

How to Use Dig to Test DNS

Objective

This document shows how to use the Dig utility for DNS queries and troubleshooting. Dig is known as the Cadillac of DNS utilities because it is the most complete and powerful of all. Dig is natively available in most Unix distributions. Email Security appliances incorporate it as a CLI command (starting at firmware version 6.0). Finally, Dig is not shipped in the Windows OS but can be installed on Windows XP. It may also be possible to install Dig on a Windows 2003 server, but this has not been tested.

All Windows systems use nslookup which is a great complimentary utility to Dig.

Table of Contents

WINDOWS INSTALLATION	2
DEFAULT AND ARBITRARY DNS SERVERS	3
A RECORD LOOK-UP:	4
MX RECORD LOOK-UP.....	5
PTR RECORD (REVERSE DNS) LOOK-UP:	7
TXT RECORD (SPF) LOOK-UP.....	9
MULTIPLE RECORD DNS LOOKUP	10
ADDITIONAL RESOURCES	12

Windows Installation

Dig is not natively available in Windows. However, the utility has been created and made available for Windows. You can download and install the files posted at <http://serghei.net/windows/dig>. Instructions are for the installation of Dig on Windows 98, ME, 2000 and XP. It is not sure if this utility will work on Windows 2000 Server and Windows 2003 Server.

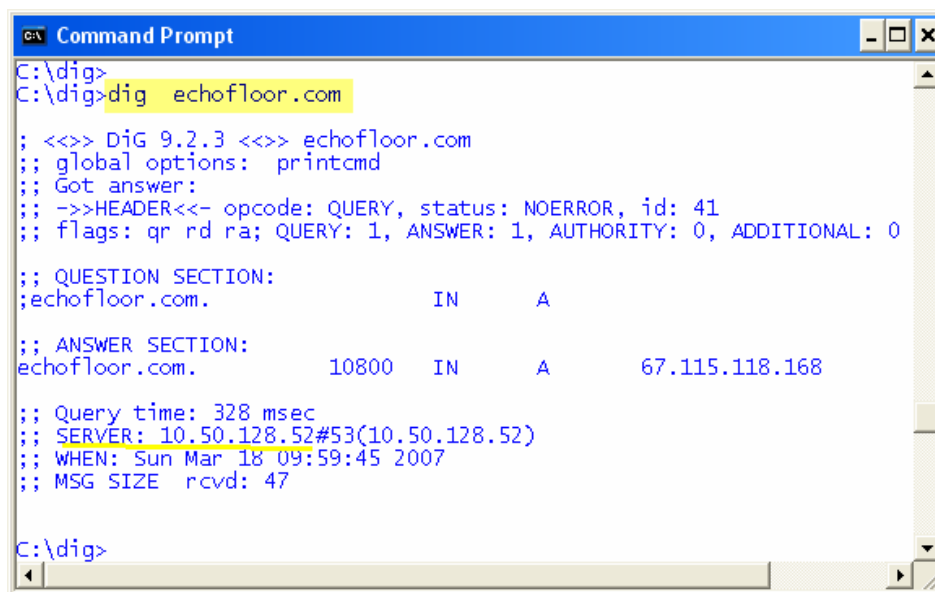
Email Security training provides a quick setup. A C:\dig folder is created and all files, except one, are placed there. The reminding file, `resolve.conf`, is placed in C:\WINDOWS\system32\drivers\etc.

This file sets the default DNS server dig will use. The Email Security setup has the following one line name `nameserver 10.50.128.52`.

Default and Arbitrary DNS Servers

Unless specified, Dig will use the DNS server specified in the resolve.conf file located in the C:\WINDOWS\system32\drivers\etc\ folder.

In the example below, the default DNS server obtained from resolve.conf is 10.50.128.52. Email Security training installation is pre-configured to use DNS server 4.2.2.2.



```

C:\dig>
C:\dig>dig echofloor.com

; <<>> DiG 9.2.3 <<>> echofloor.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
echofloor.com.                10800   IN      A      67.115.118.168

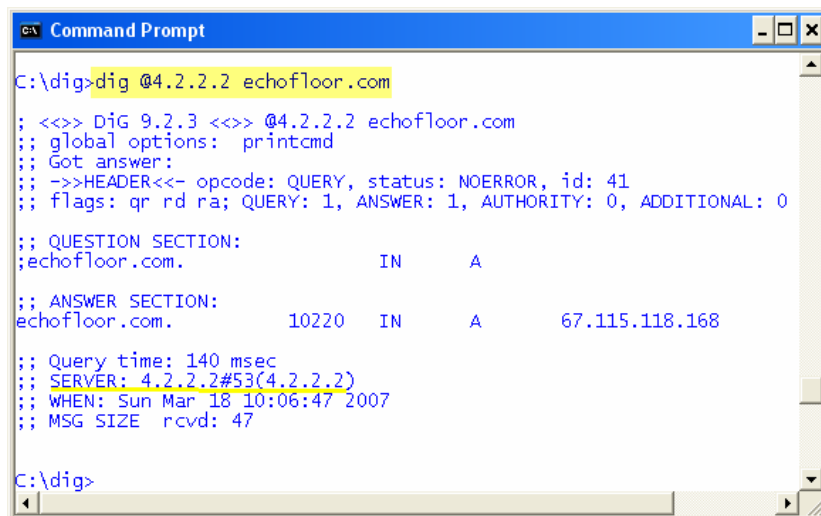
;; Query time: 328 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 09:59:45 2007
;; MSG SIZE rcvd: 47

C:\dig>

```

Sometimes because of troubleshooting, a different DNS server may have to be queried. It is possible that an arbitrary external DNS server is queried instead of the local DNS server.

The DNS server used can be changed without changing the default address in resolve.conf. This can be done on the command line by using the '@' symbol followed by the DNS server name IP address. For example, the instruction "dig @4.2.2.2 echofloor.com " uses the 4.2.2.2 to resolves the IP address of echofloor.com.



```

C:\dig>
C:\dig>dig @4.2.2.2 echofloor.com

; <<>> DiG 9.2.3 <<>> @4.2.2.2 echofloor.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
echofloor.com.                10220   IN      A      67.115.118.168

;; Query time: 140 msec
;; SERVER: 4.2.2.2#53(4.2.2.2)
;; WHEN: Sun Mar 18 10:06:47 2007
;; MSG SIZE rcvd: 47

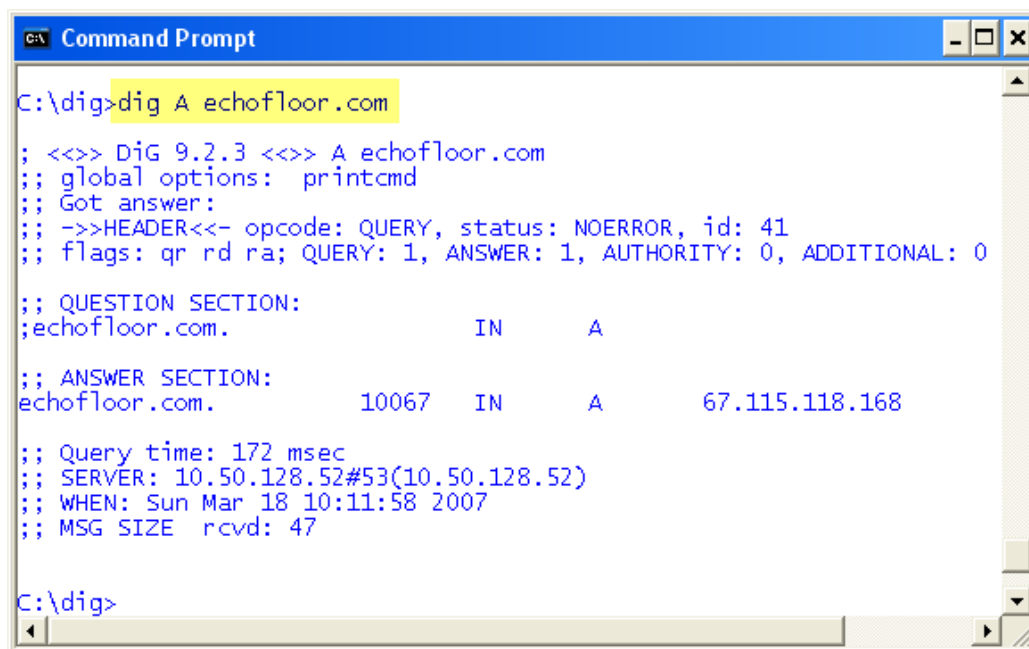
C:\dig>

```

A Record Look-Up:

A records map names to IP addresses. This is performed by placing a capital “A” or lower case “a” letter right after the dig instruction. In reality A record look-up is the default and no letter is necessary.

dig A echofloor.com



```

C:\>dig A echofloor.com

; <<>> DiG 9.2.3 <<>> A echofloor.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
echofloor.com.                10067   IN      A       67.115.118.168

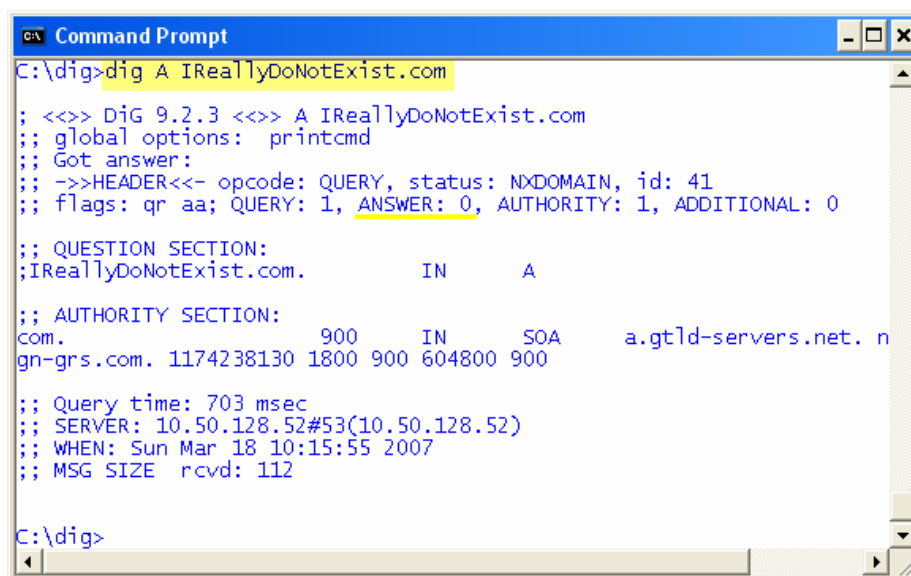
;; Query time: 172 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:11:58 2007
;; MSG SIZE rcvd: 47

C:\>dig

```

The IP address for echofloor.com is 67.115.118.168.

When the name is not found, the “ANSWER” section is missing. For example, an A look-up of IReallyDoNotExist.com yields a response without an “ANSWER” section.



```

C:\>dig A IReallyDoNotExist.com

; <<>> DiG 9.2.3 <<>> A IReallyDoNotExist.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 41
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

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

;; AUTHORITY SECTION:
com.                          900     IN      SOA     a.gtld-servers.net. n
gn-grs.com. 1174238130 1800 900 604800 900

;; Query time: 703 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:15:55 2007
;; MSG SIZE rcvd: 112

C:\>dig

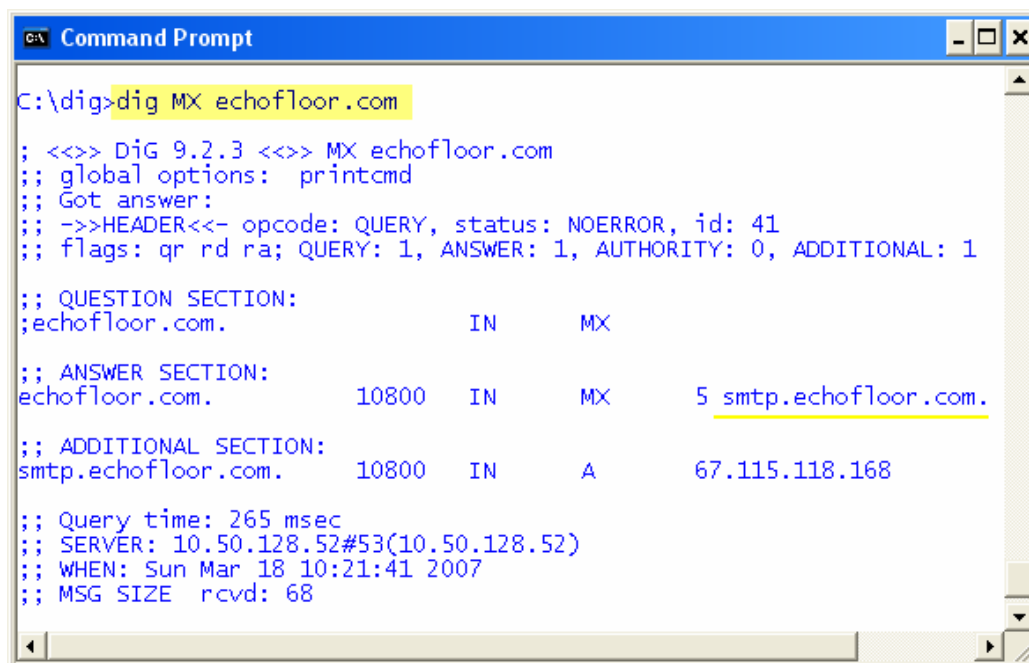
```

MX Record Look-Up

MX records point to the name address of the SMTP server handling incoming email for a particular domain.

```
dig MX echofloor.com
```

The MX record query for echofloor.com resolves to the smtp.echofloor.com domain name. This MX record name resolves to IP address 67.115.118.168.



```
C:\>dig MX echofloor.com

; <<>> DiG 9.2.3 <<>> MX echofloor.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

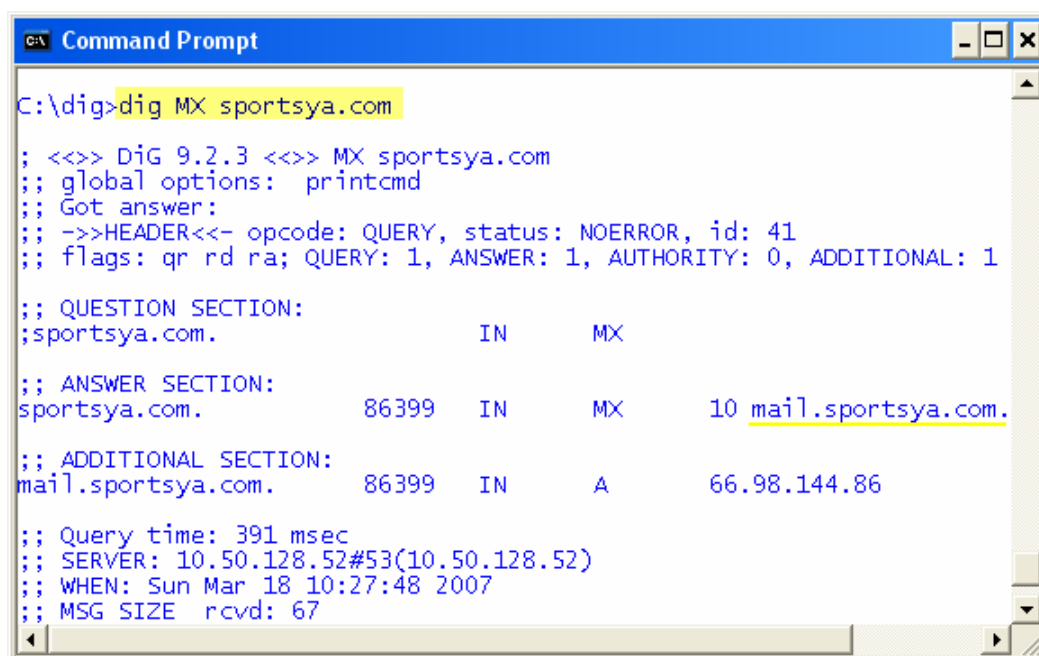
;; QUESTION SECTION:
;echofloor.com.                IN      MX

;; ANSWER SECTION:
echofloor.com.                10800  IN      MX      5 smtp.echofloor.com.

;; ADDITIONAL SECTION:
smtp.echofloor.com.          10800  IN      A       67.115.118.168

;; Query time: 265 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:21:41 2007
;; MSG SIZE rcvd: 68
```

The MX record query for sportsya.com resolves to the mail.sportsya.com domain name. This name resolves to the 66.98.144.86 IP address.



```
C:\>dig MX sportsya.com

; <<>> DiG 9.2.3 <<>> MX sportsya.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

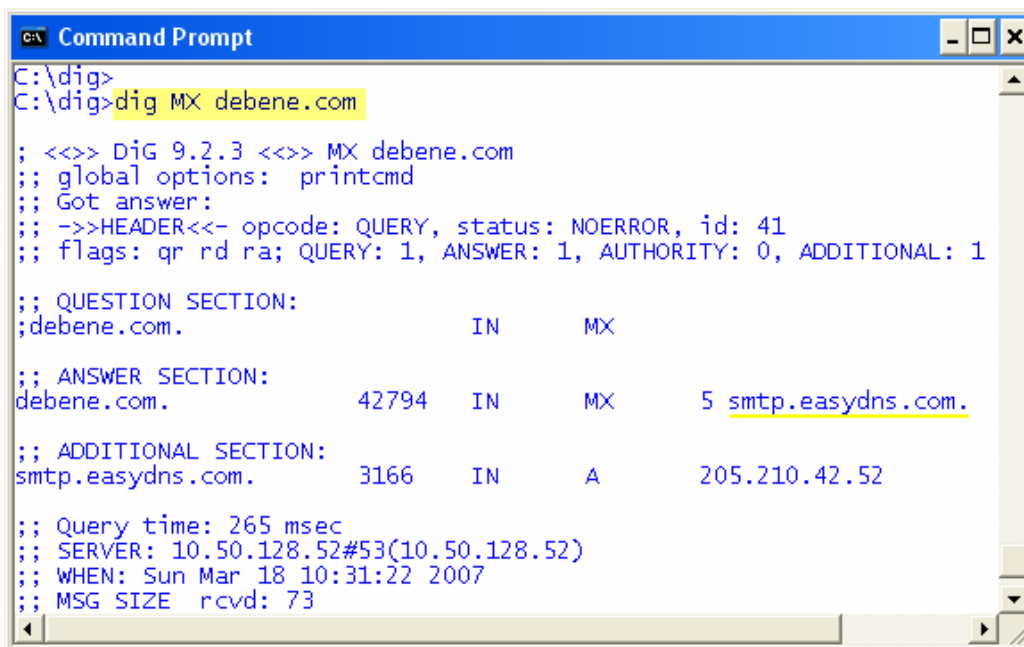
;; QUESTION SECTION:
;sportsya.com.                IN      MX

;; ANSWER SECTION:
sportsya.com.                86399  IN      MX      10 mail.sportsya.com.

;; ADDITIONAL SECTION:
mail.sportsya.com.          86399  IN      A       66.98.144.86

;; Query time: 391 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:27:48 2007
;; MSG SIZE rcvd: 67
```

The MX record query for debene.com resolves to the smtp.easydns.com domain name. This name resolves to 205.210.42.52 IP address.



```
ca Command Prompt
C:\dig>
C:\dig>dig MX debene.com

;; <<>> DiG 9.2.3 <<>> MX debene.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;debene.com.                IN      MX

;; ANSWER SECTION:
debene.com.                42794   IN      MX      5 smtp.easydns.com.

;; ADDITIONAL SECTION:
smtp.easydns.com.         3166    IN      A       205.210.42.52

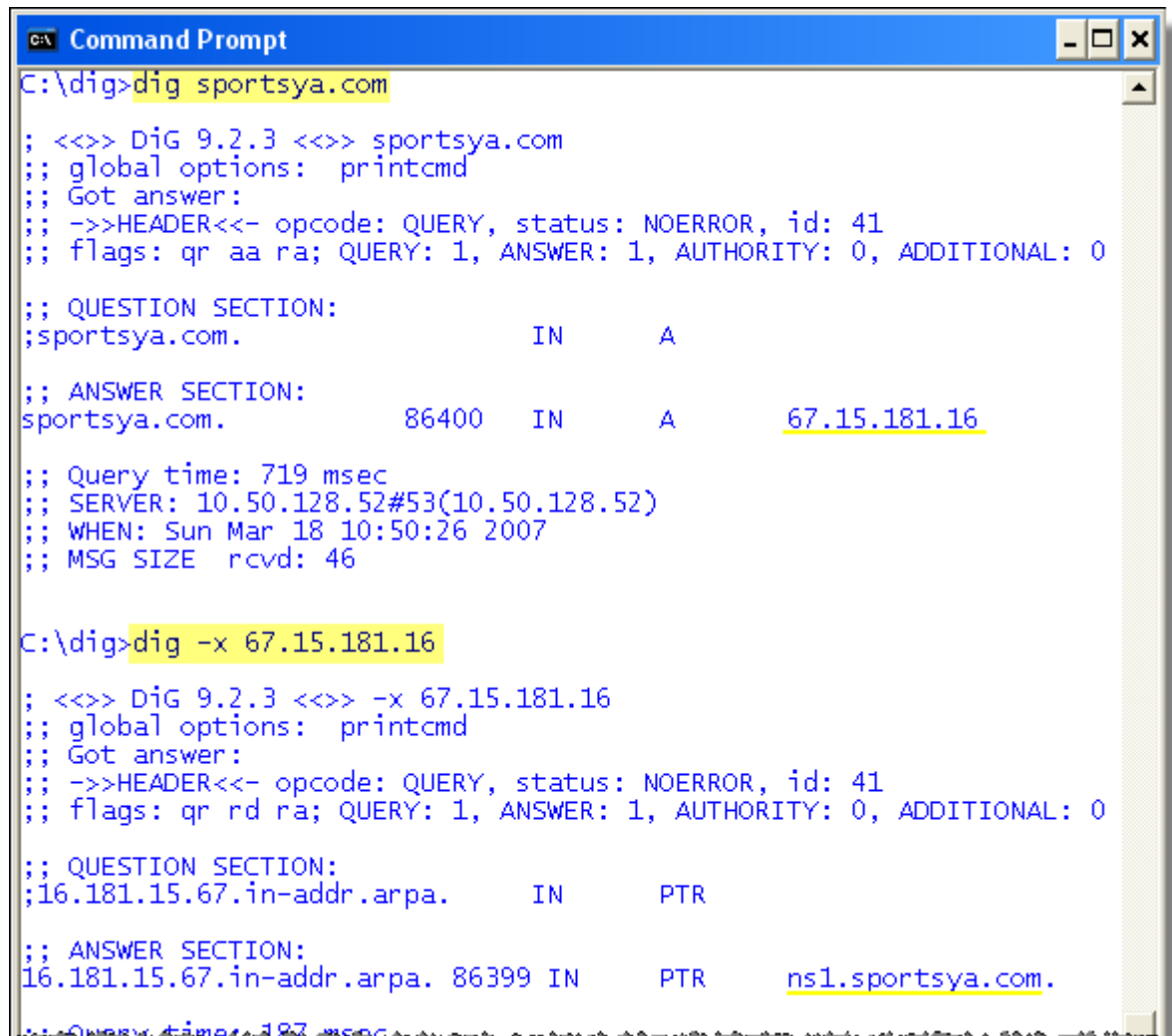
;; Query time: 265 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:31:22 2007
;; MSG SIZE rcvd: 73
```

PTR Record (Reverse DNS) Look-Up:

PTR records resolve an IP address to a name address. This process is also known as reverse DNS lookup.

```
dig -x 67.15.181.16
```

Sportsya.com domain resolves to 67.15.181.16. A reverse DNS lookup of this IP address resolves to ns1.sportsya.com name. IP addresses and domain names do not have a one-to-one relationship. Many names can be mapped to the same IP address whereas only one name can be reverse resolved from a given IP address.



```
C:\>dig>dig sportsya.com

; <<>> DjG 9.2.3 <<>> sportsya.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
sportsya.com.                86400   IN      A      67.15.181.16

;; Query time: 719 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:50:26 2007
;; MSG SIZE rcvd: 46

C:\>dig>dig -x 67.15.181.16

; <<>> DjG 9.2.3 <<>> -x 67.15.181.16
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

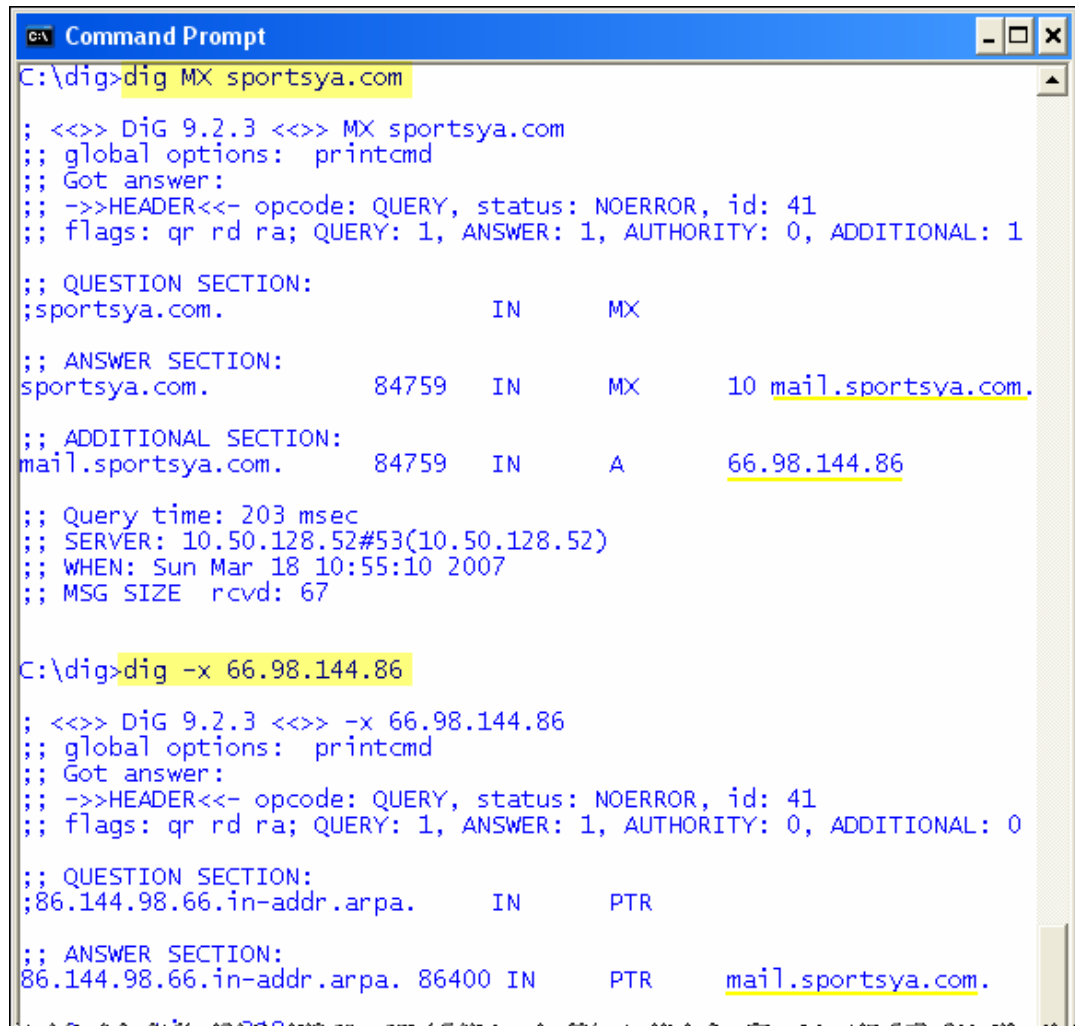
;; QUESTION SECTION:
;16.181.15.67.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
16.181.15.67.in-addr.arpa.  86399   IN      PTR    ns1.sportsya.com.

;; Query time: 187 msec
```

The MX record for sportsya.com is mail.sportsya.com which resolves to 66.98.144.86. The reverse DNS of this IP address resolves back to mail.sportsya.com. The reverse PTR record matching the forward lookup may be important to ensure mail delivery.

Companies such as AOL perform a reverse DNS on the IP address of the connecting SMTP server and compared the resolved name to the announced domain name at connection (in the EHLO/HELO command). If these do not match, the connection is dropped.



```
C:\>dig MX sportsya.com

; <<>> Dig 9.2.3 <<>> MX sportsya.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;sportsya.com.                IN      MX

;; ANSWER SECTION:
sportsya.com.                84759   IN      MX      10 mail.sportsya.com.

;; ADDITIONAL SECTION:
mail.sportsya.com.          84759   IN      A       66.98.144.86

;; Query time: 203 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:55:10 2007
;; MSG SIZE rcvd: 67

C:\>dig -x 66.98.144.86

; <<>> Dig 9.2.3 <<>> -x 66.98.144.86
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;86.144.98.66.in-addr.arpa.   IN      PTR

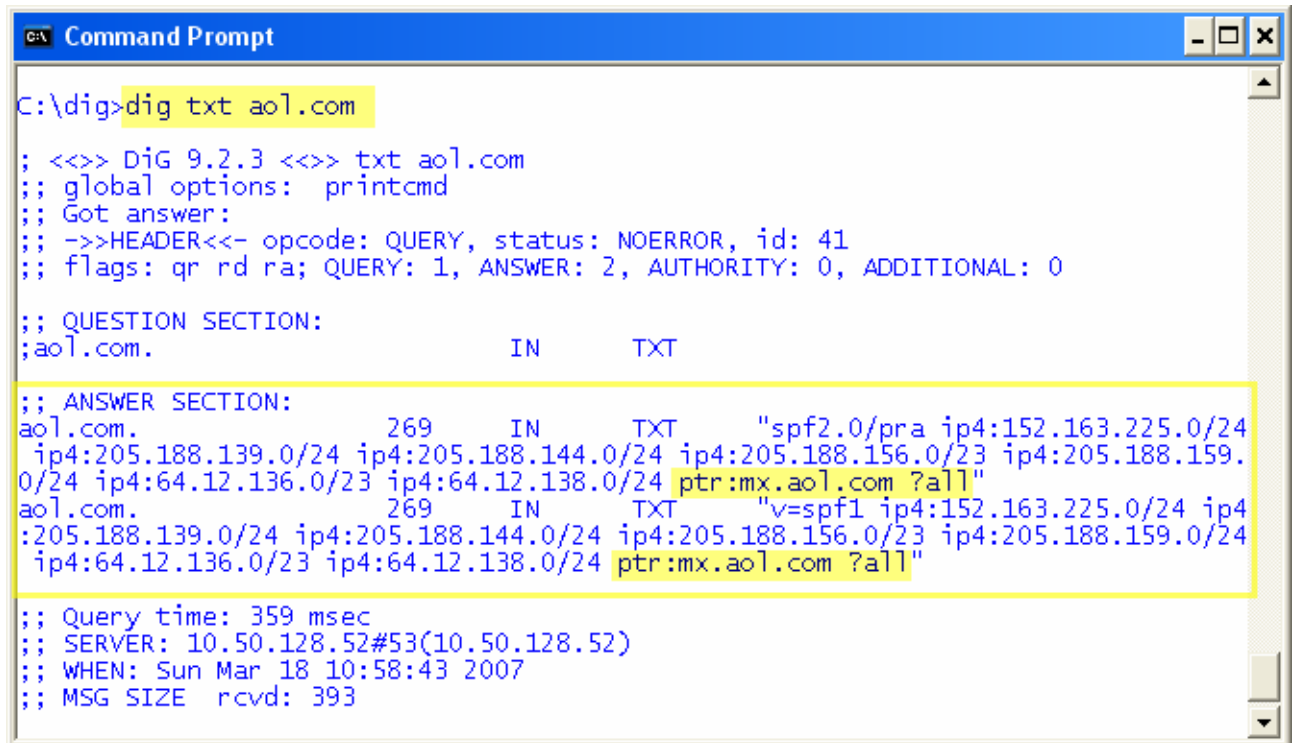
;; ANSWER SECTION:
86.144.98.66.in-addr.arpa.  86400   IN      PTR     mail.sportsya.com.
```

TXT Record (SPF) Look-Up

Reverse DNS allows for a company to announce which IP address are authorized to send email on its behalf. For example, the DNS query below can be executed to find the IPs allowed to send email for aol.com.

```
dig txt aol.com
```

The result here indicates a series of IP ranges from where email can be sent. All of the IP addresses used in this range should resolve back to mx.aol.com (ptr:mx.aol.com).



```
C:\>dig>dig txt aol.com

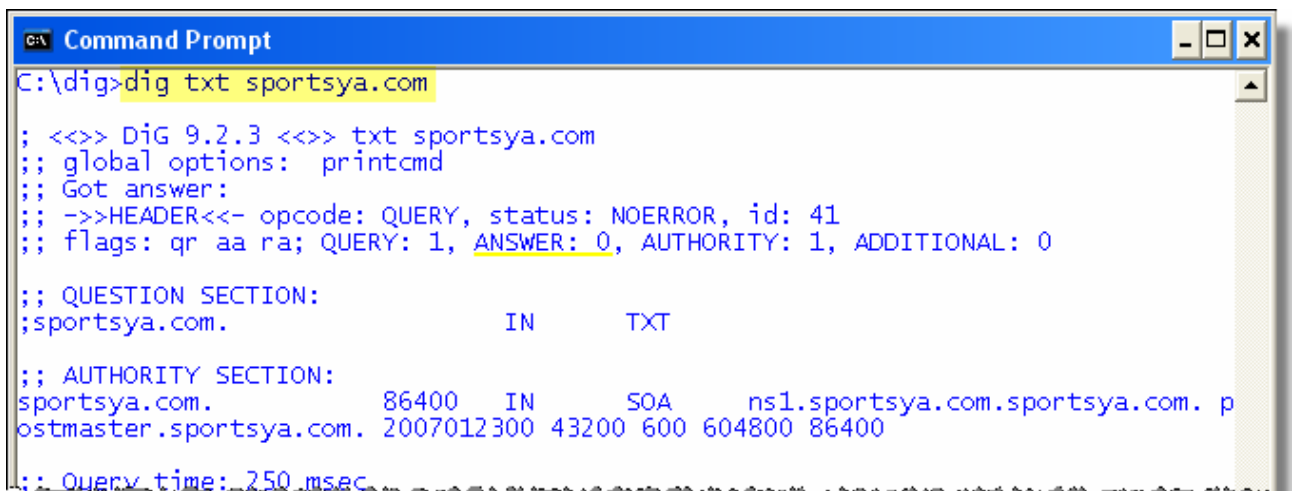
;<<>> DiG 9.2.3 <<>> txt aol.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;aol.com.                IN      TXT

;; ANSWER SECTION:
aol.com.                269     IN      TXT     "spf2.0/pra ip4:152.163.225.0/24
ip4:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.
0/24 ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"
aol.com.                269     IN      TXT     "v=spf1 ip4:152.163.225.0/24 ip4
:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.0/24
ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"

;; Query time: 359 msec
;; SERVER: 10.50.128.52#53(10.50.128.52)
;; WHEN: Sun Mar 18 10:58:43 2007
;; MSG SIZE rcvd: 393
```

On the other hand, sportsya.com does not have any registered SPF records.



```
C:\>dig>dig txt sportsya.com

;<<>> DiG 9.2.3 <<>> txt sportsya.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr aa ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;sportsya.com.          IN      TXT

;; AUTHORITY SECTION:
sportsya.com.          86400   IN      SOA     ns1.sportsya.com.sportsya.com. p
ostmaster.sportsya.com. 2007012300 43200 600 604800 86400

;; Query time: 250 msec
```

Multiple Record DNS Lookup

```
dig any aol.com
```

```

C:\>dig>dig any aol.com
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.2.3 <<>> any aol.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18467
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 19

;; QUESTION SECTION:
;aol.com.                IN      ANY

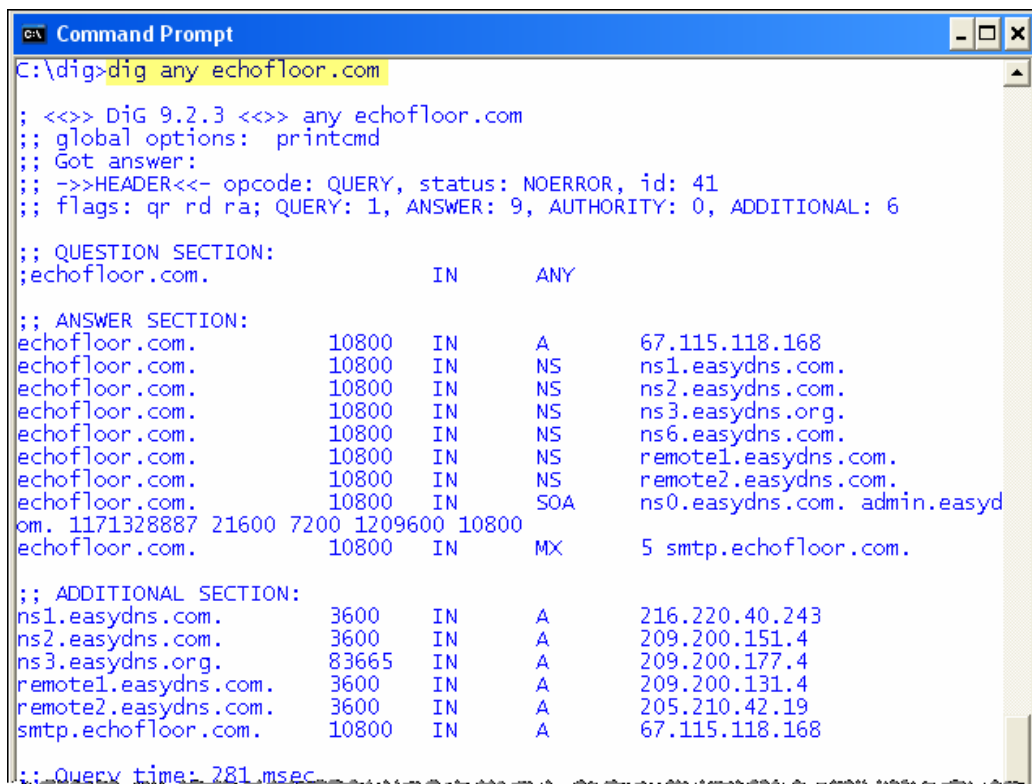
;; ANSWER SECTION:
aol.com.                 60      IN      A       205.188.142.182
aol.com.                 60      IN      A       64.12.50.151
aol.com.                 3600   IN      NS      dns-02.ns.aol.com.
aol.com.                 3600   IN      NS      dns-06.ns.aol.com.
aol.com.                 3600   IN      NS      dns-07.ns.aol.com.
aol.com.                 3600   IN      NS      dns-01.ns.aol.com.
aol.com.                 3600   IN      SOA     dns-01.ns.aol.com. hostmaster.aol.net. 2007031506 1800 300 604800 600
aol.com.                 3600   IN      MX      15 mailin-03.mx.aol.com.
aol.com.                 3600   IN      MX      15 mailin-04.mx.aol.com.
aol.com.                 3600   IN      MX      15 mailin-01.mx.aol.com.
aol.com.                 3600   IN      MX      15 mailin-02.mx.aol.com.
aol.com.                 300    IN      TXT     "spf2.0/pra ip4:152.163.225.0/24 ip4:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.0/24 ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"
aol.com.                 300    IN      TXT     "v=spf1 ip4:152.163.225.0/24 ip4:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.0/24 ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"

;; ADDITIONAL SECTION:
dns-02.ns.aol.com.       3600   IN      A       205.188.157.232
dns-06.ns.aol.com.       3600   IN      A       149.174.54.153
dns-07.ns.aol.com.       3600   IN      A       64.236.1.107
dns-01.ns.aol.com.       3600   IN      A       64.12.51.132
mailin-03.mx.aol.com.    300    IN      A       64.12.138.120
mailin-03.mx.aol.com.    300    IN      A       205.188.157.217
mailin-03.mx.aol.com.    300    IN      A       205.188.159.57
mailin-03.mx.aol.com.    300    IN      A       64.12.137.89
mailin-04.mx.aol.com.    300    IN      A       64.12.138.57
mailin-04.mx.aol.com.    300    IN      A       205.188.156.249
mailin-04.mx.aol.com.    300    IN      A       205.188.159.217
mailin-01.mx.aol.com.    300    IN      A       64.12.137.184
mailin-01.mx.aol.com.    300    IN      A       64.12.137.249
mailin-01.mx.aol.com.    300    IN      A       205.188.156.185
mailin-01.mx.aol.com.    300    IN      A       205.188.158.121
mailin-01.mx.aol.com.    300    IN      A       205.188.155.89
mailin-02.mx.aol.com.    300    IN      A       205.188.157.25
mailin-02.mx.aol.com.    300    IN      A       64.12.137.168
mailin-02.mx.aol.com.    300    IN      A       64.12.138.185

;; Query time: 218 msec

```

```
dig any echofloor.com
```



```

C:\>dig>dig any echofloor.com

;<<<> DiG 9.2.3 <<<> any echofloor.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;echofloor.com.                IN      ANY

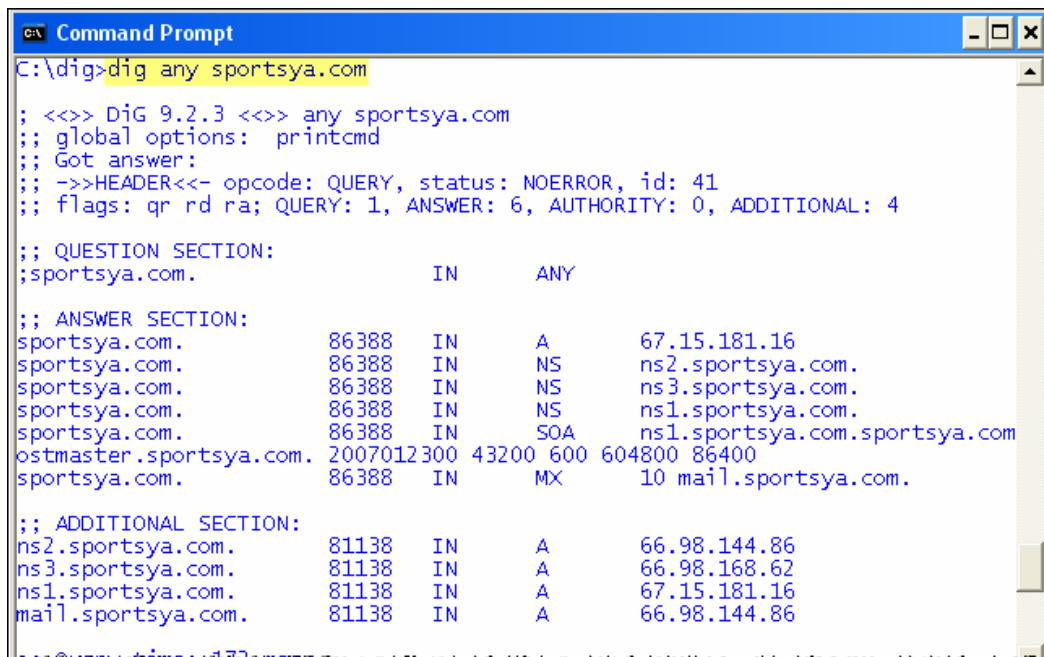
;; ANSWER SECTION:
echofloor.com.                10800   IN      A       67.115.118.168
echofloor.com.                10800   IN      NS      ns1.easydns.com.
echofloor.com.                10800   IN      NS      ns2.easydns.com.
echofloor.com.                10800   IN      NS      ns3.easydns.org.
echofloor.com.                10800   IN      NS      ns6.easydns.com.
echofloor.com.                10800   IN      NS      remote1.easydns.com.
echofloor.com.                10800   IN      NS      remote2.easydns.com.
echofloor.com.                10800   IN      SOA     ns0.easydns.com. admin.easyd
om. 1171328887 21600 7200 1209600 10800
echofloor.com.                10800   IN      MX      5 smtp.echofloor.com.

;; ADDITIONAL SECTION:
ns1.easydns.com.              3600    IN      A       216.220.40.243
ns2.easydns.com.              3600    IN      A       209.200.151.4
ns3.easydns.org.              83665   IN      A       209.200.177.4
remote1.easydns.com.          3600    IN      A       209.200.131.4
remote2.easydns.com.          3600    IN      A       205.210.42.19
smtp.echofloor.com.           10800   IN      A       67.115.118.168

.: Query time: 281 msec

```

```
dig any sportsya.com
```



```

C:\>dig>dig any sportsya.com

;<<<> DiG 9.2.3 <<<> any sportsya.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;sportsya.com.                IN      ANY

;; ANSWER SECTION:
sportsya.com.                 86388   IN      A       67.15.181.16
sportsya.com.                 86388   IN      NS      ns2.sportsya.com.
sportsya.com.                 86388   IN      NS      ns3.sportsya.com.
sportsya.com.                 86388   IN      NS      ns1.sportsya.com.
sportsya.com.                 86388   IN      SOA     ns1.sportsya.com.sportsya.com
ostmaster.sportsya.com.       2007012300 43200 600 604800 86400
sportsya.com.                 86388   IN      MX      10 mail.sportsya.com.

;; ADDITIONAL SECTION:
ns2.sportsya.com.             81138   IN      A       66.98.144.86
ns3.sportsya.com.             81138   IN      A       66.98.168.62
ns1.sportsya.com.             81138   IN      A       67.15.181.16
mail.sportsya.com.            81138   IN      A       66.98.144.86

.: Query time: 172 msec

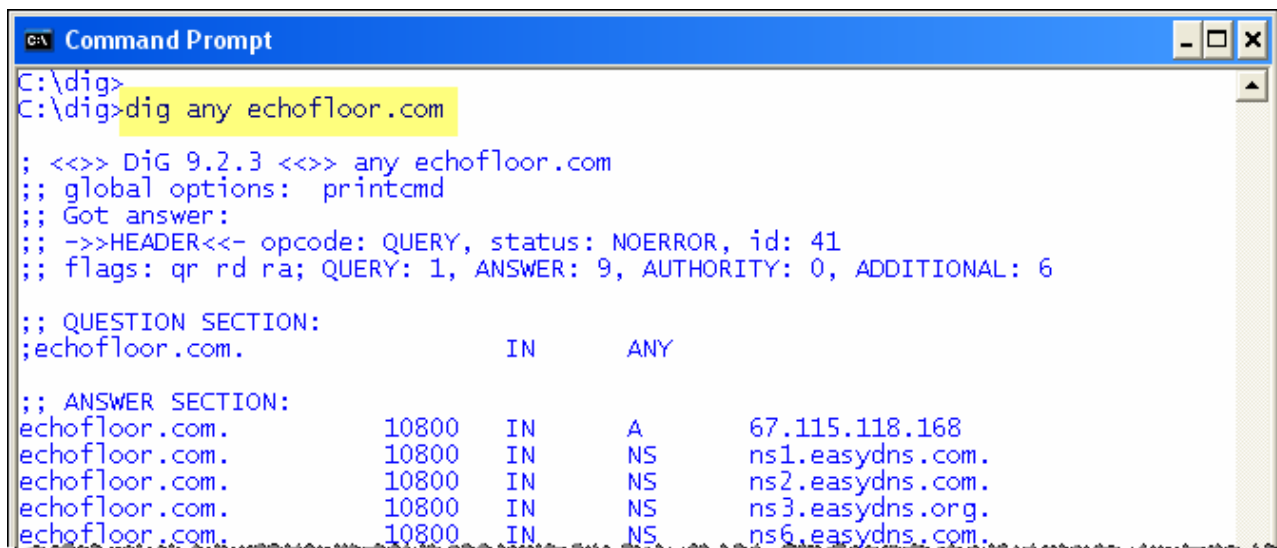
```

Additional Resources

Dig's man page can be found online...

- <http://www.stopspam.org/usenet/mmf/man/dig.html>
- <http://www.die.net/doc/linux/man/man1/dig.1.html>

Dig also has built-in help.



```
C:\> Command Prompt
C:\> dig
C:\> dig any echofloor.com

; <<>> DiG 9.2.3 <<>> any echofloor.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;echofloor.com.                IN      ANY

;; ANSWER SECTION:
echofloor.com.                10800  IN      A       67.115.118.168
echofloor.com.                10800  IN      NS      ns1.easydns.com.
echofloor.com.                10800  IN      NS      ns2.easydns.com.
echofloor.com.                10800  IN      NS      ns3.easydns.org.
echofloor.com.                10800  IN      NS      ns6.easydns.com.
```

Contacting SonicWALL Sales

- Toll free US: +1 888.557.6642
- Local US: +1 408.745.9600
- Local Fax US: +1 408.745.9300
- If you wish to be contacted, use this form: http://www.sonicwall.com/us/How_to_Buy.html

Created: MM/DD/07

Updated: 05/08/07

Created by SonicWALL Technical Publications

Updated and Maintained by: Jean-Marc Catalaa

Version 2.0