**COMP9331 LAB3 – DNS**

Changfeng LI(z5137858)

**Exercise 1,2: (not needed in the report)**

**Exercise 3: Digging into DNS**

Qs3-1: What is the IP address of www.cecs.anu.edu.au . What type of DNS query is sent to get this answer?

Qs3-2: What is the canonical name for the CECS ANU web server? What is its IP address? Suggest a reason for having an alias for this server.

Qs3-3: What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

Qs3-4: What is the IP address of the local nameserver for your machine?

Qs3-5: What are the DNS nameservers for the “cecs.anu.edu.au” domain (note: the domain name is cecs.anu.edu.au and not www.cecs.anu.edu.au )? Find out their IP addresses? What type of DNS query is sent to obtain this information?

Qs3-6: What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?

Qs3-7: Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not www.yahoo.com ). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response to determine the answer)

Qs3-8: Repeat the above (i.e. Question 7) but use one of the nameservers obtained in 3-5, What is the result?

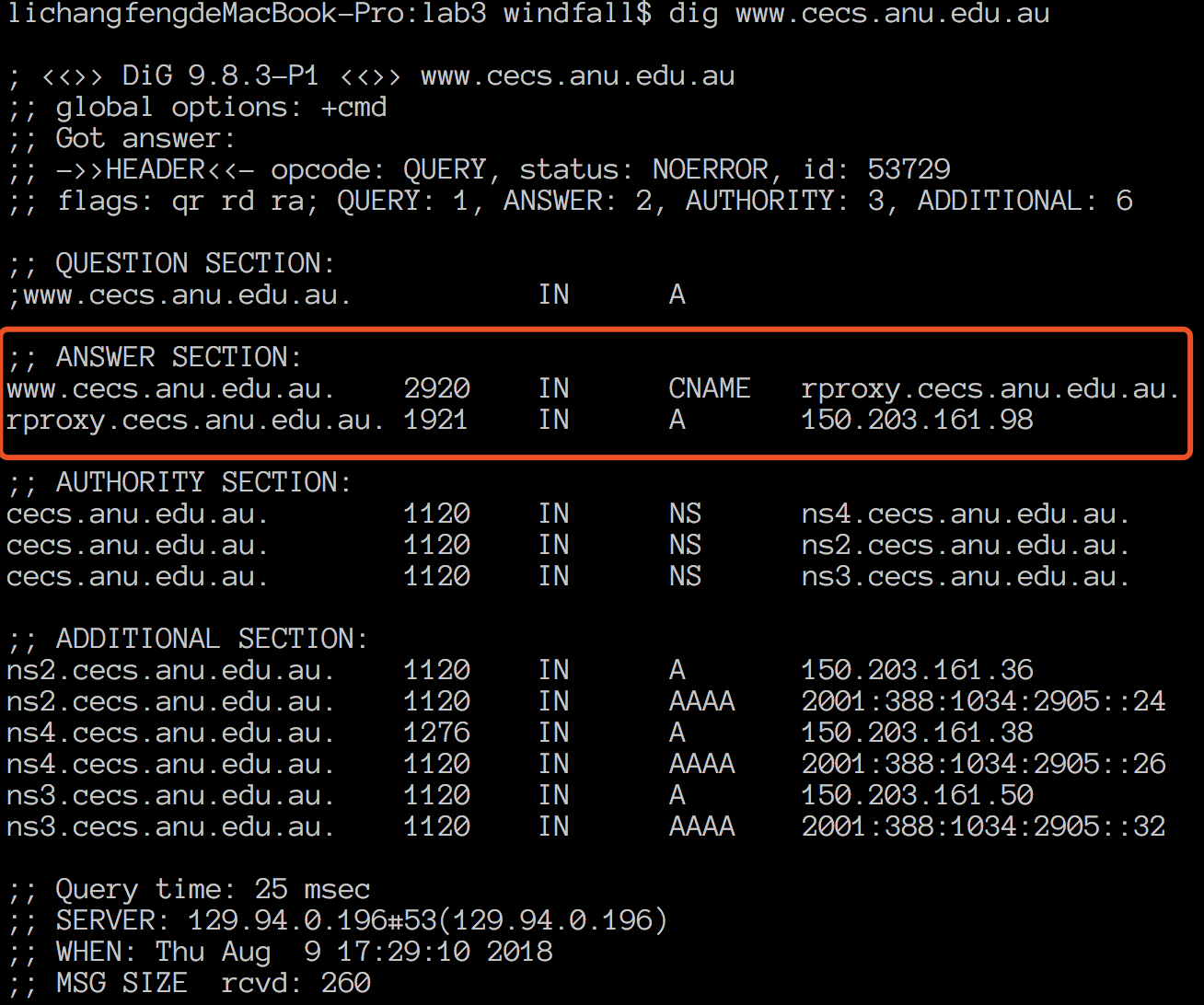
Qs3-9: Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?

Qs3-10: In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this second server to find the authoritative nameserver for the "edu.au." domain. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au". Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host. How many DNS servers do you have to query to get the authoritative answer?

Qs3-11: Can one physical machine have several names and/or IP addresses associated with it?

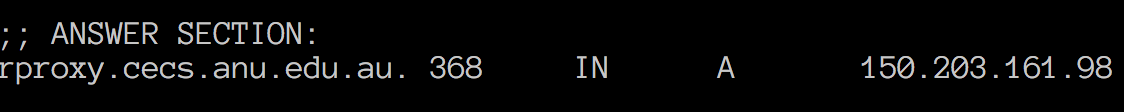
-----------

As3-1:



The IP Address is 150.203.161.98, and of Type A.

As3-2: We can find info from CNAME area that it is “rproxy.cecs.anu.edu.au”.



The IP address is 150.203.161.98 the same.

The main reason why this server has an alias is that it is the website for university, so the alias can help people remember it.

As3-3:

The Authority section indicates the server(s) that are the ultimate authority for answering DNS queries about that domain.

The Additional sections give the information of which DNS servers provide this authoritative answers and shows their IP.

As3-4:

129.94.0.196

As3-5:

The DNS server are listed below:  
ns2.cecs.anu.edu.au. => 150.203.161.36

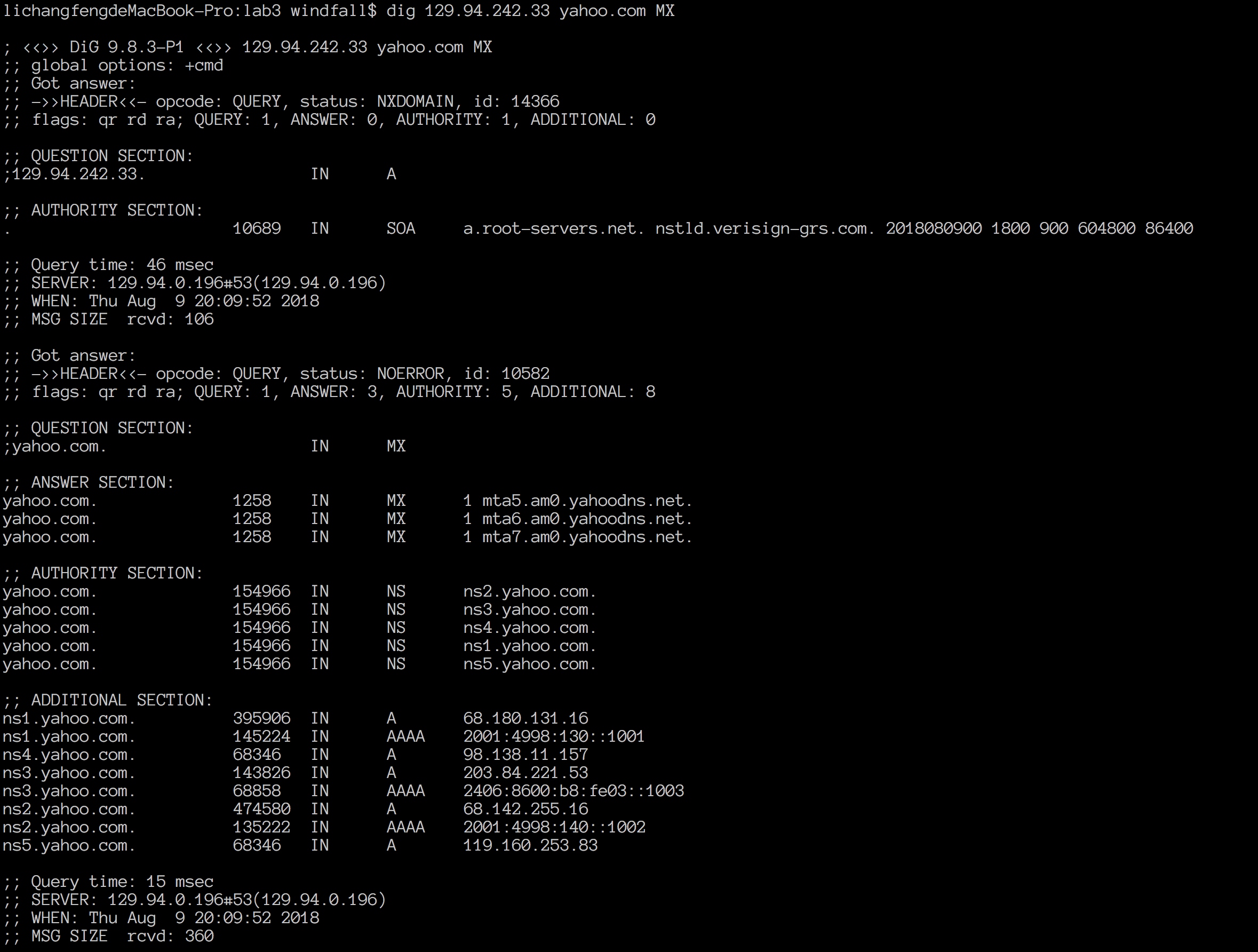
ns4.cecs.anu.edu.au. => 150.203.161.38

ns3.cecs.anu.edu.au. => 150.203.161.50

Type: NS

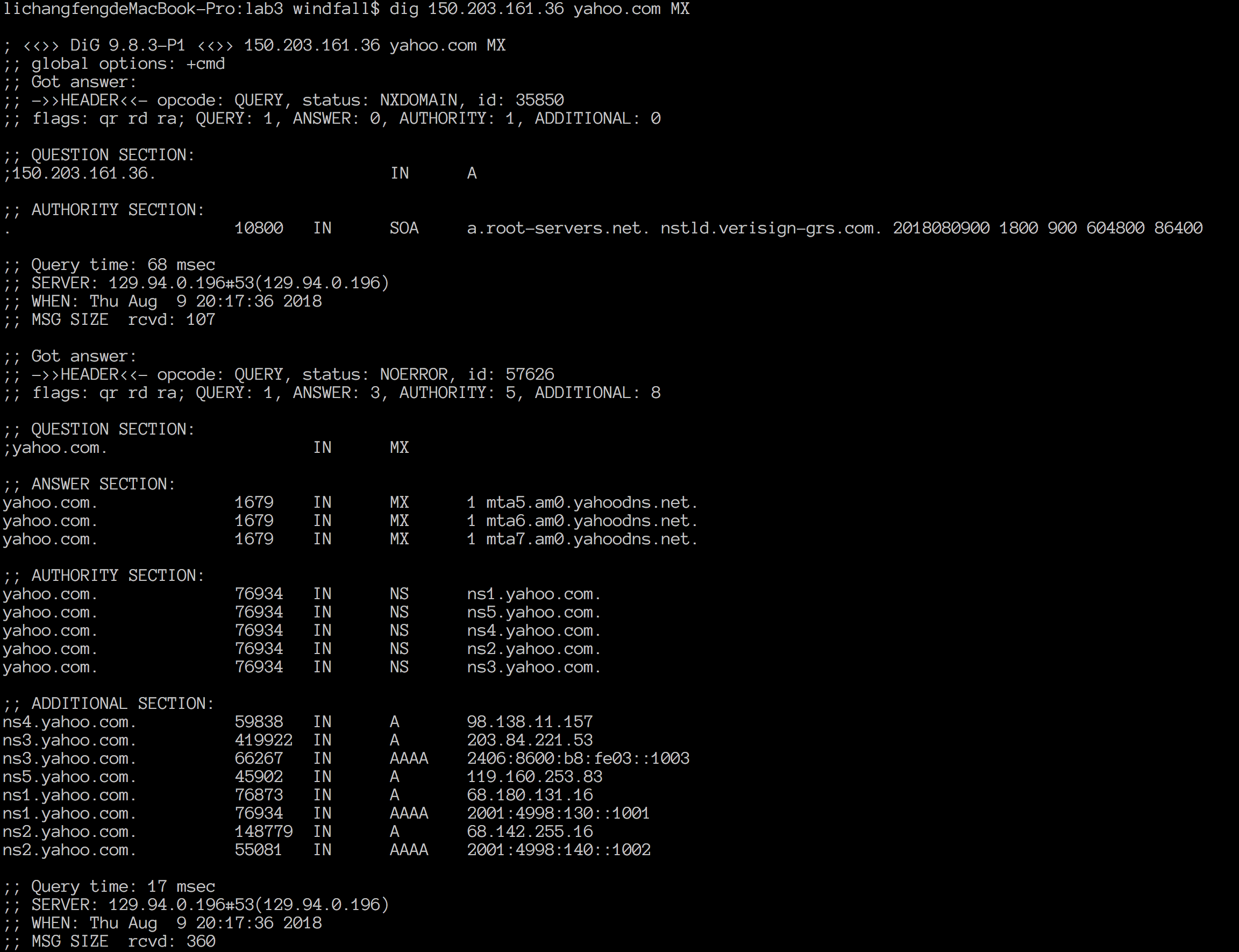
As3-6:

As3-7:



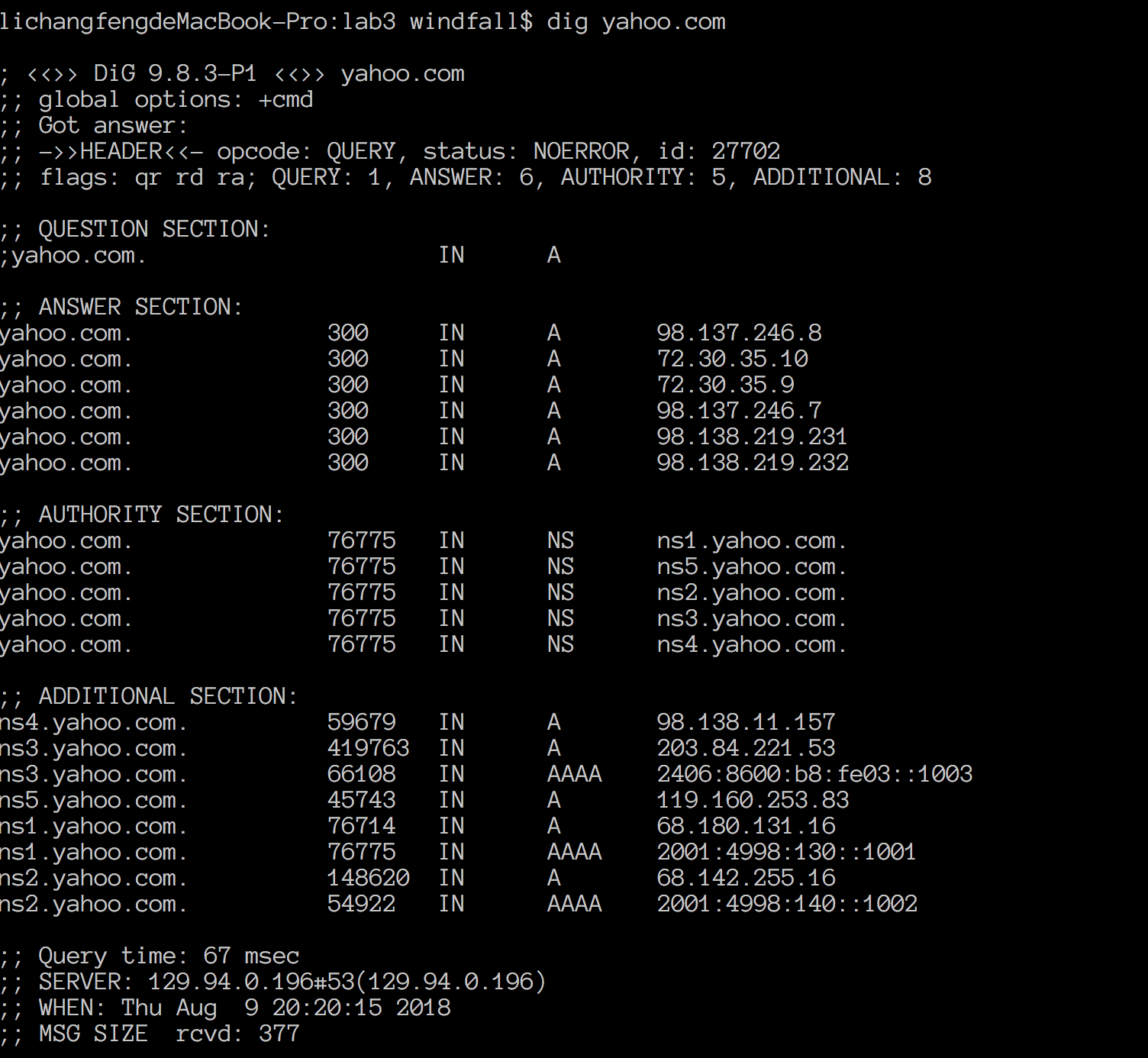
No, because I don’t find AA section, which means authoritative answers.

As3-8:

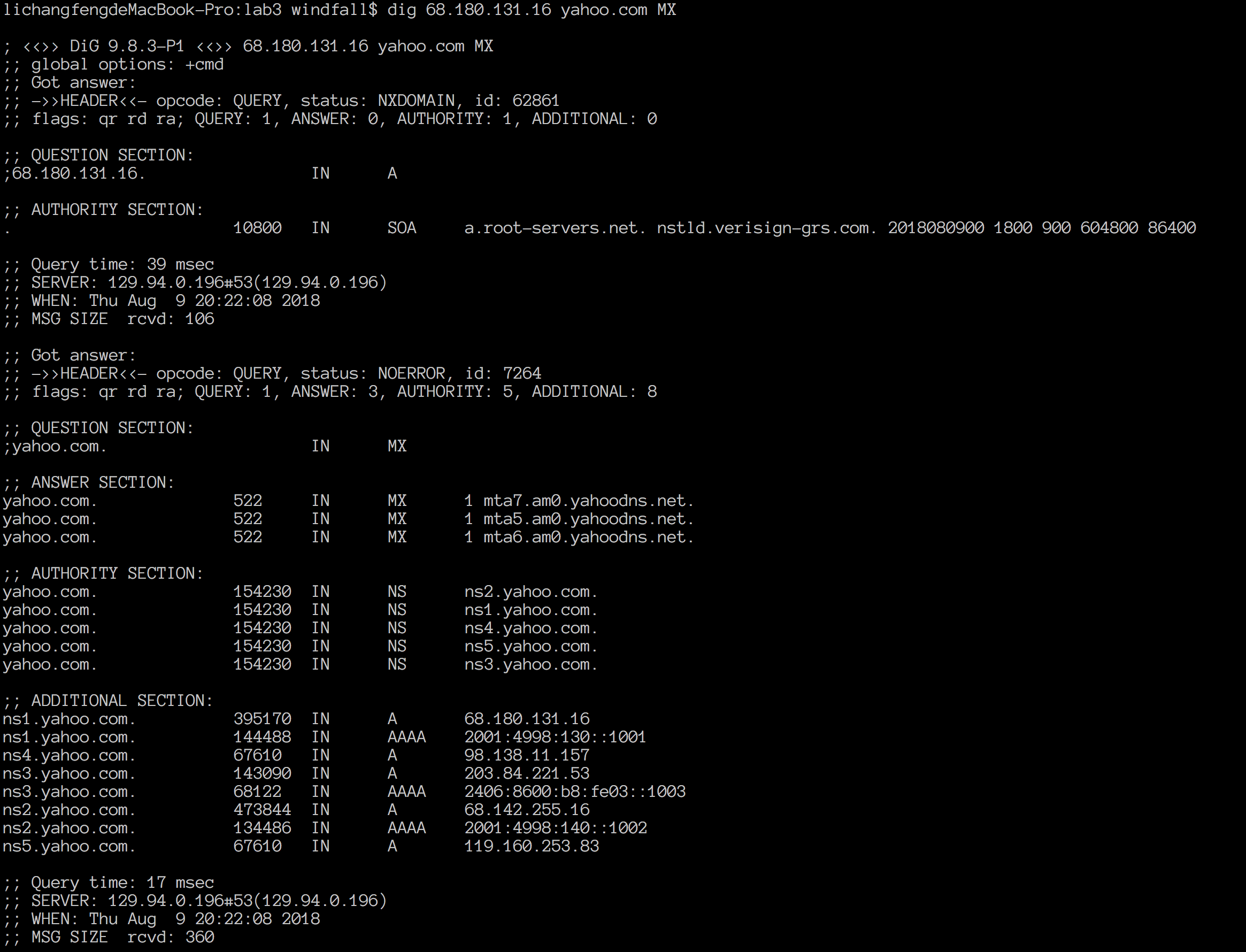


As3-9:

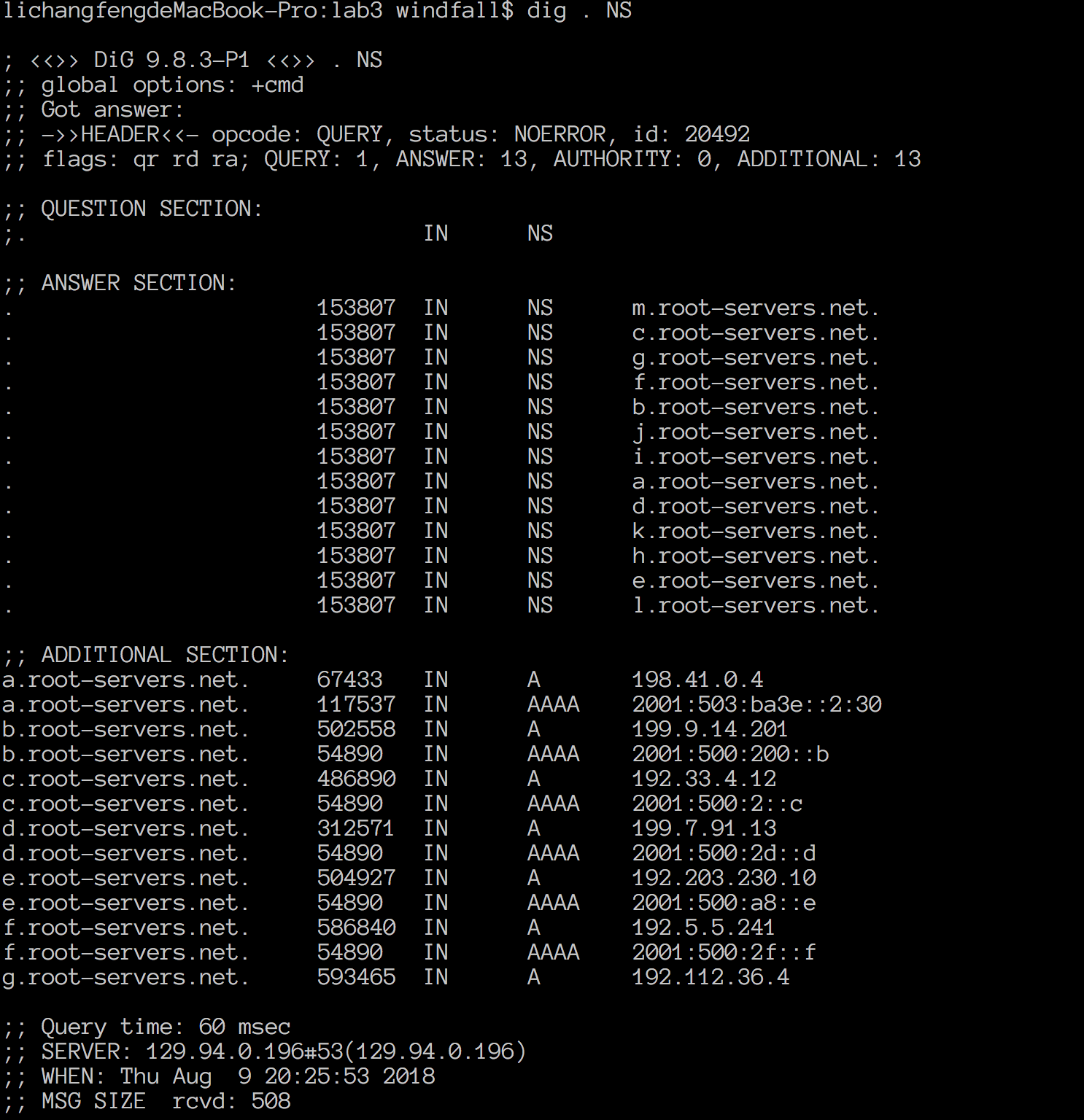
Firstly, we dig yahoo.com, we get



Then we send MX query, we get



As3-10:



1. dig @198.41.0.4 lyre00.cse.unsw.edu.au .au Authoritative NS
2. dig @58.65.254.73 lyre00.cse.unsw.edu.au .edu.au Authoritative NS
3. dig @37.209.192.5 lyre00.cse.unsw.edu.au .unsw.edu.au Authoritative NS
4. dig @129.94.0.192 lyre00.cse.unsw.edu.au .cse.unsw.edu.au Authoritative NS
5. dig @129.94.242.2 lyre00.cse.unsw.edu.au lyre100.cse.unsw.edu.au A record

IP of my machine: 129.94.210.20

As3-11:

In most cases, a physical device have a corresponding name and a corresponding IP address, but we can configure so that it will have multiple name and address. To some extent, an IP always has multiple name for different usages, that’s “alias”.

**Exercise 4: (Code only)**