

Ejercicio 1. Clasifica las siguientes tareas indicando la capa del modelo OSI a la que pertenecen:

Funcionalidad	Nº capa	Nombre de capa
Enrutamiento	3	Nivel de red
Tipos de conectores y cables	1	Nivel físico
Fragmentación	3	Nivel de red
Secuencia de pasos de una sesión	5	Nivel de sesión
Uso de aplicaciones típicas	7	Nivel de aplicación
Direccionamiento local	2	Nivel de enlace
Control de errores	3	Nivel de red
Encriptación de datos	6	Nivel de presentación
Direccionamiento global	3	Nivel de red
Características de las señales	1	Nivel físico
Detección de errores	2	Nivel de enlace
Uso de puertos	4	Nivel de transporte
Checkpointing	5	Nivel de sesión
Compresión de datos	6	Nivel de presentación
Conversación directa entre programas	4	Nivel de transporte

Ejercicio 2. Clasifica los siguientes protocolos dependiendo del nivel del modelo TCP/IP al que pertenecen:

Protocolo	Nombre del nivel
TCP	Nivel de transporte
DNS	Nivel de aplicación
IPv4/IPv6	Nivel de red
ARP	Nivel de red
DHCP	Nivel de aplicación
802.11	Nivel de enlace
ICMP	Nivel de red
UDP	Nivel de transporte
Ethernet	Nivel de enlace
HTTP	Nivel de aplicación

Ejercicio 3. ¿Verdadero o falso? Marca con el color adecuado cada frase:

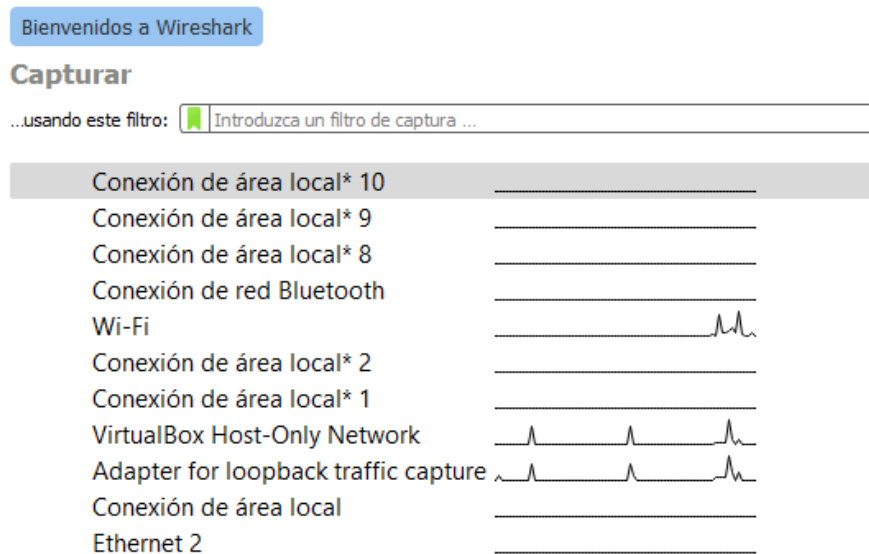
1. Los niveles superiores son cercanos al usuario mientras que los inferiores son cercanos al hardware
2. Cuando se envían datos, el emisor recorre los niveles empezando desde el inferior y acabando en el superior
3. Las redes cableadas son, en general, más seguras que las WLAN
4. Las señales analógicas son aquellas que toman únicamente dos valores
5. En el modelo OSI, el nivel de transporte está inmediatamente encima del nivel de enlace
6. El nivel de red corresponde a la capa 3 del modelo OSI
7. El nivel de transporte es el encargado de realizar el enrutamiento o encaminamiento
8. El checkpointing consiste en calcular un número mediante operaciones matemáticas y enviarlo junto con los datos, para que el receptor compruebe si durante el envío se han producido errores
9. En el nivel de transporte podemos usar dos protocolos: TCP e IP
10. Una dirección MAC ocupa 6 bytes
11. Para enviar datos fuera de una LAN, hay que enviarlos al router
12. La fragmentación la realiza el protocolo UDP
13. Un puerto es un número que identifica una aplicación o programa en un dispositivo
14. UDP es rápido y seguro mientras que TCP es lento e inseguro
15. Un RFC es un tipo de documento donde se recogen todas las características de un protocolo
16. Ethernet es la tecnología estándar más usada en redes locales
17. La cabecera Ethernet de un paquete ocupa 20 bytes
18. El orden de las cabeceras en un paquete es: Ethernet+IP+TCP
19. Si enviamos un email, enviamos un paquete de datos solamente
20. Wireshark es una herramienta que nos permite capturar paquetes de datos para su posterior análisis

Ejercicio 4. Práctica: Introducción a Wireshark.

Wireshark es un analizador de protocolos de red. Es un programa que permite visualizar en tiempo real todos los paquetes de datos (tanto los que entran como los que salen) de tu ordenador. A este tipo de programas también se les llama “sniffers”, ya que se dedican a “olfatear” la conexión de red de tu equipo constantemente. El hecho de que se presente este programa en esta unidad es porque Wireshark permite visualizar paquetes y ver claramente todas y cada una de las cabeceras del modelo TCP/IP ya estudiadas. Este programa tiene multitud de usos en una LAN, desde detectar intrusos, anomalías en el tráfico, inspección detallada de paquetes individuales, análisis del comportamiento de la red, etc.

a) **Instalación de Wireshark.** Descarga e instala Wireshark de la página oficial (<https://www.wireshark.org/>). Existen versiones tanto para Windows como para Linux. Durante la instalación, asegúrate de marcar la casilla de “Instalar Npcap” para que el programa funcione correctamente. No es necesario que instales USBPcap. El resto de opciones puedes dejarlas por defecto tal y como aparecen. Después de la instalación, abre el programa.

b) **Primera captura.** Ahora vas a realizar tu primera captura de paquetes. Cuando abres Wireshark, te aparecerá un listado con todas las conexiones de red disponibles en tu equipo, parecido a este.



En tu ordenador no tiene por qué aparecer el mismo listado de conexiones que en la imagen, dependerá de la configuración de red de tu ordenador. Ahora deberás seleccionar aquella conexión de red que tengas activa en este momento. La reconocerás porque la gráfica que aparece junto a la conexión no es una línea plana, sino que va oscilando. En el ejemplo de la imagen superior, se seleccionaría la conexión “Wi-Fi” (de las otras dos cuya gráfica no es una línea plana, una es virtual y de momento no nos interesa, y la otra está destinada a otros usos). Haz ahora doble clic en la conexión que corresponda de tu ordenador. A partir de entonces, Wireshark se pondrá a capturar, es decir, a mostrar absolutamente todos los paquetes que envíes o recibas en ese momento. Probablemente Wireshark te mostrará un listado de paquetes que irá creciendo pese a que aparentemente no estés haciendo nada con tu red. Sin cerrar Wireshark, prueba ahora a abrir el navegador y abrir dos o tres páginas web cualesquiera para tener más paquetes aún en el listado. Para terminar de capturar, vuelve a Wireshark y haz clic en el botón de parar (el del cuadrado rojo) en la barra de herramientas (segundo botón), o menú Captura, Detener:



c) **Secciones de la pantalla en Wireshark.** Además del clásico menú, la barra de herramientas y la barra de filtros (de ella hablaremos en unidades posteriores), Wireshark divide la pantalla en tres grandes secciones:

tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

▼ Domain Name System (response)

[Request In: 348]

[Time: 0.034338000 seconds]

Transaction ID: 0x2188

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

▼ Queries

> cdn-0.nflximg.com: type A, class IN

> Answers

> Authoritative nameservers

0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5....?[]....

0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6cc dn-0.nfl

0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com

0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73). ".images

0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg

0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

- La zona superior es el listado con todos los paquetes capturados, coloreados según su protocolo principal
- La zona central muestra información sobre las cabeceras y protocolos de un paquete concreto de todo el listado, que habrá seleccionado el usuario
- La zona inferior muestra lo mismo que la central, pero sin analizar ni procesar (es decir, muestra todo el paquete directamente en hexadecimal)

Vamos a seleccionar un paquete. Para ello, fíjate que en la zona superior (listado de paquetes), cada paquete va acompañado de un número. Desplázate hasta, por ejemplo, el paquete número 100 y haz clic (solo una vez) en él. Verás que la zona central y la inferior cambian, mostrando los datos de ese paquete en concreto.

d) Análisis del listado de paquetes. Vamos a centrarnos ahora en la zona superior:

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

Para cada paquete aparece, de izquierda a derecha:

- N.º de paquete
- Instante en el que se capturó: n.º de segundos transcurridos desde que se empezó a capturar hasta que apareció ese paquete en concreto
- Origen: la dirección desde donde salió el paquete (normalmente, una dirección IP)
- Destino: la dirección a la que se envió el paquete (normalmente, una dirección IP)
- Protocolo: protocolo principal del paquete (normalmente, el del nivel de aplicación)
- Longitud: tamaño total del paquete (cabeceras+datos), expresado en bytes
- Información: diversos datos sobre el paquete. Esta información es muy variable y depende del tipo de paquete. Es como un breve resumen de la utilidad del paquete

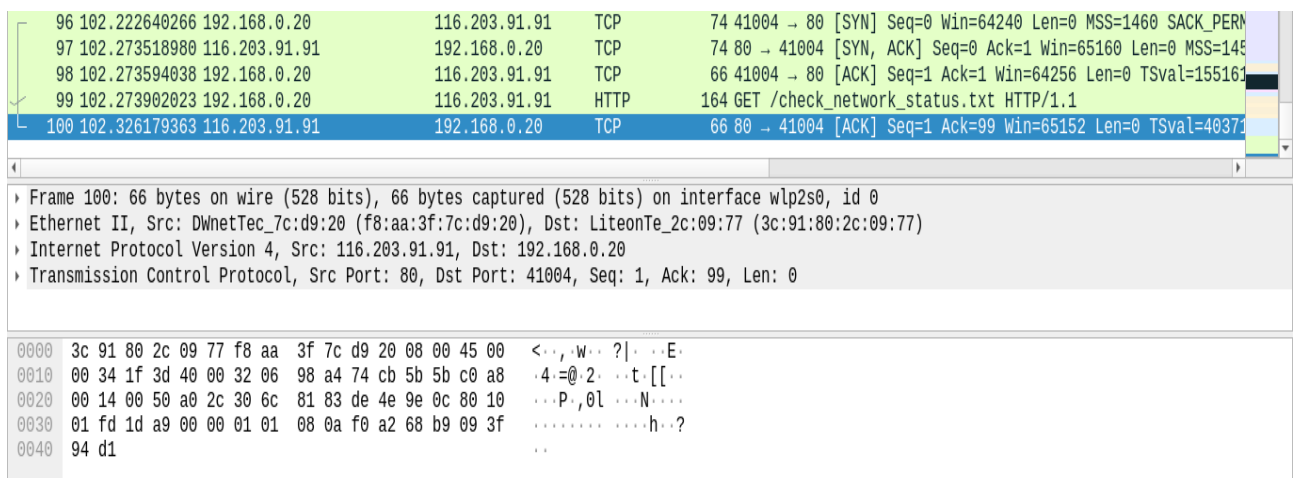
Puedes estirar cada columna si no ves toda la información. También puedes usar los botones de zoom para mostrar la fuente más o menos grande:



Pega aquí un recorte de una captura de pantalla (recuerda: Windows+Mayúsculas+S) donde aparezca solamente la línea con tu paquete número 100 e indica, de ese paquete:

- Dirección origen: 116.203.91.91
- Dirección destino: 192.168.0.20
- Longitud: 66 bytes

Captura de pantalla:



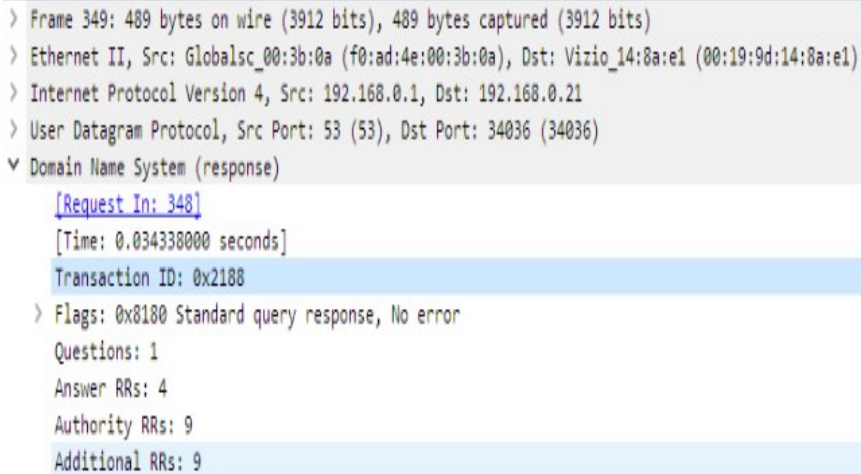
e) **Grabar una captura en fichero.** Si queremos guardarnos todos los datos de los paquetes en un fichero, bastará simplemente con hacer clic en este botón (o menú Archivo, Guardar):



Guarda el fichero con el nombre prueba1. La extensión usada por Wireshark suele ser .pcapng o también .pcap. Ahora en el fichero están guardados todos los paquetes de la sesión. En unidades posteriores, aparecerán ejercicios donde, en lugar de capturar tus

propios paquetes, deberás abrir un fichero con otra captura hecha en otro ordenador y tendrás que analizar su contenido.

f) **Detalles de un paquete.** Haz clic en un paquete cualquiera y observa la sección central de la pantalla de Wireshark:



The screenshot shows the 'Packet Details' pane in Wireshark for frame 349. The tree on the left shows the hierarchy: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The 'Domain Name System (response)' section is expanded, showing details like '[Request In: 348]', '[Time: 0.034338000 seconds]', 'Transaction ID: 0x2188', 'Flags: 0x0180 Standard query response, No error', 'Questions: 1', 'Answer RRs: 4', 'Authority RRs: 9', and 'Additional RRs: 9'. The 'Transaction ID' and 'Flags' fields are highlighted in blue.

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0
> Ethernet II, Src: GlobalSC_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
  [Request In: 348]
  [Time: 0.034338000 seconds]
  Transaction ID: 0x2188
  Flags: 0x0180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 9
  Additional RRs: 9
```

Aparecerá el contenido de tu paquete seleccionado, clasificado por los protocolos del modelo TCP/IP. De arriba a abajo, aparece una primera línea con información general del paquete (también llamado “frame”), indicando su n.º y tamaño en bytes y bits, y después aparece una línea gris por cada cabecera, empezando por la capa inferior, y luego los niveles de red, transporte y aplicación.

Responde a las siguientes preguntas respecto a la imagen anterior:

- ¿Qué protocolo usa el paquete 349 en las capas inferiores? Ethernet
- ¿Qué protocolo usa el paquete 349 en el nivel de red? IPv4
- ¿Qué protocolo usa el paquete 349 en el nivel de transporte UDP
- ¿Qué protocolo usa el paquete 349 en el nivel de aplicación? DNS

Observa que podrías abrir la sección correspondiente a cada protocolo para obtener más información del mismo haciendo clic en el símbolo “>” de cada cabecera. De momento no es necesario que lo hagas, basta con que veas la separación en cabeceras y cómo se corresponde la información que te proporciona Wireshark con la estructura del modelo TCP/IP.

Ahora escoge tres paquetes cualesquiera de entre todos los que has capturado antes, y para cada uno de ellos, pega aquí una imagen con la sección central de la pantalla y responde a las preguntas:

N.º paquete: 15

Pantallazo de la sección central:

13	12.221299625	192.168.0.1	192.168.0.20	DNS	104 Standard query response 0xe923 AAAA ping.manjaro.org AAAA
14	13.336936083	fe80::621a:76c8:ecba:49fe	ff02::2	ICMPv6	62 Router Solicitation
15	17.305530157	192.168.0.14	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "C
16	27.340617487	192.168.0.14	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "C
17	27.545936269	DWnetTec_7c:d9:20	LiteonTe_2c:09:77	ARP	60 Who has 192.168.0.20? Tell 192.168.0.1
18	27.545968778	LiteonTe_2c:09:77	DWnetTec_7c:d9:20	ARP	42 192.168.0.20 is at 3c:91:80:2c:09:77
19	29.286903979	1.1.1.2	239.255.255.250	SSDP	314 NOTIFY * HTTP/1.1

Frame 15: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface wlp2s0, id 0
Ethernet II, Src: Sagemcom_a2:1e:39 (58:2f:f7:a2:1e:39), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.0.14, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

¿Qué protocolo usa este paquete en las capas inferiores? Ethernet

¿Qué protocolo usa este paquete en el nivel de red? IPv4

¿Qué protocolo usa este paquete en el nivel de transporte UDP

¿Qué protocolo usa este paquete en el nivel de aplicación? MDNS

N.º paquete: 11

Pantallazo de la pantalla de la sección central:

9	12.083158589	LiteonTe_2c:09:77	DWnetTec_7c:d9:20	ARP	42 192.168.0.20 is at 3c:91:80:2c:09:77
10	12.201062643	192.168.0.20	192.168.0.1	DNS	76 Standard query 0xd338 A ping.manjaro.org
11	12.201131269	192.168.0.20	192.168.0.1	DNS	76 Standard query 0xe923 AAAA ping.manjaro.org
12	12.218417261	192.168.0.1	192.168.0.20	DNS	92 Standard query response 0xd338 A ping.manjaro.org A 116.2
13	12.221299625	192.168.0.1	192.168.0.20	DNS	104 Standard query response 0xe923 AAAA ping.manjaro.org AAAA
14	13.336936083	fe80::621a:76c8:ecba:49fe	ff02::2	ICMPv6	62 Router Solicitation

Frame 11: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface wlp2s0, id 0
Ethernet II, Src: LiteonTe_2c:09:77 (3c:91:80:2c:09:77), Dst: DWnetTec_7c:d9:20 (f8:aa:3f:7c:d9:20)
Internet Protocol Version 4, Src: 192.168.0.20, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 55554, Dst Port: 53
Domain Name System (query)

¿Qué protocolo usa este paquete en las capas inferiores? Ethernet

¿Qué protocolo usa este paquete en el nivel de red? IPv4

¿Qué protocolo usa este paquete en el nivel de transporte UDP

¿Qué protocolo usa este paquete en el nivel de aplicación? DNS

N.º paquete: 71

Pantallazo de la pantalla de la sección central:

69	60.724048602	34.76.0.142	192.168.0.20	TLSv1.2	108 Application Data
70	60.765376451	192.168.0.20	34.76.0.142	TCP	66 59908 → 443 [ACK] Seq=1553 Ack=4981 Win=64128 Len=0 TSval
71	66.356338684	34.76.0.142	192.168.0.20	TLSv1.2	930 Application Data
72	66.356385192	192.168.0.20	34.76.0.142	TCP	66 59908 → 443 [ACK] Seq=1553 Ack=5845 Win=64128 Len=0 TSval
73	66.358028460	192.168.0.20	34.76.0.142	TLSv1.2	108 Application Data
74	66.397932541	34.76.0.142	192.168.0.20	TCP	66 443 → 59908 [ACK] Seq=5845 Ack=1595 Win=64128 Len=0 TSval
75	67.277376574	192.168.0.14	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "C
76	74.036278777	DWnetTec_7c:d9:20	LiteonTe_2c:09:77	ARP	60 Who has 192.168.0.20? Tell 192.168.0.1

Frame 71: 930 bytes on wire (7440 bits), 930 bytes captured (7440 bits) on interface wlp2s0, id 0
Ethernet II, Src: DWnetTec_7c:d9:20 (f8:aa:3f:7c:d9:20), Dst: LiteonTe_2c:09:77 (3c:91:80:2c:09:77)
Internet Protocol Version 4, Src: 34.76.0.142, Dst: 192.168.0.20
Transmission Control Protocol, Src Port: 443, Dst Port: 59908, Seq: 4981, Ack: 1553, Len: 864
Transport Layer Security

¿Qué protocolo usa este paquete en las capas inferiores? Ethernet

¿Qué protocolo usa este paquete en el nivel de red? IPv4

¿Qué protocolo usa este paquete en el nivel de transporte TCP

¿Qué protocolo usa este paquete en el nivel de aplicación? TLS

Observa también que junto a cada protocolo, aparece información básica de ese protocolo, como las direcciones origen y destino. Recuerda que, como se ha dicho en la unidad:

- Ethernet usa direcciones MAC, que sirven para distinguir entre dispositivos en una LAN.
- El protocolo IP (nivel de red) usa direcciones IP, que sirven para distinguir entre dispositivos tanto en una LAN como fuera de ella
- Tanto el protocolo TCP como UDP (ambos en el nivel de transporte) usan puertos, que sirven para distinguir entre aplicaciones software dentro de un mismo dispositivo

Y para cada uno de ellos, aparece especificada la dirección origen (la del emisor, quien manda el paquete) y la dirección destino (la del receptor, quien recibe el paquete).

Dado el siguiente paquete:

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsec_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
▼ Domain Name System (response)
  [Request In: 348]
  [Time: 0.034338000 seconds]
  Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 9
  Additional RRs: 9
```

Escribe los siguientes datos relativos al paquete de la imagen:

- Dirección MAC origen: f0:ad:4e:00:3b:0a
- Dirección MAC destino: 00:19:9d:14:8a:e1
- Nivel de red. Dirección IP origen: 192.168.0.1
- Nivel de red. Dirección IP destino: 192.168.0.21
- Nivel de transporte. Puerto origen: 53
- Nivel de transporte. Puerto destino: 3403

Ahora repite la actividad con los mismos tres paquetes seleccionados por ti anteriormente. Puede ser que debido a los paquetes que hayas seleccionado no aparezcan algunas direcciones, en ese caso puedes dejarlas en blanco (aunque las direcciones MAC siempre deberían aparecer):

	MAC origen	MAC destino	IP origen	IP destino	Puerto origen	Puerto destino
Paquete 1	58:2f:f7:a2:1e:39	01:00:5e:00:00:fb	192.168.0.14	224.0.0.251	5353	5353
Paquete 2	3c:91:80:2c:09:77	f8:aa:3f:7c:d9:20	192.168.0.20	192.168.0.1	55554	53
Paquete 3	f8:aa:3f:7c:d9:20	3c:91:80:2c:09:77	34.76.0.2142	192.168.0.20	443	59908

g) **Contenido del paquete.** En la tercera sección de la pantalla del Wireshark aparecen, uno a uno, los bytes en hexadecimal de todo el paquete, sin procesar ni analizar:

0020	00 15 00 35 84 f4 01 c7	83 3f 21 88 81 80 00 01	...5.... ?!....
0030	00 04 00 09 00 09 05 63	64 6e 2d 30 07 6e 66 6cc dn-0.nfl
0040	78 69 6d 67 03 63 6f 6d	00 00 01 00 01 c0 0c 00	ximg.com
0050	05 00 01 00 00 05 29 00	22 06 69 6d 61 67 65 73). ".images
0060	07 6e 65 74 66 6c 69 78	03 63 6f 6d 09 65 64 67	.netflix .com.edg
0070	65 73 75 69 74 65 03 6e	65 74 00 c0 2f 00 05 00	esuite.n et../...

Como ves, aparecen organizados en 3 partes:

- En la izquierda, aparece el n.º de byte de cada paquete (0010, 0020, 0030, etc), por si nos interesa localizar un byte concreto según su posición.
- En la segunda se nos muestra directamente en hexadecimal el contenido del paquete. Así es como realmente viajan los paquetes por la red, como una secuencia de bytes uno detrás de otro. Por suerte, Wireshark es capaz de mostrar la información de manera que la podamos entender, como has visto en el apartado anterior. Pero tanto esta sección como la anterior en realidad muestran lo mismo, solo que aquí aparecen los datos sin procesar (por eso a esta sección se le llama también “raw content” o “contenido crudo”).
- A la derecha aparece lo mismo que en la parte central, solo que para cada byte aparece asociado su código ASCII si es posible, mostrando la letra o símbolo correspondiente (o un punto si el carácter no es imprimible). A veces mirando esta sección aparece texto que podemos leer y entender, dándonos pistas sobre el contenido del paquete.

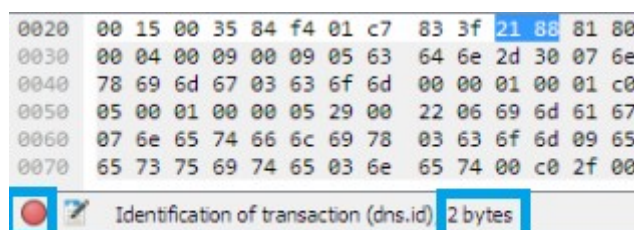
Cada vez que haces clic en un elemento de la parte central, aparece resaltada su posición exacta en la parte inferior:

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
▼ Domain Name System (response)
  [Request In: 348]
  [Time: 0.034338000 seconds]
  Transaction ID: 0x2188
  > Flags: 0x0180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 9
  Additional RRs: 9
  ▼ Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

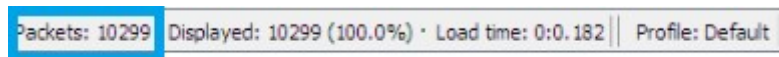
0020	00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01	...5.... .?!.
0030	00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6cc dn-0.nfl
0040	78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00	ximg.com
0050	05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73). ".images
0060	07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67	.netflix .com.edg
0070	65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00	esuite.n et../...

Prueba a hacer clic en varios elementos de la parte central de un paquete y observa cómo Wireshark marca en qué localización exacta del paquete está cada byte seleccionado.

Para terminar con la información que aparece en la pantalla, en la parte inferior tienes la barra de estado. Cada vez que haces clic en un elemento del paquete, aparece su tamaño en bytes. Además se muestra un punto rojo (si has parado de capturar paquetes) o un punto verde (si aún estás capturando paquetes en este momento):

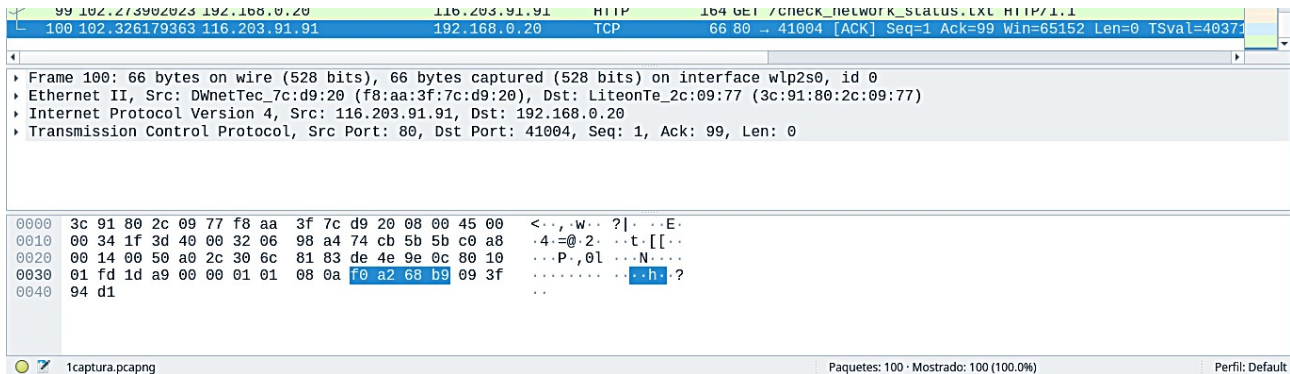


Y en la misma barra de estado, en la parte derecha aparece más información, como por ejemplo el n.º total de paquetes que has capturado:

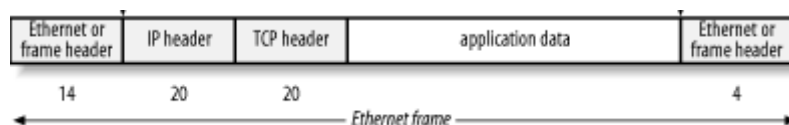


¿Cuántos paquetes has capturado tú? 100 paquetes.

Adjunta aquí una captura de pantalla de tu barra de estado completa.



h) **Tamaños de las cabeceras en TCP/IP.** Recuerda que los paquetes están formados por una serie de cabeceras (tres en total, una por cada nivel: inferiores+red+transporte) más los datos (nivel de aplicación). En la imagen tienes los tamaños en bytes más habituales para cada cabecera:



En las siguientes imágenes tienes ejemplos de varias cabeceras y su tamaño:

Tamaño de la cabecera Ethernet:

> Frame 92: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits)			
> Ethernet II, Src: Giga-Byt_00:48:a1 (fc:aa:14:00:48:a1), Dst: TendaTec_90:69:18 (04:95:e6:90:69:18)			
> Internet Protocol Version 4, Src: 192.168.31.2, Dst: 172.217.168.173			
> Transmission Control Protocol, Src Port: 51532, Dst Port: 443, Seq: 674, Ack: 2666, Len: 823			
> Transport Layer Security			

0000	04 95 e6 90 69 18 fc aa 14 00 48 a1 08 00 45 00i... ..H...E.
0010	03 5f d0 b7 40 00 80 06 00 00 c0 a8 1f 02 ac d9	...@... ..
0020	a8 ad c9 4c 01 bb 5a 28 ab 64 7c 68 59 ea 50 18	...L..Z(..d hY.P.
0030	02 01 38 83 00 00 17 03 03 03 32 5e cd 1e 00 18	..8..... ..2^....
0040	3c 4f cc 81 b6 8c cc b9 e8 f6 4d de 9c 56 41 0d	<O..... ..M..VA.
0050	70 3e f3 38 2d a6 3a cc c6 02 37 87 c2 08 d0 bd	p>8-:.. ..7.....

Ethernet (eth), 14 byte(s)

Tamaño de la cabecera IP (nivel de red):

> Frame 92: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits)			
> Ethernet II, Src: Giga-Byt_00:48:a1 (fc:aa:14:00:48:a1), Dst: TendaTec_90:69:18 (04:95:e6:90:69:18)			
> Internet Protocol Version 4, Src: 192.168.31.2, Dst: 172.217.168.173			
> Transmission Control Protocol, Src Port: 51532, Dst Port: 443, Seq: 674, Ack: 2666, Len: 823			
> Transport Layer Security			

0000	04 95 e6 90 69 18 fc aa 14 00 48 a1 08 00 45 00i... ..H...E.
0010	03 5f d0 b7 40 00 80 06 00 00 c0 a8 1f 02 ac d9	...@... ..
0020	a8 ad c9 4c 01 bb 5a 28 ab 64 7c 68 59 ea 50 18	...L..Z(..d hY.P.
0030	02 01 38 83 00 00 17 03 03 03 32 5e cd 1e 00 18	..8..... ..2^....
0040	3c 4f cc 81 b6 8c cc b9 e8 f6 4d de 9c 56 41 0d	<O..... ..M..VA.
0050	70 3e f3 38 2d a6 3a cc c6 02 37 87 c2 08 d0 bd	p>8-:.. ..7.....

Internet Protocol Version 4 (ip), 20 byte(s)

Tamaño de la cabecera TCP (nivel de transporte):

> Frame 92: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits)			
> Ethernet II, Src: Giga-Byt_00:48:a1 (fc:aa:14:00:48:a1), Dst: TendaTec_90:69:18 (04:95:e6:90:69:18)			
> Internet Protocol Version 4, Src: 192.168.31.2, Dst: 172.217.168.173			
> Transmission Control Protocol, Src Port: 51532, Dst Port: 443, Seq: 674, Ack: 2666, Len: 823			
> Transport Layer Security			

0020	a8 ad c9 4c 01 bb 5a 28 ab 64 7c 68 59 ea 50 18	...L..Z(..d hY.P.
0030	02 01 38 83 00 00 17 03 03 03 32 5e cd 1e 00 18	..8..... ..2^....
0040	3c 4f cc 81 b6 8c cc b9 e8 f6 4d de 9c 56 41 0d	<O..... ..M..VA.
0050	70 3e f3 38 2d a6 3a cc c6 02 37 87 c2 08 d0 bd	p>8-:.. ..7.....
0060	b3 e8 5a 4d cc b1 f9 4a a2 ab 5d 41 0d 02 64 3a	..ZM...J ..]A..d:
0070	55 ca f5 47 ca 4e 5d 04 bf 36 85 0c 84 63 c7 a0	U..G.N]. ..6...c..

Transmission Control Protocol (tcp), 20 byte(s)

> Frame 92: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits)			
> Ethernet II, Src: Giga-Byt_00:48:a1 (fc:aa:14:00:48:a1), Dst: TendaTec_90:69:18 (04:95:e6:90:69:18)			
> Internet Protocol Version 4, Src: 192.168.31.2, Dst: 172.217.168.173			
> Transmission Control Protocol, Src Port: 51532, Dst Port: 443, Seq: 674, Ack: 2666, Len: 823			
> Transport Layer Security			

Tamaño de los datos del nivel de aplicación:

0030	02 01 38 83 00 00 17 03 03 03 32 5e cd 1e 00 18	..8..... ..2^....
0040	3c 4f cc 81 b6 8c cc b9 e8 f6 4d de 9c 56 41 0d	<O..... ..M..VA.
0050	70 3e f3 38 2d a6 3a cc c6 02 37 87 c2 08 d0 bd	p>8-:.. ..7.....
0060	b3 e8 5a 4d cc b1 f9 4a a2 ab 5d 41 0d 02 64 3a	..ZM...J ..]A..d:
0070	55 ca f5 47 ca 4e 5d 04 bf 36 85 0c 84 63 c7 a0	U..G.N]. ..6...c..
0080	b8 5d 5d 02 97 8c 74 cc 0e 65 0b fa 73 8e 73 80	..]]...t. .e..s.s.

Transport Layer Security (tls), 823 byte(s)

Rellena ahora la siguiente tabla con los tres paquetes que usaste en ejercicios anteriores (aparece ya rellenado un ejemplo, correspondiente a las imágenes recién mostradas):

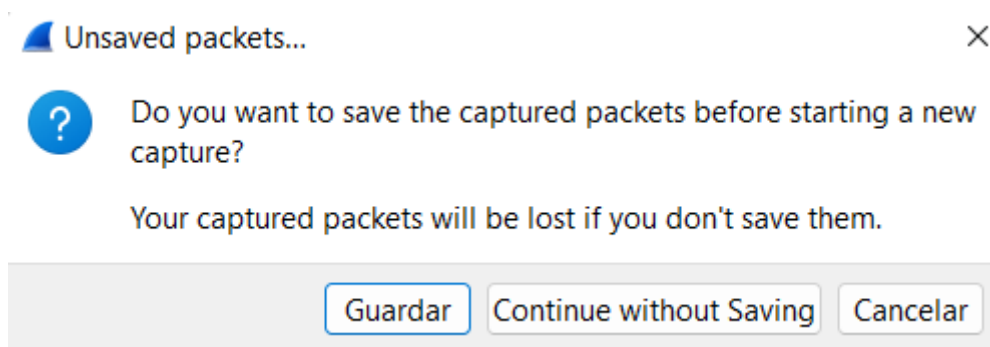
	N.º paquete	Tamaño total	Proto capa inferior	Tamaño cab. Ethernet	Proto nivel red	Tamaño cab. red	Proto nivel trans.	Tamaño cab. trans.	Proto apl.	Tamaño datos
Paquete ejemplo	92	877	Ethernet	14	IPv4	20	TCP	20	TLS	823
Paquete 1	15	87	Ethernet	14	IPv4	20	UDP	8	MDNS	45
Paquete 2	11	76	Ethernet	14	IPv4	20	UDP	8	DNS	34
Paquete 3	71	930	Ethernet	14	IPv4	20	TCP	32	TLS	864

En las unidades siguientes veremos qué hay dentro de cada cabecera. En esta unidad basta con que entiendas la estructura general de un paquete en cabeceras y datos, sin entrar en su interior, así como los tamaños y la localización de las direcciones (MAC, IP, puertos) en cada nivel.

i) **Opciones avanzadas de captura.** Si queremos volver a capturar paquetes bastará con hacer clic en el primer botón de la barra de herramientas (o menú Captura, Iniciar):



Si teníamos una captura abierta y no la habíamos guardado en fichero, se nos pedirá si queremos guardarla en fichero, si queremos continuar y no nos importa perderla, o si queremos cancelar el guardado. Ahora escogeremos la segunda opción:

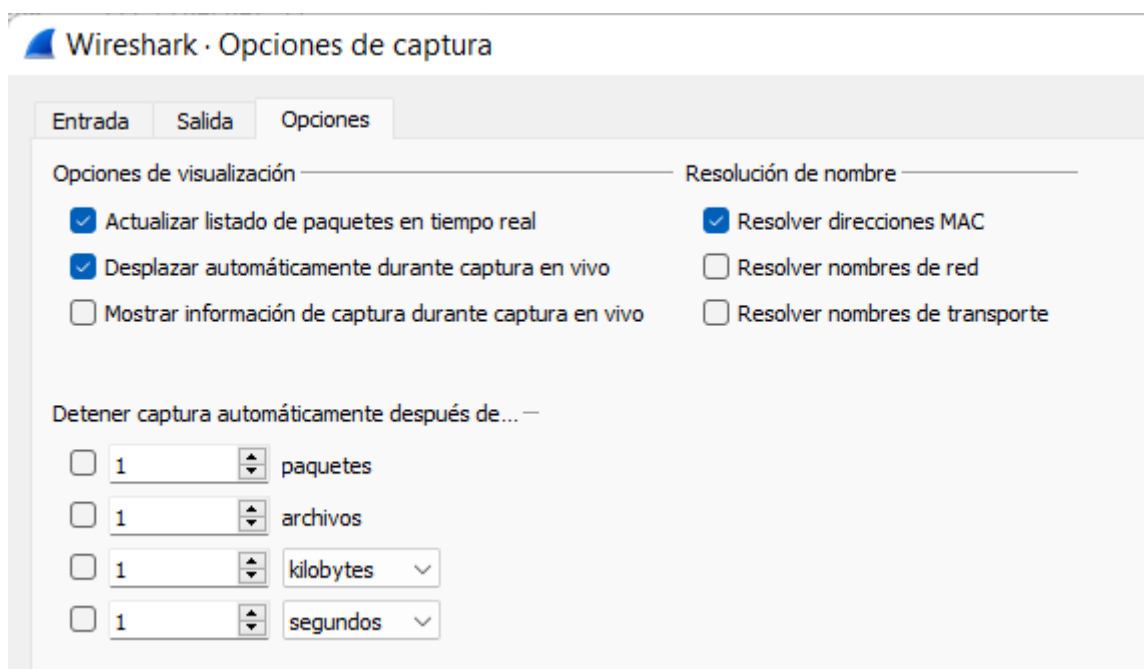


Ahora Wireshark comenzará a capturar. Recuerda que puedes parar la captura de paquetes en cualquier momento dándole al botón del cuadrado rojo. Hazlo.

Normalmente durante este curso capturaremos y dejaremos de capturar cuando nosotros decidamos. Pero a veces nos puede interesar que la captura de paquetes pare automáticamente cuando se cumpla determinada condición. Para ello tendremos que ir a las opciones de captura (cuarto botón o menú Captura, Opciones):



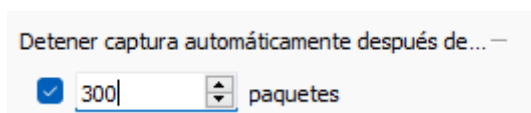
Aparecerá una pantalla e iremos a la pestaña Opciones:

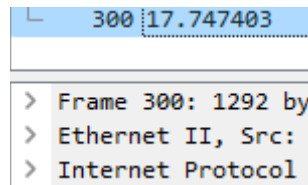


En la sección “Detener captura automáticamente después de” podemos elegir la condición con la que la captura de paquetes se detendrá automáticamente. Como ves, podemos elegir, entre otras cosas, que Wireshark pare de capturar cuando alcance un número determinado de paquetes, o cuando el total de paquetes capturados llegue a una cantidad de KB/MB/GB concreta, o simplemente cuando transcurra un número específico de segundos/minutos/horas. Tras seleccionar la opción deseada, dándole al botón Iniciar empezaría la captura de paquetes, deteniéndose automáticamente cuando se cumpla la condición.

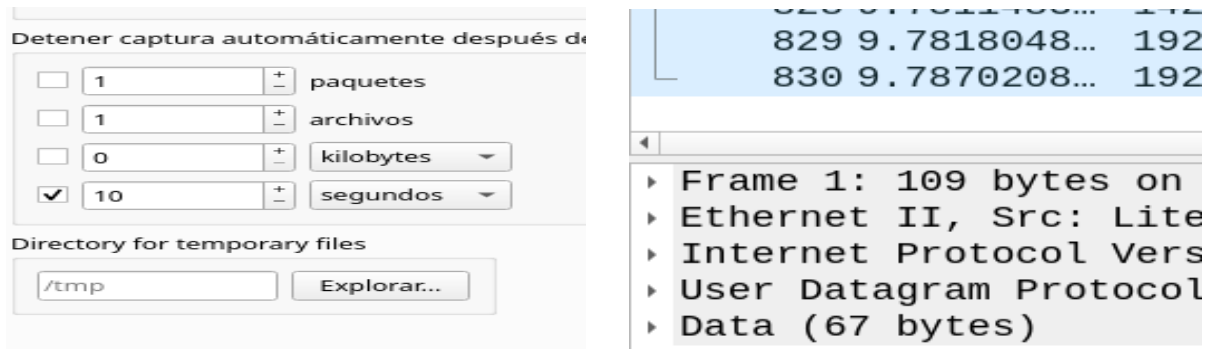
Para cada uno de los siguientes casos, pega aquí dos pantallazos: uno con la opción que necesitas marcar y otro con el listado de paquetes obtenido. Se te proporciona hecho el primer ejemplo:

- Parar de capturar cuando se llegue a 300 paquetes:

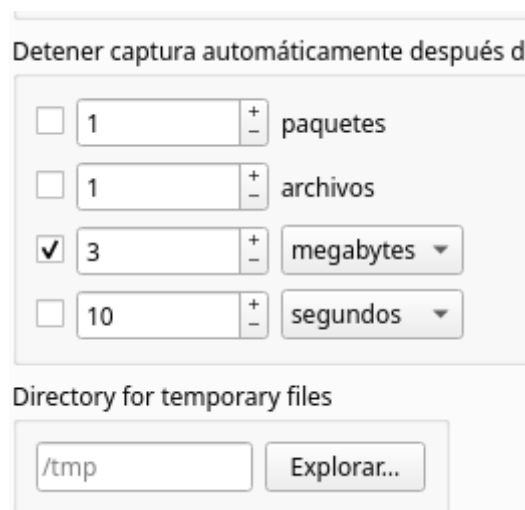








- Capturar únicamente durante 10 segundos (pega aquí el pantallazo con la opción seleccionada y el valor de la columna Time del último paquete):
















- Parar de capturar cuando el total de paquetes capturados llegue a 3 Megabytes.



j) **Barra de herramientas.** Deja el ratón quieto unos instantes sobre cada uno de los botones que se te indican en la siguiente tabla y copia aquí para qué sirve cada uno de ellos:

Botón	Sirve para...
	Inicia captura de paquetes
	Detiene captura de paquetes
	Opciones de captura
	Abre un archivo de captura

	Guarda este archivo de captura
	Cierra este archivo de captura
	Va al paquete anterior
	Va al paquete siguiente
	Va al paquete especificado
	Va al primer paquete
	Va al último paquete
	Desplaza automáticamente al último paquete durante la captura
	Dibuja paquetes usando sus reglas de coloreado
	Amplia el texto de la ventana principal
	Reduce el texto de la ventana principal
	Devuelve el texto de la ventana principal a su tamaño original
	Cambia el tamaño de las columnas de listado de paquetes para ajustar los contenidos

El significado de algunos botones es evidente, pero el de otros requiere cierta explicación:



- Con este botón se despliega una barra para teclear el n.º de paquete al que queremos ir, para ahorrarnos tiempo en el desplazamiento.



- Este botón se puede activar o desactivar según si está pulsado o no. Solo tiene utilidad si estamos capturando en directo. Si lo activamos, siempre mostrará en el listado de paquetes el último paquete capturado, que irá cambiando durante la captura. Si está desactivado, la lista de paquetes no se desplazará automáticamente al último.



- Al igual que el anterior, puede hacerse clic en él para activarlo/desactivarlo. Si lo activamos, el listado de paquetes aparecerá coloreado, es decir, según el protocolo principal se mostrará resaltado con un color u otro. Si lo desactivamos, todos aparecerán sin color. El coloreado de paquetes permite destacar visualmente de manera muy cómoda aquellos paquetes de nuestro interés que cumplan determinadas condiciones según su protocolo, y se puede configurar para, por ejemplo, marcar en amarillo todos los paquetes que usen TCP en el nivel de transporte y en rojo los que usen UDP.



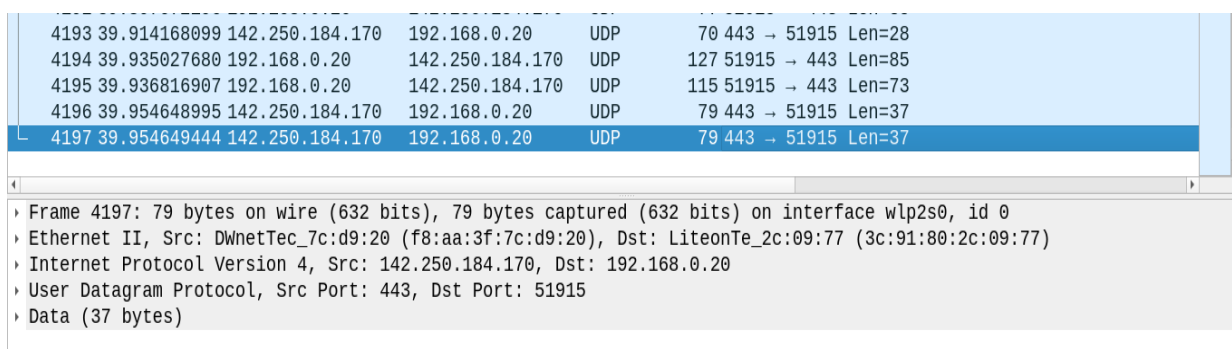
- Si hemos ampliado/reducido mucho el tamaño de la letra en el listado de paquetes, dándole a este botón volveremos al tamaño por defecto.



- En el listado de paquetes puedes estirar de los bordes de cada columna (N.º, Time, Source, ...) para poder mostrar más o menos texto. Si hemos modificado la longitud de varias columnas, dándole a este botón las columnas volverán al tamaño que tenían por defecto.

k) **Actividad resumen.** Realiza los siguientes ejercicios para comprobar si has entendido bien toda esta introducción a Wireshark:

- Captura paquetes en tu conexión de red durante 40 segundos exactos. Recuerda abrir varias páginas web con el navegador durante la captura para forzar a que aparezcan muchos más paquetes. Pega aquí un pantallazo que demuestre que la captura ha parado automáticamente al llegar a los 40 segundos.



- Graba el fichero poniéndole de nombre tu nombre y apellidos. ¿Cuántos paquetes en total contiene la captura?
- La captura contiene 4197 paquetes.
- Busca el paquete nº20 y rellena las siguientes tablas:

	Tamaño total	Proto capa inferior	Tamaño cab. Ethernet	Proto nivel red	Tamaño cab. red	Proto nivel trans.	Tamaño cab. trans.	Proto apl.	Tamaño datos
Paquete 20	86	Ethernet	14 bytes	IPv4	20 bytes	UDP	8 bytes		

	MAC origen	MAC destino	IP origen	IP destino	Puerto origen	Puerto destino
Paquete 20	3c:91:80:2c:09:20	f8:aa:3f:7c:d9:20	192.168.0.20	142.250:184:170	51915	443

- Para poder comprobar que el ejercicio es correcto, pega aquí tres pantallazos: uno con el listado de paquetes (donde aparezca seleccionado el paquete 20), otro con la sección central con los detalles del paquete 20 y otro con la sección inferior donde se vea el contenido en hexadecimal del paquete (incluyendo la barra de estado).

No.	Time	Source	Destination	Protocol	Length	Info
16	0.091466538	142.250.184.170	192.168.0.20	UDP	79	443 → 51915 Len=37
17	0.095987869	192.168.0.20	142.250.184.170	UDP	77	51915 → 443 Len=35
18	0.119994355	142.250.184.170	192.168.0.20	UDP	265	443 → 51915 Len=223
19	0.119994858	142.250.184.170	192.168.0.20	UDP	316	443 → 51915 Len=274
20	0.120406509	192.168.0.20	142.250.184.170	UDP	86	51915 → 443 Len=44
21	0.125403014	192.168.0.20	142.250.184.170	UDP	77	51915 → 443 Len=35
22	0.125660663	192.168.0.20	142.250.184.170	UDP	115	51915 → 443 Len=73
23	0.146424084	142.250.184.170	192.168.0.20	UDP	69	443 → 51915 Len=27
24	0.146424778	142.250.184.170	192.168.0.20	UDP	71	443 → 51915 Len=29
25	0.151481317	192.168.0.20	142.250.184.170	UDP	77	51915 → 443 Len=35
26	0.178724998	142.250.184.170	192.168.0.20	UDP	267	443 → 51915 Len=225

▶ Frame 20: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlp2s0, id 0
 ▶ Ethernet II, Src: LiteonTe_2c:09:77 (3c:91:80:2c:09:77), Dst: DWnetTec_7c:d9:20 (f8:aa:3f:7c:d9:20)
 ▶ Internet Protocol Version 4, Src: 192.168.0.20, Dst: 142.250.184.170
 ▶ User Datagram Protocol, Src Port: 51915, Dst Port: 443
 ▶ Data (44 bytes)

0000	f8 aa 3f 7c d9 20 3c 91 80 2c 09 77 08 00 45 00	..? <.,W..E.
0010	00 48 d8 f9 40 00 40 11 59 4a c0 a8 00 14 8e fa	.H..@.@. YJ.....
0020	b8 aa ca cb 01 bb 00 34 08 a7 4b 45 dd 20 86 ae4..KE..
0030	70 80 b2 58 3d 91 b5 29 4c 76 96 c8 46 b7 e0 e4	p..X=..) LV..F...
0040	95 c1 47 ff cb 05 7e 50 b4 82 ca 0a ce 5e 82 c5	..G...~P.....^..
0050	bb bb a7 8f e6 7aZ

Destination Address (ip.dst), 4 byte(s)
 Paquetes: 4197 - Mostrado: 4197 (100.0%)
 Perfil: Default

EnriqueMartinez.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

20

No.	Time	Source	Destination	Protocol	Length	Info
16	0.091466538	142.250.184.170	192.168.0.20	UDP	79	443 → 51915 Len=37
17	0.095987869	192.168.0.20	142.250.184.170	UDP	77	51915 → 443 Len=35
18	0.119994355	142.250.184.170	192.168.0.20	UDP	265	443 → 51915 Len=223
19	0.119994858	142.250.184.170	192.168.0.20	UDP	316	443 → 51915 Len=274
20	0.120406509	192.168.0.20	142.250.184.170	UDP	86	51915 → 443 Len=44
21	0.125403014	192.168.0.20	142.250.184.170	UDP	77	51915 → 443 Len=35
22	0.125660663	192.168.0.20	142.250.184.170	UDP	115	51915 → 443 Len=73
23	0.146424084	142.250.184.170	192.168.0.20	UDP	69	443 → 51915 Len=27
24	0.146424778	142.250.184.170	192.168.0.20	UDP	71	443 → 51915 Len=29
25	0.151481317	192.168.0.20	142.250.184.170	UDP	77	51915 → 443 Len=35
26	0.178724998	142.250.184.170	192.168.0.20	UDP	267	443 → 51915 Len=225

▶ Frame 20: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlp2s0, id 0
 ▶ Ethernet II, Src: LiteonTe_2c:09:77 (3c:91:80:2c:09:77), Dst: DWnetTec_7c:d9:20 (f8:aa:3f:7c:d9:20)
 ▶ Internet Protocol Version 4, Src: 192.168.0.20, Dst: 142.250.184.170
 ▶ User Datagram Protocol, Src Port: 51915, Dst Port: 443
 ▶ Data (44 bytes)

0000	f8 aa 3f 7c d9 20 3c 91 80 2c 09 77 08 00 45 00	..? <.,W..E.
0010	00 48 d8 f9 40 00 40 11 59 4a c0 a8 00 14 8e fa	.H..@.@. YJ.....
0020	b8 aa ca cb 01 bb 00 34 08 a7 4b 45 dd 20 86 ae4..KE..
0030	70 80 b2 58 3d 91 b5 29 4c 76 96 c8 46 b7 e0 e4	p..X=..) LV..F...
0040	95 c1 47 ff cb 05 7e 50 b4 82 ca 0a ce 5e 82 c5	..G...~P.....^..
0050	bb bb a7 8f e6 7aZ

Destination Address (ip.dst), 4 byte(s)
 Paquetes: 4197 - Mostrado: 4197 (100.0%)
 Perfil: Default