The '**dig command**' is used in network administration that **check and lookup domain name server** (DNS) It is **dnssec** and the part of information gathering.

Well further can't be discussed much until I give you the definition of name servers….until then everything I say will be moot.

What is a domain name server?

A name server is a software and hardware server that provides provides a network service present at the application layer of the OSI model response to the queries against a directory service. The server component of the domain name system is the perfect example of that. Its job is to translate the IP address from the domain names provided.

So, bottom line dig is the shorthand of **domain information groper (dig command)**, it uses DNS (Domain servers) lookups and gropes the information from the **name servers**. Why didn't they use grabber is beyond me!!

So now the usage of this command in

Dig command basic syntax

When you are going to use any command you must know the basic syntax. Dig command basic syntax is useful and necessary.

If you will not follow the basic syntax, you will not get the appropriate result. You can use the following command to know more about dig command

```
$dig -h
or
$man dig
```

Basic syntax as follows:

dig [server] [name] [type]

Server
It is the domain name or IP address of the name server to query. This can be an IPv4 address in dotted-decimal notation or an IPv6 address in colon-delimited notation. When the supplied server argument is a hostname, dig resolves that name before querying that name server. If no server argument is provided, dig consults /etc/resolv.conf; if an address is found there, it queries the name server at that address. If either of the -4 or -6 options are in use, then only addresses for the corresponding transport will be tried. If no usable addresses are found, dig will send the query to the localhost. The reply from the name server that responds is displayed.

Name: is the name of the resource record that is to be looked up.

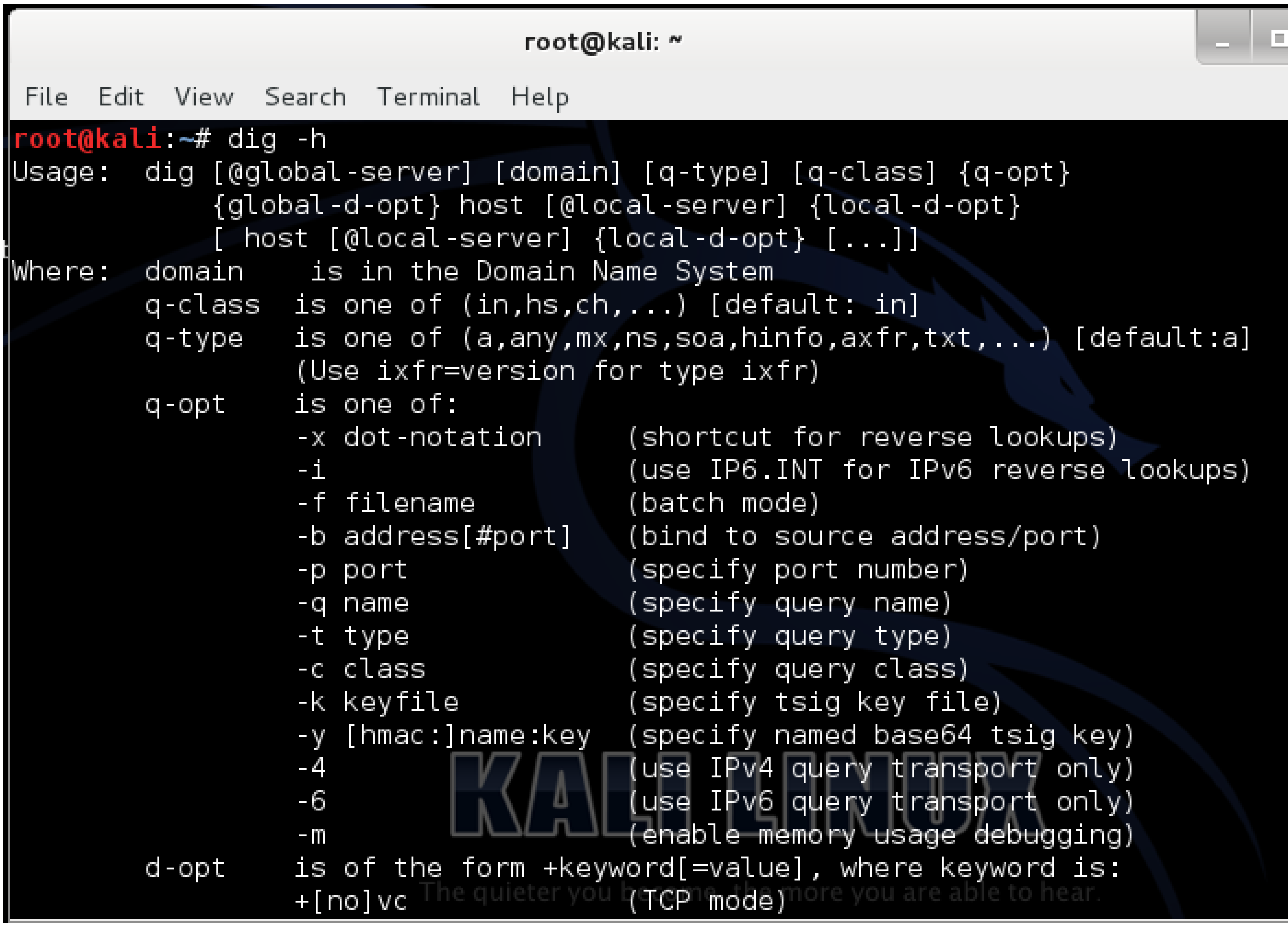
Type: indicates what type of query is required — ANY, A, MX, SIG, etc. type can be any valid query type. If no type argument is supplied, dig will perform a lookup for an A record.

Usage of the dig command.

First on the terminal use the command

dig -h

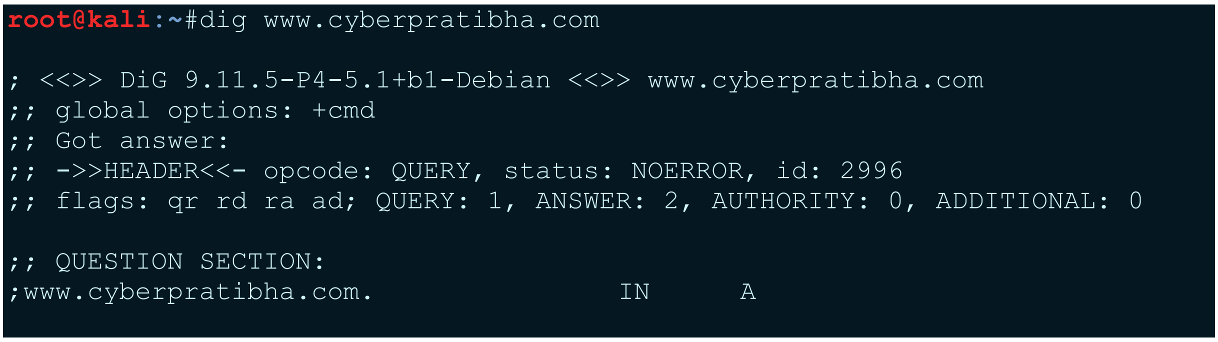
This command would show all the options used in dig


root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

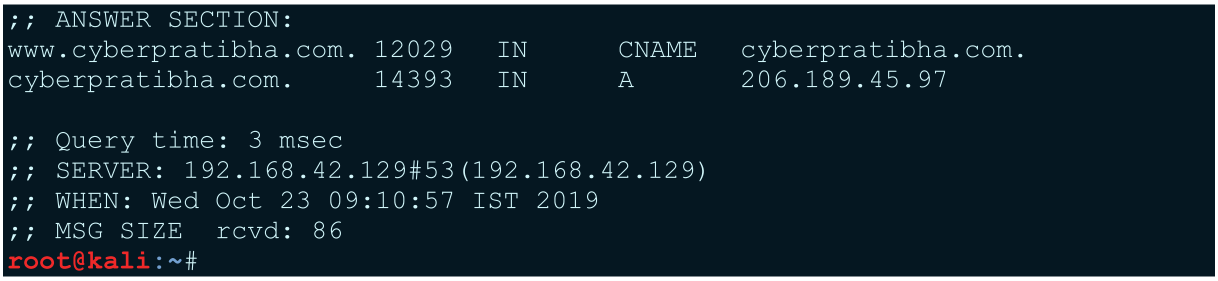
```
root@kali:~# dig -h
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
            {global-d-opt} host [@local-server] {local-d-opt}
            [ host [@local-server] {local-d-opt} [...]]
Where:  domain    is in the Domain Name System
        q-class  is one of (in,hs,ch,...) [default: 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:
                 -x dot-notation     (shortcut for reverse lookups)
                 -i                  (use IP6.INT for IPv6 reverse lookups)
                 -f filename         (batch mode)
                 -b address[#port]   (bind to source address/port)
                 -p port             (specify port number)
                 -q name             (specify query name)
                 -t type             (specify query type)
                 -c class            (specify query class)
                 -k keyfile          (specify tsig key file)
                 -y [hmac:]name:key  (specify named base64 tsig key)
                 -4                  (use IPv4 query transport only)
                 -6                  (use IPv6 query transport only)
                 -m                  (enable memory usage debugging)
        d-opt    is of the form +keyword[=value], where keyword is:
                 +[no]vc             (TCP mode)
```

In a similar way, many of the given commands can be used. For eg, let’s use authority now.

Dig command followed by the domain name

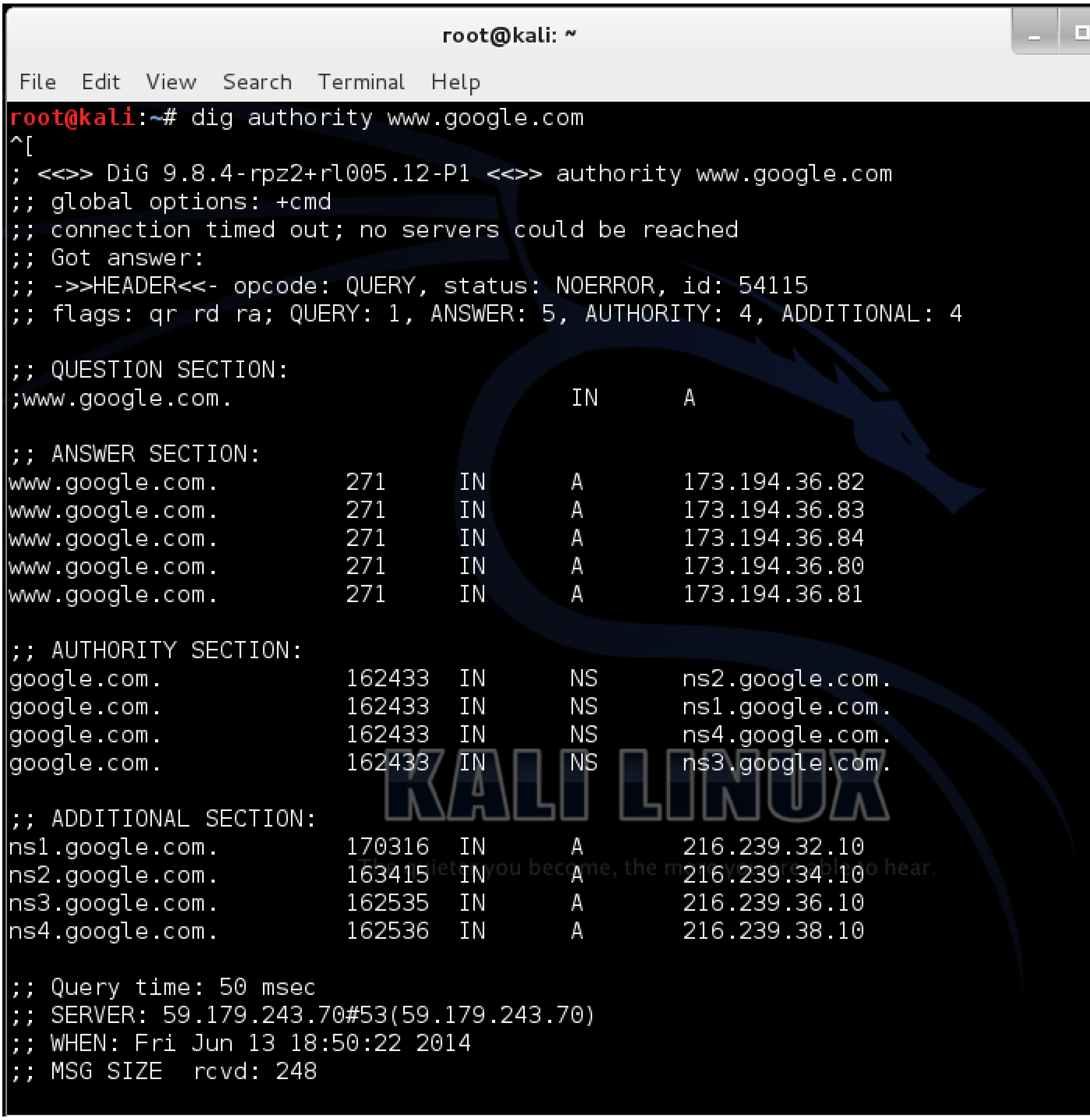


```
root@kali:~#dig www.cyberpratibha.com

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> www.cyberpratibha.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2996
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cyberpratibha.com.              IN      A
```



```
;; ANSWER SECTION:
www.cyberpratibha.com. 12029   IN      CNAME   cyberpratibha.com.
cyberpratibha.com.     14393   IN      A       206.189.45.97

;; Query time: 3 msec
;; SERVER: 192.168.42.129#53(192.168.42.129)
;; WHEN: Wed Oct 23 09:10:57 IST 2019
;; MSG SIZE  rcvd: 86
root@kali:~#
```

dig authority www.google.com



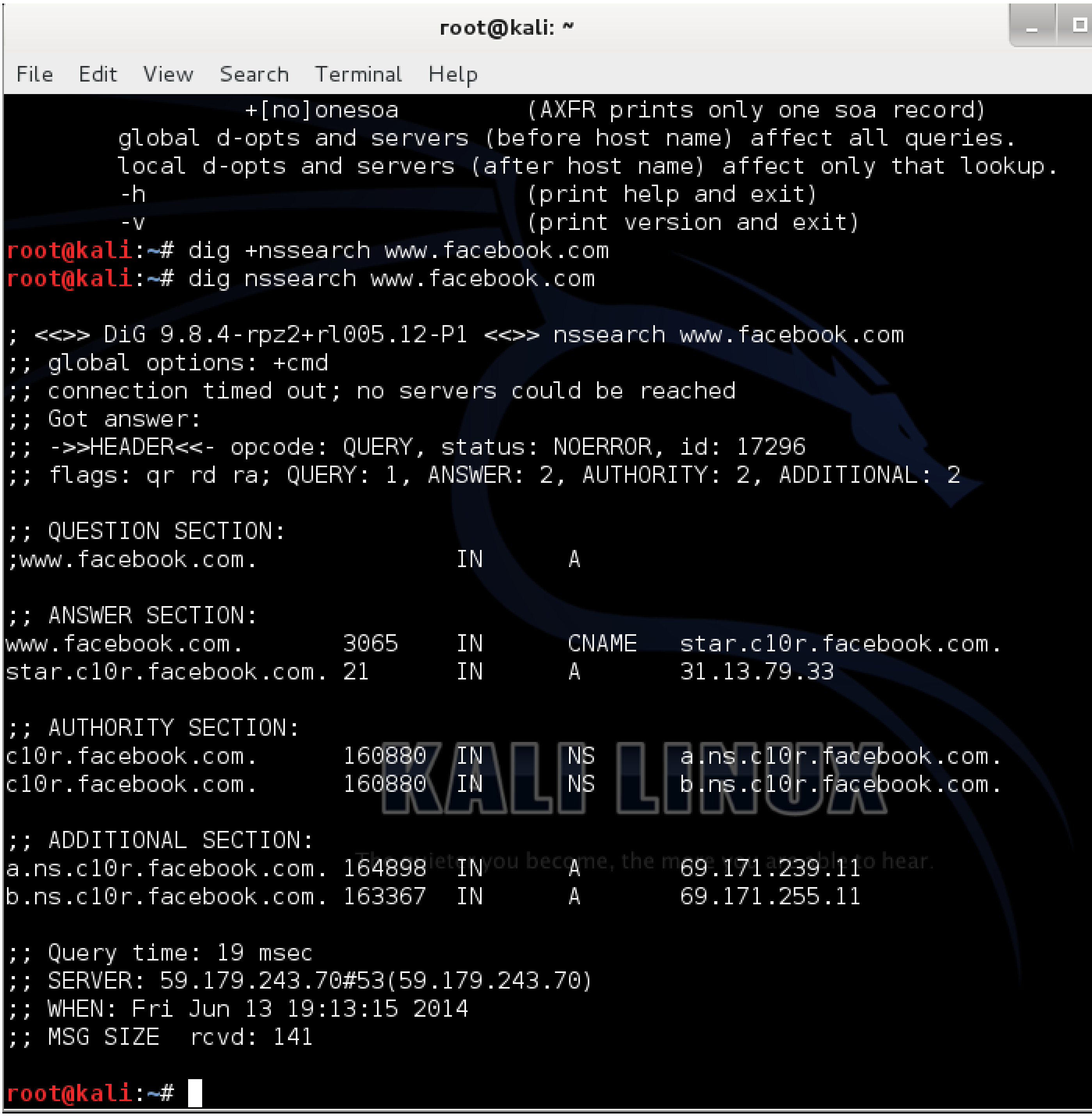
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

```
root@kali:~# dig authority www.google.com
^[
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> authority www.google.com
;; global options: +cmd
;; connection timed out; no servers could be reached
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54115
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 4

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

;; ANSWER SECTION:
www.google.com.         271     IN      A       173.194.36.82
www.google.com.         271     IN      A       173.194.36.83
www.google.com.         271     IN      A       173.194.36.84
www.google.com.         271     IN      A       173.194.36.80
www.google.com.         271     IN      A       173.194.36.81

;; AUTHORITY SECTION:
google.com.             162433  IN      NS      ns2.google.com.
google.com.             162433  IN      NS      ns1.google.com.
google.com.             162433  IN      NS      ns4.google.com.
google.com.             162433  IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         170316  IN      A       216.239.32.10
ns2.google.com.         163415  IN      A       216.239.34.10
ns3.google.com.         162535  IN      A       216.239.36.10
ns4.google.com.         162536  IN      A       216.239.38.10

;; Query time: 50 msec
;; SERVER: 59.179.243.70#53(59.179.243.70)
;; WHEN: Fri Jun 13 18:50:22 2014
;; MSG SIZE  rcvd: 248
```

in the above command, the result indicates that the authoritative search went from ns2->ns1->ns4->ns3, which means name server 2 has more authority over the search according to the context of the domain name over name server 1.

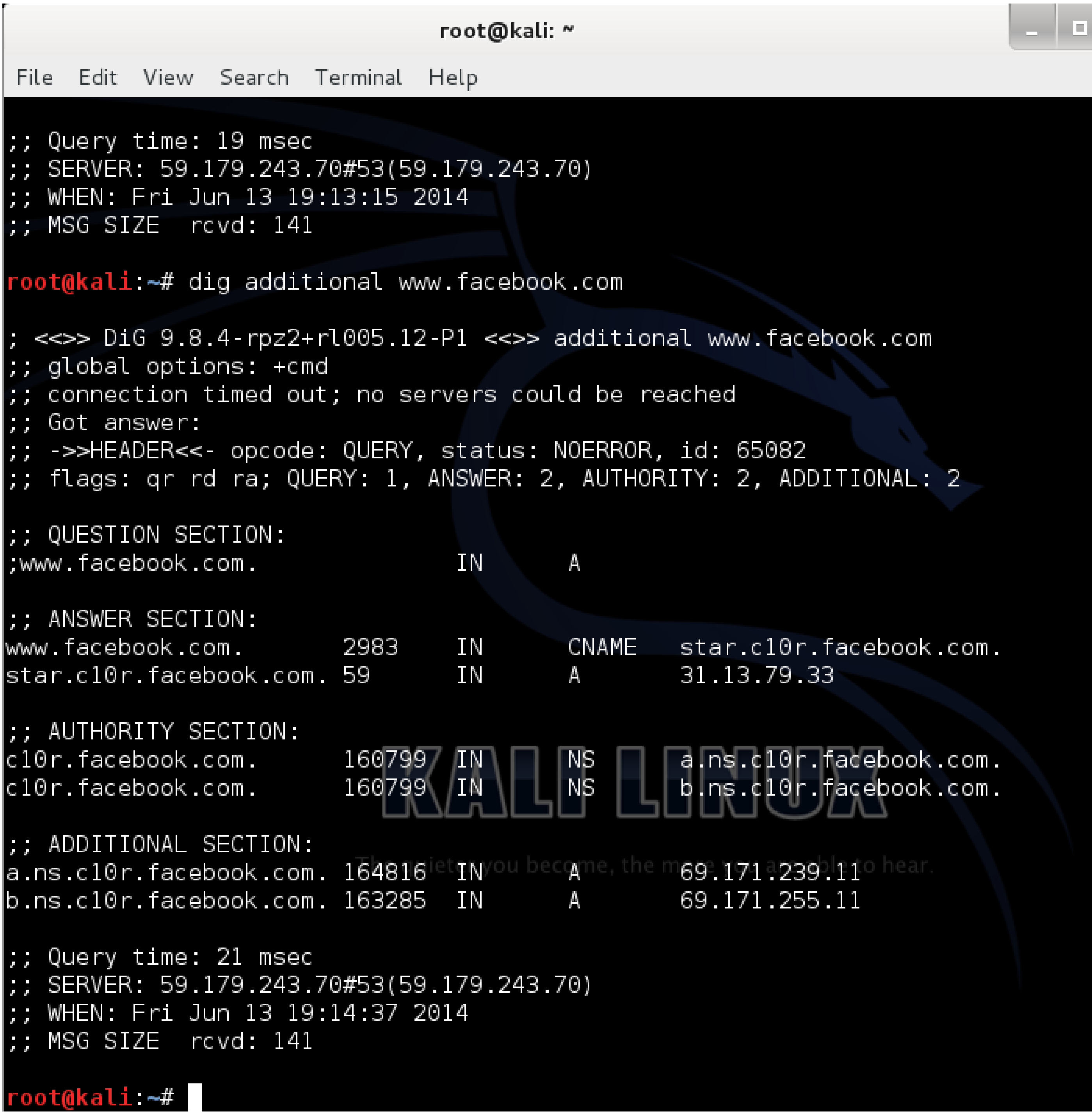
Another Example:

Now let us fool around with some other commands



```
                 +[no]onesoa         (AXFR prints only one soa record)
        global d-opts and servers (before host name) affect all queries.
        local d-opts and servers (after host name) affect only that lookup.
        -h                           (print help and exit)
        -v                           (print version and exit)
root@kali:~# dig +nssearch www.facebook.com
root@kali:~# dig nssearch www.facebook.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> nssearch www.facebook.com
;; global options: +cmd
;; connection timed out; no servers could be reached
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17296
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       3065    IN      CNAME   star.c10r.facebook.com.
star.c10r.facebook.com. 21      IN      A       31.13.79.33

;; AUTHORITY SECTION:
c10r.facebook.com.      160880  IN      NS      a.ns.c10r.facebook.com.
c10r.facebook.com.      160880  IN      NS      b.ns.c10r.facebook.com.

;; ADDITIONAL SECTION:
a.ns.c10r.facebook.com. 164898  IN      A       69.171.239.11
b.ns.c10r.facebook.com. 163367  IN      A       69.171.255.11

;; Query time: 19 msec
;; SERVER: 59.179.243.70#53(59.179.243.70)
;; WHEN: Fri Jun 13 19:13:15 2014
;; MSG SIZE  rcvd: 141

root@kali:~#
```

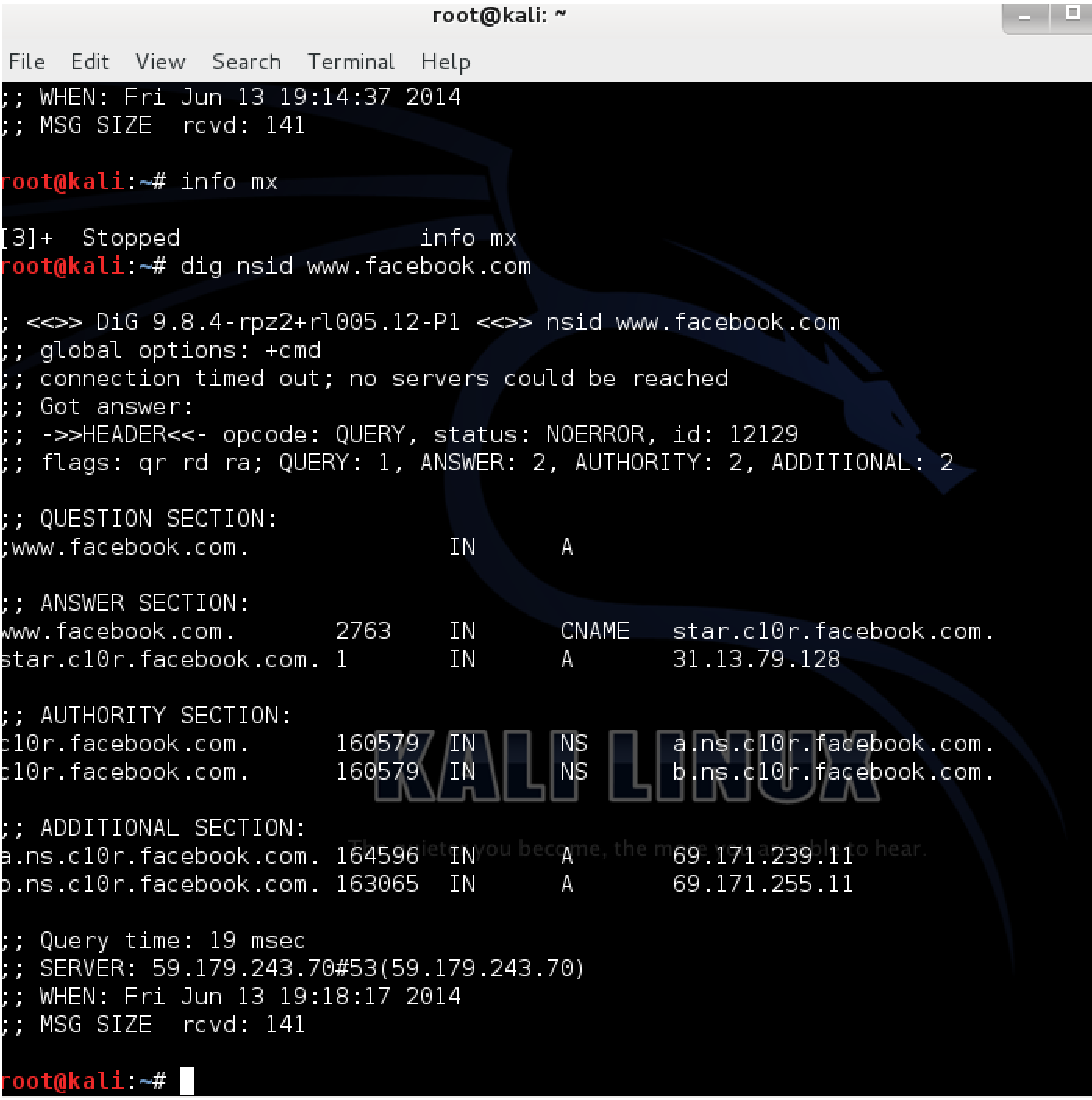
*dig nssearch www.facebook.com **searches for name servers***



```
;; Query time: 19 msec
;; SERVER: 59.179.243.70#53(59.179.243.70)
;; WHEN: Fri Jun 13 19:13:15 2014
;; MSG SIZE  rcvd: 141

root@kali:~# dig additional www.facebook.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> additional www.facebook.com
;; global options: +cmd
;; connection timed out; no servers could be reached
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65082
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       2983    IN      CNAME   star.c10r.facebook.com.
star.c10r.facebook.com. 59      IN      A       31.13.79.33

;; AUTHORITY SECTION:
c10r.facebook.com.      160799  IN      NS      a.ns.c10r.facebook.com.
c10r.facebook.com.      160799  IN      NS      b.ns.c10r.facebook.com.

;; ADDITIONAL SECTION:
a.ns.c10r.facebook.com. 164816  IN      A       69.171.239.11
b.ns.c10r.facebook.com. 163285  IN      A       69.171.255.11

;; Query time: 21 msec
;; SERVER: 59.179.243.70#53(59.179.243.70)
;; WHEN: Fri Jun 13 19:14:37 2014
;; MSG SIZE  rcvd: 141

root@kali:~#
```

dig additional www.facebook.com **controls all additional queries **

dig nsid www.facebook.com ** searches for the name servers ID**



```
;; WHEN: Fri Jun 13 19:14:37 2014
;; MSG SIZE  rcvd: 141

root@kali:~# info mx

[3]+  Stopped                 info mx
root@kali:~# dig nsid www.facebook.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> nsid www.facebook.com
;; global options: +cmd
;; connection timed out; no servers could be reached
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12129
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       2763    IN      CNAME   star.c10r.facebook.com.
star.c10r.facebook.com. 1       IN      A       31.13.79.128

;; AUTHORITY SECTION:
c10r.facebook.com.      160579  IN      NS      a.ns.c10r.facebook.com.
c10r.facebook.com.      160579  IN      NS      b.ns.c10r.facebook.com.

;; ADDITIONAL SECTION:
a.ns.c10r.facebook.com. 164596  IN      A       69.171.239.11
b.ns.c10r.facebook.com. 163065  IN      A       69.171.255.11

;; Query time: 19 msec
;; SERVER: 59.179.243.70#53(59.179.243.70)
;; WHEN: Fri Jun 13 19:18:17 2014
;; MSG SIZE  rcvd: 141

root@kali:~# 
```

Similarly , there are other options that can be used for several other purposes. Here we go folks yet another command prominent in information gathering.