name resolution

John Hanley

16th May 2025

DNS lookup — a worked example

Suppose you'd like to read some news from the Guardian. What exactly happens behind the scenes when you click that link? Let's examine the details.

tl;dr

```
% host www.guardian.co.uk
www.guardian.co.uk is an alias for prod.guardian.map.fastlylb.net.
prod.guardian.map.fastlylb.net has address 151.101.201.111
```

BTW, that "alias" or "canonical name" RR, resource record, is essentially a symlink. It instructs the client to "begin again", resolving a new name; this one happens to be under `.net`.

You see a pair of name resolutions there. We will follow just the first one.

`+trace`

What follows is essentially a long way of doing this:

```
% dig +trace a www.guardian.co.uk
```

individual queries

the root servers

```
% dig +norecurs +nottl +noadd ns .

; <<>> DiG 9.10.6 <<>> +noadd +norecurs +nottl ns .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31401
;; flags: qr ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;.          IN  NS

;; ANSWER SECTION:
.           IN  NS  i.root-servers.net.
.           IN  NS  j.root-servers.net.
.           IN  NS  k.root-servers.net.
.           IN  NS  l.root-servers.net.
.           IN  NS  m.root-servers.net.
.           IN  NS  a.root-servers.net.
.           IN  NS  b.root-servers.net.
.           IN  NS  c.root-servers.net.
.           IN  NS  d.root-servers.net.
.           IN  NS  e.root-servers.net.
.           IN  NS  f.root-servers.net.
.           IN  NS  g.root-servers.net.
.           IN  NS  h.root-servers.net.

;; Query time: 96 msec
;; SERVER: 2001:558:feed::1#53(2001:558:feed::1)
;; WHEN: Fri May 16 21:47:47 PDT 2025
;; MSG SIZE  rcvd: 811
```

The "additional" RRs, not shown, listed fun facts such as:

```
m.root-servers.net. IN  A       202.12.27.33
m.root-servers.net. IN  AAAA    2001:dc3::35
```

We will need that for our next query.

```
% dig +norecurs +nottl +noadd a www.guardian.co.uk @m.root-servers.net

; <<>> DiG 9.10.6 <<>> +norecurs +nottl +noadd a www.guardian.co.uk @m.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1214
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 17

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.guardian.co.uk.    IN  A

;; AUTHORITY SECTION:
uk.          IN  NS  dns2.nic.uk.
uk.          IN  NS  nsd.nic.uk.
uk.          IN  NS  nsb.nic.uk.
uk.          IN  NS  nsa.nic.uk.
uk.          IN  NS  nsc.nic.uk.
uk.          IN  NS  dns3.nic.uk.
uk.          IN  NS  dns4.nic.uk.
uk.          IN  NS  dns1.nic.uk.

;; Query time: 22 msec
;; SERVER: 2001:dc3::35#53(2001:dc3::35)
;; WHEN: Fri May 16 21:53:13 PDT 2025
;; MSG SIZE  rcvd: 555
```

Notice that we got zero "answer" RRs. As a consolation prize we got a referral, over to those 8 British nameservers. The root knows those 8 are authoritative for `uk`.

country TLD

Britain has a top level domain. Let's try our luck there, with "nameserver A".

```
% dig +norecurs +nottl +noadd a www.guardian.co.uk @nsa.nic.uk

; <<>> DiG 9.10.6 <<>> +norecurs +nottl +noadd a www.guardian.co.uk @nsa.nic.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38100
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.guardian.co.uk.    IN  A

;; AUTHORITY SECTION:
guardian.co.uk.     IN  NS  dns2.p02.nsone.net.
guardian.co.uk.     IN  NS  ns01.theguardiandns.com.
guardian.co.uk.     IN  NS  dns4.p02.nsone.net.
guardian.co.uk.     IN  NS  ns02.theguardiandns.com.
guardian.co.uk.     IN  NS  dns3.p02.nsone.net.
guardian.co.uk.     IN  NS  ns03.theguardiandns.com.
guardian.co.uk.     IN  NS  ns04.theguardiandns.com.
guardian.co.uk.     IN  NS  dns1.p02.nsone.net.

;; Query time: 20 msec
;; SERVER: 2001:502:ad09::3#53(2001:502:ad09::3)
;; WHEN: Fri May 16 21:54:53 PDT 2025
;; MSG SIZE  rcvd: 230
```

Ooohhh, we're getting closer already!

Notice there is no zone cut between `co` and `uk`. So nameserver A didn't have to refer us to some random collection of `co` nameservers, since nameserver A is omniscient about everything down at that level, too. That's why resolving clients usually send the full name to each nameserver, just in case we get lucky, as we did here.

Well, I lied slightly. A zone cut is defined by the presence of an SOA record and an NS set. It happens that we **do** find those at both `uk` and `co.uk`. However, the 8 nameservers in both are identical, so the effect is they're all omniscient about both levels, and can offer a good answer without client needing to suffer an extra WAN roundtrip delay.

corporate level

Let's ask nameserver 4 over at the Guardian.

```
% dig +norecurs +nottl +noadd a www.guardian.co.uk @ns04.theguardiandns.com

; <<>> DiG 9.10.6 <<>> +norecurs +nottl +noadd a www.guardian.co.uk @ns04.theguardiandns.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5175
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.guardian.co.uk.    IN  A

;; ANSWER SECTION:
www.guardian.co.uk. IN  CNAME   prod.guardian.map.fastlylb.net.

;; Query time: 66 msec
;; SERVER: 45.54.51.193#53(45.54.51.193)
;; WHEN: Fri May 16 22:01:14 PDT 2025
;; MSG SIZE  rcvd: 91
```

Bingo! That's our answer. Well, kind of. The query specified, "gimme an A record", an address record. But all we got was a CNAME pointing to another part of the DNS graph. So now the client gets to start over, hoping the Fastly CDN can resolve *that* name to an A record.

As we saw at the start of this, yes it can. It works out to 151.101.201.111, which a browser can then use when making a TCP connection to https port number 443.