Using *nslookup* to query Internet Name servers

- DNS is a hierarchical, tree structured, system. The top is written '**.**' and pronounced **'root'**.

- Under **.** there are a number of Top Level Domains (TLDs), the best known ones are ORG, COM, EDU and NET, but there are many more. Just like a tree it has a root and it branches out.

- When looking for a machine the query proceeds recursively into the hierarchy starting at the top.

- If you want to find out the address of **prep.ai.mit.edu** your name server has to find a name server that serves **edu**. It asks a **.** server (it already knows the **.** servers, that's what the root.hints file is for), the **.** server gives a list of **edu** servers:

- Here is an example session:

  $ nslookup
  Default Server: mozart.bcit.ca
  Address: 142.232.189.1

- Start asking a root server:

  > server c.root-servers.net.
  Default Server: c.root-servers.net
  Address: 192.33.4.12

- Set the Query type to NS (name server records):

  > set q=ns

- Ask about **edu**:

  > edu.

- The trailing **.** here is significant, it tells ***nslookup*** we're asking that edu is right under . (and not under any of our search domains, it speeds the search).

- You should see the following:

```
Server:         c.root-servers.net.
Address:        192.33.4.12#53

Non-authoritative answer:
*** Can't find edu.: No answer

Authoritative answers can be found from:
edu     nameserver = L3.NSTLD.COM.
edu     nameserver = D3.NSTLD.COM.
edu     nameserver = A3.NSTLD.COM.
edu     nameserver = E3.NSTLD.COM.
edu     nameserver = C3.NSTLD.COM.
edu     nameserver = F3.NSTLD.COM.
edu     nameserver = G3.NSTLD.COM.
edu     nameserver = B3.NSTLD.COM.
edu     nameserver = M3.NSTLD.COM.
L3.NSTLD.COM    internet address = 192.41.162.32
D3.NSTLD.COM    internet address = 192.31.80.32
A3.NSTLD.COM    internet address = 192.5.6.32
E3.NSTLD.COM    internet address = 192.12.94.32
C3.NSTLD.COM    internet address = 192.26.92.32
F3.NSTLD.COM    internet address = 192.35.51.32
G3.NSTLD.COM    internet address = 192.42.93.32
B3.NSTLD.COM    internet address = 192.33.14.32
M3.NSTLD.COM    internet address = 192.55.83.32
```

- This tells us that the **c.root-server** does not serve EDU., but it does provide us with a list of **edu** servers so we can go on asking any of them.

- We'll ask **C3.NSTLD.COM**. Now we want to now who serves the next level of the domain name: **mit.edu.**:

```
> server C3.NSTLD.COM
Default server: C3.NSTLD.COM
Address: 192.26.92.32

> set q=ns
> edu.
Server:         C3.NSTLD.COM
Address:        192.26.92.32#53

edu     nameserver = A3.NSTLD.COM.
edu     nameserver = E3.NSTLD.COM.
edu     nameserver = C3.NSTLD.COM.
edu     nameserver = F3.NSTLD.COM.
edu     nameserver = G3.NSTLD.COM.
edu     nameserver = B3.NSTLD.COM.
edu     nameserver = M3.NSTLD.COM.
edu     nameserver = L3.NSTLD.COM.
edu     nameserver = D3.NSTLD.COM.
```

```
> mit.edu.
Server:         C3.NSTLD.COM
Address:        192.26.92.32#53

Non-authoritative answer:
mit.edu nameserver = STRAWB.mit.edu.
mit.edu nameserver = W20NS.mit.edu.
mit.edu nameserver = BITSY.mit.edu.

Authoritative answers can be found from:
STRAWB.mit.edu  internet address = 18.71.0.151
W20NS.mit.edu   internet address = 18.70.0.160
BITSY.mit.edu   internet address = 18.72.0.3
```

- **STRAWB, W20NS** and **BITSY** all serve **mit.edu**, we select one and inquire about the name one more level up: **ai.mit.edu**:

  > **server W20NS.mit.edu.**

  Server: W20NS.mit.edu
  Address: 18.70.0.160

  > ai.mit.edu.
  Server: W20NS.mit.edu
  Address: 18.70.0.160

  Non-authoritative answer:
  ai.mit.edu nameserver = BEET-CHEX.ai.mit.edu
  ai.mit.edu nameserver = FEDEX.ai.mit.edu
  ai.mit.edu nameserver = LIFE.ai.mit.edu
  ai.mit.edu nameserver = ALPHA-BITS.ai.mit.edu

  Authoritative answers can be found from:
  BEET-CHEX.ai.mit.edu internet address = 128.52.32.22
  FEDEX.ai.mit.edu internet address = 192.148.252.3
  LIFE.ai.mit.edu internet address = 128.52.32.80
  ALPHA-BITS.ai.mit.edu internet address = 128.52.32.5

- So **FEDEX.ai.mit.edu** is a nameserver for **ai.mit.edu**:

  > server FEDEX.ai.mit.edu
  Default Server: FEDEX.ai.mit.edu
  Address: 192.148.252.43

- Now we can change the query type, we've found the name server so now we're going to ask about everything **FEDEX** knows about **prep.ai.mit.edu**:

```
> set q=any
> prep.ai.mit.edu
Server:         FEDEX.ai.mit.edu
Address:        192.148.252.43

Name:   prep.ai.mit.edu
Address: 199.232.41.9
prep.ai.mit.edu mail exchanger = 1 mail.gnu.org.
prep.ai.mit.edu mail exchanger = 2 mail2.gnu.org.
```

- So starting at . we found the successive name servers for the each level in the domain name.
- In the tree analogue each "." in the name is a branching point. And each part between the "."s are the names of individual branches in the tree.
- We climb the tree by taking the name we want (prep.ai.mit.edu) first finding the root (.) and then looking for the next branch to climb, in this case edu.
- Once we have found it we climb it by switching to the server that knows about that part of the name.
- Next we look for the mit branch over the edu branch (the combined name is mit.edu) and climb it by switching to a server that knows about mit.edu.
- Again we look for the next branch, it's ai.mit.edu and again we switch to the server that knows about it.
- Now we have arrived at the right server, at the right branching point. The last part is finding prep.ai.mit.edu, which is simple.