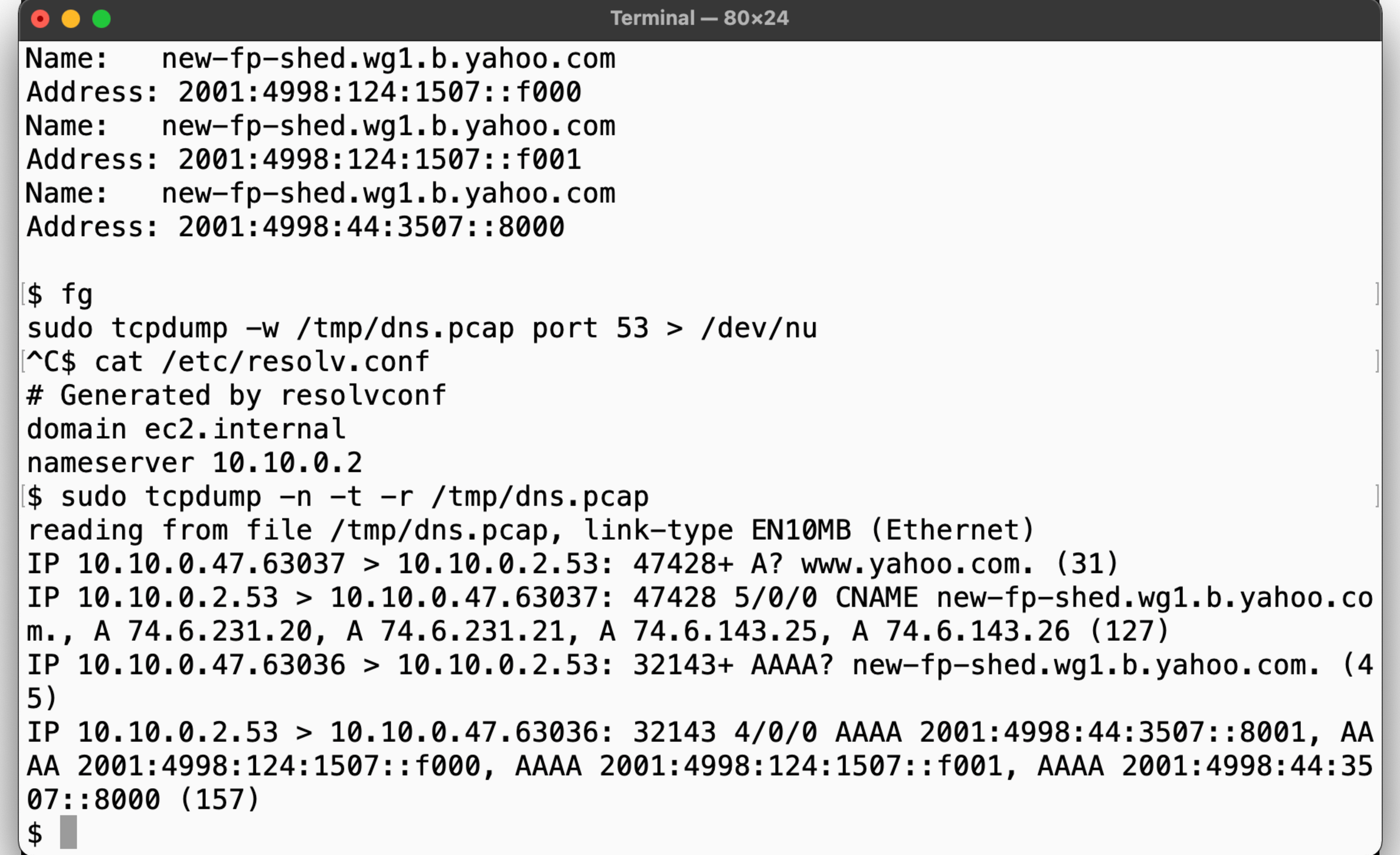
https://commons.wikimedia.org/wiki/File:Telefonbog_ubt-1.JPG
Photograph by Tomasz Sienicki

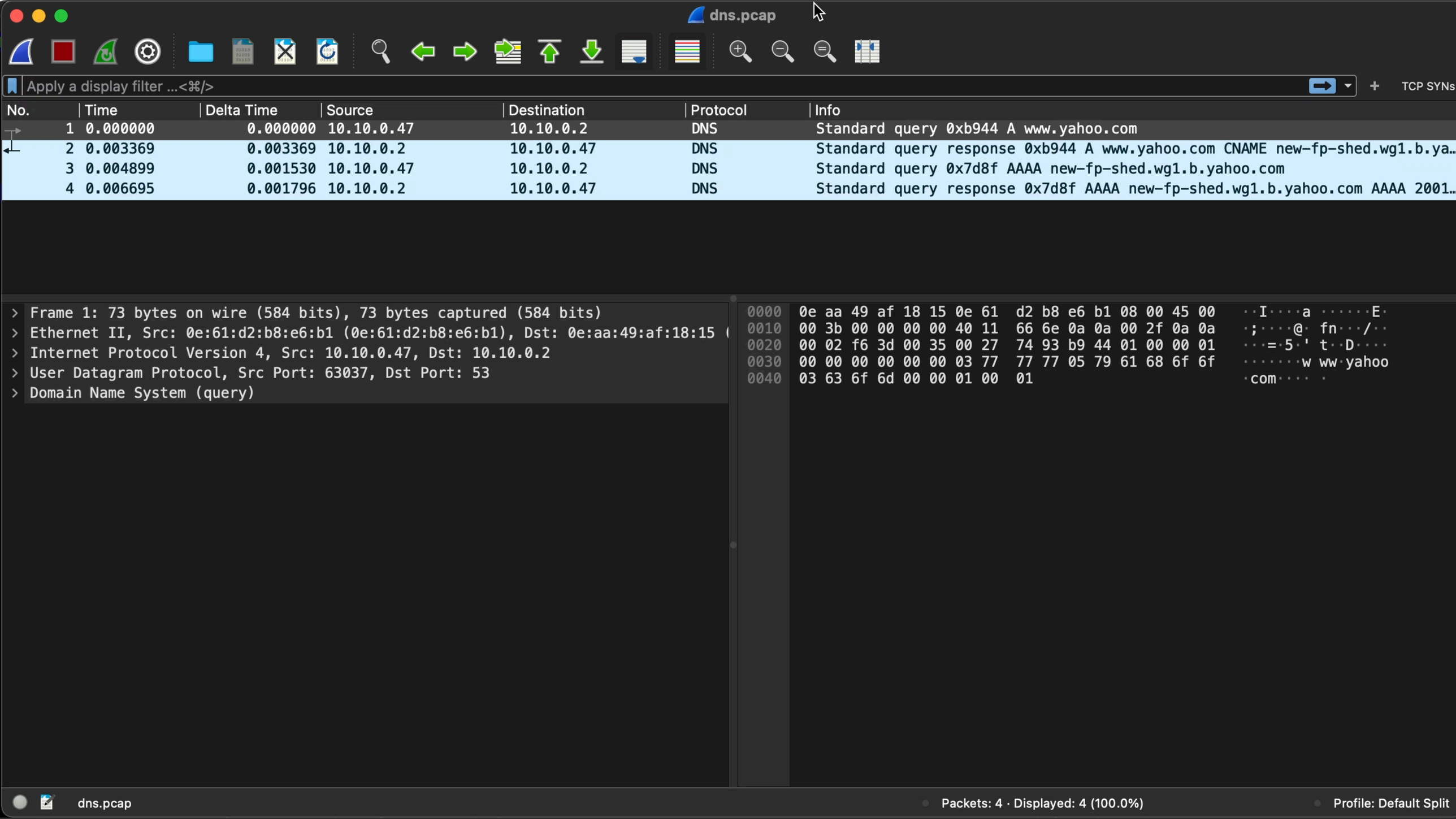
System Administration

Week 07, Segment 2
The Domain Name System, Part II

Department of Computer Science
Stevens Institute of Technology

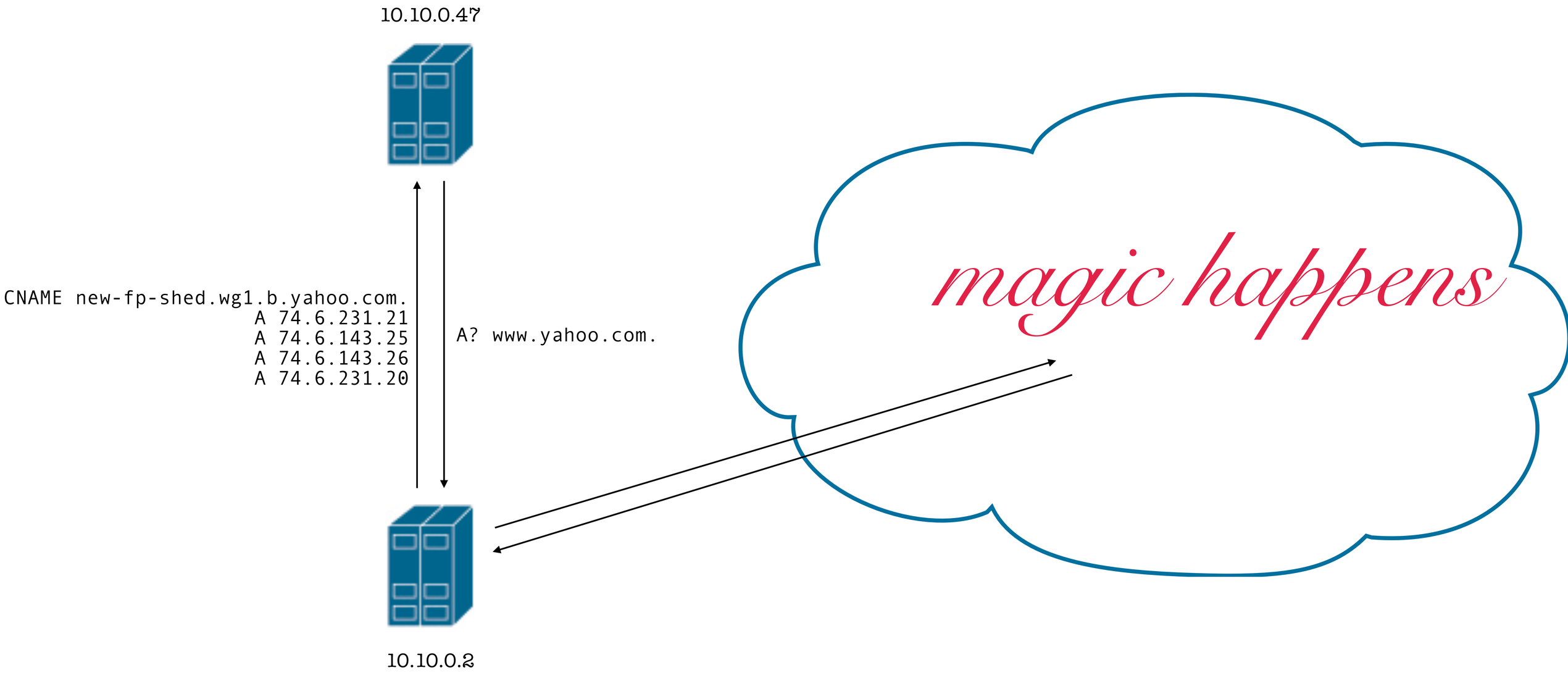
Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

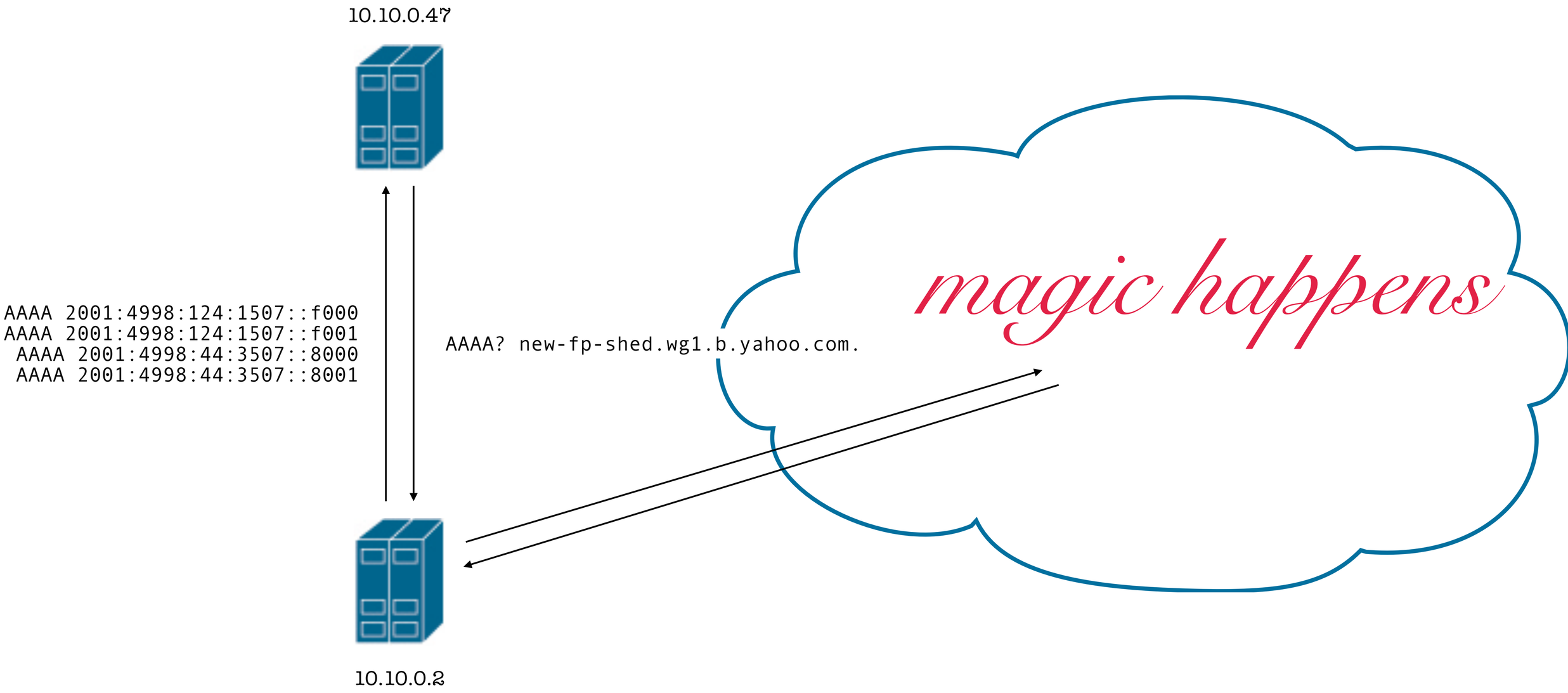

Terminal — 80×24
Name: new-fp-shed.wg1.b.yahoo.com
Address: 2001:4998:124:1507::f000
Name: new-fp-shed.wg1.b.yahoo.com
Address: 2001:4998:124:1507::f001
Name: new-fp-shed.wg1.b.yahoo.com
Address: 2001:4998:44:3507::8000
$ fg
sudo tcpdump -w /tmp/dns.pcap port 53 > /dev/nu
^C$ cat /etc/resolv.conf
Generated by resolvconf
domain ec2.internal
nameserver 10.10.0.2
$ sudo tcpdump -n -t -r /tmp/dns.pcap
reading from file /tmp/dns.pcap, link-type EN10MB (Ethernet)
IP 10.10.0.47.63037 > 10.10.0.2.53: 47428+ A? www.yahoo.com. (31)
IP 10.10.0.2.53 > 10.10.0.47.63037: 47428 5/0/0 CNAME new-fp-shed.wg1.b.yahoo.com., A 74.6.231.20, A 74.6.231.21, A 74.6.143.25, A 74.6.143.26 (127)
IP 10.10.0.47.63036 > 10.10.0.2.53: 32143+ AAAA? new-fp-shed.wg1.b.yahoo.com. (45)
IP 10.10.0.2.53 > 10.10.0.47.63036: 32143 4/0/0 AAAA 2001:4998:44:3507::8001, AAAA 2001:4998:124:1507::f000, AAAA 2001:4998:124:1507::f001, AAAA 2001:4998:44:3507::8000 (157)
$

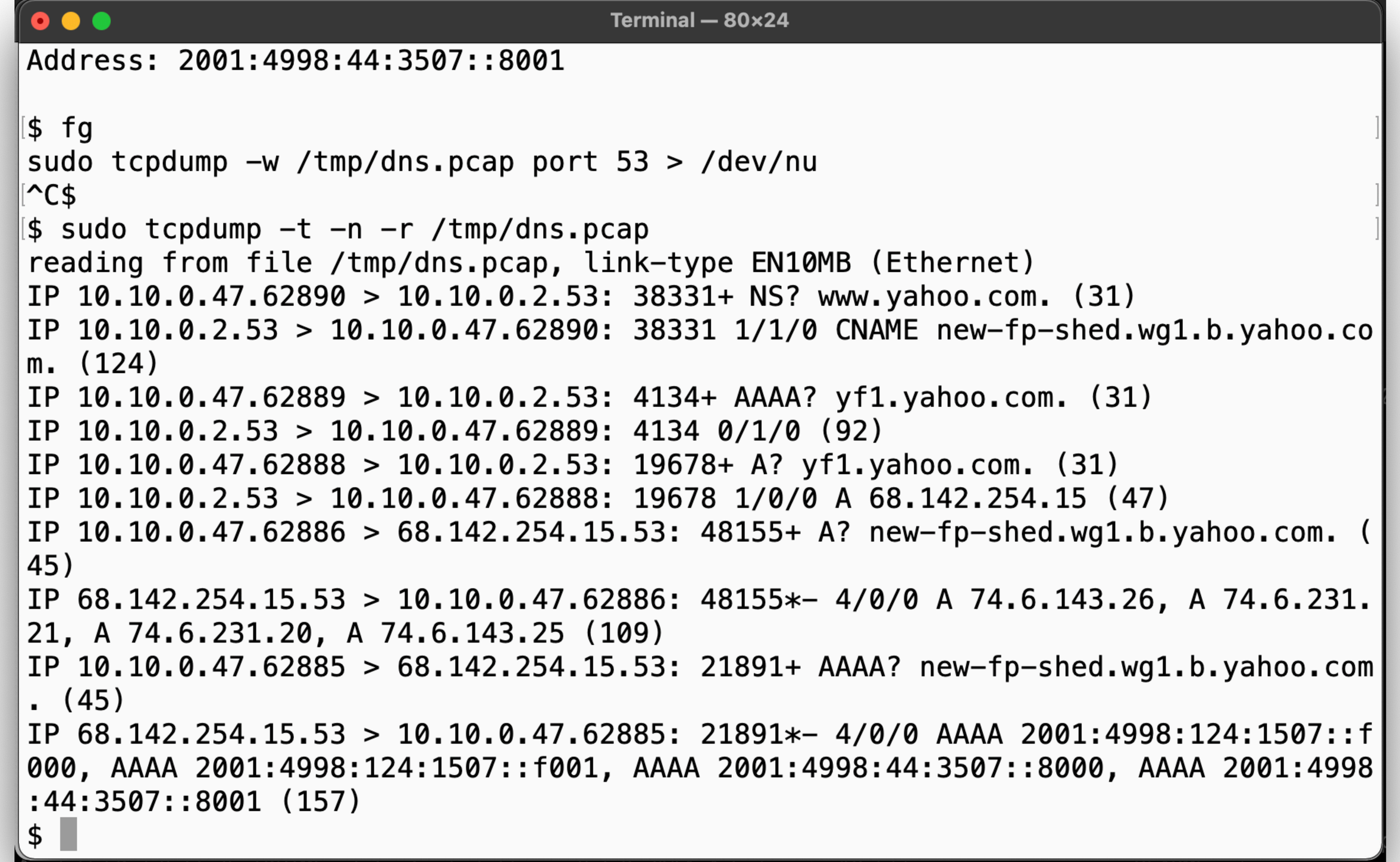

dns.pcap
Apply a display filter ...<⌘/>
TCP SYNs
No. Time Delta Time Source Destination Protocol Info
1 0.000000 0.000000 10.10.0.47 10.10.0.2 DNS Standard query 0xb944 A www.yahoo.com
2 0.003369 0.003369 10.10.0.2 10.10.0.47 DNS Standard query response 0xb944 A www.yahoo.com CNAME new-fp-shed.wg1.b.ya…
3 0.004899 0.001530 10.10.0.47 10.10.0.2 DNS Standard query 0x7d8f AAAA new-fp-shed.wg1.b.yahoo.com
4 0.006695 0.001796 10.10.0.2 10.10.0.47 DNS Standard query response 0x7d8f AAAA new-fp-shed.wg1.b.yahoo.com AAAA 2001…
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 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 4, Src: 10.10.0.47, Dst: 10.10.0.2
User Datagram Protocol, Src Port: 63037, Dst Port: 53
Domain Name System (query)
0000 0e aa 49 af 18 15 0e 61 d2 b8 e6 b1 08 00 45 00 ··I····a ·····E·
0010 00 3b 00 00 00 00 40 11 66 6e 0a 0a 00 2f 0a 0a ·;····@· fn···/··
0020 00 02 f6 3d 00 35 00 27 74 93 b9 44 01 00 00 01 ···=·5·' t··D····
0030 00 00 00 00 00 00 03 77 77 77 05 79 61 68 6f 6f ·······w ww·yahoo
0040 03 63 6f 6d 00 00 01 00 01 ·com···· ·
dns.pcap
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default Split

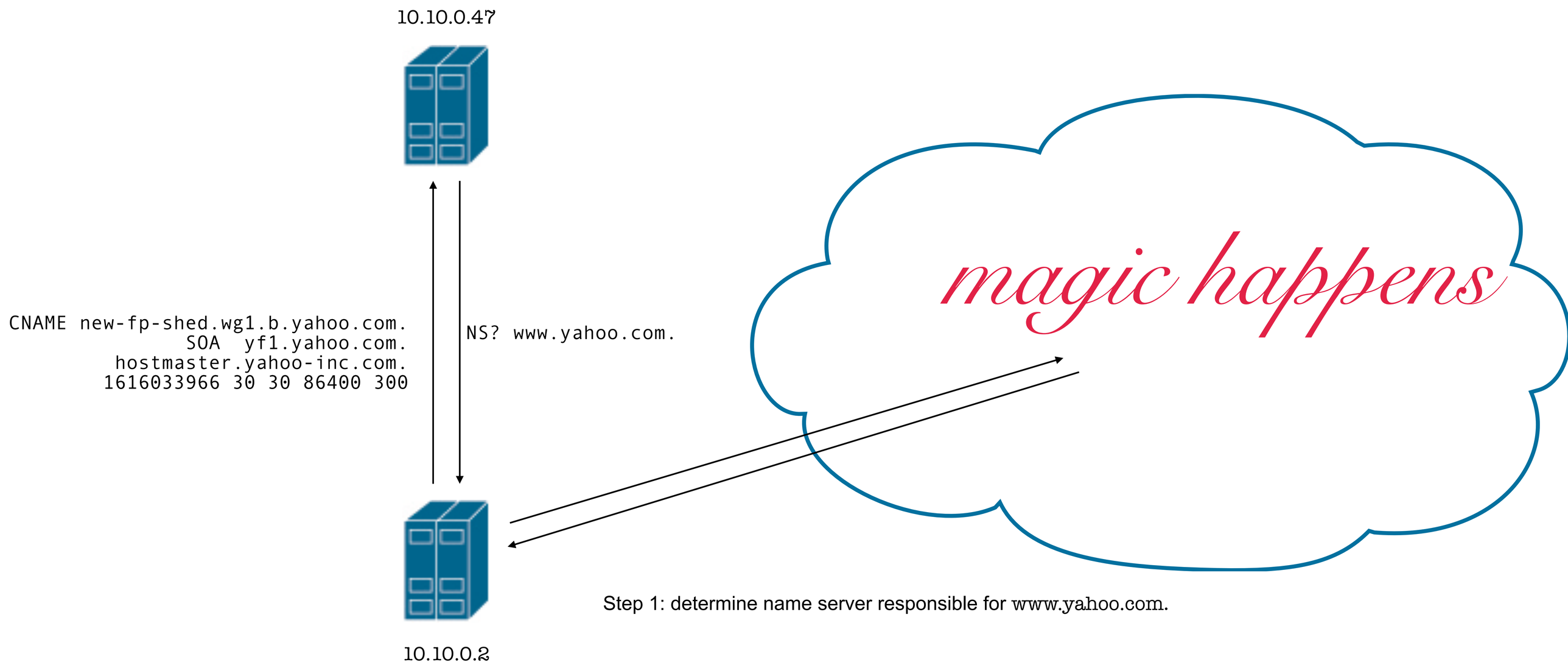
A simple DNS query

- The DNS server we talk to is *non-authoritative*, meaning it simply *resolves* things for us by asking other servers.
- An *authoritative* name server provides (authoritative) answers; a *resolver* relays answers it determined by asking the right authoritative name servers.
- A simple request to resolve e.g., `www.yahoo.com` can lead to multiple queries and involve multiple RR types:
  - a CNAME record
  - several A records
  - several AAAA records

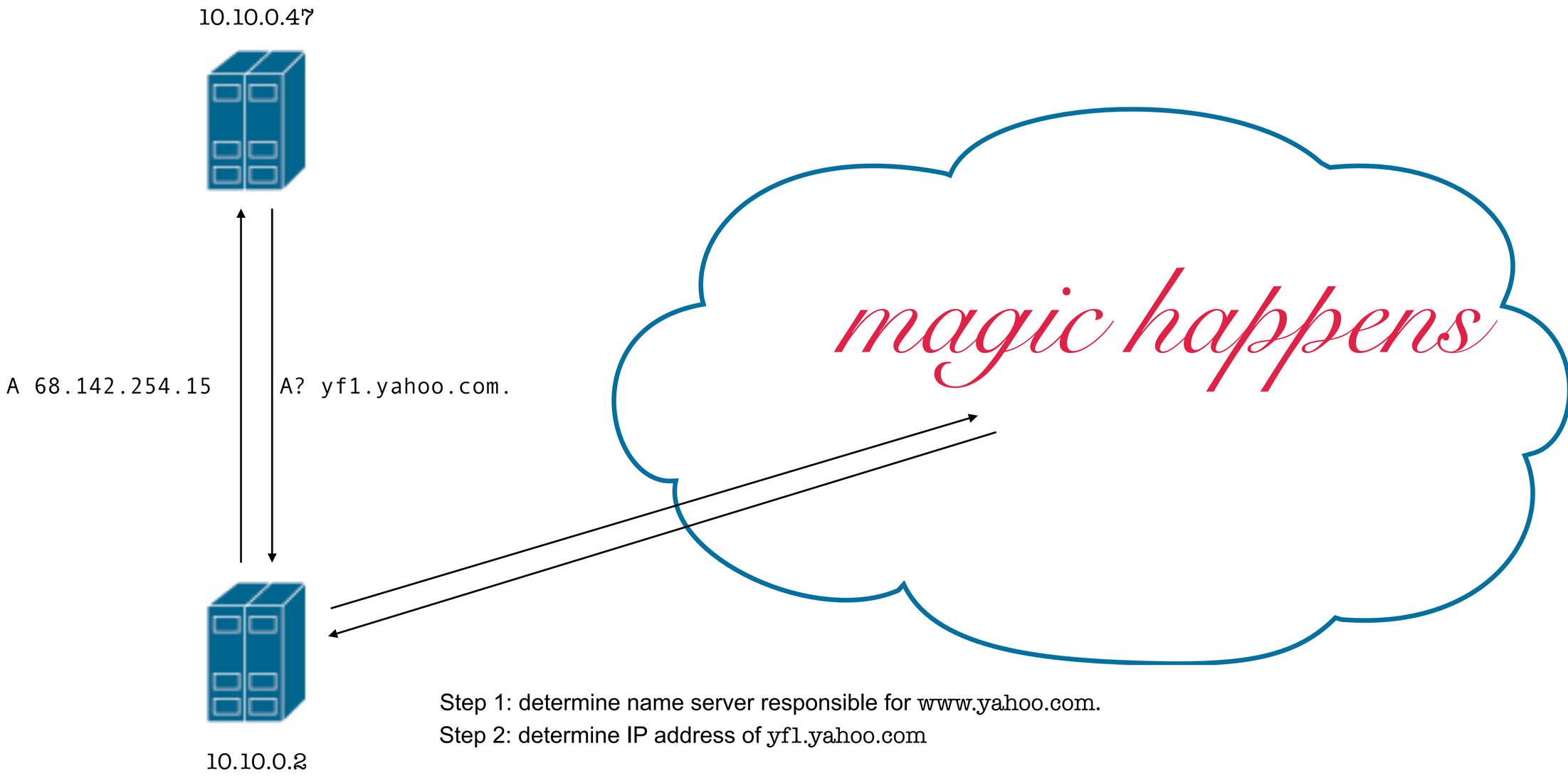

10.10.0.47
CNAME new-fp-shed.wg1.b.yahoo.com.
A 74.6.231.21
A 74.6.143.25
A 74.6.143.26
A 74.6.231.20
A? www.yahoo.com.
magic happens
10.10.0.2


10.10.0.47
AAAA 2001:4998:124:1507::f000
AAAA 2001:4998:124:1507::f001
AAAA 2001:4998:44:3507::8000
AAAA 2001:4998:44:3507::8001
AAAA? new-fp-shed.wg1.b.yahoo.com.
magic happens
10.10.0.2

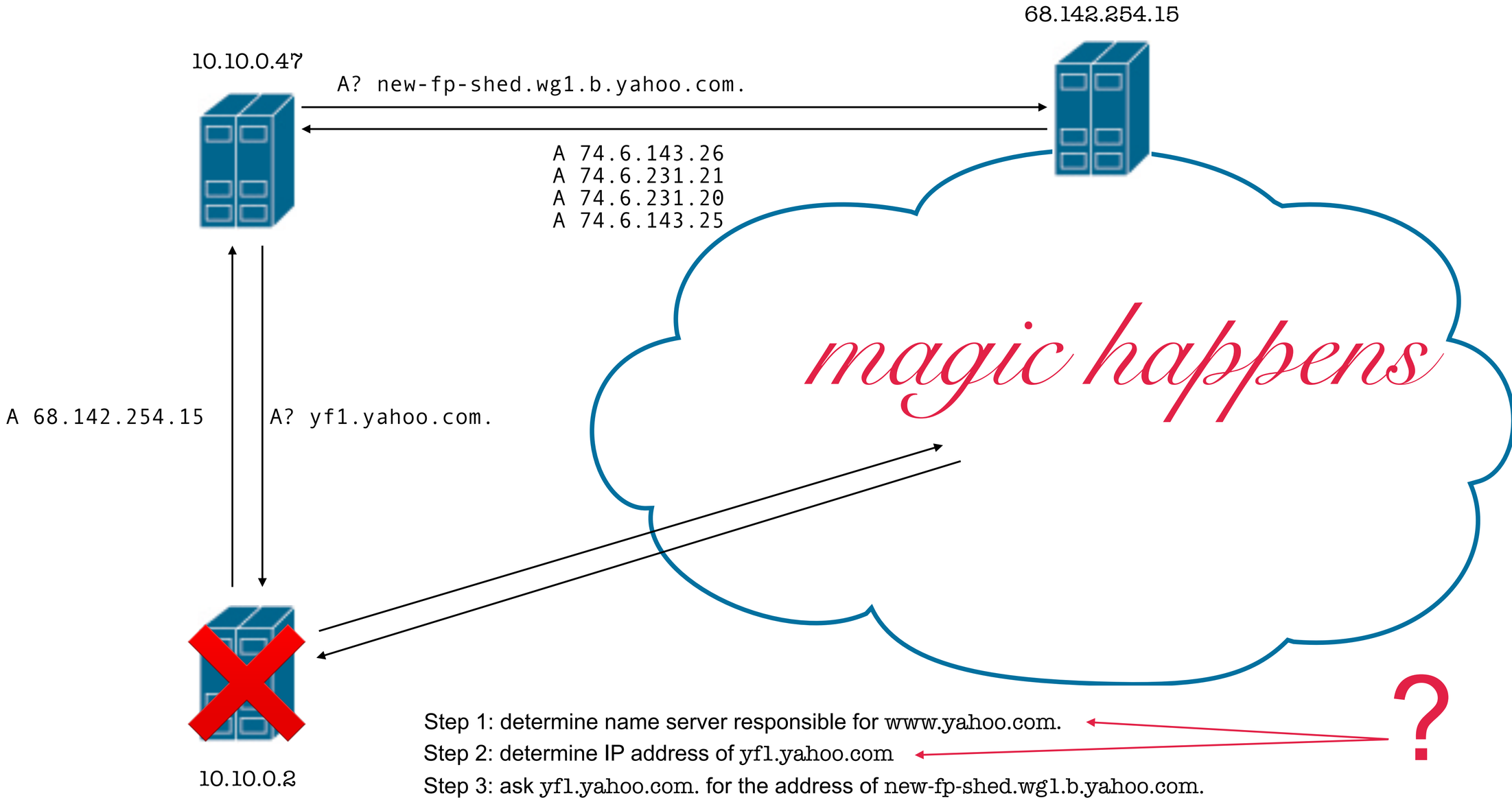

Terminal — 80×24
Address: 2001:4998:44:3507::8001
$ fg
sudo tcpdump -w /tmp/dns.pcap port 53 > /dev/nu
^C$
$ sudo tcpdump -t -n -r /tmp/dns.pcap
reading from file /tmp/dns.pcap, link-type EN10MB (Ethernet)
IP 10.10.0.47.62890 > 10.10.0.2.53: 38331+ NS? www.yahoo.com. (31)
IP 10.10.0.2.53 > 10.10.0.47.62890: 38331 1/1/0 CNAME new-fp-shed.wg1.b.yahoo.com. (124)
IP 10.10.0.47.62889 > 10.10.0.2.53: 4134+ AAAA? yf1.yahoo.com. (31)
IP 10.10.0.2.53 > 10.10.0.47.62889: 4134 0/1/0 (92)
IP 10.10.0.47.62888 > 10.10.0.2.53: 19678+ A? yf1.yahoo.com. (31)
IP 10.10.0.2.53 > 10.10.0.47.62888: 19678 1/0/0 A 68.142.254.15 (47)
IP 10.10.0.47.62886 > 68.142.254.15.53: 48155+ A? new-fp-shed.wg1.b.yahoo.com. (45)
IP 68.142.254.15.53 > 10.10.0.47.62886: 48155*- 4/0/0 A 74.6.143.26, A 74.6.231.21, A 74.6.231.20, A 74.6.143.25 (109)
IP 10.10.0.47.62885 > 68.142.254.15.53: 21891+ AAAA? new-fp-shed.wg1.b.yahoo.com. (45)
IP 68.142.254.15.53 > 10.10.0.47.62885: 21891*- 4/0/0 AAAA 2001:4998:124:1507::f000, AAAA 2001:4998:124:1507::f001, AAAA 2001:4998:44:3507::8000, AAAA 2001:4998:44:3507::8001 (157)
$



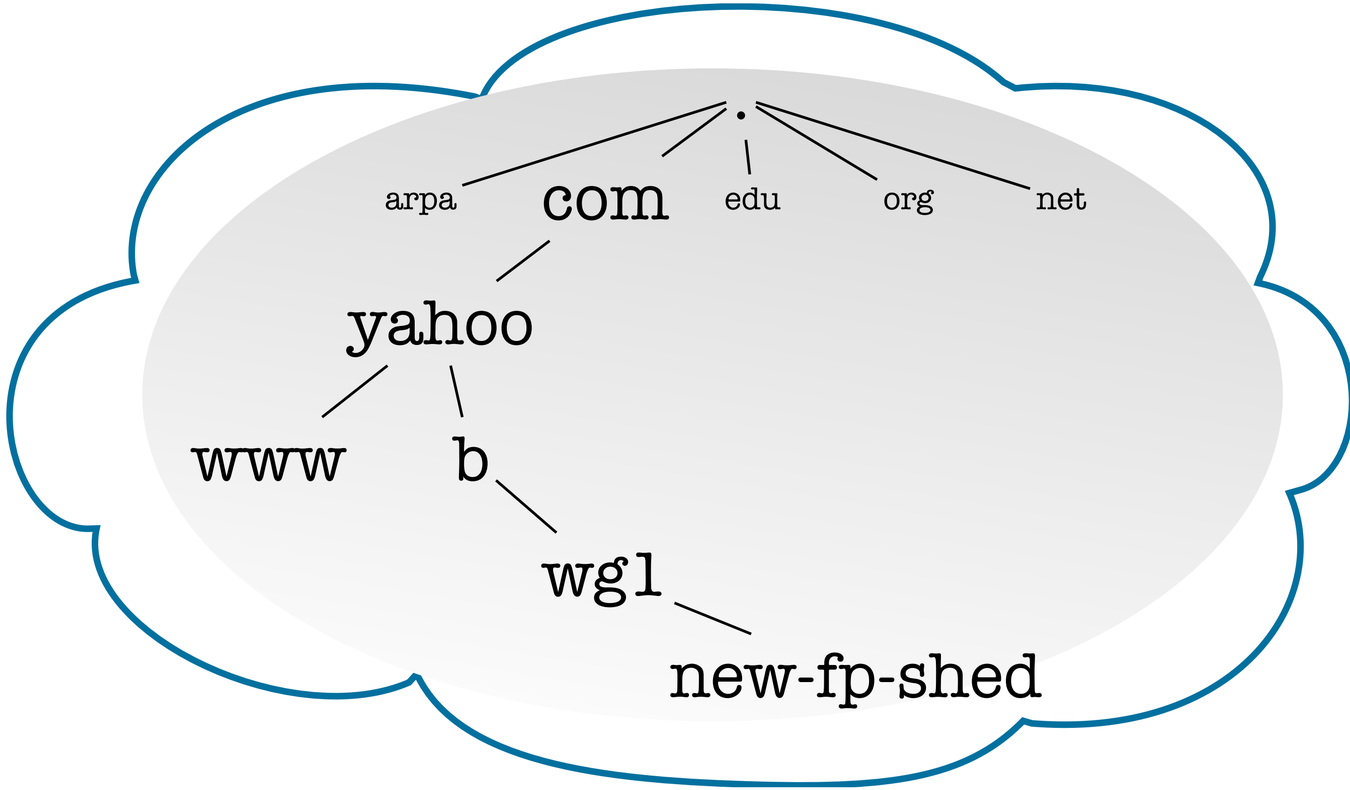
Step 1: determine name server responsible for www.yahoo.com.



Step 1: determine name server responsible for www.yahoo.com.
Step 2: determine IP address of yf1.yahoo.com

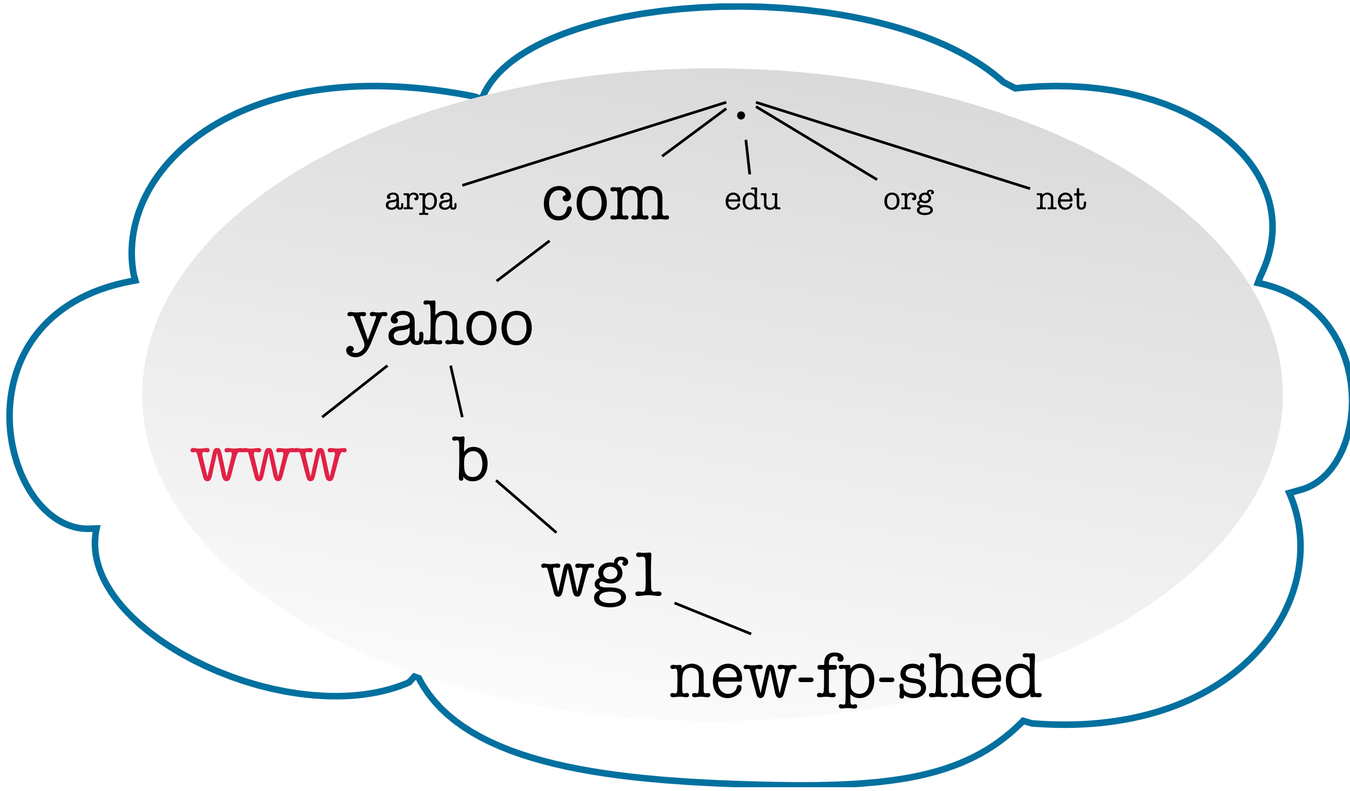

68.142.254.15
10.10.0.47
A? new-fp-shed.wg1.b.yahoo.com.
A 74.6.143.26
A 74.6.231.21
A 74.6.231.20
A 74.6.143.25
magic happens
A 68.142.254.15
A? yf1.yahoo.com.
10.10.0.2
Step 1: determine name server responsible for www.yahoo.com.
Step 2: determine IP address of yf1.yahoo.com
Step 3: ask yf1.yahoo.com. for the address of new-fp-shed.wg1.b.yahoo.com.
?

10.10.0.47



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

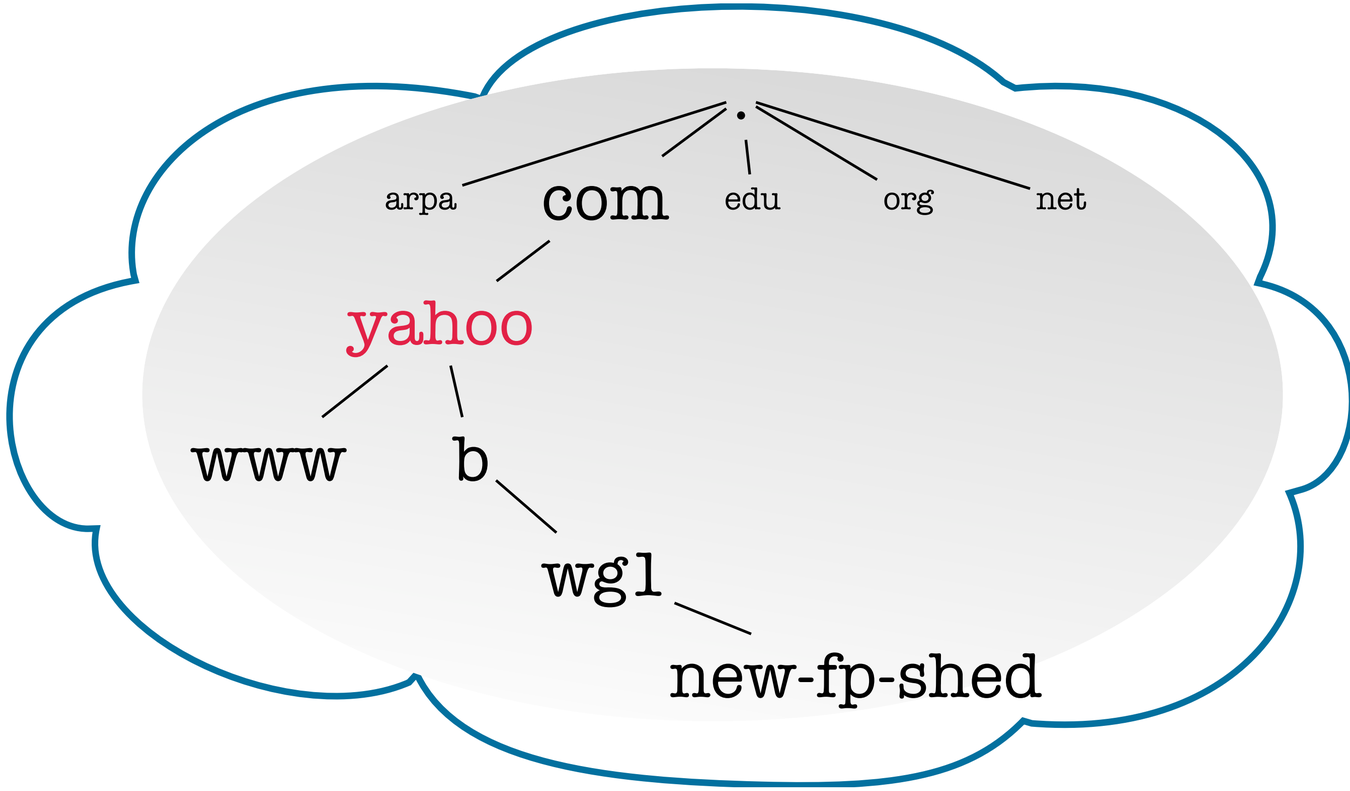
10.10.0.47



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

- find out who is responsible for yahoo.com.

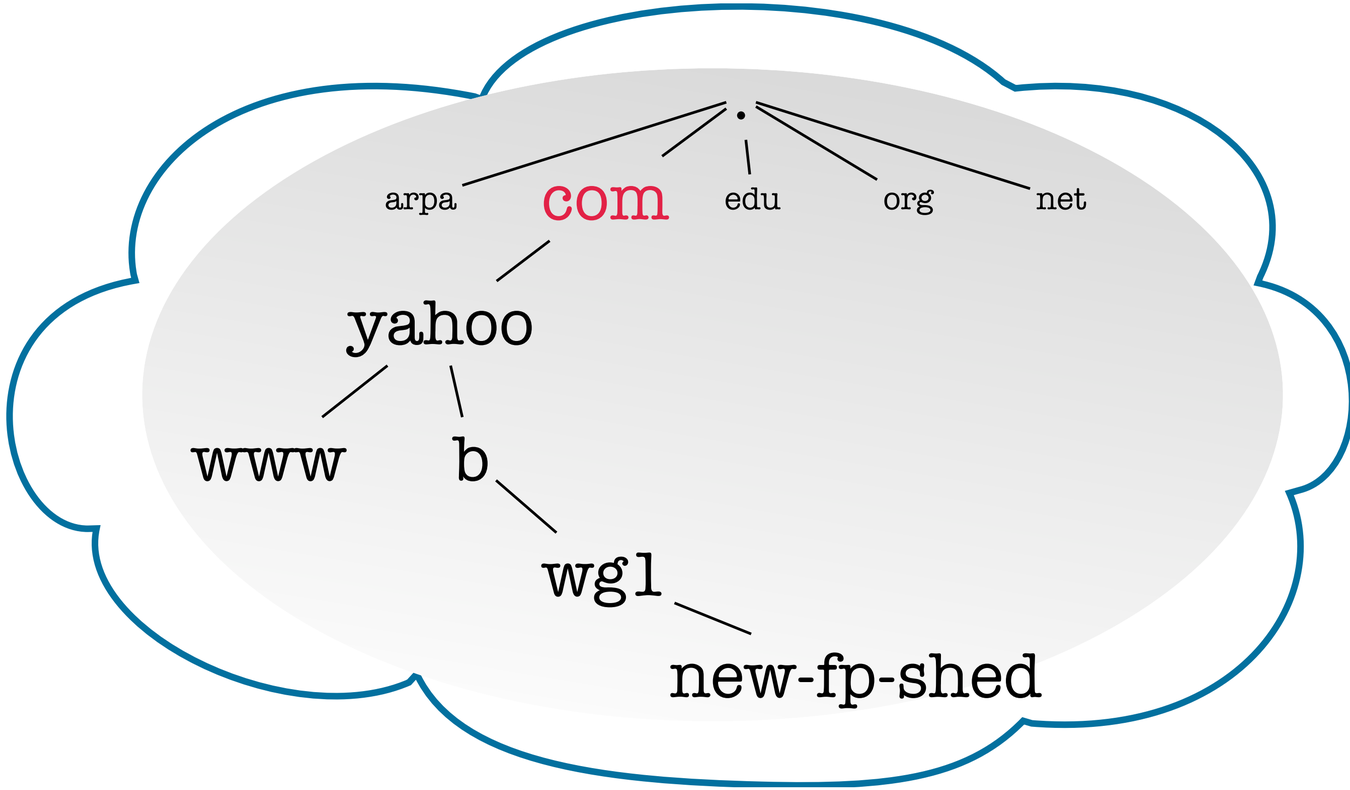
10.10.0.47



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

- find out who is responsible for yahoo.com.
- find out who is responsible for com.

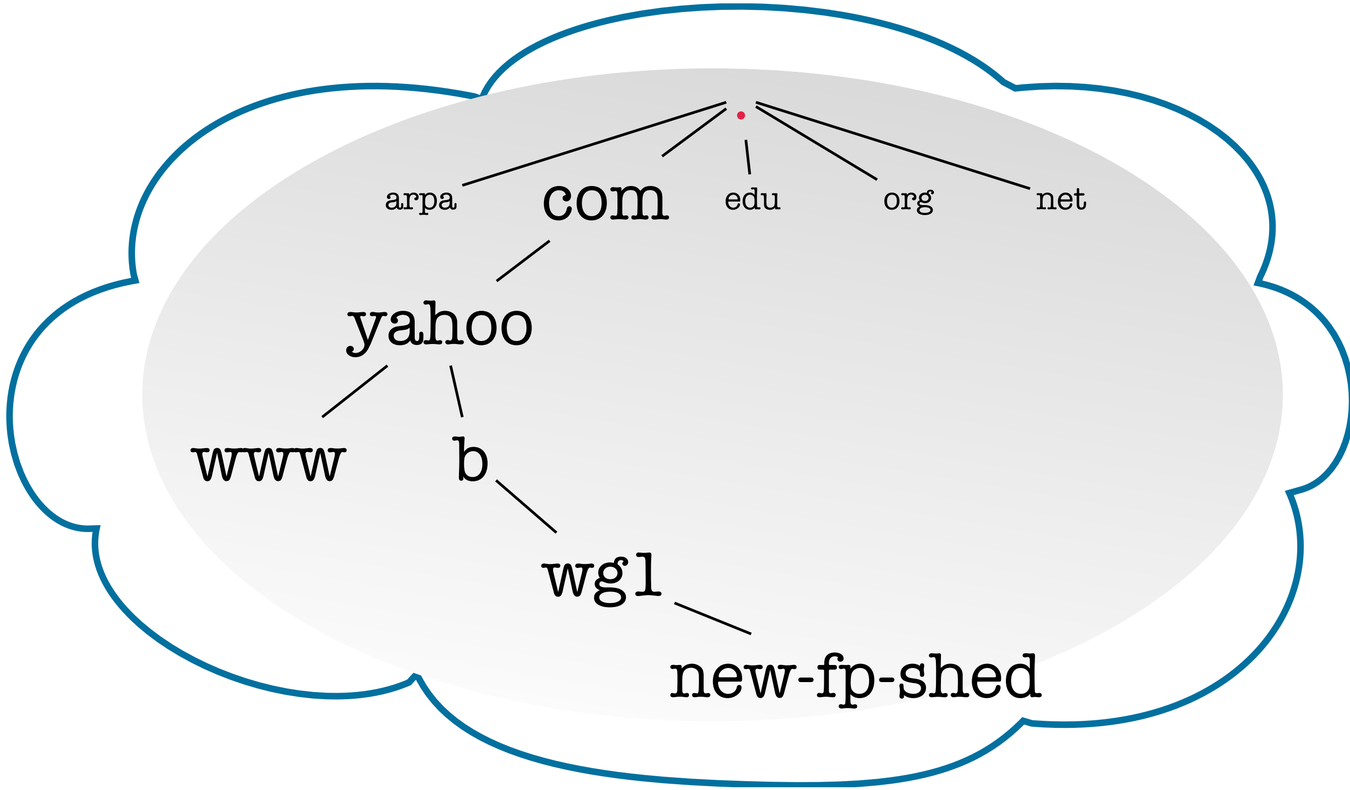
10.10.0.47



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

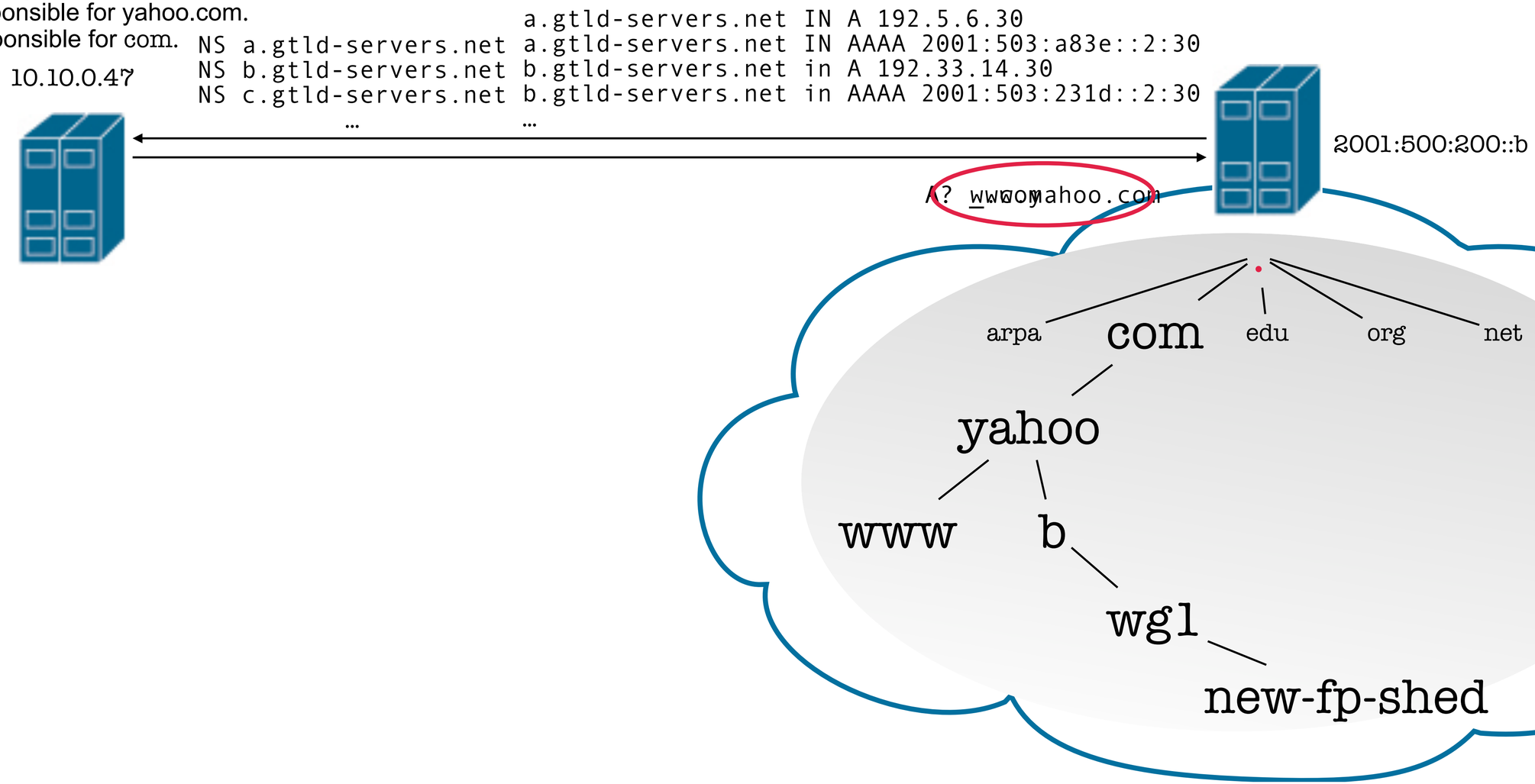
- find out who is responsible for yahoo.com.
- find out who is responsible for com.
- let's ask the root!

10.10.0.47



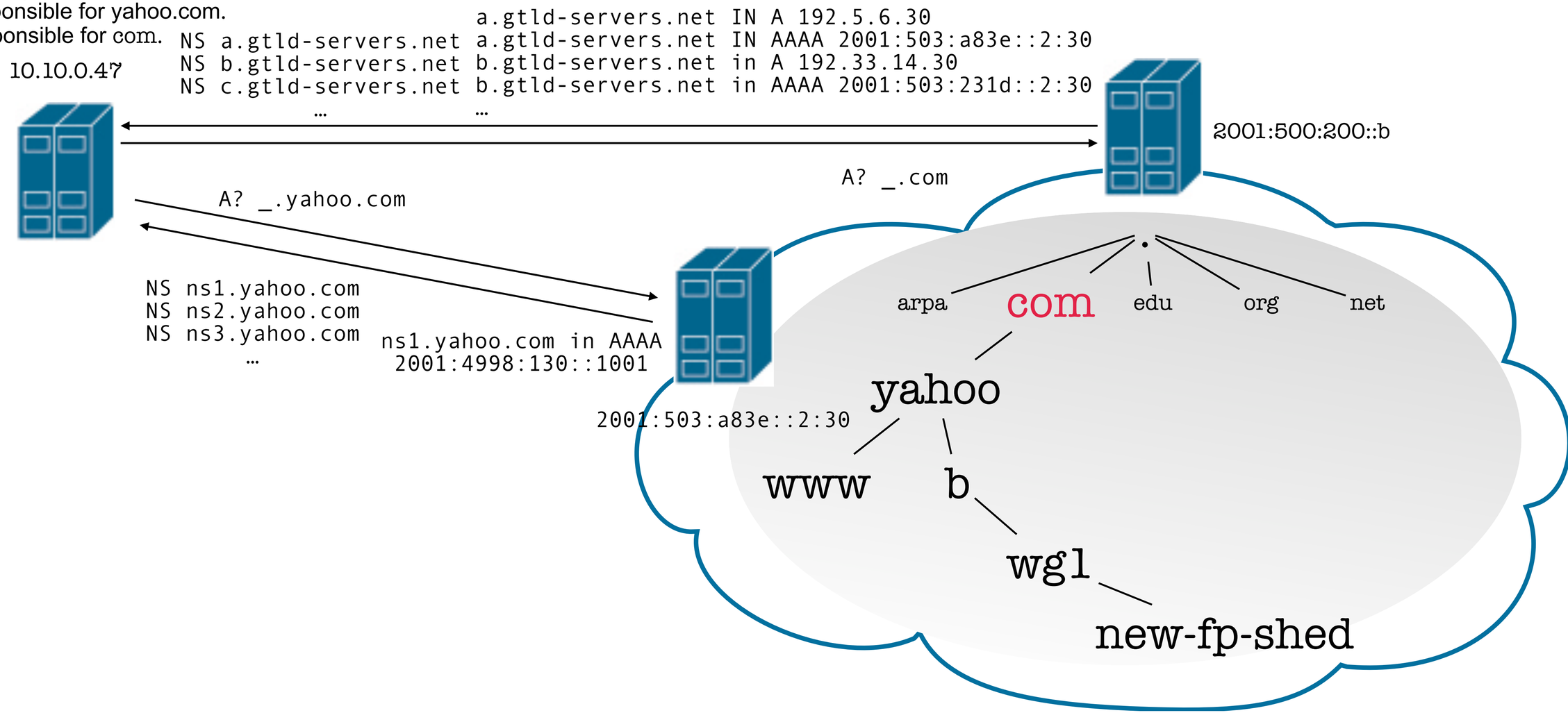
To find out where www.yahoo.com. is:

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



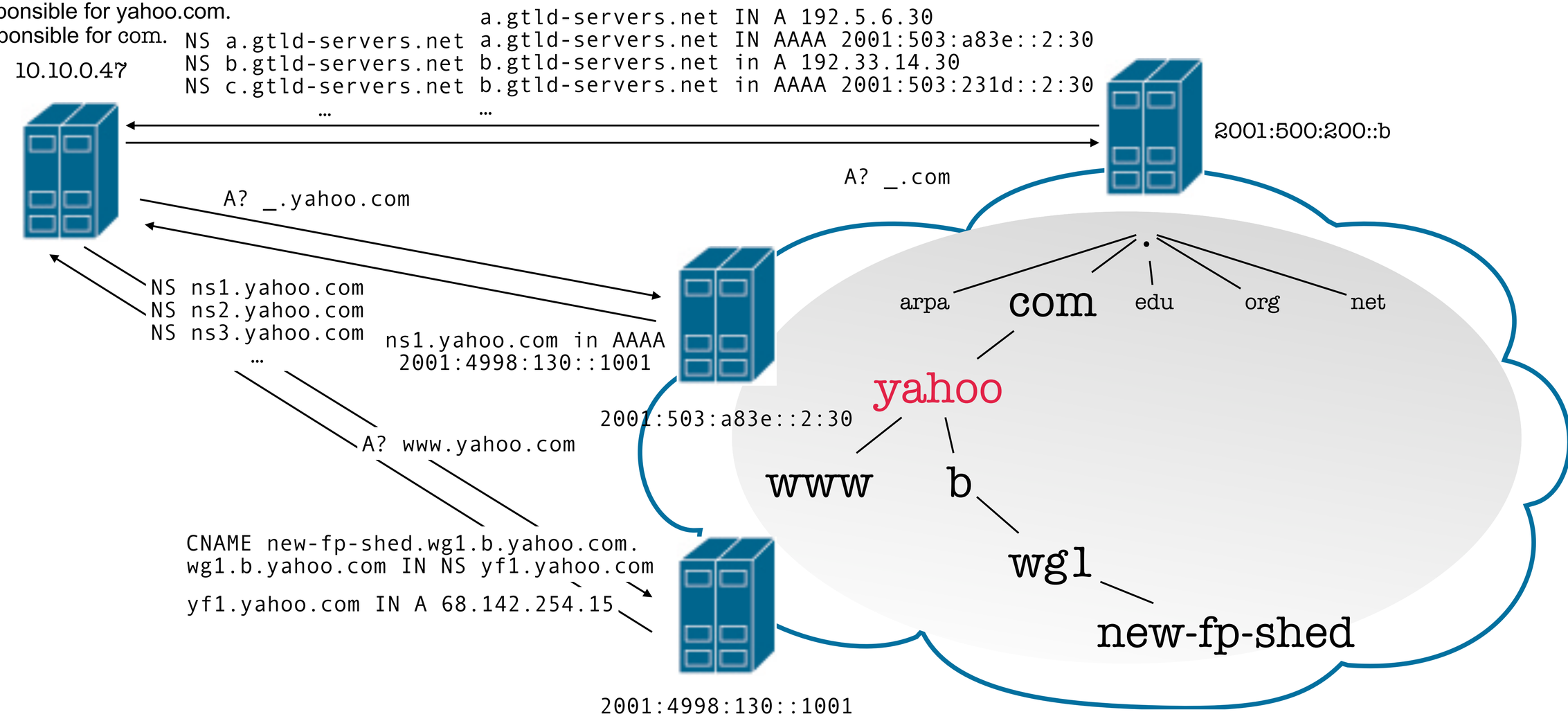
The root tells me a.gtld-servers.net is responsible for com.
The root also told me what that server's IP addresses are.

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!

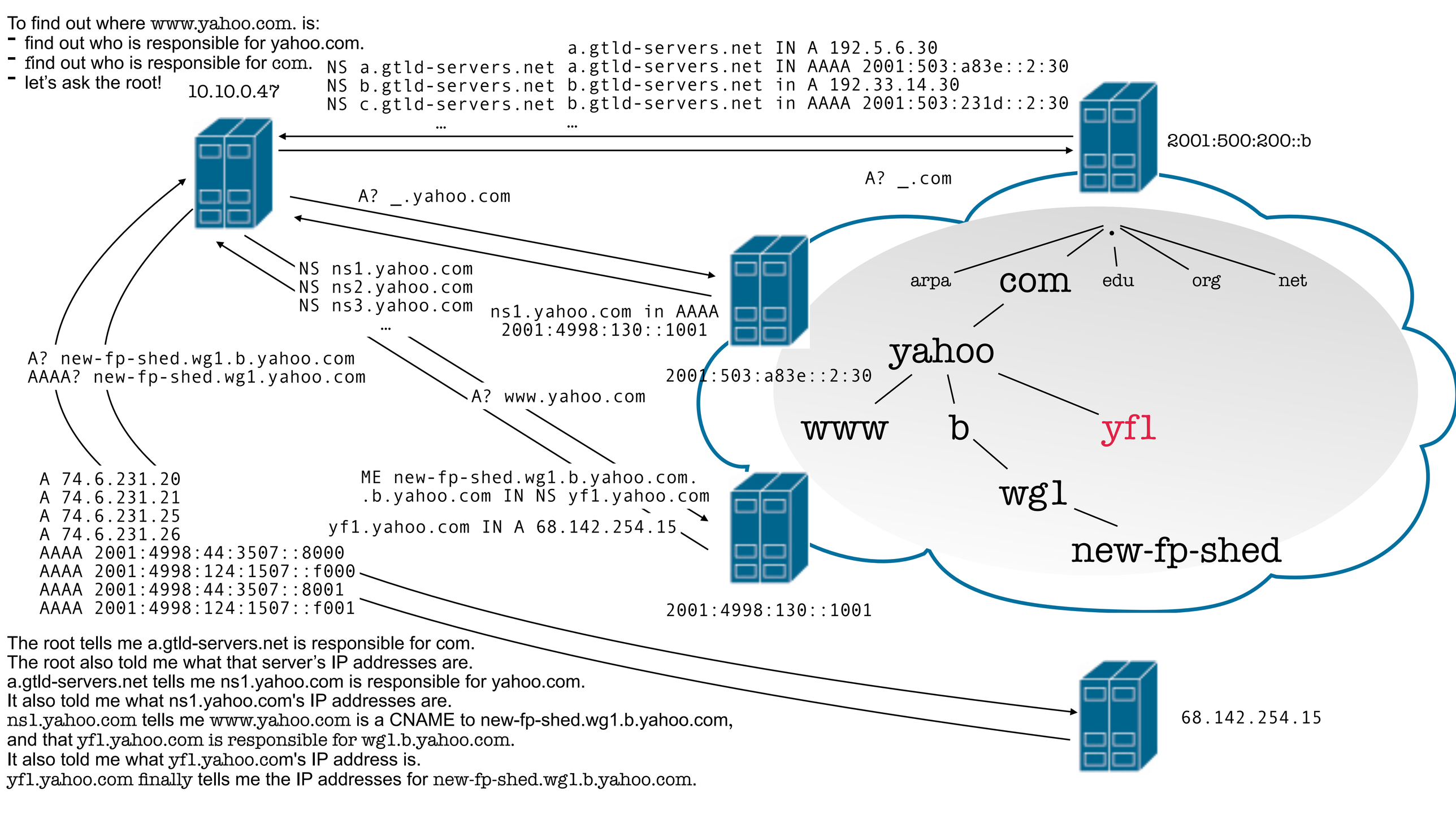


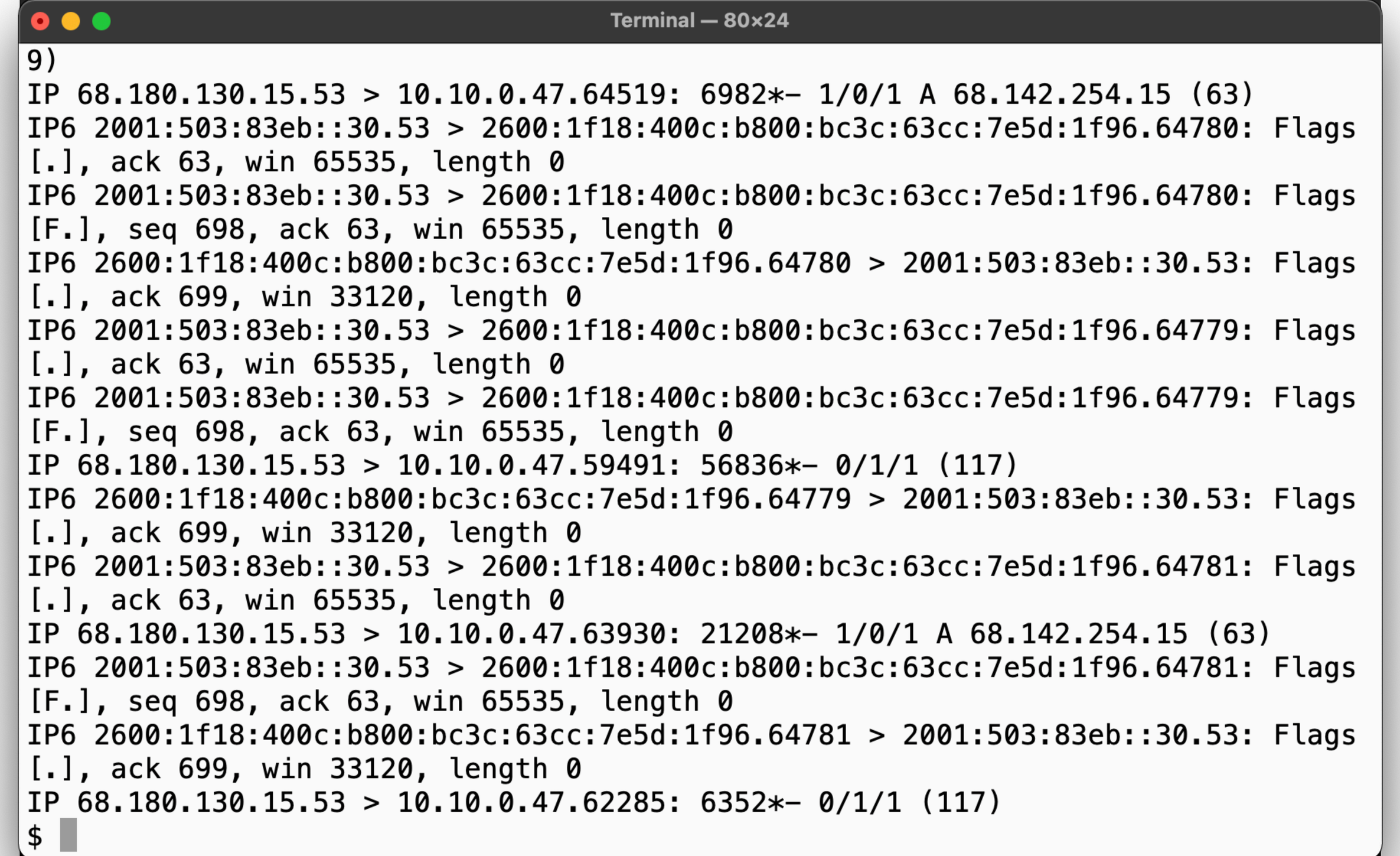
The root tells me a.gtld-servers.net is responsible for com.
The root also told me what that server's IP addresses are.
a.gtld-servers.net tells me ns1.yahoo.com is responsible for yahoo.com.
It also told me what ns1.yahoo.com's IP addresses are.

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!



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.


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
wgl
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


Terminal — 80×24
9)
IP 68.180.130.15.53 > 10.10.0.47.64519: 6982*- 1/0/1 A 68.142.254.15 (63)
IP6 2001:503:83eb::30.53 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64780: Flags
[.], ack 63, win 65535, length 0
IP6 2001:503:83eb::30.53 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64780: Flags
[F.], seq 698, ack 63, win 65535, length 0
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64780 > 2001:503:83eb::30.53: Flags
[.], ack 699, win 33120, length 0
IP6 2001:503:83eb::30.53 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64779: Flags
[.], ack 63, win 65535, length 0
IP6 2001:503:83eb::30.53 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64779: Flags
[F.], seq 698, ack 63, win 65535, length 0
IP 68.180.130.15.53 > 10.10.0.47.59491: 56836*- 0/1/1 (117)
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64779 > 2001:503:83eb::30.53: Flags
[.], ack 699, win 33120, length 0
IP6 2001:503:83eb::30.53 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64781: Flags
[.], ack 63, win 65535, length 0
IP 68.180.130.15.53 > 10.10.0.47.63930: 21208*- 1/0/1 A 68.142.254.15 (63)
IP6 2001:503:83eb::30.53 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64781: Flags
[F.], seq 698, ack 63, win 65535, length 0
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.64781 > 2001:503:83eb::30.53: Flags
[.], ack 699, win 33120, length 0
IP 68.180.130.15.53 > 10.10.0.47.62285: 6352*- 0/1/1 (117)
$

Links

- DNS Query Name Minimisation to Improve Privacy:

  https://tools.ietf.org/html/rfc7816
- APNIC DNS Query Privacy Blog Post:

  https://blog.apnic.net/2020/09/11/dns-query-privacy-revisited/
- DNS tcpdump by example:

  https://www.netmeister.org/blog/dns-tcpdump.html
- DNS packet capture homework:

  https://stevens.netmeister.org/615/s21-hw3.html