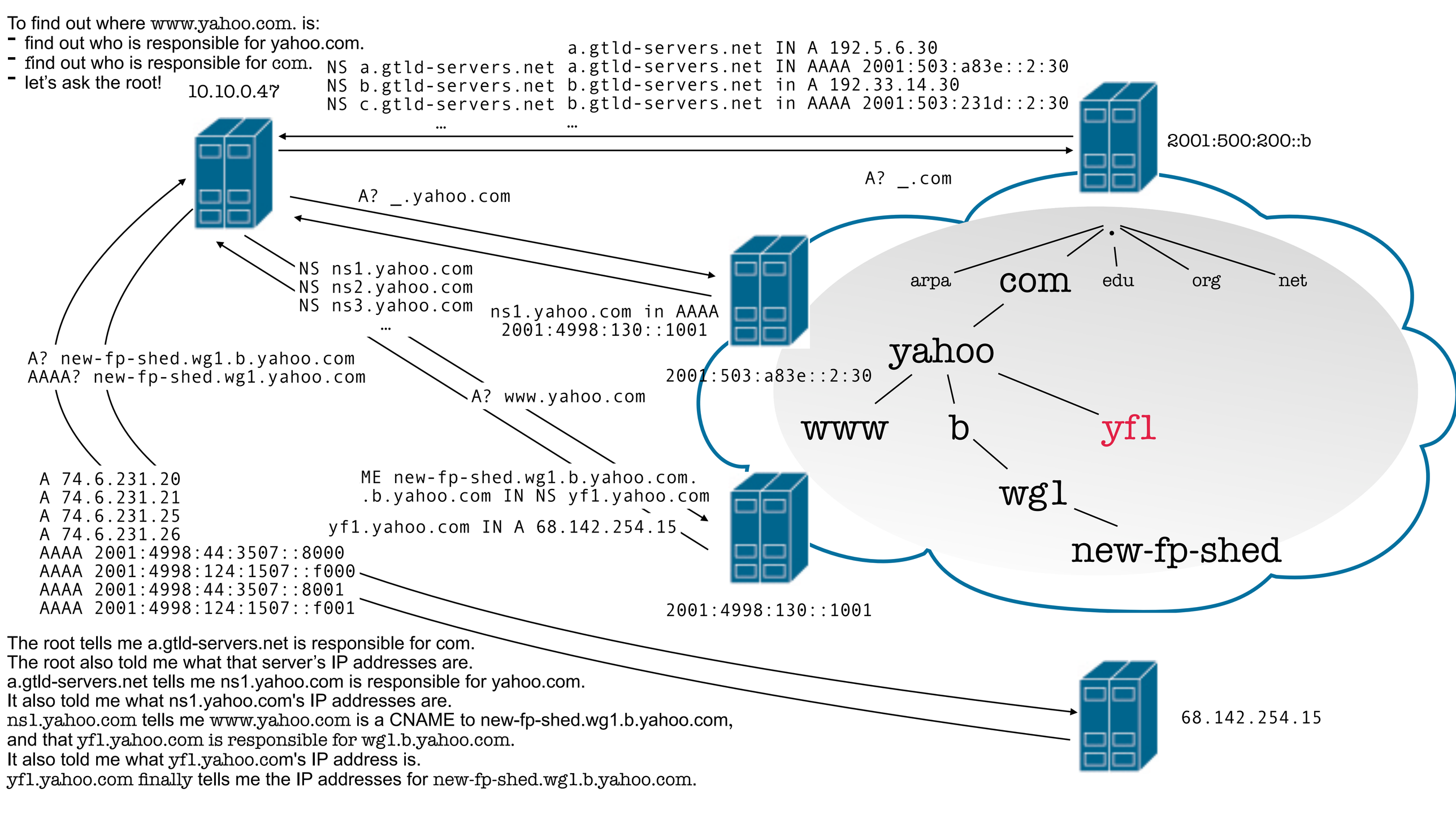
https://commons.wikimedia.org/wiki/File:Telefonbog_ubt-1.JPG
Photograph by Tomasz Sienicki

System Administration

Week 07, Segment 3
The Domain Name System, Part III

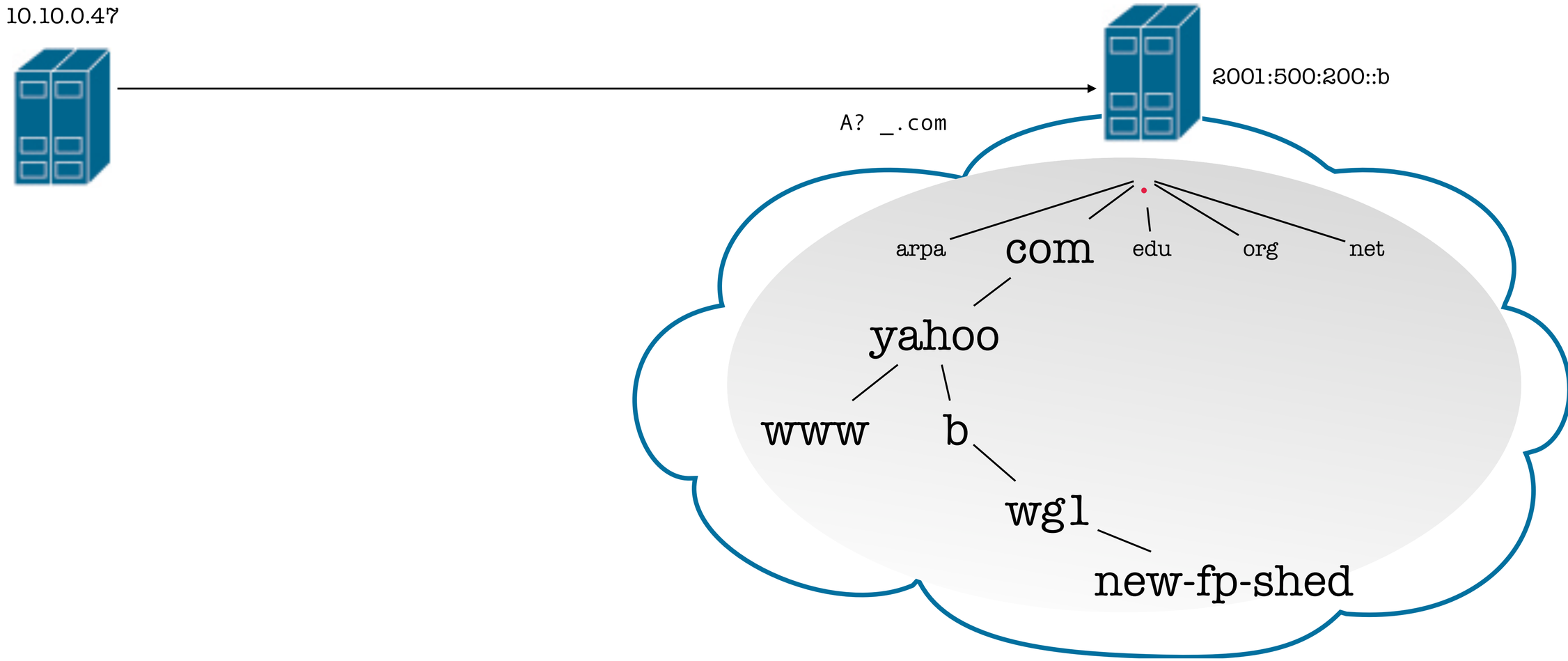
Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

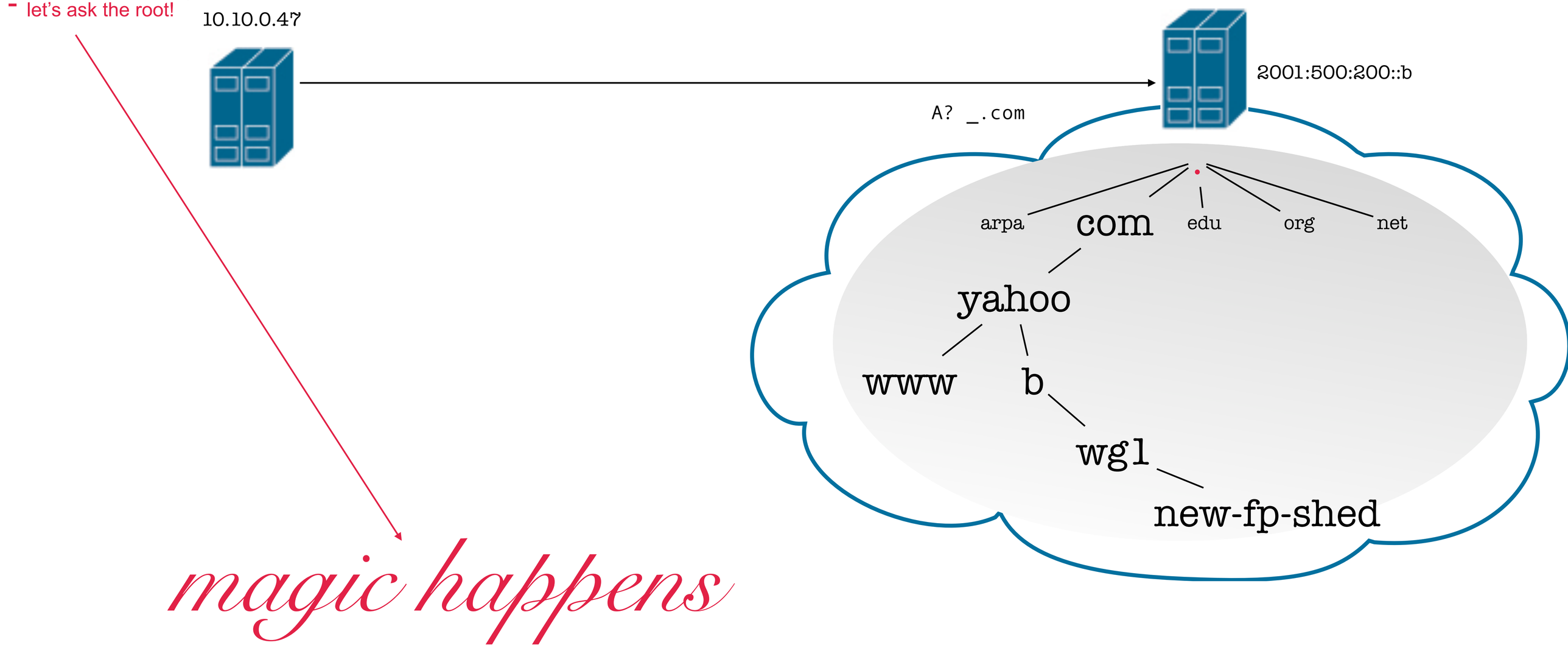

To find out where www.yahoo.com. is:
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let's ask the root!
10.10.0.47
NS a.gtld-servers.net
NS b.gtld-servers.net
NS c.gtld-servers.net
…
a.gtld-servers.net IN A 192.5.6.30
a.gtld-servers.net IN AAAA 2001:503:a83e::2:30
b.gtld-servers.net in A 192.33.14.30
b.gtld-servers.net in AAAA 2001:503:231d::2:30
…
2001:500:200::b
A? _.com
A? _.yahoo.com
NS ns1.yahoo.com
NS ns2.yahoo.com
NS ns3.yahoo.com
…
ns1.yahoo.com in AAAA
2001:4998:130::1001
2001:503:a83e::2:30
A? new-fp-shed.wg1.b.yahoo.com
AAAA? new-fp-shed.wg1.yahoo.com
A? www.yahoo.com
ME new-fp-shed.wg1.b.yahoo.com.
.b.yahoo.com IN NS yf1.yahoo.com
yf1.yahoo.com IN A 68.142.254.15
A 74.6.231.20
A 74.6.231.21
A 74.6.231.25
A 74.6.231.26
AAAA 2001:4998:44:3507::8000
AAAA 2001:4998:124:1507::f000
AAAA 2001:4998:44:3507::8001
AAAA 2001:4998:124:1507::f001
2001:4998:130::1001
.
arpa
com
edu
org
net
yahoo
www
b
yfl
wg1
new-fp-shed
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 www.yahoo.com is a CNAME to new-fp-shed.wg1.b.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.
68.142.254.15

To find out where www.yahoo.com. is:

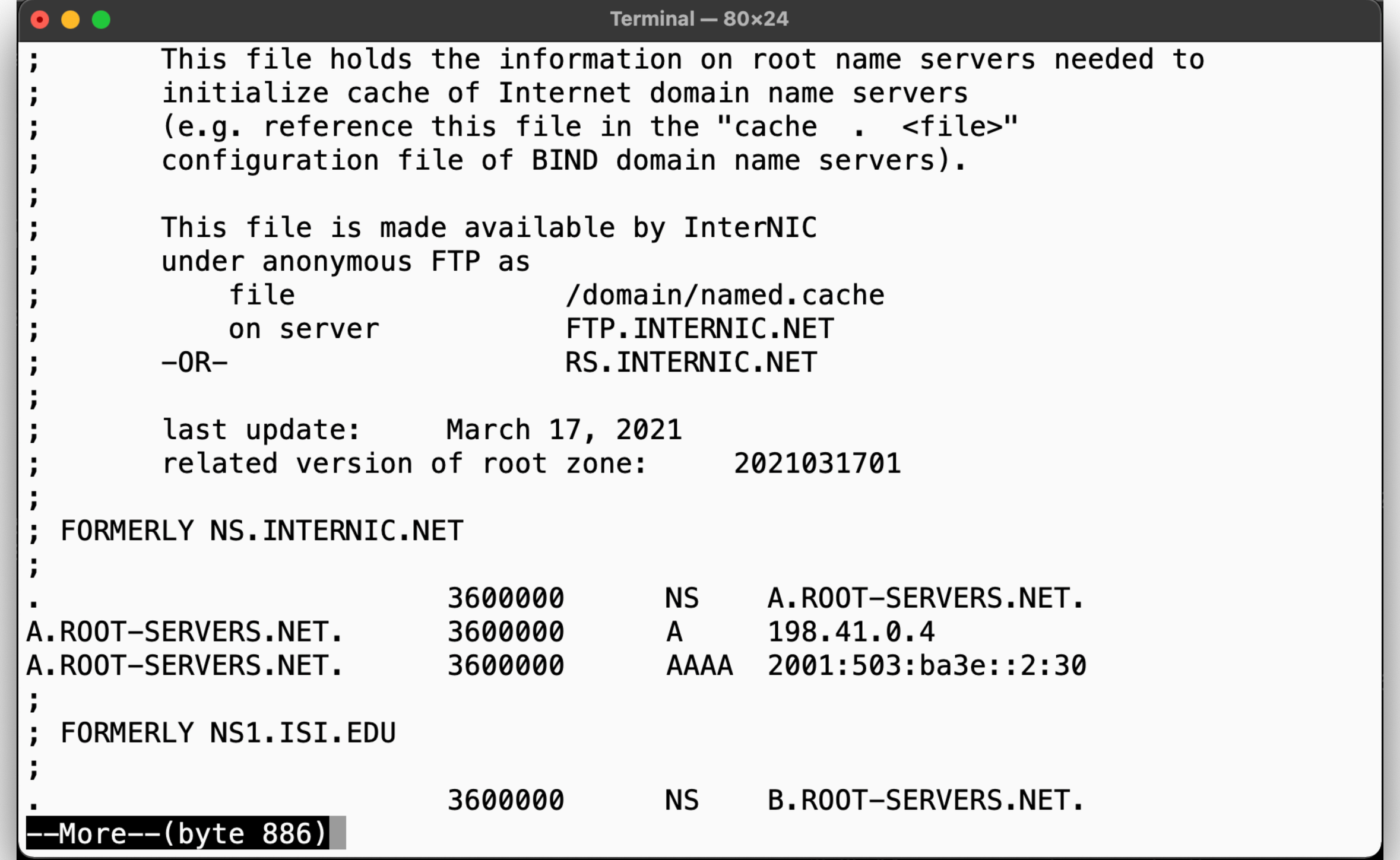
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let's ask the root!

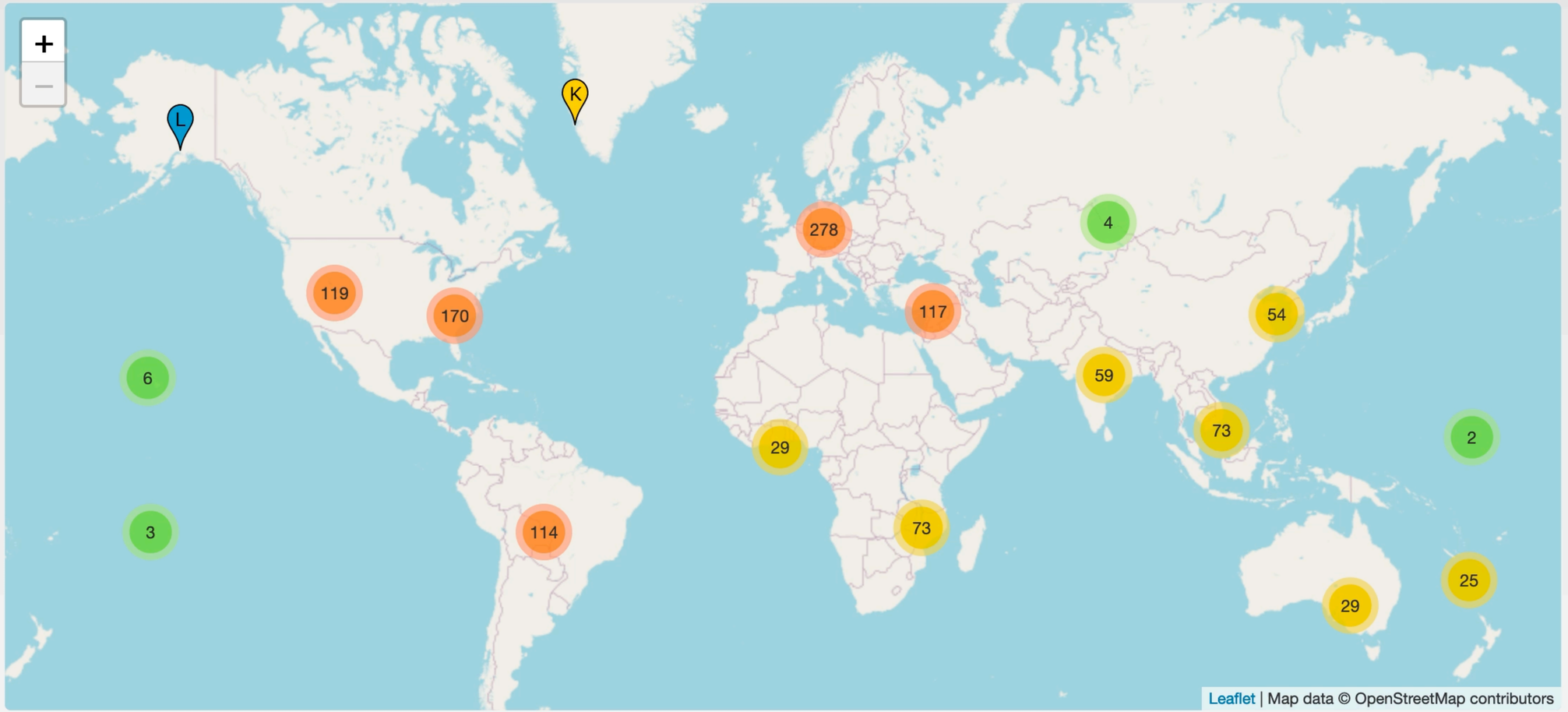


To find out where www.yahoo.com. is:
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let's ask the root!



magic happens

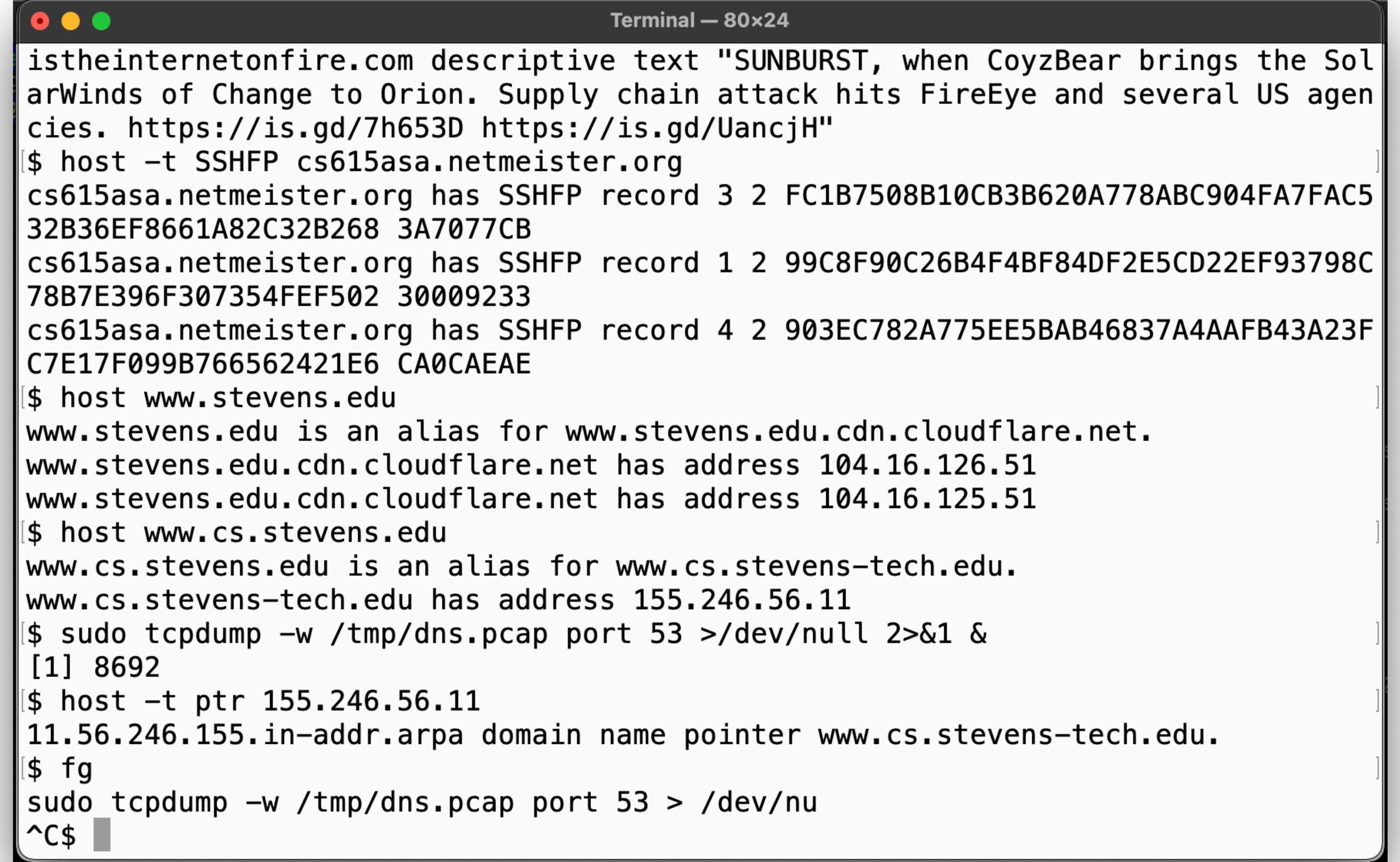

Terminal — 80×24
;   This file holds the information on root name servers needed to
;   initialize cache of Internet domain name servers
;   (e.g. reference this file in the "cache . <file>"
;   configuration file of BIND domain name servers).
;
;   This file is made available by InterNIC
;   under anonymous 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
;
.   3600000   NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.   3600000   A   198.41.0.4
A.ROOT-SERVERS.NET.   3600000   AAAA 2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.   3600000   NS   B.ROOT-SERVERS.NET.
--More--(byte 886)

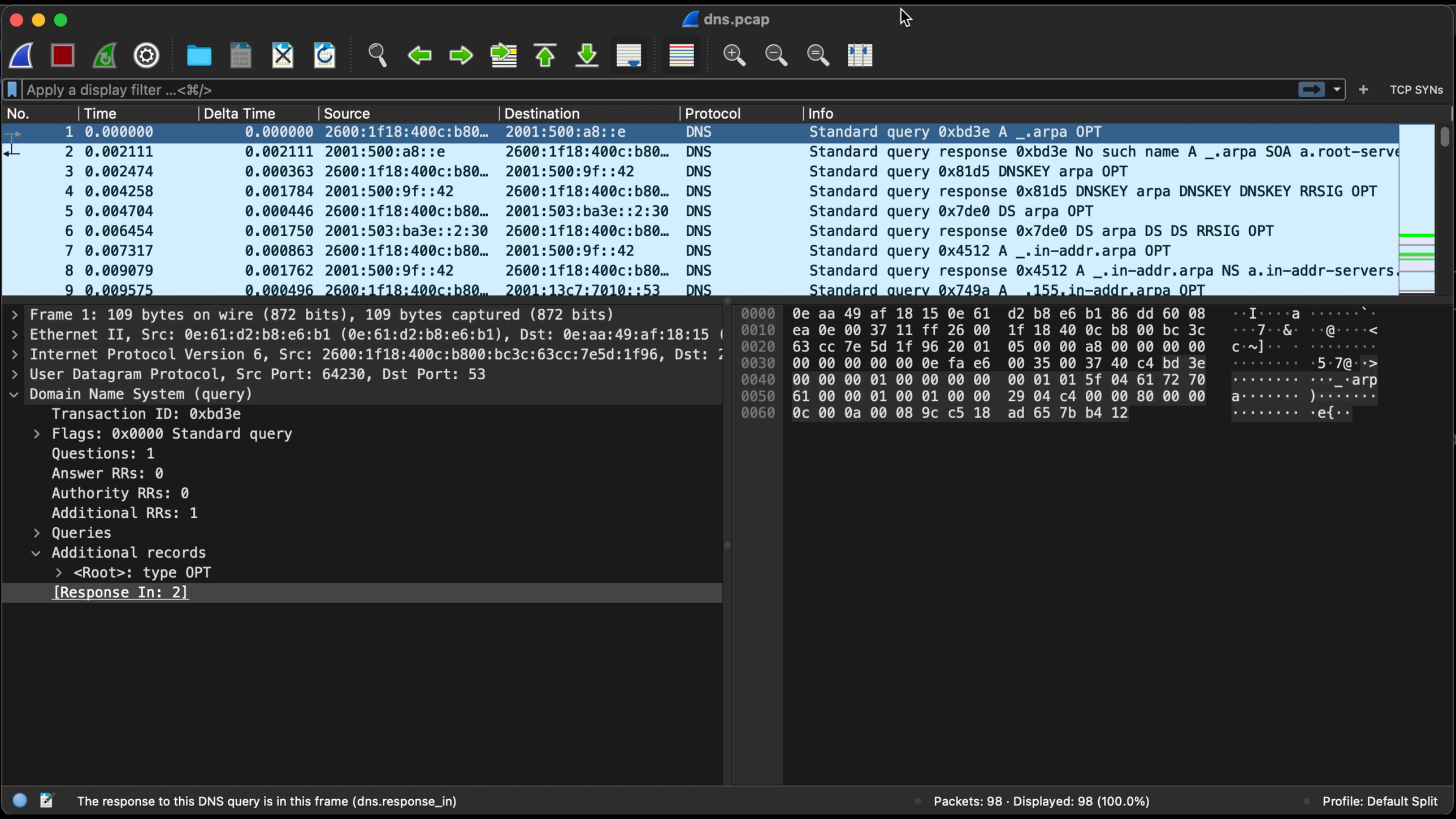


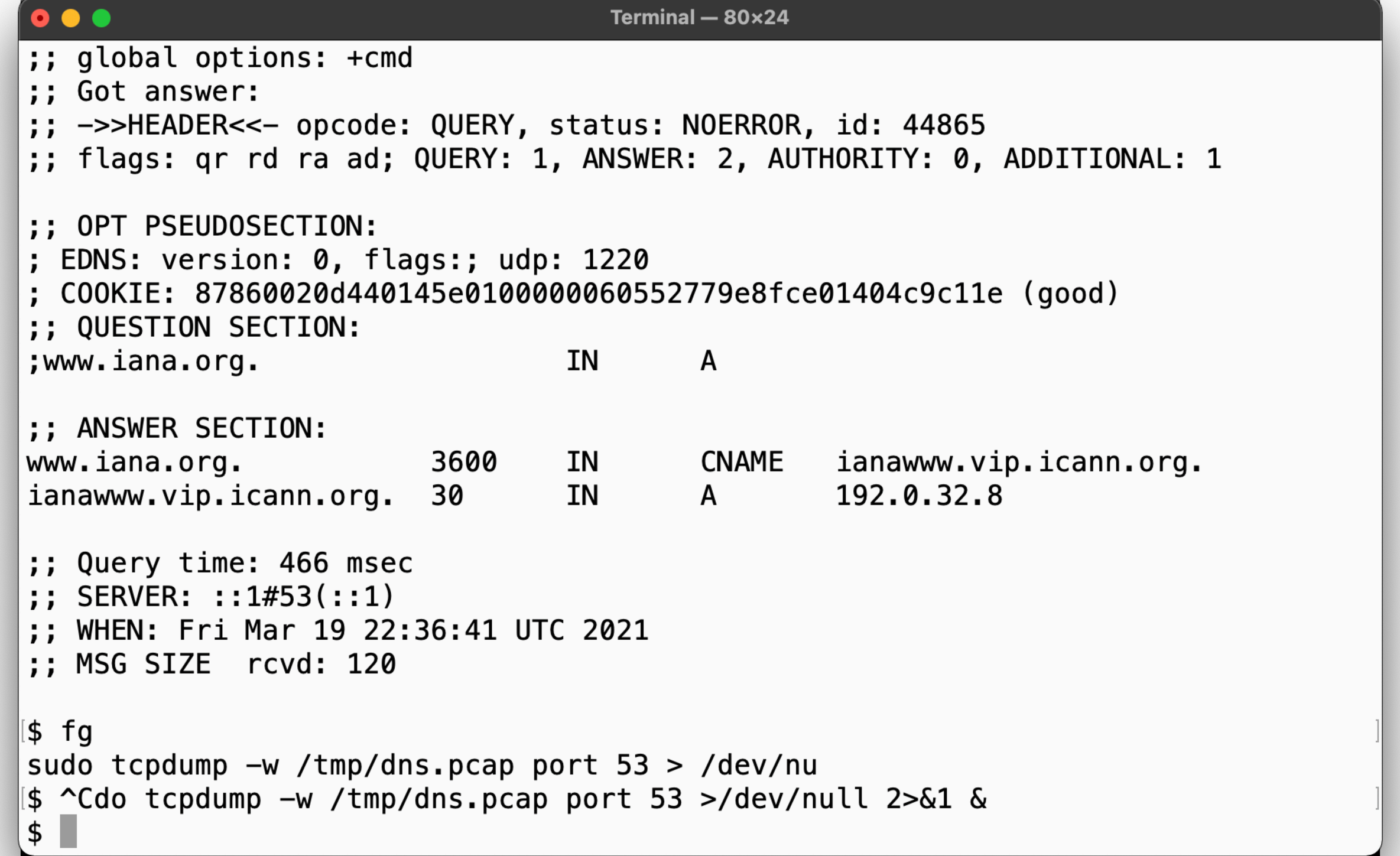
As of 03/19/2021 6:26 p.m., the root server system consists of 1375 instances operated by the 12 independent root server operators.

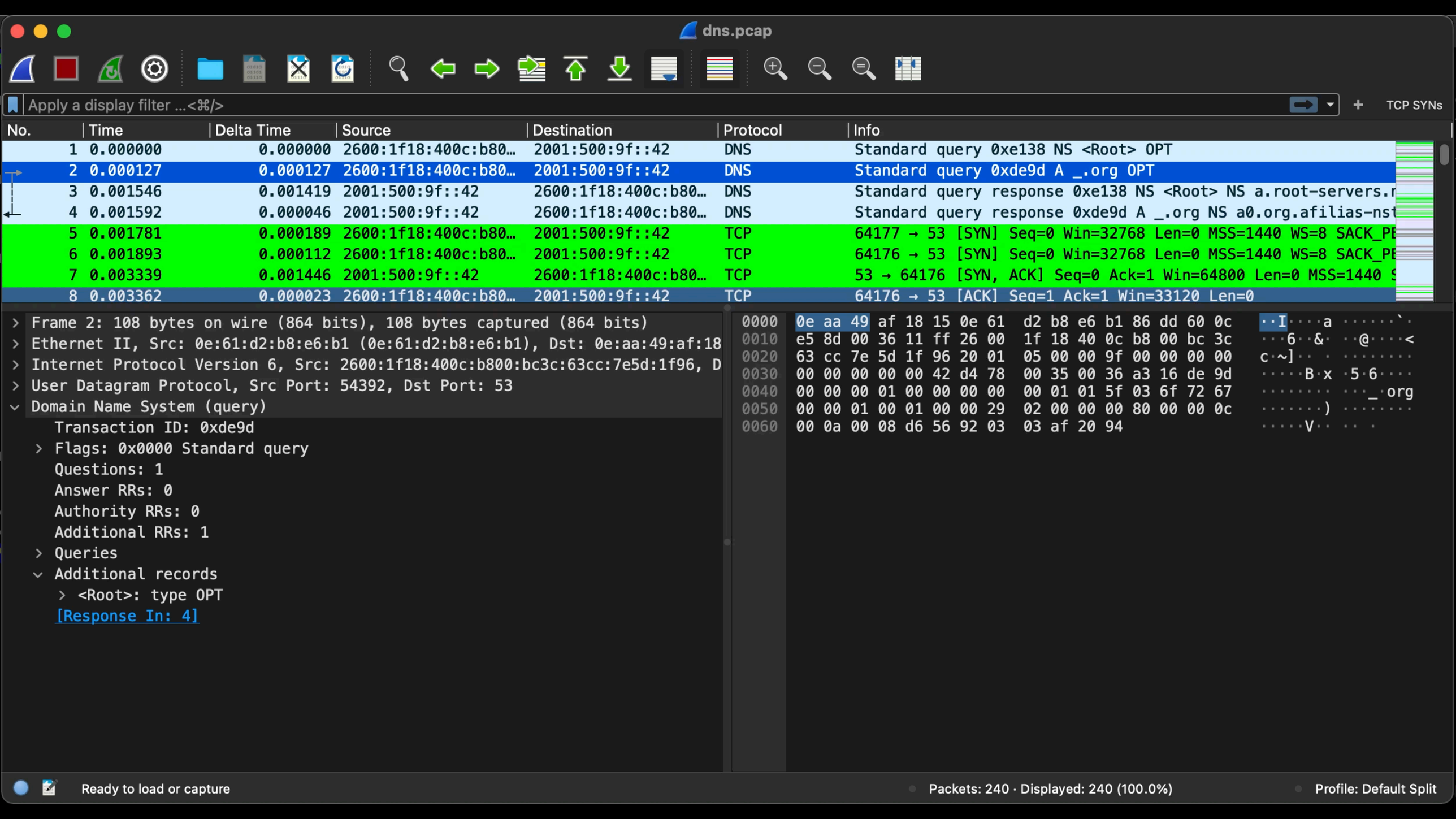
The 13 root name servers are operated by 12 independent organisations.

You can find more information about each of these organisations by visiting their homepage as found in the 'Operator' field below.


Terminal — 80×24
istheinternetonfire.com descriptive text "SUNBURST, when CoyzBear brings the Sol
arWinds of Change to Orion. Supply chain attack hits FireEye and several US agen
cies. https://is.gd/7h653D https://is.gd/UancjH"
$ host -t SSHFP cs615asa.netmeister.org
cs615asa.netmeister.org has SSHFP record 3 2 FC1B7508B10CB3B620A778ABC904FA7FAC5
32B36EF8661A82C32B268 3A7077CB
cs615asa.netmeister.org has SSHFP record 1 2 99C8F90C26B4F4BF84DF2E5CD22EF93798C
78B7E396F307354FEF502 30009233
cs615asa.netmeister.org has SSHFP record 4 2 903EC782A775EE5BAB46837A4AAFB43A23F
C7E17F099B766562421E6 CA0CAEAE
$ 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.edu is an alias for www.cs.stevens-tech.edu.
www.cs.stevens-tech.edu has address 155.246.56.11
$ sudo tcpdump -w /tmp/dns.pcap port 53 >/dev/null 2>&1 &
[1] 8692
$ host -t ptr 155.246.56.11
11.56.246.155.in-addr.arpa domain name pointer www.cs.stevens-tech.edu.
$ fg
sudo tcpdump -w /tmp/dns.pcap port 53 > /dev/nu
^C$


dns.pcap
Apply a display filter ...<⌘/>
TCP SYNs
No. Time Delta Time Source Destination Protocol Info
1 0.000000 0.000000 2600:1f18:400c:b80… 2001:500:a8::e DNS Standard query 0xbd3e A _.arpa OPT
2 0.002111 0.002111 2001:500:a8::e 2600:1f18:400c:b80… DNS Standard query response 0xbd3e No such name A _.arpa SOA a.root-serve
3 0.002474 0.000363 2600:1f18:400c:b80… 2001:500:9f::42 DNS Standard query 0x81d5 DNSKEY arpa OPT
4 0.004258 0.001784 2001:500:9f::42 2600:1f18:400c:b80… DNS Standard query response 0x81d5 DNSKEY arpa DNSKEY DNSKEY RRSIG OPT
5 0.004704 0.000446 2600:1f18:400c:b80… 2001:503:ba3e::2:30 DNS Standard query 0x7de0 DS arpa OPT
6 0.006454 0.001750 2001:503:ba3e::2:30 2600:1f18:400c:b80… DNS Standard query response 0x7de0 DS arpa DS DS RRSIG OPT
7 0.007317 0.000863 2600:1f18:400c:b80… 2001:500:9f::42 DNS Standard query 0x4512 A _.in-addr.arpa OPT
8 0.009079 0.001762 2001:500:9f::42 2600:1f18:400c:b80… DNS Standard query response 0x4512 A _.in-addr.arpa NS a.in-addr-servers.
9 0.009575 0.000496 2600:1f18:400c:b80… 2001:13c7:7010::53 DNS Standard query 0x749a A .155.in-addr.arpa OPT
Frame 1: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
Ethernet II, Src: 0e:61:d2:b8:e6:b1 (0e:61:d2:b8:e6:b1), Dst: 0e:aa:49:af:18:15
Internet Protocol Version 6, Src: 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96, Dst:
User Datagram Protocol, Src Port: 64230, 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]
0000 0e aa 49 af 18 15 0e 61 d2 b8 e6 b1 86 dd 60 08
0010 ea 0e 00 37 11 ff 26 00 1f 18 40 0c b8 00 bc 3c
0020 63 cc 7e 5d 1f 96 20 01 05 00 00 a8 00 00 00 00
0030 00 00 00 00 00 0e fa e6 00 35 00 37 40 c4 bd 3e
0040 00 00 00 01 00 00 00 00 00 01 01 5f 04 61 72 70
0050 61 00 00 01 00 01 00 00 29 04 c4 00 00 80 00 00
0060 0c 00 0a 00 08 9c c5 18 ad 65 7b b4 12
The response to this DNS query is in this frame (dns.response_in)
Packets: 98 · Displayed: 98 (100.0%)
Profile: Default Split


Terminal — 80×24
;; 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. IN A
;; 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/nu
$ ^Cdo tcpdump -w /tmp/dns.pcap port 53 >/dev/null 2>&1 &
$


dns.pcap
Apply a display filter ...<⌘/>
TCP SYNs
No. | Time | Delta Time | Source | Destination | Protocol | Info
1 0.000000 0.000000 2600:1f18:400c:b80… 2001:500:9f::42 DNS Standard query 0xe138 NS <Root> OPT
2 0.000127 0.000127 2600:1f18:400c:b80… 2001:500:9f::42 DNS Standard query 0xde9d A _.org OPT
3 0.001546 0.001419 2001:500:9f::42 2600:1f18:400c:b80… DNS Standard query response 0xe138 NS <Root> NS a.root-servers.r
4 0.001592 0.000046 2001:500:9f::42 2600:1f18:400c:b80… DNS Standard query response 0xde9d A _.org NS a0.org.afilias-nst
5 0.001781 0.000189 2600:1f18:400c:b80… 2001:500:9f::42 TCP 64177 → 53 [SYN] Seq=0 Win=32768 Len=0 MSS=1440 WS=8 SACK_PE
6 0.001893 0.000112 2600:1f18:400c:b80… 2001:500:9f::42 TCP 64176 → 53 [SYN] Seq=0 Win=32768 Len=0 MSS=1440 WS=8 SACK_PE
7 0.003339 0.001446 2001:500:9f::42 2600:1f18:400c:b80… TCP 53 → 64176 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1440 S
8 0.003362 0.000023 2600:1f18:400c:b80… 2001:500:9f::42 TCP 64176 → 53 [ACK] Seq=1 Ack=1 Win=33120 Len=0
Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
Ethernet II, Src: 0e:61:d2:b8:e6:b1 (0e:61:d2:b8:e6:b1), Dst: 0e:aa:49:af:18
Internet Protocol Version 6, Src: 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96, D
User Datagram Protocol, Src Port: 54392, Dst Port: 53
Domain Name System (query)
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]
0000 0e aa 49 af 18 15 0e 61 d2 b8 e6 b1 86 dd 60 0c
0010 e5 8d 00 36 11 ff 26 00 1f 18 40 0c b8 00 bc 3c
0020 63 cc 7e 5d 1f 96 20 01 05 00 00 9f 00 00 00 00
0030 00 00 00 00 00 42 d4 78 00 35 00 36 a3 16 de 9d
0040 00 00 00 01 00 00 00 00 00 01 01 5f 03 6f 72 67
0050 00 00 01 00 01 00 00 29 02 00 00 00 80 00 00 0c
0060 00 0a 00 08 d6 56 92 03 03 af 20 94
Ready to load or capture
Packets: 240 · Displayed: 240 (100.0%)
Profile: Default Split

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://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- https://www.netmeister.org/blog/doh-dot-dnssec.html