Exploring DNS

- dig
  - Should be available by default on macOS
  - Part of “bind” package on Linux (and if brave enough, on Windows)
  - https://www.digwebinterface.com/

Searching the Truth (1/2)

```
✔  22:39 ~ $ dig +noall +answer amazon.com a @8.8.8.8
amazon.com.             39      IN      A       54.239.17.7
amazon.com.             39      IN      A       54.239.25.200
amazon.com.             39      IN      A       54.239.26.128
amazon.com.             39      IN      A       54.239.25.208
amazon.com.             39      IN      A       54.239.17.6
amazon.com.             39      IN      A       54.239.25.192
```

```
✔  22:35 ~ $ dig +noall +answer amazon.com a @131.179.196.160
amazon.com.             3600    IN      A       54.239.26.128
amazon.com.             3600    IN      A       54.239.17.7
amazon.com.             3600    IN      A       54.239.17.6
amazon.com.             3600    IN      A       54.239.25.208
amazon.com.             3600    IN      A       54.239.25.192
amazon.com.             3600    IN      A       54.239.25.200
```

Searching the Truth (2/2)

```
✔ 22:35 ~ $ dig +noall +answer www.amazon.com a @8.8.8.8
www.amazon.com.           1461    IN      CNAME   www.cdn.amazon.com.
www.cdn.amazon.com.       238     IN      CNAME
        d3ag4hukkh62yn.cloudfront.net.
d3ag4hukkh62yn.cloudfront.net. 59 IN      A       54.230.140.143
d3ag4hukkh62yn.cloudfront.net. 59 IN      A       54.230.140.28
d3ag4hukkh62yn.cloudfront.net. 59 IN      A       54.230.140.212
d3ag4hukkh62yn.cloudfront.net. 59 IN      A       54.230.140.148
```

```
✔  22:35 ~ $ dig +noall +answer www.amazon.com a @131.179.196.160
www.amazon.com.           3600    IN      A       131.179.196.70
```

DNS “Features”

- Depending on which caching resolver you ask, the result may not be the same
  - Some resolvers can simply lie
    - WiFi captive portals
  - Some resolvers are legitimately configured to give different results when asked by different consumers
    - Direct traffic from customers on east coast to the replica on east coast
    - From customers in France to servers in France
    - …

DNS Problems & Fixes

- **What can go wrong with DNS protocol**
  - FYI Reading assignment
    - http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

- DNS Security Extension (DNSSEC)
  - Each Resource Record set is signed with a cryptographic signature
  - Bad guys should not be able to create face DNS records
  - Only partial deployment ☹
  - Optional ☹
  - Stub resolvers don't do actual verification, allowing caching resolvers to lie ☹

Revised DNS Scavenger Hunt Challenge for This Week (Until Monday)

- As I mentioned, depending on which caching resolver you ask, result may be (legitimately) different, as is in case of google.com
- Your task
  - Find 20 or more valid A records for “google.com” domain
  - Show dig command you used to get A record
  - For each found A record
    - very gross estimate how far is that server (using ping)
      - 200,000 km/s * ping time / 2
    - How many hops (using traceroute)
    - If you can / possible at all, which country / continent

For you to start

- dig +short google.com a @8.8.8.8
  - 172.217.5.78
  - 12ms ping ~ within 750 miles
  - 14 hops (~ in Los Angeles, based on lax17s15-in-f78.1e100.net)
- dig +short google.com a @92.62.96.27
  - 216.58.211.142
  - 179ms ping ~ within 11,187 miles
  - 25 hops (~ may be in Stockholm, based on arn09s10-in-f14.1e100.net)