Dig Command in Linux

The **dig** (domain information groper) command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s). Most DNS administrators use the dig command to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output.
Although dig is normally used with command-line arguments, it also has a batch mode for reading lookup requests from a file.

Flags: -

1. **Dig:** It is a Linux networking utility used for querying DNS servers to retrieve information about domain

names and DNS records.

2. **+short:** The "+short" switch in the dig command is used to provide a concise output, typically returning only the resolved IP address(es) without additional information such as the query time, DNS server used, or other details.

3. **+nocomments:** The "+nocomments" option in the **dig** command instructs it to suppress comment lines from the output, providing a cleaner result without any

commentary.

```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com +nocomments

; <<>> DiG 9.19.21-1-Debian <<>> google.com +nocomments
;; global options: +cmd
;google.com.                    IN      A
google.com.             18      IN      A       142.250.194.14
;; Query time: 7 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed May 01 19:10:21 EDT 2024
;; MSG SIZE  rcvd: 55
```

4. **+noall:** The "+noall" option in the dig command tells it not to print all the section headers in the output, displaying only the relevant information.

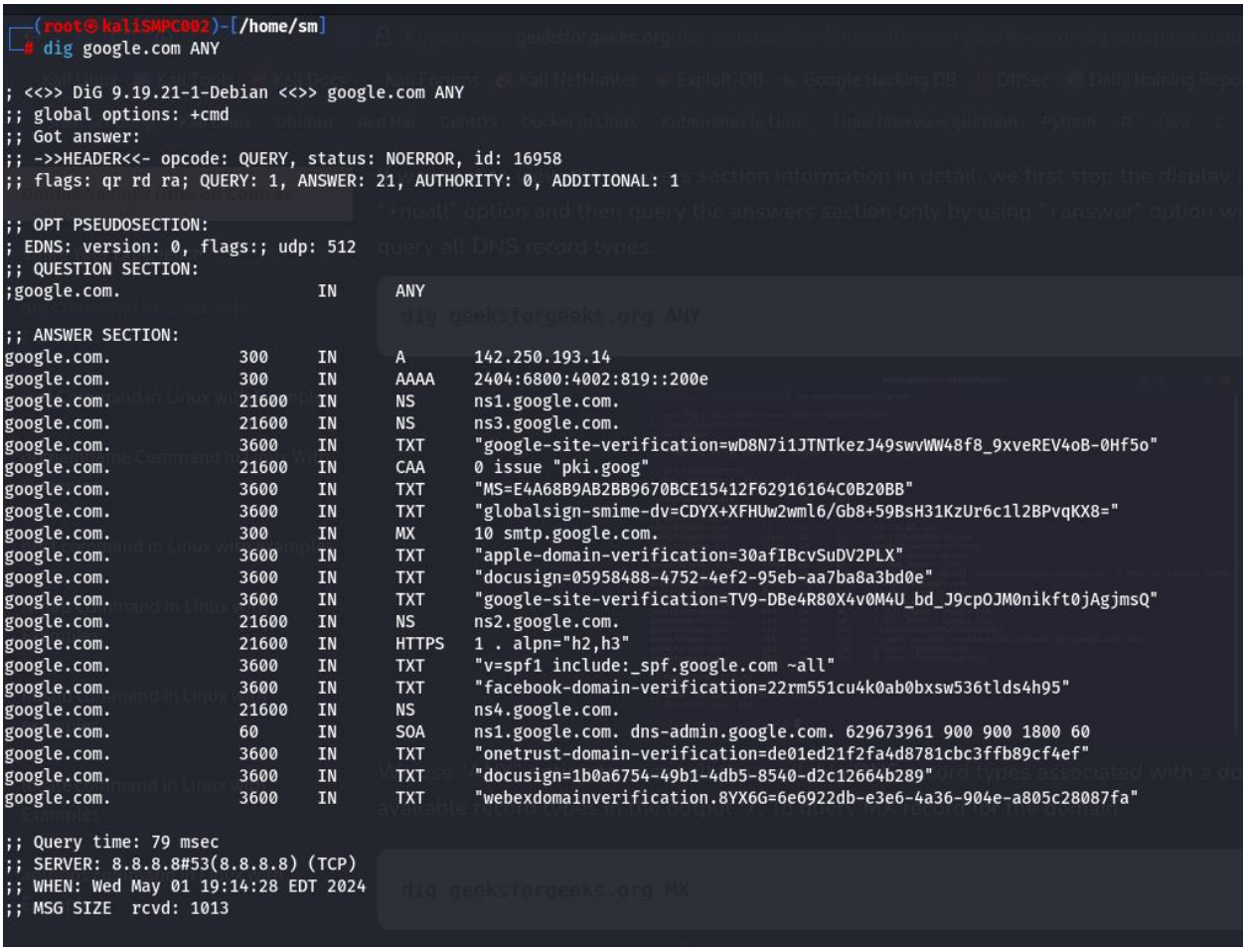
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com +noall

┌──(root㉿kaliSMPC002)-[/home/sm]
└─#
```

5. **+noall +answer:** The "+noall +answer" options in the dig command specify to only display the answer section of the DNS query response, omitting any additional sections such as authority or additional records.

```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com +noall +answer
google.com.             235     IN      A       142.250.193.238
```

6. **ANY:** If you use just "any" with dig, it will retrieve all records, including but not limited to A, AAAA, MX, NS, and TXT records associated with the queried domain.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com ANY

; <<>> DiG 9.19.21-1-Debian <<>> google.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16958
;; flags: qr rd ra; QUERY: 1, ANSWER: 21, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.com.             300     IN      A       142.250.193.14
google.com.             300     IN      AAAA    2404:6800:4002:819::200e
google.com.             21600   IN      NS      ns1.google.com.
google.com.             21600   IN      NS      ns3.google.com.
google.com.             3600    IN      TXT     "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com.             21600   IN      CAA     0 issue "pki.goog"
google.com.             3600    IN      TXT     "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com.             3600    IN      TXT     "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com.             300     IN      MX      10 smtp.google.com.
google.com.             3600    IN      TXT     "apple-domain-verification=30afIBcvSuDV2PLX"
google.com.             3600    IN      TXT     "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com.             3600    IN      TXT     "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com.             21600   IN      NS      ns2.google.com.
google.com.             21600   IN      HTTPS   1 . alpn="h2,h3"
google.com.             3600    IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.             3600    IN      TXT     "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com.             21600   IN      NS      ns4.google.com.
google.com.             60      IN      SOA     ns1.google.com. dns-admin.google.com. 629673961 900 900 1800 60
google.com.             3600    IN      TXT     "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com.             3600    IN      TXT     "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com.             3600    IN      TXT     "webexdomainverification.8YX6G=6e6922db-e3e6-4a36-904e-a805c28087fa"

;; Query time: 79 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (TCP)
;; WHEN: Wed May 01 19:14:28 EDT 2024
;; MSG SIZE  rcvd: 1013
```

7. **MX:** If you use "mx" with dig, it will specifically query and retrieve the Mail Exchange (MX) records associated with the domain. These records specify the mail servers responsible for receiving email for the domain.

```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com MX

; <<>> DiG 9.19.21-1-Debian <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47036
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.com.             220     IN      MX      10 smtp.google.com.

;; Query time: 7 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed May 01 19:15:12 EDT 2024
;; MSG SIZE  rcvd: 60
```

8. **+trace:** If you use "trace" with dig, it performs a trace of the DNS lookup, showing the full resolution path from the root DNS servers down to the authoritative name servers for the queried domain.

```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com +trace

; <<>> DiG 9.19.21-1-Debian <<>> google.com +trace
;; global options: +cmd
.                       87203   IN      NS      a.root-servers.net.
.                       87203   IN      NS      b.root-servers.net.
.                       87203   IN      NS      c.root-servers.net.
.                       87203   IN      NS      d.root-servers.net.
.                       87203   IN      NS      e.root-servers.net.
.                       87203   IN      NS      f.root-servers.net.
.                       87203   IN      NS      g.root-servers.net.
.                       87203   IN      NS      h.root-servers.net.
.                       87203   IN      NS      i.root-servers.net.
.                       87203   IN      NS      j.root-servers.net.
.                       87203   IN      NS      k.root-servers.net.
.                       87203   IN      NS      l.root-servers.net.
.                       87203   IN      NS      m.root-servers.net.
.                       87203   IN      RRSIG   NS 8 0 518400 20240514190000 20240501180000 5613 . aEAnFwtA9ZAThnTTPrmL5Ld5vhlPUQ/dV/1PF740DYsGhccyTEJcDKfW uYRHoKyjgE/5TO0Av9dbelDEeIJ/RtD4Dlf2u6QFZj
n6R/sWpy9MCKnw aM4I3/vZJMP+Cjf9+TJuNs2TOCln6IsicPtDyJ6nRnrbLybmGPRtb546 S3f5oRZCP1sDWacSDRdk2P8cWg++kDpp5H0GxN5mCypg2/7FmxdtDlN/ oWUQ0Ci0sz0t0z+0wk5zLPzVDfScEtM9GP5zd3lyhRTx8u9rs2BFQzS+ fNt64LgVqnOr
dK1sKNrAdAd9u8UmnNOXV3dfgrneVCh4b+b+47hpgv+f dw9sMQ==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 11 ms

com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    86400   IN      DS      19718 13 2 8ACBB0CD28F41250A80A491389424D341522D946B0DA0C0291F2D3D7 71D7805A
com.                    86400   IN      RRSIG   DS 8 1 86400 20240514190000 20240501180000 5613 . PHe/B1RoNCJhz4AqPyFgWqm/N9iJ+r9vwcXj8Wxz95QoGwqlret3EE+p rBxsk42cdCDvMdkSxiALb7a3YirCKaUpnlgiaXsXSJ/
u5mpidjtGS1+W CFvAhsnq7DIw/aXxOMQ1swvyAkxA81ahnq3FDzWTL2cdE7CiIAL5FpZQ 5cdLo78Lt3Rkkla5rW9qcnyEHSUiw1WnwOIkSgjQ8JKyF8TL2Oqk3VzG dVsRWRGQooY+qQL6HH7xyFH+yJcMcsVfJ/+0wgS7gLUF6uhnCuqQ3uge Tt1MWlWJUUEcB
5/aiFGdyqFRbMCnW4NLejhx7V8xq/3GuQGZ0FzWlAhO lY3abA==
;; Received 1170 bytes from 192.203.230.10#53(e.root-servers.net) in 275 ms

;; UDP setup with 2001:500:d937::30#53(2001:500:d937::30) for google.com failed: network unreachable.
;; no servers could be reached
```