

REDES DE COMUNICACIONES I

Práctica 1

Alberto Ayala, Mihai Blidaru

Grupo **1311**

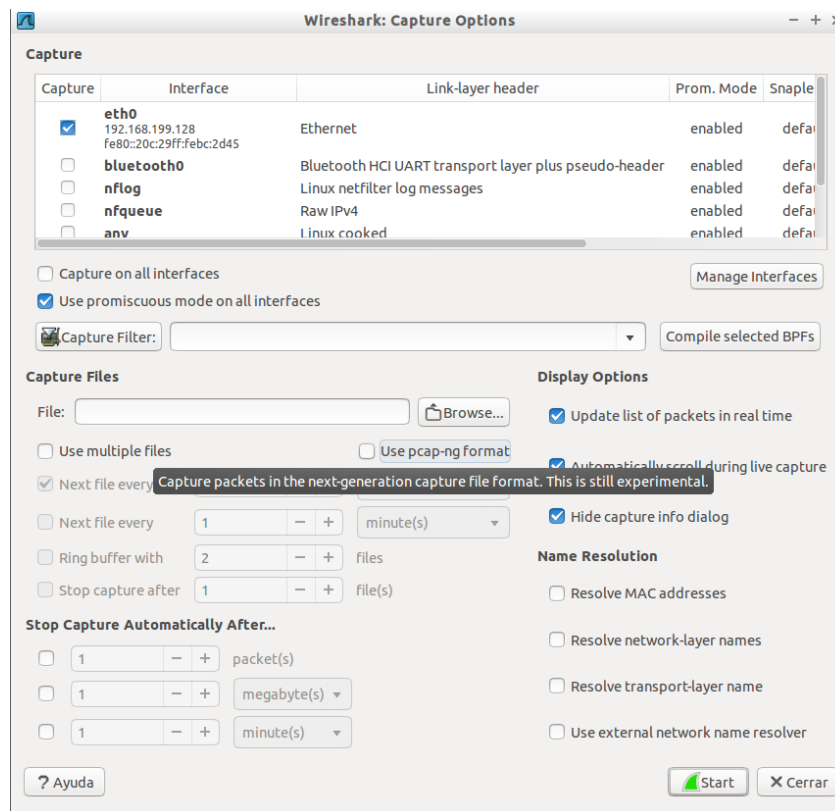
Pareja 05

Ejercicios Wireshark

- 1. Ejercicio 1 2
- 2. Ejercicio 2 4
- 3. Ejercicio 3 5
- 4. Ejercicio 4 6
- 5. Ejercicio 5 7

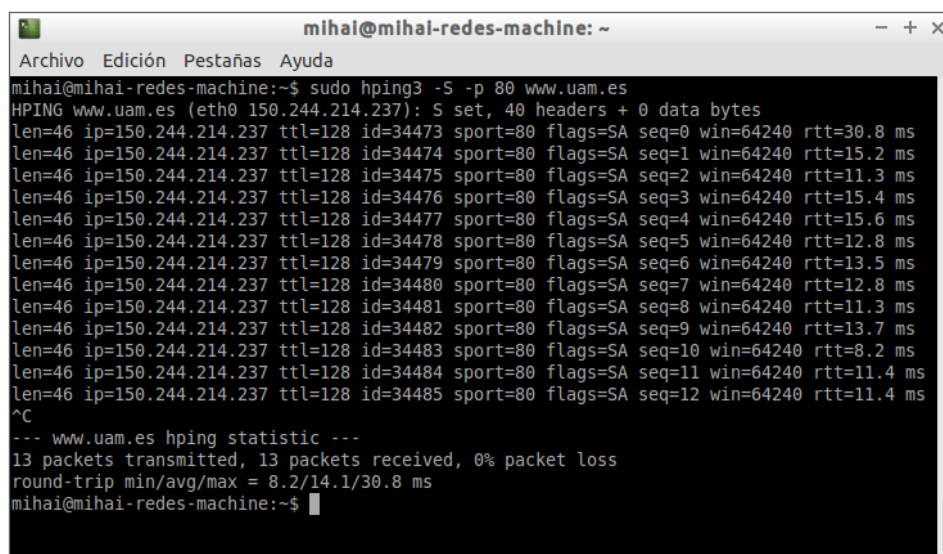
1. Ejercicio 1

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 “*use pcap-ng format*” para poder guardar la captura en el formato *pcap*.

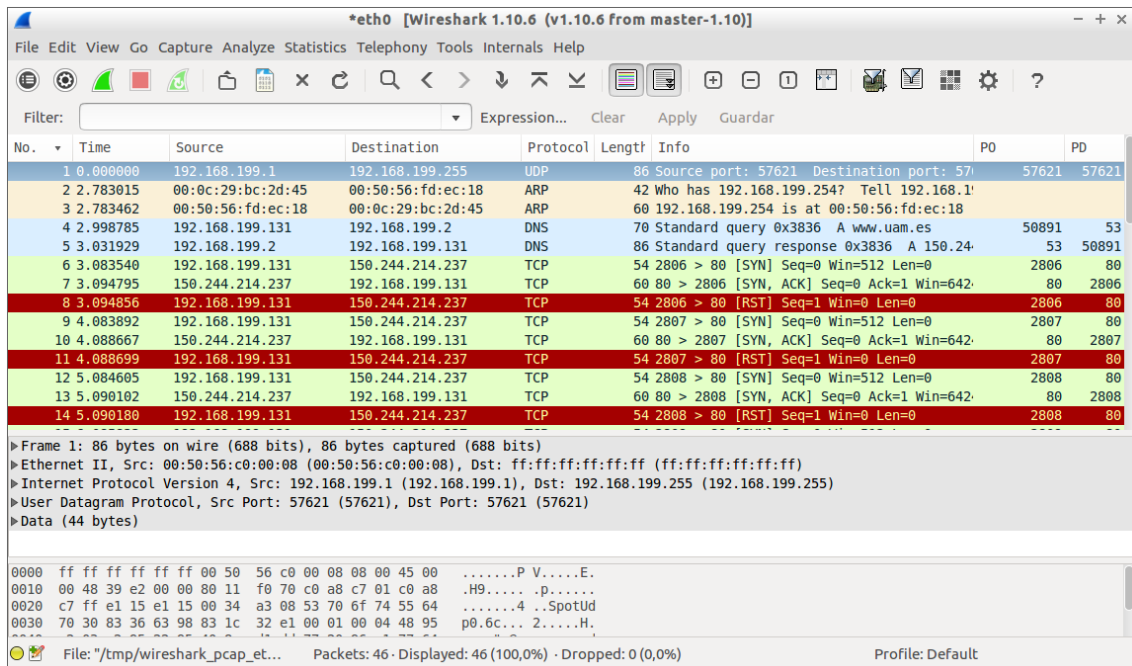


Iniciamos la captura haciendo Click en *Start* y a continuación abrimos otra consola y ejecutamos durante unos segundos el siguiente comando

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

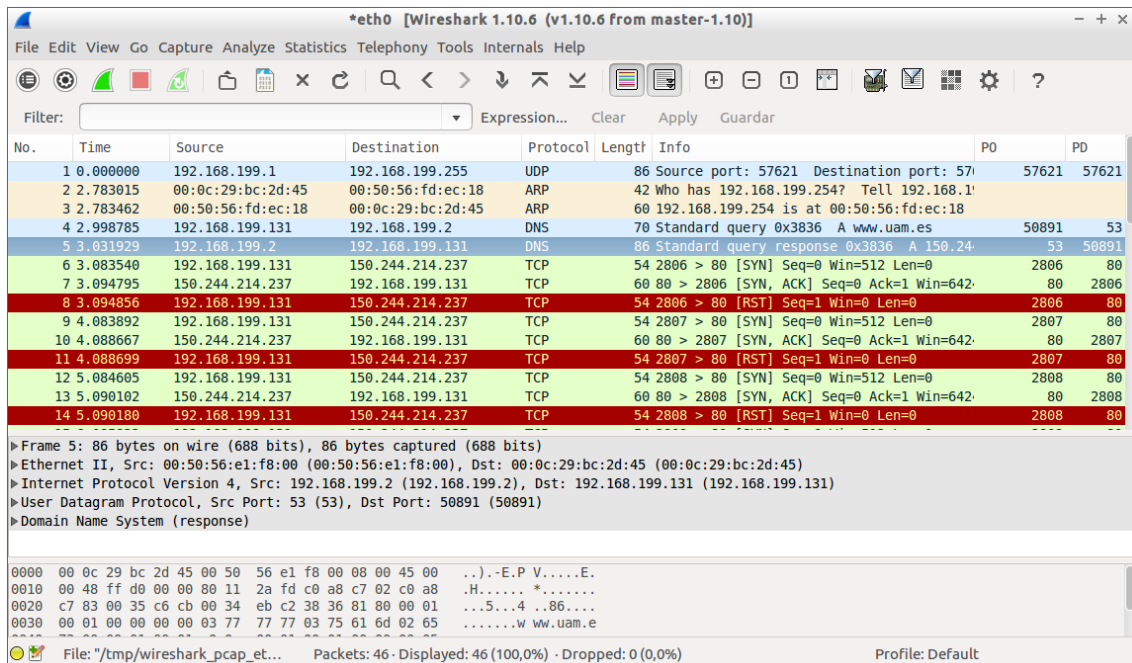


Volvemos a la ventana de *Wireshark*, paramos la captura pulsando *Stop* y analizamos los paquetes que aparecen.



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).



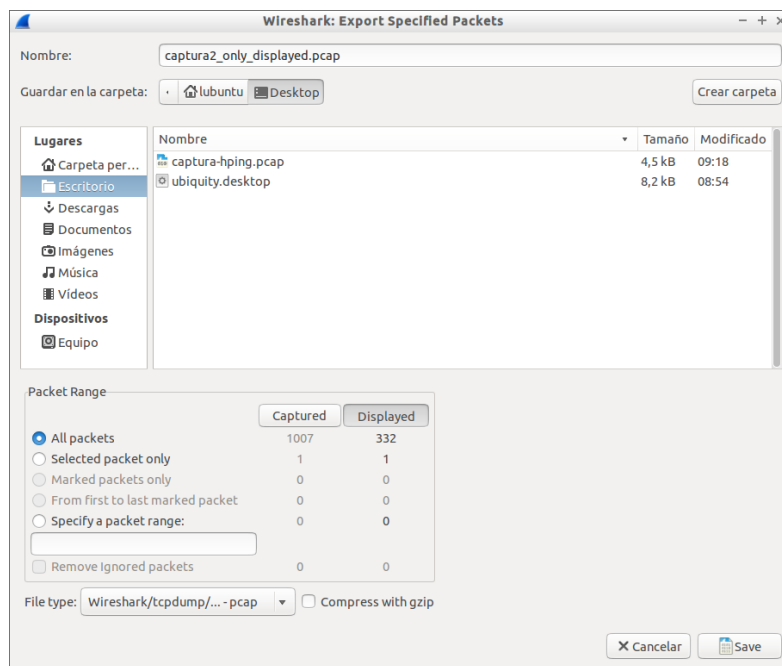
2. Ejercicio 2

2.1 El filtro que hemos usado es:

```
ip && frame.len > 1000
```

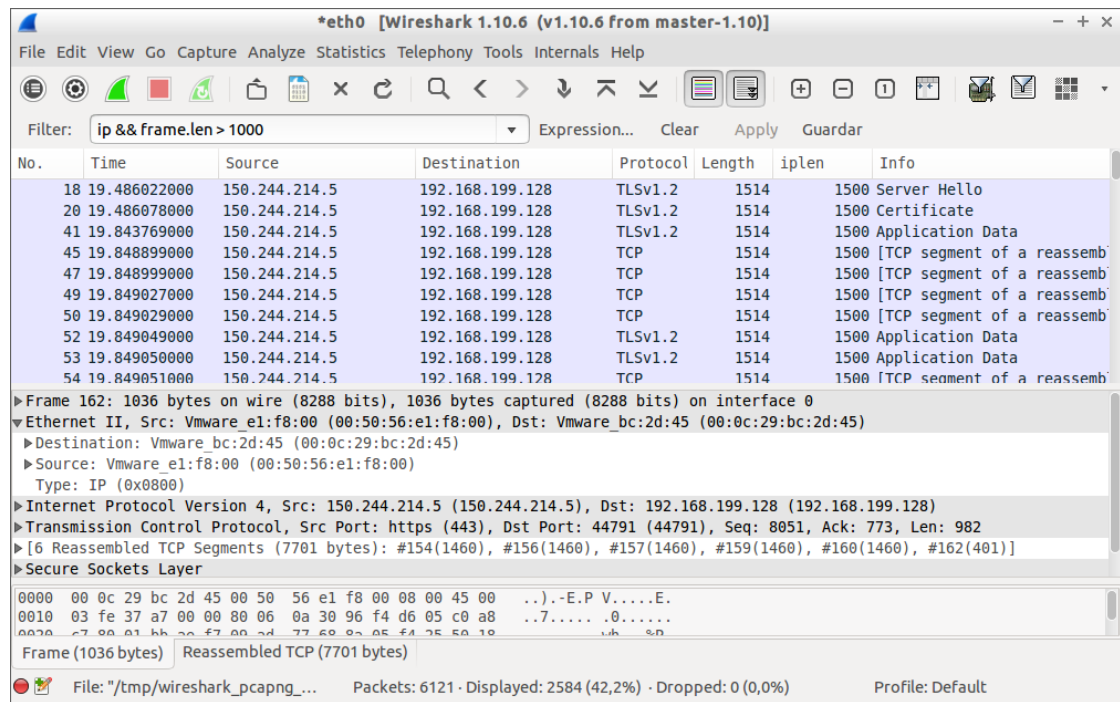
De esta forma podemos filtrar los paquetes que tengan un protocolo IP y cuyo peso sea superior a 1000Bytes.

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



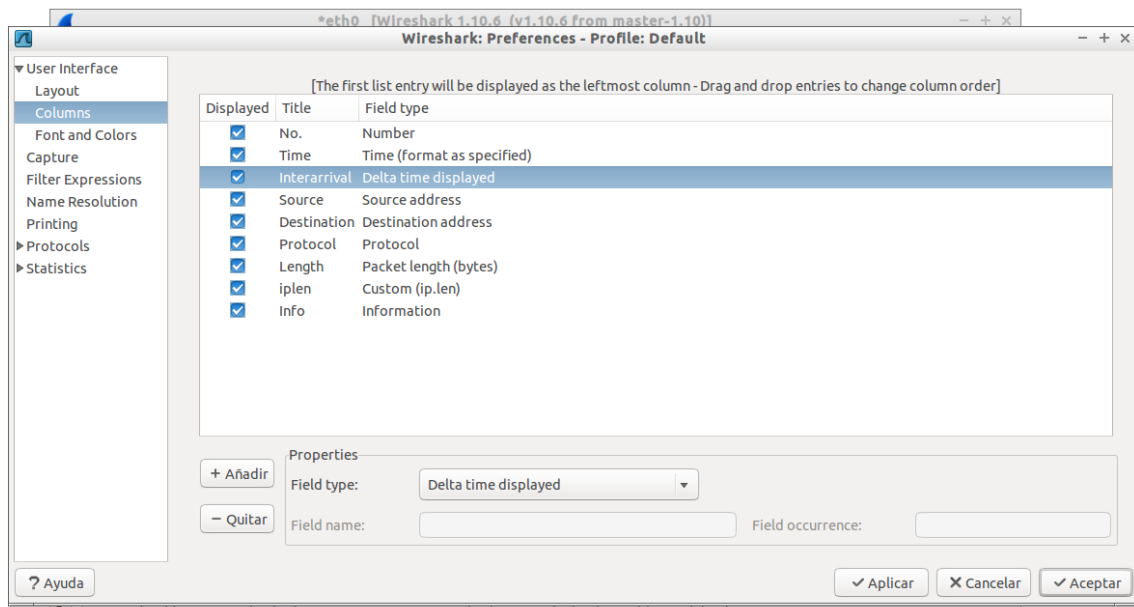
Cuando guardamos usando esta opción descubrimos que se guardaban paquetes de menos de 1000Bytes. Buscando información descubrimos que esto se debe a que *Wireshark* guarda todas las demás *frames* necesarias para la reconstrucción de toda la información de los paquetes mostrados. Fuentes: [Link 1](#) [Link 2](#) [Link 3](#) [Link 4](#)

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.



3. 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).



***eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]**

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **ip && frame.len > 1000** Expression... Clear Apply Guardar

No.	Time	Interarrival	Source	Destination	Protocol	Length	ip len	Info
18	19.486022000	0.000000000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Server Hello
20	19.486078000	0.000056000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Certificate
41	19.843769000	0.357691000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Application Data
45	19.848899000	0.005130000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
47	19.848999000	0.000100000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
49	19.849027000	0.000028000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
50	19.849029000	0.000002000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
52	19.849049000	0.000020000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Application Data
53	19.849050000	0.000001000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Application Data
54	19.849051000	0.000001000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]

▶ Frame 41: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

▼ Ethernet II, Src: Vmware_e1:f8:00 (00:50:56:e1:f8:00), Dst: Vmware_bc:2d:45 (00:0c:29:bc:2d:45)

▶ Destination: Vmware_bc:2d:45 (00:0c:29:bc:2d:45)

▶ Source: Vmware_e1:f8:00 (00:50:56:e1:f8:00)

Type: IP (0x0800)

▶ Internet Protocol Version 4, Src: 150.244.214.5 (150.244.214.5), Dst: 192.168.199.128 (192.168.199.128)

▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 44789 (44789), Seq: 3176, Ack: 688, Len: 1460

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http

0000 00 0c 29 bc 2d 45 00 50 56 e1 f8 00 08 00 45 00 ...-E.P V....E.

0010 05 dc 37 69 00 00 00 06 08 90 96 f4 d6 05 c0 a8 ..7i....

0020 c7 00 01 bb ae f5 4c b7 29 e3 e9 b1 9d 5d 50 10L.)....]P.

0030 fa f0 38 9c 00 00 17 03 03 03 10 a3 ba 37 e5 65 ..8.....7.e

0040 1a 66 4b 0b f6 02 11 62 50 6a e2 43 17 00 4a 26 ...V.C.M.

File: "/tmp/wireshark_pcapng_..." Packets: 6121 - Displayed: 2584 (42,2%) - Dropped: 0 (0,0%) Profile: Default

4. Ejercicio 4

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

***eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]**

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **ip && frame.len > 1000** Expression... Clear Apply Guardar

No.	Time	Interarrival	Source	Destination	Protocol	Length	ip len	Info
18	2018-10-08 20:23:56.264073000	0.000000000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Server Hello
20	2018-10-08 20:23:56.264129000	0.000056000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Certificate
41	2018-10-08 20:23:56.621820000	0.357691000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Application Data
45	2018-10-08 20:23:56.626950000	0.005130000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
47	2018-10-08 20:23:56.627050000	0.000100000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
49	2018-10-08 20:23:56.627078000	0.000028000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
50	2018-10-08 20:23:56.627080000	0.000002000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]
52	2018-10-08 20:23:56.627100000	0.000020000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Application Data
53	2018-10-08 20:23:56.627101000	0.000001000	150.244.214.5	192.168.199.128	TLSv1.2	1514		1500 Application Data
54	2018-10-08 20:23:56.627102000	0.000001000	150.244.214.5	192.168.199.128	TCP	1514		1500 [TCP segment]

▶ Frame 41: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

▼ Ethernet II, Src: Vmware_e1:f8:00 (00:50:56:e1:f8:00), Dst: Vmware_bc:2d:45 (00:0c:29:bc:2d:45)

▶ Destination: Vmware_bc:2d:45 (00:0c:29:bc:2d:45)

▶ Source: Vmware_e1:f8:00 (00:50:56:e1:f8:00)

Type: IP (0x0800)

▶ Internet Protocol Version 4, Src: 150.244.214.5 (150.244.214.5), Dst: 192.168.199.128 (192.168.199.128)

▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 44789 (44789), Seq: 3176, Ack: 688, Len: 1460

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http

0000 00 0c 29 bc 2d 45 00 50 56 e1 f8 00 08 00 45 00 ...-E.P V....E.

0010 05 dc 37 69 00 00 00 06 08 90 96 f4 d6 05 c0 a8 ..7i....

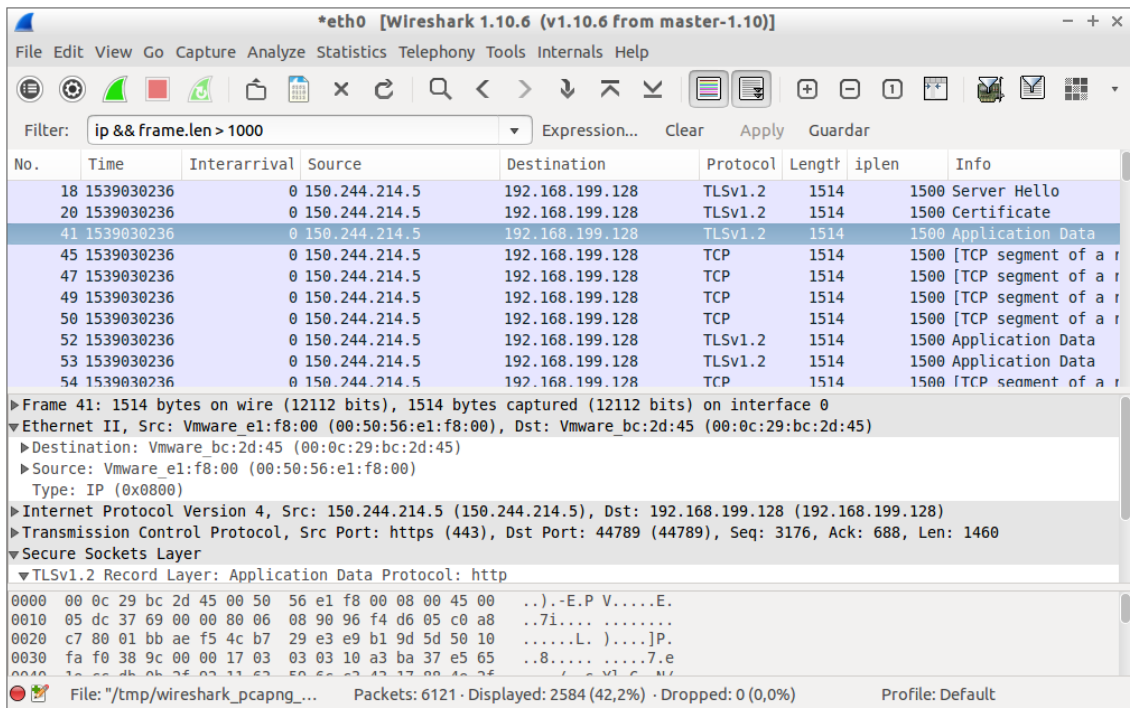
0020 c7 00 01 bb ae f5 4c b7 29 e3 e9 b1 9d 5d 50 10L.)....]P.

0030 fa f0 38 9c 00 00 17 03 03 03 10 a3 ba 37 e5 65 ..8.....7.e

0040 1a 66 4b 0b f6 02 11 62 50 6a e2 43 17 00 4a 26 ...V.C.M.

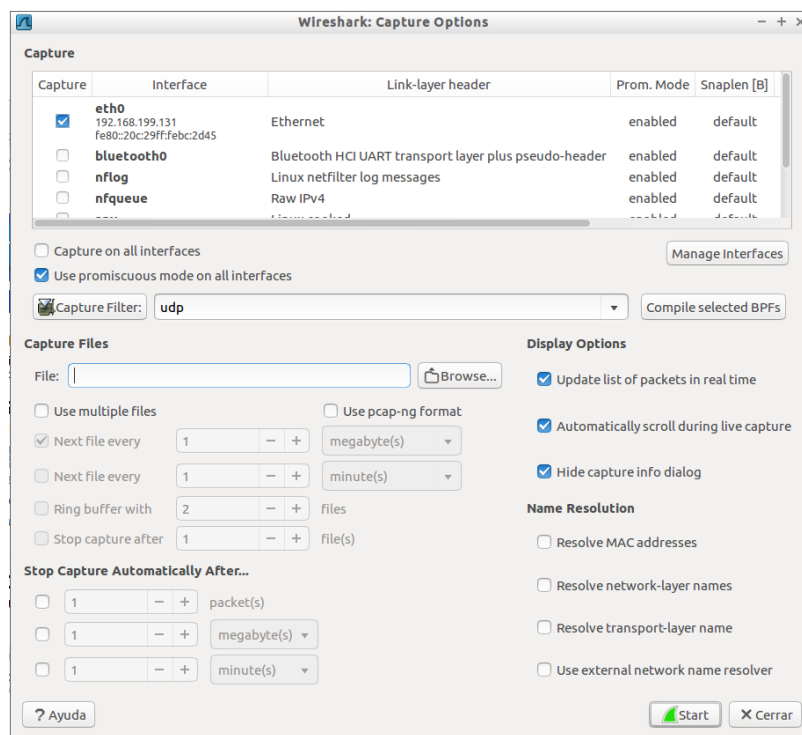
File: "/tmp/wireshark_pcapng_..." Packets: 6121 - Displayed: 2584 (42,2%) - Dropped: 0 (0,0%) Profile: Default

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.

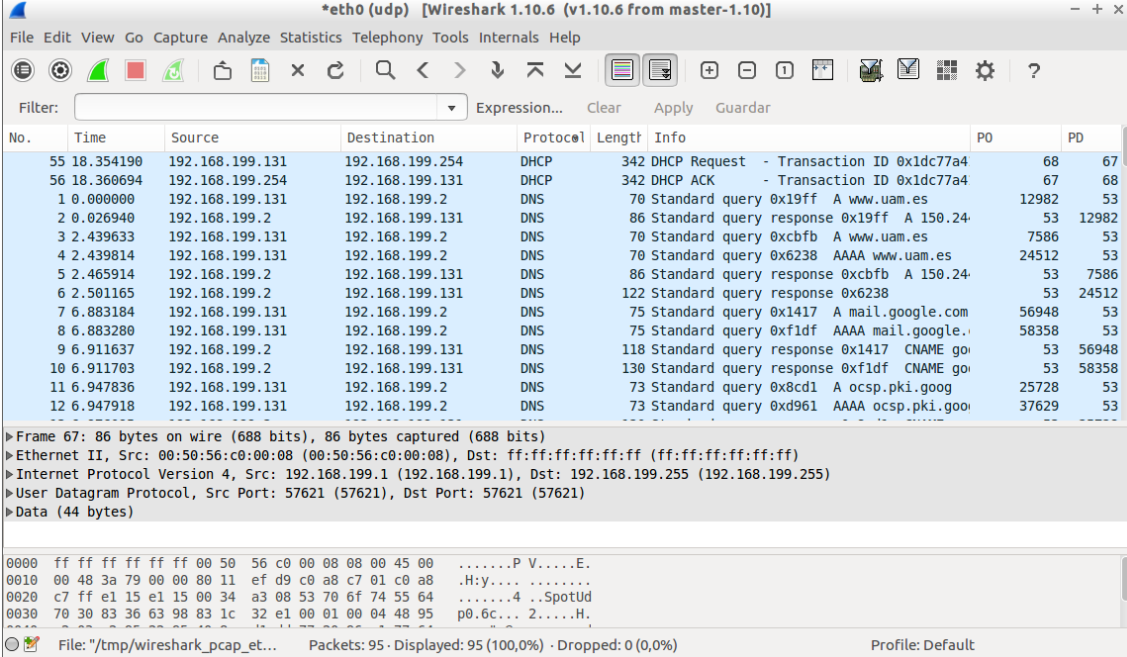


5. Ejercicio 5

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.

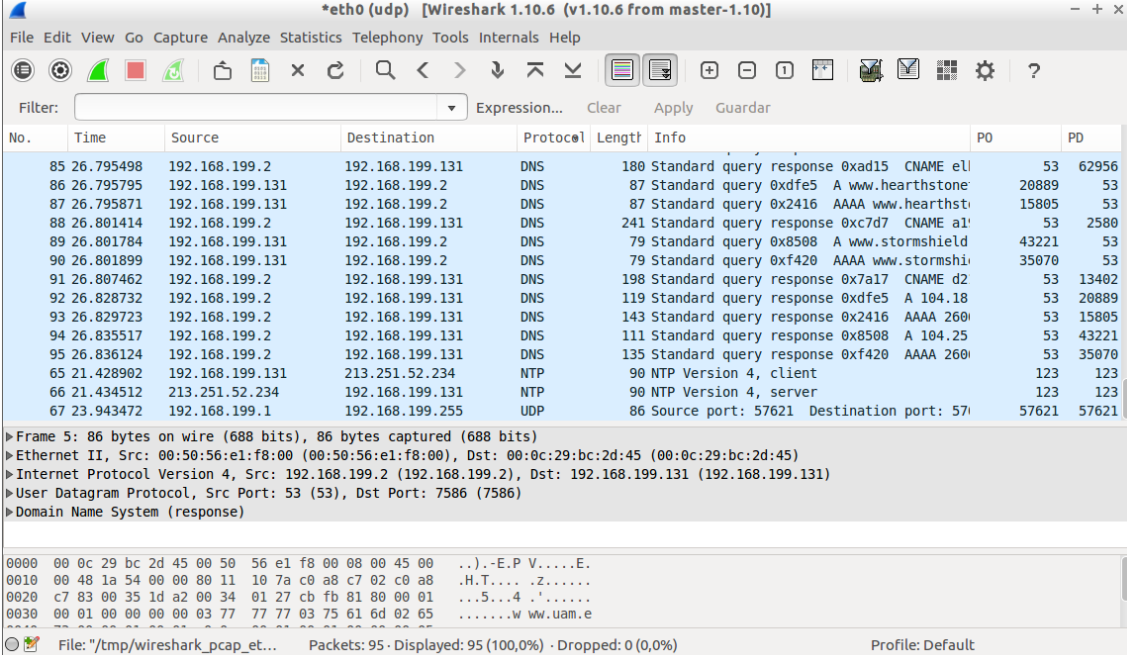


Wireshark 1.10.6 (v1.10.6 from master-1.10) interface showing a capture on *eth0 (udp). The packet list shows 12 packets, including DHCP requests and acknowledgments, and several DNS standard queries and responses. The packet details pane for packet 67 shows Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (44 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info	PO	PD
55	18.354190	192.168.199.131	192.168.199.254	DHCP	342	DHCP Request - Transaction ID 0x1dc77a4	68	67
56	18.360694	192.168.199.254	192.168.199.131	DHCP	342	DHCP ACK - Transaction ID 0x1dc77a4	67	68
1	0.000000	192.168.199.131	192.168.199.2	DNS	70	Standard query 0x19ff A www.uam.es	12982	53
2	0.026940	192.168.199.2	192.168.199.131	DNS	86	Standard query response 0x19ff A 150.24.	53	12982
3	2.439633	192.168.199.131	192.168.199.2	DNS	70	Standard query 0xcfbf A www.uam.es	7586	53
4	2.439814	192.168.199.131	192.168.199.2	DNS	70	Standard query 0x6238 AAAA www.uam.es	24512	53
5	2.465914	192.168.199.2	192.168.199.131	DNS	86	Standard query response 0xcfbf A 150.24.	53	7586
6	2.501165	192.168.199.2	192.168.199.131	DNS	122	Standard query response 0x6238	53	24512
7	6.883184	192.168.199.131	192.168.199.2	DNS	75	Standard query 0x1417 A mail.google.com	56948	53
8	6.883280	192.168.199.131	192.168.199.2	DNS	75	Standard query 0xf1df AAAA mail.google.	58358	53
9	6.911637	192.168.199.2	192.168.199.131	DNS	118	Standard query response 0x1417 CNAME go	53	56948
10	6.911703	192.168.199.2	192.168.199.131	DNS	130	Standard query response 0xf1df CNAME go	53	58358
11	6.947836	192.168.199.131	192.168.199.2	DNS	73	Standard query 0x8cd1 A ocs.pki.goog	25728	53
12	6.947918	192.168.199.131	192.168.199.2	DNS	73	Standard query 0xd961 AAAA ocs.pki.goog	37629	53

Frame 67: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:50:56:c0:00:08 (00:50:56:c0:00:08), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.199.1 (192.168.199.1), Dst: 192.168.199.255 (192.168.199.255)
User Datagram Protocol, Src Port: 57621 (57621), Dst Port: 57621 (57621)
Data (44 bytes)

0000 ff ff ff ff ff ff 00 50 56 c0 00 08 00 00 45 00P V.....E.
0010 00 48 3a 79 00 00 80 11 ef d9 c0 a8 c7 01 c0 a8 ..H:y.....
0020 c7 ff e1 15 e1 15 00 34 a3 08 53 70 6f 74 55 644 ..SpotUd
0030 70 30 83 36 63 98 83 1c 32 e1 00 01 00 04 48 95 p0.6c... 2.....H.



Wireshark 1.10.6 (v1.10.6 from master-1.10) interface showing a capture on *eth0 (udp). The packet list shows 17 packets, including several DNS standard queries and responses, and two NTP Version 4 packets. The packet details pane for packet 5 shows Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info	PO	PD
85	26.795498	192.168.199.2	192.168.199.131	DNS	180	Standard query response 0xad15 CNAME el	53	62956
86	26.795795	192.168.199.131	192.168.199.2	DNS	87	Standard query 0xdfe5 A www.hearthstone	20889	53
87	26.795871	192.168.199.131	192.168.199.2	DNS	87	Standard query 0x2416 AAAA www.hearthsto	15805	53
88	26.801414	192.168.199.2	192.168.199.131	DNS	241	Standard query response 0xc7d7 CNAME al	53	2580
89	26.801784	192.168.199.131	192.168.199.2	DNS	79	Standard query 0x8508 A www.stormshield	43221	53
90	26.801899	192.168.199.131	192.168.199.2	DNS	79	Standard query 0xf420 AAAA www.stormshi	35070	53
91	26.807462	192.168.199.2	192.168.199.131	DNS	198	Standard query response 0x7a17 CNAME d2	53	13402
92	26.828732	192.168.199.2	192.168.199.131	DNS	119	Standard query response 0xdfe5 A 104.18	53	20889
93	26.829723	192.168.199.2	192.168.199.131	DNS	143	Standard query response 0x2416 AAAA 260	53	15805
94	26.835517	192.168.199.2	192.168.199.131	DNS	111	Standard query response 0x8508 A 104.25	53	43221
95	26.836124	192.168.199.2	192.168.199.131	DNS	135	Standard query response 0xf420 AAAA 260	53	35070
65	21.428902	192.168.199.131	213.251.52.234	NTP	90	NTP Version 4, client	123	123
66	21.434512	213.251.52.234	192.168.199.131	NTP	90	NTP Version 4, server	123	123
67	23.943472	192.168.199.1	192.168.199.255	UDP	86	Source port: 57621 Destination port: 57621	57621	57621

Frame 5: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:50:56:e1:f8:00 (00:50:56:e1:f8:00), Dst: 00:0c:29:bc:2d:45 (00:0c:29:bc:2d:45)
Internet Protocol Version 4, Src: 192.168.199.2 (192.168.199.2), Dst: 192.168.199.131 (192.168.199.131)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 7586 (7586)
Domain Name System (response)

0000 00 0c 29 bc 2d 45 00 50 56 e1 f8 00 08 00 45 00 ...).-E.P V.....E.
0010 00 48 1a 54 00 00 80 11 10 7a c0 a8 c7 02 c0 a8 ..H.T....Z.....
0020 c7 83 00 35 1d a2 00 34 01 27 cb fb 81 80 00 01 ...5...4 '.....
0030 00 01 00 00 00 00 03 77 77 77 03 75 61 6d 02 65w www.uam.e