

Realiza un documento en el que muestres:

1-El resultado del traceroute a www.elmundo.es

2-Los paquetes enviados y recibidos capturados con Wireshark, mostrando especial atención a:

TTL, IP origen, IP destino

3-Una explicación del traceroute

1.

```
a@a:~$ traceroute -I www.elmundo.es
traceroute to www.elmundo.es (151.101.133.50), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.071 ms  0.058 ms  0.054 ms
 2  192.168.10.1 (192.168.10.1)  0.877 ms  1.153 ms  1.448 ms
 3  * 10.195.160.1 (10.195.160.1)  16.725 ms  *
 4  * * *
 5  * * *
 6  157.52.127.128 (157.52.127.128)  12.365 ms  11.147 ms  11.382 ms
 7  151.101.133.50 (151.101.133.50)  11.234 ms  10.308 ms  10.804 ms
a@a:~$
```

2.

En estos ejemplos vemos tanto la ip de origen como la ip destino, además un TTL de 64

Además con la segunda captura nos cercioramos que el TTL es el mismo en los protocolos DNS

The image displays two Wireshark packet captures. The top capture shows a series of packets including DNS queries and responses, and ICMP echo requests. The bottom capture shows a single ICMP echo request packet.

**Top Capture (Frame 7):** This frame shows an ICMP Echo (ping) request from 10.0.2.15 to 192.168.10.1. The packet details show the Internet Protocol Version 4 header with Source: 10.0.2.15 and Destination: 192.168.10.1. The UDP header shows Port: 54243. The ICMP header shows Type: 8 (Echo) and Code: 0. The packet bytes show the ICMP Echo request structure.

**Bottom Capture (Frame 5):** This frame shows an ICMP Echo (ping) request from 192.168.10.1 to 10.0.2.15. The packet details show the Internet Protocol Version 4 header with Source: 192.168.10.1 and Destination: 10.0.2.15. The UDP header shows Port: 54243. The ICMP header shows Type: 8 (Echo) and Code: 0. The packet bytes show the ICMP Echo request structure.

Pero cuando nos encontramos el ICMP vemos que los paquetes tienen un TTL de 1,2,3,4 etc tal y como vemos en las capturas.

8	0.367460799	192.168.10.1	10.0.2.15	DNS	162 Standard query response 0xab40 AAAA unidadeditorial.
9	0.367621669	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=1/256, ttl=1 (no
10	0.367633719	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=2/512, ttl=1 (no
11	0.367637730	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=3/768, ttl=1 (no
12	0.367643980	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=4/1024, ttl=2 (n
13	0.367667831	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=5/1280, ttl=2 (n

  

Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0					
Ethernet II, Src: PcsCompu_19:03:00 (08:00:27:19:03:00), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)					
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 151.101.133.50					
0100 .... = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 60					
Identification: 0x2e5d (11869)					
Flags: 0x0000					
Fragment offset: 0					
Time to live: 1					
Protocol: ICMP (1)					
Header checksum: 0x62be [validation disabled]					
[Header checksum status: Unverified]					
Source: 10.0.2.15					
Destination: 151.101.133.50					

  

0000	52	54	00	12	35	02	08	00	27	19	03	00	08	00	45	00	RT	..5	..	....	E
0010	00	3c	2e	5d	00	00	01	01	62	be	0a	00	02	0f	97	65	<	0	...	b	.....
0020	85	32	08	00	82	76	00	02	00	02	48	49	4a	4b	4c	4d	2	...	v	...	HIJKLM
0030	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d					NOPQRSTU VwXYZ[\
0040	5e	5f	60	61	62	63	64	65	66	67											^_ abcde fg

5	0.310949519	192.168.10.1	10.0.2.15	DNS	140 Standard query response 0xa42a A www.elmundo.es CNAME
6	0.325599593	192.168.10.1	10.0.2.15	DNS	190 Standard query response 0xf029 AAAA www.elmundo.es C
7	0.325790145	10.0.2.15	192.168.10.1	DNS	101 Standard query 0xab40 AAAA unidadeditorial.map.fastl
8	0.367460799	192.168.10.1	10.0.2.15	DNS	162 Standard query response 0xab40 AAAA unidadeditorial.
9	0.367621669	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=1/256, ttl=1 (no
10	0.367633719	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=2/512, ttl=1 (no
11	0.367637730	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=3/768, ttl=1 (no
12	0.367643980	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=4/1024, ttl=2 (n
13	0.367667831	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=5/1280, ttl=2 (n

  

Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0					
Ethernet II, Src: PcsCompu_19:03:00 (08:00:27:19:03:00), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)					
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 151.101.133.50					
0100 .... = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 60					
Identification: 0x2e60 (11872)					
Flags: 0x0000					
Fragment offset: 0					
Time to live: 2					
Protocol: ICMP (1)					
Header checksum: 0x61bb [validation disabled]					
[Header checksum status: Unverified]					
Source: 10.0.2.15					
Destination: 151.101.133.50					

19	0.367739246	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=8/2048, ttl=3 (n
20	0.367745556	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=9/2304, ttl=3 (n
21	0.367765997	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=10/2560, ttl=4 (
22	0.367770798	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=11/2816, ttl=4 (
23	0.367796669	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=12/3072, ttl=4 (
24	0.367803540	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=13/3328, ttl=5 (
25	0.367821021	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=14/3584, ttl=5 (
26	0.367825651	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=15/3840, ttl=5 (
27	0.367854473	10.0.2.15	151.101.133.50	ICMP	74 Echo (ping) request id=0x0002, seq=16/4096, ttl=6 (
28	0.368466704	192.168.10.1	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in tran
29	0.368718319	192.168.10.1	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in tran
30	0.369342706	192.168.10.1	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in tran
31	0.380541275	157.52.127.128	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in tran

  

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0					
Ethernet II, Src: PcsCompu_19:03:00 (08:00:27:19:03:00), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)					
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 151.101.133.50					
0100 .... = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 60					
Identification: 0x2e64 (11876)					
Flags: 0x0000					
Fragment offset: 0					
Time to live: 3					
Protocol: ICMP (1)					
Header checksum: 0x60b7 [validation disabled]					
[Header checksum status: Unverified]					
Source: 10.0.2.15					
Destination: 151.101.133.50					

  

0000	52	54	00	12	35	02	08	00	27	19	03	00	08	00	45	00	RT	..5	..	....	E
0010	00	3c	2e	64	00	00	01	01	60	b7	0a	00	02	0f	97	65	<	0	...	d	.....

3.

La utilidad de diagnóstico TRACERT determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino. En estos paquetes, TRACERT usa valores de período de vida (TTL) IP variables, poniendo un TTL muy bajo en cada paquete para ver en que IP/RED desaparece, así sacando las IP por donde pasa el paquete