## Syntax

dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-x addr] [-y [hmac:]name:key] [-4] [-6] [name] [type] [class] [query-opt...]

## Config

| Tired of always typing the same options ? Create a Run Control file for dig. | `vi $HOME/.digrc` |
|---|---|
| $ cat $HOME/.digrc +noall +answer | |

## List specific types of RRs (Resource Records)

| List address records | `dig -t A tme520.net` |
|---|---|
| List aliases | `dig -t CNAME tme520.net` |
| Find who manages a domain | `dig -t SOA tme520.net` |
| List mail servers | `dig tme520.net MX` |
| List name servers | `dig tme520.net NS` |
| List any type of Resource Record | `dig tme520.net ANY` |

There are about 40 DNS Resources Records types, but you only have to know 5 of them:

- **A** : Address record (IPv4); AAAA for IPv6,
- **CNAME** : Canonical Name. Aliases to A or AAAA records,
- **SOA** : Start Of Authority: primary name server, email of the domain admin, domain serial number, and timers relating to refreshing the zone,
- **MX** : Mail eXchange. Points to a mail server,
- **NS** : Name Server (a DNS).

## Output sections (cont)

| QUESTION | This is your input, the question that has been asked to the DNS. |
|---|---|
| ANSWER | The 2nd field is the time in seconds that the record may be cached (0 = don't cache), the 3rd field is the class (Internet (IN), Chaos (CH), Hesiod (HS)...), the 4th is the type (A, NS, CNAME, MX...) and the 5th, the IP. |
| AUTHORITY | This section contains the DNS name server that has the authority to answer your query (type: NS, Name Server). |
| ADDITIONAL | The additional section carries Resource Records related to the RRs from the other sections. |
| STATISTICS | Displays the time it took to get an answer, the IP of the DNS server used, the date and size of the message. |

If you ever get confused about whether or not *dig* found any result for your query, check the ANSWER field from the header; if it's at 0, your query returned no proper answer.

## Batch mode: multiple queries in one go

| Using a list | `dig -f names.list` |
|---|---|
| Using several arguments | `dig centos.org MX +noall +answer suckless.org ANY +short` |

Batch mode takes a filename as input; the file must be plain text and contain one domain per line:

```
$ cat names.list

redhat.com
ubuntu.com
perdu.com
```

## Make that DNS talk !

| Display only the ANSWER section | `dig opensuse.org +noallr` |
|---|---|
| Activate the short output | `dig perdu.com +short` |
| Reverse DNS (get name from IP) | `dig -x 208.97.17 7.124` |
| Use a specific DNS server | `dig @8.8.4.4 redhat.com` |
| Display the name resolution path | `dig google.com +trace` |
| Request a zone transfer | `dig micros oft.com AXFR` |

A zone transfer is a mechanism allowing an administrator to replicate DNS databases across a set of DNS servers. There are two methods: full (aka AXFR) and incremental (aka IXFR). Zone transfers were often used by people wanting to retrieve a list of all the Resource Records of a DNS server. Nowadays, most servers will refuse your request, mostly for security reasons.

## Output sections

| | |
|---|---|
| HEADER | Displays the dig command version, the global options used, the type of operation (opcode), the status of the operation (NOERROR) and the message id (necessary to match responses to queries). |

By **TME520** (TME520)

cheatography.com/tme520/

tme520.com