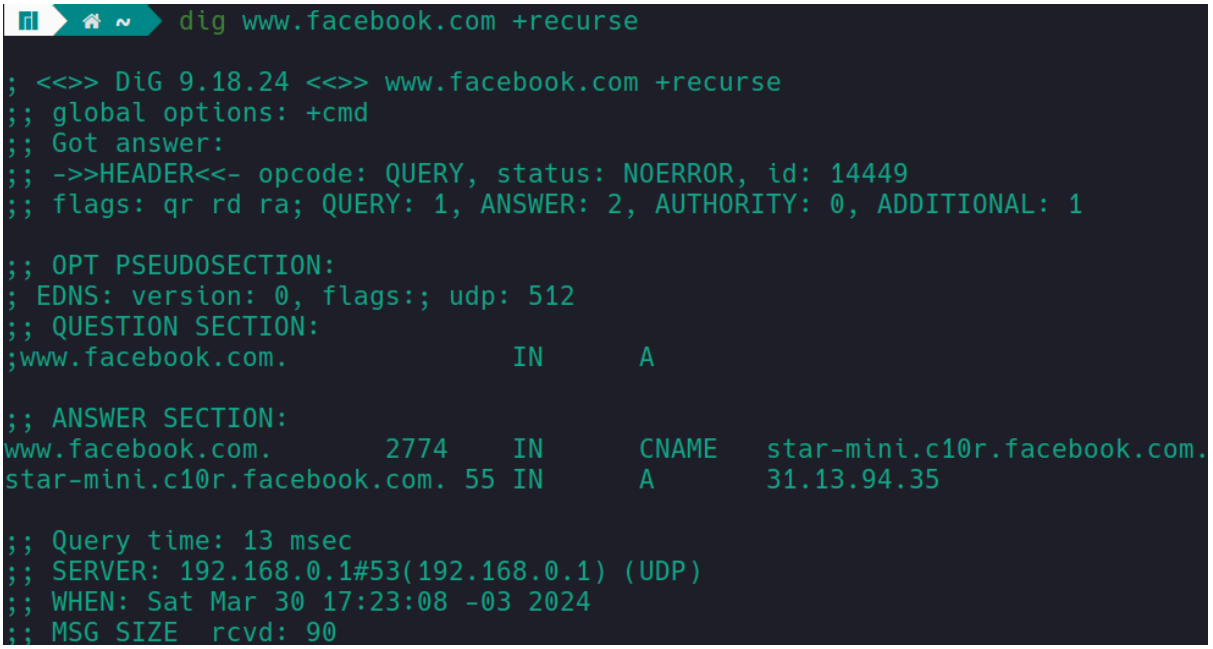
# TP - DNS

Con el fin de poder obtener resultados comparables entre sí, para la ejecución de cada comando dig se utiliza el alias www.facebook.com. A su vez, para la comparación entre terminal y Wireshark solo se utilizará una captura de pantalla de las respuestas para este último debido a que la respuesta contiene todos los campos de la query.

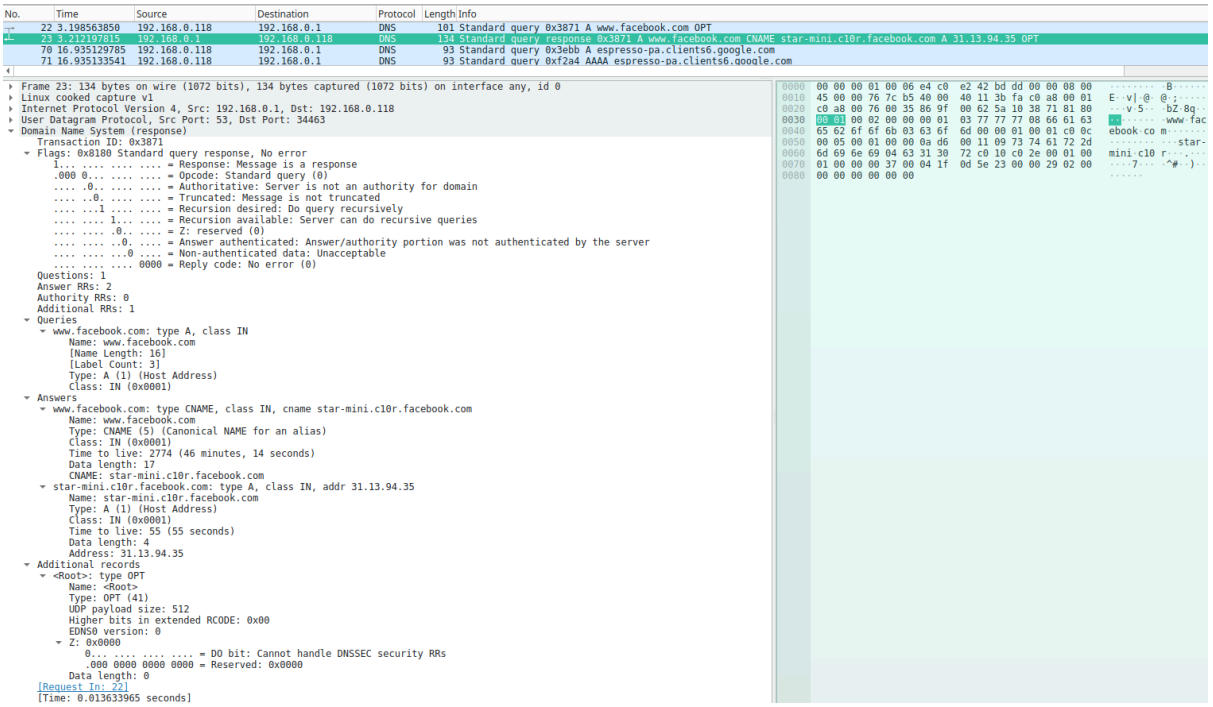
**Ejecución recursiva:**

Al utilizar el flag +recurse, se le indica al servidor DNS que debe resolver recursivamente la solicitud o query. Esto significa que, en caso de no tener la respuesta guardada en caché, el servidor DNS es el encargado de realizar las sucesivas consultas a root, TLD y authoritative servers.




El header posee tres flags los cuales significan, respectivamente, que se está observando una response, que se desea que la query sea resuelta de forma recursiva y que el servidor DNS consultado soporta la realización de queries recursivas.

A su vez, se observa que se obtuvieron dos respuestas: una indicando que el alias www.facebook.com corresponde al canonical name (CNAME) star-mini.c10r.facebook.com, y otra indicando que dicho canonical name corresponde a la dirección IPv4 31.13.94.35 (el record obtenido es de tipo A lo cual indica v4 de IP mientras que si fuese un record AAAA la respuesta sería una dirección IPv6).




Si se compara la respuesta obtenida de realizar dig a www.facebook.com con la de realizarlo a facebook.com, se puede observar que la response en este caso no devuelve en su respuesta el CNAME record. Esto se debe a que el authoritative DNS server de facebook.com no contiene un CNAME record cuyo authoritative DNS server contiene el A record con la IP buscada, sino que directamente posee el A record recién mencionado.

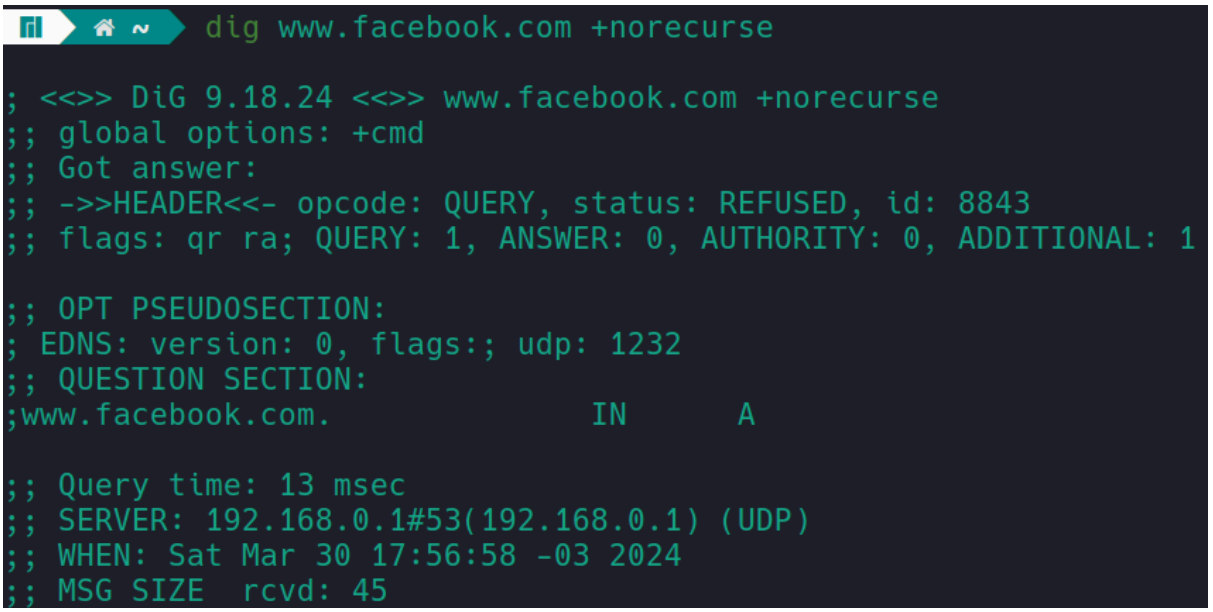
Cabe destacar que si bien esta ejecución no se realizó con el flag +recurse, la query aún así fue realizada de forma recursiva por defecto ya que su header posee los mismos flags que en la consulta original.

```
dig facebook.com

; <<>> DiG 9.18.24 <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39229
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           29      IN      A       31.13.94.35

;; Query time: 13 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Sat Mar 30 17:49:07 -03 2024
;; MSG SIZE  rcvd: 57
```

**Ejecución Iterativa:**

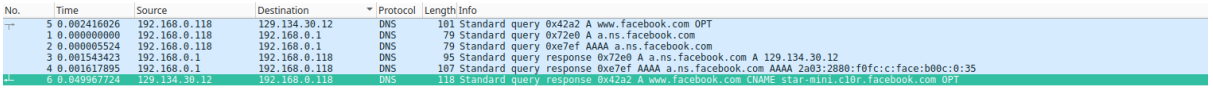
La ejecución iterativa funciona de la misma forma que la recursiva, con la salvedad de que es el cliente el que realiza las sucesivas solicitudes DNS en caso de ser necesarias. De esta forma, en caso de no tener cacheada la respuesta, cada consulta devolverá una referencia de a quien se le debe realizar la siguiente query para llegar a la respuesta.

Rápidamente se puede observar que la query falló retornando un status refused. Esto quiere decir que en alguna de las queries realizadas, el cliente no posee los permisos necesarios para llevarla a cabo de forma directa.

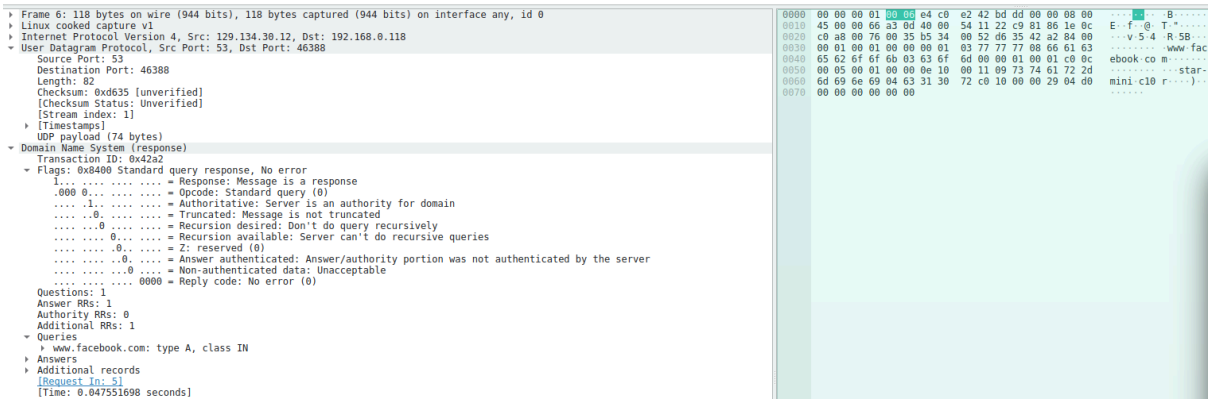



Si es un defecto se elige un servidor particular en donde realizar la búsqueda, el resultado es el esperado.

```
~ dig @a.ns.facebook.com www.facebook.com +norecurse

; <<>> DiG 9.18.24 <<>> @a.ns.facebook.com www.facebook.com +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41050
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       3600    IN      CNAME   star-mini.c10r.facebook.com.

;; Query time: 43 msec
;; SERVER: 129.134.30.12#53(a.ns.facebook.com) (UDP)
;; WHEN: Sun Mar 31 10:13:22 -03 2024
;; MSG SIZE  rcvd: 74
```



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 0.002416026 | 192.168.0.118 | 129.134.30.12 | DNS | 101 | Standard query 0x42a2 A www.facebook.com OPT |
| 1 | 0.000000000 | 192.168.0.118 | 192.168.0.1 | DNS | 79 | Standard query 0x72e0 A a.ns.facebook.com |
| 2 | 0.000005524 | 192.168.0.118 | 192.168.0.1 | DNS | 79 | Standard query 0xe7ef AAAA a.ns.facebook.com |
| 3 | 0.001543423 | 192.168.0.1 | 192.168.0.118 | DNS | 95 | Standard query response 0x72e0 A a.ns.facebook.com A 129.134.30.12 |
| 4 | 0.001617895 | 192.168.0.1 | 192.168.0.118 | DNS | 107 | Standard query response 0xe7ef AAAA a.ns.facebook.com AAAA 2a03:2880:f0fc:c:face:b00c:0:35 |
| 6 | 0.049967724 | 129.134.30.12 | 192.168.0.118 | DNS | 118 | Standard query response 0x42a2 A www.facebook.com CNAME star-mini.c10r.facebook.com OPT |



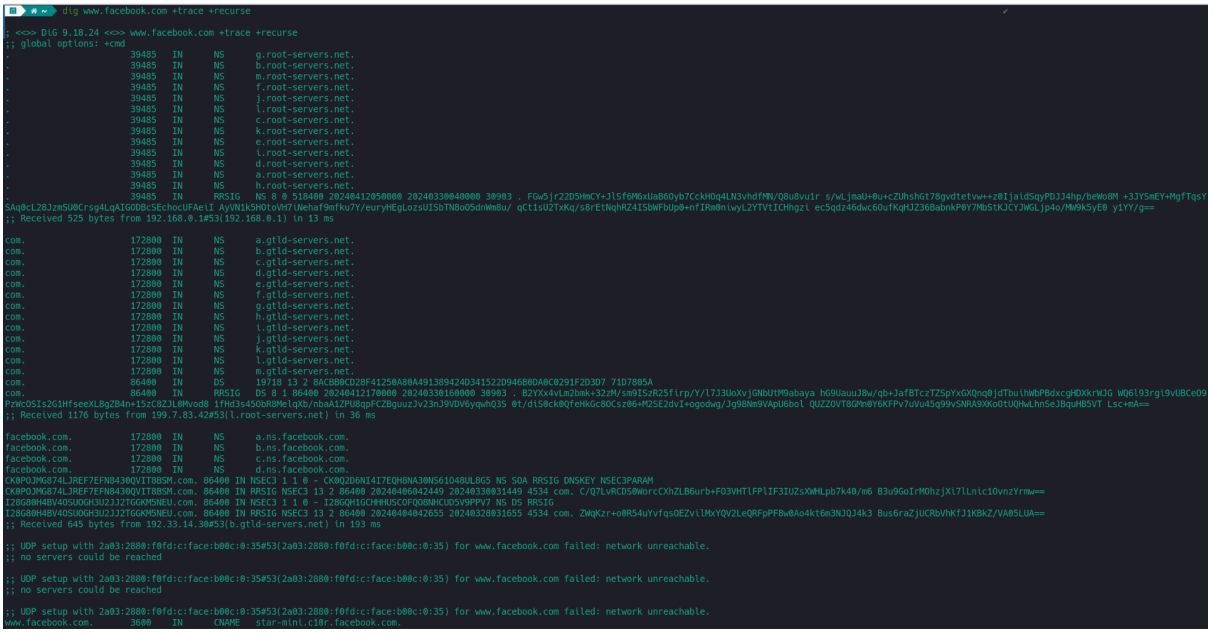
```
▸ Frame 6: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 129.134.30.12, Dst: 192.168.0.118
▾ User Datagram Protocol, Src Port: 53, Dst Port: 46388
    Source Port: 53
    Destination Port: 46388
    Length: 82
    Checksum: 0xd635 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
    UDP payload (74 bytes)
▾ Domain Name System (response)
    Transaction ID: 0x42a2
  ▾ Flags: 0x8400 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... 0... .... = Recursion available: Server can't do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.facebook.com: type A, class IN
  ▸ Answers
  ▸ Additional records
    [Request In: 5]
    [Time: 0.047551698 seconds]
```

```
0000  00 00 00 01 00 06 e4 c0  e2 42 bd dd 00 00 08 00   ·········B·····
0010  45 00 00 66 a3 0d 40 00  54 11 22 c9 81 86 1e 0c   E··f··@· T·"·····
0020  c0 a8 00 76 00 35 b5 34  00 52 d6 35 42 a2 84 00   ···v·5·4 ·R·5B···
0030  00 01 00 01 00 00 00 01  03 77 77 77 08 66 61 63   ·········www·fac
0040  65 62 6f 6f 6b 03 63 6f  6d 00 00 01 00 01 c0 0c   ebook·co m·······
0050  00 05 00 01 00 00 0e 10  00 11 09 73 74 61 72 2d   ···········star-
0060  6d 69 6e 69 04 63 31 30  72 c0 10 00 00 29 04 d0   mini·c10 r····)··
0070  00 00 00 00 00 00                                 ······
```

Como se puede observar, por la naturaleza de la consulta hecha a través de un DNS server particular (a.ns.facebook.com), a la hora de ejecutar la query en búsqueda del canonical name de www.facebook.com, primero se debe obtener la dirección IP del servidor mencionado. Es por esto que se puede observar que inmediatamente después de ser detectada la query de www.facebook.com en Wireshark, se disparan dos nuevas queries en búsqueda de un record A o AAAA de a.ns.facebook.com para poder traducir este hostname en una dirección IPv4 o IPv6.

**Ejecución Verborrágica:**

La ejecución verborrágica provee información detallada sobre la ejecución del comando, indicando el paso a paso realizado para resolver la query original.



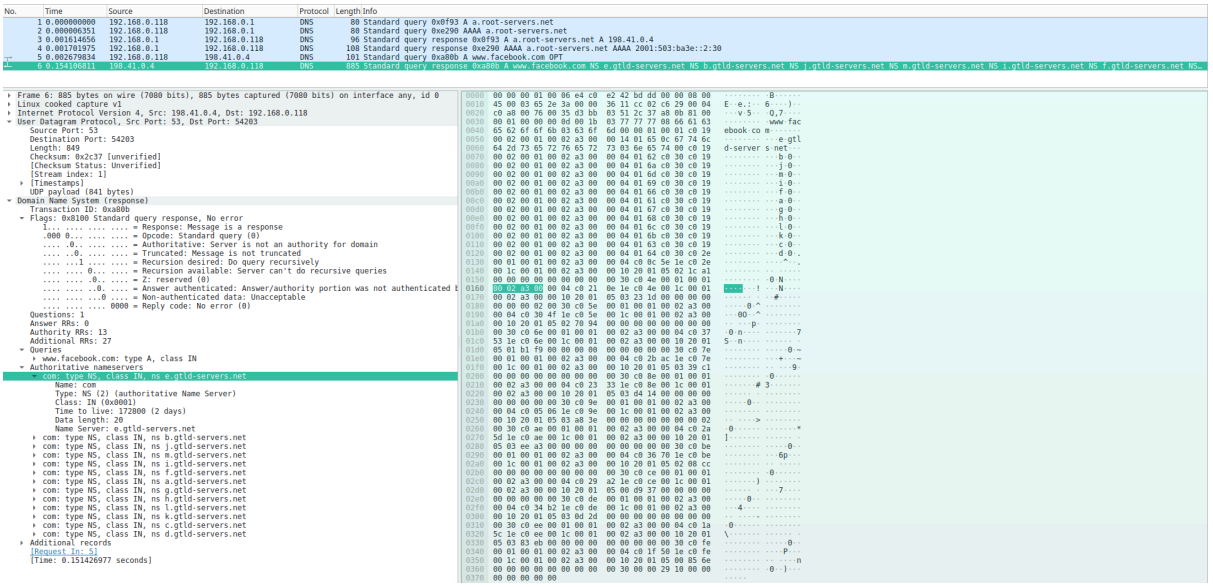

Se puede observar como primero se obtienen los distintos name servers (NS) para los servidores DNS root. A partir de estos es que se obtienen múltiples top-level domain (TLD) servers y a partir de los cuales se obtienen los authoritative servers.

Se debe notar que la respuesta obtenida es nuevamente un CNAME record ya que www.facebook.com se traduce a este canonical name y este canonical name es luego traducido a la dirección IP correspondiente, como se pudo apreciar anteriormente.

**Ejecución Autorizada:**

El flag +authority permite obtener los authoritative servers de una dirección.

```
dig @a.root-servers.net www.facebook.com +authority

; <<>> DiG 9.18.24 <<>> @a.root-servers.net www.facebook.com +authority
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43019
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; AUTHORITY SECTION:
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.

;; ADDITIONAL SECTION:
e.gtld-servers.net.     172800  IN      A       192.12.94.30
e.gtld-servers.net.     172800  IN      AAAA    2001:502:1ca1::30
b.gtld-servers.net.     172800  IN      A       192.33.14.30
b.gtld-servers.net.     172800  IN      AAAA    2001:503:231d::2:30
j.gtld-servers.net.     172800  IN      A       192.48.79.30
j.gtld-servers.net.     172800  IN      AAAA    2001:502:7094::30
m.gtld-servers.net.     172800  IN      A       192.55.83.30
m.gtld-servers.net.     172800  IN      AAAA    2001:501:b1f9::30
i.gtld-servers.net.     172800  IN      A       192.43.172.30
i.gtld-servers.net.     172800  IN      AAAA    2001:503:39c1::30
f.gtld-servers.net.     172800  IN      A       192.35.51.30
f.gtld-servers.net.     172800  IN      AAAA    2001:503:d414::30
a.gtld-servers.net.     172800  IN      A       192.5.6.30
a.gtld-servers.net.     172800  IN      AAAA    2001:503:a83e::2:30
g.gtld-servers.net.     172800  IN      A       192.42.93.30
g.gtld-servers.net.     172800  IN      AAAA    2001:503:eea3::30
h.gtld-servers.net.     172800  IN      A       192.54.112.30
h.gtld-servers.net.     172800  IN      AAAA    2001:502:8cc::30
l.gtld-servers.net.     172800  IN      A       192.41.162.30
l.gtld-servers.net.     172800  IN      AAAA    2001:500:d937::30
k.gtld-servers.net.     172800  IN      A       192.52.178.30
k.gtld-servers.net.     172800  IN      AAAA    2001:503:d2d::30
c.gtld-servers.net.     172800  IN      A       192.26.92.30
c.gtld-servers.net.     172800  IN      AAAA    2001:503:83eb::30
d.gtld-servers.net.     172800  IN      A       192.31.80.30
d.gtld-servers.net.     172800  IN      AAAA    2001:500:856e::30

;; Query time: 149 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Sun Mar 31 14:00:34 -03 2024
;; MSG SIZE  rcvd: 841
```




En este caso, se consultaron los authoritative servers de [www.facebook.com](http://www.facebook.com) dentro de a.root-servers.net. Si se realiza la misma query pero dentro de alguno de los servidores encontrados, se puede observar que se obtiene un nivel más profundo de la búsqueda del alias [www.facebook.com](http://www.facebook.com):

```
dig @a.gtld-servers.net facebook.com +authority

; <<>> DiG 9.18.24 <<>> @a.gtld-servers.net facebook.com +authority
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23159
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; AUTHORITY SECTION:
facebook.com.           172800  IN      NS      a.ns.facebook.com.
facebook.com.           172800  IN      NS      b.ns.facebook.com.
facebook.com.           172800  IN      NS      c.ns.facebook.com.
facebook.com.           172800  IN      NS      d.ns.facebook.com.

;; ADDITIONAL SECTION:
a.ns.facebook.com.      172800  IN      A       129.134.30.12
a.ns.facebook.com.      172800  IN      AAAA    2a03:2880:f0fc:c:face:b00c:0:35
b.ns.facebook.com.      172800  IN      A       129.134.31.12
b.ns.facebook.com.      172800  IN      AAAA    2a03:2880:f0fd:c:face:b00c:0:35
c.ns.facebook.com.      172800  IN      A       185.89.218.12
c.ns.facebook.com.      172800  IN      AAAA    2a03:2880:f1fc:c:face:b00c:0:35
d.ns.facebook.com.      172800  IN      A       185.89.219.12
d.ns.facebook.com.      172800  IN      AAAA    2a03:2880:f1fd:c:face:b00c:0:35

;; Query time: 166 msec
;; SERVER: 192.5.6.30#53(a.gtld-servers.net) (UDP)
;; WHEN: Sun Mar 31 14:03:47 -03 2024
;; MSG SIZE  rcvd: 284
```

Esto quiere decir que en cualquiera de los servidores encontrados, desde a.ns.facebook.com hasta d.ns.facebook.com, se puede obtener el canonical name de [www.facebook.com](http://www.facebook.com) o bien la dirección IP de facebook.com.