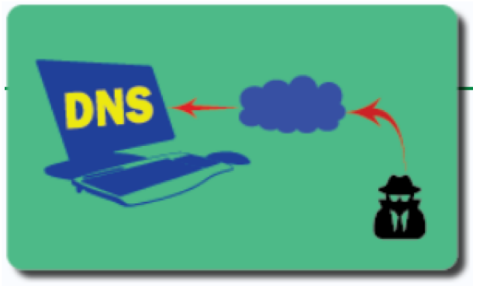
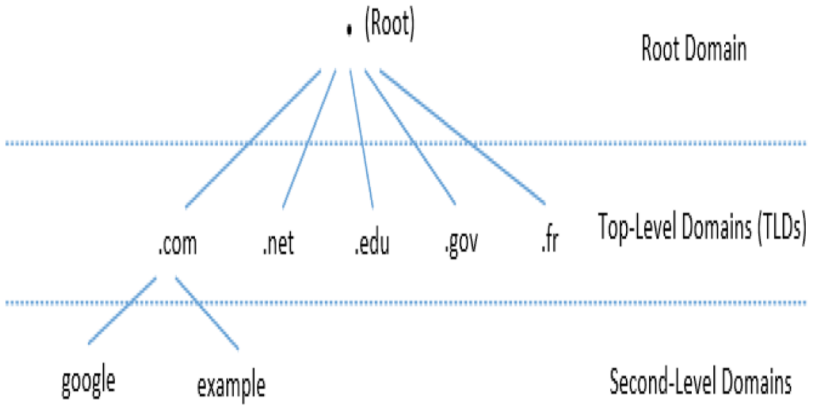
Computer and Network Security

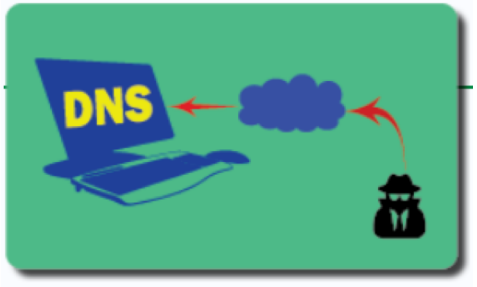
Domain Name System



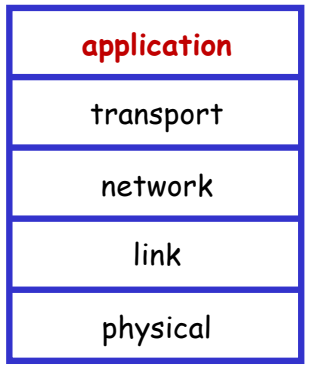
Outline

- DNS Protocol, Hierarchy and Servers
- DNS Query Process
- DNS Attacks : Overview
  - Local DNS Cache Poisoning Attack
  - Remote DNS Cache Poisoning Attack
  - Reply Forgery Attacks from Malicious DNS Servers
  - DNS Rebinding Attack
- Protection Against DNS Cache Poisoning Attacks
- Denial of Service Attacks on DNS Servers





Domain Name System (DNS)



Identifiers

- People:
  - many identifiers
  - SSN, name, passport #
- Internet hosts, routers:
  - IP address (e.g., 10.2.0.21) - used for addressing datagrams
  - name, e.g., www.yahoo.com - used by humans

Q: how to map between IP address and name, and vice versa ?

- DNS: a distributed database implemented in hierarchy of many name servers
- application-layer protocol:
  - hosts, name servers communicate to resolve names (address/name translation)
  - core Internet function

DNS records

RR format: `(name, value, type, ttl)`

DNS: distributed db storing resource records (RR)

1. Type=A
   - name is hostname
   - value is IP address

   (relay1.bar.foo.com, 145.111. 93. 26, A)

2. Type=NS
   - name is domain (e.g. foo.com)
   - value is hostname of authoritative name server for this domain

   (foo.com, dns.foo.com, NS)

3. Type=CNAME
   - name is alias name for some "canonical" (the real) name (value)
   - www.ibm.com is really servereast.backup2.ibm.com

   (www.ibm.com, servereast.backup2.ibm.com, CNAME)

4. Type=MX
   - value is name of mail server associated with name

   (foo.com, mail.bar.foo.com, MX)

Type = A

RR format: (name, value, type, ttl)

1. Type=A

- name is hostname
- value is IP address
- (relay1.bar.foo.com, 145.111.93.26, A)

```
LAS-23445:~ yunwang$ nslookup -type=A bradley.edu
Server:         136.176.190.111
Address:        136.176.190.111#53

Non-authoritative answer:
Name:   bradley.edu
Address: 52.2.159.182
```

Type = NS

RR format: (**name**, **value**, **type**, ttl)

2. Type=NS
   - name is domain (e.g. foo.com)
   - value is hostname of **authoritative** name server for this domain

(foo.com, dns.foo.com, NS)

- Each DNS zone has at least one authoritative nameserver that publishes information about the zone.
- It provides the original and definitive answers to DNS queries.

```
LAS-23445:~ yunwang$ nslookup -type=NS bradley.edu
Server:         136.176.190.111
Address:        136.176.190.111#53

Non-authoritative answer:
bradley.edu     nameserver = auth1.dns.cogentco.com.
bradley.edu     nameserver = auth2.dns.cogentco.com.
bradley.edu     nameserver = dns1.bradley.edu.
bradley.edu     nameserver = dns2.bradley.edu.

Authoritative answers can be found from:
dns1.bradley.edu        internet address = 136.176.200.10
dns2.bradley.edu        internet address = 136.176.200.100
auth1.dns.cogentco.com  internet address = 66.28.0.14
auth1.dns.cogentco.com  has AAAA address 2001:550:1:a::d
auth2.dns.cogentco.com  internet address = 66.28.0.30

LAS-23445:~ yunwang$ nslookup -type=CNAME bradley.edu
```

Type = CNAME

RR format: (**name**, **value**, **type**, ttl)

3. Type=CNAME

- name is alias name for some "canonical" (the real) name (value)
- www.ibm.com is really servereast.backup2.ibm.com
- (www.ibm.com, servereast.backup2.ibm.com, **CNAME**)

```
LAS-23445:~ yunwang$ nslookup -type=CNAME bradley.edu
Server:         136.176.190.111
Address:        136.176.190.111#53

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

Authoritative answers can be found from:
bradley.edu
        origin = dns1.bradley.edu
        mail addr = dns.bradley.edu
        serial = 2016219510
        refresh = 300
        retry = 1800
        expire = 604800
        minimum = 86400

LAS-23445:~ yunwang$ nslookup -type=MX bradley.edu
```

Type = MX

RR format: (**name**, **value**, **type**, ttl)

4. Type=MX
- value is name of mail server associated with name
- (foo.com, mail.bar.foo.com, MX)

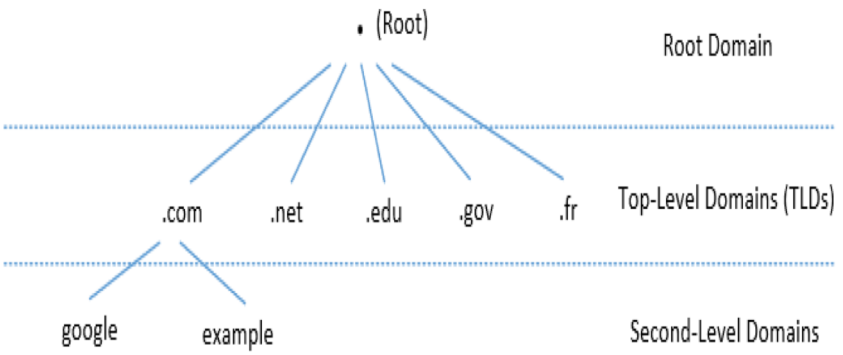
```
LAS-23445:~ yunwang$ nslookup -type=MX bradley.edu
Server:         136.176.190.111
Address:        136.176.190.111#53

Non-authoritative answer:
bradley.edu     mail exchanger = 10 alt3.aspmx.l.google.com.
bradley.edu     mail exchanger = 5 alt2.aspmx.l.google.com.
bradley.edu     mail exchanger = 5 alt1.aspmx.l.google.com.
bradley.edu     mail exchanger = 10 alt4.aspmx.l.google.com.
bradley.edu     mail exchanger = 1 aspmx.l.google.com.

Authoritative answers can be found from:
bradley.edu     nameserver = auth2.dns.cogentco.com.
bradley.edu     nameserver = auth1.dns.cogentco.com.
bradley.edu     nameserver = dns1.bradley.edu.
bradley.edu     nameserver = dns2.bradley.edu.
dns1.bradley.edu        internet address = 136.176.200.10
dns2.bradley.edu        internet address = 136.176.200.100
auth1.dns.cogentco.com  internet address = 66.28.0.14
auth1.dns.cogentco.com  has AAAA address 2001:550:1:a::d
auth2.dns.cogentco.com  internet address = 66.28.0.30

LAS-23445:~ yunwang$
```

DNS Domain Hierarchy

- Domain namespace is organized in a hierarchical tree-like structure.
- Each node is called a domain, or subdomain.
- The root of the domain is called ROOT, denoted as ' . '.

Below ROOT, we have Top-Level Domain (TLD). Ex: In www.example.com, the TLD is .com.

The next level of domain hierarchy is second-level domain which are usually assigned to specific entities such as companies, schools etc



DNS ROOT Servers

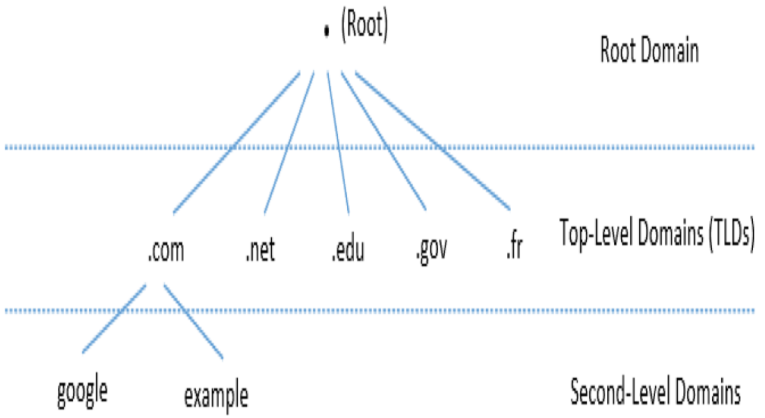
- The root zone is called ROOT.
- There are **13** authoritative nameservers (DNS root servers) for this zone.
- They provide the nameserver information about all TLDs https://www.internic.net/domain/root.zone
- They are the starting point of DNS queries and the most critical infrastructure on the Internet.

List of Root Servers

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

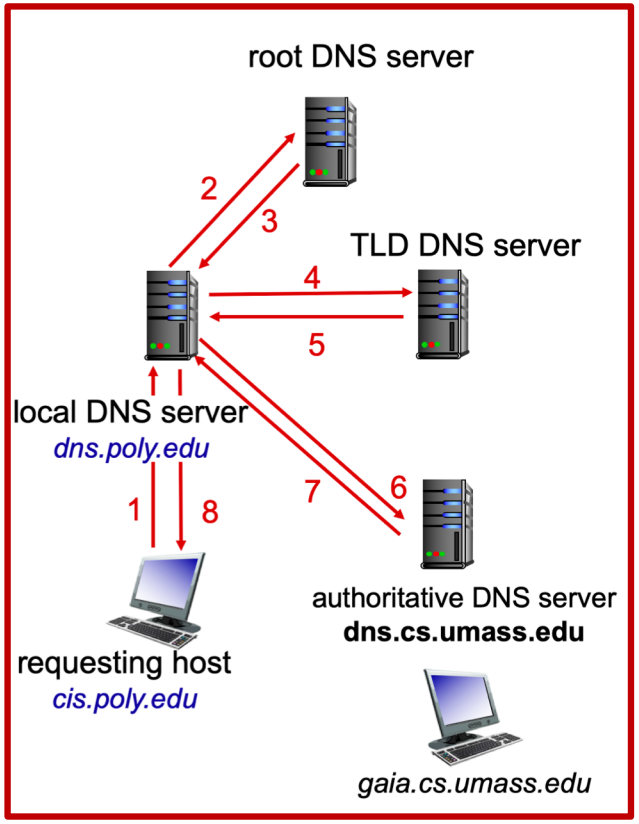
Top Level Domain (TLD)

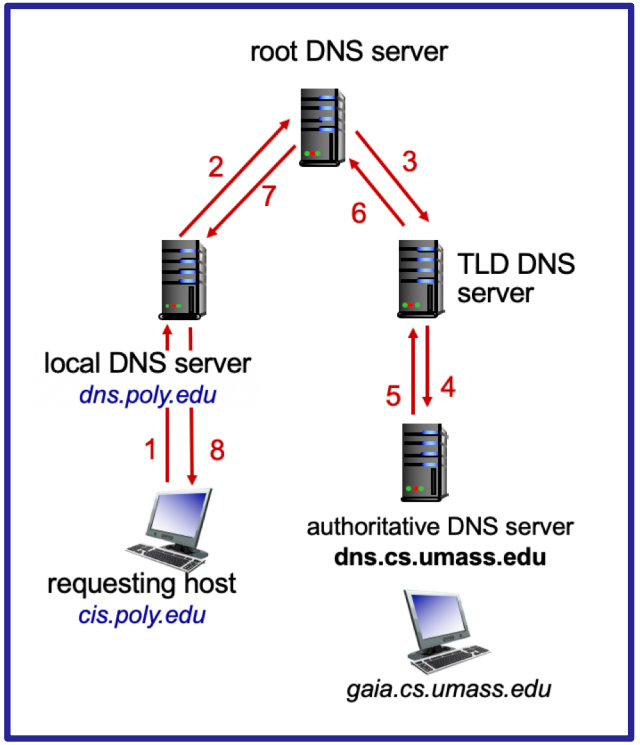
1. Infrastructure TLD: .arpa
2. Generic TLD (gTLD): .com, .net,
3. Sponsored TLD (sTLD): These domains are proposed and sponsored by private agencies or organizations that establish and enforce rules restricting the eligibility to use the TLD: .edu, .gov, .mil, .travel, .jobs
4. Country Code TLD (ccTLD): .au (Australia), .cn (China), .fr (France)
5. Reserved TLD: .example, .test, .localhost, .invalid



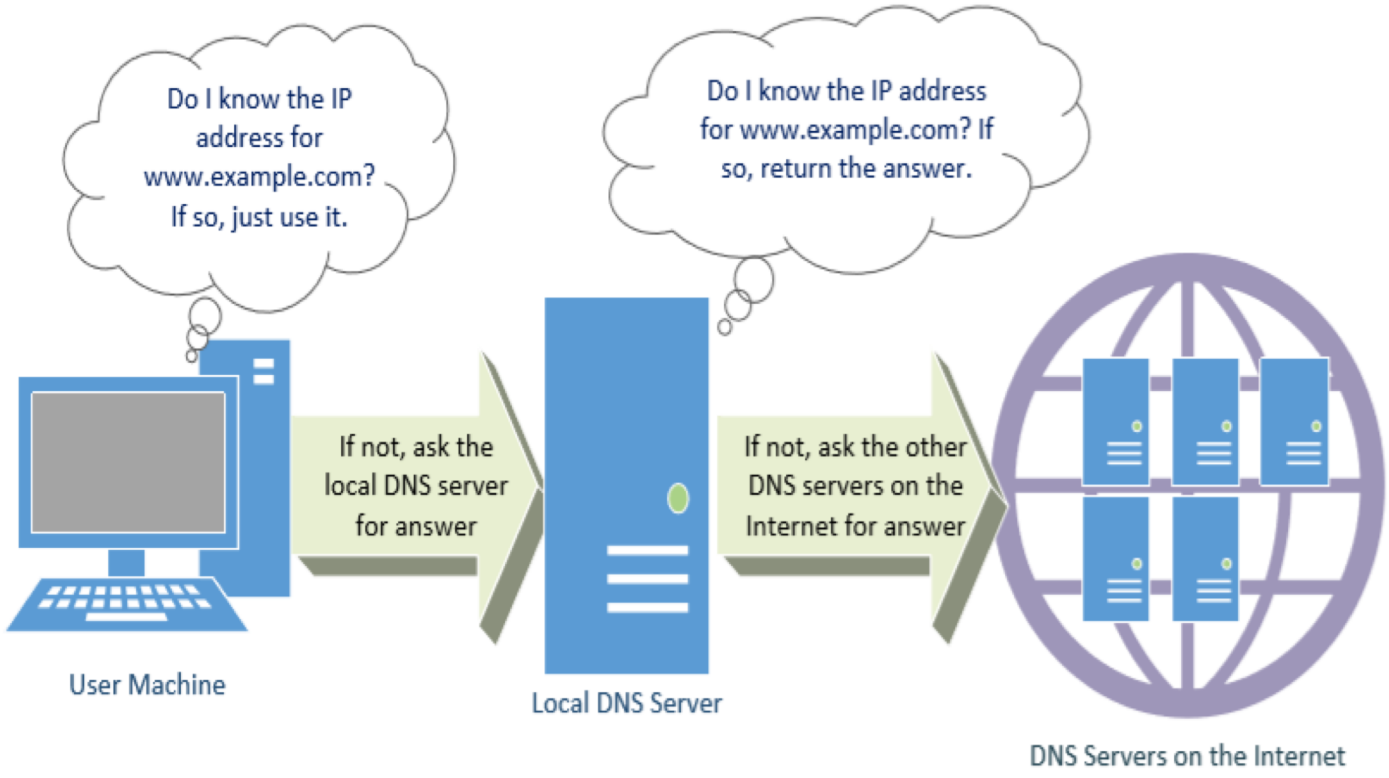
DNS Name Resolution

- Q: host at cis.poly.edu wants IP address for gaia.cs.umass.edu
- **Iterative query**
  - contacted server replies with name of server to contact
  - "I don't know this name, but ask this server"
- **recursive query**
  - puts burden of name resolution on contacted name server
  - heavy load at upper levels of hierarchy?

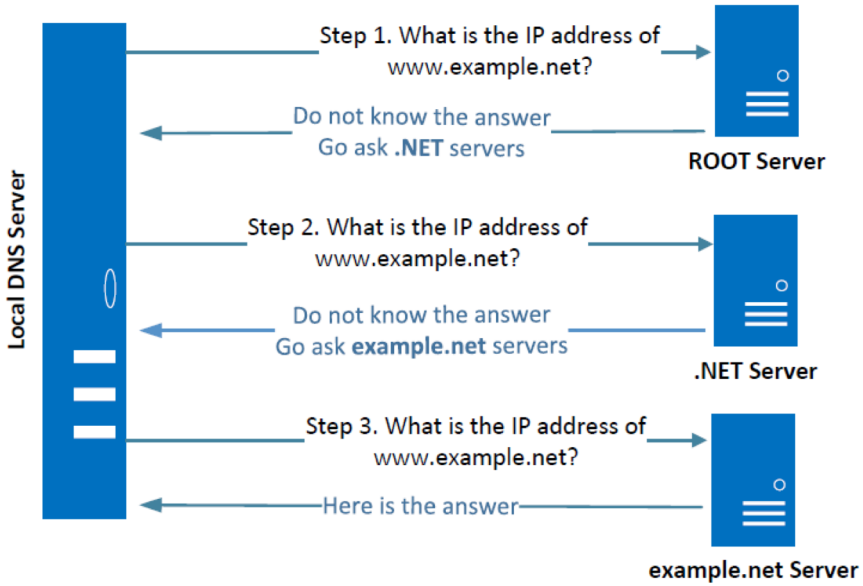




DNS Query Process



Local DNS Server and Iterative Query Process



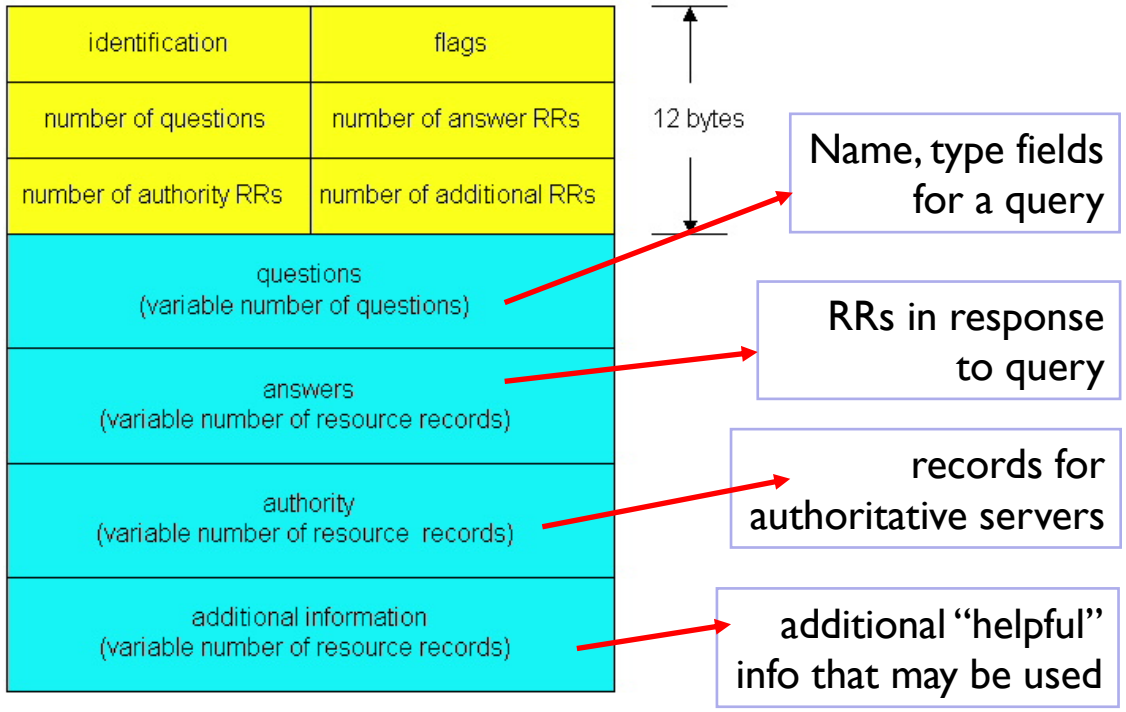
- The iterative process starts from the ROOT Server. If it doesn't know the IP address, it sends back the IP address of the nameservers of the next level server (.NET server)

DNS protocol, messages

DNS protocol : *query* and *reply* messages, both with same *message format*

msg header

- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative



DNS Response/Reply packet

There are 4 types of sections in a DNS response :

1. Question section : Describes a question to a nameserver
2. Answer section : Records that answer the question
3. Authority section : Records that point toward authoritative nameservers
4. Additional section : Records that are related to the query.

Step #1: Ask root DNS server

```
yunW_00@Client_v16(10.0.2.18):~$ dig @a.root-servers.net www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @a.root-servers.net www.example.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34523
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; AUTHORITY SECTION:
net.                    172800  IN      NS      e.gtld-servers.net.
net.                    172800  IN      NS      f.gtld-servers.net.
net.                    172800  IN      NS      m.gtld-servers.net.
net.                    172800  IN      NS      i.gtld-servers.net.
net.                    172800  IN      NS      j.gtld-servers.net.
net.                    172800  IN      NS      b.gtld-servers.net.
```

No answer (the **root** does not know the answer)

Go ask them!

```
;; ADDITIONAL SECTION:
e.gtld-servers.net.     172800  IN      A       192.12.94.30
e.gtld-servers.net.     172800  IN      AAAA    2001:502:1ca1::30
f.gtld-servers.net.     172800  IN      A       192.35.51.30
f.gtld-servers.net.     172800  IN      AAAA    2001:503:d414::30
m.gtld-servers.net.     172800  IN      A       192.55.83.30
m.gtld-servers.net.     172800  IN      AAAA    2001:501:b1f9::30
```

Step #2: Ask .net DNS server

```
yunW_00@Client_v16(10.0.2.18):~$ dig @e.gtld-servers.net www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @e.gtld-servers.net www.example.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19869
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; AUTHORITY SECTION:
example.net.            172800  IN      NS      a.iana-servers.net.
example.net.            172800  IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     172800  IN      A       199.43.135.53
a.iana-servers.net.     172800  IN      AAAA    2001:500:8f::53
b.iana-servers.net.     172800  IN      A       199.43.133.53
b.iana-servers.net.     172800  IN      AAAA    2001:500:8d::53

;; Query time: 52 msec
;; SERVER: 192.12.94.30#53(192.12.94.30)
;; WHEN: Mon Jun 22 13:29:03 EDT 2020
```

Ask a .net nameservers.

Go ask them!

Step #3 : Ask example.net DNS server

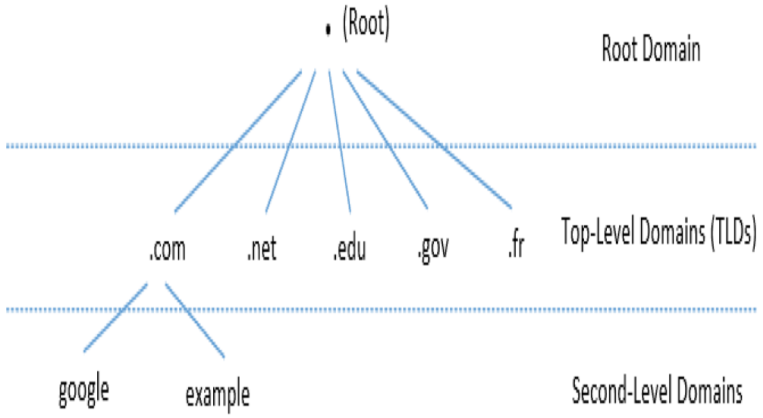
```
yunW_00@Client_v16(10.0.2.18):~$ dig @a.iana-servers.net www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @a.iana-servers.net www.example.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45430
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        86400   IN      A       93.184.216.34

;; Query time: 21 msec
;; SERVER: 199.43.135.53#53(199.43.135.53)
;; WHEN: Mon Jun 22 13:31:14 EDT 2020
;; MSG SIZE  rcvd: 60
```

Ask an example.net nameservers.

Finally got the answer

Summary and Reference

- DNS
  - DNS Record
  - Data Types
    - (A, NS, MX, CNAME)
- Hierarchy and Servers
  - Root, TLD
  - Second-Level Domains
- DNS Query Process
  - Iterative vs. Recursive
  - Protocol format (header and message)
  - Emulation on VM



Reference:

1. "Computer Security: A Hands-on Approach" by Wenliang Du. Publisher: CreateSpace Independent Publishing Platform (2017). ISBN-10: 154836794X,ISBN-13: 978-1548367947
2. "Computer Networking: A Top Down Approach", 7th edition, Jim Kurose, Keith Ross Pearson/Addison Wesley April 2016, ISBN-13: 978-0133594140, ISBN-10: 9780133594140