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.

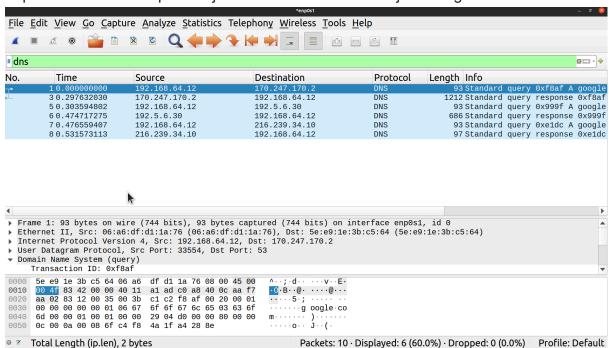
Captura de dig con las opciones activadas:

```
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
                                                    h.root-servers.net.
                          3750
                                           NS
                                                    f.root-servers.net.
                                  IN
                          3750
                                  IN
                                           NS
                                                    j.root-servers.net.
                          3750
                                   ΙN
                                           NS
                                                    l.root-servers.net.
                          3750
                                   IN
                                           NS
                                                   a.root-servers.net.
                          3750
                                           NS
                                                   c.root-servers.net.
                                  IN
                                                   g.root-servers.net.
                          3750
                                   IN
                                           NS
                          3750
                                   IN
                                           NS
                                                   e.root-servers.net.
                          3750
                                   ΙN
                                           NS
                                                   m.root-servers.net.
                          3750
                                           NS
                                                    i.root-servers.net.
                                  IN
                          3750
                                                    k.root-servers.net.
                                  ΙN
                                           NS
                          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
                                                                                                      I
;; 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.
                                                    a.gtld-servers.net.
                          172800 IN
                                           NS
                                                    b.gtld-servers.net.
com.
                          172800
                                  IN
                                                    c.gtld-servers.net.
com.
                          172800
                                   ΙN
                                           NS
                          172800
                                           NS
                                                    d.gtld-servers.net.
COM.
                                                   e.gtld-servers.net.
                          172800
                                   IN
                                           NS
com.
                                                    f.gtld-servers.net.
                          172800
                                           NS
COM.
                                   ΙN
                                                    g.gtld-servers.net.
com.
                          172800
                                  IN
                                           NS
                          172800
                                   IN
                                           NS
                                                    h.gtld-servers.net.
COM.
com.
                          172800
                                  IN
                                                    i.gtld-servers.net.
                                                    j.gtld-servers.net.
                                           NS
                          172800
                                   IN
COM.
                                                    k.gtld-servers.net.
COM.
                          172800
                                   TN
                                           NS
                          172800
                                  IN
                                           NS
                                                    l.gtld-servers.net.
COM.
com.
                          172800
                                   IN
                                           NS
                                                    m.gtld-servers.net.
                          86400
                                                    19718 13 2 8ACBB0CD28F41250A80A491389424D341522D94
                                   IN
COM.
6B0DA0C0291F2D3D7 71D7805A
                                                    DS 8 1 86400 20250416200000 20250403190000 53148
                          86400
                                   IN
                                           RRSIG
HI/7SZNA1tSi+bDHAhxX674eQ1VDoN1XhCH2/NZzhsIm47UOAScIM7TE j5M5Ns6SpRjdLT7A61q59fr9Y6NnbUM8YSIXGrkB
nGP/H5h8cvR2OeYq szPpK+F7+k2G094veHTGTfnI/cf+lUHeNDU4yjskUVKmvBkqReQTzY8X UPQ1zDsOxaUtlH7N3ZTP/C/H
YWqoyLQVS2JsLapKHbKP+t4hgeLGicMT jSc7fudmAshJ1dRaolBiJR+Z5M8u/Xl/Cvc3mGIlVd8immQUt/Zn8OeO N+NjP2Hd
ZLc0YMQMc8JTk8mfWoEVFviMTNX/4jB2i4AOlUesCL48h1vz vfrWXw==
```

```
Query time: 300 msec
;; MSG SIZE rcvd: 1170
;; UDP setup with 2001:503:83eb::30#53(2001:503:83eb::30) for google.com failed: network unreachab
le.
google.com.
                         172800
                                                  ns2.google.com.
                         172800
                                         NS
                                                  ns1.google.com.
aooale.com.
                                 IN
                                                  ns3.google.com.
google.com.
                         172800
                                 IN
                                         NS
google.com.
                         172800 IN
                                         NS
                                                  ns4.google.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 900 IN NSEC3 1 1 0 - CK0Q3UDG8CEKKAE7RUKPGCT1DVSSH8LL NS SOA
RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 900 IN RRSIG NSEC3 13 2 900 20250409002636 20250401231636 23 202 com. Dbaltv0z92QJvY2nAt0d55b8q5sSwao3YVweFQuonJsZ2ilokw7lkNuh b6Pk/kdRYB5qrnr0Fp5dWDGqQMofdw==
S84BOR4DK28HNHPLC2180483V000D5D8.com. 900 IN NSEC3 1 1 0 - S84BR9CIB2A20L3ETR1M2415ENPP99L8 NS DS
S84BOR4DK28HNHPLC2180483V000D5D8.com. 900 IN RRSIG NSEC3 13 2 900 20250410013910 20250403002910 23
202 com. UA3WZJJXAreuA8rOavJptjAKJYf+qY06GAOy3yQ1w7Rwx/B3hxWEbfXX oTzfomd1FFSJ+OYqW7mPJuDfZQ9agg==
;; 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 unr
;; UDP setup with 2001:4860:4802:32::a#53(2001:4860:4802:32::a) for google.com failed: network unr
eachable.
google.com
                         300
                                 IN
                                                  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:



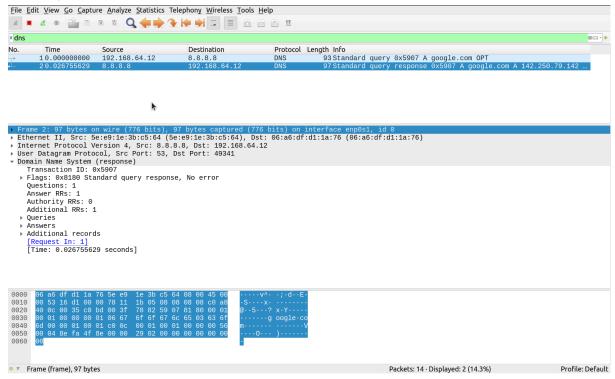
Se puede ver el paquete 1, realiza la consulta sale desde mi dirección (192.168.64.12) hacia 170.247.170.2 y el paquete 3 es la respuesta a esta consulta.

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:
                                IN
;google.com.
                                        Α
;; ANSWER SECTION:
google.com.
                        86
                                IN
                                         Α
                                                 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



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