DIG Command: Complete Guide for Cybersecurity and DNS Analysis

> **Tool:** `dig` – Domain Information Groper\ **Platform:** Kali Linux / Linux-based OS\ **Category:** DNS Investigation, Networking, Enumeration\ **Usage:** DNS record lookup, enumeration, debugging DNS configurations, testing name servers, zone transfers.

📌1. Introduction

`dig` is a command-line utility used to query Domain Name System (DNS) servers. It provides detailed answers about DNS queries and is especially useful for penetration testers, network engineers, and system administrators.

🔗Why use `dig`?

- Lightweight and flexible
- Easily scriptable
- Offers granular control over queries
- Preferred in recon and DNS enumeration phases

🧱2. Basic Syntax of `dig`

```
dig [@server] [name] [type] [class] [q-options] [global-options]
```

🕑Explanation of Parameters:

Parameter	Description	Example
`@server`	DNS server to use (e.g., @8.8.8.8)	`@1.1.1.1`
`name`	Domain to query	`example.com`
`type`	Record type (A, MX, TXT, CNAME, etc.)	`A`, `MX`, `TXT`
`class`	DNS class (default: IN for Internet)	`IN`
`q-options`	Options affecting query behavior	`-t`, `-x`, `-4`
`global-options`	Display/output formatting options	`+short`, `+trace`

🧪 3. Common Query Types with Examples

🕰️ A Record (IPv4 Address)

```
dig example.com
```

🕰️ MX Record (Mail Exchange)

```
dig example.com -t MX
```

🕰️ TXT Records (SPF, DMARC, etc.)

```
dig google.com -t TXT
```

🕰️ CNAME (Canonical Name)

```
dig www.example.com -t CNAME
```

🕰️ NS (Nameservers)

```
dig example.com -t NS
```

🕰️ SOA (Start of Authority)

```
dig example.com -t SOA
```

🕰️ AAAA (IPv6 Address)

```
dig example.com -t AAAA
```

🕰️ PTR (Reverse Lookup)

```
dig -x 8.8.8.8
```

🛠️4. Advanced Query Options (`q-opt`)

Option	Description	Example
`-4`	Force use of IPv4 transport	`dig -4 example.com`
`-6`	Force use of IPv6 transport	`dig -6 example.com`
`-b IP[#port]`	Bind to specific source IP and port	`dig -b 192.168.1.5#5353 domain.com`
`-c class`	Set query class (usually IN)	`dig -c IN example.com`
`-f file`	Batch query domains listed in a file	`dig -f domains.txt`
`-k file`	Use TSIG key for authentication	`dig -k tsig.key example.com`
`-m`	Memory debugging output (rarely used)	
`-p port`	Set DNS server port	`dig -p 5353 example.com`
`-q name`	Set query name explicitly	`dig -q google.com`
`-t type`	Set record type	`dig -t MX gmail.com`
`-u`	Microsecond timing output	`dig -u example.com`
`-x addr`	Simplified reverse lookup	`dig -x 8.8.8.8`
`-y`	Use TSIG key (inline or from file)	See secure update examples
`-z`	Perform zone transfer (AXFR/IXFR)	`dig @ns1.example.com example.com AXFR`

🖥️5. Global and Local Display Options (`+options`)

Option	Description
`+short`	Minimal output, shows only answers
`+stats`	Show query statistics
`+nocomments`	Hide comments in output
`+nocmd`	Suppress command line echo
`+noquestion`	Hide question section
`+noanswer`	Hide answer section
`+noauthority`	Hide authority section

Option	Description
`+noadditional`	Hide additional section
`+trace`	Follow DNS resolution from root to target
`+dnssec`	Request DNSSEC information
`+multiline`	Print answers in structured format
`+ttlid`	Include TTL for each record
`+nssearch`	Query authoritative name servers
`+recurse`	Enable recursive query (default)
`+norecurse`	Disable recursion
`+search`	Use `resolv.conf` search list
`+defname`	Use default domain name (from `resolv.conf`)
`+subnet`	Send EDNS0 client subnet info

---

6. Real-World Use Cases

🔗Trace Full DNS Path

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

Shows how DNS is resolved from root nameservers to the domain.

🔗Find Authoritative Name Servers

```
dig example.com NS
```

🔗Zone Transfer Attempt (Ethical Use Only)

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

May return full zone data if misconfigured.

🔗Batch Lookup

```
cat domains.txt | xargs -n1 dig +short
```

Script-friendly DNS resolution for multiple domains.

🔗Lookup with Custom DNS and Port

```
dig @8.8.8.8 -p 5353 example.com
```

📚7. Additional Resources (for Further Notes)

- man dig
- `dnsutils` package documentation
- Wireshark DNS filter examples: `dns.qry.name == "example.com"`
- Online Tool: https://toolbox.googleapps.com/apps/dig/

🗒️8. Add Your Own Notes Here (For Expansion)

🔍Record Type Details:

- **A** – IPv4 address
- **AAAA** – IPv6 address
- **MX** – Mail server
- **NS** – Name server
- **CNAME** – Canonical name (alias)
- **TXT** – Text records (SPF, DMARC)

📌DNSSEC Concepts:

- RRSIG
- DNSKEY
- NSEC/NSEC3
- DS record

📌TSIG Authentication:

- Format: `hmac-sha256:name:key`
- Base64-encoded key via `tsig-keygen`

🧪 Testing Local DNS Server:

```
dig @127.0.0.1 -p 53 example.com +short
```

Last updated: August 1, 2025\ Created by: Muhammad Naveed Ul Hassan (Cybersotz)