

Jose Antonio Lorenzo Abril
2º PCEO
Redes de Comunicaciones

2ª Tarea: Arquitectura de Red

1. Especifica los comandos / programas utilizados durante la captura para asegurarte de que se generaban tramas con los dos tipos de tráfico (DNS y HTTP) solicitados.

Una vez abierto wireshark e iniciada la captura, ejecuto en terminal los comandos

```
~$ nslookup www.facebook.com
```

```
Server:      127.0.0.53
```

```
Address:     127.0.0.53#53
```

Non-authoritative answer:

www.facebook.com canonical name = star-mini.c10r.facebook.com.

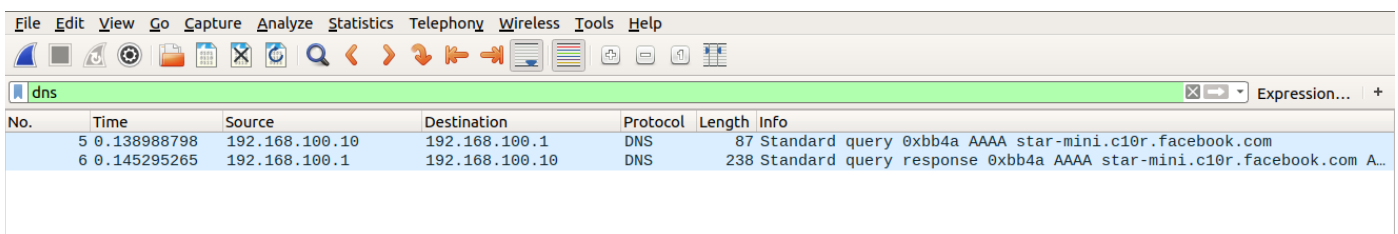
Name: star-mini.c10r.facebook.com

Address: 31.13.83.36

Name: star-mini.c10r.facebook.com

Address: 2a03:2880:f104:83:face:b00c:0:25de

Así me aseguro de que se produzca tráfico DNS. Y usando el filtro dns lo veo.

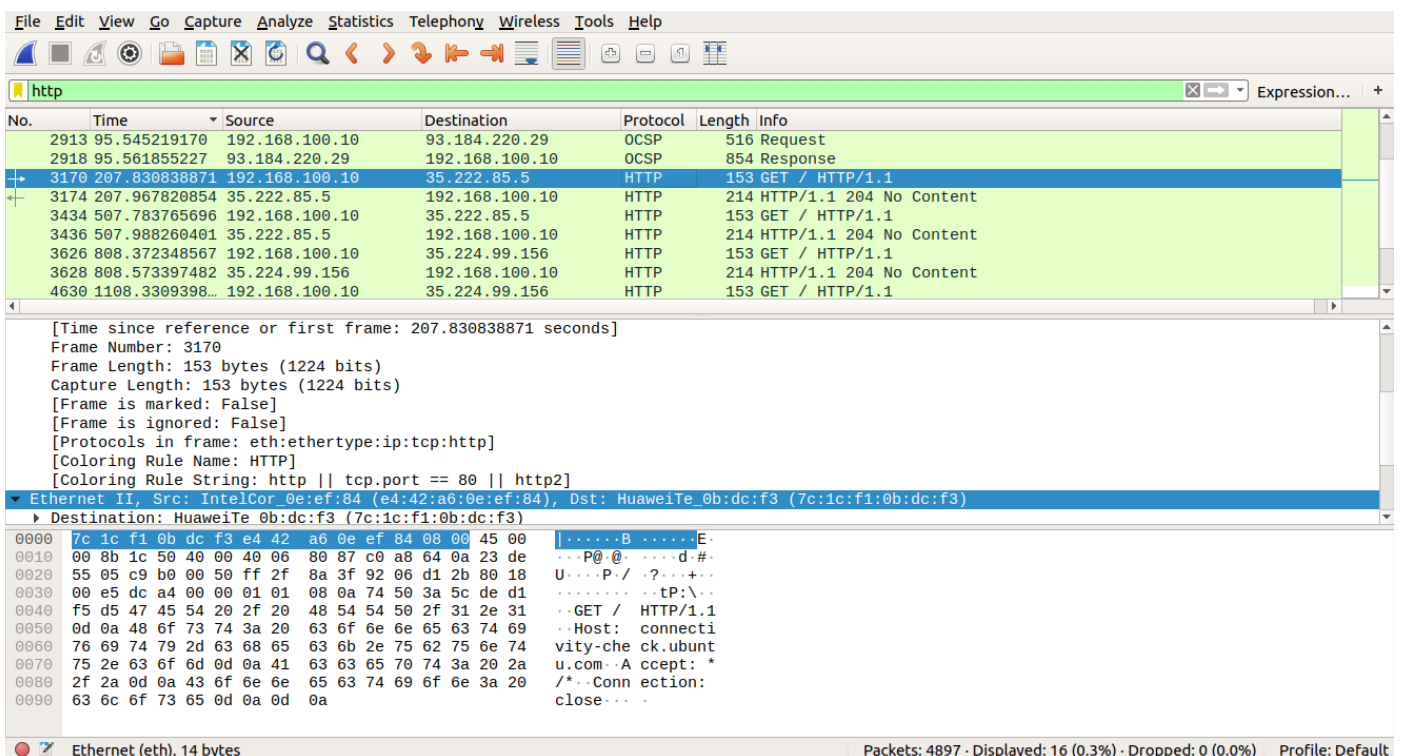


The screenshot shows the Wireshark interface with the 'dns' filter applied. The packet list shows two DNS packets. The first is a query from 192.168.100.10 to 192.168.100.1. The second is a response from 192.168.100.1 to 192.168.100.10.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.138988798	192.168.100.10	192.168.100.1	DNS	87	Standard query 0xbb4a AAAA star-mini.c10r.facebook.com
6	0.145295265	192.168.100.1	192.168.100.10	DNS	238	Standard query response 0xbb4a AAAA star-mini.c10r.facebook.com A...

Para asegurarme de obtener tráfico http simplemente he usado el comando

```
~$ firefox www.twitter.com
```



The screenshot shows the Wireshark interface with the 'http' filter applied. The packet list shows several HTTP packets. The selected packet is a GET request from 192.168.100.10 to 35.222.85.5. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

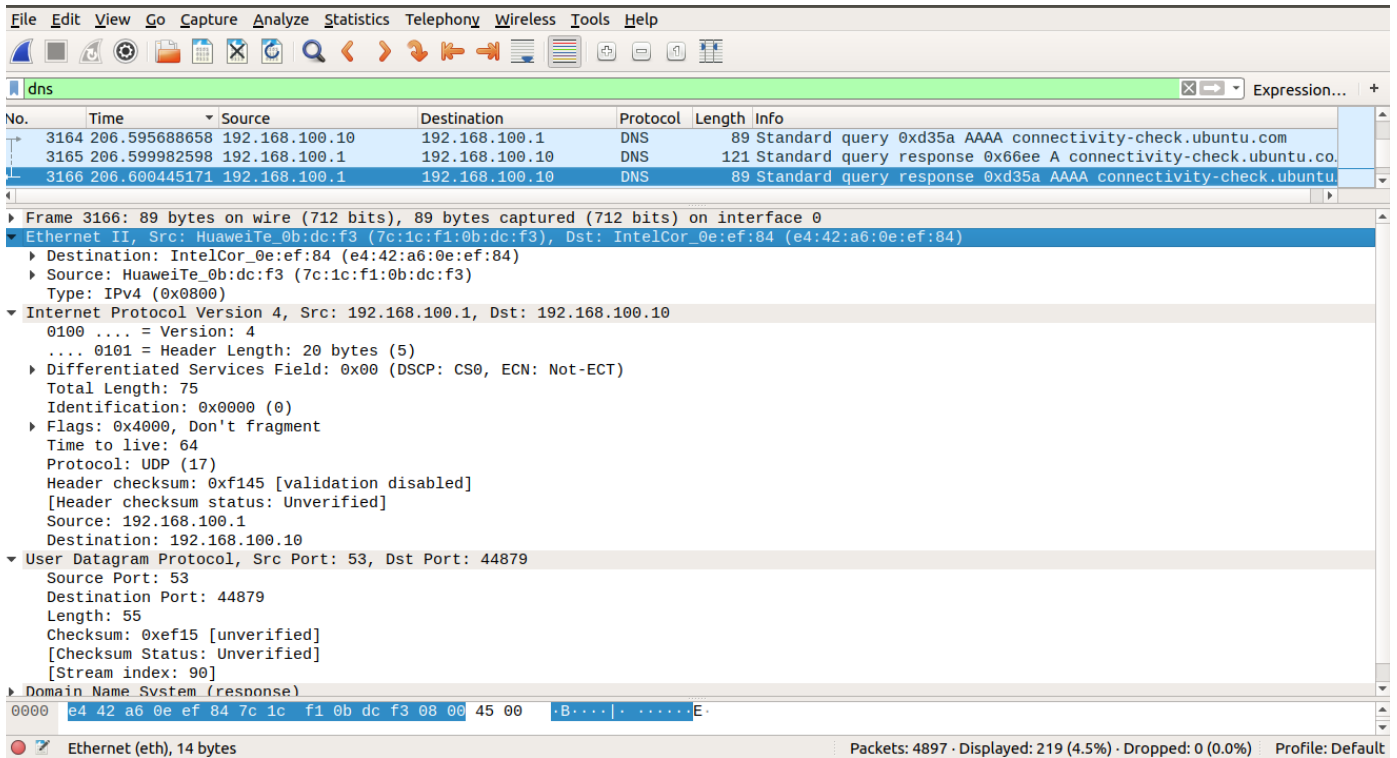
No.	Time	Source	Destination	Protocol	Length	Info
2913	95.545219170	192.168.100.10	93.184.220.29	OCSP	516	Request
2918	95.561855227	93.184.220.29	192.168.100.10	OCSP	854	Response
3170	207.830838871	192.168.100.10	35.222.85.5	HTTP	153	GET / HTTP/1.1
3174	207.967820854	35.222.85.5	192.168.100.10	HTTP	214	HTTP/1.1 204 No Content
3434	507.783765696	192.168.100.10	35.222.85.5	HTTP	153	GET / HTTP/1.1
3436	507.988260401	35.222.85.5	192.168.100.10	HTTP	214	HTTP/1.1 204 No Content
3626	808.372348567	192.168.100.10	35.224.99.156	HTTP	153	GET / HTTP/1.1
3628	808.573397482	35.224.99.156	192.168.100.10	HTTP	214	HTTP/1.1 204 No Content
4630	1108.3309398...	192.168.100.10	35.224.99.156	HTTP	153	GET / HTTP/1.1

[Time since reference or first frame: 207.830838871 seconds]
Frame Number: 3170
Frame Length: 153 bytes (1224 bits)
Capture Length: 153 bytes (1224 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
▼ Ethernet II, Src: IntelCor_0e:ef:84 (e4:42:a6:0e:ef:84), Dst: HuaweiTe_0b:dc:f3 (7c:1c:f1:0b:dc:f3)
► Destination: HuaweiTe_0b:dc:f3 (7c:1c:f1:0b:dc:f3)

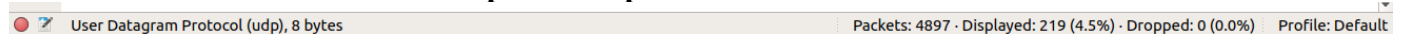
0000 7c 1c f1 0b dc f3 e4 42 a6 0e ef 84 08 00 45 00 |.....B.....E-
0010 00 8b 1c 50 40 00 40 06 80 87 c0 a8 64 0a 23 de |...P@...d.#.
0020 55 05 c9 b0 00 50 ff 2f 8a 3f 92 06 d1 2b 80 18 |U...P/?...+..
0030 00 e5 dc a4 00 00 01 01 08 0a 74 50 3a 5c de d1 |.....tP:\..
0040 f5 d5 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 |..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 63 6f 6e 6e 65 63 74 69 |..Host: connecti
0060 76 69 74 79 2d 63 68 65 63 6b 2e 75 62 75 6e 74 |vity-che ck.ubunt
0070 75 2e 63 6f 6d 0d 0a 41 63 63 65 70 74 3a 20 2a |u.com..A ccept: *
0080 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 |/*..Conn ection:
0090 63 6c 6f 73 65 0d 0a 0d 0a |close... ..

Ethernet (eth), 14 bytes Packets: 4897 · Displayed: 16 (0.3%) · Dropped: 0 (0.0%) Profile: Default

2. Escoge una cualquiera de las ramas DNS capturadas y, adjuntando un pantallazo de la misma en el que aparezca claramente toda la información necesaria, contesta a las siguientes preguntas:



a) ¿Qué protocolo de transporte encapsula al mensaje original DNS de la capa de aplicación? Especifica cuál es el tamaño exacto (en bytes) del mensaje a nivel de aplicación, así como el de la cabecera añadida por dicho protocolo.



Como puede verse en la imagen, el protocolo es UDP, y añade una cabecera de 8 B. Puesto que la longitud total es de 55 B, se deduce que la longitud del mensaje a nivel de aplicación es de 47 B.

b) ¿Dentro de qué protocolo de red viaja el anterior segmento? ¿Cuál es el tamaño en bytes añadido por la cabecera de este otro protocolo?

Como puede observarse, el protocolo de red es IPv4. Además, más arriba, se indica que añade una cabecera de 20 B.

c) ¿Cuál es el tamaño total de la trama Ethernet que encapsula al segmento anterior?

89 bytes. (55 + 20 + 14)

d) Calcula la eficiencia de uso en %.

Hemos visto que el mensaje es de 47 bytes, y la longitud total incluyendo cabeceras es 89 bytes, así, la eficiencia es $47 / 89 * 100 = 52,81\%$.

3. Repite el ejercicio anterior, pero en este caso para una trama cualquiera correspondiente al tráfico HTTP generado durante la captura.

The image shows a Wireshark packet capture. The top pane shows a list of packets. Packet 3170 is selected, showing an HTTP GET request. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2913	95.545219170	192.168.100.10	93.184.220.29	OCSP	516	Request
2918	95.561855227	93.184.220.29	192.168.100.10	OCSP	854	Response
3170	207.830838871	192.168.100.10	35.222.85.5	HTTP	153	GET / HTTP/1.1

Frame 3170: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0

Ethernet II, Src: IntelCor_0e:ef:84 (e4:42:a6:0e:ef:84), Dst: HuaweiTe_0b:dc:f3 (7c:1c:f1:0b:dc:f3)

Internet Protocol Version 4, Src: 192.168.100.10, Dst: 35.222.85.5

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 139
Identification: 0x1c50 (7248)
Flags: 0x4000, Don't fragment
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x8087 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.100.10
Destination: 35.222.85.5

Transmission Control Protocol, Src Port: 51632, Dst Port: 80, Seq: 1, Ack: 1, Len: 87

Source Port: 51632
Destination Port: 80
[Stream index: 105]
[TCP Segment Len: 87]
Sequence number: 1 (relative sequence number)
[Next sequence number: 88 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window size value: 229

0000 7c 1c f1 0b dc f3 e4 42 a6 0e ef 84 08 00 45 00 |B.....E..

Ethernet (eth), 14 bytes

Packets: 4897 · Displayed: 16 (0.3%) · Dropped: 0 (0.0%) · Profile: Default

a) ¿Qué protocolo de transporte encapsula al mensaje original HTTP de la capa de aplicación? Especifica cuál es el tamaño exacto (en bytes) del mensaje a nivel de aplicación, así como el de la cabecera añadida por dicho protocolo.

Como vemos, el protocolo es TCP, y la longitud de la cabecera es 32 B. Puesto que vemos que la longitud del mensaje es 87 B.

b) ¿Dentro de qué protocolo de red viaja el anterior segmento? ¿Cuál es el tamaño en bytes añadido por la cabecera de este otro protocolo?

The image shows a Wireshark packet capture. The top pane shows a list of packets. Packet 3170 is selected, showing an HTTP GET request. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2913	95.545219170	192.168.100.10	93.184.220.29	OCSP	516	Request
2918	95.561855227	93.184.220.29	192.168.100.10	OCSP	854	Response
3170	207.830838871	192.168.100.10	35.222.85.5	HTTP	153	GET / HTTP/1.1

Frame 3170: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0

Ethernet II, Src: IntelCor_0e:ef:84 (e4:42:a6:0e:ef:84), Dst: HuaweiTe_0b:dc:f3 (7c:1c:f1:0b:dc:f3)

Destination: HuaweiTe_0b:dc:f3 (7c:1c:f1:0b:dc:f3)
Source: IntelCor_0e:ef:84 (e4:42:a6:0e:ef:84)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.100.10, Dst: 35.222.85.5

Transmission Control Protocol, Src Port: 51632, Dst Port: 80, Seq: 1, Ack: 1, Len: 87

Hypertext Transfer Protocol

Vemos que el protocolo de red es, de nuevo, IPv4. Y en la captura anterior puede verse que la cabecera es de 20 B (lo que concuerda con lo visto para DNS).

c) ¿Cuál es el tamaño total de la trama Ethernet que encapsula al segmento anterior? 153 B, como se observa en la imagen. (87 + 32 + 20 + 14)

d) Calcula la eficiencia de uso en %.
 $87 / 153 * 100 = 56,86\%$

4. En función de los resultados que obtengas en las preguntas anteriores, ¿podrías afirmar cuál de los dos casos es más eficiente desde el punto de vista del porcentaje de datos útiles enviados?

No, las diferencias no son sustancialmente significativas.

5. Dada una arquitectura de red, reflexiona brevemente sobre las implicaciones derivadas de tener un número determinado de capas. Por ejemplo, ¿crees que a mayor número de capas siempre habrá un mayor número de bytes de cabecera?

A mayor número de capas, puesto que cada capa necesita saber qué le llega y qué tiene que hacer con ello, aumenta necesariamente el número de bytes de cabecera. Podemos pensar que si simplificásemos las capas, por ejemplo diviendo una capa en dos, y haciendo que la cabecera también se divida en dos, esto no tiene por qué suceder. Sin embargo, al hacer esto, lo que hacemos es aumentar el tiempo que dedicamos a analizar el mensaje, pues ahora pasará por dos capas en lugar de una.

6. Finalmente, ¿crees que un router necesita acceder a los datos del nivel de aplicación para hacer su trabajo? ¿Podrías citar algún tipo de analogía similar relacionada con el transporte de información para reafirmar tu respuesta?

No, el router solo necesita saber quién envía y hacia quién va el mensaje, o al revés, de quién es el mensaje recibido, y a quién va dirigido.

El famoso ejemplo visto en clase es el del sistema de correos. Para entregar una carta de la que esperas respuesta, solo necesitas indicar quién eres y dónde vives y hacia quién va dirigida la carta y dónde vive, y llevar la carta a un buzón.

El cartero cogerá la carta independientemente de quién la haya dejado ahí y la llevará a la oficina de correos, donde se despreocupará de ella.

En la oficina de correos se verá cuán lejos debe ser enviada la carta y será enviada a otra oficina si es necesario.

Se dará a un cartero la carta para que la deje en el buzón correspondiente, donde el destinatario la recogerá.