dig cheat sheet

The dig queries I actually use for DNS migrations and mail issues – searchable and copyable in one click.

daniele.michelin // cheat sheet

Basic lookups

Query the IPv4 address (A record)

```
dig example.com A
```

Query the IPv6 address (AAAA record)

```
dig example.com AAAA
```

Show mail servers with priority

```
dig example.com MX +short
```

All TXT records (SPF, verifications)

```
dig example.com TXT +short
```

Nameservers responsible for the zone

```
dig example.com NS +short
```

SOA with serial number (check zone changes)

```
dig example.com SOA +short
```

CAA: which CAs may issue certificates

```
dig example.com CAA +short
```

Show the CNAME target of a hostname

```
dig www.example.com CNAME +short
```

Print only the answer section incl. TTL

```
dig +noall +answer example.com
```

Resolvers & nameservers

Query through a specific resolver (Cloudflare)

```
dig @1.1.1.1 example.com A +short
```

Ask the authoritative nameserver directly (no cache)

```
dig @ns1.example.com example.com A +norecurse
```

Follow the delegation from the root zone

```
dig +trace example.com
```

Compare answers from several public resolvers

```
for r in 1.1.1.1 8.8.8.8 9.9.9.9; do echo "$r: $(dig +short @$r example.com A)"; done
```

Check the remaining TTL in the resolver cache

```
dig @1.1.1.1 +noall +answer example.com A
```

Force the query over TCP instead of UDP

```
dig +tcp example.com A
```

Send the query over IPv6 transport

```
dig -6 @2606:4700:4700::1111 example.com A
```

Mail: SPF, DKIM, DMARC, PTR

Filter out the SPF record

```
dig example.com TXT +short | grep spf1
```

Query the DMARC policy

```
dig _dmarc.example.com TXT +short
```

Query the DKIM public key for a selector

```
dig SELECTOR._domainkey.example.com TXT +short
```

Reverse lookup (PTR) of an IPv4 address

```
dig -x 203.0.113.10 +short
```

Reverse lookup (PTR) of an IPv6 address

```
dig -x 2001:db8::1 +short
```

Query an SRV record (e.g. mail autoconfig)

```
dig _submission._tcp.example.com SRV +short
```

DNSSEC

Show the answer with RRSIG signatures

```
dig example.com A +dnssec +multi
```

Query the zone's DNSKEY records

```
dig example.com DNSKEY +short
```

Check the DS record in the parent zone

```
dig example.com DS +short
```

Check validation: ad flag = DNSSEC valid

```
dig @1.1.1.1 example.com A +dnssec | grep flags
```

Query with validation disabled (isolate SERVFAIL)

```
dig @1.1.1.1 example.com A +cd
```

Zones & advanced

! Attempt a zone transfer (should be REFUSED for outsiders)

```
dig @ns1.example.com example.com AXFR
```

Show the nameserver ID (identify anycast node)

```
dig @ns1.example.com example.com SOA +nsid
```

Run queries in batch from a file

```
dig -f hosts.txt +noall +answer
```