Ejercicios Wireshark

[1. Ejercicio 1 2](#_Toc527554759)

[2. Ejercicio 2 4](#_Toc527554760)

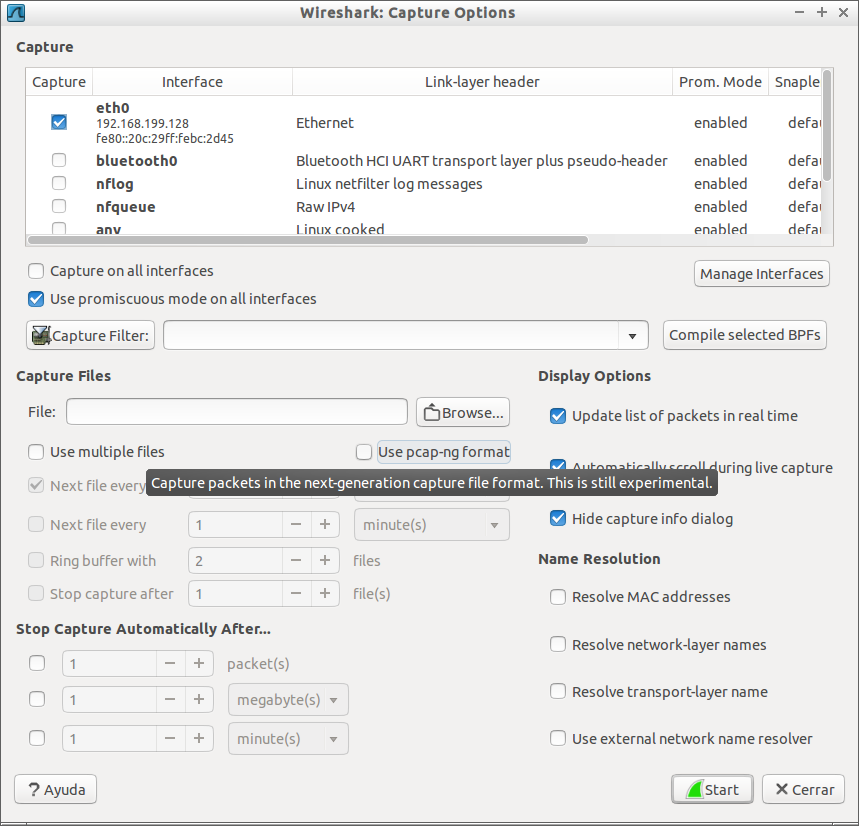
[3. Ejercicio 3 5](#_Toc527554761)

[4. Ejercicio 4 6](#_Toc527554762)

[5. Ejercicio 5 7](#_Toc527554763)

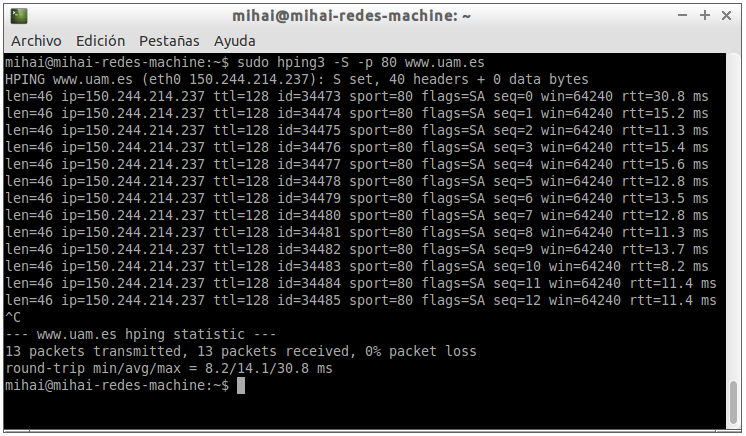
# Ejercicio 1

Ejecutamos *Wireshark* como superusuario y configuramos la captura de tráfico; seleccionamos la interfaz *eth0*, deshabilitamos todas las opciones de *Name Resolution* y desmarcamos la opción “u*se pcap-ng format”* para poder guardar la captura en el formato *pcap*.

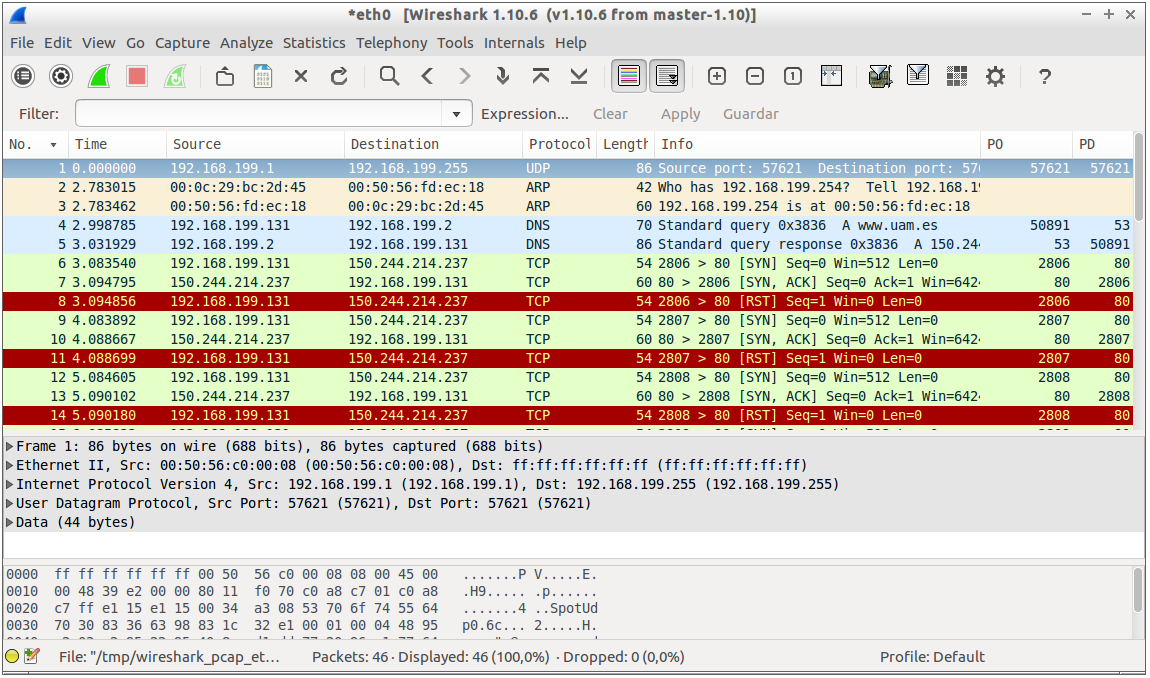


Iniciamos la captura haciendo Click en *Start* y a continuación abrimos otra consola y ejecutamos durante unos segundos el siguiente comando

**$ sudo** hping3 -S -p 80 www.uam.es

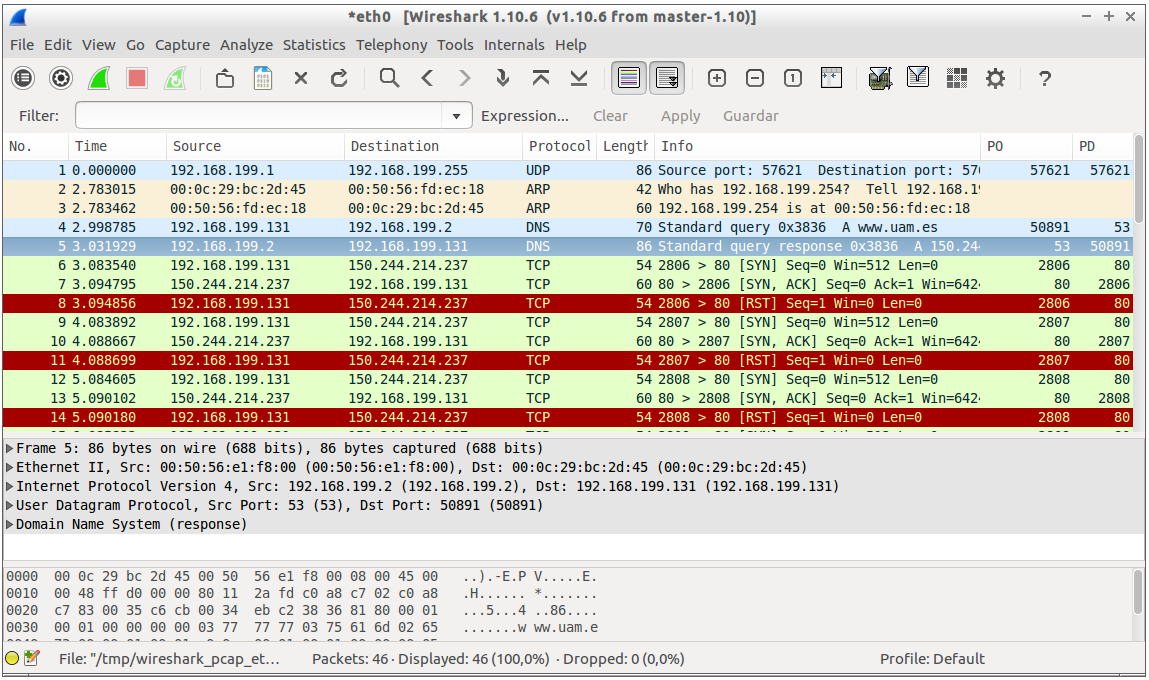


Volvemos a la ventana de *Wireshark*, paramos la captura pulsando *Stop* y analizamos los paquetes que aparecen.



Como podemos ver en la imagen podemos dividir la ventana en tres partes en función de la información que nos proporciona. La parte superior muestra un listado con los paquetes que hayamos capturado, la siguiente parte hacia abajo nos muestra una decodificación del paquete seleccionado con los campos que Wireshark conoce, por último, la parte inferior nos muestra el volcado hexadecimal de ese mismo paquete.

A continuación, guardamos la captura en un archivo *pcap* (File > Save) para después abrirlo (File > Open) y ordenarlo por el campo PO contando los paquetes con el puerto origen 53 (un solo paquete).



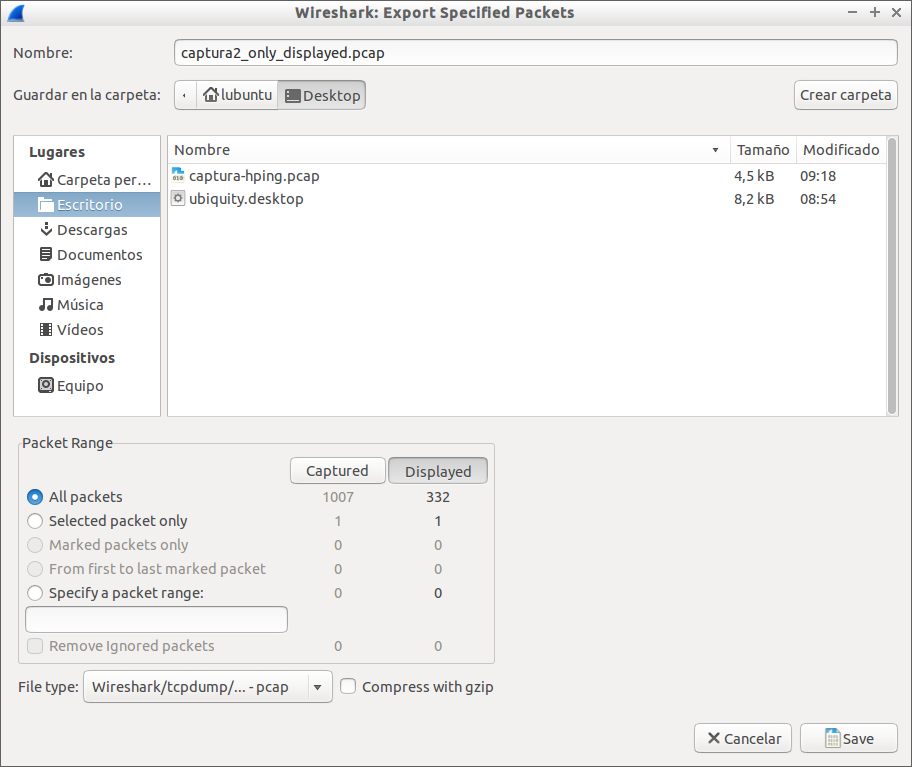
# Ejercicio 2

* 1. El filtro que hemos usado es:

ip **&&** frame**.**len **>** 1000

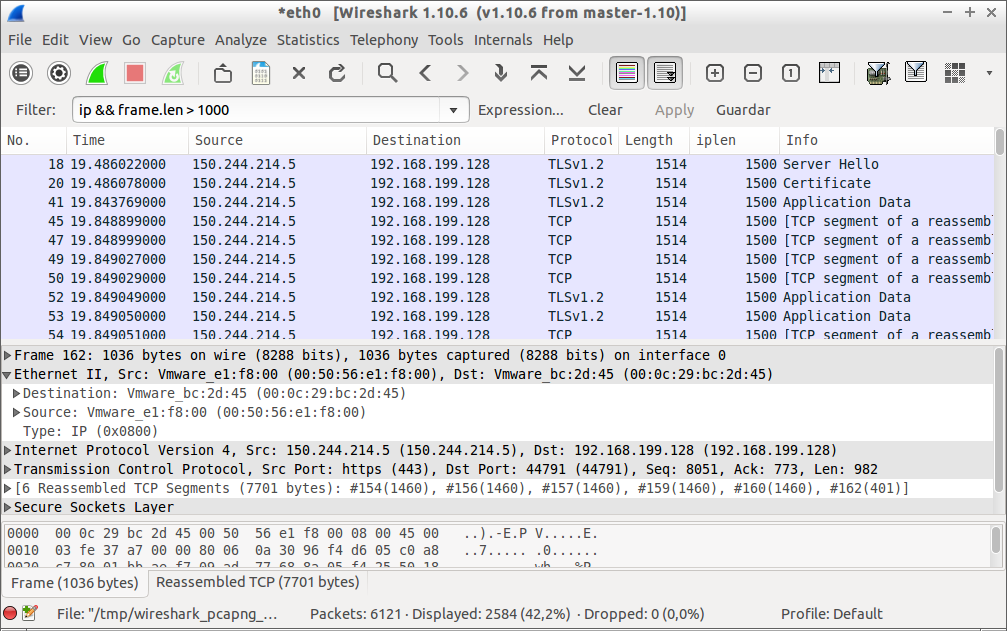
De esta forma podemos filtrar los paquetes que tengan un protocolo IP y cuyo peso sea superior a 1000Bytes.

* 1. Para guardar solo los paquetes visibles hemos usado la opción *File>Export Specified Packets* y seleccionando los paquetes mostrados.



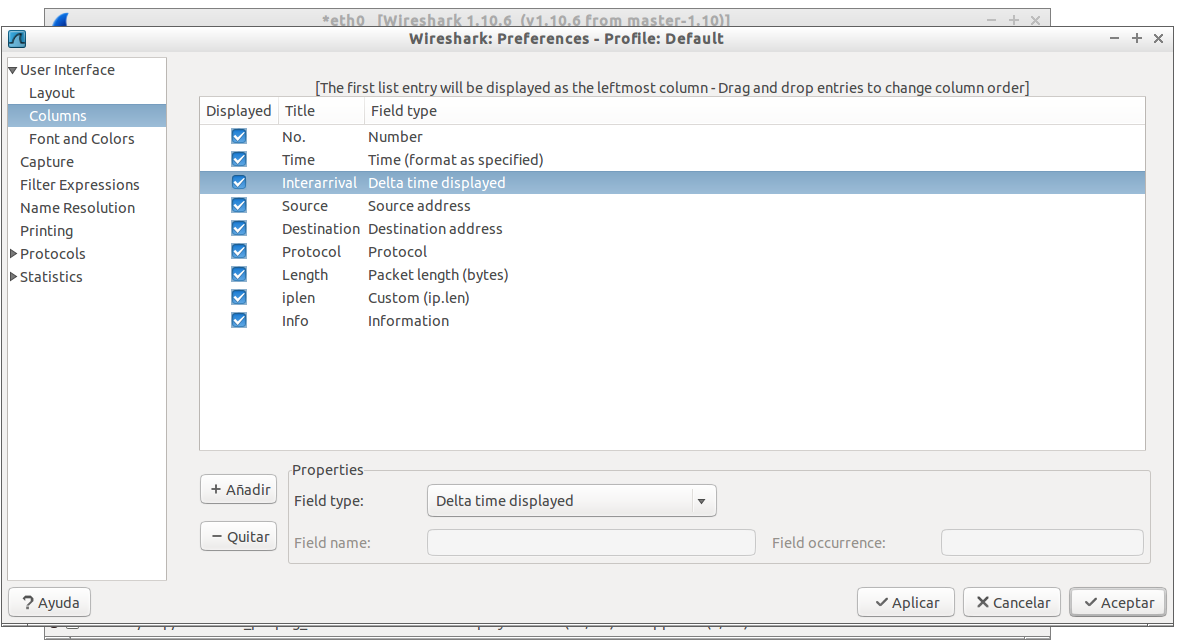
Cuando guardamos usando esta opción descubrimos que se guardaban paquetes de menos de 1000Bytes. Buscando información descubrimos que esto se debe a que *Wireshark* guarda todas las demás *frames* necesarias para la reconstrucción de toda la información de los paquetes mostrados. *Fuentes:* [*Link 1*](https://ask.wireshark.org/question/3077/displayed-packets-counter-differs-between-bottom-right-corner-and-file-export-specified-packets/)[*Link 2*](https://osqa-ask.wireshark.org/questions/53541/export-packets-saves-more-packets-than-displayed)[*Link 3*](https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=7667)[*Link 4*](https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12760)

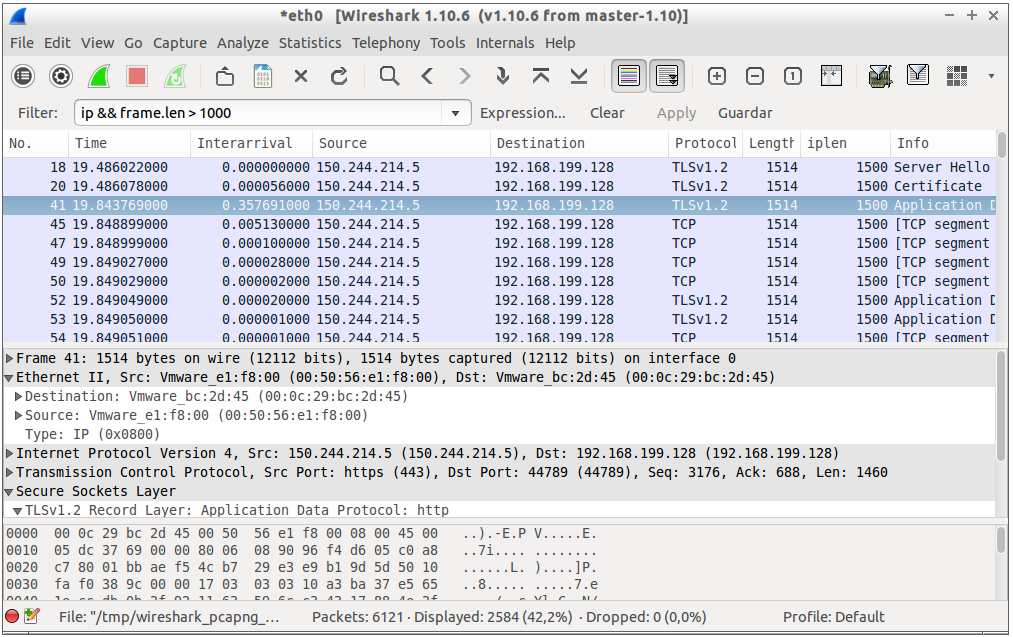
2.3. Añadiendo una nueva columna para la longitud del paquete IP podemos observar que la diferencia entre las dos longitudes es siempre de 14Bytes que es el tamaño de la cabecera Ethernet. También en nuestro caso los primeros 5 paquetes IP tienen el mismo tamaño, 1500Bytes que corresponde con la unidad máxima de transferencia (MTU) de Ethernet.



# Ejercicio 3

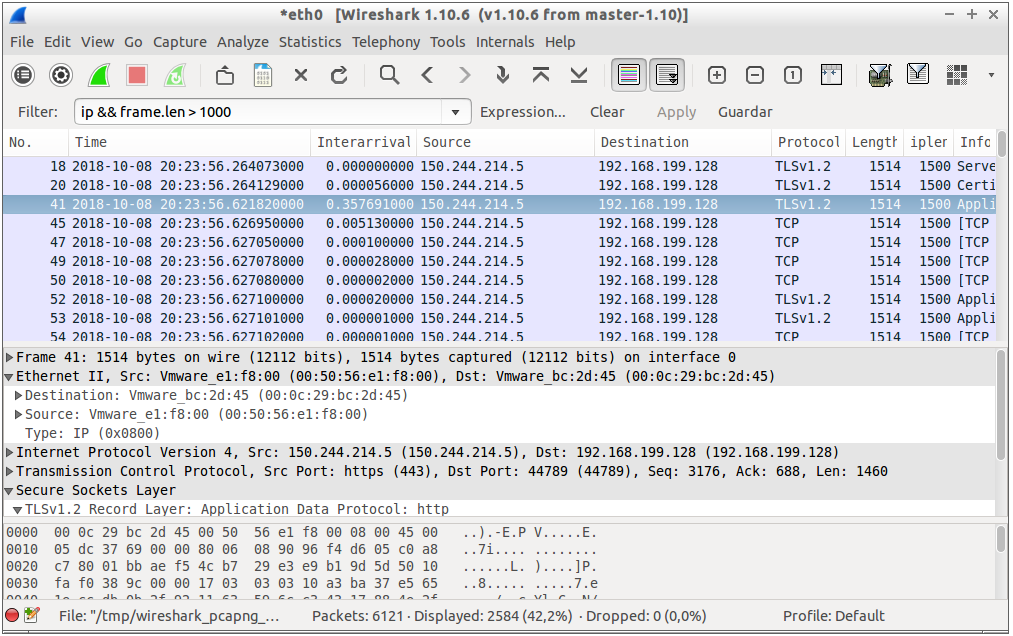
Vamos a Edit > Preferences y después seleccionamos columns. Pulsamos añadir, cambiamos el titulo de la columna a Interarrival, al campo Field Type le asignamos el valor Delta Time Displayed y aplicamos lo cambios. A continuación, tenemos que volver a entrar nuevo en Edit > Preferences > Columns y marcar la columna otra vez, aunque ya estaba activa (esto parece ser un bug en esa versión de Wireshark).



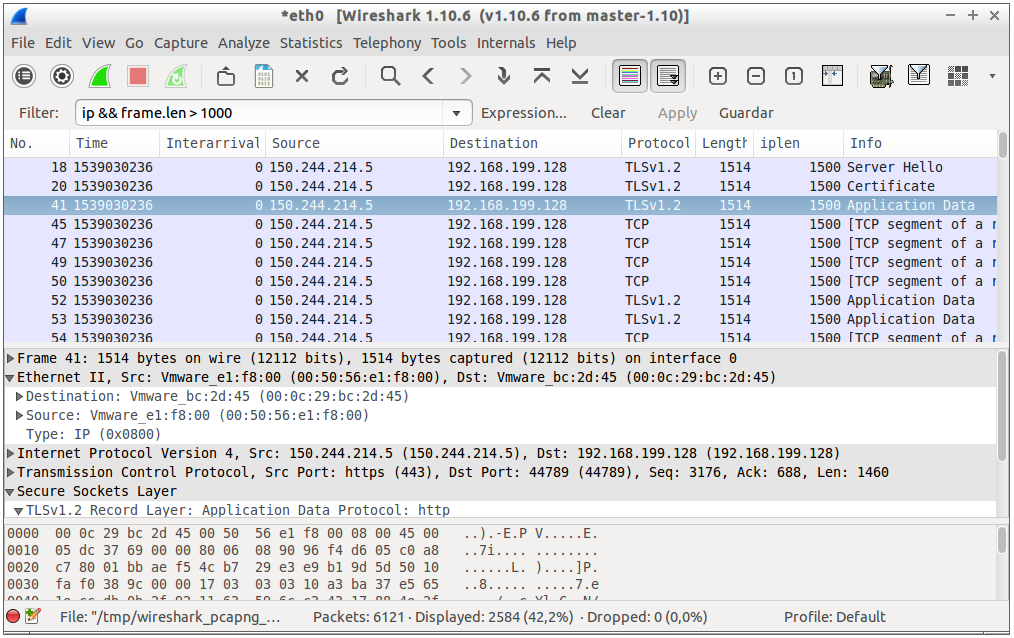


# Ejercicio 4

Para ver el tiempo en formato humano seleccionamos en la barra de herramientas View > Time Display Format > Date and Time of Day

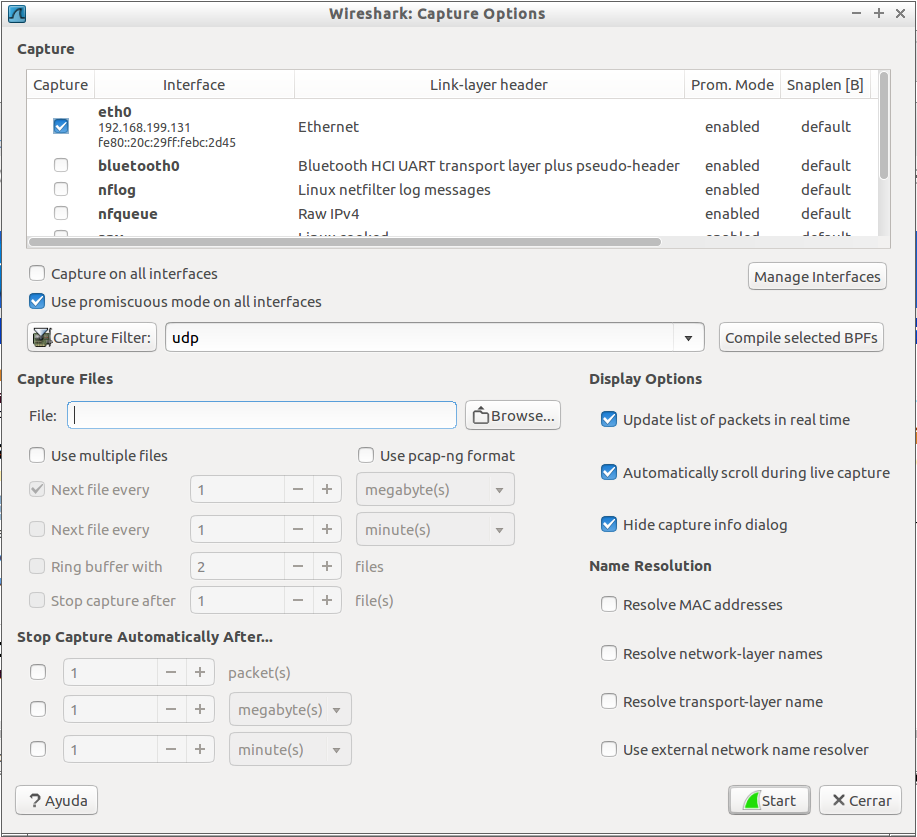


Para cambiar el formato a tiempo UNIX con resolución en segundos en la barra de herramientas seleccionamos View > Time Display Format > Seconds since Epoch y para cambiar la resolución View > Time Display Format > Seconds.



# Ejercicio 5

Al igual que en las capturas anteriores aplicamos el filtro de captura ***udp*** y desmarcamos todas las opciones de *Name Resolution*, de esta forma capturaremos paquetes con este protocolo.



Como podemos ver en la imagen hemos capturado paquetes DNS, NTP y DHCP, protocolos que funcionan sobre el protocolo de transporte UDP.

