Domain Name System

Required reading:
Kurose 2.4

EECS 3214, Winter 2020
Instructor: N. Vlajic

DNS Overview

Internet-Host Identifiers

- **IP addresses** – unique, universal identifiers (e.g. 72.14.203.99)
  - by scanning address from left to right more and more information about specific location of host can be obtained 👍
  - difficult to remember 👎
- **symbolic (DNS) names** – unique user friendly names (e.g. www.google.com)
  - easy to remember – preferred by humans 👍
  - provide little information about host location ⇒ difficult to aggregate by routers 👎
  - consist of variable number of alphanumeric characters ⇒ difficult to process by routers 👎

Domain Name System (DNS) – enables IP address to Symbolic Name translation and vice versa.

DNS Overview (cont.)

DNS Names vs. URLs – **DNS Name ≠ URL,** **global address of a document**

- **typical URL contains three parts:**

URL = protocol + DNS name + path

http://www.cs.yorku.ca/course/4213/index.html

protocol **DNS name of Server machine** **path**

IP address

host specific

both must be globally unique
(mapping from one to another done by DNS)

Would the following URL work:

http://130.63.92.24/course/4213/index.html ???

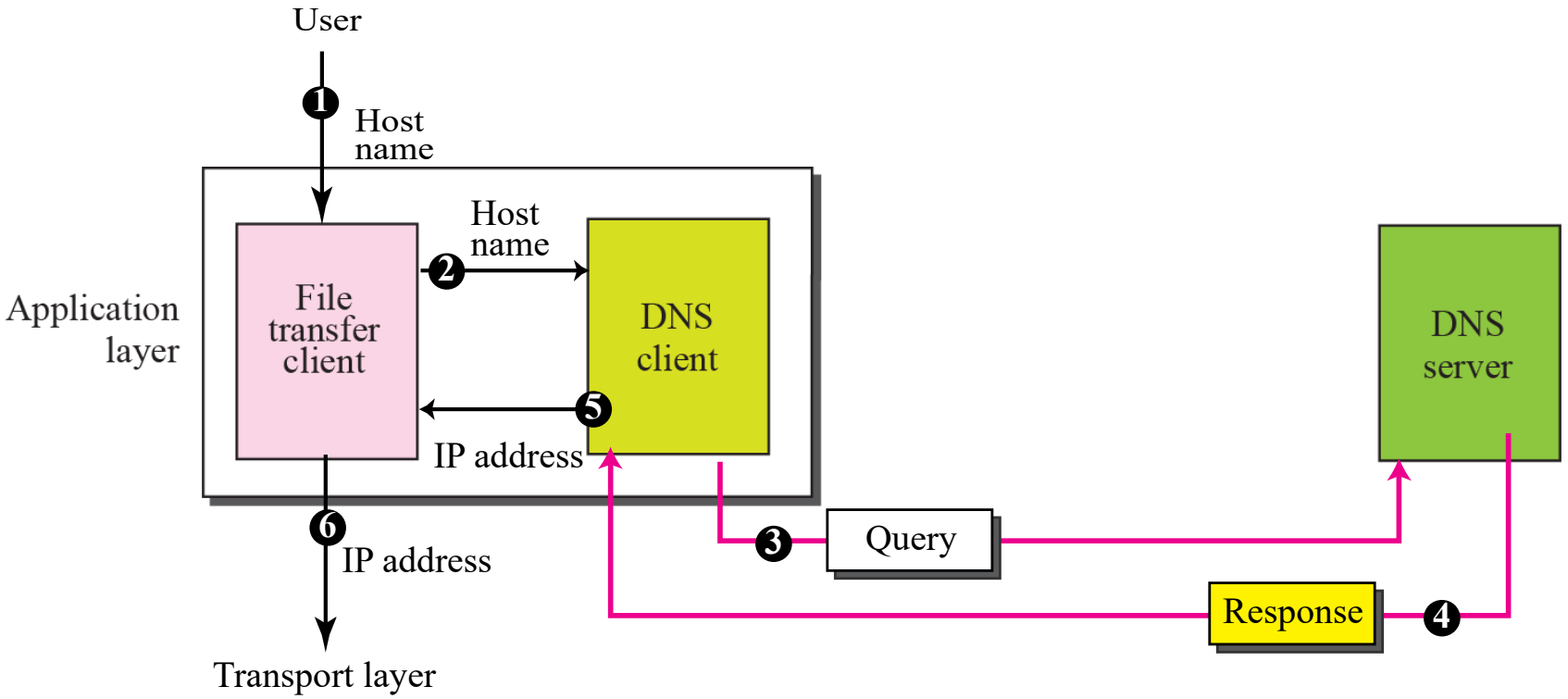
DNS Overview (cont.)

Elements of DNS

1) **distributed database** - implemented as a hierarchy of many name (DNS) servers

2) **application-layer protocol** - allows hosts to query distributed database

- runs over UDP (server on port 53)
- unlike HTTP, DNS is not an application with which users directly interact – DNS provides service to other software



DNS Overview (cont.)

DNS Services

- **Symbolic name (hostname) to IP address translation.**
- **Reverse IP address to symbolic name translation.**
- **Host aliasing – allows hosts with complicated hostnames to have one or more simpler alias names.**
  (e.g. colony.cs.utoronto.edu → web.cs.toronto.edu)
- **Mail server aliasing – allows use of mnemonic e-mail addresses (e.g. bob@hotmail.com, although the name of Hotmail mail server is more complicated, e.g. jun07.ny.hotmail.com)**
- **Load distribution. One symbolic name can be associated with a number of IP addresses, to perform load distribution. DNS servers respond with entire set of IP addresses, but rotate the ordering of addresses within each reply.**

DNS Overview (cont.)

Example **[DNS query for www.cnn.com using nslookup]**

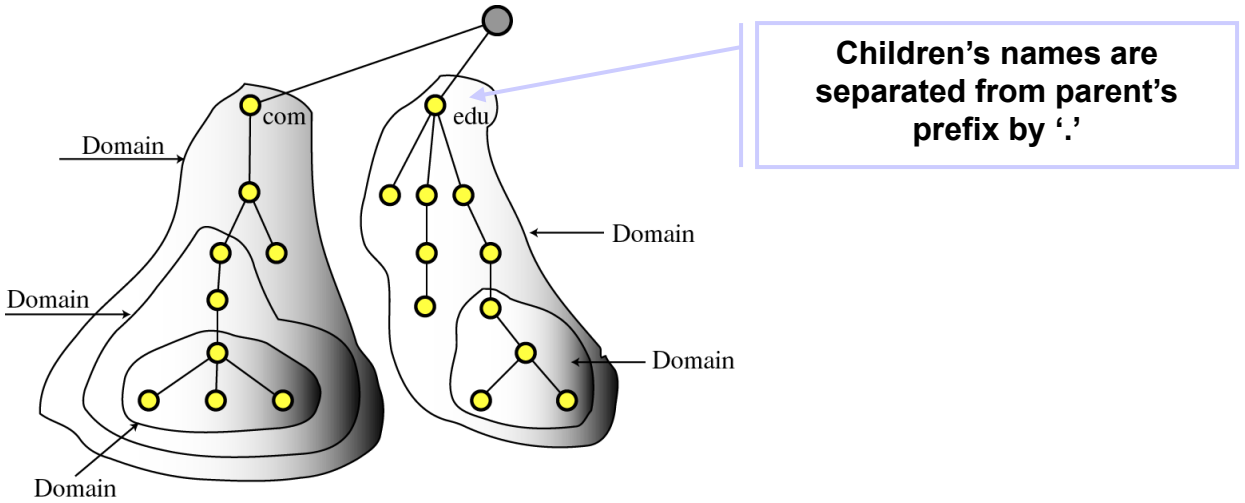
```
> cnn.com
Server:  hitronhub.home
Address:  2607:fea8:12e0:5696:ae20:2eff:fe7c:9502

Non-authoritative answer:
Name:    cnn.com
Addresses:  2a04:4e42:200::323
          2a04:4e42:400::323
          2a04:4e42::323
          2a04:4e42:600::323
          151.101.1.67
          151.101.65.67
          151.101.129.67
          151.101.193.67
```

DNS Name Space (cont.)

DNS Name Space – **hierarchical name space for the global Internet – uses dots (.) to form internal structure**

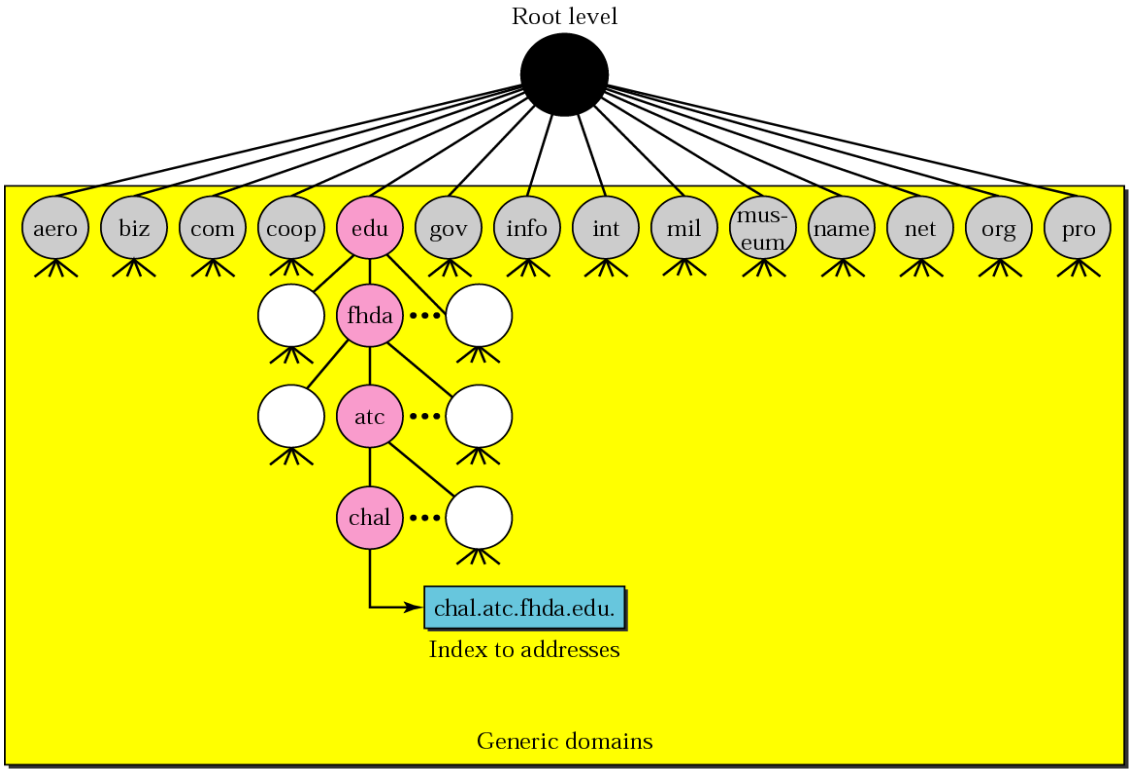
- **one additional top-level introduced comprising top-level domains**
- **properties of DNS Name Space tree:**
  1) **inverted-tree structure with an 'imaginary' root at the top**
  2) **level-one nodes = roots of domains, leaf = specific device**
  3) **up to 127 levels are possible (although more than 4 are rare)**
  4) **each node has a label with max 63 characters**
  5) **children of each node must have different labels to guarantee uniqueness of names within the given domain**

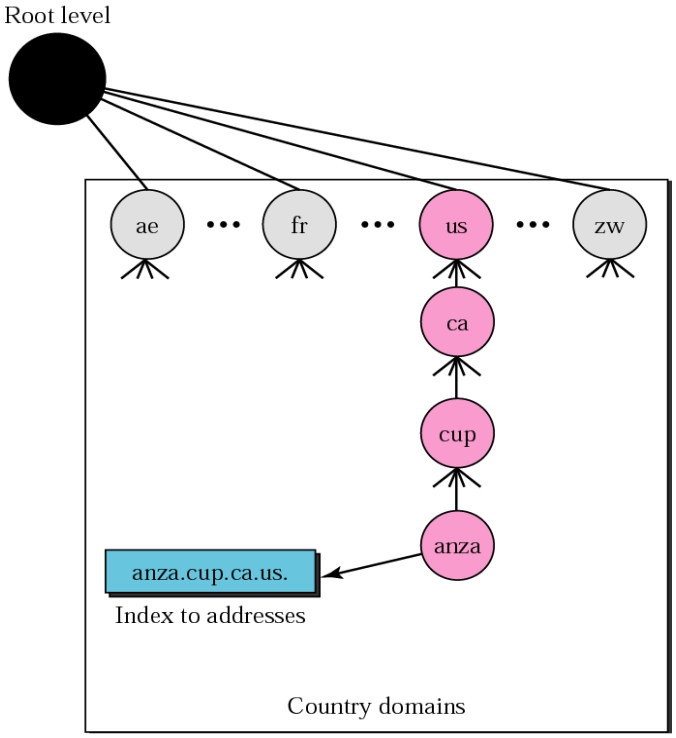


DNS Name Space (cont.)

Top Level Domains – **are divided into 2 main sections**

- **generic (organizational) domains – define their hosts according to their organization type**
- **country domains – two-character country abbreviations**





DNS Name Space (cont.)

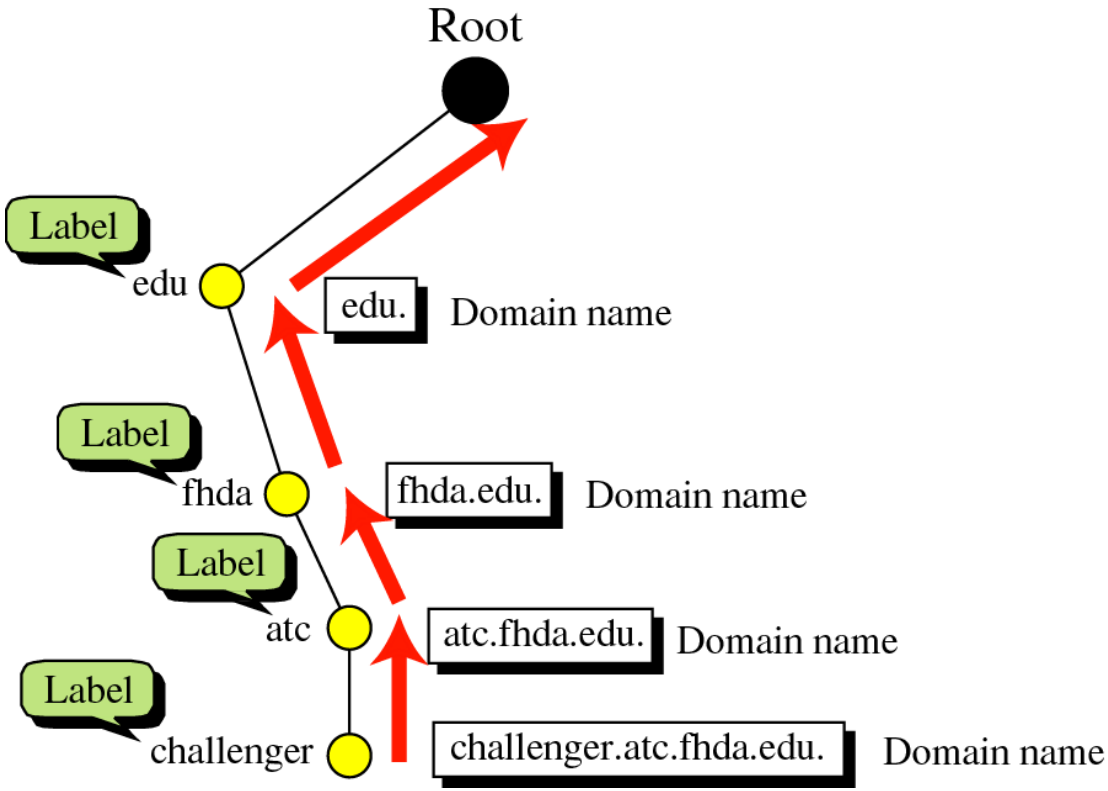
Example **[generic domain labels]**

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

DNS Name Space (cont.)

Full DNS Name – **sequence of labels from the node up to the root separated by dots (.) that uniquely identifies the given node in DNS name space**

- **DNS name space root is given a zero-length "null' label**
- **full DNS names are limited to 255 characters – most domain names are much shorter that the limit!**



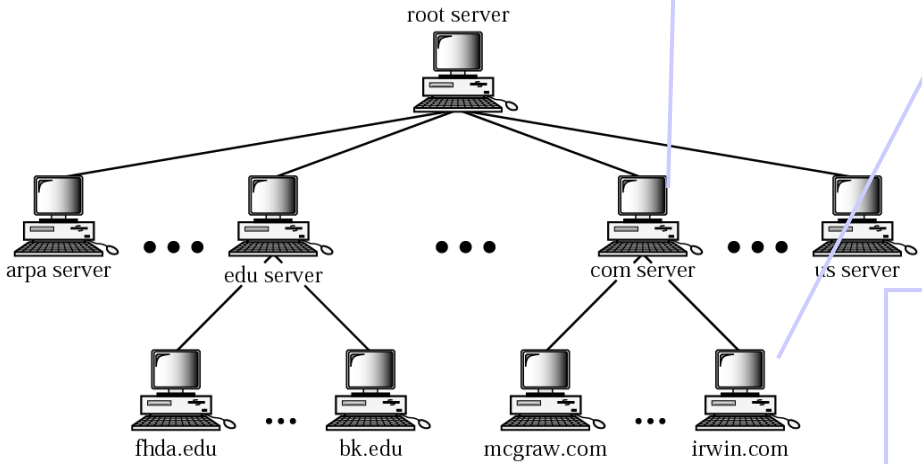
DNS Database

DNS Database – **hierarchical distributed database consisting of a large number of servers placed around the world, and partially administered by Internet Assigned Numbers Authority**

- **no single DNS server has all mappings for all hosts – mappings are divided and distributed across DNS servers**
- **hierarchy of DNS servers is organized in similar fashion as hierarchy of names:**

Root DNS server – 13 physical servers – usually does not store any info, but keep reference to TLD servers

Top-Level Domain (TLD) Servers – responsible for all top-level domains such as: com, org, net, edu, gov, and all country top-level domains: uk, fr, ca, etc.

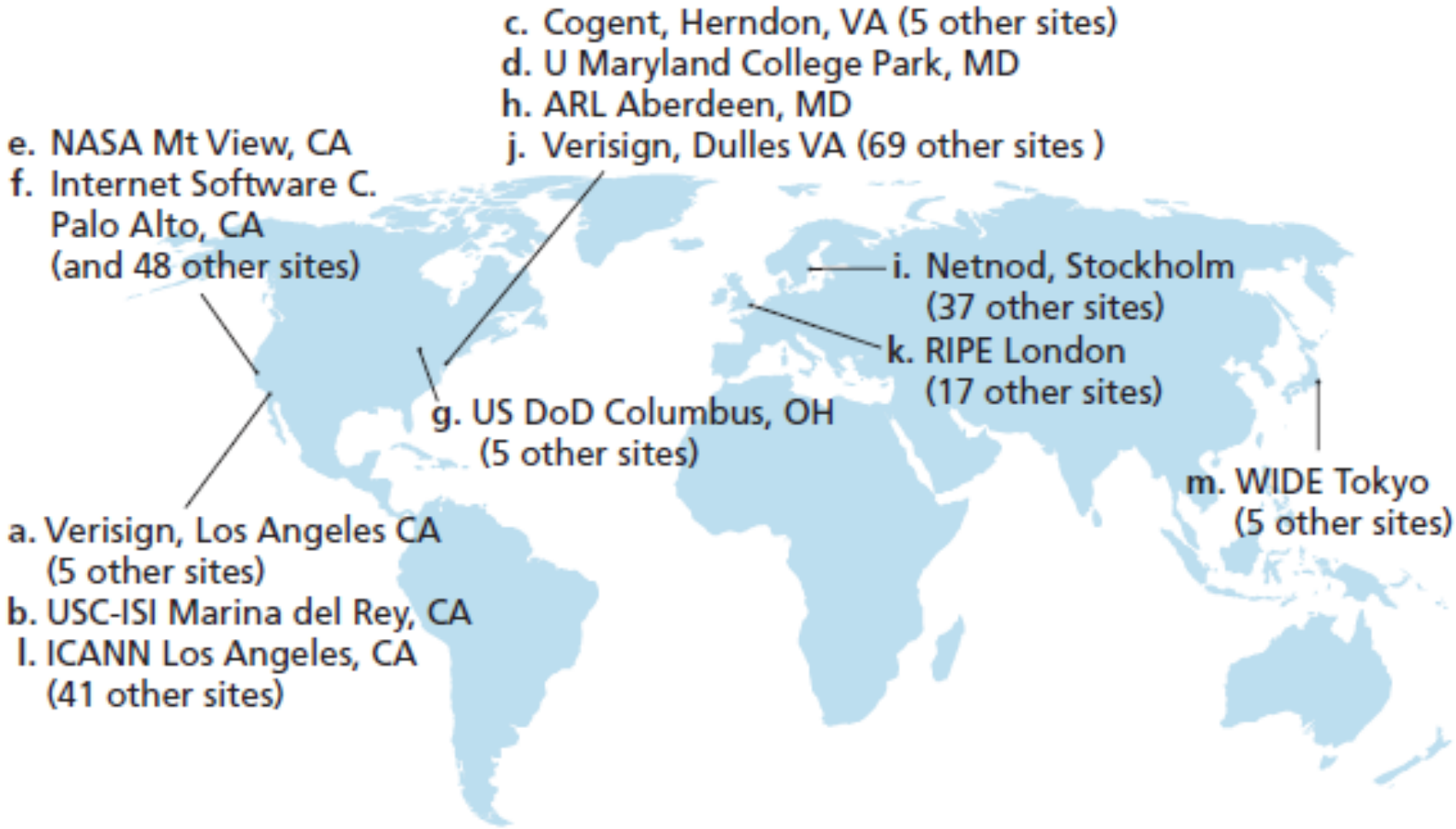


Authoritative DNS Servers – organization's DNS servers, provide hostname to IP mappings for organization's publicly accessible hosts, such as Web servers of e-mail servers.

Local DNS Servers – do not belong to hierarchy, yet crucial to DNS architecture. Each ISP (company, university, etc.) has one. Local DNS servers receive queries from hosts and (possibly) forward them into DNS hierarchy.

DNS Database (cont.)

In the internet there are 13 root DNS servers (labelled A through M), most of which are located in North America.



https://electronicspost.com/dns-servers/

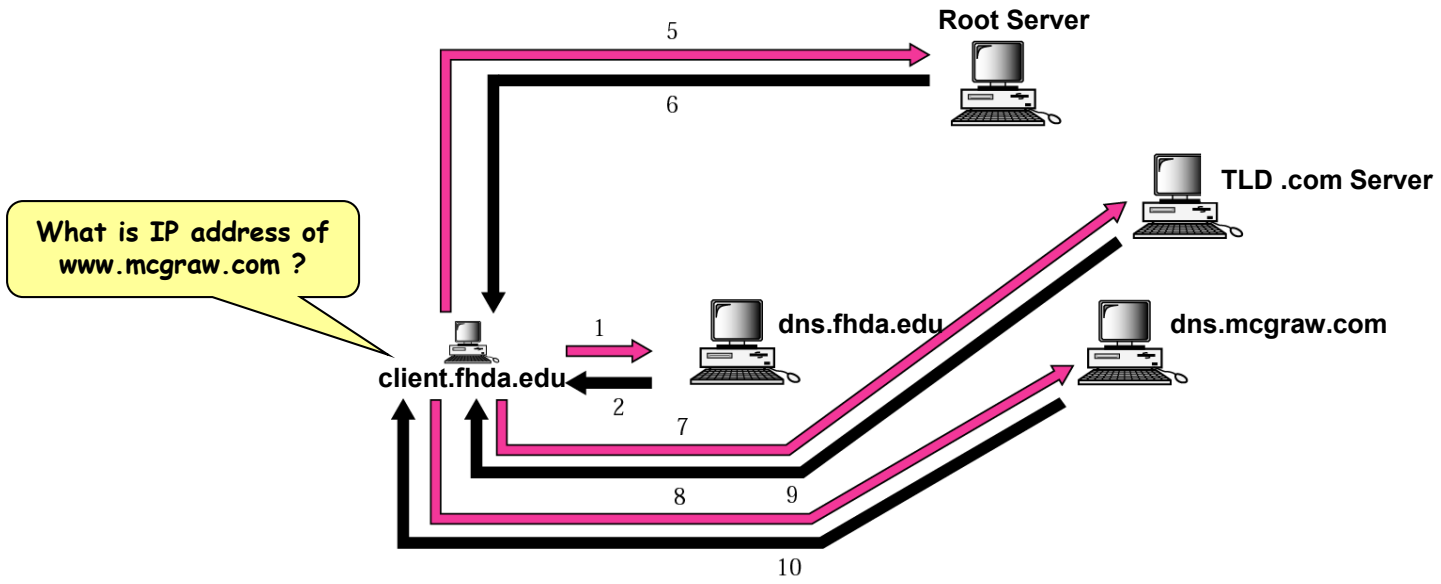
DNS Database (cont.)

Resolver – **DNS client (embedded in browser) – contacts closest local DNS server after receiving a mapping request**

- **if closest server has info it satisfies resolver; otherwise it either refers resolver to other servers or ask other servers to provide info**

Iterative Resolution – **if queried DNS server is not able to perform mapping it sends back IP address of other DNS server that it thinks can resolve query**

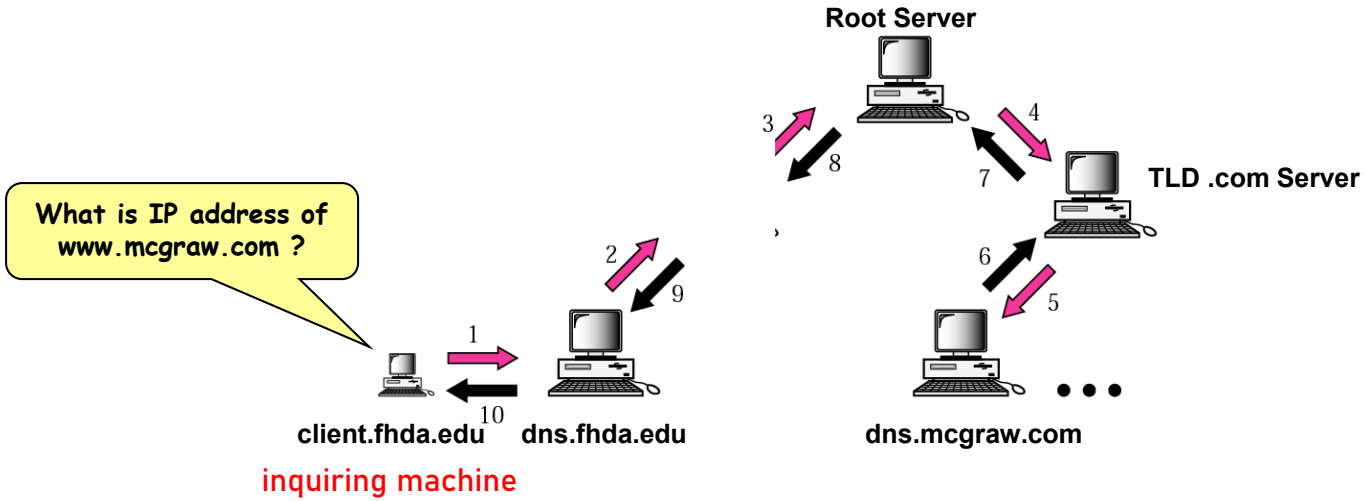
- **process is called 'iterative' since client repeats same request to multiple servers**



DNS Database (cont.)

Recursive Resolution – **if queried DNS server is not able to perform mapping itself, it forwards request to another server, waits for response, and sends response back …**

- **not all DNS servers support recursion, especially ones near the top of the hierarchy**

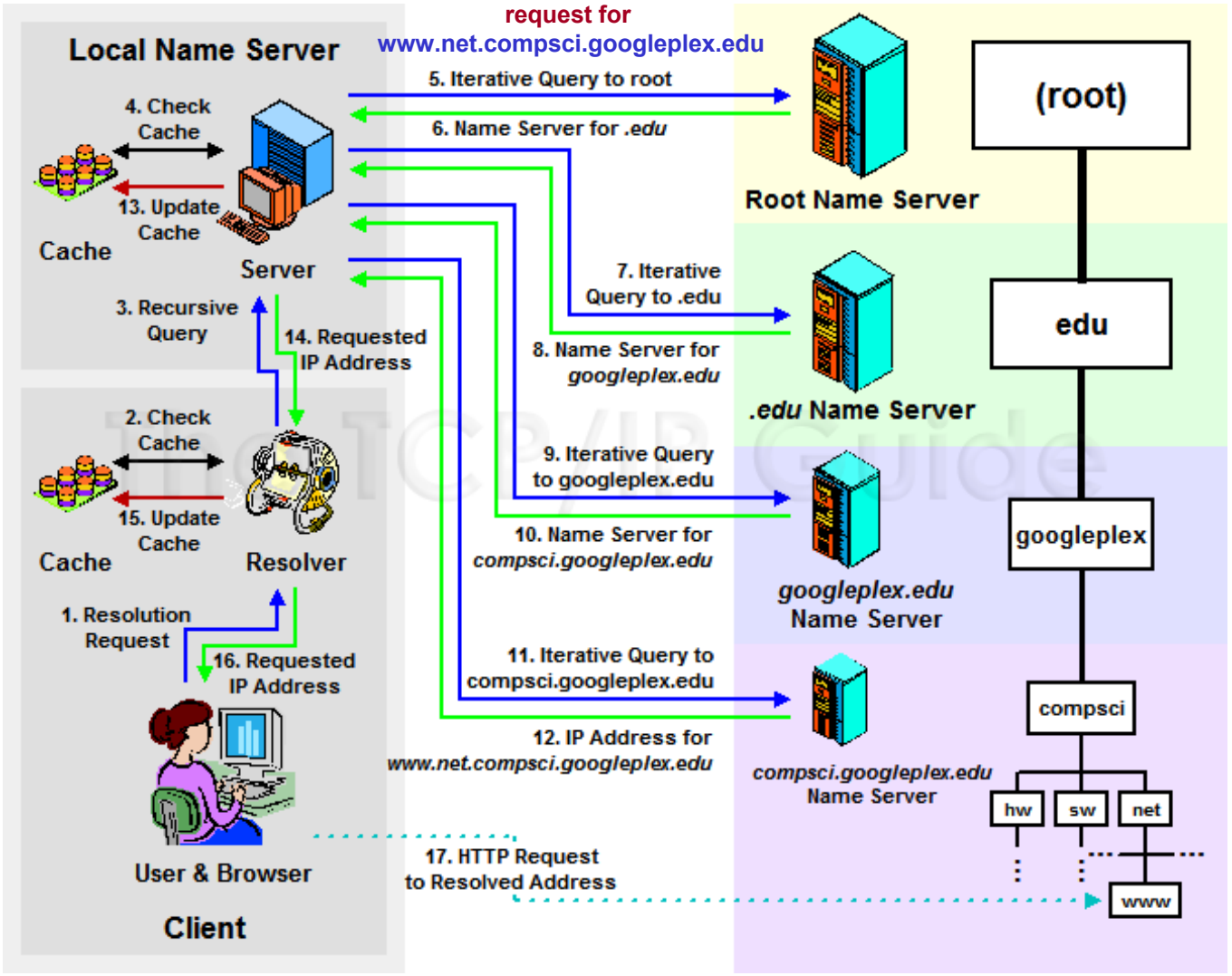


Iteration vs. Recursion – **"do job yourself" vs. "pass the buck"**

- **not all name servers support recursion, especially critical servers near the top of the hierarchy**
- **on the other hand, recursion is often supported by local DNS**

DNS Database (cont.)

Example **[combined iterative-recursive resolution]**



name resolution for **www.net.compsci.googleplex.edu**

DNS Database (cont.)

Cache – area of memory set aside for storing information that has been recently obtained so it can be used again

DNS Caching on Servers – once DNS server learns/receives a mapping it caches this mapping in local memory to speed up subsequent requests

- TLD servers are typically cached in local DNS servers, so root server is rarely queried
- hostname-IPaddress mappings are not permanent ⇒ DNS servers discard cached info after two days

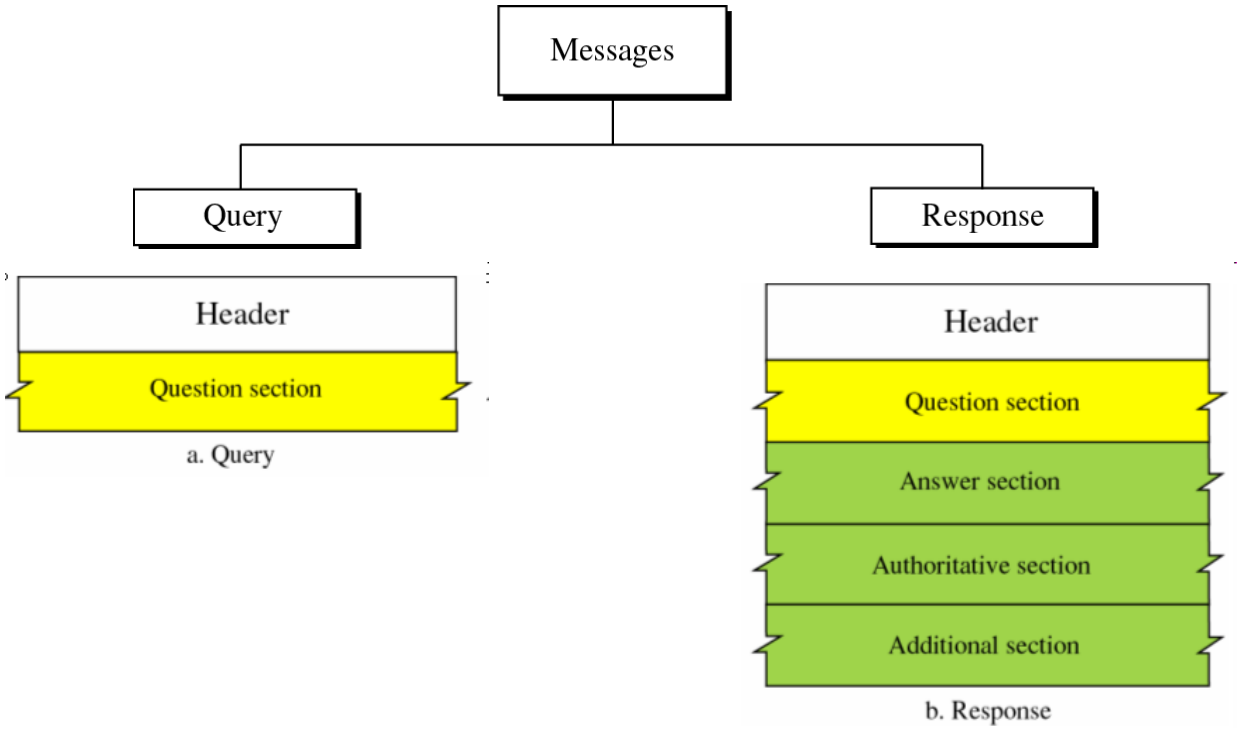
DNS Caching on Resolvers – like name servers, name resolvers (clients) can cache results to save time if same resolution is required again

- however, not all resolvers perform caching

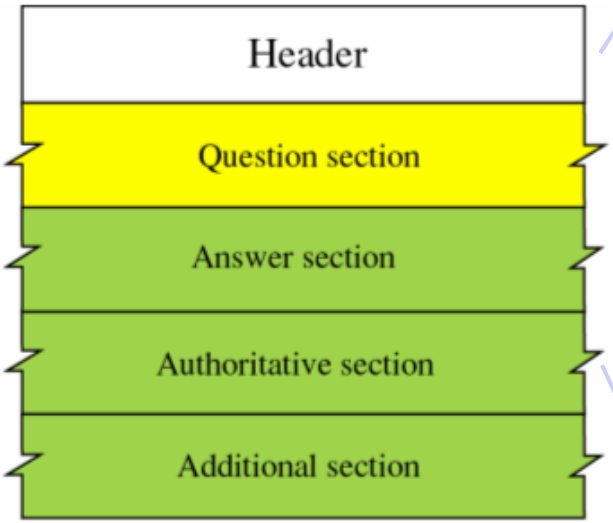
DNS Messages and Records

DNS Messages – DNS has two types of messages: **query** and **response**

- query = header + question record
- response = header + question records + answer records + authoritative records + additional records
- both query and response have the same header format with some fields set to zero for query message



DNS Messages and Records (cont.)



Contains fields that describe the type of message and provide important info about it. Also contains fields that indicate the number of entries in other sections of the message.

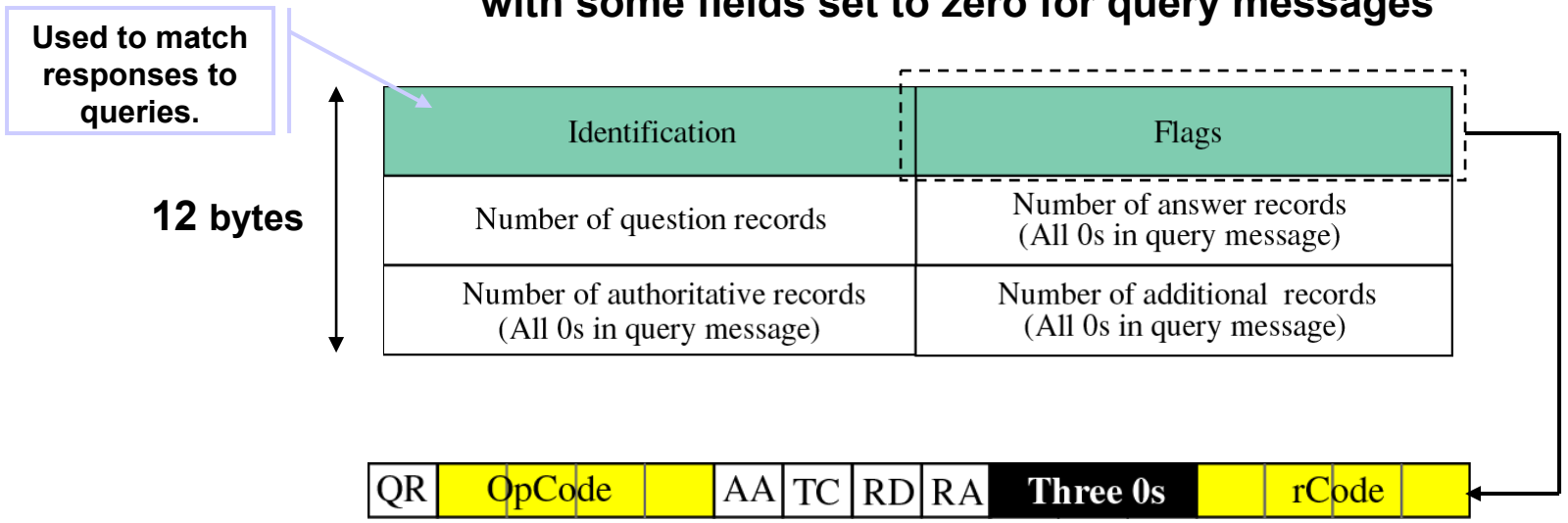
Carries one or more "questions" (i.e.) queries sent to DNS name server.

Conveys one or more resource records that answer the question indicated in the Question section.

Contains one or more resource records that point to authoritative DNS servers that can be used to continue the resolution process.

DNS Messages and Records (cont.)

DNS Header – **fixed-size (12 bytes) for both query and response message, with some fields set to zero for query messages**



QR: **Query=0, Response=1**

OpCode: **0 standard** (name to IP address), **1 inverse** (IP address to name)

AA: **Authoritative – used in response – set to 1 if authoritative server sends the message**

TC: **Truncated – message was truncated**

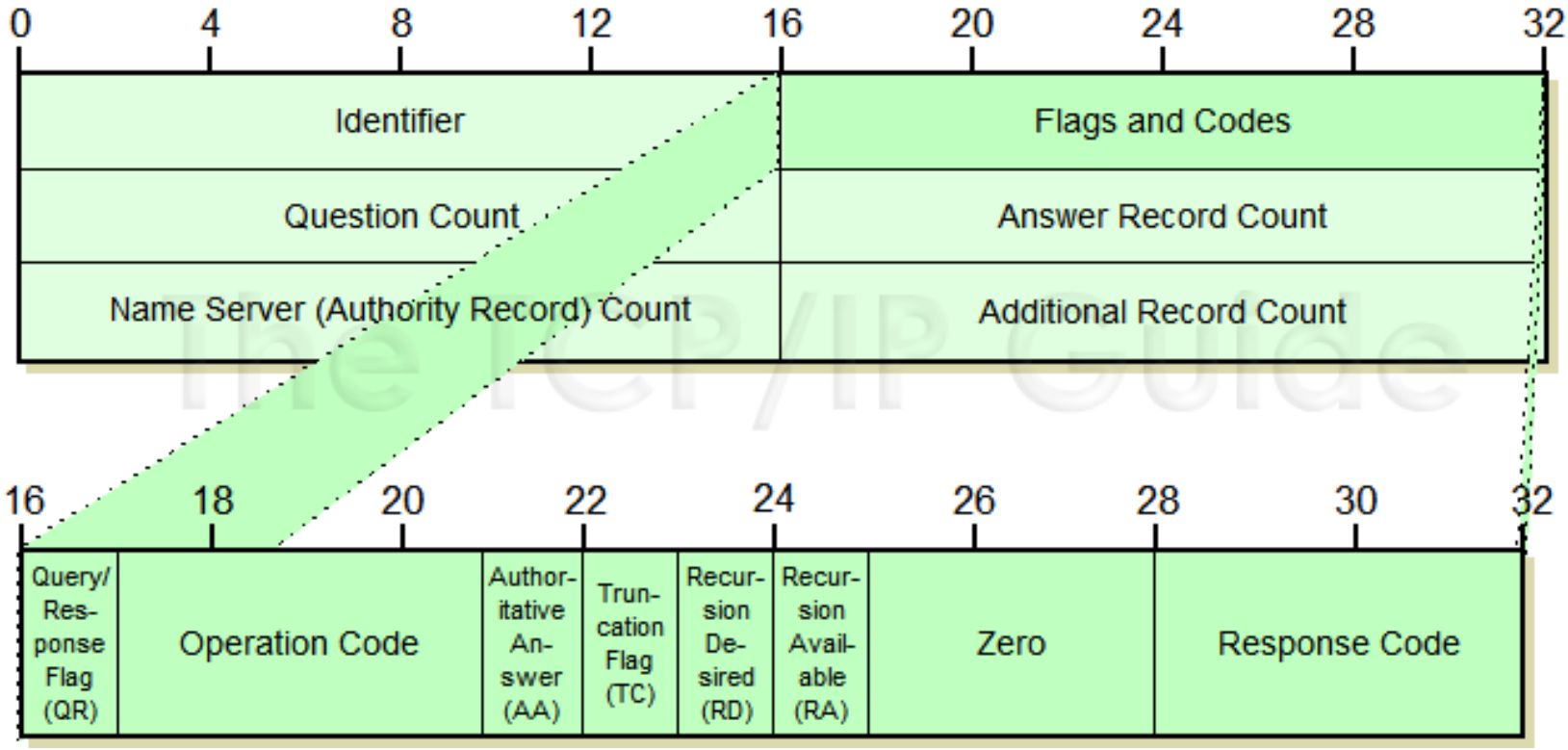
RD: **Recursion Desired – used in query – set to 1 if client desires a recursive answer**

RA: **Recursion Available – used in response – indicates that response is recursive**

rCode: **Error Status – used in response to indicate that query had error / was illegal**

DNS Messages and Records (cont.)

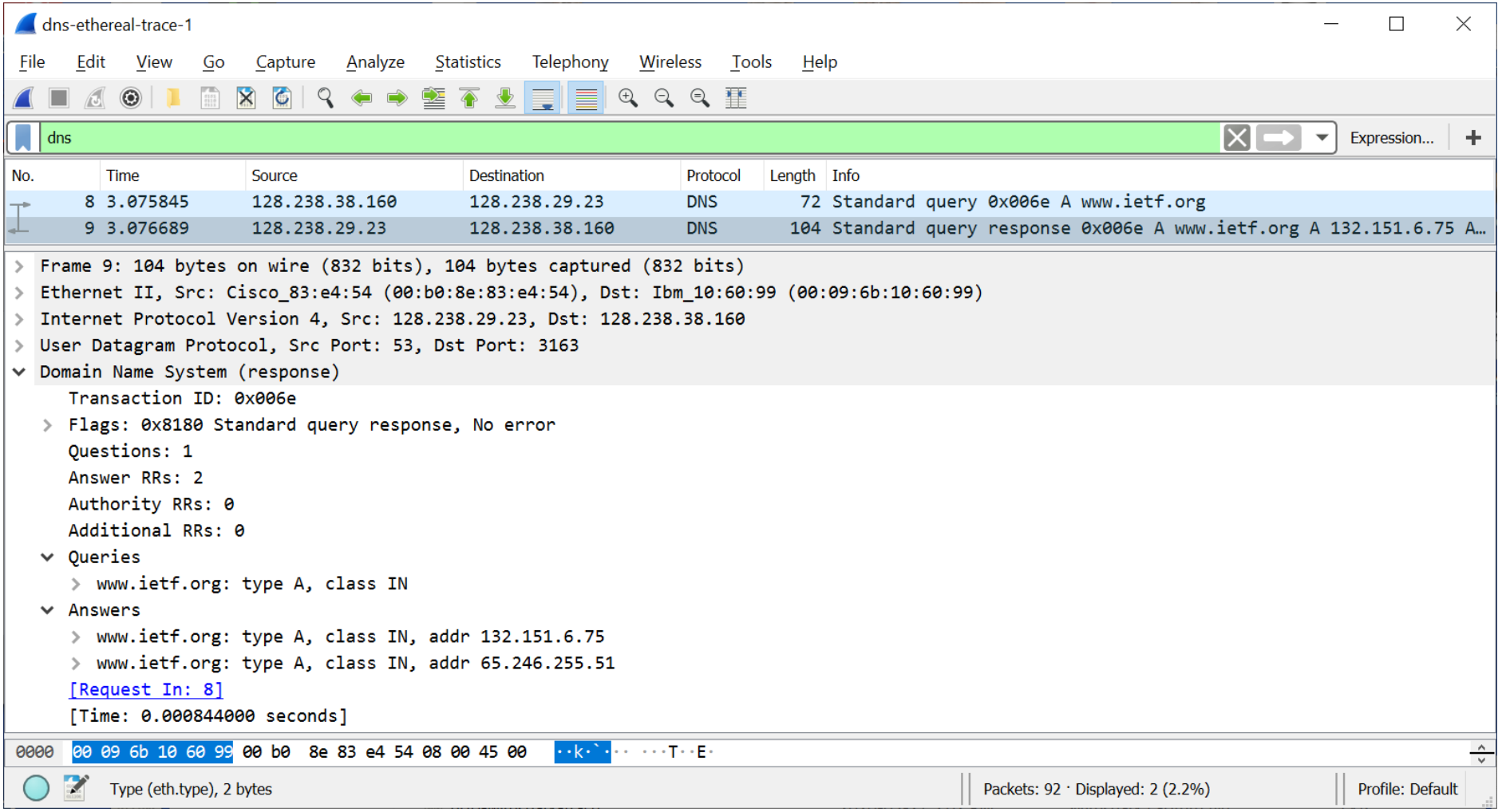
Example **[Fields of DNS Header]**



http://www.tcpipguide.com/free/t_DNSMessageHeaderandQuestionSectionFormat.htm

DNS Messages and Records (cont.)

Example [DNS query for www.ietf.org]



DNS Messages and Records (cont.)

Example **[DNS query for www.ietf.org: details of Flags in DNS Response message]**