To find out where www.yahoo.com is:
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let's ask the root!

```
10.10.0.47
```

The root tells me a.gtld-servers.net is responsible for com.
The root also told me what that server’s IP addresses are.
a.gtld-servers.net tells me ns1.yahoo.com is responsible for yahoo.com.
It also told me what ns1.yahoo.com's IP addresses are.
ns1.yahoo.com tells me new-fp-shed.wg1.b.yahoo.com is a CNAME to new-fp-shed.wg1.yahoo.com, and that yf1.yahoo.com is responsible for wg1.b.yahoo.com.
It also told me what yf1.yahoo.com's IP address is.
yf1.yahoo.com finally tells me the IP addresses for new-fp-shed.wg1.b.yahoo.com.
To find out where www.yahoo.com is:
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let’s ask the root! 10.10.0.47
To find out where www.yahoo.com is:
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let's ask the root!

magic happens
This file holds the information on root name servers needed to initialize cache of Internet domain name servers (e.g. reference this file in the "cache . <file>") configuration file of BIND domain name servers).

This file is made available by InterNIC under anonymous FTP as

file /domain/named.cache
on server FTP.INTERNIC.NET
-OR- RS.INTERNIC.NET

last update: March 17, 2021
related version of root zone: 2021031701

FORMERLY NS.INTERNIC.NET

<table>
<thead>
<tr>
<th></th>
<th>3600000</th>
<th>NS</th>
<th>A.ROOT-SERVERS.NET.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.ROOT-SERVERS.NET.</td>
<td>3600000</td>
<td>A</td>
<td>198.41.0.4</td>
</tr>
<tr>
<td>A.ROOT-SERVERS.NET.</td>
<td>3600000</td>
<td>AAAA</td>
<td>2001:503:ba3e::2:30</td>
</tr>
</tbody>
</table>

FORMERLY NS1.ISI.EDU

<table>
<thead>
<tr>
<th></th>
<th>3600000</th>
<th>NS</th>
<th>B.ROOT-SERVERS.NET.</th>
</tr>
</thead>
</table>
As of 03/19/2021 6:26 p.m., the root server system consists of 1375 instances operated by the 12 independent root server operators.

The 13 root name servers are operated by 12 independent organisations.

You can find more information about each of these organisations by visiting their homepage as found in the 'Operator' field below.
istheinternetonfire.com descriptive text "SUNBURST, when CoyzBear brings the SolarWinds of Change to Orion. Supply chain attack hits FireEye and several US agencies. https://is.gd/7h653D https://is.gd/UancjH"

$ host -t SSHFP cs615asa.netmeister.org

host cs615asa.netmeister.org has SSHFP record 3 2 FC1B7508B10CB3B620A778ABC904FA7FAC532B36EF8661A82C32B2683A7077CB
host cs615asa.netmeister.org has SSHFP record 1 2 99C8F90C26B4F4BF84DF2E5CD22EF93798C78B7E396F307354FEF50230009233
host cs615asa.netmeister.org has SSHFP record 4 2 903EC782A775EE5BAB46837A4AAFB43A23FC7E17F099B7665624212E6CA0CAEAE

$ host www.stevens.edu

www.stevens.edu is an alias for www.stevens.edu.cdn.cloudflare.net.
www.stevens.edu.cdn.cloudflare.net has address 104.16.126.51
www.stevens.edu.cdn.cloudflare.net has address 104.16.125.51

$ host www.cs.stevens.edu

www.cs.stevens-tech.edu has address 155.246.56.11

$ sudo tcpdump -w /tmp/dns.pcap port 53 > /dev/null 2>&1 &

$ host -t ptr 155.246.56.11

$ fg

$ sudo tcpdump -w /tmp/dns.pcap port 53 > /dev/null

^C$
Frame 1: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)

- User Datagram Protocol, Src Port: 64203, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0xbd3e
  - Flags: 0x0000 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 1
  - Queries
    - Additional records
    - <Root>: type OPT
  - [Response In: 2]

The response to this DNS query is in this frame (dns.response_in)
:: global options: +cmd
:: Got answer:
:: -->HEADER<<- opcode: QUERY, status: NOERROR, id: 44865
:: flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1220
; COOKIE: 87860020d440145e0100000060552779e8fce01404c9c11e (good)
:: QUESTION SECTION:
;www.iana.org.

:: ANSWER SECTION:
www.iana.org. 3600 IN CNAME ianawww.vip.icann.org.
ianawww.vip.icann.org. 30 IN A 192.0.32.8

:: Query time: 466 msec
:: SERVER: ::1#53 (::1)
:: WHEN: Fri Mar 19 22:36:41 UTC 2021
:: MSG SIZE rcvd: 120

$ fg
sudo tcpdump -w /tmp/dns.pcap port 53 > /dev/null
$ ^C
dumps tcpdump -w /tmp/dns.pcap port 53 > /dev/null 2>&1 &
$
Frame 2: 100 bytes on wire (864 bits), 100 bytes captured (864 bits)
> User Datagram Protocol, Src Port: 54392, Dst Port: 53

Transaction ID: 0xde9d
> Flags: 0x0000 Standard query
> Questions: 1
> Answer RRs: 0
> Authority RRs: 0
> Additional RRs: 1

> Queries
> <Additional records
> <Root>: type OPT

[Response In: 4]
DNS Implications and Considerations

• information from the DNS is used for authentication, authorization, and as a source of truth
• DNSSEC is not widely deployed and carries implementation challenges
• DNSSEC, DoT, and DoH each solve different problems
• DNS traffic is ubiquitous, may escape ACLs and restrictions
• faulty information can lead to unexpected and difficult to troubleshoot failures
• TTLs and caches can prolong outages as you wait for propagation of changes
• if you pwn the DNS, you pwn the entire target
• any time you outsource something, you lose control
• any time you own solving a problem, you assert that you know how to solve this better than others
Links

• https://en.wikipedia.org/wiki/Chaosnet
• https://www.isc.org/f-root/
• https://root-servers.org/
• https://www.iana.org/domains/root/files
• https://www.netmeister.org/blog/doh-dot-dnssec.html