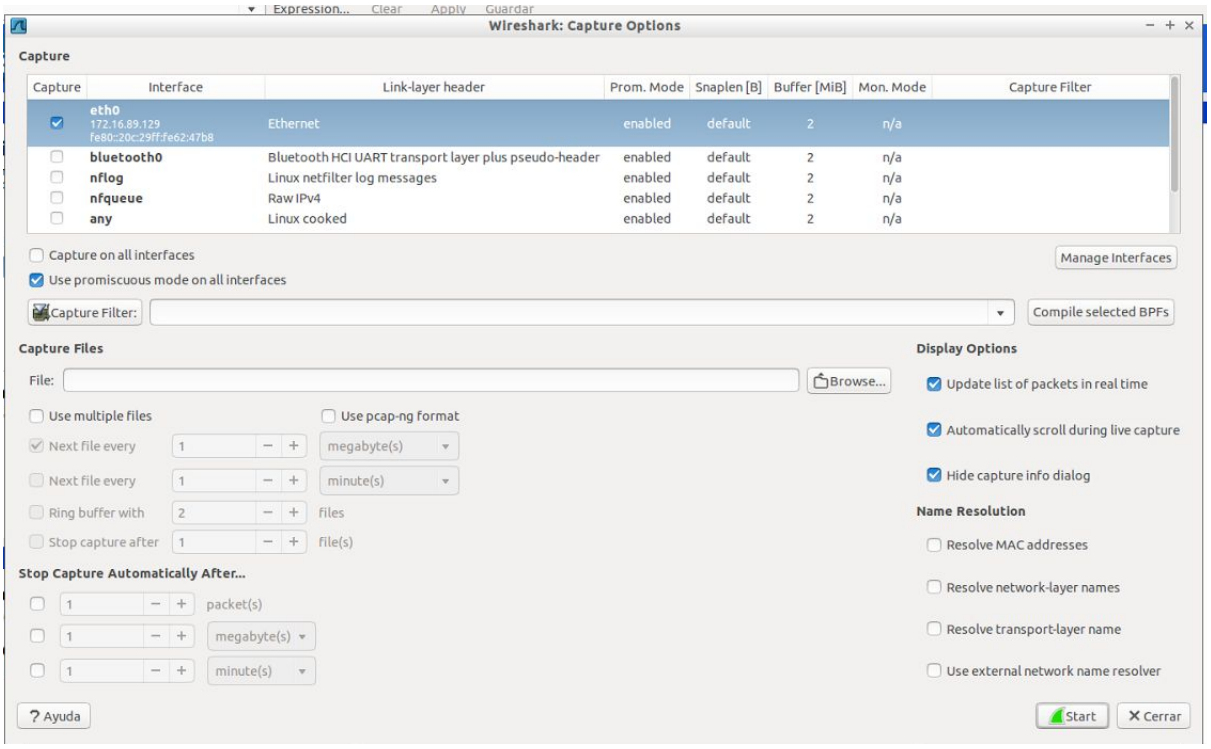
Claudia Cea, Juan Riera
Pareja 5
Grupo 1301

Ejercicios de captura de tráfico

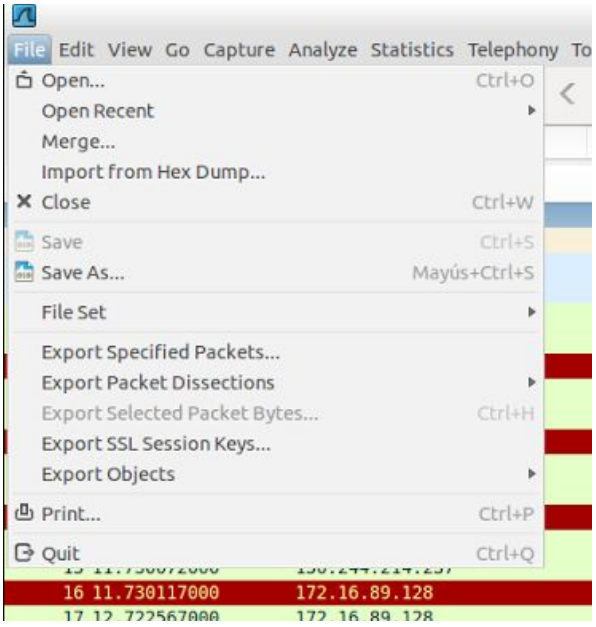
1. Durante la realización de las prácticas, será muy común disponer de una consola donde ejecutaremos comandos que mandan y reciben tramas por un interfaz de red. En paralelo tendremos en ejecución a Wireshark, que estará capturando el tráfico que nos interese. Este ejercicio muestra un ejemplo típico a realizar en prácticas posteriores:
1. Abra una consola o shell, y déjela abierta en espera de ejecutar algún comando.
2. Ejecute Wireshark y seleccione y configure el interfaz por el que se capturará el tráfico (habitualmente será eth0) Acuérdese de seleccionar las opciones de visualización que más le convenga.
3. Inicie la captura de tráfico pulsando en el botón 'Start'.
4. Vuelva a la consola y ejecute el siguiente comando (tecléelo y pulse): $ sudo hping3 -S -p 80 www.uam.es
5. Detenga la captura de tráfico mediante el botón 'Stop'.
6. Analice el tráfico capturado (aunque no lo entienda en detalle)
7. Guarde la traza en un fichero (Importante: no utilizar el formato pcap-ng).
8. Cierre Wireshark, y vuelva a abrirlo.
9. Abra el fichero almacenado y compruebe que se almacenó correctamente.
10.Utilizando las columnas que se han añadido durante el tutorial, ordene con respecto al campo 'PO' en sentido descendente y contabilice el número de paquetes en el que este campo tiene valor 53.
Describa el proceso realizado y discuta los problemas que haya encontrado durante la realización del ejercicio.

En primer lugar ejecutamos Wireshark como superusuario con el comando “sudo wireshark &”. Una vez abierto el programa, nos metemos en la ventana de configuración para la captura de tráfico y seleccionamos las opciones correspondientes, explicadas en el PDF de la práctica 0: Elegimos Eth0 como nuestra interfaz de red, seleccionamos el modo promiscuo y no guardamos los ficheros de tráfico con el formato pcap-ng.

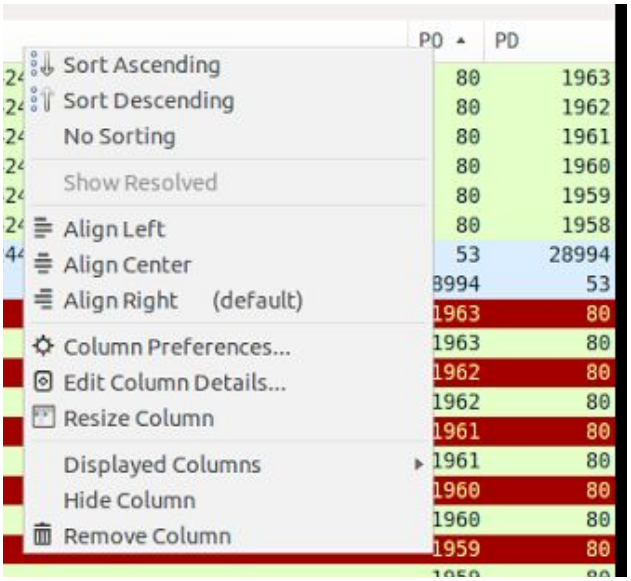


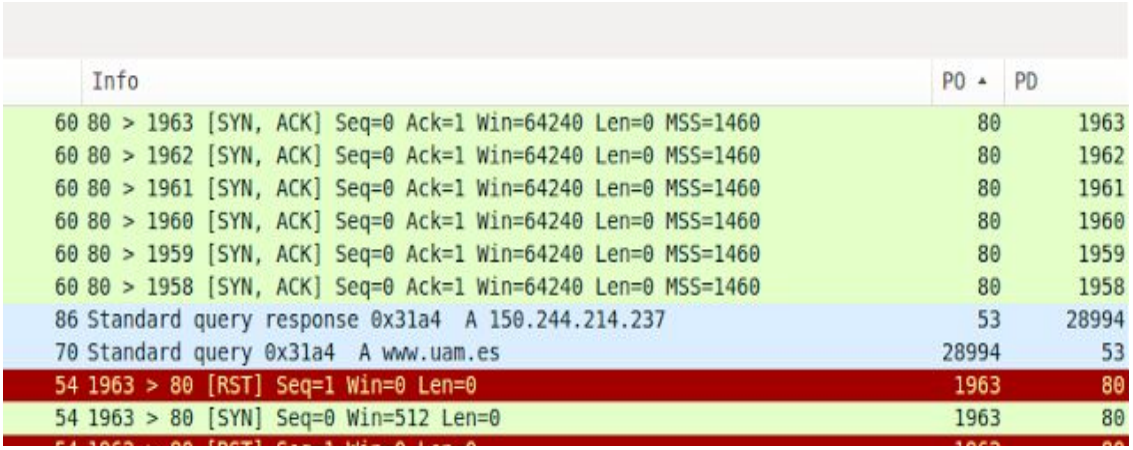
Pulsamos el botón Start y empezamos con la captura de tráfico tal y como se especifica en el enunciado. Detenemos el tráfico generado y podemos observar que se trata de un envío continuo de paquetes en el que se indica el tiempo que tarda en enviarse.

Tras el análisis del tráfico, guardamos la traza en un fichero de la siguiente manera: hacemos click en la opción File del menú principal y a continuación seleccionamos la opción Save o Save As y lo guardamos. Cerramos Wireshark, lo volvemos a abrir. Para abrir el fichero que hemos denominado ej1.pcapng hacemos click sobre la opción File, pero esta vez seleccionamos la opción Open y de ahí el paquete correspondiente.



Comprobamos que el fichero se ha almacenado correctamente así que proseguimos y ordenamos los datos con respecto a PO en sentido descendente seleccionando la opción Sort Descending. De esa manera podemos observar claramente que solo hay un paquete cuyo campo PO tenga el valor 53, el paquete número 4.





2. Tras haber leído las documentación online facilitada, empiece a capturar tráfico. Abra un navegador y genere tráfico a partir de la visualización de páginas web. Pare la captura, y añada un filtro en el interfaz de modo que solo se visualicen paquetes que sean de tipo IP y que tengan un tamaño de paquete mayor a 1000 Bytes.

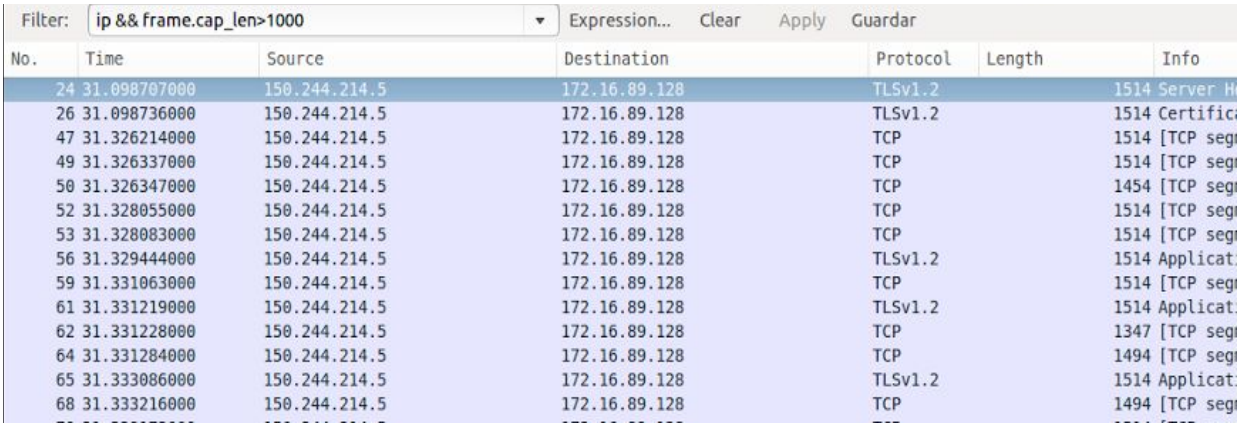
1. Copie el filtro realizado.

2. ¿Cómo almacenaría en una captura solo los paquetes mostrados?

3. Compare el tamaño del primer paquete IP, y el campo 'length' del protocolo IP del mismo. Repita para los primeros 5 paquetes, ¿qué relación encuentra?

El filtro realizado es: ip && frame.cap_len>1000 pues con el filtro ip solo se muestran los paquetes de tipo IP y con frame.cap_len>1000 indicamos que solo queremos visualizar paquetes cuyo tamaño sea mayor a 1000 bytes.

Para almacenar en una captura solo los paquetes mostrados lo que tenemos que hacer es aplicar el filtro y luego guardar la captura como hicimos en el ejercicio anterior. Si cerramos Wireshark y lo volvemos a abrir podemos comprobar que solo se muestran los paquetes filtrados.

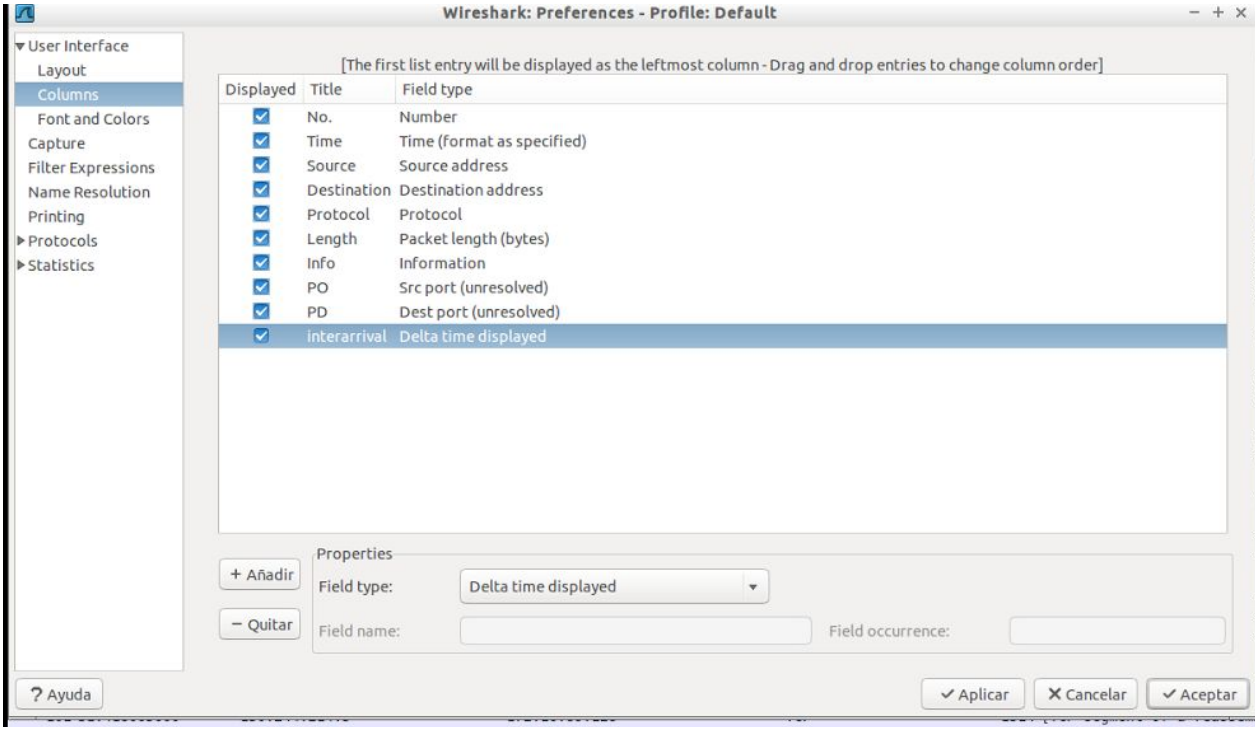


No.	Time	Source	Destination	Protocol	Length	Info
24	31.098707000	150.244.214.5	172.16.89.128	TLSv1.2	1514	Server H
26	31.098736000	150.244.214.5	172.16.89.128	TLSv1.2	1514	Certifica
47	31.326214000	150.244.214.5	172.16.89.128	TCP	1514	[TCP segr
49	31.326337000	150.244.214.5	172.16.89.128	TCP	1514	[TCP segr
50	31.326347000	150.244.214.5	172.16.89.128	TCP	1454	[TCP segr
52	31.328055000	150.244.214.5	172.16.89.128	TCP	1514	[TCP segr
53	31.328083000	150.244.214.5	172.16.89.128	TCP	1514	[TCP segr
56	31.329444000	150.244.214.5	172.16.89.128	TLSv1.2	1514	Applicat
59	31.331063000	150.244.214.5	172.16.89.128	TCP	1514	[TCP segr
61	31.331219000	150.244.214.5	172.16.89.128	TLSv1.2	1514	Applicat
62	31.331228000	150.244.214.5	172.16.89.128	TCP	1347	[TCP segr
64	31.331284000	150.244.214.5	172.16.89.128	TCP	1494	[TCP segr
65	31.333086000	150.244.214.5	172.16.89.128	TLSv1.2	1514	Applicat
68	31.333216000	150.244.214.5	172.16.89.128	TCP	1494	[TCP segr

Si comparamos el tamaño del primer paquete IP, y el campo 'length' del protocolo IP del mismo, veremos que hay una diferencia de 14 bytes.

3. Añada una columna llamada interarrival que muestre el tiempo entre paquetes consecutivos. Explique brevemente qué menús y opciones ha seleccionado.

Para añadir la columna Interarrival hacemos click en Edit->preferences. Seleccionamos Columns y ahí añadimos la columna “Interarrival” que será de tipo Delta Time Displayed.

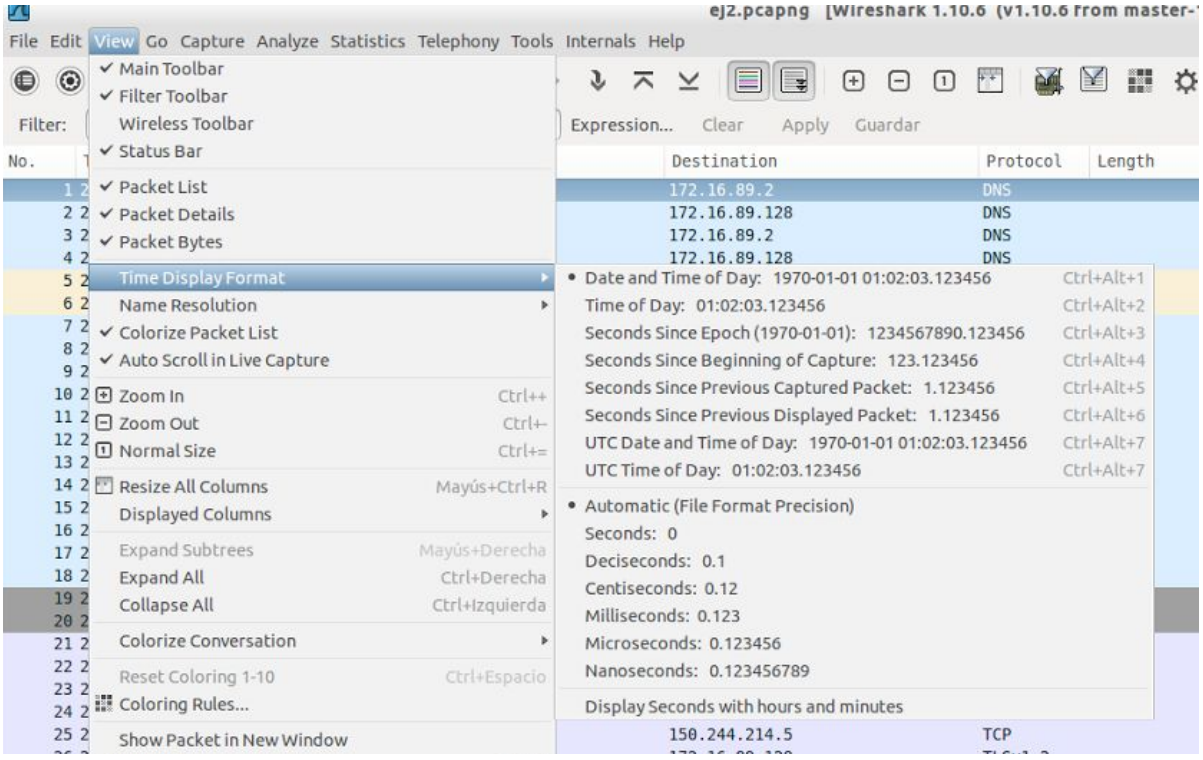


Para comprobar si la columna creada realiza verdaderamente su función abrimos, por ejemplo, el fichero ej2.pcapng y comprobamos que efectivamente muestra el tiempo entre paquetes consecutivos.

PO	PD	interarrival
9719	53	0.000000000
53	9719	0.029815000
4988	53	0.000739000
53	4988	0.006474000
		4.976774000
		0.000287000
3709	53	8.049358000
53	3709	0.013649000
1437	53	0.000735000
53	1437	0.003496000

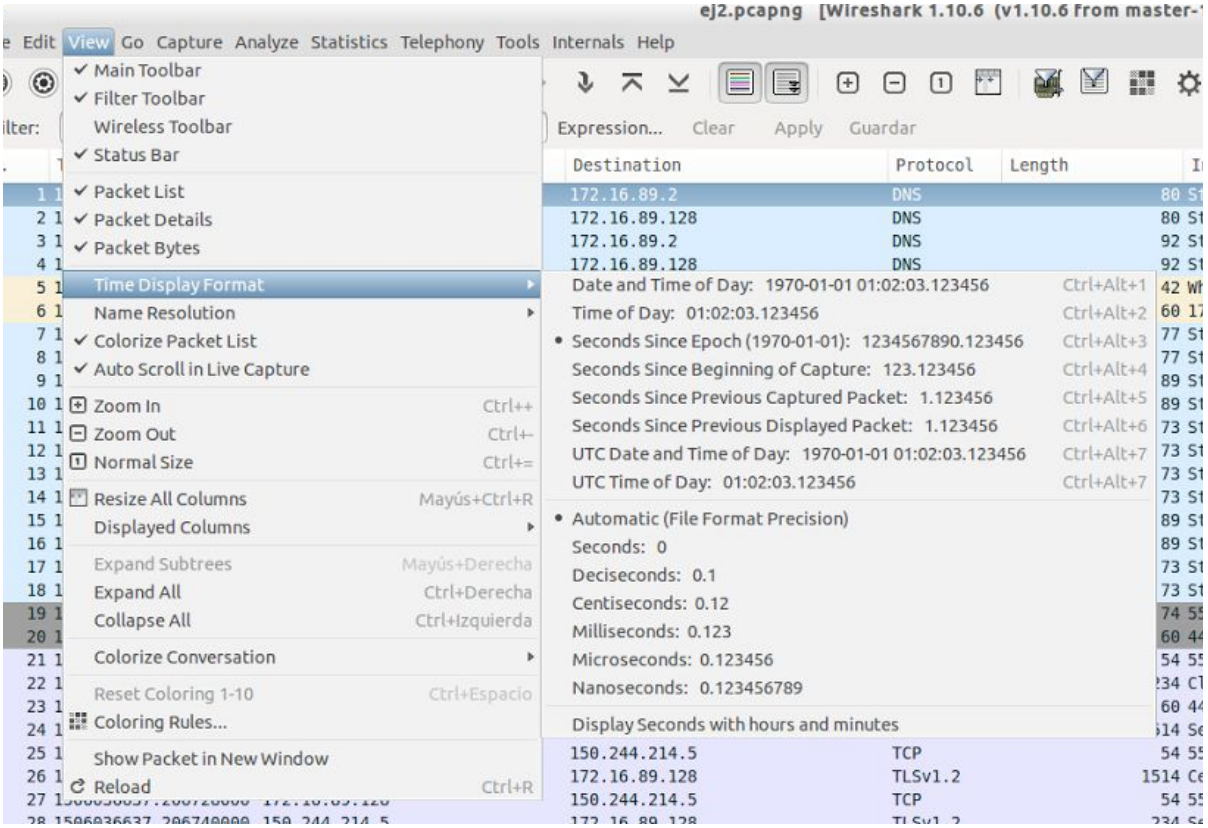
4. Modifique la forma en que Wireshark muestra la información en la columna 'Time' de cada paquete. En concreto muestre los tiempos en formato para humanos, y en tiempo Unix con resolución en segundos. Explique brevemente los pasos realizados.

Para conseguir que la columna Time muestre tiempo en formato humano, tenemos que hacer click en View->time Display Format. Seleccionamos Date and Time of Day y así cambiamos el tipo de la columna. Comprobamos que efectivamente se ve el tiempo en formato humano, así que abrimos de nuevo el fichero ej2.pcapng y observamos la columna Time.



No.	Time	Source
1	2017-09-21 23:30:06.107989000	172.16.89.128
2	2017-09-21 23:30:06.137804000	172.16.89.2
3	2017-09-21 23:30:06.138543000	172.16.89.128
4	2017-09-21 23:30:06.145017000	172.16.89.2
5	2017-09-21 23:30:11.121791000	00:0c:29:62:47:b8
6	2017-09-21 23:30:11.122078000	00:50:56:e1:72:a4
7	2017-09-21 23:30:19.171436000	172.16.89.128
8	2017-09-21 23:30:19.185085000	172.16.89.2
9	2017-09-21 23:30:19.185820000	172.16.89.128
10	2017-09-21 23:30:19.189316000	172.16.89.2
11	2017-09-21 23:30:28.279764000	172.16.89.128
12	2017-09-21 23:30:28.279956000	172.16.89.128
13	2017-09-21 23:30:33.281124000	172.16.89.128
14	2017-09-21 23:30:33.281439000	172.16.89.128
15	2017-09-21 23:30:37.114075000	172.16.89.2
16	2017-09-21 23:30:37.114090000	172.16.89.2

Para conseguir que la columna Time muestre tiempo en formato humano, tenemos que hacer click en View->time Display Format. Seleccionamos Seconds since Epoch y así cambiamos el tipo de la columna. Comprobamos que efectivamente se ve el tiempo en tiempo Unix con resolución en segundos, así que abrimos de nuevo el fichero ej2.pcapng y observamos la columna Time.



No.	Time	Source	Destination
1	1506036606.107989000	172.16.89.128	172.16.89.2
2	1506036606.137804000	172.16.89.2	172.16.89.128
3	1506036606.138543000	172.16.89.128	172.16.89.2
4	1506036606.145017000	172.16.89.2	172.16.89.128
5	1506036611.121791000	00:0c:29:62:47:b8	00:50:56:e1:72:a4
6	1506036611.122078000	00:50:56:e1:72:a4	00:0c:29:62:47:b8
7	1506036619.171436000	172.16.89.128	172.16.89.2
8	1506036619.185085000	172.16.89.2	172.16.89.128
9	1506036619.185820000	172.16.89.128	172.16.89.2
10	1506036619.189316000	172.16.89.2	172.16.89.128
11	1506036628.279764000	172.16.89.128	172.16.89.2
12	1506036628.279956000	172.16.89.128	172.16.89.2
13	1506036633.281124000	172.16.89.128	172.16.89.2

5. Inicie una captura en Wireshark pero aplicando filtros de captura, en concreto solo queremos capturar tráfico UDP. Mientras captura tráfico, genere durante algunos instantes tráfico a partir de la visualización de páginas web, y ejecute al mismo tiempo en una consola el comando $ sudo hping3 -S -p 80 www.uam.es. Compruebe que solo se capturan paquetes UDP, y describa brevemente los pasos realizados.

Hacemos click en el icono de configuración de la captura de tráfico y ahí en Capture Filter aplicamos el filtro ‘UDP’ de manera que los paquetes captados de Ethernet sean todos de ese tipo.