List DNS records, nameservers of a domain from command line

Article Number: 392 | Rating: Unrated | Last Updated: Sun, Sep 30, 2018 10:04 PM

List DNS records, nameservers of a domain from command line

If you want to find out domains DNS records like TXT, CNAME, MX, A or nameservers for the domain, there are numerous CLI tools for this task, I will show you two built in Ubuntu.

The easiest way is to use **host** command with -a option.

```
$ host -a google.com
```

Trying "google.com"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20315

;; flags: qr rd ra; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:

;google.com. IN ANY

;; ANSWER SECTION:

google.com. 82014 IN NS ns3.google.com.

google.com. 90 IN A 173.194.69.113

google.com. 144 IN MX 40 alt3.aspmx.l.google.com.

google.com. 90 IN A 173.194.69.100

google.com. 90 IN A 173.194.69.102

google.com. 144 IN MX 30 alt2.aspmx.l.google.com.

google.com. 82014 IN NS ns1.google.com.

google.com. 144 IN MX 20 alt1.aspmx.l.google.com.

google.com. 90 IN A 173.194.69.139

google.com. 144 IN MX 10 aspmx.l.google.com.

google.com. 90 IN A 173.194.69.101

google.com. 144 IN MX 50 alt4.aspmx.l.google.com.

google.com. 1478 IN TXT "v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all"

google.com. 82014 IN NS ns2.google.com.

google.com. 275 IN AAAA 2a00:1450:4008:c01::71

google.com. 31 IN SOA ns1.google.com. dns-admin.google.com. 1516687 7200 1800 1209600 300

google.com. 90 IN A 173.194.69.138

google.com. 82014 IN NS ns4.google.com.

;; ADDITIONAL SECTION:

alt3.aspmx.l.google.com. 208 IN A 74.125.142.27

alt4.aspmx.l.google.com. 208 IN A 74.125.134.27

Received 498 bytes from 192.168.0.1#53 in 12 ms

The second option is to use nslookup command with -type parameter. Change mx to a, or txt and see for your self.

```
$ nslookup -type=mx google.com


Server: 192.168.0.1

Address: 192.168.0.1#53


Non-authoritative answer:

google.com mail exchanger = 40 alt3.aspmx.l.google.com.

google.com mail exchanger = 50 alt4.aspmx.l.google.com.

google.com mail exchanger = 30 alt2.aspmx.l.google.com.

google.com mail exchanger = 20 alt1.aspmx.l.google.com.

google.com mail exchanger = 10 aspmx.l.google.com.


Authoritative answers can be found from:

alt3.aspmx.l.google.com internet address = 74.125.142.27

alt2.aspmx.l.google.com internet address = 173.194.64.27

aspmx.l.google.com internet address = 173.194.69.27

alt4.aspmx.l.google.com internet address = 74.125.134.27

alt1.aspmx.l.google.com internet address = 74.125.141.27
```

A very interesting command line tool you should also check out is **dig**.