

INFORME PRACTICA 2

Nombre y apellidos: Iker Fernández Molano

ESTA PRÁCTICA SE DEBE REALIZAR EN LOS ORDENADORES DEL LABORATORIO

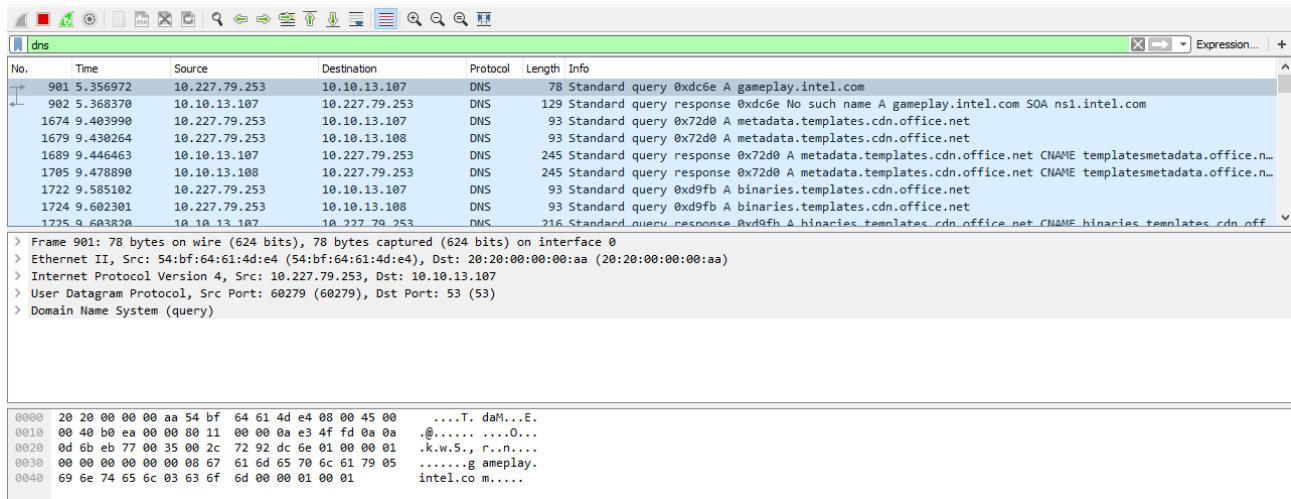
PARTE 1: PRIMEROS PASOS CON WIRESHARK

Cuestión 1: Experimenta con algunos filtros:

```
dns
ip.src == XXX.XXX.XXX.XXX ( pon tu IP)
ip.dst == XXX.XXX.XXX.XXX ( pon la IP del servidor de la página web de la EHU/UPV) *
http.host == www.google.com *
```

* Seguramente, al aplicar estos filtros no se muestre ningún paquete. ¿Por qué? No olvides que para poder ver los paquetes de una conexión tiene que existir dicha conexión, es decir, se debe abrir la página web, por ejemplo.

Utiliza el comando de red **ipconfig** para conocer la IP de tu PC y la puerta de enlace predeterminada. ¿Cómo puedes conocer la IP del servidor EHU/UPV? ¿Qué nos permiten ver nuestro analizador con los filtros anteriores? Escribiendo el comando nslookup en la terminal o el destinatario de los paquetes de servidor. Nos permiten ver los paquetes DNS que salen de nuestra ip y van a la ip del servidor.



No.	Time	Source	Destination	Protocol	Length	Info
901	5.356972	10.227.79.253	10.10.13.107	DNS	78	Standard query 0xdc6e A gameplay.intel.com
902	5.368370	10.10.13.107	10.227.79.253	DNS	129	Standard query response 0xdc6e No such name A gameplay.intel.com SOA ns1.intel.com
1674	9.403990	10.227.79.253	10.10.13.107	DNS	93	Standard query 0x72d0 A metadata.templates.cdn.office.net
1679	9.430264	10.227.79.253	10.10.13.108	DNS	93	Standard query 0x72d0 A metadata.templates.cdn.office.net
1689	9.446463	10.10.13.107	10.227.79.253	DNS	245	Standard query response 0x72d0 A metadata.templates.cdn.office.net CNAME templatesmetadata.office.n...
1705	9.478896	10.10.13.108	10.227.79.253	DNS	245	Standard query response 0x72d0 A metadata.templates.cdn.office.net CNAME templatesmetadata.office.n...
1722	9.585102	10.227.79.253	10.10.13.107	DNS	93	Standard query 0xd9fb A binaries.templates.cdn.office.net
1724	9.602301	10.227.79.253	10.10.13.108	DNS	93	Standard query 0xd9fb A binaries.templates.cdn.office.net
1735	9.603820	10.10.13.107	10.227.79.253	DNS	216	Standard query response 0xd9fb A binaries.templates.cdn.office.net CNAME binaries_templates_cdn.off...

> Frame 901: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: 54:bf:64:61:4d:e4 (54:bf:64:61:4d:e4), Dst: 20:20:00:00:00:aa (20:20:00:00:00:aa)
> Internet Protocol Version 4, Src: 10.227.79.253, Dst: 10.10.13.107
> User Datagram Protocol, Src Port: 60279 (60279), Dst Port: 53 (53)
> Domain Name System (query)

```

0000  20 20 00 00 00 aa 54 bf 64 61 4d e4 08 00 45 00  ....T. daM...E.
0010  00 40 b0 ea 00 00 80 11 00 00 0a e3 4f fd 0a 0a  ..@..... .0...
0020  0d 6b eb 77 00 35 00 2c 72 92 dc 6e 01 00 00 01  .k.w.s., r...n...
0030  00 00 00 00 00 00 00 67 61 6d 65 70 6c 61 79 05  .....g amplay.
0040  69 6e 74 65 6c 03 63 6f 6d 00 00 01 00 01  intel.co m.....

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src==10.227.79.253						
No.	Time	Source	Destination	Protocol	Length	Info
1272	7.446434	10.227.79.253	142.250.178...	TCP	55	[TCP segment of a reassembled PDU]
1298	7.555778	10.227.79.253	142.250.178...	TCP	55	[TCP segment of a reassembled PDU]
1674	9.483990	10.227.79.253	10.10.13.107	DNS	93	Standard query 0x72d0 A metadata.templates.cdn.office.net
1679	9.430264	10.227.79.253	10.10.13.108	DNS	93	Standard query 0x72d0 A metadata.templates.cdn.office.net
1680	9.447641	10.227.79.253	2.18.188.21	TCP	66	50342 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1692	9.456754	10.227.79.253	2.18.188.22	TCP	54	50342 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
1693	9.457659	10.227.79.253	2.18.188.22	TLSv1.2	252	Client Hello
1700	9.469872	10.227.79.253	2.18.188.22	TCP	54	50342 → 443 [ACK] Seq=199 Ack=3772 Win=262912 Len=0
1704	9.477120	10.227.79.253	2.18.188.22	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
1708	9.489797	10.227.79.253	2.18.188.22	TLSv1.2	490	Application Data
1721	9.555044	10.227.79.253	2.18.188.22	TCP	54	50342 → 443 [ACK] Seq=761 Ack=5189 Win=262912 Len=0
1722	9.585102	10.227.79.253	10.10.13.107	DNS	93	Standard query 0xd9fb A binaries.templates.cdn.office.net
1724	9.602301	10.227.79.253	10.10.13.108	DNS	93	Standard query 0xd9fb A binaries.templates.cdn.office.net
1726	9.604826	10.227.79.253	2.18.188.81	TCP	66	50343 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
> Frame 1724: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0						
> Ethernet II, Src: 54:bf:64:61:4d:e4 (54:bf:64:61:4d:e4), Dst: 20:20:00:00:00:aa (20:20:00:00:00:aa)						
> Internet Protocol Version 4, Src: 10.227.79.253, Dst: 10.10.13.108						
> User Datagram Protocol, Src Port: 50657 (50657), Dst Port: 53 (53)						
> Domain Name System (query)						
0000 20 20 00 00 00 aa 54 bf 64 61 4d e4 08 00 45 00T. daM....E.						
0010 00 4f 59 4d 00 00 80 11 00 00 0a e3 4f fd 00 0a .OYM.....O...						
0020 0d 6c c5 e1 00 35 0b 72 a2 d9 fb 01 00 00 01 .1...5.; r.....						
0030 00 00 00 00 00 00 08 62 69 6e 61 72 69 65 73 89b inaries.						
0040 74 65 6d 70 6c 61 74 65 73 03 63 64 6e 06 6f 66 template s.cdn.of						
0050 66 69 63 65 03 6e 65 74 00 00 01 01 01 fice.net						

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.dst==158.227.0.65						
No.	Time	Source	Destination	Protocol	Length	Info
165188	1783.366430	10.227.79.253	158.227.0.65	TCP	66	50589 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
165189	1783.367066	10.227.79.253	158.227.0.65	TCP	66	50590 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
165191	1783.367298	10.227.79.253	158.227.0.65	TCP	54	50589 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
165192	1783.367950	10.227.79.253	158.227.0.65	TLSv1.2	1807	Client Hello
165198	1783.369641	10.227.79.253	158.227.0.65	TCP	54	50589 → 443 [ACK] Seq=1754 Ack=2921 Win=2102272 Len=0
165206	1783.370048	10.227.79.253	158.227.0.65	TCP	54	50589 → 443 [ACK] Seq=1754 Ack=7068 Win=2102272 Len=0
165208	1783.371671	10.227.79.253	158.227.0.65	TLSv1.2	134	Change Cipher Spec, Application Data
165210	1783.371863	10.227.79.253	158.227.0.65	TLSv1.2	876	Application Data
> Frame 165188: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
> Ethernet II, Src: 54:bf:64:61:4d:e4 (54:bf:64:61:4d:e4), Dst: 20:20:00:00:00:aa (20:20:00:00:00:aa)						
> Internet Protocol Version 4, Src: 10.227.79.253, Dst: 158.227.0.65						
> Transmission Control Protocol, Src Port: 50589 (50589), Dst Port: 443 (443), Seq: 0, Len: 0						
0000 20 20 00 00 00 aa 54 bf 64 61 4d e4 08 00 45 00T. daM....E.						
0010 00 34 47 ab 40 00 00 00 00 0a e3 4f fd 9e e3 .4G.@... .O...						
0020 00 41 c5 9d 01 bb cc 0a e4 58 00 00 00 80 02 .A..... X.....						
0030 fa f0 fa 2a 00 00 02 04 05 b4 01 03 03 08 01 01 ...*....						
0040 04 02						

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http.host==www.google.com						
No.	Time	Source	Destination	Protocol	Length	Info

Cuestión 2: Define los filtros que:

- Presenten los paquetes cuya dirección IP de origen sea **host1** y su dirección IP de destino sea la **host2** (o viceversa, dos filtros diferentes)
 $ip.src== 10.227.79.253 \&& ip.dst== 10.227.79.252$

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
199055	2116.918094	10.227.79.253	10.227.79.252	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 199054)
199140	2117.922206	10.227.79.253	10.227.79.252	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in 199139)
199255	2118.937937	10.227.79.253	10.227.79.252	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (request in 199252)
199385	2119.953218	10.227.79.253	10.227.79.252	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request in 199384)

```
> Frame 199055: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: 54:bf:64:61:4d:e4 (54:bf:64:61:4d:e4), Dst: 54:bf:64:61:50:a9 (54:bf:64:61:50:a9)
> Internet Protocol Version 4, Src: 10.227.79.253, Dst: 10.227.79.252
> Internet Control Message Protocol

0000  54 bf 64 61 50 a9 54 bf 64 61 4d e4 08 00 45 00 T.daP.T. daM...E.
0010  00 3c 05 51 00 00 80 01 00 00 0a e3 4f fd 0a e3 .<.Q.... ....O...
0020  4f fc 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 0...UZ... .abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn oprstuv
0040  77 61 62 63 64 65 66 67 68 69 wabcdefg hi
```

$ip.src== 10.227.79.252 \&& ip.dst== 10.227.79.253$

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
199054	2116.917889	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 199055)
199139	2117.922139	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 199140)
199255	2118.937761	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 199253)
199384	2119.953034	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 199385)
203767	2175.684363	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 203766)
203854	2176.697996	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in 203853)
203949	2177.713426	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (request in 203948)
204005	2178.728966	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request in 204004)

```
> Frame 199054: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: 54:bf:64:61:50:a9 (54:bf:64:61:50:a9), Dst: 54:bf:64:61:4d:e4 (54:bf:64:61:4d:e4)
> Internet Protocol Version 4, Src: 10.227.79.252, Dst: 10.227.79.253
> Internet Control Message Protocol

0000  54 bf 64 61 4d e4 54 bf 64 61 50 a9 08 00 45 00 T.daM.T. daP...E.
0010  00 3c a1 b0 00 00 80 01 e3 51 0a e3 4f fc 0a e3 .<..... Q.O...
0020  4f fd 08 00 44 5a 00 01 00 01 61 62 63 64 65 66 0...MZ... .abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn oprstuv
0040  77 61 62 63 64 65 66 67 68 69 wabcdefg hi
```

Nos hemos hecho un ping entre los ordenadores, para que aparezcan los paquetes enviados entre los dos.

- Capturar todo el tráfico cuyo origen y destino es el host **host1** y el host **host2**, o host **host2** y el host **host1**, respectivamente (un único filtro)
 $(ip.src== 10.227.79.252 \&& ip.dst== 10.227.79.253) || (ip.src== 10.227.79.253 \&& ip.dst== 10.227.79.252)$

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

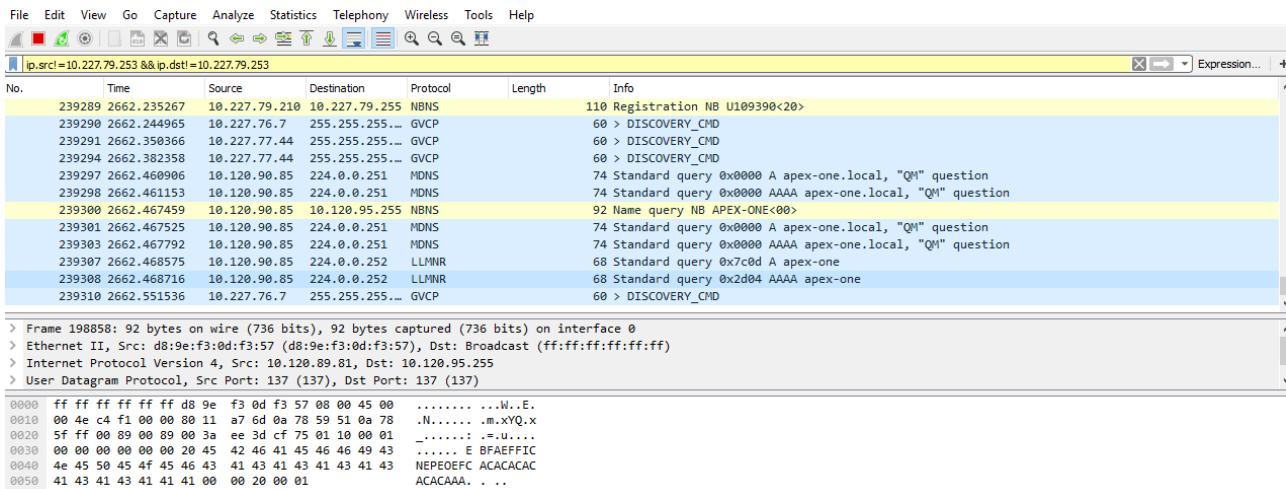
Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
199054	2116.917889	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 199055)
199055	2116.918094	10.227.79.253	10.227.79.252	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 199054)
199139	2117.922139	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 199140)
199140	2117.922206	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 199139)
199255	2118.937761	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 199253)
199384	2119.953034	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 199385)
203766	2175.683673	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (request in 203766)
203767	2175.684363	10.227.79.252	10.227.79.253	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 203766)

```
> Frame 199054: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: 54:bf:64:61:50:a9 (54:bf:64:61:50:a9), Dst: 54:bf:64:61:4d:e4 (54:bf:64:61:4d:e4)
> Internet Protocol Version 4, Src: 10.227.79.252, Dst: 10.227.79.253
> Internet Control Message Protocol

0000  54 bf 64 61 4d e4 54 bf 64 61 50 a9 08 00 45 00 T.daM.T. daP...E.
0010  00 3c a1 b0 00 00 80 01 e3 51 0a e3 4f fc 0a e3 .<..... Q.O...
0020  4f fd 08 00 44 5a 00 01 00 01 61 62 63 64 65 66 0...MZ... .abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn oprstuv
0040  77 61 62 63 64 65 66 67 68 69 wabcdefg hi
```

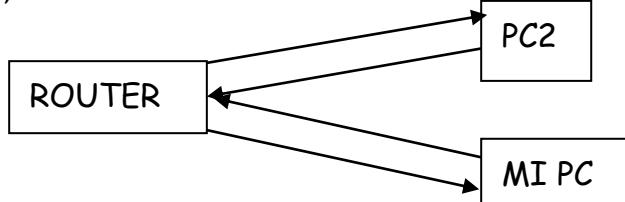
- Visualiza todo el tráfico menos el *host1*
 $ip.src!=10.227.79.253 \&& ip.dst!=10.227.79.253$



*como *host1* y *host2* elige tu dirección y la de otro ordenador del aula.

Cuestión 3: Analiza la información y realiza una representación esquemática. ¿Es lo mismo que podíamos ver en la simulación con Packet Tracer?

Sí, es lo mismo.



Cuestión 4: Permite que se vean todos los paquetes. ¿Aparecen algún paquete del protocolo ARP? Analiza la información de este paquete e intenta explicar cuál es la funcionalidad de este protocolo.

Si (ejemplo). Pregunta quién tiene la ip solicitada.

198900 2115.696417 20:20:00:00:... Broadcast ARP 60 Who has 158.227.72.122? Tell 158.227.72.1

PARTE 2: ANALIZANDO PROTOCOLOS CON WIRESHARK

Cuestión 5: Analiza la captura realizada y explica cómo funciona el comando tracert (recuerda utilizar filtros)

El recorrido que tiene que hacer un paquete hasta llegar al destino solicitado, mostrando las ips. En el ejemplo a www.google.com

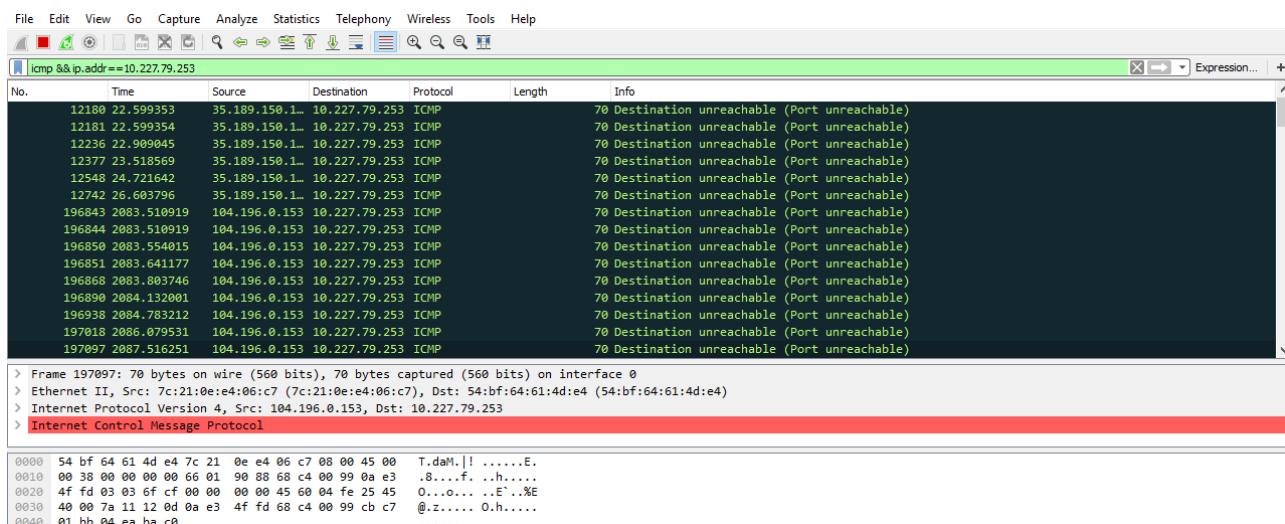
Traza a la dirección www.google.com [142.250.200.100]
 sobre un máximo de 30 saltos:

```

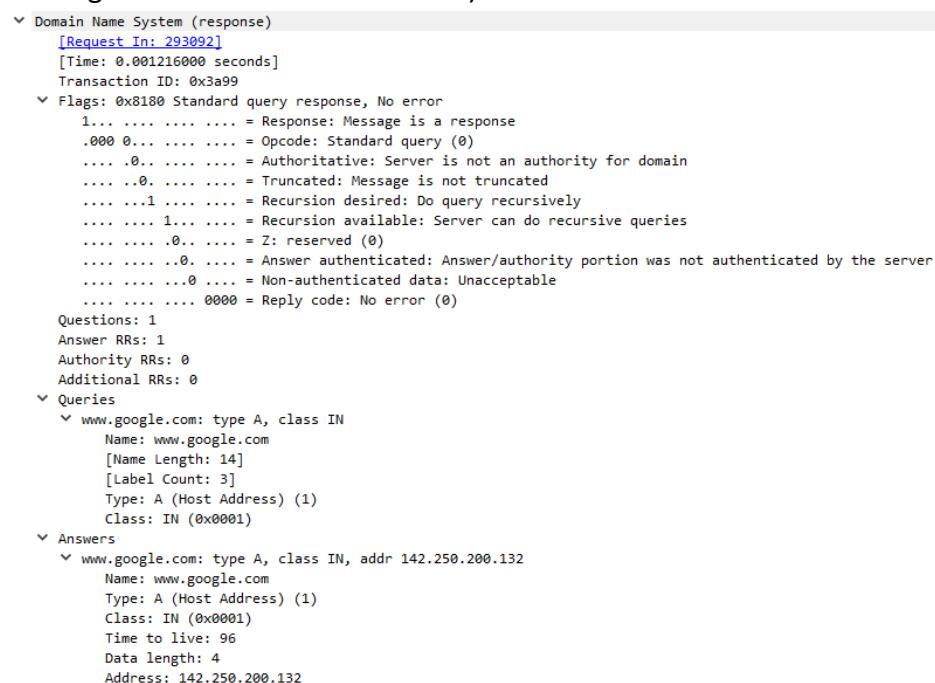
1 <1 ms <1 ms <1 ms 158.227.72.1
2 1 ms 1 ms <1 ms 10.0.1.1
3 1 ms 1 ms 1 ms pa-internal.lgp.ehu.es [10.0.1.4]
4 1 ms 1 ms 1 ms 10.10.5.41
5 1 ms 1 ms 1 ms 10.0.254.9
6 1 ms 1 ms 1 ms i2basque-pal.ethtrunk0-52.ehu.rt2.pav.red.rediris.es [130.206.210.1]
7 9 ms 9 ms 9 ms ehu-rt2.ethtrunk2.telmad.rt1.mad.red.rediris.es [130.206.245.17]
8 * * * Tiempo de espera agotado para esta solicitud.
9 12 ms 12 ms 12 ms 192.178.110.85
10 10 ms 10 ms 10 ms 209.85.247.245
11 10 ms 10 ms 10 ms mad41s13-in-f4.1e100.net [142.250.200.100]

```

Traza completa.



Cuestión 6: Analiza los paquetes del protocolo **DNS** que aparecen justo antes de los paquetes anteriores. ¿Qué función crees que tiene este protocolo? ¿Cuál es la dirección de tu servidor DNS? Describe un mensaje DNS (response), desglosando cada cabecera existente en él (y los campos más significativos de cada cabecera).



The screenshot shows a detailed analysis of a DNS response message. The tree view on the left includes sections for Domain Name System (response), Flags, Questions, Queries, and Answers. The Answers section shows a single A record for the domain www.google.com. The detailed view for this record shows the following fields: Name: www.google.com, Type: A (Host Address), Class: IN (0x0001), TTL: 96, Data length: 4, and Address: 142.250.200.132. The flags indicate a standard query response with no error.

Su función es traducir nombres de dominio (www.google.com) en direcciones IP (142.250.200.132). Mi dirección es 10.227.79.253.

- 1.... Como aparece un 1 es una respuesta
- .000 0... Consulta estándar
-0... No es autoritativo
-0. No truncado
-1 Solicita recursión
- 1... Puede hacer consultas recursivas
-0.. Reservado para el futuro, no se usa
-0. Datos no autenticados
-0 No autentificación en la respuesta
- 0000 No ha habido errores en la respuesta

Preguntas

Consulta el dominio: www.google.com de tipo A y clase Internet.

Respuestas RRs

Nombre: www.google.com de tipo A, dirección IP: 142.250.200.132 y tiene un tiempo de vida de 96 segundos.