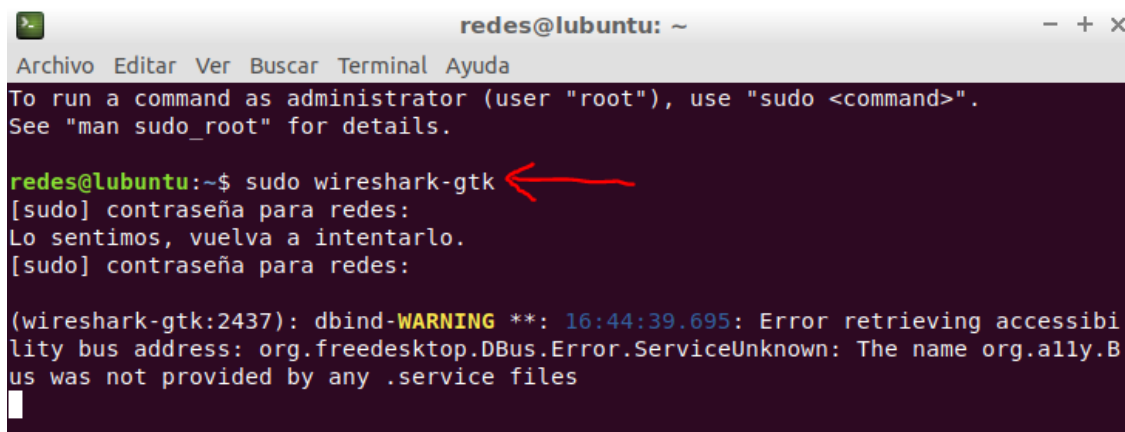


EJERCICIOS DE CAPTURA DE TRÁFICO

EJERCICIO 1.

-**Paso 1.** Abrimos Wireshark con el comando “sudo wireshark-gtk”. De esta forma obtendremos los permisos necesarios.



```

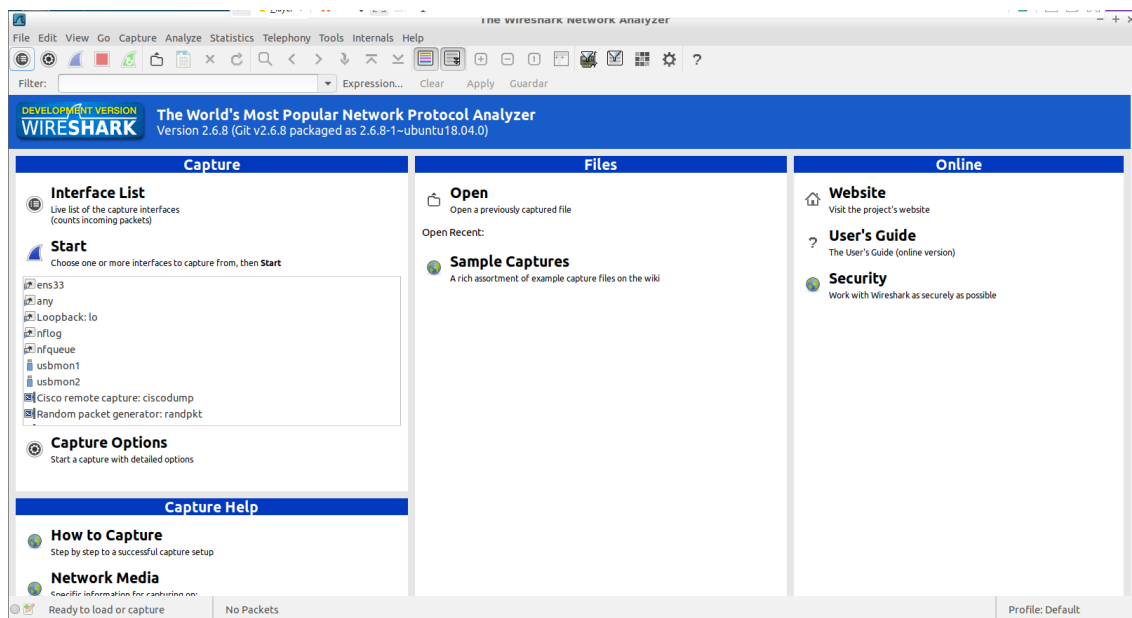
redes@lubuntu: ~
Archivo Editar Ver Buscar Terminal Ayuda
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

redes@lubuntu:~$ sudo wireshark-gtk
[sudo] contraseña para redes:
Lo sentimos, vuelva a intentarlo.
[sudo] contraseña para redes:

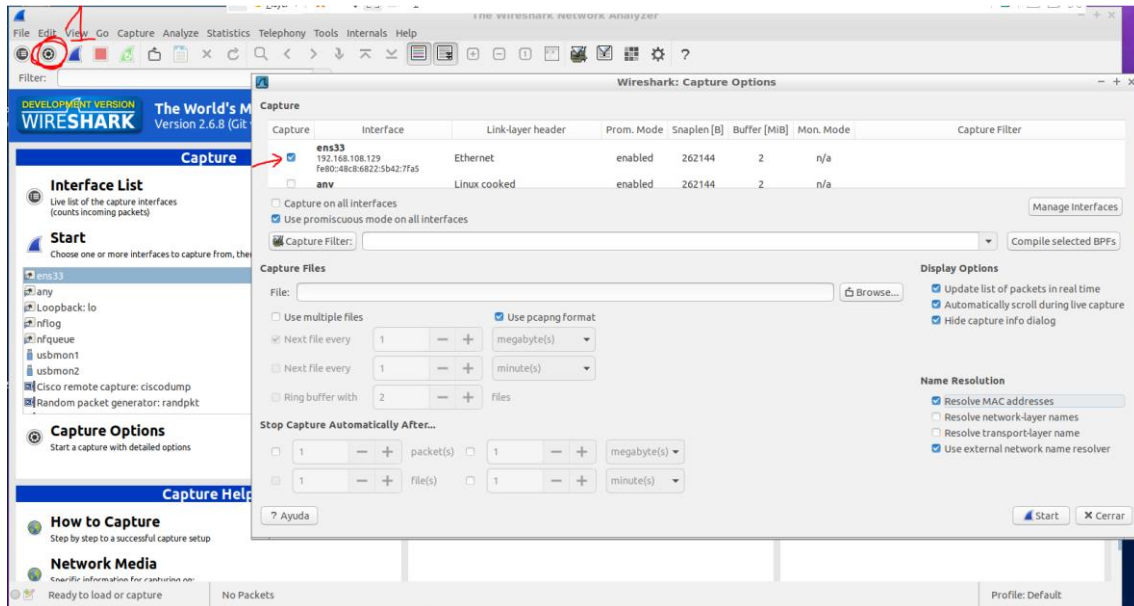
(wireshark-gtk:2437): dbind-WARNING **: 16:44:39.695: Error retrieving accessibility bus address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.a11y.Bus was not provided by any .service files
  
```

-Paso 2:

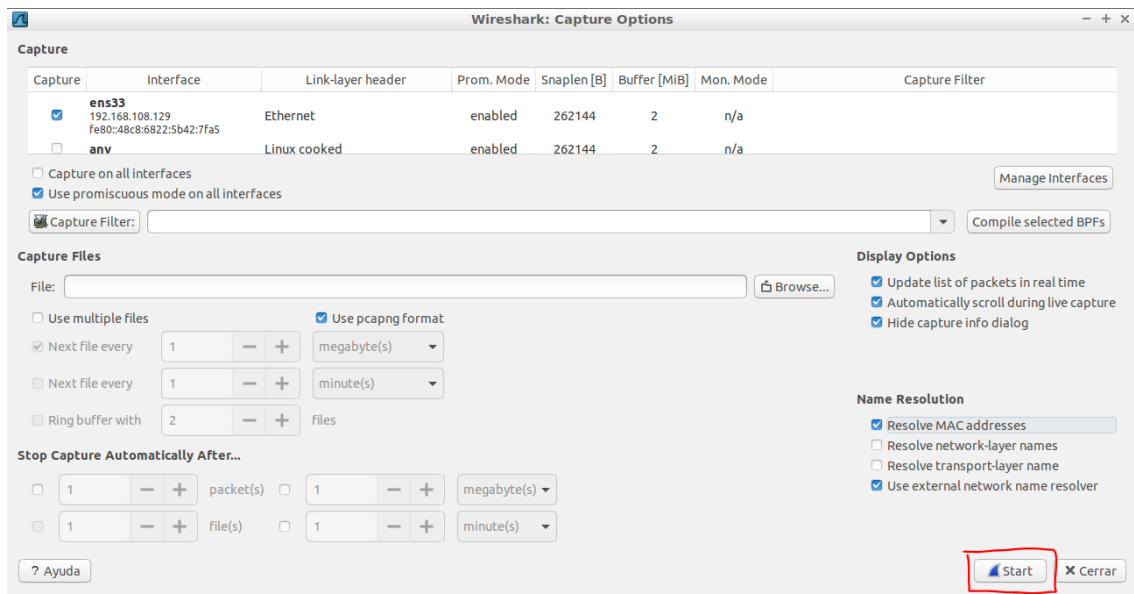
-2.1 Ejecutamos Wireshark.



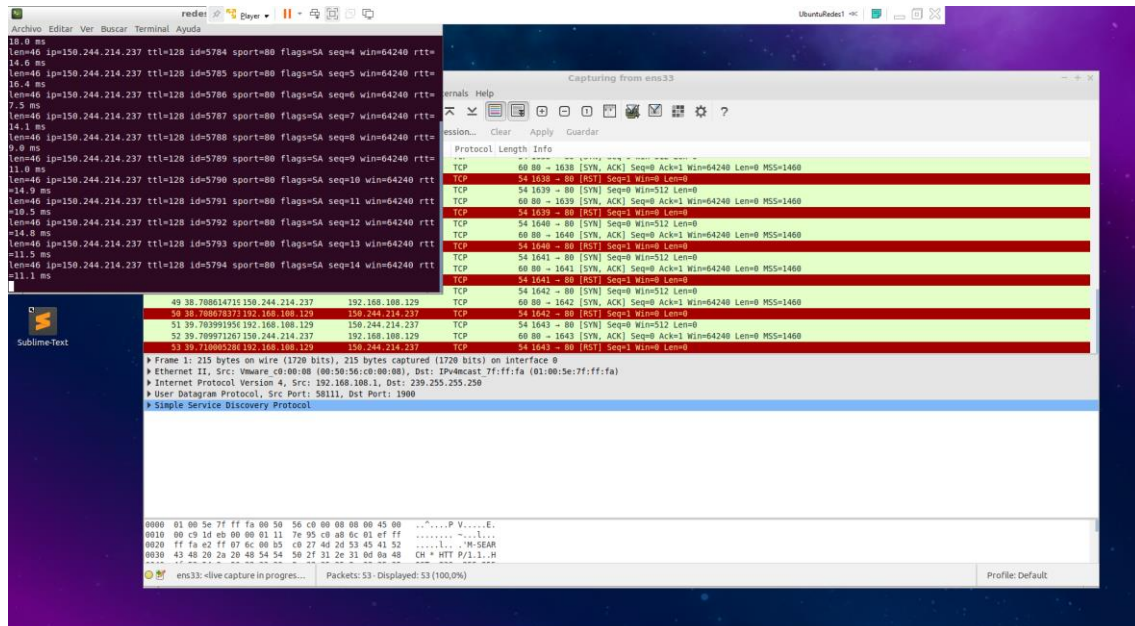
-2.2 Configuramos la interfaz a capturar (ens33).



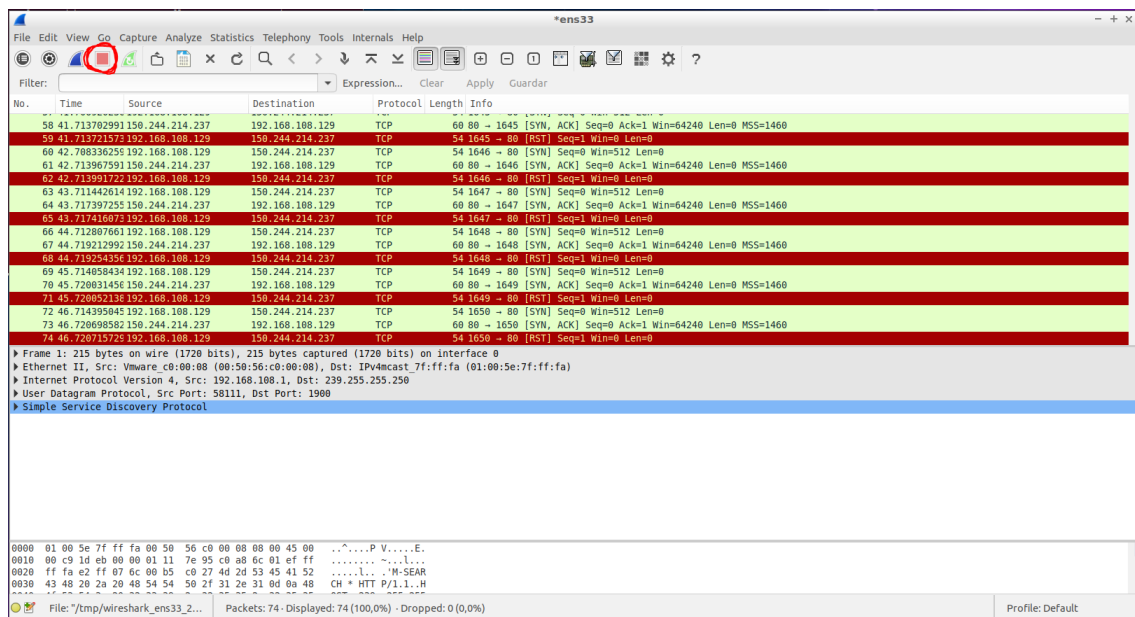
-Paso 3. Utilizamos el botón "Start" para iniciar la captura.



-Paso 4. En una nueva terminal, ahora escribimos el comando "sudo hping3 -S -p 80 www.uam.es"



-Paso 5. Utilizamos el botón "Stop" para detener la captura de tráfico.



-Paso 6. Analizamos el tráfico capturado:

The screenshot shows the Wireshark interface with a packet capture of SSDP traffic. Packet 7 is selected, which is an SSDP M-SEARCH request from 192.168.108.1 to 239.255.255.250. The details pane shows the packet structure, and the packet bytes pane shows the raw data in hex and ASCII.

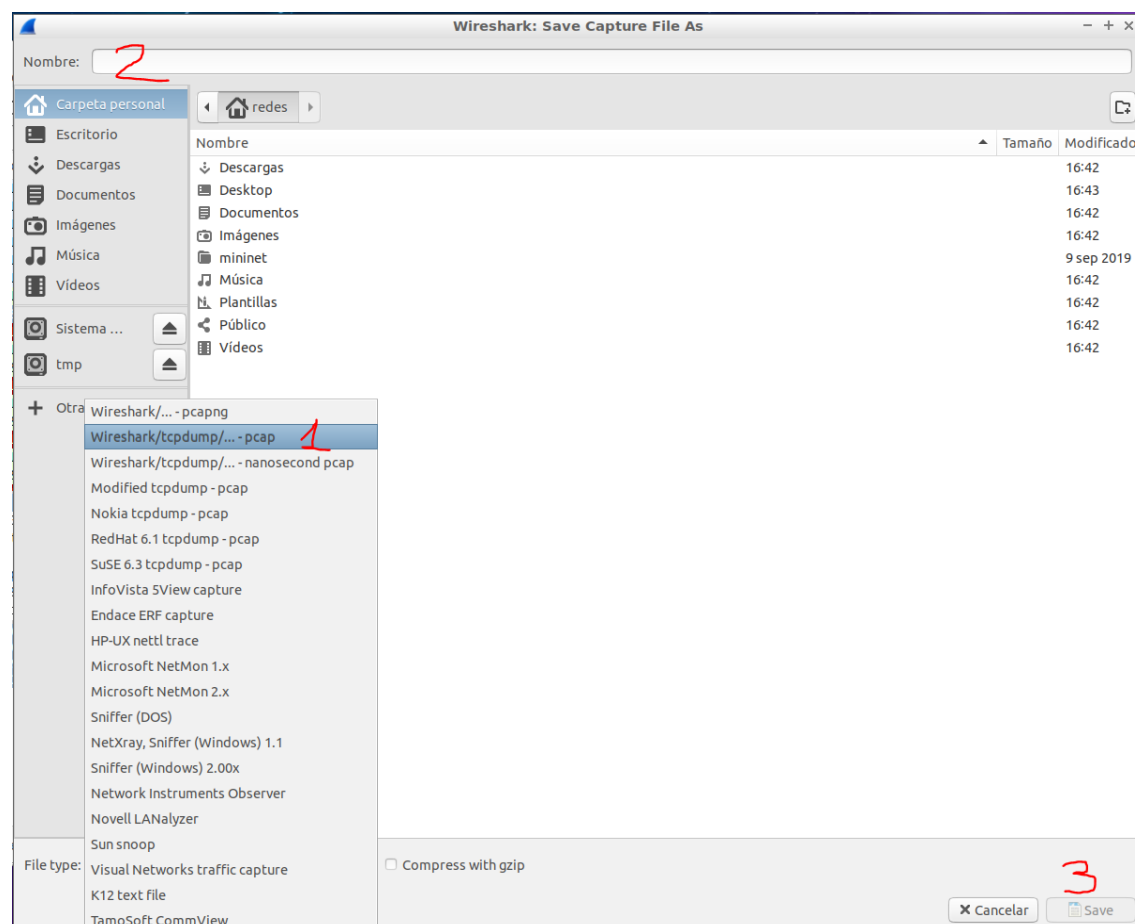
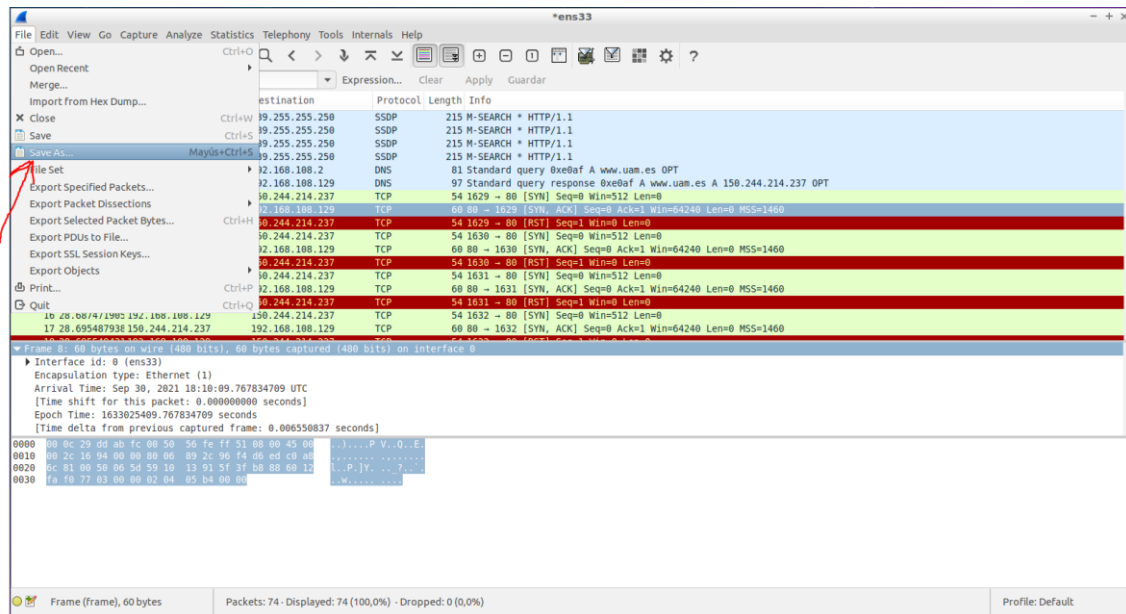
En la anterior captura podemos apreciar en la parte superior todos los paquetes capturados. Después de seleccionar un paquete, en este caso el número 7, podemos observar en la parte media, la decodificación del paquete seleccionado, viendo así datos relevantes como:

The screenshot shows the detailed view of packet 7, which is a TCP segment. The details pane shows the Transmission Control Protocol (TCP) fields, including the destination port (80) and the sequence number (1846649614). The packet bytes pane shows the raw data in hex and ASCII.

Podemos ver campos como el 'destination port', que está incluido en la cabecera de este protocolo y a su vez encapsulado en un paquete IP, así como el 'source port' y otros campos que no nos pararemos a analizar.

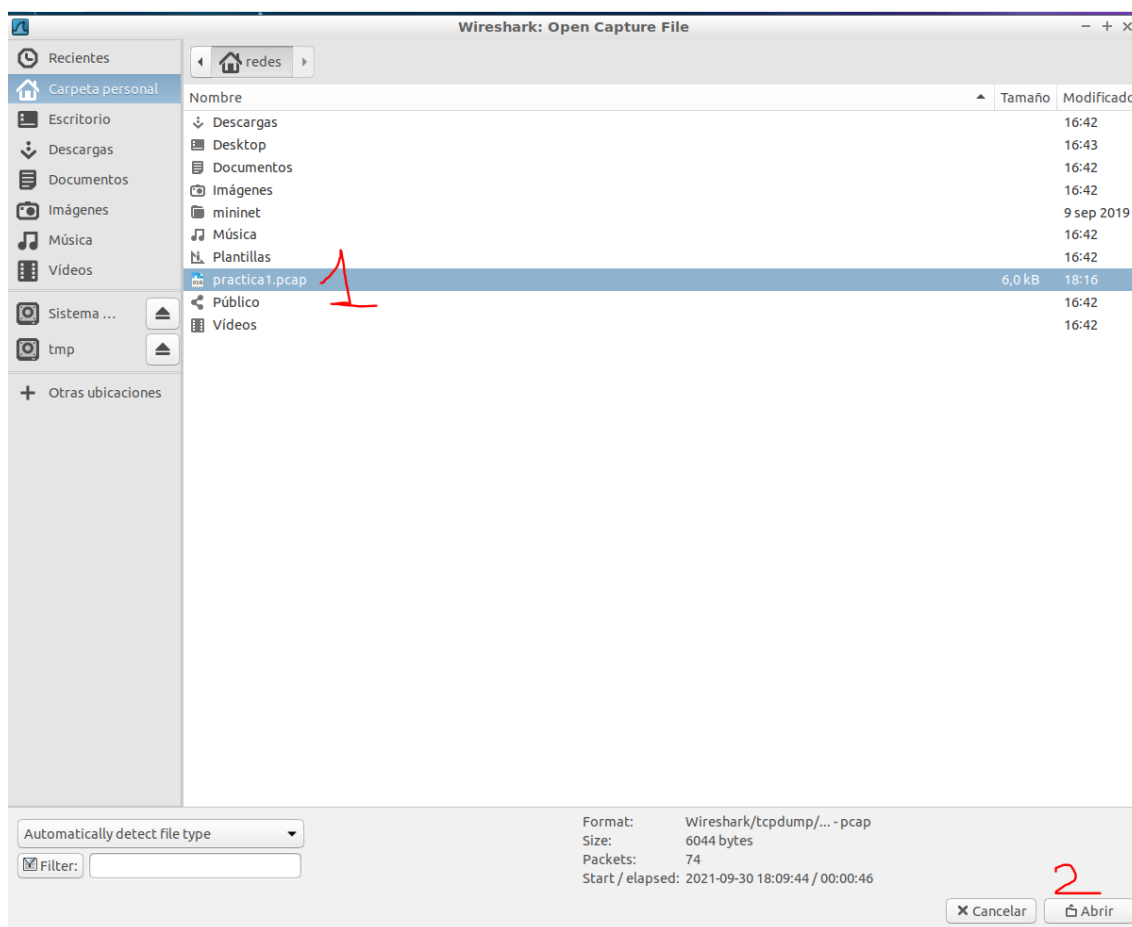
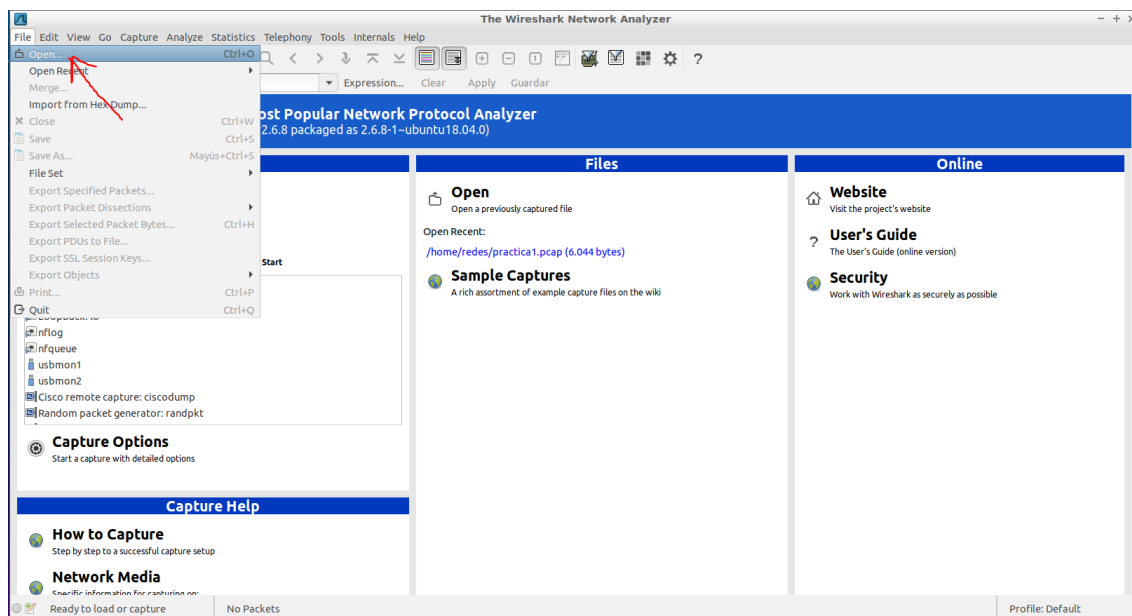
Por último, también podríamos comentar el volcado hexadecimal del paquete analizado previamente, con tan solo dar click en algún campo como por ejemplo el 'destination port' podemos ver que los bytes '0050' le configuran. Estos bytes se encuentran alineados en grupos de 16.

-Paso 7. Guardamos la traza en un fichero con formato pcap.



-Paso 8. Cerramos Wireshark y después volvemos a abrirlo. Solo tendríamos que repetir el paso 1 con su respectiva captura.

-Paso 9. Abrimos el fichero que habíamos previamente guardado para comprobar que se almacenó correctamente.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2	1.003286	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3	2.005874	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4	3.007081	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
5	25.628085	192.168.108.129	192.168.108.2	DNS	81	Standard query 0xe0af A www.uam.es OPT
6	25.632920	192.168.108.2	192.168.108.129	DNS	97	Standard query response 0xe0af A www.uam.es A 150.244.214.237 OPT
7	25.680339	192.168.108.129	150.244.214.237	TCP	54	1629 → 80 [SYN] Seq=0 Win=512 Len=0
8	25.686890	150.244.214.237	192.168.108.129	TCP	60	80 → 1629 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	25.687082	192.168.108.129	150.244.214.237	TCP	54	1629 → 80 [RST] Seq=1 Win=0 Len=0
10	26.082700	192.168.108.129	150.244.214.237	TCP	54	1630 → 80 [SYN] Seq=0 Win=512 Len=0
11	26.689374	150.244.214.237	192.168.108.129	TCP	60	80 → 1630 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
12	26.689393	192.168.108.129	150.244.214.237	TCP	54	1630 → 80 [RST] Seq=1 Win=0 Len=0
13	27.684751	192.168.108.129	150.244.214.237	TCP	54	1631 → 80 [SYN] Seq=0 Win=512 Len=0
14	27.691859	150.244.214.237	192.168.108.129	TCP	60	80 → 1631 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	27.691919	192.168.108.129	150.244.214.237	TCP	54	1631 → 80 [RST] Seq=1 Win=0 Len=0
16	28.087472	192.168.108.129	150.244.214.237	TCP	54	1632 → 80 [SYN] Seq=0 Win=512 Len=0
17	28.695400	150.244.214.237	192.168.108.129	TCP	60	80 → 1632 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on Ethernet II, Src: VMware-c8:00:08:00:50:56, Dst: IPv4mcast 7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.108.1, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 58111, Dst Port: 1900

Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 00 45 00 ...P V....E.
 0010 00 c9 1d eb 00 00 01 11 7e 95 c0 a8 6c 01 ef ffl...
 0020 ff fa e2 ff 07 6c 00 b5 c0 27 4d 20 53 45 41 52l..M-SEAR
 0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H
 0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
 0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
 0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover".
 0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1..ST: urn:
 0080 64 69 61 6c 2d 0d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen
 0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:service:dia
 00a0 6c 3a 31 0d 0a 53 53 45 52 2d 41 47 45 4e 54 3a l:1..USER-AGENT:
 00b0 20 47 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 39 Google Chrome/9
 00c0 34 7a 30 7a 34 36 3a 36 7a 36 31 70 57 69 6a 64 .A.A666..A1.Wind

-Paso 10:

Los puntos 10.1 y 10.2 se realizan al principio de manera igual, por tanto, para los puntos comunes pondremos solo una captura de pantalla.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2	1.003286	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3	2.005874	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4	3.007081	192.168.108.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
5	25.628085	192.168.108.129	192.168.108.2	DNS	81	Standard query 0xe0af A www.uam.es OPT
6	25.632920	192.168.108.2	192.168.108.129	DNS	97	Standard query response 0xe0af A www.uam.es A 150.244.214.237 OPT
7	25.680339	192.168.108.129	150.244.214.237	TCP	54	1629 → 80 [SYN] Seq=0 Win=512 Len=0
8	25.686890	150.244.214.237	192.168.108.129	TCP	60	80 → 1629 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	25.687082	192.168.108.129	150.244.214.237	TCP	54	1629 → 80 [RST] Seq=1 Win=0 Len=0
10	26.082700	192.168.108.129	150.244.214.237	TCP	54	1630 → 80 [SYN] Seq=0 Win=512 Len=0
11	26.689374	150.244.214.237	192.168.108.129	TCP	60	80 → 1630 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
12	26.689393	192.168.108.129	150.244.214.237	TCP	54	1630 → 80 [RST] Seq=1 Win=0 Len=0
13	27.684751	192.168.108.129	150.244.214.237	TCP	54	1631 → 80 [SYN] Seq=0 Win=512 Len=0
14	27.691859	150.244.214.237	192.168.108.129	TCP	60	80 → 1631 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	27.691919	192.168.108.129	150.244.214.237	TCP	54	1631 → 80 [RST] Seq=1 Win=0 Len=0
16	28.087472	192.168.108.129	150.244.214.237	TCP	54	1632 → 80 [SYN] Seq=0 Win=512 Len=0
17	28.695400	150.244.214.237	192.168.108.129	TCP	60	80 → 1632 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on Ethernet II, Src: VMware-c8:00:08:00:50:56, Dst: IPv4mcast 7f:ff:fa (01:00:5e:7f:ff:fa)

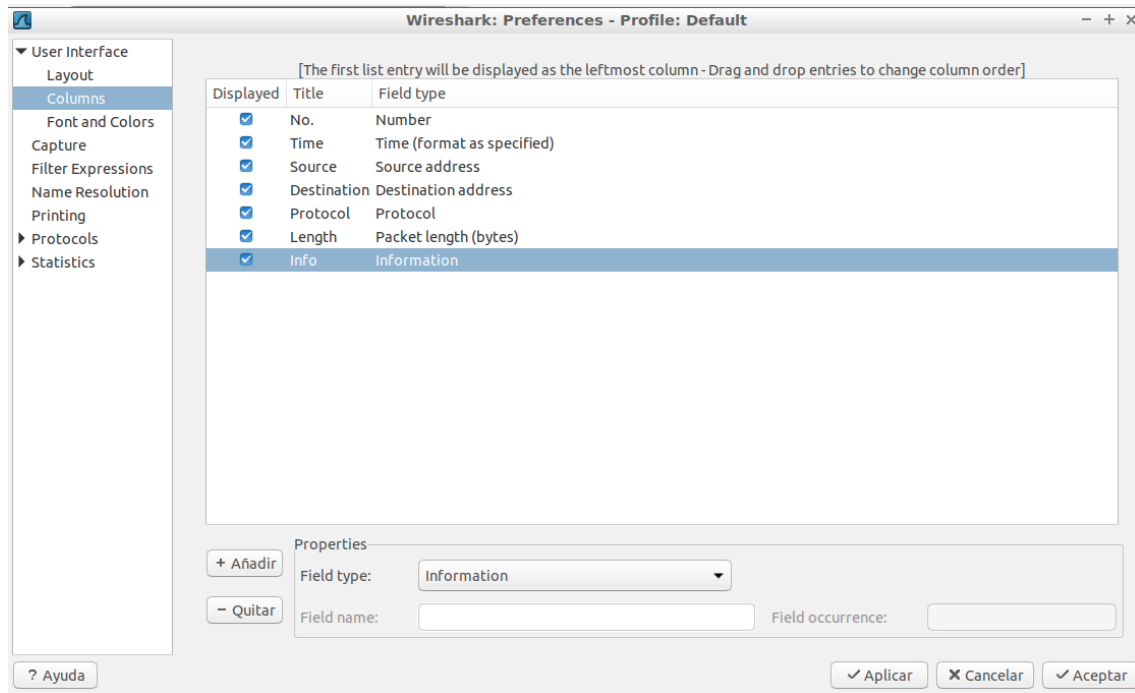
Internet Protocol Version 4, Src: 192.168.108.1, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 58111, Dst Port: 1900

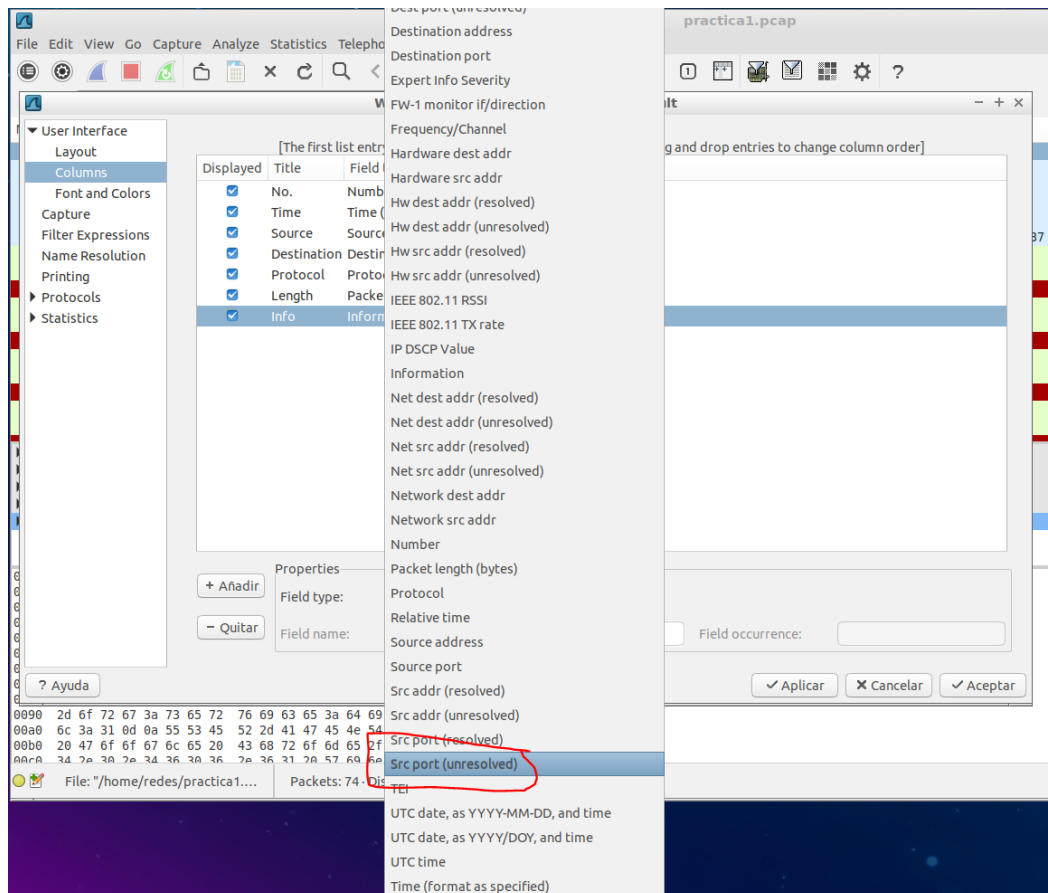
Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 00 45 00 ...P V....E.
 0010 00 c9 1d eb 00 00 01 11 7e 95 c0 a8 6c 01 ef ffl...
 0020 ff fa e2 ff 07 6c 00 b5 c0 27 4d 20 53 45 41 52l..M-SEAR
 0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H
 0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
 0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
 0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover".
 0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1..ST: urn:
 0080 64 69 61 6c 2d 0d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen
 0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:service:dia
 00a0 6c 3a 31 0d 0a 53 53 45 52 2d 41 47 45 4e 54 3a l:1..USER-AGENT:
 00b0 20 47 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 39 Google Chrome/9
 00c0 34 7a 30 7a 34 36 3a 36 7a 36 31 70 57 69 6a 64 .A.A666..A1.Wind

Abrimos el menú de columns, añadimos el tipo de campo que queremos para la nueva columna y pulsamos añadir.



-10.1 Añadimos columna 'PO'.



Para cambiar el nombre, simplemente pinchamos en el nombre actual y escribimos PO

-10.2 Añadimos columna 'PD'.

Procedemos de la misma forma que en 10.1 seleccionando esta vez el campo Dst port (unresolved) y cambiamos su nombre por PD.

Resultado final al añadir las dos columnas:

No.	Time	Source	Destination	Protocol	Length	PO	PD
1	0.000000	192.168.108.1	239.255.255.250	SSDP	215	58111	1900
2	1.003286	192.168.108.1	239.255.255.250	SSDP	215	58111	1900
3	2.005874	192.168.108.1	239.255.255.250	SSDP	215	58111	1900
4	3.007601	192.168.108.1	239.255.255.250	SSDP	215	58111	1900
5	25.628805	192.168.108.129	192.168.108.2	DNS	81	55844	53
6	25.632920	192.168.108.2	192.168.108.129	DNS	97	53	55844
7	25.688339	192.168.108.129	150.244.214.237	TCP	54	1629	80
8	25.688890	150.244.214.237	192.168.108.129	TCP	60	80	1629
9	25.687062	192.168.108.129	150.244.214.237	TCP	54	1629	80
10	26.682700	192.168.108.129	150.244.214.237	TCP	54	1630	80
11	26.688374	150.244.214.237	192.168.108.129	TCP	60	80	1630
12	26.689393	192.168.108.129	150.244.214.237	TCP	54	1630	80
13	27.684751	192.168.108.129	150.244.214.237	TCP	54	1631	80
14	27.691859	150.244.214.237	192.168.108.129	TCP	60	80	1631
15	27.691919	192.168.108.129	150.244.214.237	TCP	54	1631	80
16	28.687472	192.168.108.129	150.244.214.237	TCP	54	1632	80
17	28.695488	150.244.214.237	192.168.108.129	TCP	60	80	1632

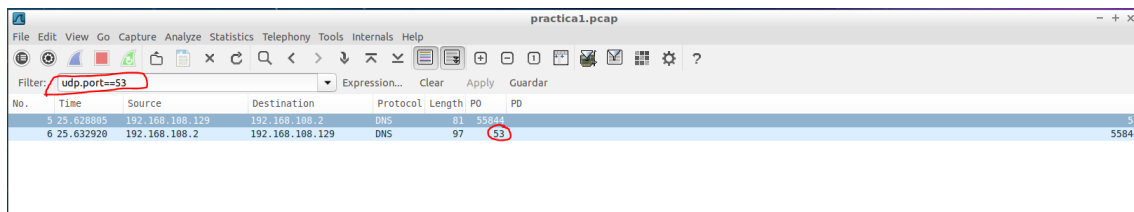
-10.3 Ordenamos en sentido descendente respecto al campo "PO".

Para ordenar en orden descendente los paquetes según el valor de "PO", tenemos dos opciones. O bien dar clic sobre el nombre de la columna ("PO") hasta que veamos una flecha hacia abajo, o bien dar click derecho y seleccionar la opción de descendente.

No.	Time	Source	Destination	Protocol	Length	PO	PD
74	46.720716	192.168.108.129	150.244.214.237	TCP	54	1650	80
72	46.714395	192.168.108.129	150.244.214.237	TCP	54	1650	80
71	45.720853	192.168.108.129	150.244.214.237	TCP	54	1649	80
69	45.714659	192.168.108.129	150.244.214.237	TCP	54	1649	80
63	43.712925	192.168.108.129	150.244.214.237	TCP	54	1648	80
66	44.712808	192.168.108.129	150.244.214.237	TCP	54	1648	80
65	43.717416	192.168.108.129	150.244.214.237	TCP	54	1647	80
63	43.711443	192.168.108.129	150.244.214.237	TCP	54	1647	80
62	42.713992	192.168.108.129	150.244.214.237	TCP	54	1646	80
60	42.708337	192.168.108.129	150.244.214.237	TCP	54	1646	80
53	41.713722	192.168.108.129	150.244.214.237	TCP	54	1645	80
57	41.706921	192.168.108.129	150.244.214.237	TCP	54	1645	80
56	40.710573	192.168.108.129	150.244.214.237	TCP	54	1644	80
54	40.704653	192.168.108.129	150.244.214.237	TCP	54	1644	80
53	39.710006	192.168.108.129	150.244.214.237	TCP	54	1643	80
51	39.703992	192.168.108.129	150.244.214.237	TCP	54	1643	80
50	38.700079	192.168.108.129	150.244.214.237	TCP	54	1642	80

-10.4 Contabilizamos el número de paquetes en el que el campo "PO" tiene valor 53.

Utilizamos un filtro de visualización (`udp.port==53`) que nos muestre los puertos de origen y destino con valor 53 y observamos que solo existe un paquete en el que el campo "PO" tiene valor 53.



No.	Time	Source	Destination	Protocol	Length	PO	PD
5	25.628885	192.168.188.129	192.168.188.2	DNS	81	55844	53
6	25.632920	192.168.188.2	192.168.188.129	DNS	97	53	55844

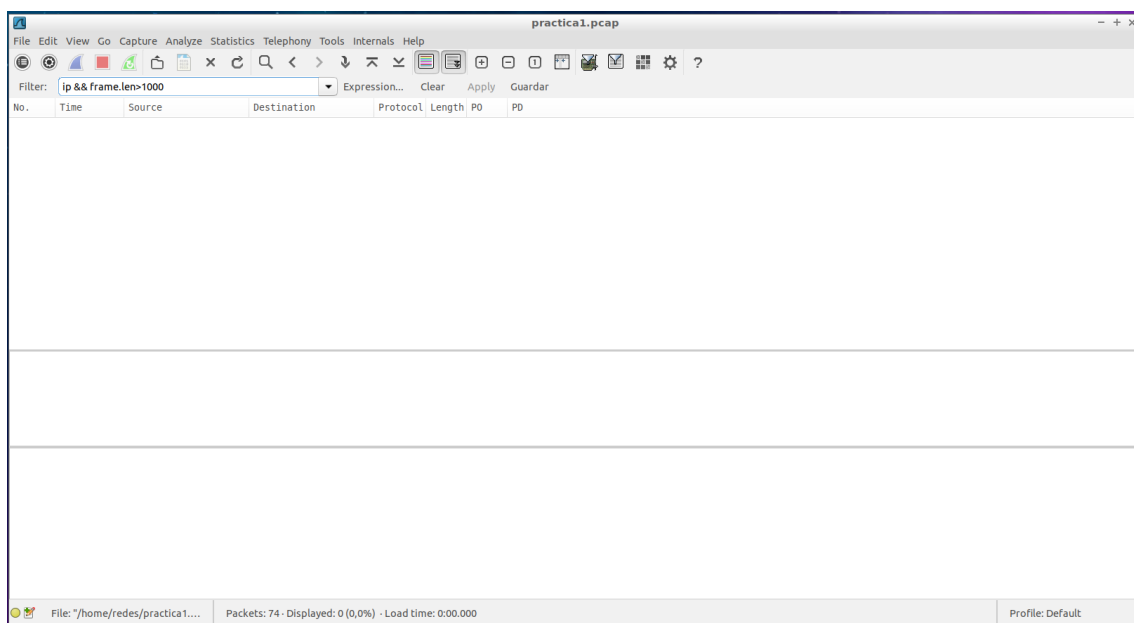
Algunos problemas que encontramos durante la realización de este ejercicio fueron:

- ✓ La interfaz para capturar no fue eth0 como el enunciado indica sino ens33.
- ✓ Wireshark daba algunos problemas como "gtk_box_gadget_distribute assertion 'size = 0' failed in gtkscrollbar", el cual se arregló reajustando la ventana.
- ✓ Además, al ordenar los paquetes en orden descendente según el campo PO, nos costó un poco darnos cuenta de que no se ordenan absolutamente todos, sino que se van ordenando agrupados por tipo.

EJERCICIO 2.

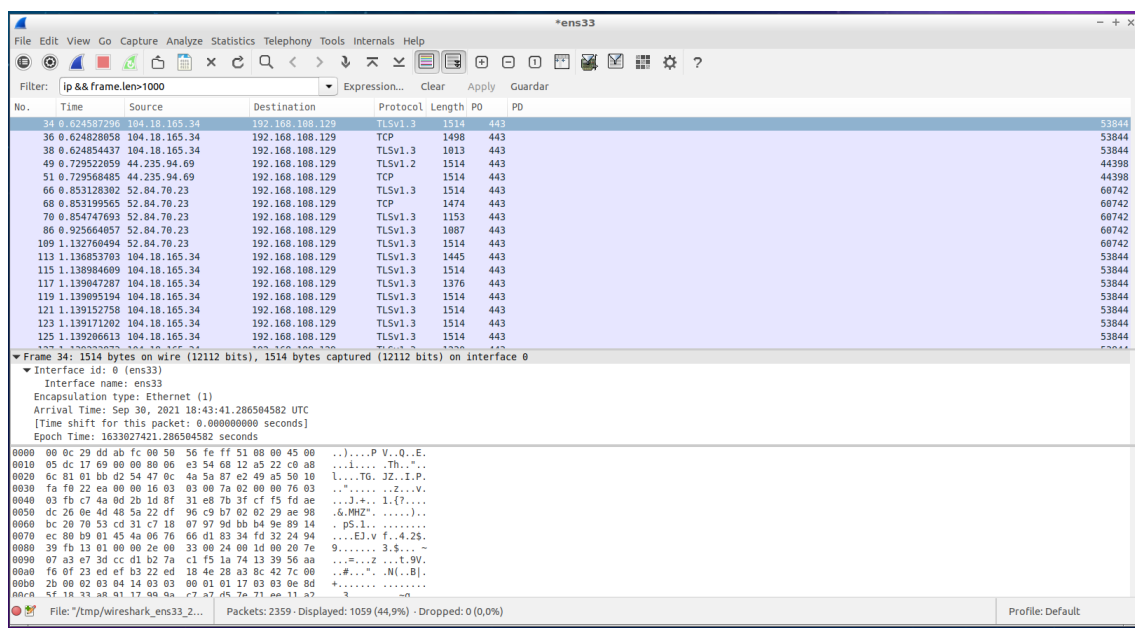
2.1 Filtro realizado:

`ip && frame.len > 1000`



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

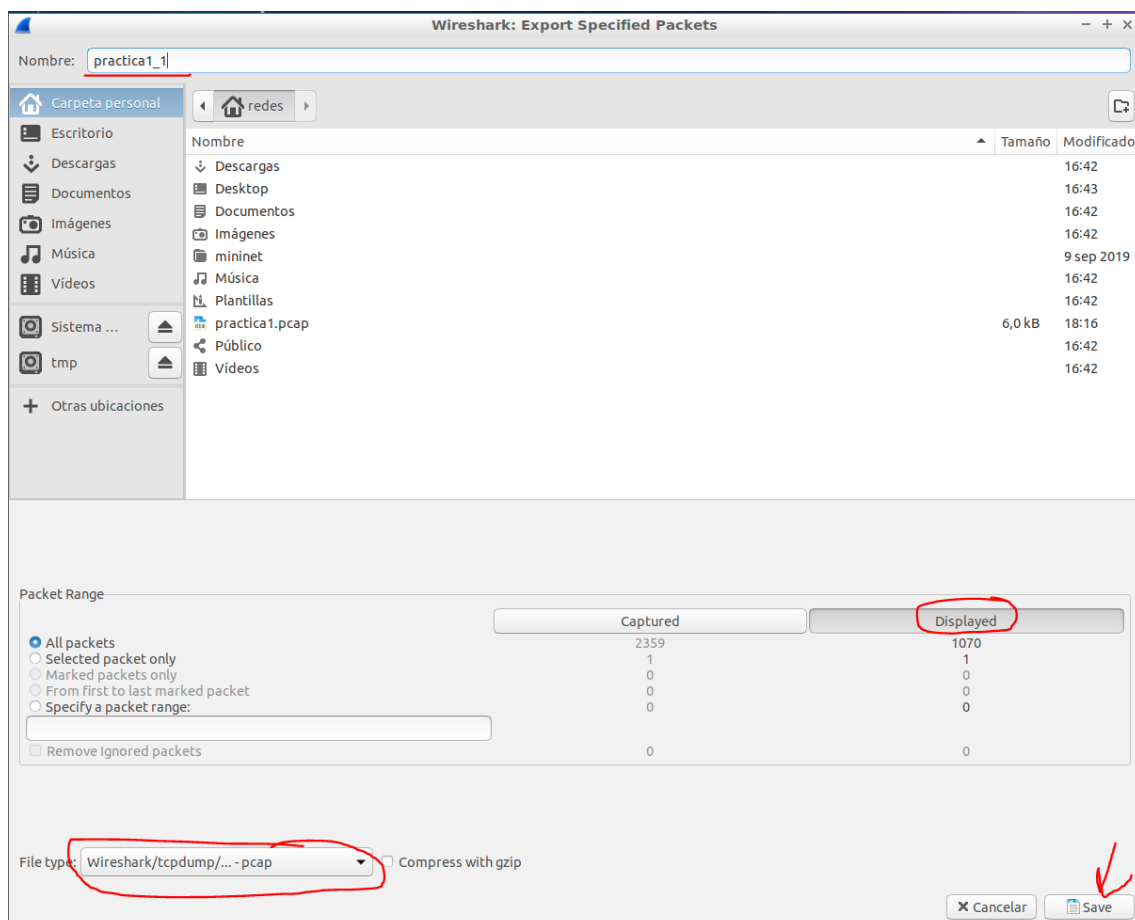
Hasta este momento no teníamos paquetes tan grandes, así que runeamos de nuevo la captura y abierto un navegador para tenerlos.



2.2 Almacenar la captura de los paquetes mostrados:

Exportamos y guardamos el fichero con formato pcap.

Desplegamos file→Export Specified Packets y nos lleva a esta ventana:



2.3 Después de comparar el tamaño del primer paquete IP, y el campo "length" del protocolo IP del mismo, y repetir este proceso para los primeros 5 paquetes, observamos:

Que el valor del campo "length" es de 1514 bytes, el cual coincide con el valor de la parte de decodificación.

Además, se observa que entre el 'frame.len' e 'ip.len' hay 14 unidades de diferencia, valor que coincide con el tamaño del header.

EJERCICIO 3.

3.1 Desplegamos la opción de "Edit" y seleccionamos "Preferences".

3.2 Seleccionamos "Columns".

3.3 En el menú de la derecha, añadimos una nueva columna con el nombre de "interarrival" y del tipo "Delta time displayed".

The screenshot shows the Wireshark interface with the following data:

No.	Time	Source	Destination	Protocol	Length	PD	PD	Interarrival
109	1.132768494	52.84.70.23	192.168.108.129	TLSv1.3	1514	443	60742	0.000429610
110	1.132771055	192.168.108.129	52.84.70.23	TCP	54	60742	443	0.000010561
111	1.132797802	52.84.70.23	192.168.108.129	TLSv1.3	213	443	60742	0.000026747
112	1.132803893	192.168.108.129	52.84.70.23	TCP	54	60742	443	0.000006691
113	1.136853703	104.18.165.34	192.168.108.129	TLSv1.3	1445	443	53844	0.004049810
114	1.136865730	192.168.108.129	104.18.165.34	TCP	54	53844	443	0.000012027
115	1.138984609	104.18.165.34	192.168.108.129	TLSv1.3	1514	443	53844	0.002118879
116	1.138996709	192.168.108.129	104.18.165.34	TCP	54	53844	443	0.000012100
117	1.139047287	104.18.165.34	192.168.108.129	TLSv1.3	1376	443	53844	0.000050578
118	1.139078942	192.168.108.129	104.18.165.34	TCP	54	53844	443	0.000023655
119	1.139095194	104.18.165.34	192.168.108.129	TLSv1.3	1514	443	53844	0.000024252
120	1.139119560	192.168.108.129	104.18.165.34	TCP	54	53844	443	0.000024372
121	1.139152758	104.18.165.34	192.168.108.129	TLSv1.3	1514	443	53844	0.000033192
122	1.139156783	192.168.108.129	104.18.165.34	TCP	54	53844	443	0.000004025
123	1.139171202	104.18.165.34	192.168.108.129	TLSv1.3	1514	443	53844	0.000014419
124	1.139174477	192.168.108.129	104.18.165.34	TCP	54	53844	443	0.000003275
125	1.139206613	104.18.165.34	192.168.108.129	TLSv1.3	1514	443	53844	0.000032136

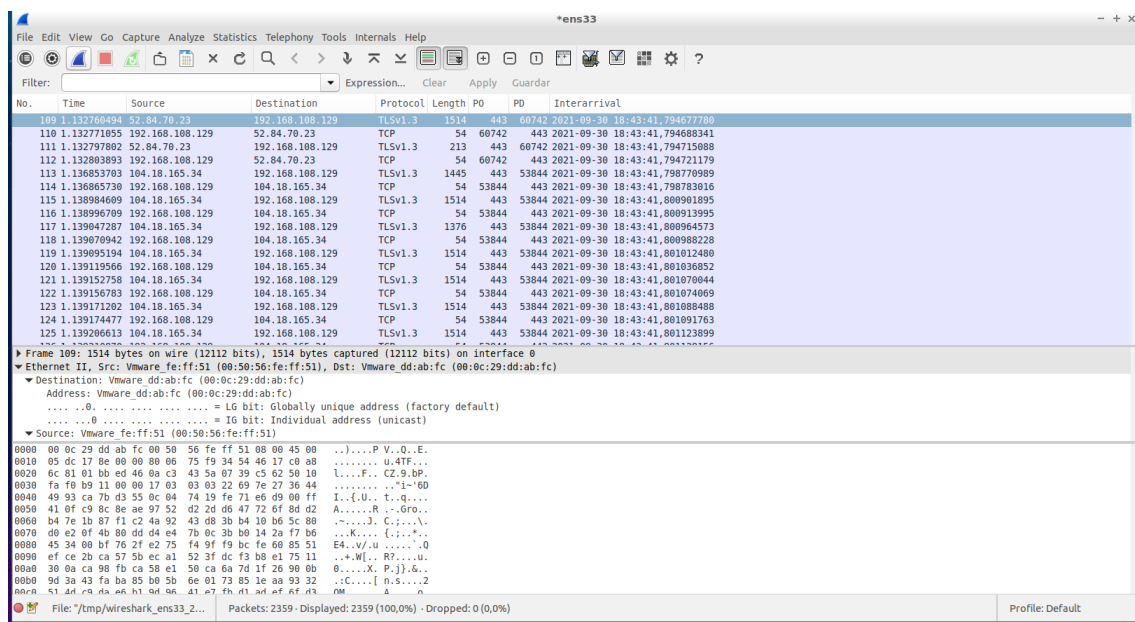
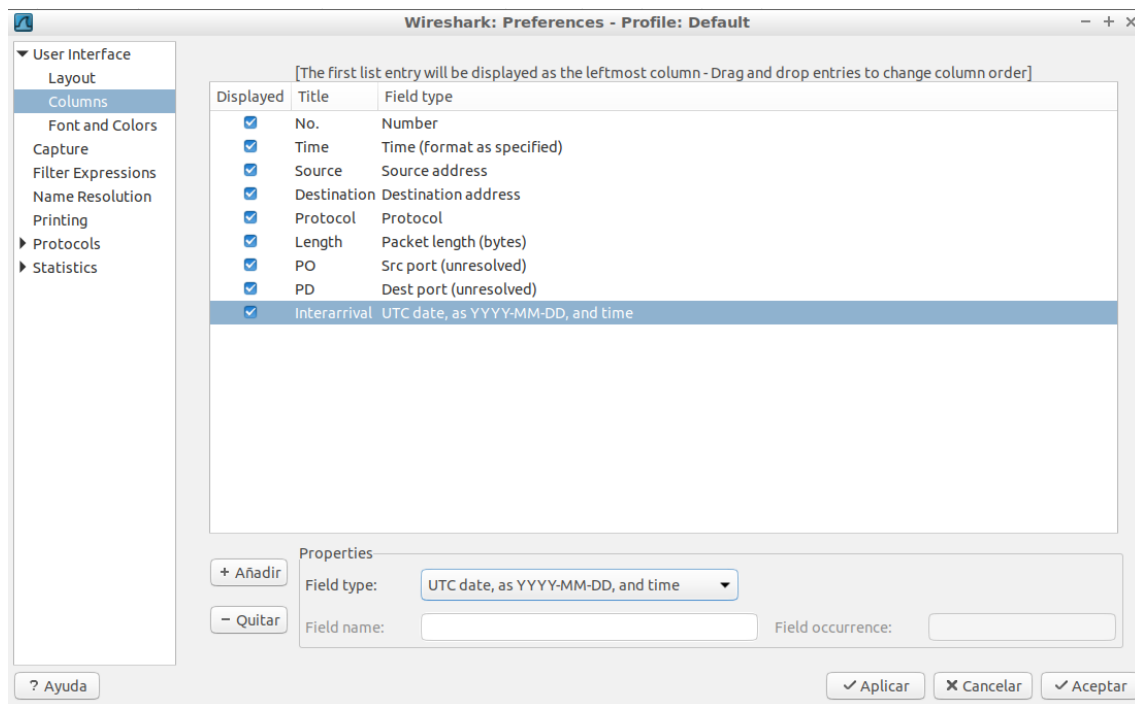
Packet 109 details:

```

Frame 109: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Vmware fe:ff:51 (00:50:56:fe:ff:51), Dst: Vmware dd:ab:fc (00:0c:29:dd:ab:fc)
  Destination: Vmware dd:ab:fc (00:0c:29:dd:ab:fc)
    Address: Vmware dd:ab:fc (00:0c:29:dd:ab:fc)
      ...0. .... = LG bit: Globally unique address (factory default)
      ...0. .... = IG bit: Individual address (unicast)
    Source: Vmware fe:ff:51 (00:50:56:fe:ff:51)
      0000 00 0c 29 dd ab fc 00 50 56 fe ff 51 00 00 45 00 ...P V..E.
      0010 05 dc 17 8e 00 00 00 06 75 19 34 54 46 17 c0 a8 .....U.4TF...
      0020 0c 01 01 bb ed 46 0a c3 43 5a 07 39 c5 62 50 10 .....F...CZ.S.bP.
      0030 fa f0 b9 11 00 00 17 03 03 03 22 69 7e 27 36 44 .....*"-60
      0040 49 93 ca 7b d3 55 0c 04 74 19 fe 71 e6 d9 00 ff I..{.U..t..q....
      0050 41 0f c9 8c 8e ae 97 52 d2 2d 06 47 72 6f 8d 02 A.....R...Gro..
      0060 b4 7e 1b 07 f1 c2 4a 92 43 d8 3b b4 10 b6 5c 80 .....J..C...N..
      0070 d0 e2 0f 4b 80 dd d4 e4 7b 0c 3b b0 14 2a f7 b6 ...K....{...*..
      0080 45 34 00 bf 76 2f e2 75 f4 9f f9 bc fe 60 85 51 E4..V/.U.....0
      0090 ef ce 2b ca 57 5b ec a1 52 3f dc f3 b8 e1 75 11 ...+W[...R7....U.
      00a0 30 0a ca 98 fb ca 58 e1 50 ca 6a 7d 1f 26 00 00 0.....X..P.jj).6..
      00b0 9d 3a 43 fa ba 85 b0 5b 6e 01 73 85 1e aa 93 32 ..C....[ n.s....2
      00c0 51 a4 c9 a8 a6 b1 04 06 a1 e7 fh a1 a4 ef 6f a3 0M...A...n
  
```

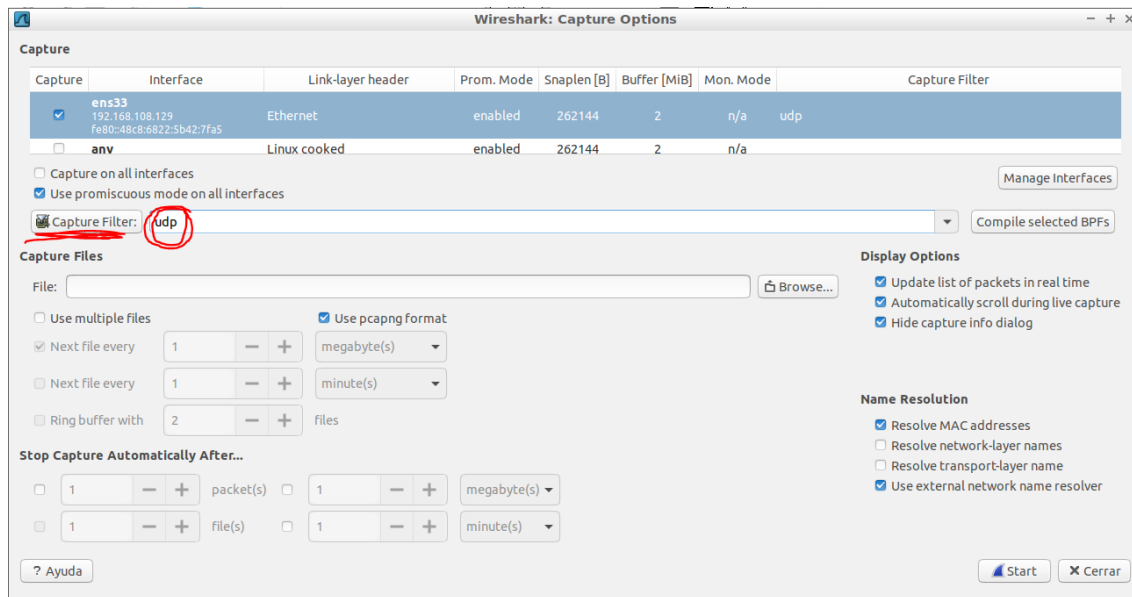
EJERCICIO 4.

Realizamos los pasos del ejercicio 3 hasta llegar al menú de las columnas. Una vez ahí, seleccionamos el “field type” correspondiente a ‘UTC Date’.



EJERCICIO 5.

5.1 Utilizamos el filtro “udp”.



5.2 Generamos tráfico.

5.3 Ejecutamos en la terminal el comando “sudo hping3 -S -p 80 www.uam.es”.

5.4 Comprobamos que solo se capturan paquetes UDP.

