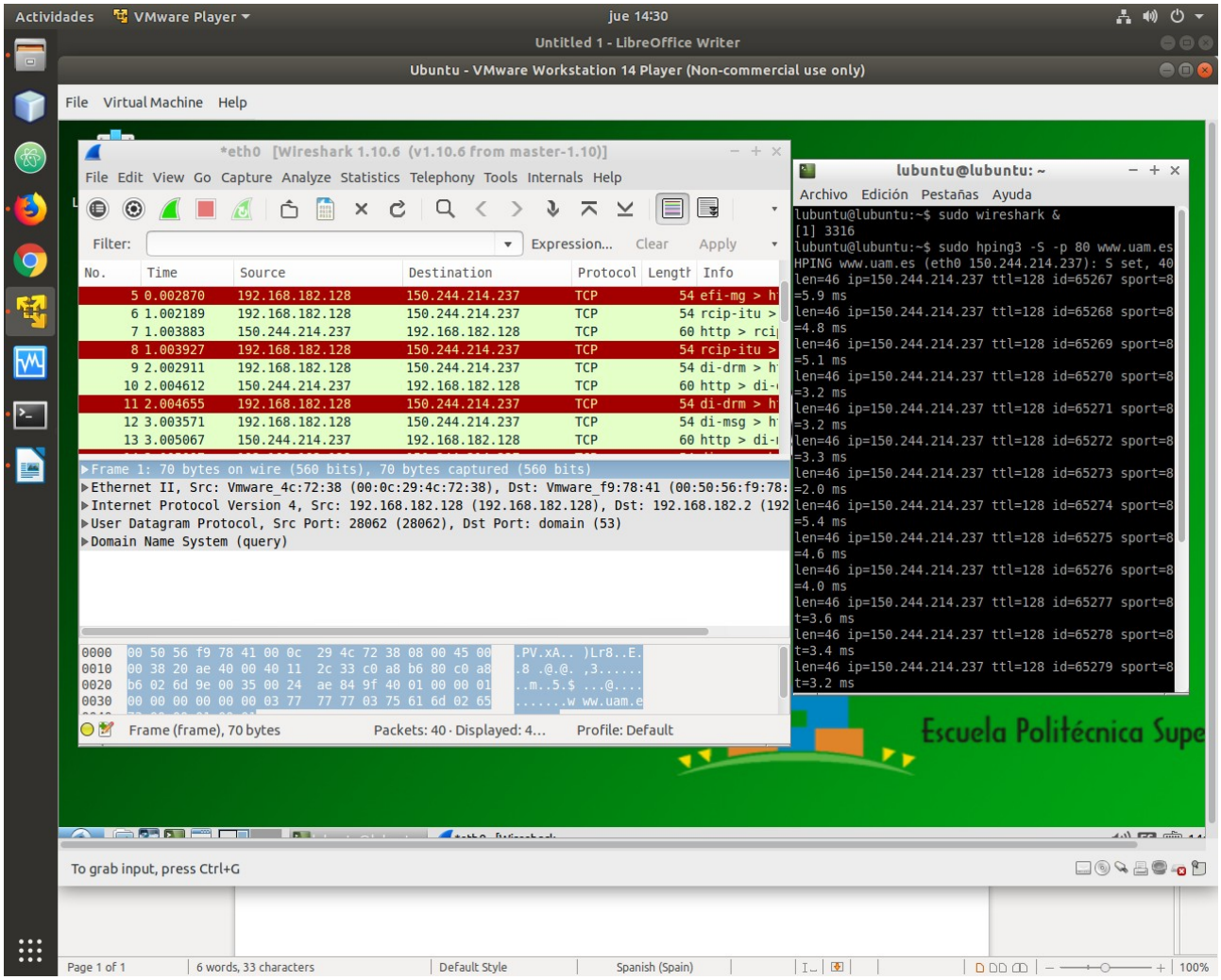
Práctica 1: Ejercicios de captura de tráfico
Autores: Nicolás Wolyniec & Cristina Soria
Grupo: 1362

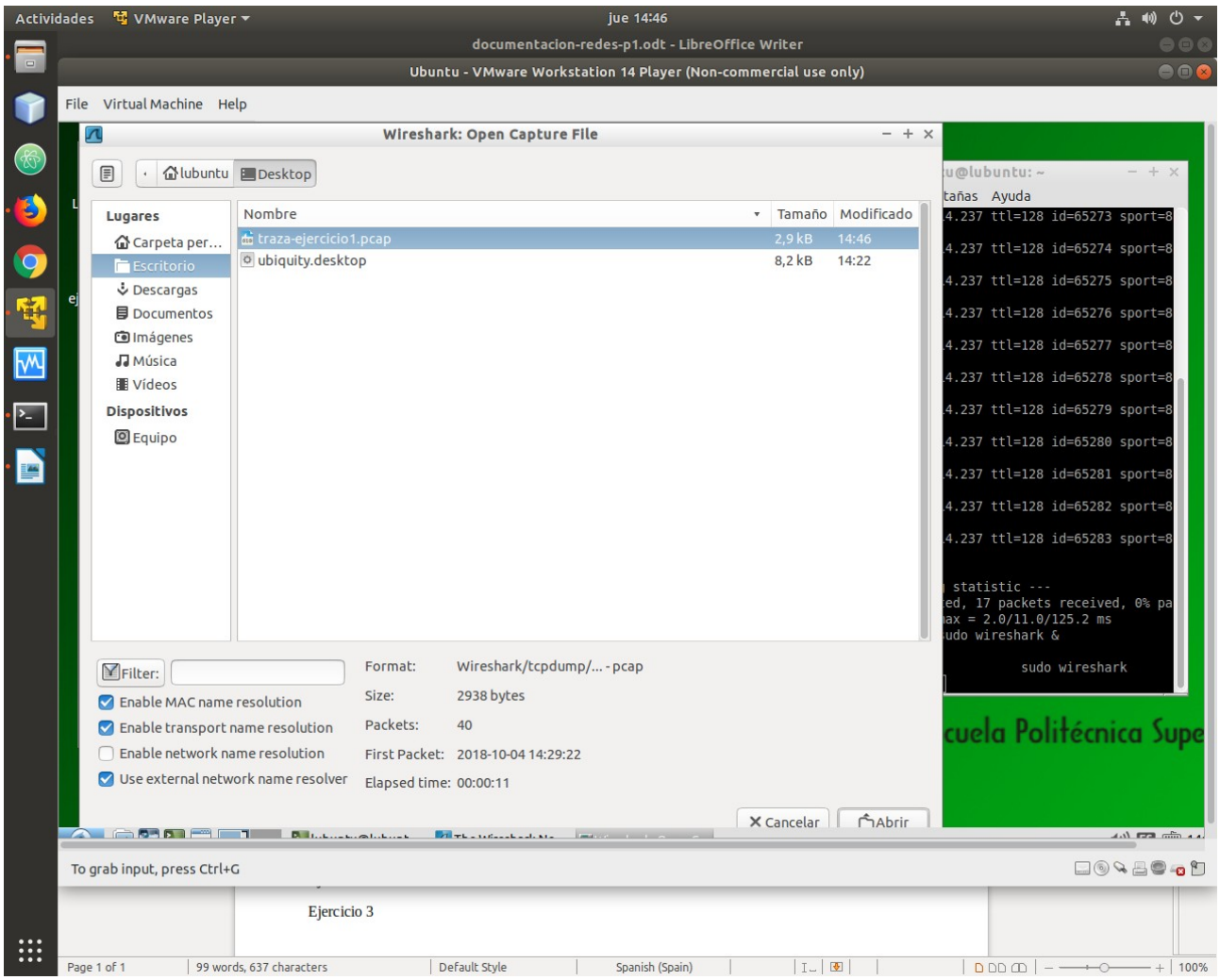
Ejercicio 1
Tras abrir wireshark, configurar el interfaz por el que capturaremos tráfico (eth0) y realizar 'sudo hping3 -S -p 80 www.uam.es' obtenemos lo siguiente:



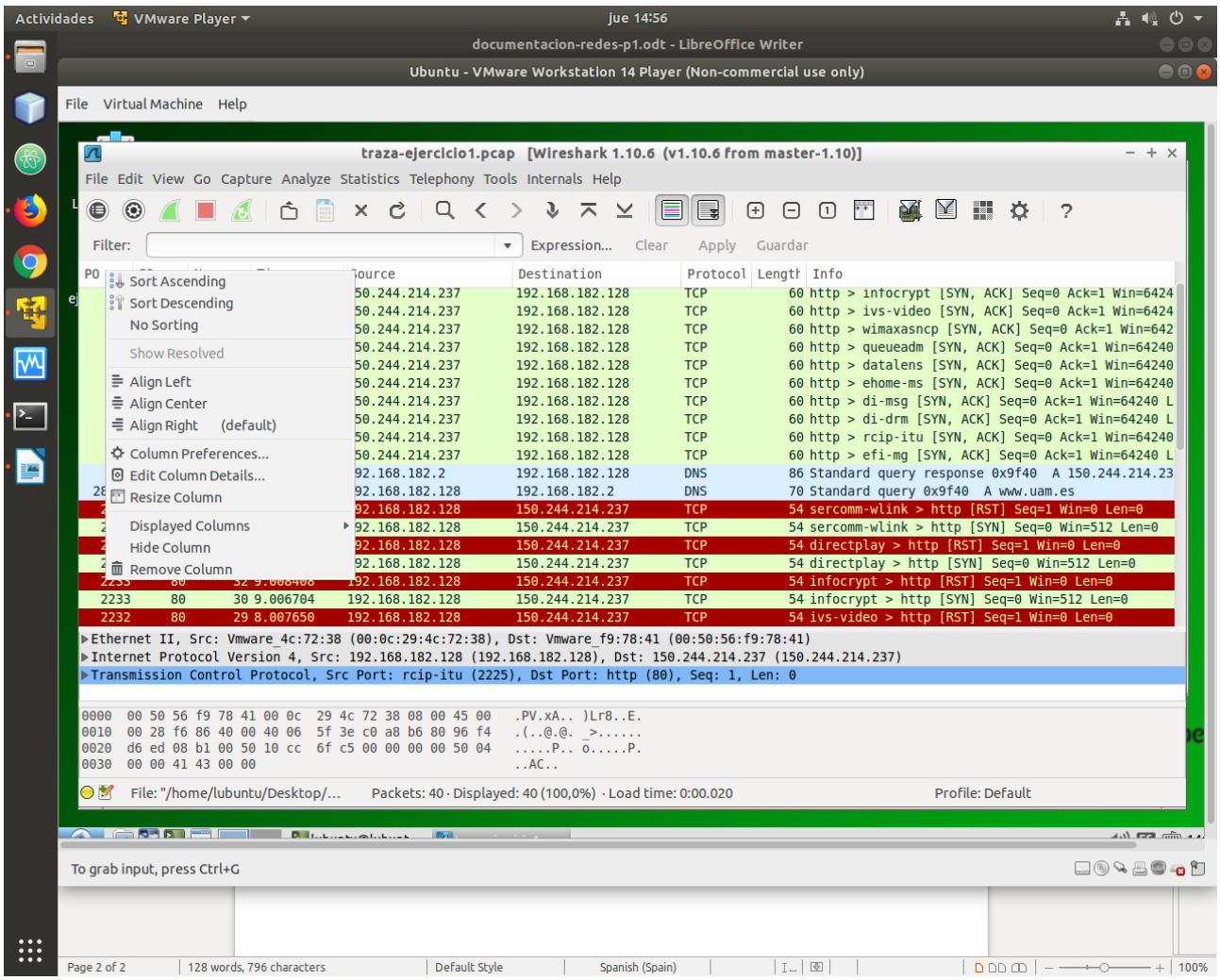
Podemos dividir la pantalla en tres partes.

- Parte arriba: muestra los paquetes capturados. Aquí podemos mirar la el menu-bar donde nos encontramos con el tipo de protocolo, origen, destino, tiempo y tamaño.
- Parte central: muestra la decodificacion que realiza wireshark sobre el paquete seleccionado en la parte de arriba.
- Parte abajo: muestra en hexadecimal el contenido del paquete seleccionado en la parte de arriba (bytes alineados en grupo de 16 siempre).

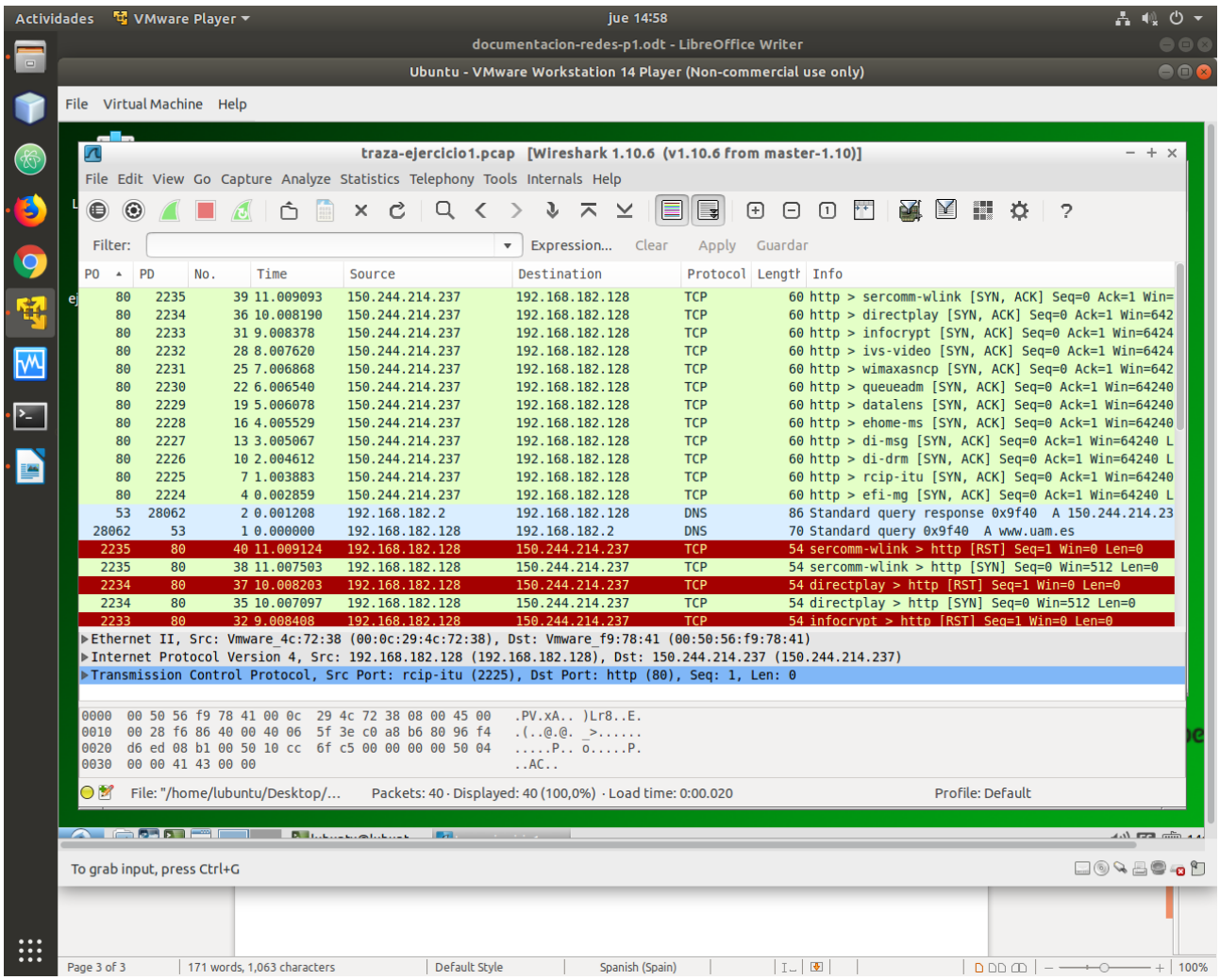
Una vez hemos salvado, cerramos wireshark y volvemos a abrirlo, esta vez en vez de realizar una captura en vivo, abrimos la traza guardada previamente.



Tras abrirlo vamos a configuración y añadimos las columnas PO y PD. Posteriormente ordenamos de forma descendente.



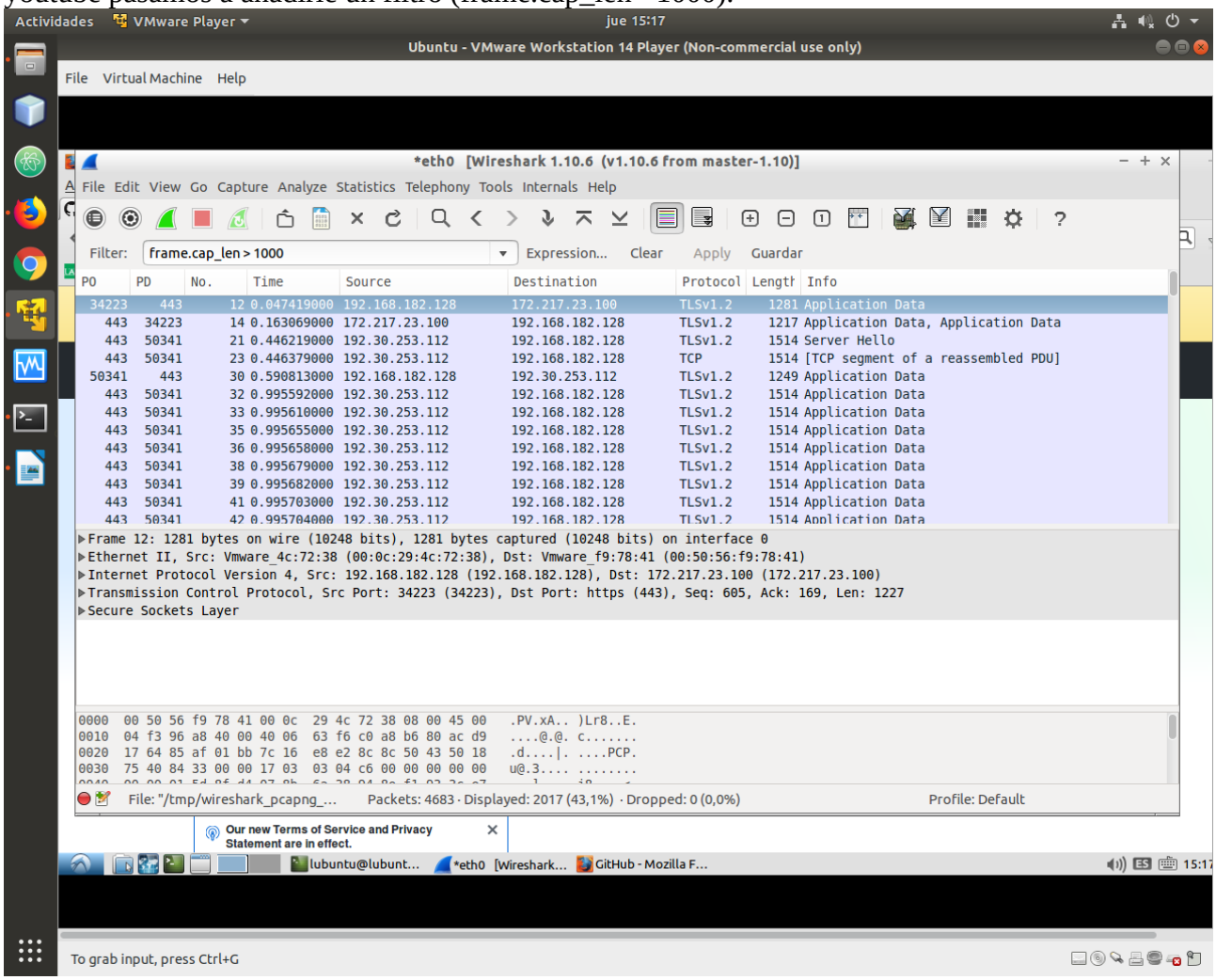
Al realizar vemos que los numeros no concuerdan. Esto se debe a que wireshark ordena por categorias y dentro de ellas está ordenado de forma descendente.



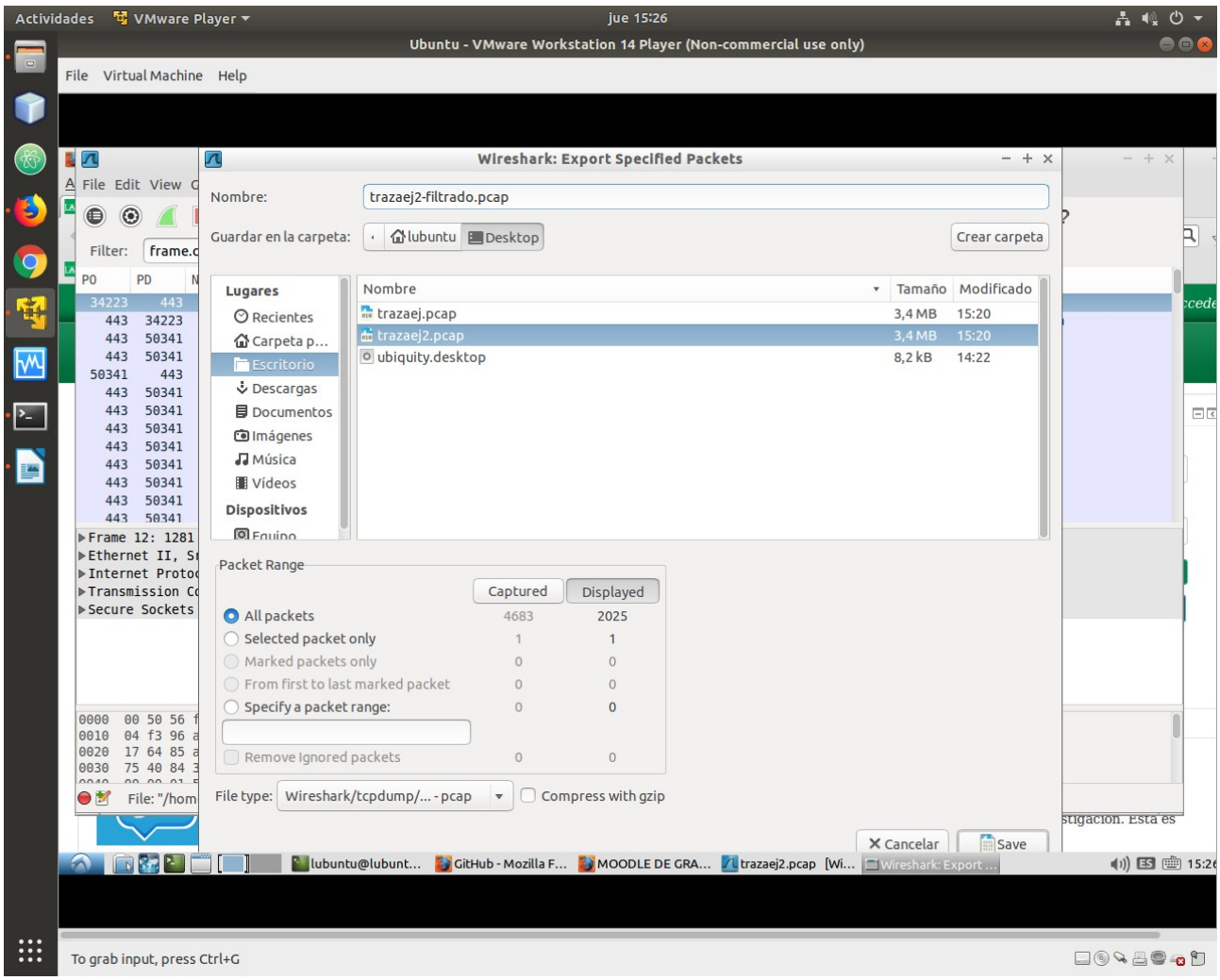
Podemos observar que hay una petición del puerto 53 al 28862 (cuando realizamos sudo hping3 -S -p 80 www.uam.es). También podemos ver la respuesta proporcionada por 28862 a 53 en la línea de abajo.

Ejercicio 2

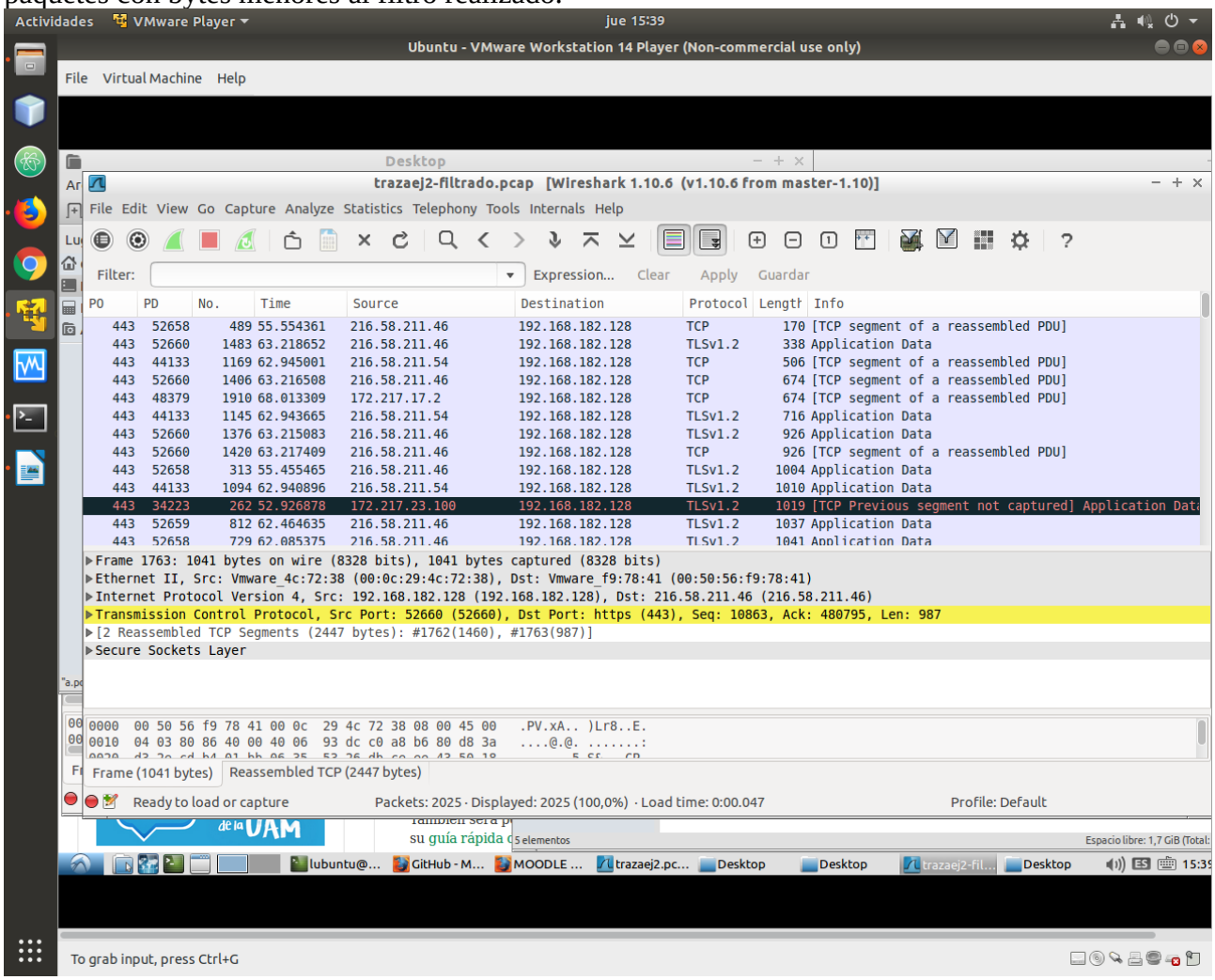
Tras realizar una nueva captura de paquetes en vivo y crear un poco de tráfico abriendo github y youtube pasamos a añadirle un filtro (frame.cap_len >1000).



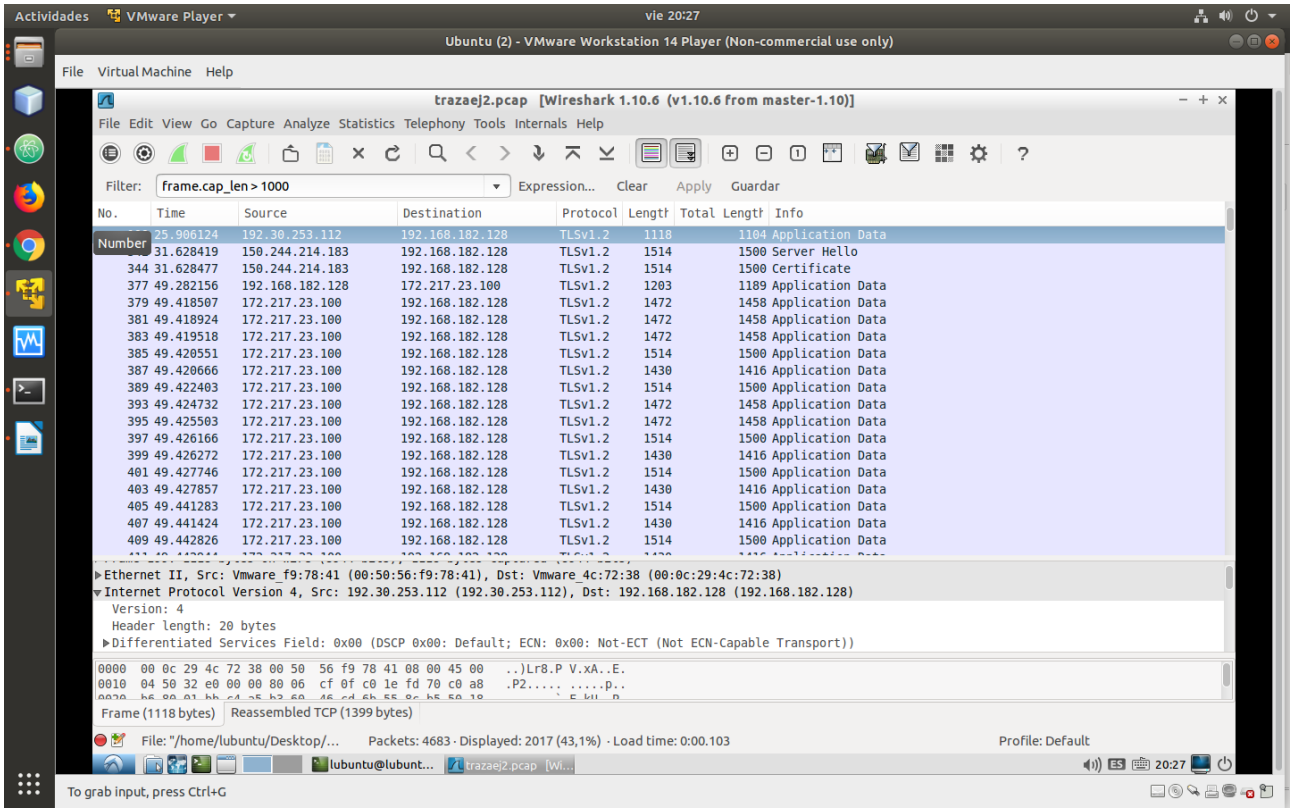
Si queremos guardar solo los paquetes en los que se realiza el filtrado debemos ir a file→export specified packet y nos aparece la siguiente pantalla. Tras esto podemos guardar la traza completa o la parte filtrada(teniendo seleccionado en packed range ‘displayed’).


Actividades
VMware Player
jue 15:26
Ubuntu - VMware Workstation 14 Player (Non-commercial use only)
File Virtual Machine Help
Wireshark: Export Specified Packets
Nombre: trazaej2-filtrado.pcap
Guardar en la carpeta: lubuntu Desktop
Crear carpeta
Lugares
Recientes
Carpeta p...
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
Dispositivos
Equipo
Nombre
Tamaño
Modificado
trazaej.pcap 3,4 MB 15:20
trazaej2.pcap 3,4 MB 15:20
ubiquity.desktop 8,2 kB 14:22
Packet Range
Captured
Displayed
All packets 4683 2025
Selected packet only 1 1
Marked packets only 0 0
From first to last marked packet 0 0
Specify a packet range: 0 0
Remove Ignored packets 0 0
File type: Wireshark/tcpdump/... - pcap
Compress with gzip
Cancelar
Save
To grab input, press Ctrl+G

Hemos observado que al abrir la nueva traza aunque se ha realizado el filtrado aparecen unos paquetes con bytes menores al filtro realizado.



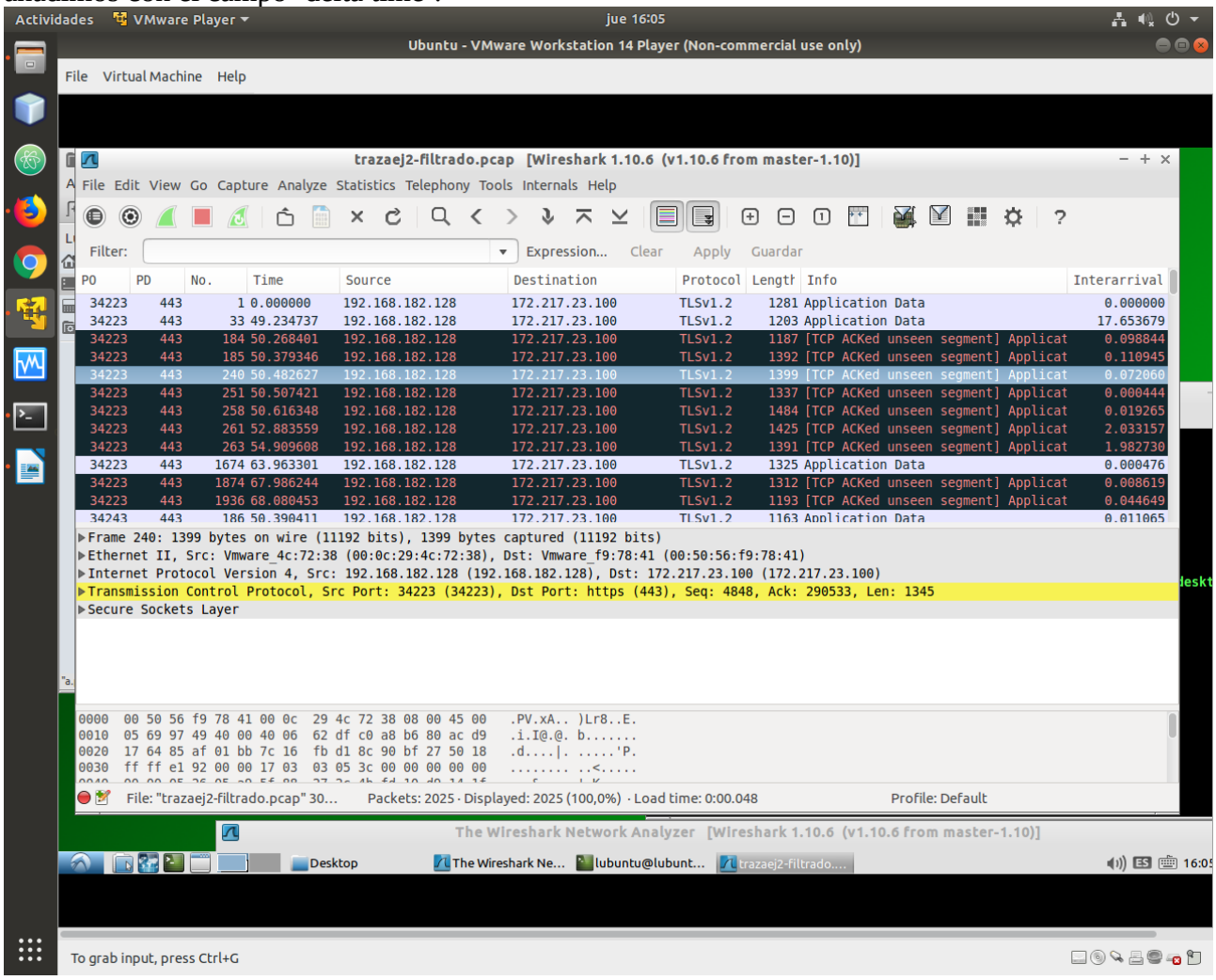
Seguimos con la traza filtrada por paquetes capturados cuyo tamaño sea mayor a 1000 bytes y miramos tanto el tamaño del paquete como el campo tamaño del protocolo IP. Podemos observar que ahora el tamaño se reduce ya que no se está teniendo en cuenta los 14 bytes de la cabecera de ethernet.



El tamaño de la IP lo podemos visualizar en la columna ‘Total Length’.

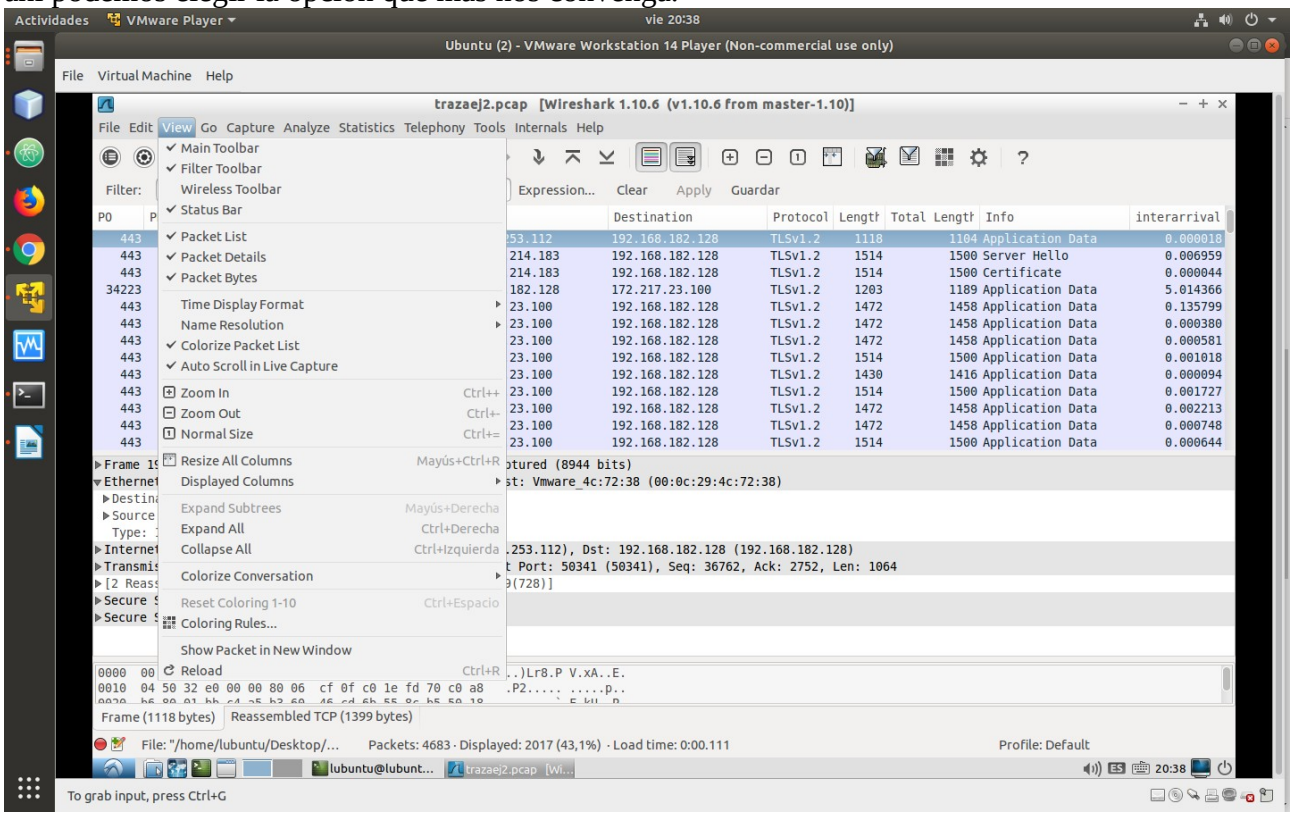
Ejercicio 3

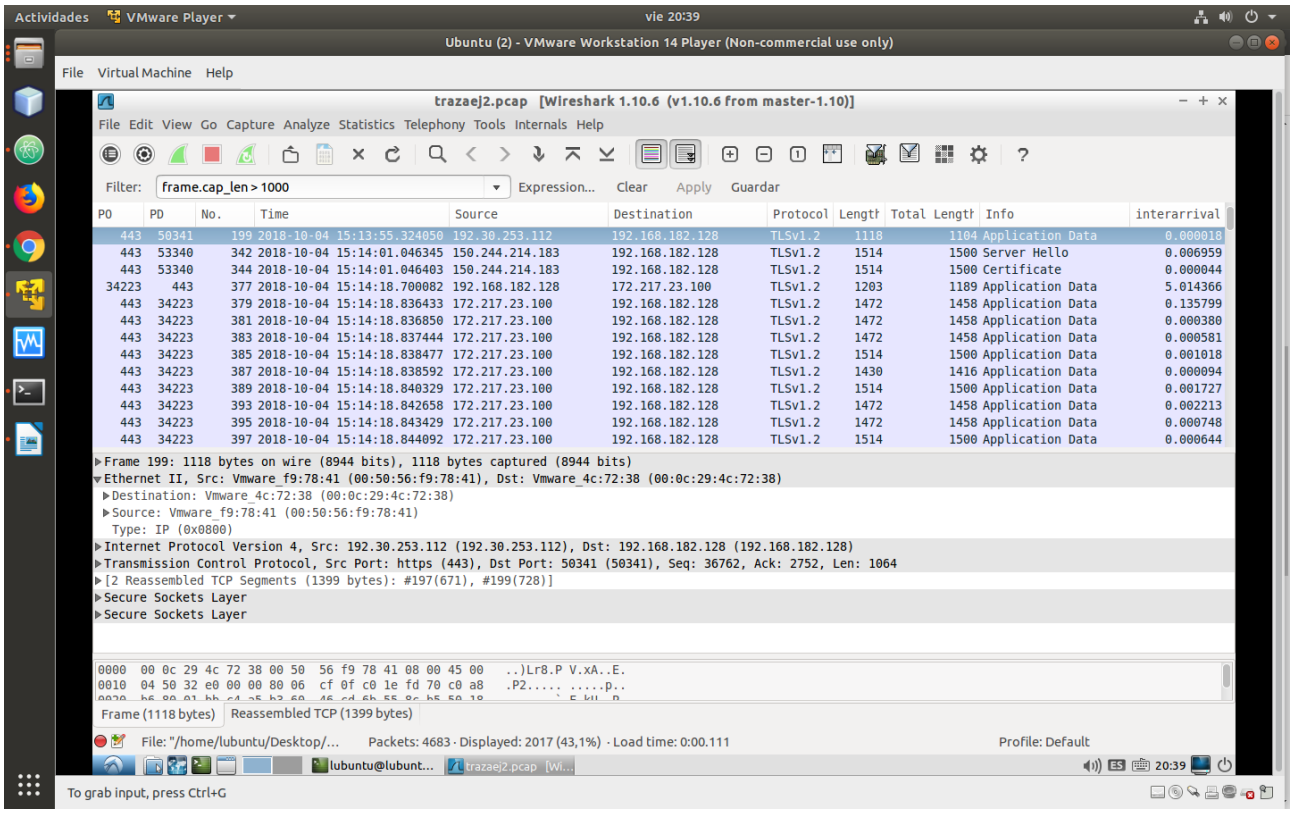
En este apartado, tener en cuenta que al querer añadir una columna con ‘delta time’ necesitaremos ejecutar wireshark con sudo, en caso contrario no dejará añadir dicha columna.
Para añadir la columna interarrival vamos a edit preferences → user interface → columns y lo añadimos con el campo ‘delta time’.



Ejercicio 4

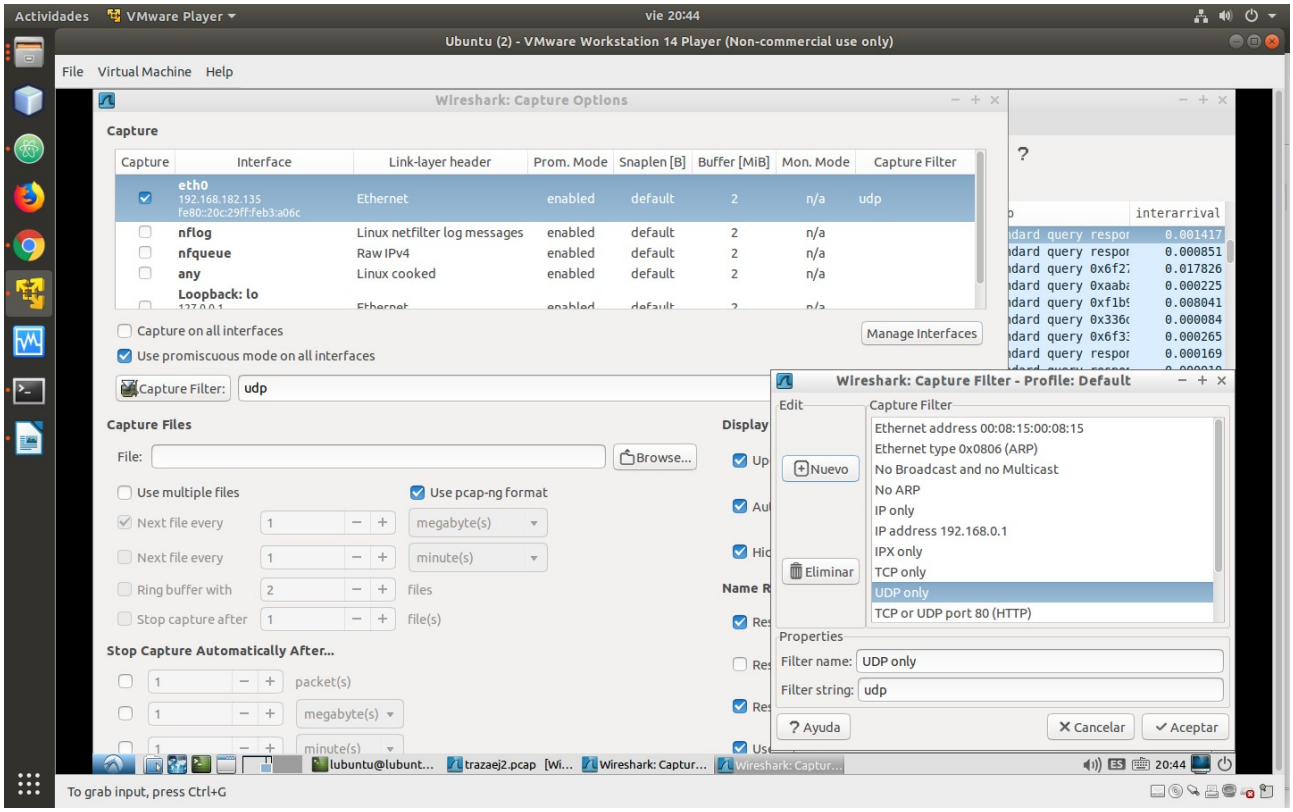
Para modificar la visualización de la columna ‘Time’ tenemos que ir a view → time display format y ahí podemos elegir la opción que más nos convenga.



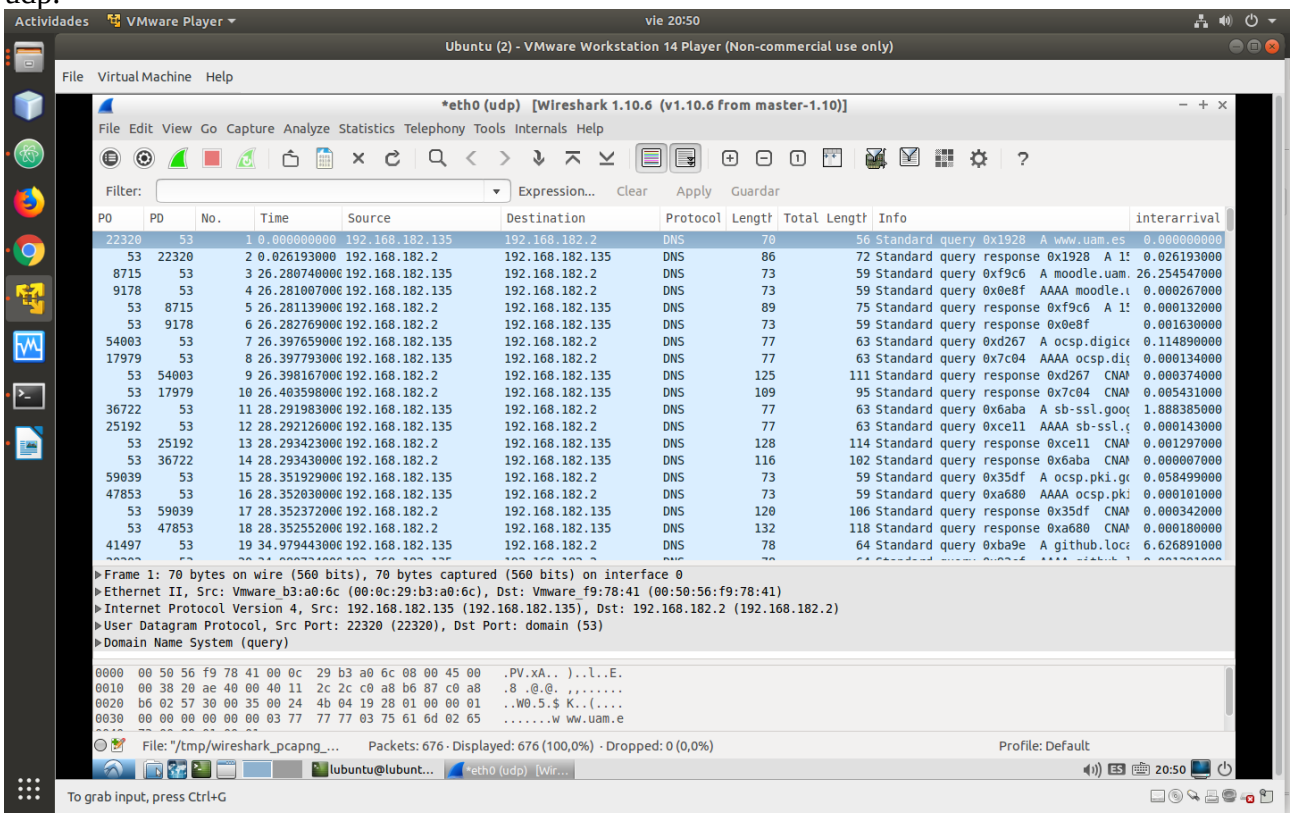


Ejercicio 5

Para este ejercicio hemos de ir a ‘show the caption option’ y en ‘capture filter’ añadimos UDP.



Una vez añadimos este filtro comenzamos la captura y podemos comprobar que solo hay paquetes udp.



Aqui vemos que todos los paquetes que se observan en la pantalla son paquetes UDP, pero si no estamos seguros podemos filtrar por ‘not udp’.