a la hora de guardar la captura, Wireshark nos da la opción de guardar todos los paquetes o solo los filtrados, seleccionando esta última opción, obtenemos los paquetes que queremos.
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.-

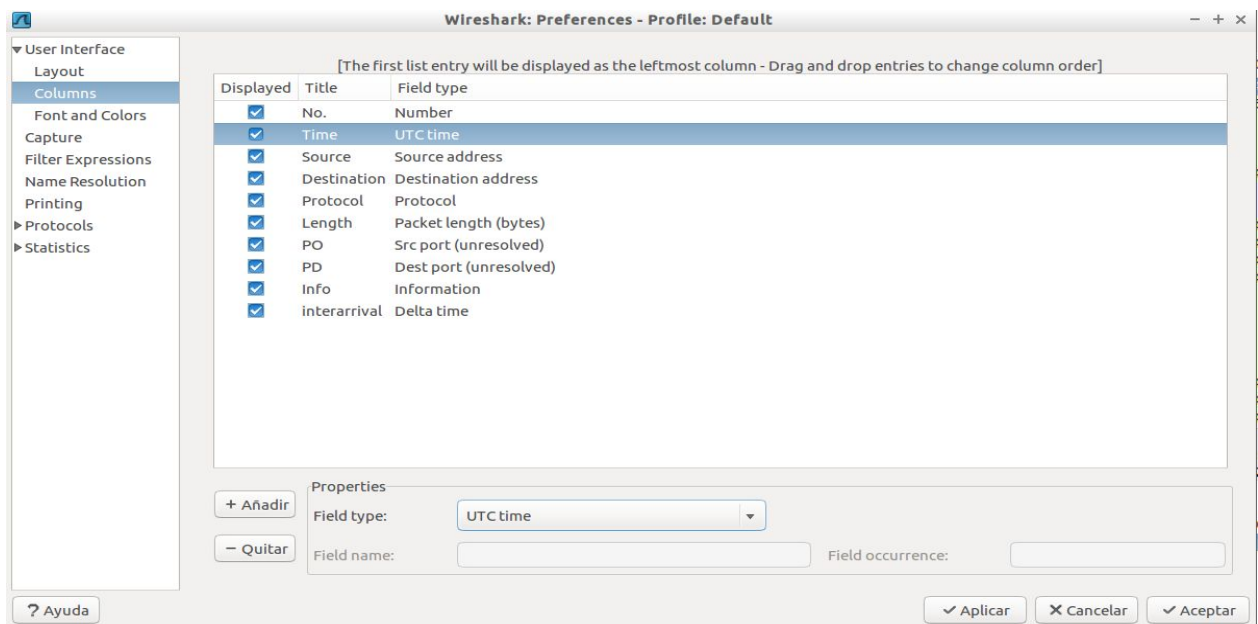
Para este apartado simplemente añadimos una columna correspondiente al *interarrival* especificado, que será de tipo “Delta Time”. El proceso seguido es pinchar en Edit -> Preferences y seleccionar dentro del grupo User Interface el grupo Columns y ahí ya añadir una nueva columna con el nombre pedido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



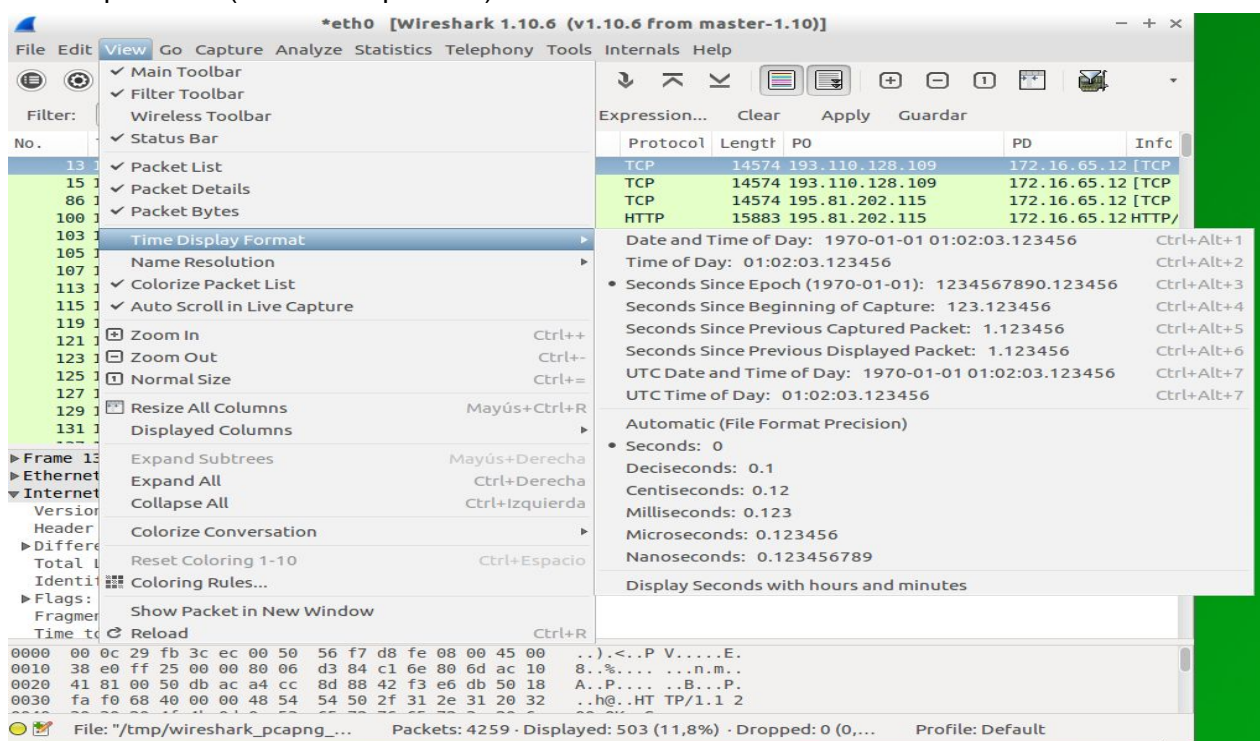


## Ejercicio 4.-

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”.

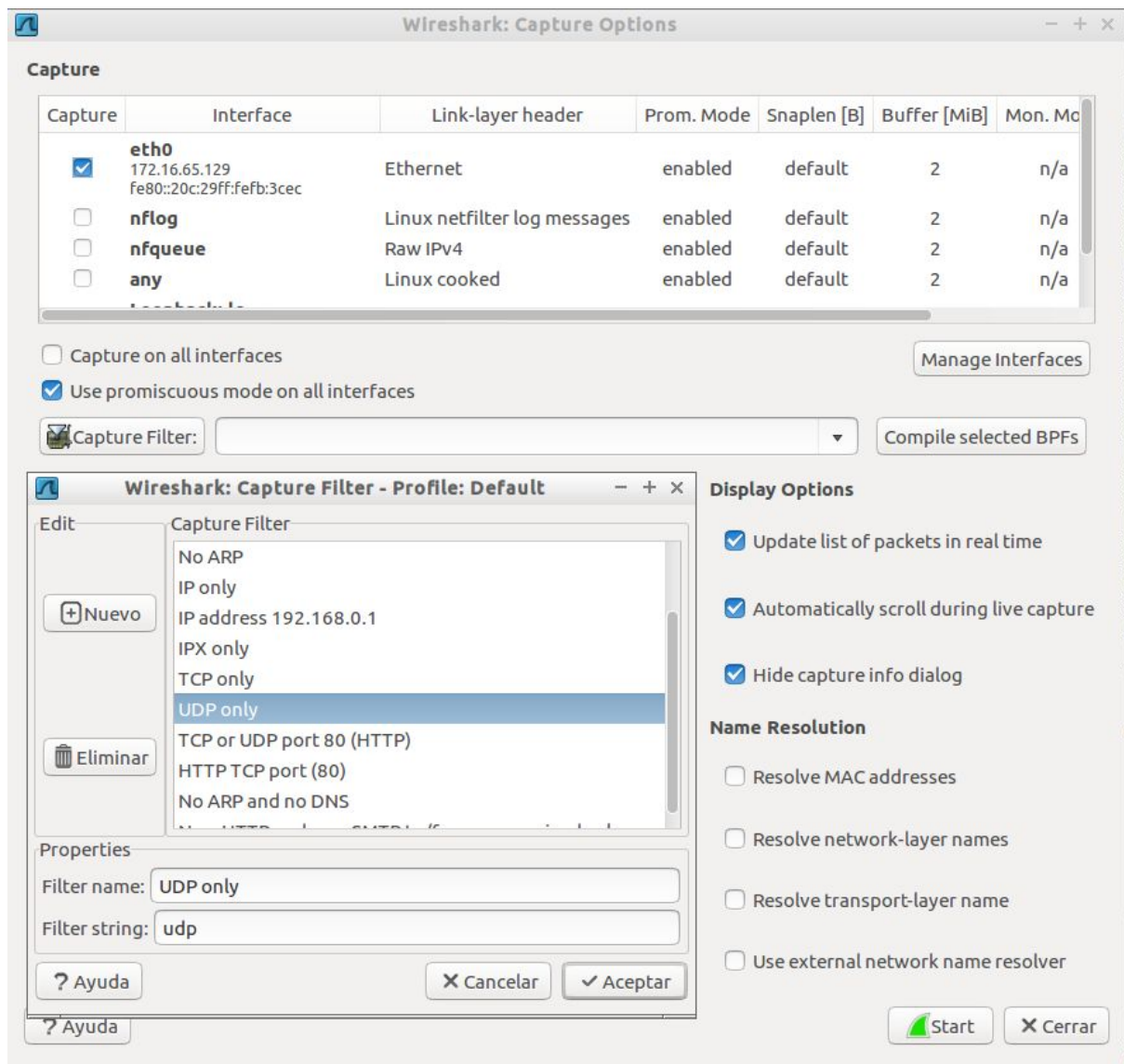


Para hacerlo en modo UNIX es algo más complejo, primero nos desplegamos por los menús principales y al pulsar sobre view, pinchamos en el desplegable en “Time Display Format” y dentro seleccionamos “Seconds since Epoch” y “Seconds”. Una vez hecho esto, solo debemos acceder de nuevo a la columna de tiempo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

The screenshot displays a virtual machine environment with two windows open. The left window is Wireshark 1.10.6, showing a list of captured packets on the 'eth0' interface. The packets are numbered 4 through 20, with columns for No., Time, Source, Destination, Protocol, Length, and Info. The right window is a terminal window titled 'lubuntu@lubuntu: ~/Desktop/codigo', showing the output of a program. The output is a hex dump of network packets, with each line representing a packet's data. The hex data is displayed in a grid format, with some text labels like 'P V...' and 'P V...' interspersed. The terminal window also shows the source and destination IP addresses for each packet, matching the information in the Wireshark window. The bottom of the screenshot shows the virtual machine's taskbar and system tray, indicating the time as 22:42.

No.	Time	Source	Destination	Protocol	Length	Info
4	1.999968	172.16.136.129	193.145.15.15	NTP	90	NTP Versio
5	2.072794	193.145.15.15	172.16.136.129	NTP	90	NTP Versio
6	2.999950	172.16.136.129	91.189.91.157	NTP	90	NTP Versio
7	3.110448	91.189.91.157	172.16.136.129	NTP	90	NTP Versio
8	20.243199	0.0.0.0	255.255.255.255	DHCP	342	DHCP Disc
9	20.243378	172.16.136.254	172.16.136.129	ICMP	62	Echo (ping
10	20.243408	00:0c:29:e3:1c:9d	ff:ff:ff:ff:ff:ff	ARP	42	Who has 17
11	20.243469	172.16.136.254	172.16.136.129	ICMP	62	Echo (ping
12	20.243587	00:50:56:f5:8c:49	00:0c:29:e3:1c:9d	ARP	60	172.16.136
13	20.243603	172.16.136.129	172.16.136.254	ICMP	62	Echo (ping
14	20.243620	172.16.136.129	172.16.136.254	ICMP	62	Echo (ping
15	23.733209	0.0.0.0	255.255.255.255	DHCP	342	DHCP Disc
16	23.733709	172.16.136.254	172.16.136.130	ICMP	62	Echo (ping
17	23.733726	00:50:56:ee:e8:dc	ff:ff:ff:ff:ff:ff	ARP	60	Who has 17
18	24.734930	00:50:56:ee:e8:dc	ff:ff:ff:ff:ff:ff	ARP	60	Who has 17
19	24.734962	172.16.136.254	172.16.136.130	DHCP	342	DHCP Offer
20	24.735335	0.0.0.0	255.255.255.255	DHCP	342	DHCP Reque

▼ Ethernet II, Src: 00:50:56:ee:e8:dc (00:50:56:ee:e8:dc), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)  
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)  
.....1. .... = LG bit: Locally administered address (this is NOT the  
.....1. .... = IG bit: Group address (multicast/broadcast)

0000 ff ff ff ff ff ff 00 50 56 ee e8 dc 08 06 00 01 .....P V.....  
0010 08 00 06 04 00 01 00 50 56 ee e8 dc ac 10 88 02 .....P V.....  
0020 00 00 00 00 00 00 ac 10 88 82 00 00 00 00 00 .....  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....