USAGE OF DIG COMMAND.

Tools : DIG on KALI
Site : google.com

DIG command (short for "Domain Information Groper") is a network administration tool used for querying DNS (Domain Name System) servers. It is typically used to gather information about DNS records, including A records (IP addresses), MX records (mail exchanges), CNAME records (canonical names), and more.

INPUT from DIG :

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use o
Player
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ dig -v
DiG 9.19.21-1+b1-Debian

┌──(kali㉿kali)-[~]
└─$ dig google.com

; <<>> DiG 9.19.21-1+b1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34944
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             17      IN      A       142.250.185.14

;; Query time: 15 msec
;; SERVER: 192.168.232.100#53(192.168.232.100) (UDP)
;; WHEN: Sun Nov 24 08:23:14 EST 2024
;; MSG SIZE  rcvd: 44


┌──(kali㉿kali)-[~]
└─$ dig google.com +short
142.250.185.14

┌──(kali㉿kali)-[~]
└─$ dig google.com +noall +answer
google.com.             138     IN      A       142.250.185.14

┌──(kali㉿kali)-[~]
└─$ dig @8.8.8.8 google.com

; <<>> DiG 9.19.21-1+b1-Debian <<>> @8.8.8.8 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5826
;; 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      A

;; ANSWER SECTION:
google.com.             10      IN      A       172.217.17.14

;; Query time: 147 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Nov 24 08:26:25 EST 2024
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use o

Player

1 2 3 4 8:46

kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ dig google.com MX

; <<>> DiG 9.19.21-1+b1-Debian <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7205
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; Query time: 227 msec
;; SERVER: 192.168.232.100#53(192.168.232.100) (UDP)
;; WHEN: Sun Nov 24 08:29:09 EST 2024
;; MSG SIZE  rcvd: 60

┌──(kali㉿kali)-[~]
└─$ dig +short +trace microsoft.com
;; communications error to 192.168.232.100#53: timed out
;; communications error to 192.168.232.100#53: timed out
NS a.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS m.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS k.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS j.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS c.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS d.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS f.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS h.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS b.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS g.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS i.root-servers.net. from server 192.168.232.100 in 2104 ms.
NS l.root-servers.net. from server 192.168.232.100 in 2104 ms.
RRSIG NS 8 0 518400 20241207050000 20241124040000 61050 . WLvyqIE5kiYD+iqA6Md4S0RcvCu61QvcONMEleC/lJAxcxiZRk08QAKR 3
lsSeaN1MRod1KYJKGf/VaoOAC886Wgz8dAirI/jmQXf17JuyzoN+/YY lTyTuodXigS+y+wgSw9+z1ddCI8Fh3+E053jy7fkejX+3HEE105Zxe0W Sw2
vCjdFFESdaiQfsOu7qJFiaN/zM/IPSZ7PCiYUG3j7GantzHeHPoB3 j97FX3iKhrrhaLcZzCyJKTW1/9CeGfvk/jjE9j95bRpl64NxxjSbE0k+ AClel
X7k9au2njnmMuTb3LAv+qNHReGz4j329Y8Xf4UUodR8ByPsp5mj /XWXew== from server 192.168.232.100 in 2104 ms.
;; UDP setup with 2001:500:2f::f#53(2001:500:2f::f) for microsoft.com failed: network unreachable.
;; UDP setup with 2801:1b8:10::b#53(2801:1b8:10::b) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:500:2::c#53(2001:500:2::c) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:7fd::1#53(2001:7fd::1) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:7fe::53#53(2001:7fe::53) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:502:8cc::30#53(2001:502:8cc::30) for microsoft.com failed: network unreachable.
A 20.112.250.133 from server 150.171.10.39 in 124 ms.
A 20.231.239.246 from server 150.171.10.39 in 124 ms.
A 20.76.201.171 from server 150.171.10.39 in 124 ms.
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use o

Player

1 2 3 4 8:46

kali@kali: ~

File Actions Edit View Help

```
;; UDP setup with 2001:500:2f::f#53(2001:500:2f::f) for microsoft.com failed: network unreachable.
;; UDP setup with 2801:1b8:10::b#53(2801:1b8:10::b) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:500:2::c#53(2001:500:2::c) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:7fd::1#53(2001:7fd::1) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:7fe::53#53(2001:7fe::53) for microsoft.com failed: network unreachable.
;; UDP setup with 2001:502:8cc::30#53(2001:502:8cc::30) for microsoft.com failed: network unreachable.
A 20.112.250.133 from server 150.171.10.39 in 124 ms.
A 20.231.239.246 from server 150.171.10.39 in 124 ms.
A 20.76.201.171 from server 150.171.10.39 in 124 ms.
A 20.70.246.20 from server 150.171.10.39 in 124 ms.
A 20.236.44.162 from server 150.171.10.39 in 124 ms.

┌──(kali㉿kali)-[~]
└─$ dig -x 74.125.193.102

; <<>> DiG 9.19.21-1+b1-Debian <<>> -x 74.125.193.102
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51516
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;102.193.125.74.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
102.193.125.74.in-addr.arpa. 3600 IN    PTR     di-in-f102.1e100.net.
102.193.125.74.in-addr.arpa. 3600 IN    PTR     ig-in-f102.1e100.net.

;; Query time: 275 msec
;; SERVER: 192.168.232.100#53(192.168.232.100) (UDP)
;; WHEN: Sun Nov 24 08:32:38 EST 2024
;; MSG SIZE  rcvd: 115

┌──(kali㉿kali)-[~]
└─$ dig -f domain_names.txt +short
domain_names.txt: No such file or directory
dig: couldn't open specified batch file

┌──(kali㉿kali)-[~]
└─$ dig -f santorini.txt +short

┌──(kali㉿kali)-[~]
└─$ dig +short TXT hackaday.com
"google-site-verification=lXv4FJCKtO39C05Cy0mNT4j9zLRbWSO3GIicV4x-iQg"
"facebook-domain-verification=ie1lkz19o2lsbploq4owagf1snbzsy"
"projects google-site-verification=RjppnbZuuM-LhJ6Xb1EGOvnZeM6xvkkMxBxGmOm7ekQ"
"ZOOM_verify_cuY_AVoeSBi4AAVJQvMu-A"
"v=spf1 include:aspmx.googlemail.com include:mailer.postageapp.com include:mailgun.org include:servers.mcsv.net ~all
"

┌──(kali㉿kali)-[~]
└─$ sSsS
```

PROCEDURES AND SOME EXAMPLES OF HOW TO USE DIG COMMAND

We would begin by checking its version by using the following command : dig -v
Then , We will begin by performing a simple dig command. Type the following into a terminal: dig google.com

The above command will include several pieces of information. There may be a time when you only want the result of the query. This can be achieved in dig with the following command:dig google.com +short

As you can see, there can be more than one IP for a host record.

This next command will get rid of all information before the answer section, for easier reading. We can specify this using the following command: dig google.com +noall +answer

We can also specify the nameservers we wish to query using the following command: dig @8.8.8.8 google.com This command queries the “google.com” record from the Name Server with IP address 8.8.8.8.

If we want to query all DNS record types, we can use the “ANY” option. This will display all the available record types in the output: dig google.com ANY

We can also look up a specific record. For example, if we want to get only the mail exchange section associated with a domain, we can use the following command: dig google.com MX We can query a number of specific record types using the following tags in place of MX: TXT, CNAME, NS, A

Dig +short +trace {site of your choice}

We can trace the DNS path, similar to traceroute, using the following command: dig -x 74.125.193.102 It is also possible to make DNS queries for IP addresses.

Dig has a useful feature which allows you to perform a number of DNS lookups for a list of domains instead of doing the same for each one individually. This can be done by performing a lookup using a file: dig -f{ domain_names}.txt +short

Dig +short TXT hackaday.com It is possible to access domain verification data by making a DNS TXT query. Dig is a tool with multiple uses and can be very useful for gathering a broad range of DNS information about a target site.