

DIG COMMAND

TOOL: KALI LINUX

EXAMPLE: GOOGLE.COM

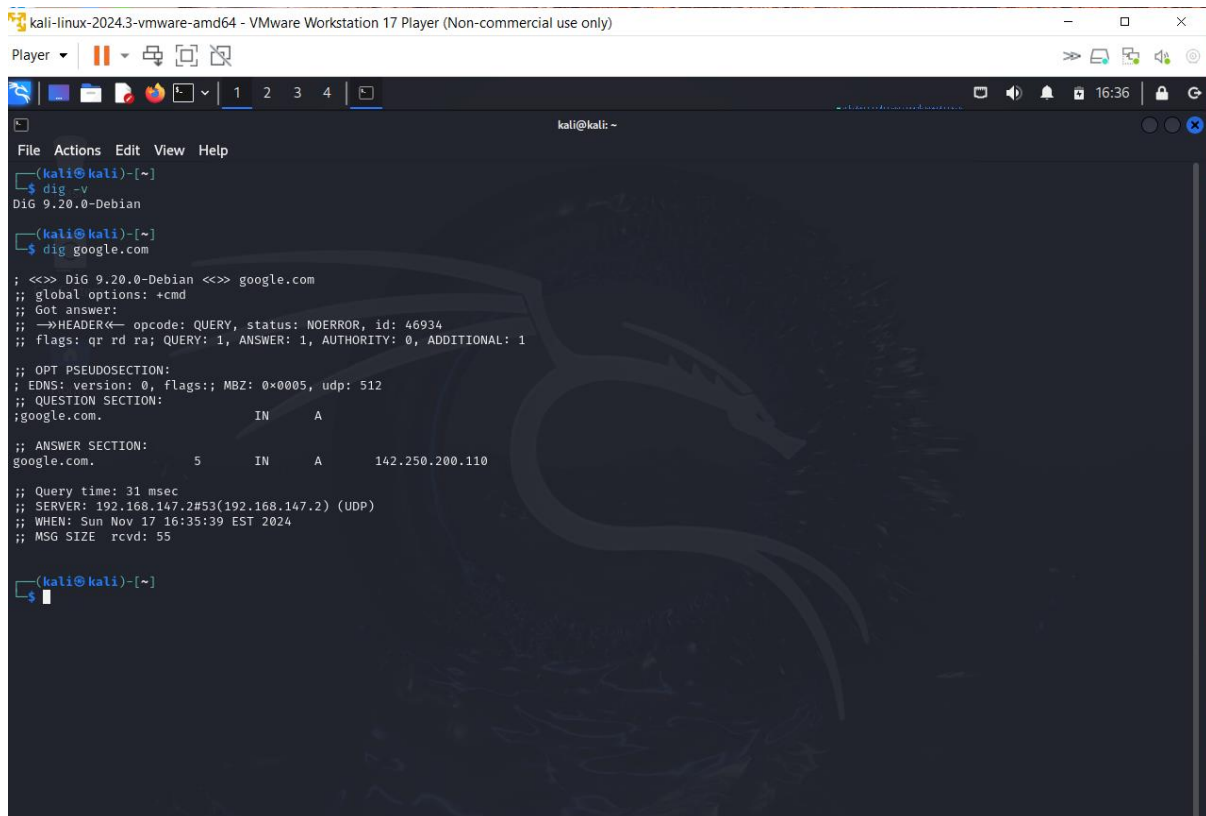
The dig command (domain information groper) is a network administration command-line tool used for querying Domain Name System (DNS) servers. It performs DNS lookups and displays the answers that are returned from the queried name servers.

It is often used for troubleshooting DNS issues or gathering DNS information about a domain.

Basic Syntax

```
dig [@server] [domain] [type]
```

- @server: The DNS server to query
- domain: The domain name to query.
- type: The type of DNS record to look up (optional; defaults to A for IPv4 address).



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali ~  
$ dig -v  
Dig 9.20.0-Debian  
kali@kali ~  
$ dig google.com  
  
;<<<> Dig 9.20.0-Debian <<> google.com  
;; global options: +cmd  
;; Got answer:  
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 46934  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags: MBZ: 0x0005, udp: 512  
;; QUESTION SECTION:  
;google.com. IN A  
  
;; ANSWER SECTION:  
google.com. 5 IN A 142.250.200.110  
  
;; Query time: 31 msec  
;; SERVER: 192.168.147.2#53(192.168.147.2) (UDP)  
;; WHEN: Sun Nov 17 16:35:39 EST 2024  
;; MSG SIZE rcvd: 55  
kali@kali ~  
$
```

Common Use Cases

1. Basic DNS Lookup (A Record)

```
dig example.com
```

This queries the A record for `example.com` (IPv4 address).

2. Lookup Specific DNS Record Types

- **A Record (IPv4 address)**

```
dig example.com A
```

- **AAAA Record (IPv6 address)**

```
dig example.com AAAA
```

- **MX Record (Mail Exchange server)**

```
dig example.com MX
```

- **NS Record (Name Server)**

```
dig example.com NS
```

- **TXT Record (Text data)**

```
dig example.com TXT
```

3. Query a Specific DNS Server

```
dig @8.8.8.8 example.com
```

This queries the 8.8.8.8 Google DNS server for `example.com`.

4. Get Full Output (Verbose)

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

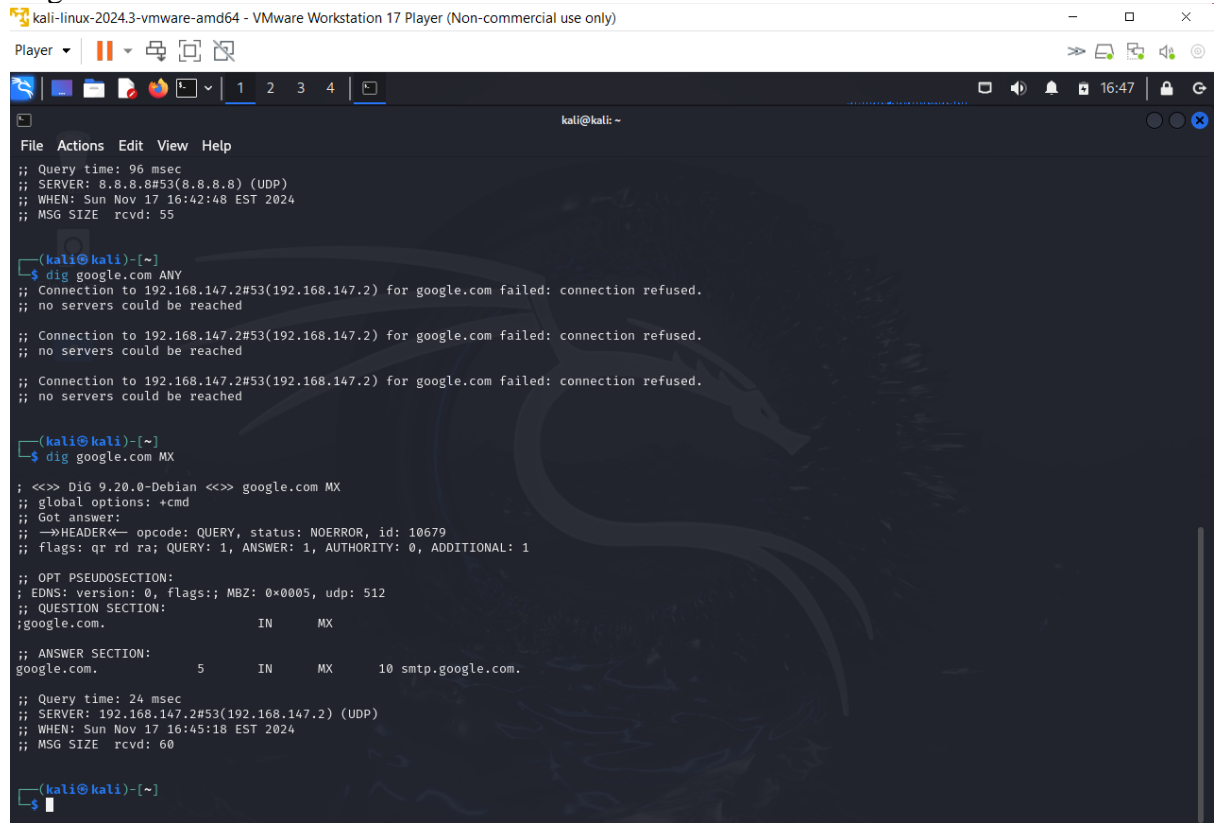
This gives just the answer section (reducing unnecessary information).

5. Reverse DNS Lookup

Reverse DNS lookups are done by querying PTR records for an IP address:

```
dig -x 8.8.8.8
```

6. **Querying for Multiple Record Types** You can query multiple record types in a single command:



The screenshot shows a terminal window titled "kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)". The terminal output shows the results of a dig query for google.com. The first query is for google.com ANY, which fails with a connection refused error. The second query is for google.com MX, which succeeds and shows the MX record for google.com.

```
kali@kali: ~  
File Actions Edit View Help  
;; Query time: 96 msec  
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)  
;; WHEN: Sun Nov 17 16:42:48 EST 2024  
;; MSG SIZE rcvd: 55  
  
(kali@kali)-[~]  
$ dig google.com ANY  
;; Connection to 192.168.147.2#53(192.168.147.2) for google.com failed: connection refused.  
;; no servers could be reached  
  
;; Connection to 192.168.147.2#53(192.168.147.2) for google.com failed: connection refused.  
;; no servers could be reached  
  
;; Connection to 192.168.147.2#53(192.168.147.2) for google.com failed: connection refused.  
;; no servers could be reached  
  
(kali@kali)-[~]  
$ dig google.com MX  
  
; <<> DiG 9.20.0-Debian <<> google.com MX  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 10679  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags: MBZ: 0x0005, udp: 512  
;; QUESTION SECTION:  
;google.com. IN MX  
  
;; ANSWER SECTION:  
google.com. 5 IN MX 10 smtp.google.com.  
  
;; Query time: 24 msec  
;; SERVER: 192.168.147.2#53(192.168.147.2) (UDP)  
;; WHEN: Sun Nov 17 16:45:18 EST 2024  
;; MSG SIZE rcvd: 60  
  
(kali@kali)-[~]  
$
```

7.

```
dig example.com A MX
```

```
kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
;; Query time: 96 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Nov 17 16:42:48 EST 2024
;; MSG SIZE rcvd: 55

(kali@kali)-[~]
$ dig google.com ANY
;; Connection to 192.168.147.2#53(192.168.147.2) for google.com failed: connection refused.
;; no servers could be reached

;; Connection to 192.168.147.2#53(192.168.147.2) for google.com failed: connection refused.
;; no servers could be reached

;; Connection to 192.168.147.2#53(192.168.147.2) for google.com failed: connection refused.
;; no servers could be reached

(kali@kali)-[~]
$ dig google.com MX
; <<>> DiG 9.20.0-Debian <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 10679
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;google.com.                IN      MX

;; ANSWER SECTION:
google.com.                5      IN      MX      10 smtp.google.com.

;; Query time: 24 msec
;; SERVER: 192.168.147.2#53(192.168.147.2) (UDP)
;; WHEN: Sun Nov 17 16:45:18 EST 2024
;; MSG SIZE rcvd: 60

(kali@kali)-[~]
$
```

```
kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
;; UDP setup with 2620:1ec:8ec:10::27#53(2620:1ec:8ec:10::27) for microsoft.com failed: network unreachable.
;; no servers could be reached

;; UDP setup with 2620:1ec:8ec:10::27#53(2620:1ec:8ec:10::27) for microsoft.com failed: network unreachable.
A 20.112.250.133 from server 13.107.206.39 in 128 ms.
A 20.231.239.246 from server 13.107.206.39 in 128 ms.
A 20.76.201.171 from server 13.107.206.39 in 128 ms.
A 20.70.246.20 from server 13.107.206.39 in 128 ms.
A 20.236.44.162 from server 13.107.206.39 in 128 ms.

(kali@kali)-[~]
$ dig -x 142.250.200.110
; <<>> DiG 9.20.0-Debian <<>> -x 142.250.200.110
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 38545
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;110.200.250.142.in-addr.arpa. IN      PTR

;; ANSWER SECTION:
110.200.250.142.in-addr.arpa. 5 IN      PTR      mad41s13-in-f14.1e100.net.

;; Query time: 40 msec
;; SERVER: 192.168.147.2#53(192.168.147.2) (UDP)
;; WHEN: Sun Nov 17 16:57:25 EST 2024
;; MSG SIZE rcvd: 96

(kali@kali)-[~]
$ dig +short TXT hackaday.com
"projects google-site-verification=RjppnbZuuM-LhJ6Xb1EG0vnZeM6xvkkMxBxGmOm7ekQ"
"facebook-domain-verification=iellkz19o2lsbploq4owagf1snbzy"
"v=spf1 include:aspmx.googlemail.com include:mailer.postageapp.com include:mailgun.org include:servers.mcsv.net ~all"
"google-site-verification=LXv4FJCKt039C05Cy0mMT4j9zLRBWS03GIcV4x-10g"
"ZOOM_verify_cuYAVoeSBi4AAVJQvMu-A"
```