

## Dig Demo:

### Dig Command Usage and Where

```
eros@kali:~
File Actions Edit View Help
(eros@kali) [~]
$ ~
(eros@kali) [~]
$ dig -h
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
    {@global-d-opt} host {@local-server} [local-d-opt]
    [ host {@local-server} {local-d-opt} [ ... ] ]
Where: domain is in the Domain Name System
    q-class is one of (in,hs,ch, ...) [default: in]
    q-type is one of (a,any,mx,ns,soa,hinfo,axfr,txt, ...) [default:a]
        (Use ixfr=version for type ixfr)
    q-opt is one of:
        -4          (use IPv4 query transport only)
        -6          (use IPv6 query transport only)
        -b address[#port] (bind to source address/port)
        -c class   (specify query class)
        -f filename (batch mode)
        -k keyfile  (specify tsig key file)
        -m          (enable memory usage debugging)
        -p port     (specify port number)
        -q name     (specify query name)
        -r          (do not read ~/.digrc)
        -t type     (specify query type)
        -u          (display times in usec instead of msec)
        -x dot-notation (shortcut for reverse lookups)
        -y [hmac:]name:key (specify named base64 tsig key)
    d-opt is of the form +keyword[=value], where keyword is:
        +[no]aaflag (Set AA flag in query (+[no]aaflag))
```

Dig authority [www.tamusa.edu](http://www.tamusa.edu) & [www.google.com](http://www.google.com)

```
eros@kali:~
File Actions Edit View Help
(eros@kali) [~]
$ dig authority www.tamusa.edu

; <>> DiG 9.18.16-1-Debian <>> authority www.tamusa.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 24515
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION:
;authority.           IN      A

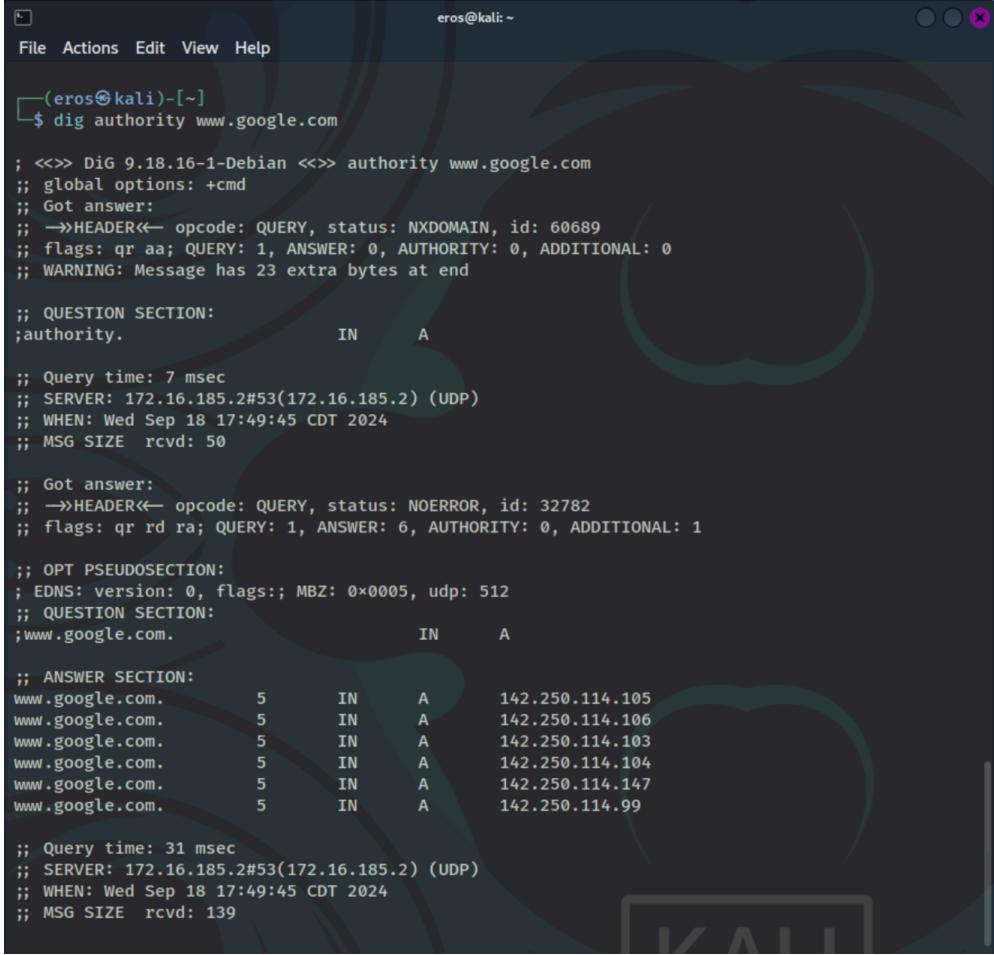
;; Query time: 24 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:48:54 CDT 2024
;; MSG SIZE rcvd: 50

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 40135
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;www.tamusa.edu.       IN      A

;; ANSWER SECTION:
www.tamusa.edu.      5       IN      CNAME   proxy-ext.tamusa.edu.
proxy-ext.tamusa.edu. 5       IN      A       96.46.160.131
proxy-ext.tamusa.edu. 5       IN      A       96.46.160.132

;; Query time: 32 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:48:54 CDT 2024
;; MSG SIZE rcvd: 99
```



```
eros@kali: ~
File Actions Edit View Help
(eros@kali)-[~]
$ dig authority www.google.com

; <>> DiG 9.18.16-1-Debian <>> authority www.google.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NXDOMAIN, id: 60689
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION:
;authority.           IN      A

;; Query time: 7 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:49:45 CDT 2024
;; MSG SIZE rcvd: 50

;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 32782
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

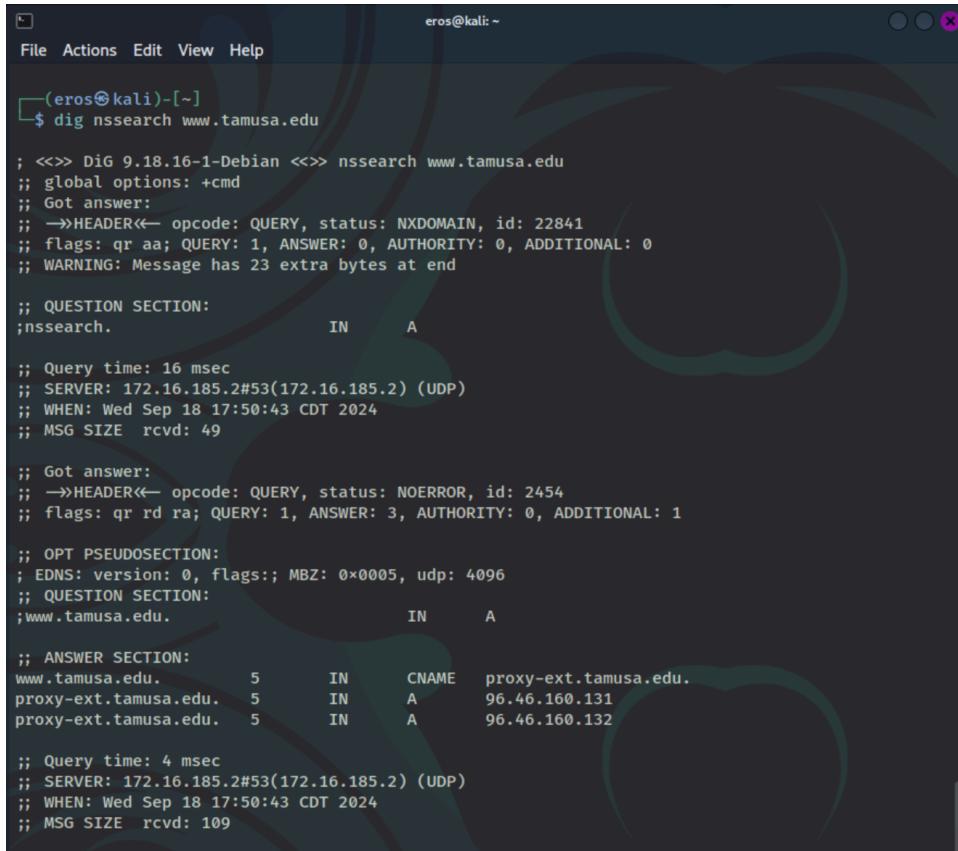
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;www.google.com.        IN      A

;; ANSWER SECTION:
www.google.com.      5       IN      A      142.250.114.105
www.google.com.      5       IN      A      142.250.114.106
www.google.com.      5       IN      A      142.250.114.103
www.google.com.      5       IN      A      142.250.114.104
www.google.com.      5       IN      A      142.250.114.147
www.google.com.      5       IN      A      142.250.114.99

;; Query time: 31 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:49:45 CDT 2024
;; MSG SIZE rcvd: 139
```

The TAMUSA dig query receives two proxy server answers (96.46.160.131 and 96.46.160.132). Being a .edu TLD (Top-level domain) security is a priority so having a proxy provides the website and the user requesting the website more security by requiring a user login. In the case of the Google dig query there are six server answers and being a public domain there are no proxies, unlike [www.tamusa.edu](#). Neither query could find an authoritative answer.

Dig nssearch [www.tamus.edu](http://www.tamus.edu)



```
(eros㉿kali)-[~]
$ dig nssearch www.tamus.edu

; <>> DiG 9.18.1-1-Debian <>> nssearch www.tamus.edu
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 22841
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION:
;nssearch.           IN      A

;; Query time: 16 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:50:43 CDT 2024
;; MSG SIZE rcvd: 49

;; Got answer:
;; ->>>HEADER<- opcode: QUERY, status: NOERROR, id: 2454
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;www.tamus.edu.        IN      A

;; ANSWER SECTION:
www.tamus.edu.      5       IN      CNAME   proxy-ext.tamus.edu.
proxy-ext.tamus.edu. 5       IN      A       96.46.160.131
proxy-ext.tamus.edu. 5       IN      A       96.46.160.132

;; Query time: 4 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:50:43 CDT 2024
;; MSG SIZE rcvd: 109
```

*This query for name servers is almost identical to the authoritative search. There are two proxy answers and the message size is smaller because of the id: 2454.*

Dig nssearch [www.facebook.com](http://www.facebook.com)

```
eros@kali: ~
File Actions Edit View Help

(eros@kali)-[~]
$ dig nssearch www.facebook.com

; <>> DiG 9.18.16-1-Debian <>> nssearch www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 39674
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION:
;nssearch.           IN      A

;; Query time: 16 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:51:33 CDT 2024
;; MSG SIZE rcvd: 49

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30051
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;www.facebook.com.    IN      A

;; ANSWER SECTION:
www.facebook.com.      5      IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 5  IN      A       157.240.24.35

;; Query time: 32 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:51:33 CDT 2024
;; MSG SIZE rcvd: 90
```

## Dig additional [www.tamusa.edu](http://www.tamusa.edu) & [www.facebook.com](http://www.facebook.com)

```
eros@kali: ~
$ dig additional www.tamusa.edu

; <>> DiG 9.18.16-1-Debian <>> additional www.tamusa.edu
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 13356
; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
; WARNING: Message has 23 extra bytes at end

; QUESTION SECTION:
;additional.           IN      A

; Query time: 12 msec
; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
; WHEN: Wed Sep 18 17:51:50 CDT 2024
; MSG SIZE rcvd: 51

; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 53271
; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
; QUESTION SECTION:
;www.tamusa.edu.        IN      A

; ANSWER SECTION:
www.tamusa.edu.      5       IN      CNAME   proxy-ext.tamusa.edu.
proxy-ext.tamusa.edu. 5       IN      A       96.46.160.132
proxy-ext.tamusa.edu. 5       IN      A       96.46.160.131

; Query time: 4 msec
; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
; WHEN: Wed Sep 18 17:51:50 CDT 2024
; MSG SIZE rcvd: 109
```

```
eros@kali: ~
File Actions Edit View Help

(eros@kali)-[~]
$ dig additional www.facebook.com

; <>> DiG 9.18.16-1-Debian <>> additional www.facebook.com
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 20647
; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
; WARNING: Message has 23 extra bytes at end

; QUESTION SECTION:
;additional.           IN      A

; Query time: 16 msec
; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
; WHEN: Wed Sep 18 17:52:17 CDT 2024
; MSG SIZE rcvd: 51

; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 5502
; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
; QUESTION SECTION:
;www.facebook.com.     IN      A

; ANSWER SECTION:
www.facebook.com.    5       IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 5 IN      A       157.240.24.35

; Query time: 32 msec
; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
; WHEN: Wed Sep 18 17:52:17 CDT 2024
; MSG SIZE rcvd: 90
```

## Dig nsid [www.tamusa.edu](http://www.tamusa.edu) & [www.facebook.com](http://www.facebook.com)

```
eros@kali: ~
$ dig nsid www.tamusa.edu

; <>> DiG 9.18.16-1-Debian <>> nsid www.tamusa.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 5785
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION:
;nsid.           IN      A

;; Query time: 15 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:52:28 CDT 2024
;; MSG SIZE rcvd: 45

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 31949
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;www.tamusa.edu.        IN      A

;; ANSWER SECTION:
www.tamusa.edu.      5       IN      CNAME   proxy-ext.tamusa.edu.
proxy-ext.tamusa.edu. 5       IN      A       96.46.160.131
proxy-ext.tamusa.edu. 5       IN      A       96.46.160.132

;; Query time: 3 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:52:28 CDT 2024
;; MSG SIZE rcvd: 109
```

```
eros@kali: ~
$ dig nsid www.facebook.com

; <>> DiG 9.18.16-1-Debian <>> nsid www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 43021
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION:
;nsid.           IN      A

;; Query time: 15 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:52:47 CDT 2024
;; MSG SIZE rcvd: 45

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 43060
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;www.facebook.com.        IN      A

;; ANSWER SECTION:
www.facebook.com.      5       IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 5 IN      A       31.13.93.35

;; Query time: 39 msec
;; SERVER: 172.16.185.2#53(172.16.185.2) (UDP)
;; WHEN: Wed Sep 18 17:52:47 CDT 2024
;; MSG SIZE rcvd: 90
```

*Nslookup -type=NS www.tamusa.edu & www.facebook.com*

```
eros@kali: ~
File Actions Edit View Help
(eros㉿kali)-[~]
$ nslookup -type=NS www.tamusa.edu
Server:      172.16.185.2
Address:     172.16.185.2#53

Non-authoritative answer:
www.tamusa.edu canonical name = proxy-ext.tamusa.edu.

Authoritative answers can be found from:
tamusa.edu
    origin = ns1.tamusa.edu
    mail addr = hostmaster.tamusa.edu
    serial = 474
    refresh = 900
    retry = 600
    expire = 86400
    minimum = 3600

(eros㉿kali)-[~]
$ nslookup -type=NS www.facebook.com
Server:      172.16.185.2
Address:     172.16.185.2#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.

Authoritative answers can be found from:
facebook.com
    origin = a.ns.facebook.com
    mail addr = dns.facebook.com
    serial = 4207849484
    refresh = 14400
    retry = 1800
    expire = 604800
    minimum = 300
```

## Nslookup [www.tamusa.edu](http://www.tamusa.edu) & [www.facebook.com](http://www.facebook.com)

```
[eros㉿kali)-[~]
$ nslookup www.tamusa.edu
Server:      172.16.185.2
Address:     172.16.185.2#53

Non-authoritative answer:
www.tamusa.edu canonical name = proxy-ext.tamusa.edu.
Name: proxy-ext.tamusa.edu
Address: 96.46.160.132
Name: proxy-ext.tamusa.edu
Address: 96.46.160.131

[eros㉿kali)-[~]
$ nslookup www.facebook.com
Server:      172.16.185.2
Address:     172.16.185.2#53

Non-authoritative answer:
www.facebook.com      canonical name = star-mini.c10r.facebook.com.
Name: star-mini.c10r.facebook.com
Address: 157.240.19.35
Name: star-mini.c10r.facebook.com
Address: 2a03:2880:f162:81:face:b00c:0:25de
```

I learned to check and look for domain name servers (DNS) using Nslookup and Dig in Kali Linux. Dig (Domain Information Groper) retrieves information about DNS name servers. I used the authority command to attempt to display the authority section reply and the nssearch command to find the authoritative name servers. I also used additional to view the additional section to a query reply and nsid to receive the DNS nameserver ID. Additionally, I used Nslookup to view servers and their addresses and Nslookup -type=NS to view authoritative answers.