dig DNS lookups

CONCEPTS

dig talks to the DNS server directly and ignores /etc/hosts, so it can differ from what your applications resolve.

Your machine dig
↓ query
Resolver @server or resolv.conf
↓ +trace skips it
Root / TLD delegations
↓ refers to
Authoritative the final answer

Options starting with + change a query; options starting with - change dig itself. Order is free: name, type and @server may come anywhere.

BASIC QUERIES

`dig <name>`
Query A records

`dig <name> <type>`
Query a record type

`dig <name> AAAA`
IPv6 address

`dig <name> MX`
Mail servers

`dig <name> NS`
Name servers of a zone

`dig <name> TXT`
Text records (SPF, verification)

`dig <name> CNAME`
Alias target

`dig <name> SOA`
Zone start of authority and serial

CHOOSE THE SERVER

`dig @<server> <name>`
Ask this resolver or server

`dig @1.1.1.1 <name>`
Use a public resolver

CHOOSE THE SERVER (cont.)

`dig @<ns> <name> +norecurse`
Ask without recursion

`dig +tcp <name>`
Query over TCP

OUTPUT CONTROL

`dig +short <name>`
Print only the answer data

`dig +noall +answer <name>`
Answer section only, with TTLs

`dig +noall +answer +ttlunits <name>`
TTLs as 1h30m style

REVERSE AND TRACING

`dig -x <ip>`
Reverse (PTR) lookup

`dig +trace <name>`
Walk from the root servers down

BATCH AND CONFIG

`dig -f <file>`
Run lookups listed in a file

READING THE OUTPUT

Header flags

Item	Meaning
`status: NOERROR`	Query succeeded (answer may be empty)
`status: NXDOMAIN`	Name does not exist
`status: SERVFAIL`	Server could not answer
`status: REFUSED`	Server will not answer you
`flags: qr`	This is a response
`flags: aa`	Authoritative answer
`flags: rd ra`	Recursion asked / available
`flags: ad`	DNSSEC validated
`flags: tc`	Truncated, retry over TCP

NOERROR with an empty answer means the name exists but has no record of that type. NXDOMAIN means the name does not exist at all.