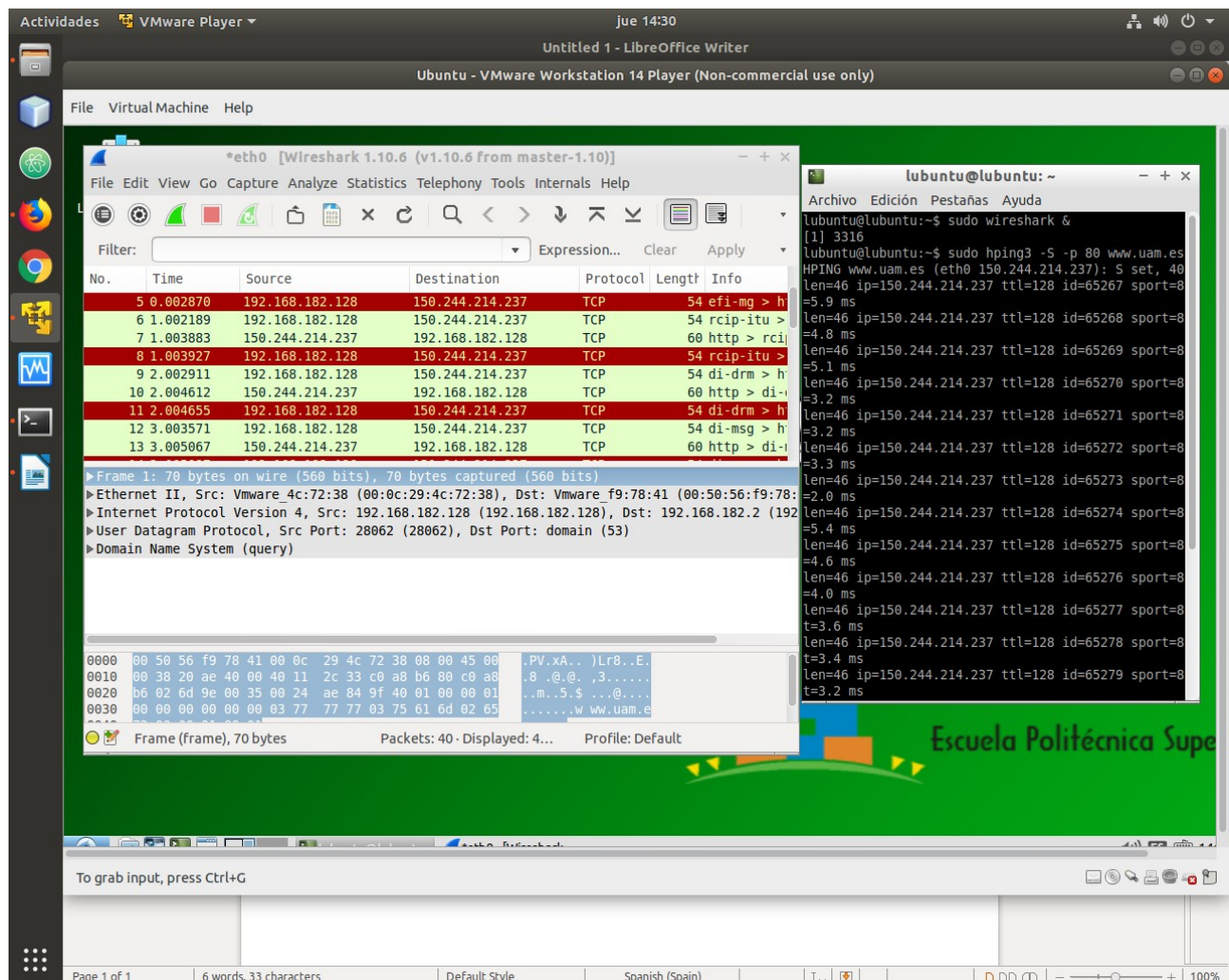


Práctica 1: Ejercicios de captura de tráfico

Autores: Nicolás Wolyniec & Cristina Soria
Grupo: 1362

Ejercicio 1

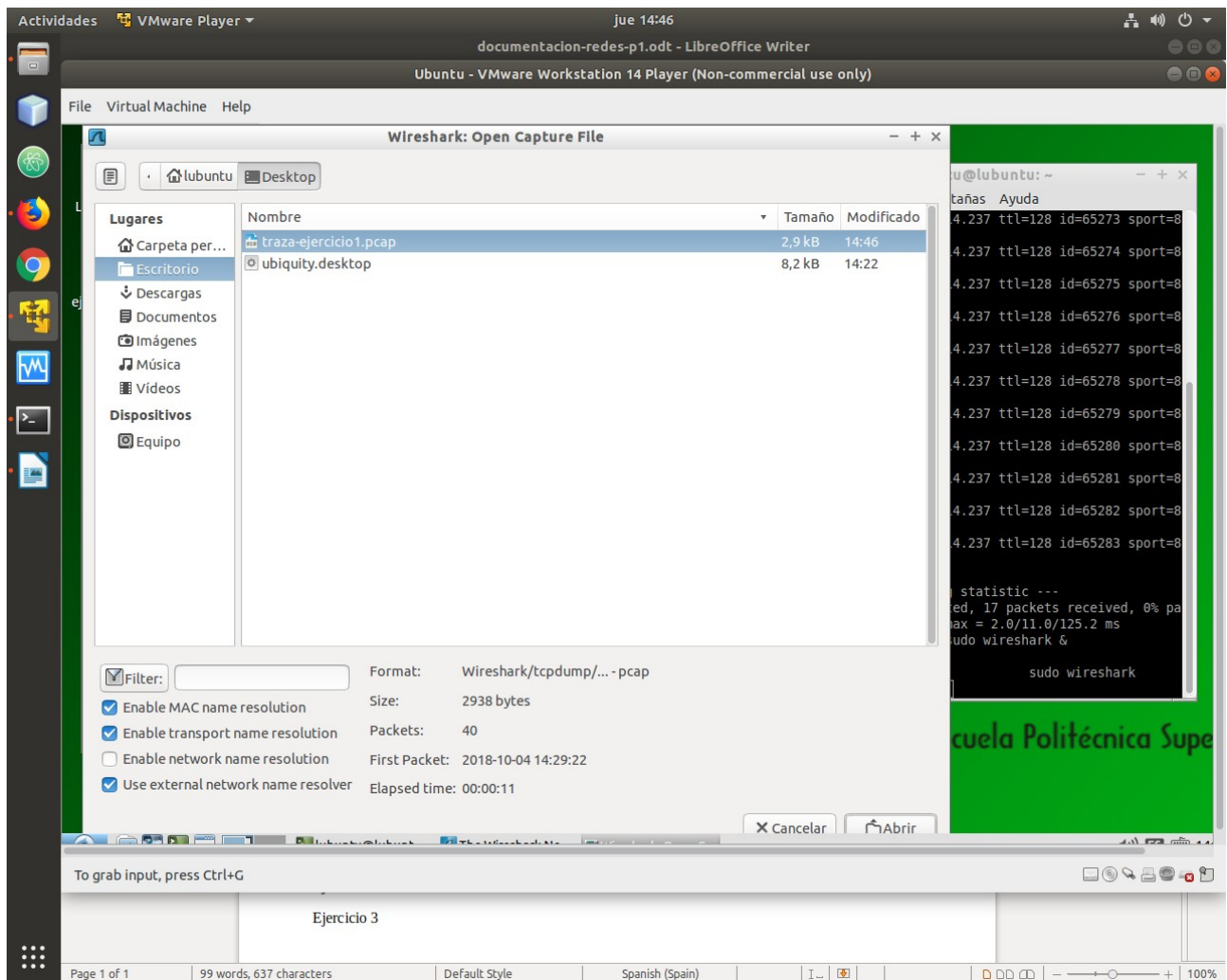
Tras abrir wireshark, configurar el interfaz por el que capturaremos tráfico (eth0) y realizar 'sudo hping3 -S -p 80 www.uam.es' obtenemos lo siguiente:



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 decodificación 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.

Actividades VMware Player Jue 14:56

documentacion-redes-p1.odt - LibreOffice Writer

Ubuntu - VMware Workstation 14 Player (Non-commercial use only)

File Virtual Machine Help

traza-ejercicio1.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Guardar

Sort Ascending
Sort Descending
No Sorting
Show Resolved
Align Left
Align Center
Align Right (default)
Column Preferences...
Edit Column Details...
Resize Column
Displayed Columns
Hide Column
Remove Column

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > infocrypt [SYN, ACK] Seq=0 Ack=1 Win=6424
2	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > ivs-video [SYN, ACK] Seq=0 Ack=1 Win=6424
3	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > wimaxsnpc [SYN, ACK] Seq=0 Ack=1 Win=642
4	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > queueadm [SYN, ACK] Seq=0 Ack=1 Win=64240
5	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > datalens [SYN, ACK] Seq=0 Ack=1 Win=64240
6	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > ehome-ms [SYN, ACK] Seq=0 Ack=1 Win=64240
7	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > di-msg [SYN, ACK] Seq=0 Ack=1 Win=64240 L
8	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > rcip-itu [SYN, ACK] Seq=0 Ack=1 Win=64240
9	0.000000	50.244.214.237	192.168.182.128	TCP	60	http > efi-mg [SYN, ACK] Seq=0 Ack=1 Win=64240 L
10	0.000000	92.168.182.2	192.168.182.128	DNS	86	Standard query response 0x9f40 A 150.244.214.23
11	0.000000	92.168.182.128	192.168.182.2	DNS	70	Standard query 0x9f40 A www.uam.es
12	0.000000	92.168.182.128	150.244.214.237	TCP	54	sercomm-wlink > http [RST] Seq=1 Win=0 Len=0
13	0.000000	92.168.182.128	150.244.214.237	TCP	54	sercomm-wlink > http [SYN] Seq=0 Win=512 Len=0
14	0.000000	92.168.182.128	150.244.214.237	TCP	54	directplay > http [RST] Seq=1 Win=0 Len=0
15	0.000000	92.168.182.128	150.244.214.237	TCP	54	directplay > http [SYN] Seq=0 Win=512 Len=0
16	0.000000	192.168.182.128	150.244.214.237	TCP	54	infocrypt > http [RST] Seq=1 Win=0 Len=0
17	0.000000	2233 80 30 9.006704	192.168.182.128	TCP	54	infocrypt > http [SYN] Seq=0 Win=512 Len=0
18	0.000000	2232 80 29 8.007650	192.168.182.128	TCP	54	ivs-video > http [RST] Seq=1 Win=0 Len=0

► Ethernet II, Src: Vmware_4c:72:38 (00:0c:29:4c:72:38), Dst: Vmware_f9:78:41 (00:50:56:f9:78:41)
 ► Internet Protocol Version 4, Src: 192.168.182.128 (192.168.182.128), Dst: 150.244.214.237 (150.244.214.237)
 ► Transmission Control Protocol, Src Port: rcip-itu (2225), Dst Port: http (80), Seq: 1, Len: 0

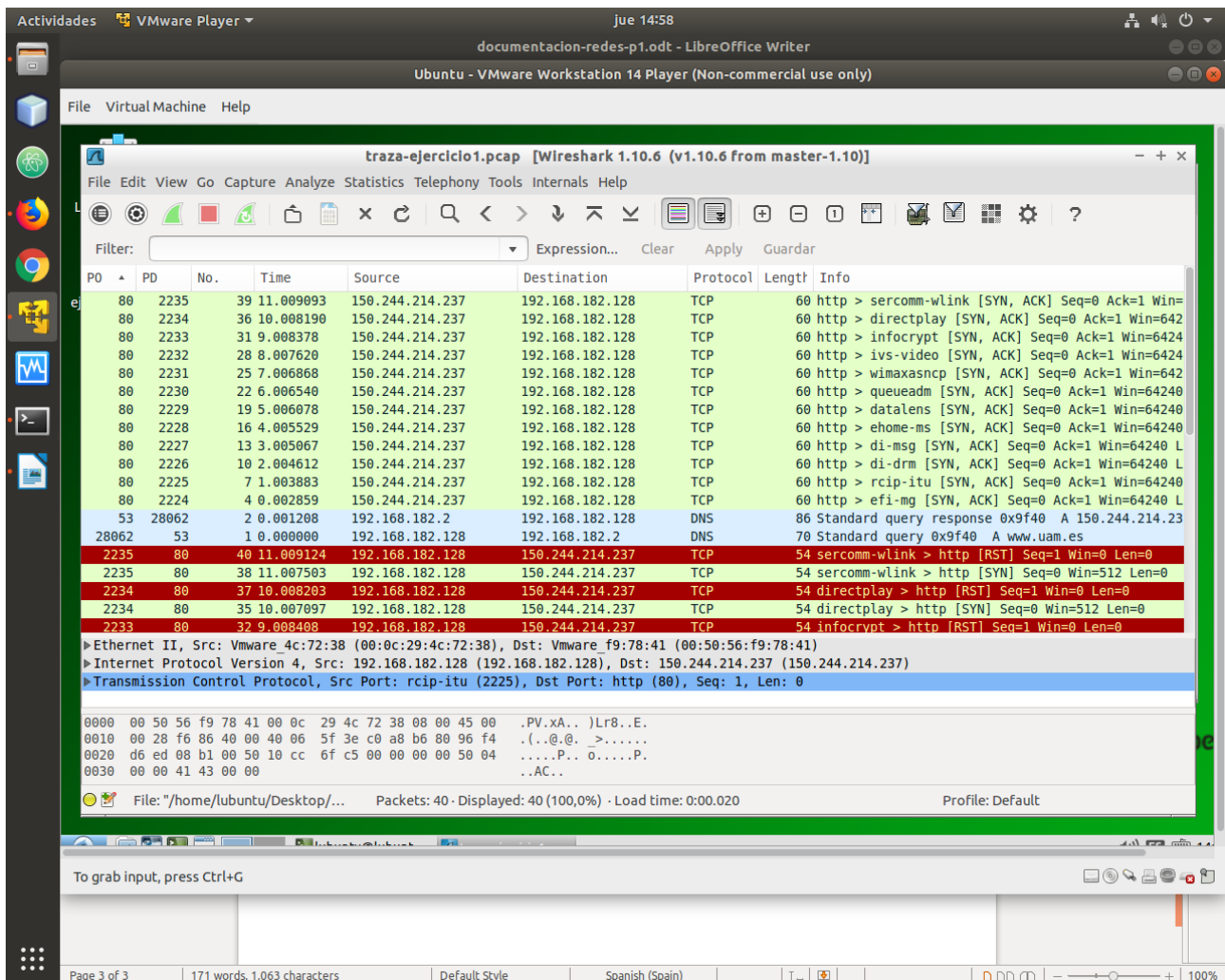
0000 00 50 56 f9 78 41 00 0c 29 4c 72 38 08 00 45 00 .PV.XA..)Lr8..E.
 0010 00 28 f6 86 40 00 00 06 5f 3e c0 a8 b6 80 96 f4 ..(.@.@. >.....
 0020 d6 ed 08 b1 00 50 10 cc 6f c5 00 00 00 00 50 04P. o.....P.
 0030 00 00 41 43 00 00 ..AC..

File: "/home/lubuntu/Desktop/... Packets: 40 · Displayed: 40 (100,0%) · Load time: 0:00.020 Profile: Default

To grab input, press Ctrl+G

Page 2 of 2 | 128 words, 796 characters | Default Style | Spanish (Spain) | I... | 100%

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).

The screenshot shows the Wireshark 1.10.6 interface. The filter bar at the top contains the expression `frame.cap_len > 1000`. The packet list pane displays a table of captured packets:

Pk	PD	No.	Time	Source	Destination	Protocol	Length	Info
34223	443	12	0.047419000	192.168.182.128	172.217.23.100	TLSv1.2	1281	Application Data
443	34223	14	0.163069000	172.217.23.100	192.168.182.128	TLSv1.2	1217	Application Data, Application Data
443	50341	21	0.446219000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Server Hello
443	50341	23	0.446379000	192.30.253.112	192.168.182.128	TCP	1514	[TCP segment of a reassembled PDU]
50341	443	30	0.590813000	192.168.182.128	192.30.253.112	TLSv1.2	1249	Application Data
443	50341	32	0.995592000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	33	0.995610000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	35	0.995655000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	36	0.995658000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	38	0.995679000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	39	0.995682000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	41	0.995703000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data
443	50341	42	0.995704000	192.30.253.112	192.168.182.128	TLSv1.2	1514	Application Data

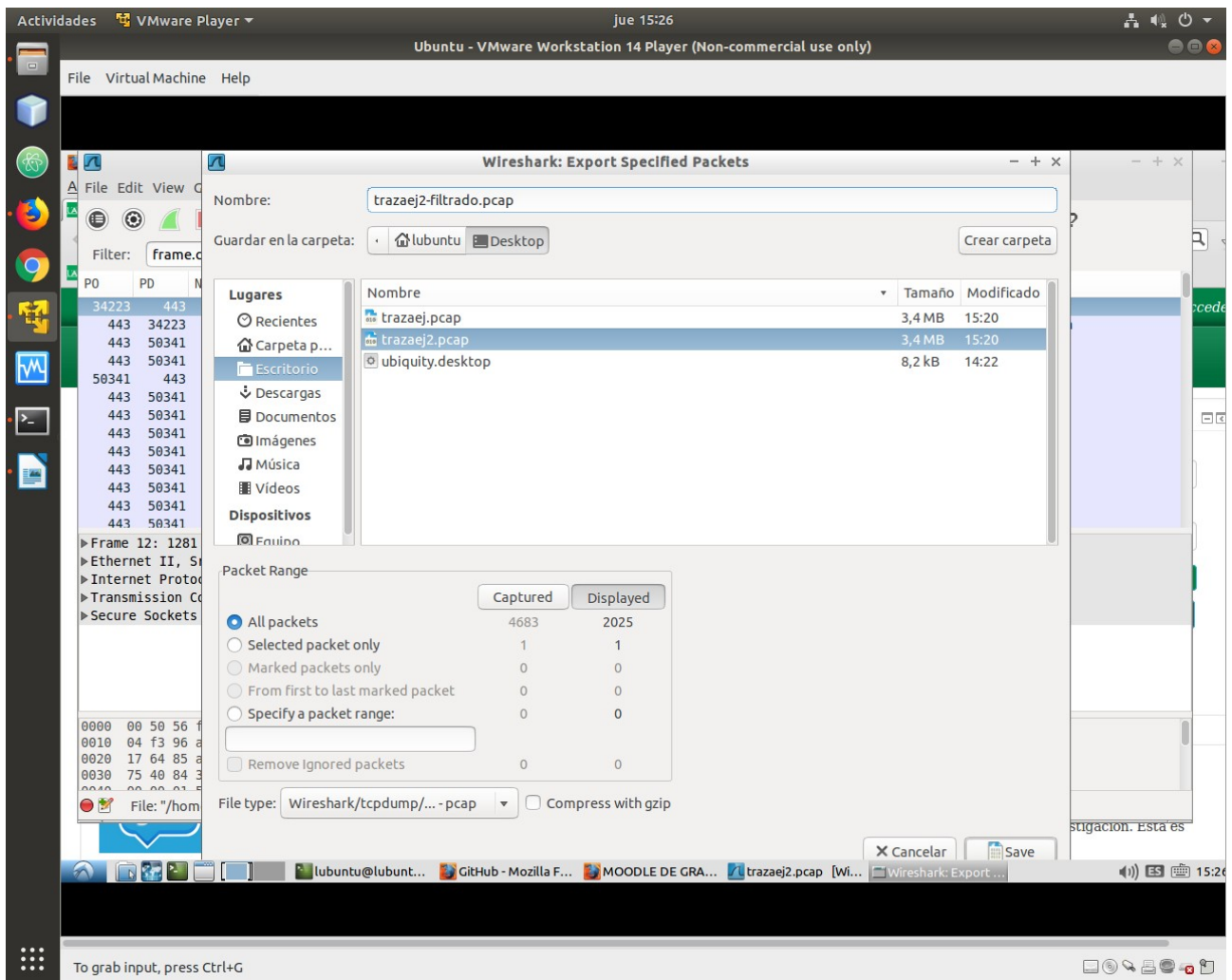
The packet details pane for the selected packet (Frame 12) shows the following structure:

- Frame 12: 1281 bytes on wire (10248 bits), 1281 bytes captured (10248 bits) on interface 0
- Ethernet II, Src: Vmware_4c:72:38 (00:0c:29:4c:72:38), Dst: Vmware_f9:78:41 (00:50:56:f9:78:41)
- Internet Protocol Version 4, Src: 192.168.182.128 (192.168.182.128), Dst: 172.217.23.100 (172.217.23.100)
- Transmission Control Protocol, Src Port: 34223 (34223), Dst Port: https (443), Seq: 605, Ack: 169, Len: 1227
- Secure Sockets Layer

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 50 56 f9 78 41 00 0c 29 4c 72 38 08 00 45 00 .PV.xA.. )Lr8..E.
0010 04 f3 96 a8 40 00 40 06 63 f6 c0 a8 b6 80 ac d9 ....@. C.....
0020 17 64 85 af 01 bb 7c 16 e8 e2 8c 8c 50 43 50 18 .d....|. ....PCP.
0030 75 40 84 33 00 00 17 03 03 04 c6 00 00 00 00 00 u@.3.... .....
```

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').



The screenshot displays a VMware Workstation 14 Player window. The virtual machine is named "Ubuntu - VMware Workstation 14 Player (Non-commercial use only)". The desktop environment shows a terminal window with the following output:

```

0000 00 50 56 f9 78 41 00 0c 29 4c 72 38 08 00 45 00 .PV.XA..)Lr8..E.
0010 04 03 80 86 40 00 00 06 93 dc c0 a8 b6 80 d8 3a ....@.@. ....:
0020 d3 2e cd b4 81 bb 06 25 53 26 db 0c 42 50 18 ...f...CP...

```

The packet details pane shows the following information:

- Frame 1763: 1041 bytes on wire (8328 bits), 1041 bytes captured (8328 bits)
- Ethernet II, Src: Vmware_4c:72:38 (00:0c:29:4c:72:38), Dst: Vmware_f9:78:41 (00:50:56:f9:78:41)
- Internet Protocol Version 4, Src: 192.168.182.128 (192.168.182.128), Dst: 216.58.211.46 (216.58.211.46)
- Transmission Control Protocol, Src Port: 52660 (52660), Dst Port: https (443), Seq: 10863, Ack: 480795, Len: 987
- [2 Reassembled TCP Segments (2447 bytes): #1762(1460), #1763(987)]
- Secure Sockets Layer

The packet list pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
443	52658	489 55.554361	216.58.211.46	TCP	170	[TCP segment of a reassembled PDU]
443	52660	1483 63.218652	216.58.211.46	TLSv1.2	338	Application Data
443	44133	1169 62.945001	216.58.211.54	TCP	506	[TCP segment of a reassembled PDU]
443	52660	1406 63.216508	216.58.211.46	TCP	674	[TCP segment of a reassembled PDU]
443	48379	1910 68.013309	172.217.17.2	TCP	674	[TCP segment of a reassembled PDU]
443	44133	1145 62.943665	192.168.182.128	TLSv1.2	716	Application Data
443	52660	1376 63.215083	216.58.211.46	TLSv1.2	926	Application Data
443	52660	1420 63.217409	216.58.211.46	TCP	926	[TCP segment of a reassembled PDU]
443	52658	313 55.455465	216.58.211.46	TLSv1.2	1004	Application Data
443	44133	1094 62.940896	192.168.182.128	TLSv1.2	1010	Application Data
443	34223	262 52.926878	172.217.23.100	TLSv1.2	1019	[TCP Previous segment not captured] Application Data
443	52659	812 62.464635	216.58.211.46	TLSv1.2	1037	Application Data
443	52658	729 62.085375	216.58.211.46	TLSv1.2	1041	Application Data

The packet details pane shows the following information:

- Frame 1763: 1041 bytes on wire (8328 bits), 1041 bytes captured (8328 bits)
- Ethernet II, Src: Vmware_4c:72:38 (00:0c:29:4c:72:38), Dst: Vmware_f9:78:41 (00:50:56:f9:78:41)
- Internet Protocol Version 4, Src: 192.168.182.128 (192.168.182.128), Dst: 216.58.211.46 (216.58.211.46)
- Transmission Control Protocol, Src Port: 52660 (52660), Dst Port: https (443), Seq: 10863, Ack: 480795, Len: 987
- [2 Reassembled TCP Segments (2447 bytes): #1762(1460), #1763(987)]
- Secure Sockets Layer

The packet list pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
443	52658	489 55.554361	216.58.211.46	TCP	170	[TCP segment of a reassembled PDU]
443	52660	1483 63.218652	216.58.211.46	TLSv1.2	338	Application Data
443	44133	1169 62.945001	216.58.211.54	TCP	506	[TCP segment of a reassembled PDU]
443	52660	1406 63.216508	216.58.211.46	TCP	674	[TCP segment of a reassembled PDU]
443	48379	1910 68.013309	172.217.17.2	TCP	674	[TCP segment of a reassembled PDU]
443	44133	1145 62.943665	192.168.182.128	TLSv1.2	716	Application Data
443	52660	1376 63.215083	216.58.211.46	TLSv1.2	926	Application Data
443	52660	1420 63.217409	216.58.211.46	TCP	926	[TCP segment of a reassembled PDU]
443	52658	313 55.455465	216.58.211.46	TLSv1.2	1004	Application Data
443	44133	1094 62.940896	192.168.182.128	TLSv1.2	1010	Application Data
443	34223	262 52.926878	172.217.23.100	TLSv1.2	1019	[TCP Previous segment not captured] Application Data
443	52659	812 62.464635	216.58.211.46	TLSv1.2	1037	Application Data
443	52658	729 62.085375	216.58.211.46	TLSv1.2	1041	Application Data

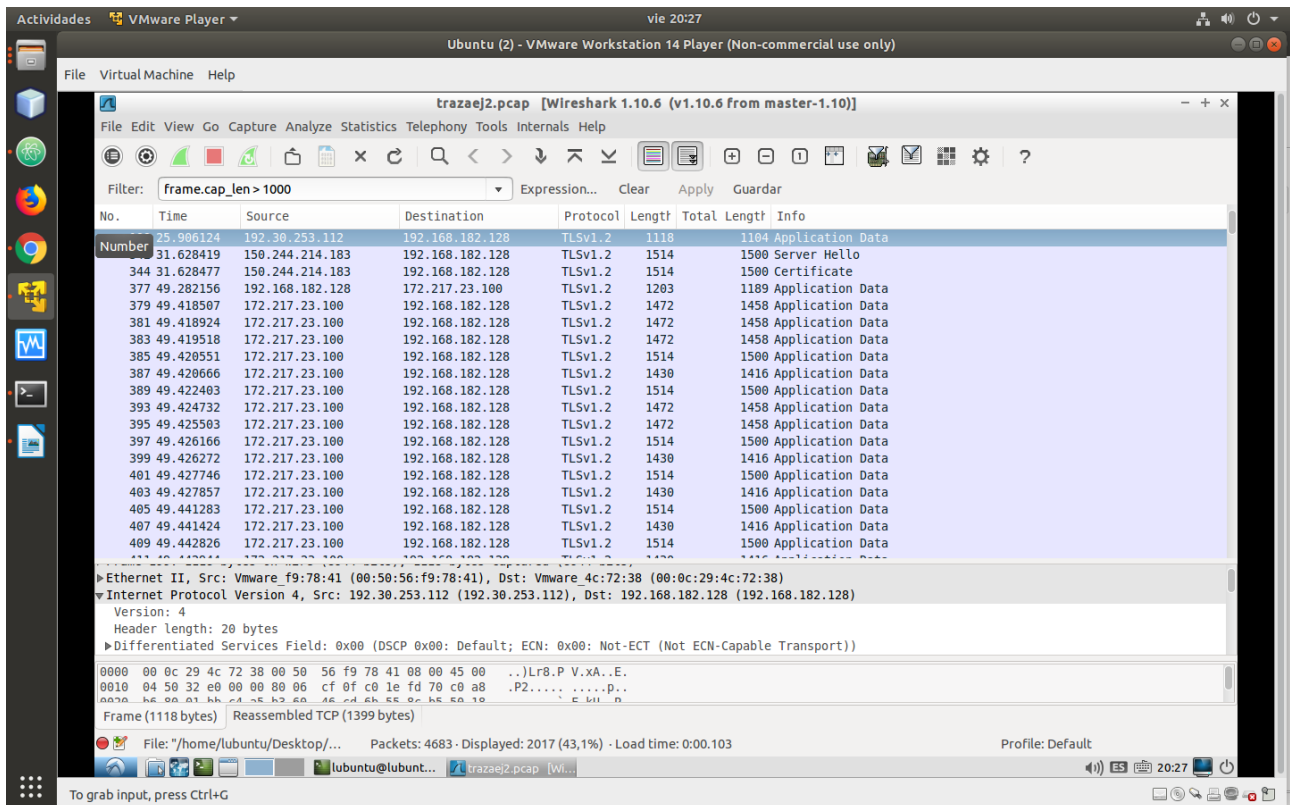
The packet details pane shows the following information:

- Frame 1763: 1041 bytes on wire (8328 bits), 1041 bytes captured (8328 bits)
- Ethernet II, Src: Vmware_4c:72:38 (00:0c:29:4c:72:38), Dst: Vmware_f9:78:41 (00:50:56:f9:78:41)
- Internet Protocol Version 4, Src: 192.168.182.128 (192.168.182.128), Dst: 216.58.211.46 (216.58.211.46)
- Transmission Control Protocol, Src Port: 52660 (52660), Dst Port: https (443), Seq: 10863, Ack: 480795, Len: 987
- [2 Reassembled TCP Segments (2447 bytes): #1762(1460), #1763(987)]
- Secure Sockets Layer

The packet list pane shows the following information:

No.	Time	Source	Destination	Protocol	Length
-----	------	--------	-------------	----------	--------

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'.

The screenshot shows a VMware Workstation 14 Player window titled 'Ubuntu - VMware Workstation 14 Player (Non-commercial use only)'. Inside the VM, the Ubuntu desktop environment is visible. The Wireshark Network Analyzer is running, displaying a packet capture file named 'trazaej2-filtrado.pcap'. The interface shows the packet list, packet details, and packet bytes panes. The packet list pane shows a list of captured packets, with packet 240 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Secure Sockets Layer. The packet bytes pane shows the raw hex and ASCII data of the selected packet. The status bar at the bottom indicates 'To grab input, press Ctrl+G'.

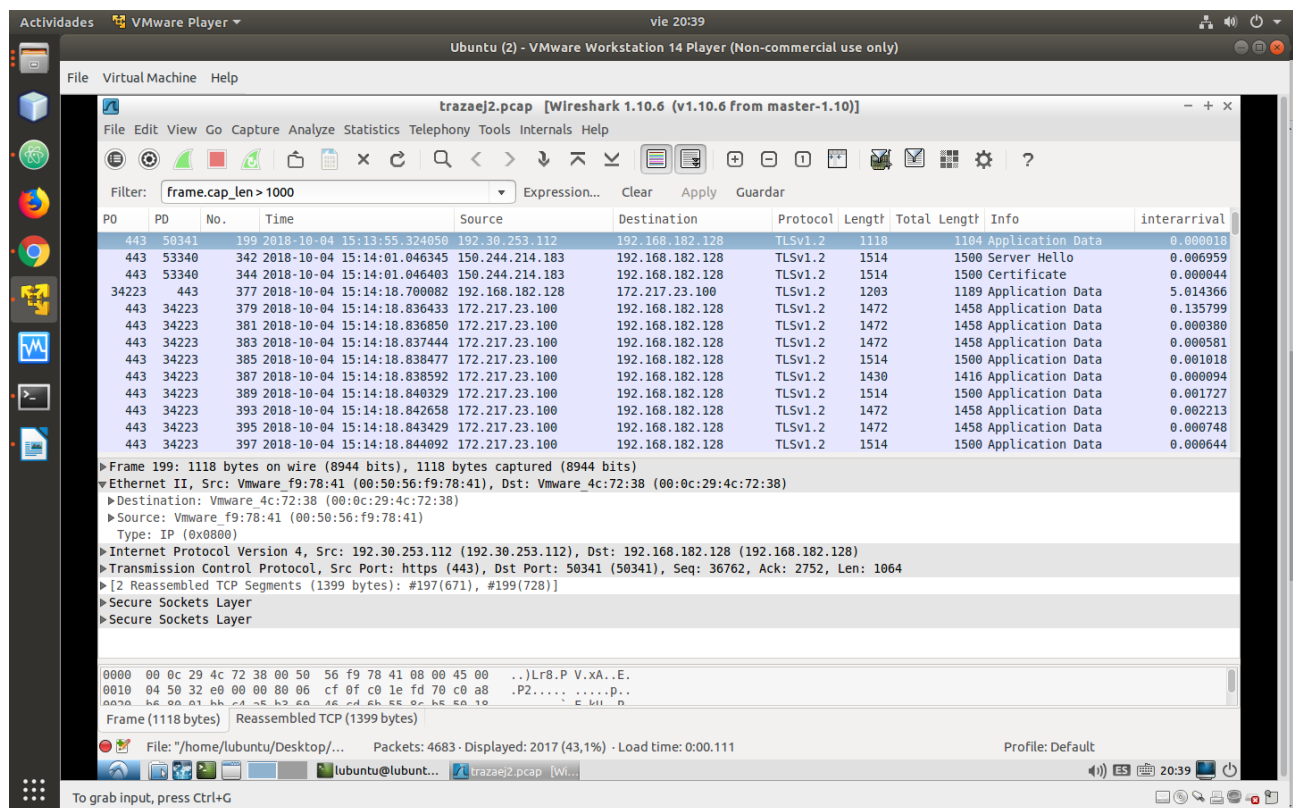
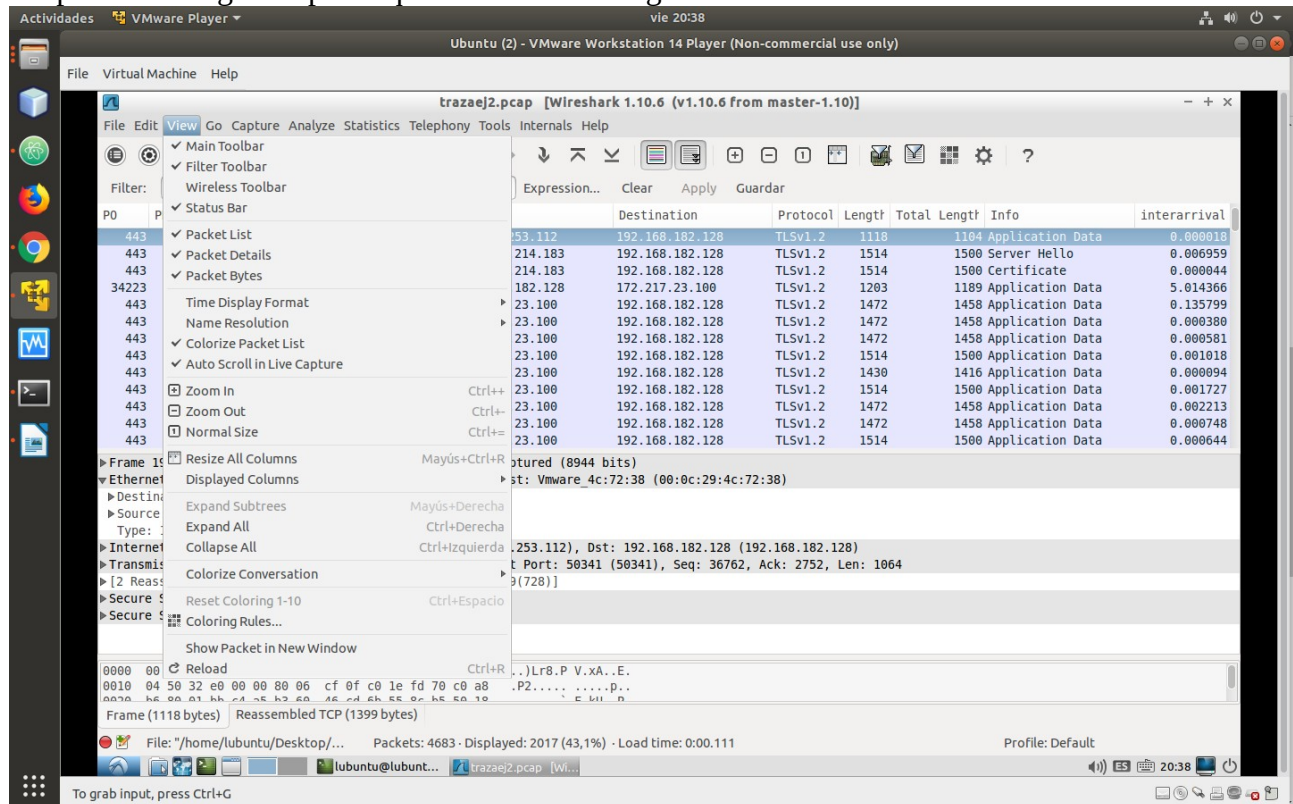
PO	PD	No.	Time	Source	Destination	Protocol	Length	Info	Interarrival
34223	443	1	0.000000	192.168.182.128	172.217.23.100	TLSv1.2	1281	Application Data	0.000000
34223	443	33	49.234737	192.168.182.128	172.217.23.100	TLSv1.2	1203	Application Data	17.653679
34223	443	184	50.268401	192.168.182.128	172.217.23.100	TLSv1.2	1187	[TCP ACKed unseen segment] Applicat	0.098844
34223	443	185	50.379346	192.168.182.128	172.217.23.100	TLSv1.2	1392	[TCP ACKed unseen segment] Applicat	0.110945
34223	443	240	50.482627	192.168.182.128	172.217.23.100	TLSv1.2	1399	[TCP ACKed unseen segment] Applicat	0.072060
34223	443	251	50.507421	192.168.182.128	172.217.23.100	TLSv1.2	1337	[TCP ACKed unseen segment] Applicat	0.000444
34223	443	258	50.616348	192.168.182.128	172.217.23.100	TLSv1.2	1484	[TCP ACKed unseen segment] Applicat	0.019265
34223	443	261	52.883559	192.168.182.128	172.217.23.100	TLSv1.2	1425	[TCP ACKed unseen segment] Applicat	2.033157
34223	443	263	54.909608	192.168.182.128	172.217.23.100	TLSv1.2	1391	[TCP ACKed unseen segment] Applicat	1.982730
34223	443	1674	63.963301	192.168.182.128	172.217.23.100	TLSv1.2	1325	Application Data	0.000476
34223	443	1874	67.986244	192.168.182.128	172.217.23.100	TLSv1.2	1312	[TCP ACKed unseen segment] Applicat	0.008619
34223	443	1936	68.080453	192.168.182.128	172.217.23.100	TLSv1.2	1193	[TCP ACKed unseen segment] Applicat	0.044649
34243	443	186	50.390411	192.168.182.128	172.217.23.100	TLSv1.2	1163	Application Data	0.011065

Frame 240: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits)
Ethernet II, Src: Vmware_4c:72:38 (00:0c:29:4c:72:38), Dst: Vmware_f9:78:41 (00:50:56:f9:78:41)
Internet Protocol Version 4, Src: 192.168.182.128 (192.168.182.128), Dst: 172.217.23.100 (172.217.23.100)
Transmission Control Protocol, Src Port: 34223 (34223), Dst Port: https (443), Seq: 4848, Ack: 290533, Len: 1345
Secure Sockets Layer

File: "trazaej2-filtrado.pcap" ... Packets: 2025 · Displayed: 2025 (100,0%) · Load time: 0:00.048 Profile: Default

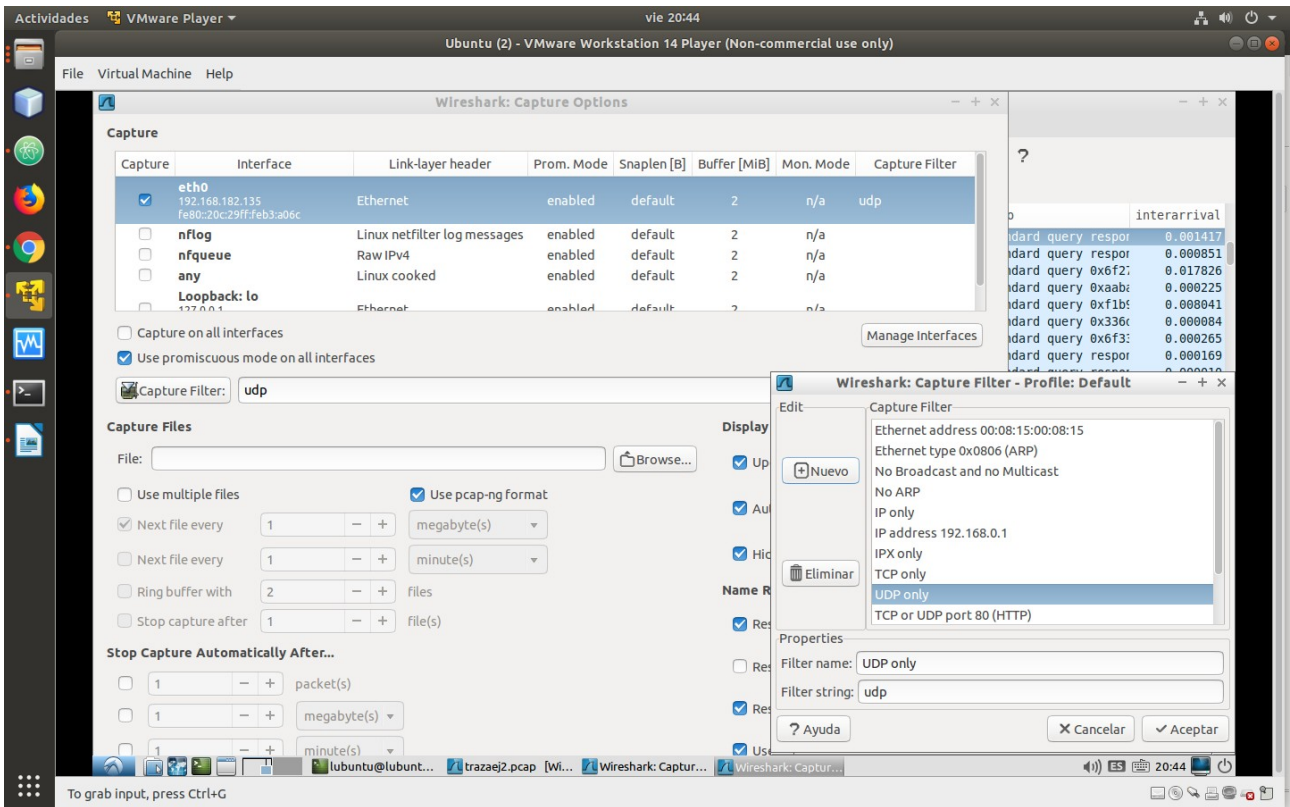
Ejercicio 4

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.

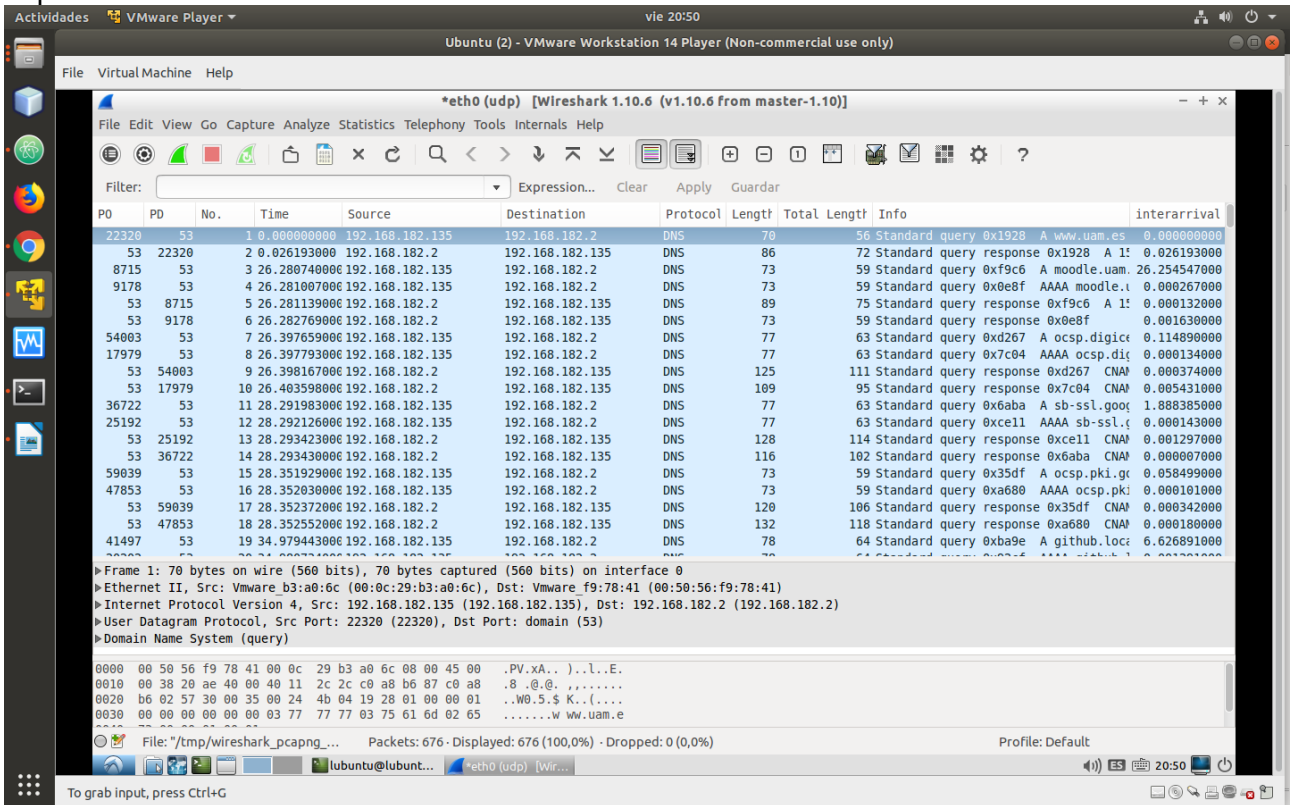


Ejercicio 5

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



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



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

