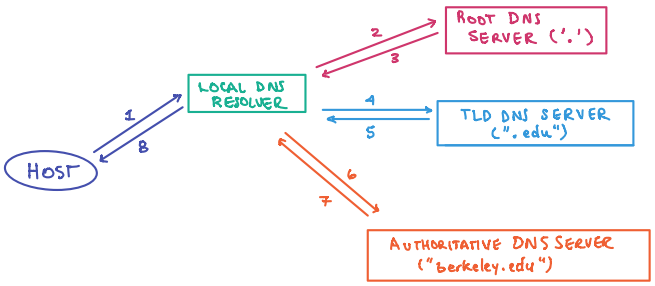
## REVIEW: DNS → Domain Name Service

eecs.berkeley.edu ⟶ 172.23.253.47




## Other Notes:

- Domain-name registrars allow the registration of domain names (accredited by ICANN)
- Name Servers = DNS Servers
- DIG: a program that allows querying the DNS System.

## dig eecs.berkeley.edu

TRANSACTION ID: MATCHES RESPONSE TO REQUEST

```
; <<>> DiG 9.10.6 <<>> eecs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18809
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;eecs.berkeley.edu.             IN      A

;; ANSWER SECTION:
eecs.berkeley.edu.      86173   IN      A       23.185.0.1

;; Query time: 17 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Jul 22 11:27:36 PDT 2020
;; MSG SIZE  rcvd: 62
```

QUESTION SECTION: the query we sent the server

Cache Time

TTL

A = IP Address

NS = Name Server

## DNS SECURITY RISKS

- Malicious Name Server
- On-Path Attacker
- Off-Path Attacker: Blind Spoofing
  - ↳ Randomize ID Field?
  - ↳ KAMINSKY ATTACK!
    - ↳ Randomize Destination Port

## DNS Security: DNSSec

Idea: use a certificate chain to validate responses

Root key is hardcoded

Children signed with parent's secret key

Caveat: because signing is expensive, we need to do something special for "No Record" responses

→ Return Consecutive Valid Domains, signed...