

Grupo: Tarde

El tipo de la trama ICMP es 8 y con un code = 0, esto significa "Echo (ping) request".

```
unknown_0A:3A:26:1C:E2:DE
Dirección IP : 192.168.1.115
Dirección MAC : 0A:3A:26:1C:E2:DE
última conexión :
2022/04/02 10:32:34
```

Restricción de acceso a Internet

Personaliza tu dispositivo

```

Destination Address: 192.168.1.115
- Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x247a [correct]
  [Checksum Status: Good]

```

2.- Seleccione ahora uno de los mensajes ICMP echo reply del ping en b) ¿Cuáles son las direcciones Ethernet origen y destino y a quién corresponden? ¿Qué valor tiene el campo “Tipo de trama” y qué indica?

El mensaje ICMP echo reply nos aporta como información que la dirección de origen es “0a:3a:26:1c:e2:de” y la de destino es la “90:32:4b:5b:47:53”. Esto se puede confirmar con la imagen que encontramos abajo.

El campo de tipo de trama contiene 0 y el code también es 0. Esto nos indica que estamos ante un “Echo (ping) reply”.

119	34.906473673	192.168.1.77	192.168.1.115	ICMP	98 Echo (ping) request	id=0x0006, seq=1/256, ttl=64 (reply in 120)
120	34.912032392	192.168.1.115	192.168.1.77	ICMP	98 Echo (ping) reply	id=0x0006, seq=1/256, ttl=64 (request in 119)
121	35.903998390	192.168.1.77	192.168.1.115	ICMP	98 Echo (ping) request	id=0x0006, seq=2/512, ttl=64 (reply in 122)
122	35.911195689	192.168.1.115	192.168.1.77	ICMP	98 Echo (ping) reply	id=0x0006, seq=2/512, ttl=64 (request in 121)
132	36.905114581	192.168.1.77	192.168.1.115	ICMP	98 Echo (ping) request	id=0x0006, seq=3/768, ttl=64 (reply in 134)
134	36.920600858	192.168.1.115	192.168.1.77	ICMP	98 Echo (ping) reply	id=0x0006, seq=3/768, ttl=64 (request in 132)

▶ Frame 120: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
 ▼ Ethernet II, Src: 0a:3a:26:1c:e2:de (0a:3a:26:1c:e2:de), Dst: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)
 ▶ Destination: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)
 ▶ Source: 0a:3a:26:1c:e2:de (0a:3a:26:1c:e2:de)
 Type: IPv4 (0x0800)
 ▼ Internet Protocol Version 4, Src: 192.168.1.115, Dst: 192.168.1.77

```

Destination Address: 192.168.1.77
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x2c7a [correct]
  
```

3.- Respecto al último mensaje, ¿qué valor tiene el campo “CRC” de la trama Ethernet? ¿dónde se encuentra ubicado?

En mi caso, la validación en la cabecera la tengo deshabilitada como se observa en la imagen.

En cuanto al contenido, si que realizar el checksum y es correcto.

Tras estar buscando un poco de información, en caso de que el checksum sea incorrecto se nos mostraría como en la tercera imagen.

```

Header Checksum: 0x5f3c [validation disabled]
[Header checksum status: Unverified]
  
```

```

Destination Address: 192.168.1.77
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x2c7a [correct]
  [Checksum Status: Good]
  Identifier (RF): 6 (0x0006)
  
```

```

Padding: 0000
▼ Frame check sequence: 0xcae2ff21 [incorrect, should be 0x885d6559]
  [FCS Good: False]
▼ [FCS Bad: True]
  ▼ [Expert Info (Error/Checksum): Bad checksum]
  
```

4.- Observe ahora uno de los mensajes ICMP echo request de cada ping realizado en c) a diferentes destinos ¿Cuál es la dirección Ethernet origen? ¿Cuál es la dirección Ethernet destino, coincide con la dirección Ethernet de los servidores www.google.es o www.yahoo.es? Dibuje un pequeño esquema con las direcciones IP y Ethernet que entran en juego para explicar lo que sucede.

La dirección de origen es “ 192.68.1.77” con mac “90:32:4b:5b:47:53” y la destino “142.250.185.3” con mac “48:8d:36:4f:b3:6b”.

Tras buscar información, podemos llegar a ver y afirmar que es la dirección de un servidor de google.

Realizo un traceroute como se observa en la tercera imagen. Lo primero que hace es una ARP para conocer la dirección de nuestro router.

Una vez conocida la mac de nuestro router, empezamos a enviar paquetes de 3 con TTL desde 1 y vamos incrementándolo por cada paso de un nodo. Estos nos irán devolviendo por donde van pasando nuestros paquetes y así podremos saber el camino que han seguido.

Nosotros enviamos paquetes UDP y como no llegan al destino a causa de su TTL tan bajo, recibiremos paquetes ICMP indicando que el TTL ha expirado.

Para que quede más clara la explicación, inserto un dibujo que describe muy bien como van pasando los paquetes por cada router y estos nos van contestando. Esta imagen está sacada de “<https://www.hackingarticles.in/working-of-traceroute-using-wireshark/>”.

Durante el camino del traceroute puedo ir viendo las direcciones IP de por donde pasa pero las direcciones mac no.

6 2.1/28b3b78	Arcadyan_4f:b3:6b	HonHaiPr_5b:47:53	ARP	60 192.168.1.1 is at 48:8d:36:4f:b3:6b
9 3.338255907	192.168.1.77	142.250.185.3	ICMP	98 Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 10)
10 3.834254126	142.250.185.3	192.168.1.77	ICMP	98 Echo (ping) reply id=0x0004, seq=1/256, ttl=118 (request in 9)
11 4.339570380	192.168.1.77	142.250.185.3	ICMP	98 Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 12)

Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
 Ethernet II, Src: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53), Dst: Arcadyan_4f:b3:6b (48:8d:36:4f:b3:6b)
 Destination: Arcadyan_4f:b3:6b (48:8d:36:4f:b3:6b)
 Source: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)

142.250.185.3 - Lookup information

here you can find all the gathered information whe could find about the public IP address

142.250.185.3. We locate the IP address to the country United States.

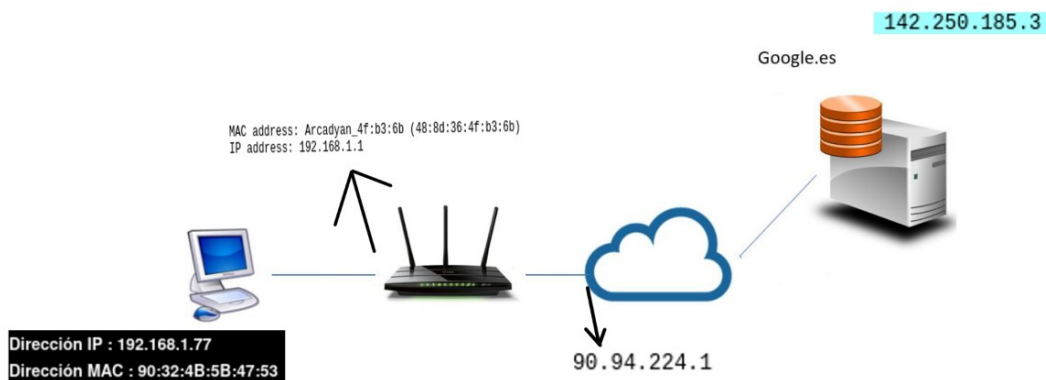
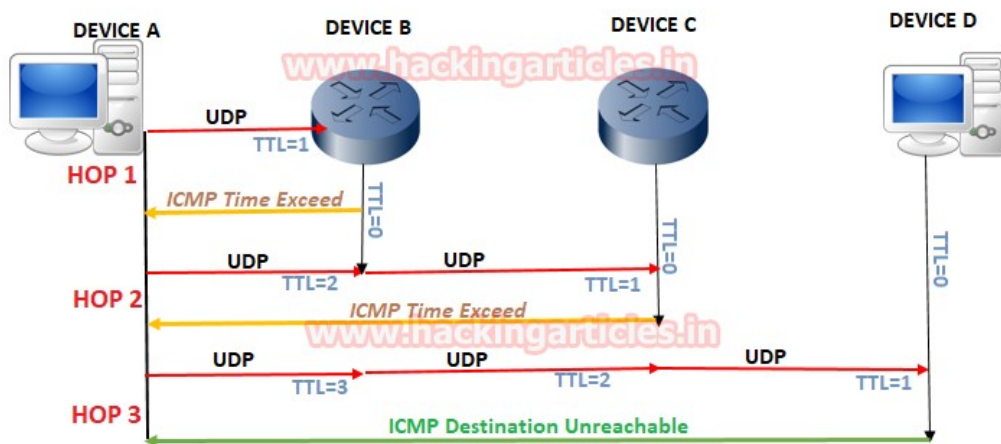
The organisation with owned this IP address is **Google**. We provide this information for free and for personal investigation purpose.

```
[rufo@localhost ~]$ traceroute www.google.es
traceroute to www.google.es (142.250.185.3), 30 hops max, 60 byte packets
 1  gateway (192.168.1.1)  6.126 ms  6.053 ms  6.021 ms
 2  1.224.94.90.dynamic.jazztel.es (90.94.224.1)  14.164 ms  14.151 ms  14.141 ms
 3  10.34.37.17 (10.34.37.17)  14.131 ms  10.34.37.13 (10.34.37.13)  14.121 ms  10.34.37.17 (10.34.37.17)  14.110 ms
 4  10.34.0.47 (10.34.0.47)  32.754 ms  32.744 ms  14.078 ms
 5  72.14.212.54 (72.14.212.54)  32.723 ms  14.056 ms  34.482 ms
 6  108.170.253.225 (108.170.253.225)  15.872 ms  28.139 ms *
 7  142.251.54.152 (142.251.54.152)  9.485 ms  142.251.49.53 (142.251.49.53)  26.458 ms  26.424 ms
 8  mad41s11-in-f3.1e100.net (142.250.185.3)  26.411 ms  26.397 ms  74.125.242.164 (74.125.242.164)  8.488 ms
```

no.	time	source	destination	protocol	length	info
1	0.000000000	HonHaiPr_5b:47:53	Broadcast	ARP		42 Who has 192.168.1.1? Tell 192.168.1.77
2	0.003659331	Arcadyan_4f:b3:6b	HonHaiPr_5b:47:53	ARP		60 192.168.1.1 is at 48:8d:36:4f:b3:6b

3	0.003662994	192.168.1.77	142.250.185.3	UDP	74	37162	→	33434	Len=32
4	0.003665935	192.168.1.77	142.250.185.3	UDP	74	44303	→	33435	Len=32
5	0.003666689	192.168.1.77	142.250.185.3	UDP	74	49285	→	33436	Len=32
6	0.003667303	192.168.1.77	142.250.185.3	UDP	74	33476	→	33437	Len=32
7	0.003667993	192.168.1.77	142.250.185.3	UDP	74	58493	→	33438	Len=32
8	0.003668600	192.168.1.77	142.250.185.3	UDP	74	42991	→	33439	Len=32
9	0.003669234	192.168.1.77	142.250.185.3	UDP	74	52652	→	33440	Len=32
10	0.003669839	192.168.1.77	142.250.185.3	UDP	74	56206	→	33441	Len=32
11	0.003670528	192.168.1.77	142.250.185.3	UDP	74	60062	→	33442	Len=32
12	0.003671145	192.168.1.77	142.250.185.3	UDP	74	44700	→	33443	Len=32
13	0.003671806	192.168.1.77	142.250.185.3	UDP	74	47253	→	33444	Len=32
14	0.003672475	192.168.1.77	142.250.185.3	UDP	74	37174	→	33445	Len=32
15	0.003673087	192.168.1.77	142.250.185.3	UDP	74	34490	→	33446	Len=32
16	0.003673697	192.168.1.77	142.250.185.3	UDP	74	56460	→	33447	Len=32
17	0.003674299	192.168.1.77	142.250.185.3	UDP	74	34352	→	33448	Len=32
18	0.003674944	192.168.1.77	142.250.185.3	UDP	74	42103	→	33449	Len=32
19	0.006103966	192.168.1.1	192.168.1.77	ICMP	102	Time-to-live exceeded			
20	0.006104033	192.168.1.1	192.168.1.77	ICMP	102	Time-to-live exceeded			
21	0.006104065	192.168.1.1	192.168.1.77	ICMP	102	Time-to-live exceeded			
22	0.006579089	192.168.1.77	142.250.185.3	UDP	74	56912	→	33450	Len=32
23	0.006595255	192.168.1.77	142.250.185.3	UDP	74	47646	→	33451	Len=32
24	0.006628260	192.168.1.77	142.250.185.3	UDP	74	53965	→	33452	Len=32

Working of Traceroute



5.- ¿Qué significado tiene cada columna de las que se muestran al ejecutar la orden “arp -a”?

Con el comando arp -a muestra todos los host's que están almacenados en ese momento en cache.

El resultado esta compuesto por la direccion IP del dispositivo (no es la nuestra), su dirección mac y la interfaz por la que se puede llegar a el.

Las columnas pueden varias según el entorno en el que ejecutemos el comando. En la segunda imagen se observa la ejecución del mismo comando pero desde un sistema windows y observamos que este muestra si es de tipo estático o dinámico. En otros sistemas llega incluso a mostrar la hora en la que se ha creado esa entrada.

```
? (192.168.1.115) at 0a:3a:26:1c:e2:de [ether] on wlo1
_gateway (192.168.1.1) at 48:8d:36:4f:b3:6b [ether] on wlo1
```

```
C:\>arp -a

Interfaz: 172.20.1.68 --- 0x2
Dirección de Internet      Dirección física      Tipo
172.20.1.69                14-da-e9-...         dinámico
172.20.1.70                14-da-e9-...         dinámico
172.20.1.72                14-da-e9-...         dinámico
```

6.- Si tras el borrado consultamos de nuevo la tabla caché de ARP, ¿qué información se muestra? Como curiosidad espere 1 o 2 minutos sin interactuar con su PC y vuelva a consultar por tercera vez dicha tabla, ¿observa algún cambio? ¿qué está sucediendo?

Tras borrar la caché, el resultado obtenido es ninguno ya que no le ha dado tiempo a realizar un ARP.

Tras esperar unos minutos obsevamos que ha creado una entrada y es la que nos conectaria con el router, esto se debe a que aunque nosotros no estemos haciendo nada, por detras puede haber un proceso que haya realizado una consulta o petición a fuera de nuestro ordenador y para llevarla a cabo, es necesario realizar un ARP

```
[rufo@localhost ~]$ sudo ip -s -s neigh flush all
Nothing to flush.
[rufo@localhost ~]$ sudo ip -s -s neigh flush all
192.168.1.1 dev wlo1 lladdr 48:8d:36:4f:b3:6b ref 1 used 3/3/3 probes 4 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
[rufo@localhost ~]$ arp -a
[rufo@localhost ~]$
```

```
[rufo@localhost ~]$ arp -a
_gateway (192.168.1.1) at 48:8d:36:4f:b3:6b [ether] on wlo1
```


7.- ¿Qué valores hexadecimales contienen las direcciones Ethernet origen y destino en la petición ARP (ARP Request)?

Observamos que la dirección de origen es “192.168.1.77” y la destino es “192.168.1.115”.

1	0.00000000	HonHaiPr_5b:47:53	ARP	44	Who has 192.168.1.115? Tell 192.168.1.77
2	0.191438209	0a:3a:26:1c:e2:de	ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de


```

Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
Linux cooked capture v1
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)
  Sender IP address: 192.168.1.77
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.115

```

8.- ¿Qué valor tiene el campo “Tipo de trama”? y ¿qué indica?

Asumiendo que “Tipo de trama” hace referencia a “Packet type”, observamos que tiene como valor 4 que significa que el paquete ha sido enviado por nosotros.

1	0.00000000	HonHaiPr_5b:47:53	ARP	44	Who has 192.168.1.115? Tell 192.168.1.77
2	0.191438209	0a:3a:26:1c:e2:de	ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de


```

Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
Linux cooked capture v1
Packet type: Sent by us (4)
  Link-layer address type: Ethernet (1)
  Link-layer address length: 6
  Source: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)
  Unused: 0000
  Protocol: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)
  Sender IP address: 192.168.1.77
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.115

```

9.- ¿Qué valor tiene el campo “opcode” del mensaje ARP? ¿qué significa?

EL CAMPO OPCODE INDICA EL TIPO DE PAQUETE ARP, SOLO EXISTEN 2 VALORES (1 Ó 2) Y ESTE CONTIENE EL VALOR 1 QUE INDICE ARP REQUEST.

```

Protocol size: 4
Opcode: request (1)
Sender MAC address: H

```

10.- ¿Contiene el mensaje ARP la dirección IP de la máquina que envía la petición? ¿dónde aparece la petición en sí, cómo la podemos identificar?

Si, el mensaje ARP contiene nuestra dirección ya que al llegar al destino, este debe saber a donde tiene que responder.

Podemos identificar viendo el primer paquete ARP que es capaz de capturar Wireshark que es el que enviamos nosotros y si bajamos hasta “sender IP” o “sender MAC”, estos campos contendrán tanto la ip como la dirección MAC de nuestro dispositivo.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	HonHaiPr_5b:47:53		ARP	44	Who has 192.168.1.115? Tell 192.168.1.77
2	0.191438209	0a:3a:26:1c:e2:de		ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de

▶ Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0

▶ Linux cooked capture v1

Packet type: Sent by us (4)

Link-layer address type: Ethernet (1)

Link-layer address length: 6

Source: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)

Unused: 0000

Protocol: ARP (0x0806)

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)

Sender IP address: 192.168.1.77

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.1.115

11.- ¿Cuáles son las direcciones Ethernet origen y destino de esta nueva trama? ¿a quién pertenecen? ¿qué diferencias hay entre la petición y la respuesta ARP?

La dirección de origen del paquete ARP Reply es “0a:3a:26:1c:e2:de” y la de destino es “0a:3a:26:1c:e2:de”.

La dirección de origen pertenece al dispositivo contra el que hemos hecho el ping y la de destino es nuestra propia máquina.

La diferencia entre una y otra es que se intercambia la Mac de origen por la de destino y viceversa. Y cambia el “Packet type” que al enviarlo es 4 “Sent by us” y a la vuelta es 0 “Unicast to us”.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	HonHaiPr_5b:47:53		ARP	44	Who has 192.168.1.115? Tell 192.168.1.77
2	0.191438209	0a:3a:26:1c:e2:de		ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de

▶ Frame 2: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0

▶ Linux cooked capture v1

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: 0a:3a:26:1c:e2:de (0a:3a:26:1c:e2:de)

Sender IP address: 192.168.1.115

Target MAC address: HonHaiPr_5b:47:53 (90:32:4b:5b:47:53)

Target IP address: 192.168.1.77

El móvil

unknown_0A:3A:26:1C:E2:DE
Dirección IP : 192.168.1.115
Dirección MAC : 0A:3A:26:1C:E2:DE
última conexión :
2022/04/02 10:32:34

El ordenador

```
unknown_0A:3A:26:1C:E2:DE
Dirección IP : 192.168.1.115
Dirección MAC : 0A:3A:26:1C:E2:DE
última conexión :
2022/04/02 10:32:34
```

Request

1	0.000000000	HonHaiPr_5b:47:53	ARP	44	Who has 192.168.1.115? Tell 192.168.1.77
2	0.191438209	0a:3a:26:1c:e2:de	ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de
▶ Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0					
▼ Linux cooked capture v1					
Packet type: Sent by us (4)					
Link-layer address type: Ethernet (1)					
Link-layer address length: 6					

Reply

2	0.191438209	0a:3a:26:1c:e2:de	ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de
▶ Frame 2: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0					
▼ Linux cooked capture v1					
Packet type: Unicast to us (0)					
Link-layer address type: Ethernet (1)					

12.- ¿Explique el proceso ARP tras el primer ping?, ¿qué sucede cuando ejecuta el segundo ping?

Tras el primer ping, el ordenador tiene almacenado en caché el resultado del ARP por lo que no le hace falta volver a enviar una consulta para saber la MAC del destinatario.

Hará uso de esta entrada y continuará con el ping

1	0.000000000	HonHaiPr_5b:47:53	ARP	44	Who has 192.168.1.115? Tell 192.168.1.77
2	0.191438209	0a:3a:26:1c:e2:de	ARP	44	192.168.1.115 is at 0a:3a:26:1c:e2:de
3	0.191445301	192.168.1.77	192.168.1.115	100	Echo (ping) request id=0x000c, seq=1/256, ttl=64 (reply in 5)
5	0.401673077	192.168.1.115	192.168.1.77	100	Echo (ping) reply id=0x000c, seq=1/256, ttl=64 (request in 3)
6	1.001676828	192.168.1.77	192.168.1.115	100	Echo (ping) request id=0x000c, seq=2/512, ttl=64 (reply in 7)
7	1.144658001	192.168.1.115	192.168.1.77	100	Echo (ping) reply id=0x000c, seq=2/512, ttl=64 (request in 6)
12	2.002919889	192.168.1.77	192.168.1.115	100	Echo (ping) request id=0x000c, seq=3/768, ttl=64 (reply in 13)
13	2.600990909	192.168.1.115	192.168.1.77	100	Echo (ping) reply id=0x000c, seq=3/768, ttl=64 (request in 12)
14	3.003711912	192.168.1.77	192.168.1.115	100	Echo (ping) request id=0x000c, seq=4/1024, ttl=64 (no response found!)

13.- ¿Cree que es posible diferenciar cuándo se ha emitido un ARP y cuándo no, en el terminal, viendo los resultados (tiempos) que muestra la orden ping ejecutada? Razone la respuesta

Dependiendo de lo lejano que se encuentre el dispositivo al que queremos realizar el ping.

Si ha de pasar por muchos intermediarios podremos llegar a ver una demora superior a la media en el primer paquete enviado. Pero si por el contrario el dispositivo se encuentra muy cerca (1 o 2 saltos), el tiempo en realizar ARP será tan pequeño que será difícil observar desde consola esto.

14.- Finalmente, busque en la captura otras peticiones ARP (ARP Request) no emitidos por su máquina, ¿qué significa esto? ¿Por qué sin embargo no se ve ninguna respuesta (ARP Reply) aparte de la que se generó con el comando ping?

En mi caso no he encontrado un paquete como el se está pidiendo pero podría llegarse a encontrar cuando alguno de los hosts que se encuentran en mi misma red estuviesen intentando hacer un ARP para encontrar a otro equipo.

No veríamos ningún ARP Reply ya que no están atentando contra nuestro equipo, sino con otro mediante un unicast.

OPCIONAL

Op 1.- ¿Qué ocurre? ¿Es capaz ARP de resolver este problema de forma automática?, ¿hasta cuándo se tendrá esta situación?

Observamos que se ha creado una nueva entrada con los datos que hemos introducido.

No es capaz de resolver este problema ya que para la máquina no existe ningún problema. Al intentar hacer un ping contra el dispositivo, seremos incapaces de llegar a el pero esto no se cambiará hasta que pase el tiempo que dura cada entrada en la tabla de ARP.

```
[rufo@localhost ~]$ arp -a
gateway (192.168.1.1) at 48:8d:36:4f:b3:6b [ether] on wlo1
[rufo@localhost ~]$ sudo arp -s 192.168.1.115 01:00:5f:ab:cc:de
[sudo] password for rufo:
[rufo@localhost ~]$ arp -n
```

Address	Hwtype	Hwaddress	Flags	Mask	Iface
192.168.1.115	ether	01:00:5f:ab:cc:de	CM		wlo1
192.168.1.1	ether	48:8d:36:4f:b3:6b	C		wlo1

```
[rufo@localhost ~]$
```

Op 2.- ¿Cuánto tiempo dura una entrada en la caché? (/proc/sys/net/ipv4/Leigh/eth0/gc_stale_time).

El tiempo que dura una nueva entrada en caché es de 60 segundos en mi ordenador, esto puede variar segun el dispositivo o lo que nosotros queramos configurar.

```
[rufo@localhost ~]$ cat /proc/sys/net/ipv4/neigh/wlo1/gc_stale_time
60
[rufo@localhost ~]$
```