

Redes - 1er Cuatrimestre 2025
Alumna: Lara Converso
Padrón: 107632

Tarea: usar el comando "dig" con las opciones iterativa, autorizada y verborrágica capturando por la pantalla de la terminal y también mediante "Wireshark".

Comando utilizado: **dig google.com +stats +comments +trace**

Flags:

+trace hace consultas iterativas desde el root hasta encontrar el servidor autoritativo del dominio consultado (en este caso google.com).

+comments agrega comentarios explicando la salida de dig.

+stat brinda más información sobre el paso a paso del recorrido del DNS.

Captura de dig con las opciones activadas:

```
larac@larac:~$ dig google.com +comments +trace +stat

; <<>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <<>> google.com +comments +trace +stat
;; global options: +cmd
.          3750      IN      NS      d.root-servers.net.
.          3750      IN      NS      h.root-servers.net.
.          3750      IN      NS      f.root-servers.net.
.          3750      IN      NS      j.root-servers.net.
.          3750      IN      NS      l.root-servers.net.
.          3750      IN      NS      a.root-servers.net.
.          3750      IN      NS      c.root-servers.net.
.          3750      IN      NS      g.root-servers.net.
.          3750      IN      NS      e.root-servers.net.
.          3750      IN      NS      m.root-servers.net.
.          3750      IN      NS      i.root-servers.net.
.          3750      IN      NS      k.root-servers.net.
.          3750      IN      NS      b.root-servers.net.
;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Apr 03 21:54:11 -03 2025
;; MSG SIZE rcvd: 262

;; UDP setup with 2001:dc3::35#53(2001:dc3::35) for google.com failed: network unreachable.
;; no servers could be reached
;; UDP setup with 2001:dc3::35#53(2001:dc3::35) for google.com failed: network unreachable.
;; no servers could be reached
;; UDP setup with 2001:dc3::35#53(2001:dc3::35) for google.com failed: network unreachable.
com.      172800     IN      NS      a.gtld-servers.net.
com.      172800     IN      NS      b.gtld-servers.net.
com.      172800     IN      NS      c.gtld-servers.net.
com.      172800     IN      NS      d.gtld-servers.net.
com.      172800     IN      NS      e.gtld-servers.net.
com.      172800     IN      NS      f.gtld-servers.net.
com.      172800     IN      NS      g.gtld-servers.net.
com.      172800     IN      NS      h.gtld-servers.net.
com.      172800     IN      NS      i.gtld-servers.net.
com.      172800     IN      NS      j.gtld-servers.net.
com.      172800     IN      NS      k.gtld-servers.net.
com.      172800     IN      NS      l.gtld-servers.net.
com.      172800     IN      NS      m.gtld-servers.net.
com.      86400      IN      DS      19718 13 2 8ACBB0CD28F41250A80A491389424D341522D94
6B0DA0C0291F2D3D7 71D7805A
com.      86400      IN      RRSIG   DS 8 1 86400 20250416200000 20250403190000 53148 .
HI/7SZNA1tSi+bDHAHxX674eQ1VDoN1XhCH2/NZzhsIm47U0A5cIM7TE j5M5Ns6SprjdLT7A61q59fr9Y6NnbUM8YSIXGrkB
nGP/H5h8cVR20eYq szPpK+F7+k2G094veHTGTfni/cf+LUHeNDU4yjskUVKmvBkqReQTzY8X UPQ1zDs0xaUtlH7N3ZTP/C/H
YWqoyLQVS2JsLapKHbKP+t4hgeLGicMT jSc7fudmAshJ1dRaolBiJR+Z5M8u/Xl/Cvc3mGILVd8immQUt/Zn80eO N+Njp2Hd
ZLc0YMQMc8JTk8mfwoEVFviMTNX/4jB2i4A0LuesCL48h1vz vfrWxw==
```

```

;; Query time: 300 msec
;; SERVER: 170.247.170.2#53(b.root-servers.net) (UDP)
;; WHEN: Thu Apr 03 21:54:12 -03 2025
;; MSG SIZE rcvd: 1170

;; UDP setup with 2001:503:83eb::30#53(2001:503:83eb::30) for google.com failed: network unreachable.
google.com.          172800 IN      NS      ns2.google.com.
google.com.          172800 IN      NS      ns1.google.com.
google.com.          172800 IN      NS      ns3.google.com.
google.com.          172800 IN      NS      ns4.google.com.
CK0P0JMG874LJREF7EFN8430QVIT8BSM.com. 900 IN NSEC3 1 1 0 - CK0Q3UDG8CEKKA7RUKPGCT1DVSSH8LL NS SOA
RRSIG DNSKEY NSEC3PARAM
CK0P0JMG874LJREF7EFN8430QVIT8BSM.com. 900 IN RRSIG NSEC3 13 2 900 20250409002636 20250401231636 23
202 com. Dbaltv0z92QJvY2nAt0d55b8q5sSwao3YVweFQuonJsZ2ilokw7lkNuh b6Pk/kdRYB5qnrnOFp5dWDGqQMofdw==
S84BOR4DK28HNHPLC2180483V000D5D8.com. 900 IN NSEC3 1 1 0 - S84BR9CIB2A20L3ETR1M2415ENPP99L8 NS DS
RRSIG
S84BOR4DK28HNHPLC2180483V000D5D8.com. 900 IN RRSIG NSEC3 13 2 900 20250410013910 20250403002910 23
202 com. UA3WZJJXAreuA8rOavJptjAKJYf+qY06GA0y3yQ1w7Rwx/B3hxWEbfXX oTzfomd1FFSj+OYqW7mPJduDfZQ9agg==
;; Query time: 176 msec
;; SERVER: 192.5.6.30#53(a.gtld-servers.net) (UDP)
;; WHEN: Thu Apr 03 21:54:12 -03 2025
;; MSG SIZE rcvd: 644

;; UDP setup with 2001:4860:4802:38::a#53(2001:4860:4802:38::a) for google.com failed: network unreachable.
;; UDP setup with 2001:4860:4802:32::a#53(2001:4860:4802:32::a) for google.com failed: network unreachable.
google.com.          300      IN      A       216.58.202.110
;; Query time: 56 msec
;; SERVER: 216.239.34.10#53(ns2.google.com) (UDP)
;; WHEN: Thu Apr 03 21:54:12 -03 2025
;; MSG SIZE rcvd: 55

```

Se puede ver que se realizan las consultas comenzando en la raíz(root) y luego a través del .com hasta encontrar ns 1, 2, 3 y 4 de google. Y luego la consulta final al NS autoritativo (ns2.google.com) a la dirección 216.239.34.10

Captura de wireshark que refleja lo ocurrido mientras se ejecutó dig:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.12	170.247.170.2	DNS	93	Standard query 0xf8af A google
3	0.297632030	170.247.170.2	192.168.64.12	DNS	1212	Standard query response 0xf8af
5	0.303594802	192.168.64.12	192.5.6.30	DNS	93	Standard query 0x999f A google
6	0.474717275	192.5.6.30	192.168.64.12	DNS	686	Standard query response 0x999f
7	0.476559407	192.168.64.12	216.239.34.10	DNS	93	Standard query 0xe1dc A google
8	0.531573113	216.239.34.10	192.168.64.12	DNS	97	Standard query response 0xe1dc

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface enp0s1, id 0
 Ethernet II, Src: 06:a6:df:d1:1a:76 (06:a6:df:d1:1a:76), Dst: 5e:e9:1e:3b:c5:64 (5e:e9:1e:3b:c5:64)
 Internet Protocol Version 4, Src: 192.168.64.12, Dst: 170.247.170.2
 User Datagram Protocol, Src Port: 33554, Dst Port: 53
 Domain Name System (query)
 Transaction ID: 0xf8af

0000 5e e9 1e 3b c5 64 06 a6 df d1 1a 76 08 00 45 00 ^.; d. . . v. E.
 0010 00 4f 83 42 00 00 40 11 a1 ad c0 a8 40 0c aa f7 .O.B..@.@..
 0020 aa 02 83 12 00 35 00 3b c1 c2 f8 af 00 20 00 015;
 0030 00 00 00 00 00 01 06 67 6f 6f 67 6c 65 03 63 6fg oogle-co
 0040 6d 00 00 01 00 01 00 00 29 04 d0 00 00 80 00 00 m.....).
 0050 0c 00 0a 00 08 6f c4 f8 4a 1f a4 28 8eo.. J..(

Total Length (ip.len), 2 bytes Packets: 10 · Displayed: 6 (60.0%) · Dropped: 0 (0.0%) Profile: Default

Se puede ver el paquete 1, realiza la consulta sale desde mi dirección (192.168.64.12) hacia 170.247.170.2 y el paquete 3 es la respuesta a esta consulta.

Lo mismo ocurre en los paquetes 5 y 6, y por último entre el 7 y 8 es la última consulta y respuesta con el NS autoritativo elegido de google.

Para comparación adjunto una captura de pantalla comando dig consultando al dns de google (@8.8.8.8) por el dominio google.com, sin ninguna flag

```
larac@larac:~$ dig @8.8.8.8 google.com

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> @8.8.8.8 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22791
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;google.com.                                IN      A

;; ANSWER SECTION:
google.com.      86      IN      A      142.250.79.142

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Mar 31 23:35:59 -03 2025
;; MSG SIZE rcvd: 55
```

y como se visualiza en wireshark, simplemente se realiza la request con dig y se obtiene una respuesta, en este caso es una única consulta directa al DNS

The image shows a Wireshark network capture of a DNS transaction. The top pane displays a list of packets, with packet 2 selected. The middle pane shows the details of packet 2, which is a DNS Standard query response from 8.8.8.8 to 192.168.64.12. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.12	8.8.8.8	DNS	93	Standard query 0x5907 A google.com OPT
2	0.026755629	8.8.8.8	192.168.64.12	DNS	97	Standard query response 0x5907 A google.com A 142.250.79.142

Frame 2: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface enp0s1, id 0

- Ethernet II, Src: 5e:e9:1e:3b:c5:64 (5e:e9:1e:3b:c5:64), Dst: 06:a6:df:d1:1a:76 (06:a6:df:d1:1a:76)
- Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.64.12
- User Datagram Protocol, Src Port: 53, Dst Port: 49341
- Domain Name System (response)
 - Transaction ID: 0x5907
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - Additional records
 - [\[Request In: 1\]](#)

[Time: 0.026755629 seconds]

0000 06 a6 df d1 1a 76 5e e9 1e 3b c5 64 08 00 45 00v^.;d..E.
0010 00 53 16 d1 00 00 78 11 1b 05 08 08 08 08 c0 a8 ..S...x.....
0020 40 0c 00 00 35 c0 bd 00 3f 78 82 59 07 81 80 00 01 @.5...?x.Y....
0030 00 01 00 00 00 01 06 67 6f 6f 67 6c 65 03 63 6fg oogle:co
0040 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 56 m.....V
0050 00 04 8e fa 4f 8e 00 00 29 02 00 00 00 00 00 00Q...).....
0060 00

Frame (frame), 97 bytes Packets: 14 · Displayed: 2 (14.3%) Profile: Default

El paquete 1 representa la consulta enviada (dig) y el paquete nro 2 la respuesta que recibí.