

Práctica 2

Apellidos: **López Pérez**

Nombre: **Marta**

Titulación: Grado de Ingeniería Informática

Grupo: **2ºA**

PC de la práctica: **PC CASA**

Lea el enunciado de la práctica para saber cómo generar el tráfico de cada ejercicio.

Ejercicio 1. Observe la cabecera IP de los diferentes datagramas:

- ¿Qué protocolo se indica en el campo “protocolo” en la cabecera de los datagramas que transportan mensajes ICMP, FTP y HTTP?

Protocolo	Valor Campo protocolo	Valor (HEX)	Número de trama
ICMP	ICMP (1)	01	34987
HTTP	TCP (6)	06	1557
FTP	TCP (6)	06	9761

No.	Time	Source	Destination
1463	2.978790	192.168.1.138	192.168.1.1
1469	2.982821	192.168.1.1	192.168.1.138
1478	2.988845	192.168.1.138	192.168.1.1
1482	2.993281	192.168.1.1	192.168.1.138
1486	2.995703	192.168.1.138	216.58.209.80
1493	3.021718	216.58.209.80	192.168.1.1
1557	3.284756	192.168.1.138	172.217.168.138
1599	3.361435	192.168.1.138	192.168.1.1
1655	3.462213	192.168.1.138	192.168.1.1
1711	3.562409	172.217.168.138	192.168.1.1

> Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: 08:00:0c:2c:8d:12 (08:00:0c:2c:8d:12)
> Internet Protocol Version 4, Src: 192.168.1.138, Destination: 172.217.168.138
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 664
Identification: 0x6c8a (27834)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x73f6 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.138
Destination: 172.217.168.138

0010 02 98 6c ba 40 00 80 06 73 f6 c0 a8 01 8a ac d5
0020 a8 a3 e3 27 00 50 ad cc 87 41 0a 74 ce 9a 50 18
0030 02 00 18 05 00 00 47 45 54 20 2f 20 48 54 54 56

No.	Time	Source	Destination
9620	19.652134	150.214.40.67	192.168.1.138
9624	19.652404	192.168.1.138	150.214.40.67
9664	19.707025	150.214.40.67	192.168.1.138
9666	19.707129	192.168.1.138	150.214.40.67
9697	19.762008	150.214.40.67	192.168.1.138
9736	19.817801	192.168.1.138	150.214.40.67
9761	19.874312	150.214.40.67	192.168.1.138
9790	19.931020	150.214.40.67	192.168.1.138
9792	19.931224	192.168.1.138	150.214.40.67
9831	19.987095	150.214.40.67	192.168.1.138

> Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: 08:00:0c:2c:8d:12 (08:00:0c:2c:8d:12)
> Internet Protocol Version 4, Src: 150.214.40.67, Destination: 192.168.1.138
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 95
Identification: 0x2e2c (12012)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 51
Protocol: TCP (6)
Header checksum: 0x9761 [validation disabled]
[Header checksum status: Unverified]
Source: 150.214.40.67
Destination: 192.168.1.138

000 84 ef 18 41 77 f6 8c e1 17 ef c3 79 08 00 00 00
010 00 5f 2e ec 40 00 33 06 97 61 96 d6 28 4 00
020 01 8a 00 15 e3 50 8c c7 34 cf af 92 85 00 00 00

No.	Time	Source	Destination
34947	62.737703	192.168.1.138	150.214.54.249
34987	62.791901	150.214.54.249	192.168.1.138

> Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: 08:00:0c:2c:8d:12 (08:00:0c:2c:8d:12)
> Internet Protocol Version 4, Src: 150.214.54.249, Destination: 192.168.1.138
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x9213 (37395)
Flags: 0x0000
Fragment offset: 0
Time to live: 40
Protocol: ICMP (1)
Header checksum: 0x67ac [validation disabled]
[Header checksum status: Unverified]
Type: 8 (Echo (reply))
Code: 0
Checksum: 0x0000

0000 84 ef 18 41 77 f6 8c e1 17 ef c3 79 08 00 00 45
0010 00 3c 92 13 00 00 31 01 67 ac 96 d6 36 f9 c6
0020 01 8a 00 00 54 41 00 01 01 1a 61 62 63 64 65

- ¿Qué indica este campo?

El protocolo que se utiliza en cada trama.

```
Microsoft Windows [Versión 10.0.18362.778]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 150.214.54.249: bytes=32 tiempo=54ms TTL=49

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 54ms, Máximo = 54ms, Media = 54ms

C:\WINDOWS\system32>
```

Ejercicio 2. Seleccione una petición de ICMP de su equipo (el mensaje *echo request*) y complete la siguiente tabla indicando la dirección IP destino (en la cabecera IP) y la dirección MAC destino (en la cabecera Ethernet). Repita el proceso con una petición FTP (en *Info* poner *request*).

	ICMP	FTP
Dirección IP destino (cab IP)	150.214.54.249	192.168.1.138
Dirección MAC destino (cab Ethernet)	8c:e1:17:ef:c3:79	84:ef:18:41:77:f6
Número de trama	34947	9790

icmp

No.	Time	Source	Destination	Protocol	Length	Info
34947	62.737703	192.168.1.138	150.214.54.249	ICMP	74	Echo (ping) request
34987	62.791901	150.214.54.249	192.168.1.138	ICMP	74	Echo (ping) response

Frame 34947: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
 Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
 Internet Protocol Version 4, Src: 192.168.1.138, Dst: 150.214.54.249
 Internet Control Message Protocol

ftp

No.	Time	Source	Destination	Protocol	Length	Info
9761	19.874312	150.214.40.67	192.168.1.138	FTP	109	Response: 200
9790	19.931020	150.214.40.67	192.168.1.138	FTP	77	Response: 200
9792	19.931224	192.168.1.138	150.214.40.67	FTP	60	Request: Q
9831	19.987095	150.214.40.67	192.168.1.138	FTP	68	Response: 200

Frame 9790: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF...
 Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: IntelCor_41:77:f6 (84:ef:18:41:77:f6)
 Internet Protocol Version 4, Src: 150.214.40.67, Dst: 192.168.1.138
 Transmission Control Protocol, Src Port: 21, Dst Port: 58192, Seq: 1285, Ack: 91, Len: 23
 File Transfer Protocol (FTP)
 [Current working directory: /]

- ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

La dirección MAC es la dirección física del dispositivo y por eso no cambia, mientras que la dirección IP cambia dependiendo del protocolo, por eso es distinta.

```
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns
Configuración IP de Windows
Se vació correctamente la caché de resolución de DNS.
C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 1200
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 1200 bytes de datos:
Respuesta desde 150.214.54.249: bytes=1200 tiempo=56ms TTL=49

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 56ms, Máximo = 56ms, Media = 56ms
C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 3100
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 3100 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```

Ejercicio 3. Responda las siguientes preguntas:

- ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)?

No.	Time	Source	Destination	Protocol	Length	Info
25192	49.395974	192.168.1.139	150.214.54.249	ICMP	1242	Echo (ping) request
25216	49.452333	150.214.54.249	192.168.1.139	ICMP	1242	Echo (ping) reply
28223	56.518672	192.168.1.139	150.214.54.249	ICMP	182	Echo (ping) request

> Frame 25192: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF...
> Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
> Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0

No.	Time	Source	Destination	Protocol	Length	Info
25192	49.395974	192.168.1.139	150.214.54.249	ICMP	1242	Echo (ping) request
25216	49.452333	150.214.54.249	192.168.1.139	ICMP	1242	Echo (ping) reply
28223	56.518672	192.168.1.139	150.214.54.249	ICMP	182	Echo (ping) request

> Frame 25216: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF...
> Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: IntelCor_41:77:f6 (84:ef:18:41:77:f6)
> Internet Protocol Version 4, Src: 150.214.54.249, Dst: 192.168.1.139
> Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0

Para el resto de preguntas y rellenar la tabla considere solo las peticiones.

- ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto?
ip.id == identificador
- Completa la siguiente tabla, indicando los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento, separados por comas (,) cuando hay varios fragmentos).

Tamaño	Número de tramas	Identificadores	Flags	Desplazamientos
1200	1	0xb057	0x0000	0
3100	3	0xb058	0x0172	2960

Time	Source	Destination
15532 31.971813	188.122.88.193	192.168.1.139
25192 49.395974	192.168.1.139	150.214.54.249

Frame 25192: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF...
Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
Total Length: 1228
Identification: 0xb057 (45143)
Flags: 0x0000
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)

Tamaño = 1200

Time	Source	Destination
15533 31.974794	188.122.88.193	192.168.1.139
28221 56.518671	192.168.1.139	150.214.54.249
28222 56.518671	192.168.1.139	150.214.54.249
28223 56.518672	192.168.1.139	150.214.54.249

Frame 28223: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface \Device\NPF...
Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
Total Length: 168
Identification: 0xb058 (45144)
Flags: 0x0172
Fragment offset: 2960
Time to live: 128
Protocol: ICMP (1)

Tamaño = 3100

Ejercicio 4. Realice dos pings a **informatica.cv.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). Añada una captura de pantalla.

```
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 1472 -f

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 1472 bytes de datos:
Respuesta desde 150.214.54.249: bytes=1472 tiempo=55ms TTL=49

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 55ms, Máximo = 55ms, Media = 55ms

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 1473 -f

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 1473 bytes de datos:
Es necesario fragmentar el paquete pero se especificó DF.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```

- ¿Cuál es el valor máximo?

1472

- ¿Por qué es ese tamaño?

Para calcular ese número tenemos que coger y al valor máximo de la MTU que es 1500 bytes le tenemos que restar 20 bytes de la cabecera del protocolo IP y 8 bytes de la cabecera de ICMP.

$1500 - 20 - 8 = 1472$.

- ¿En la traza de wireshark aparece el segundo ping? ¿Por qué?

No aparece, porque si observamos la terminal, aparece que se pierde el paquete, ya que no se puede fragmentar y no puede mandar todos sus bytes.

Ejercicio 5. Haga un ping a **informatica.cv.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta del servidor. Observe en Wireshark el intercambio de paquetes que se produce.

```
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -i 1

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -i 2

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 100.85.0.1: TTL expirado en tránsito.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
```

- Número de trama analizado
5101

icmp

Time	Source	Destination	Protocol
2812 6.424138	192.168.1.139	150.214.54.249	ICMP
5090 13.770884	192.168.1.139	150.214.54.249	ICMP
5101 13.798822	100.85.0.1	192.168.1.139	ICMP

Frame 5101: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: IntelCor_41:77:f6

Internet Protocol Version 4, Src: 100.85.0.1, Dst: 192.168.1.139

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0x9fa3 [correct]
 [Checksum Status: Good]
 Unused: 00000000

Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0xb3df (46047)
 > Flags: 0x0000
 Fragment offset: 0
 > Time to live: 1
 > Expert Info (Note/Sequence): "Time To Live" only 1
 ["Time To Live" only 1]
 [Severity level: Note]

• ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?

• ¿Qué incluye dicho mensaje ICMP como información adicional?

Ejercicio 6. Responda a las siguientes preguntas:

```

C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>tracert informatica.cv.uma.es

Trazo a la dirección frontalcv7.cv.uma.es [150.214.54.249]
sobre un máximo de 30 saltos:

 1      *         *         *         Tiempo de espera agotado para esta solicitud.
 2     26 ms     24 ms     24 ms     100.85.0.1
 3     17 ms     16 ms     18 ms     10.15.4.81
 4     16 ms     17 ms     16 ms     10.0.24.54
 5     17 ms     17 ms     17 ms     be4430.rcr22.svq01.atlas.cogentco.com [149.11.19.193]
 6     30 ms     30 ms     30 ms     be3240.ccr31.vlc02.atlas.cogentco.com [154.54.59.13]
 7     34 ms     34 ms     35 ms     be3356.ccr32.mad05.atlas.cogentco.com [154.54.57.241]
 8     35 ms     34 ms     35 ms     be3379.agr22.mad05.atlas.cogentco.com [154.54.39.146]
 9     35 ms     35 ms     35 ms     be3481.nr51.b015537-1.mad05.atlas.cogentco.com [154.25.1.110]
10     42 ms     35 ms     35 ms     149.14.242.226
11     44 ms     43 ms     44 ms     130.206.245.122
12     60 ms     62 ms     76 ms     cica-router-backup.red.rediris.es [130.206.211.42]
13     61 ms     61 ms     60 ms     uma-router.red.cica.es [150.214.231.170]
14     54 ms     53 ms     63 ms     tuneles.uma.es [150.214.47.249]
15     55 ms     55 ms     54 ms     te6009dixie.ruma.uma.es [150.214.41.238]
16      *         *         *         Tiempo de espera agotado para esta solicitud.
17     54 ms     54 ms     55 ms     frontalcv7.cv.uma.es [150.214.54.249]

Trazo completa.

```

- Indique el número de los paquetes utilizados para responder estas preguntas

Números indicados en cada pregunta.

- ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función?

Los de tipo ICMP. Paquetes 3,4,5,53,54,55,56... hay 93 en total que se usan al hacer el tracert.

ip.dst == 150.214.54.249 && ip.src == 192.168.1.139						
	Time	Source	Destination	Protocol	Length	Info
3	0.039988	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1000/59395, ttl=1 (r
4	3.698818	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1001/59651, ttl=1 (r
5	7.685441	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1002/59907, ttl=1 (r
53	11.699653	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1003/60163, ttl=2 (r
54	11.725579	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
55	11.727705	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1004/60419, ttl=2 (r
56	11.751832	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
57	11.753955	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1005/60675, ttl=2 (r
58	11.778176	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
67	17.336530	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1006/60931, ttl=3 (r
68	17.354103	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transi
69	17.356188	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1007/61187, ttl=3 (r
70	17.372971	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transi
71	17.375057	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1008/61443, ttl=3 (r
72	17.393073	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transi

- Además de los mensajes propios para obtener el camino, **tracert** puede provocar que se realicen otros envíos auxiliares para conseguir información o mostrar de forma más amistosa la información, ¿qué otros mensajes pueden ser necesarios?

Podría ser necesario algunos de tipo DNS, ya que traduce las direcciones IP a las URL que les corresponde

Tramas 163,165,166,167,168 las del siguiente ejemplo.

Time	Source	Destination	Protocol	Length	Info
161 33.146821	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1025/260, ttl=9 (n
162 33.182375	154.25.1.110	192.168.1.139	ICMP	110	Time-to-live exceeded (Time to live exceeded in transi
163 33.182914	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1026/516, ttl=9 (n
164 33.218342	154.25.1.110	192.168.1.139	ICMP	110	Time-to-live exceeded (Time to live exceeded in transi
165 33.220669	192.168.1.139	46.6.113.34	DNS	85	Standard query 0x70e5 PTR 110.1.25.154.in-addr.arpa
166 33.476347	46.6.113.34	192.168.1.139	DNS	145	Standard query response 0x70e5 PTR 110.1.25.154.in-add
167 33.550150	192.168.1.139	46.6.113.34	DNS	91	Standard query 0xa3e6 A settings-win.data.microsoft.co
168 33.589053	46.6.113.34	192.168.1.139	DNS	154	Standard query response 0xa3e6 A settings-win.data.mic
169 33.589464	192.168.1.139	51.124.78.146	TCP	66	62132 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25

```

Name: 110.1.25.154.in-addr.arpa
[Name Length: 25]
[Label Count: 6]
Type: PTR (domain name PointeR) (12)
Class: IN (0x0001)

Answers
  110.1.25.154.in-addr.arpa: type PTR, class IN, be3481.nr51.b015537-1.mad05.atlas.cogentco.com
    Name: 110.1.25.154.in-addr.arpa
    Type: PTR (domain name PointeR) (12)
    Class: IN (0x0001)
    Time to live: 43200 (12 hours)
    Data length: 48
    Domain Name: be3481.nr51.b015537-1.mad05.atlas.cogentco.com

```

Si nos fijamos en la captura de la consola de este ejercicio en el ttl 9, observamos que esta trama DNS le devuelve la IP del nodo intermedio para que se vaya moviendo, pero esta IP está invertida.

```

[Request In: 165]
[Time: 0.055638000 seconds]

84 ef 18 41 77 f6 8c e1 17 ef c3 79 08 00 45 00 ...Aw...y..E.
00 83 b5 b8 40 00 fc 11 67 55 2e 06 71 22 c0 a8 ...@...gU..q"
01 8b 00 35 c6 a9 00 6f be ad 70 e5 81 80 00 01 ...5...o..p....
00 01 00 00 00 00 03 31 30 01 31 02 32 35 03 .....1 10.1.25.
31 35 34 07 69 6e 2d 61 64 64 72 04 61 72 70 61 154.in-a ddr.arpa
00 00 0c 00 01 c0 0c 00 0c 00 01 00 00 a8 c0 00 .....
30 06 62 65 33 34 38 31 04 6e 72 35 31 09 62 30 0-be3481 .nr51.b0
31 35 35 33 37 2d 31 05 6d 61 64 30 35 05 61 74 15537-1. mad05.at
6c 61 73 08 63 6f 67 65 6e 74 63 6f 03 63 6f 6d las.coge ntco.com
00

```

- ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete?

Según las diferentes tablas de encaminamiento de router a router se envían ICMP hasta que llega al destino determinado. Las tramas en negro devuelven la IP de los nodos intermedios y las tramas DNS las IPs de destino de los nodos intermedios, así es como se ve todos los pasos que hace.