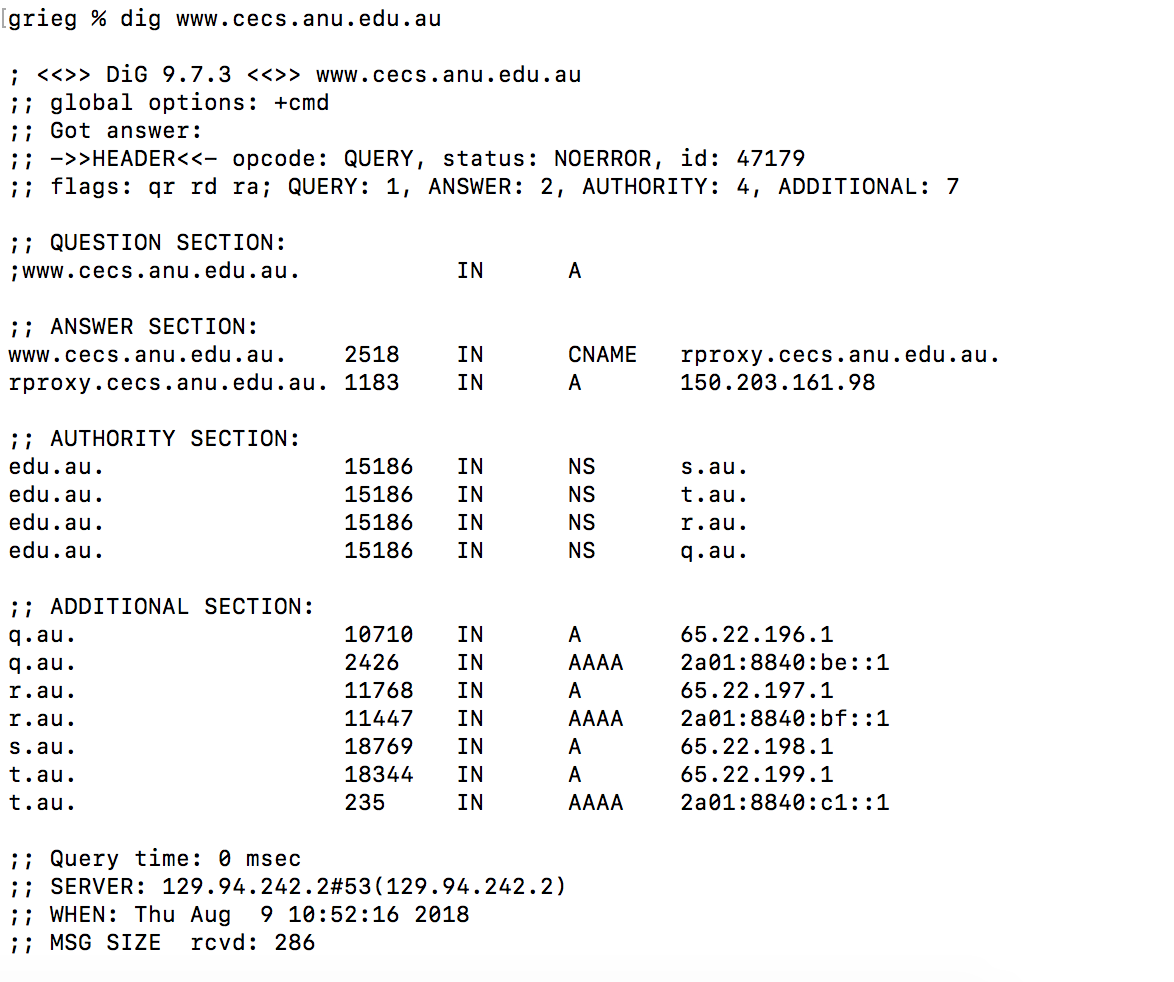
**Exercise 3: Digging into DNS (marked, include in the lab report)**

Question 1. What is the IP address of [www.cecs.anu.edu.au](http://www.cse.unsw.edu.au/). What type of DNS query is sent to get this answer?



**The IP address is : 150.203.161.98**

**Type of DNS query: A**

Question 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.

**The canonical name: rproxy.cecs.anu.edu.au**

**The IP address is: 150.203.161.98**

**Having an alias can be used to provide multiple network addresses on a single physical interface.** **It can prove convenient when running multiple services.** **If the IP address ever changes, one only has to record the change in one place within the network.**

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

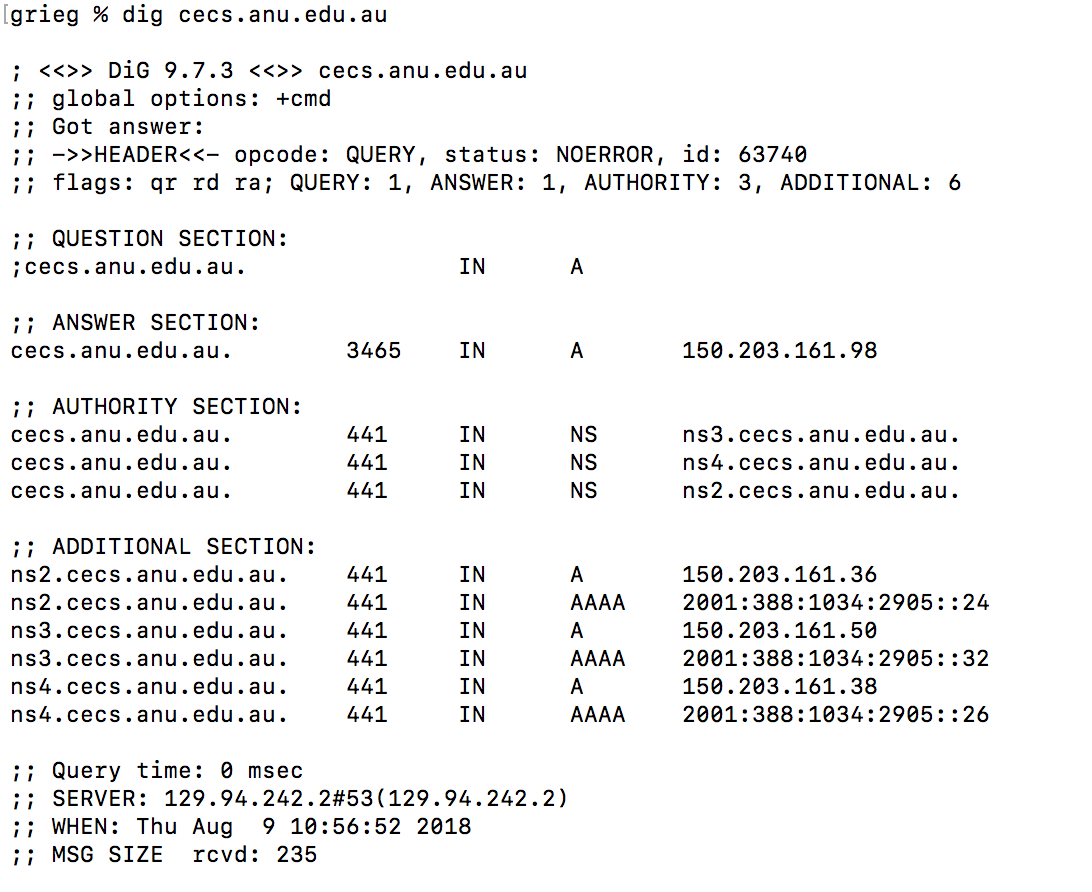
**An authoritative stores all DNS names in the domain that it has authority for.**

**Additional section is the authoritative servers that may be used.**

Question 4. What is the IP address of the local nameserver for your machine?

**IP: 129.94.242.2 (In Server Section)**

Question 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](http://www.cse.unsw.edu.au/))? Find out their IP addresses? What type of DNS query is sent to obtain this information?



**They are:**

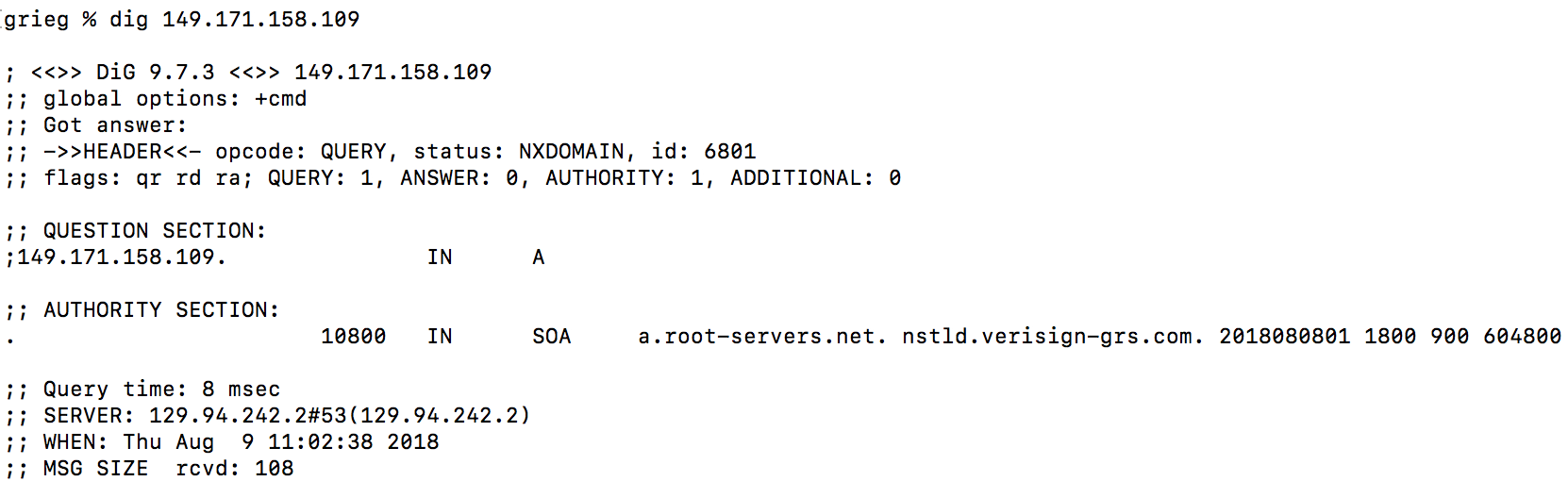
**ns2.cecs.anu.edu.au 150.203.161.36**

**ns3.cecs.anu.edu.au 150.203.161.50**

**ns4.cecs.anu.edu.au 150.203.161.38**

**The type of DNS query is NS.**

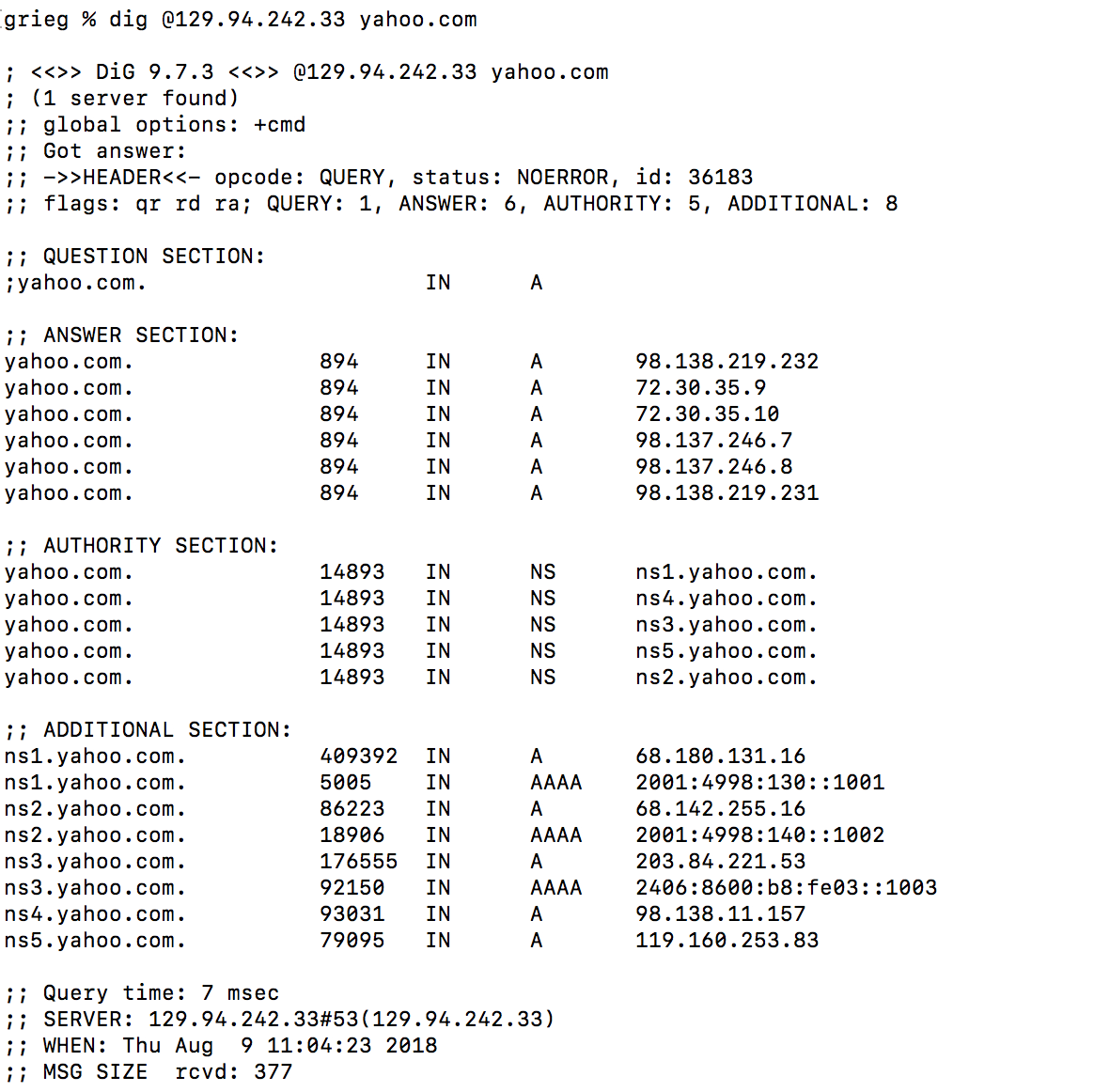
Question 6. What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?



**DNS name : a.root-servers.net nstld.verisign-grs.com**

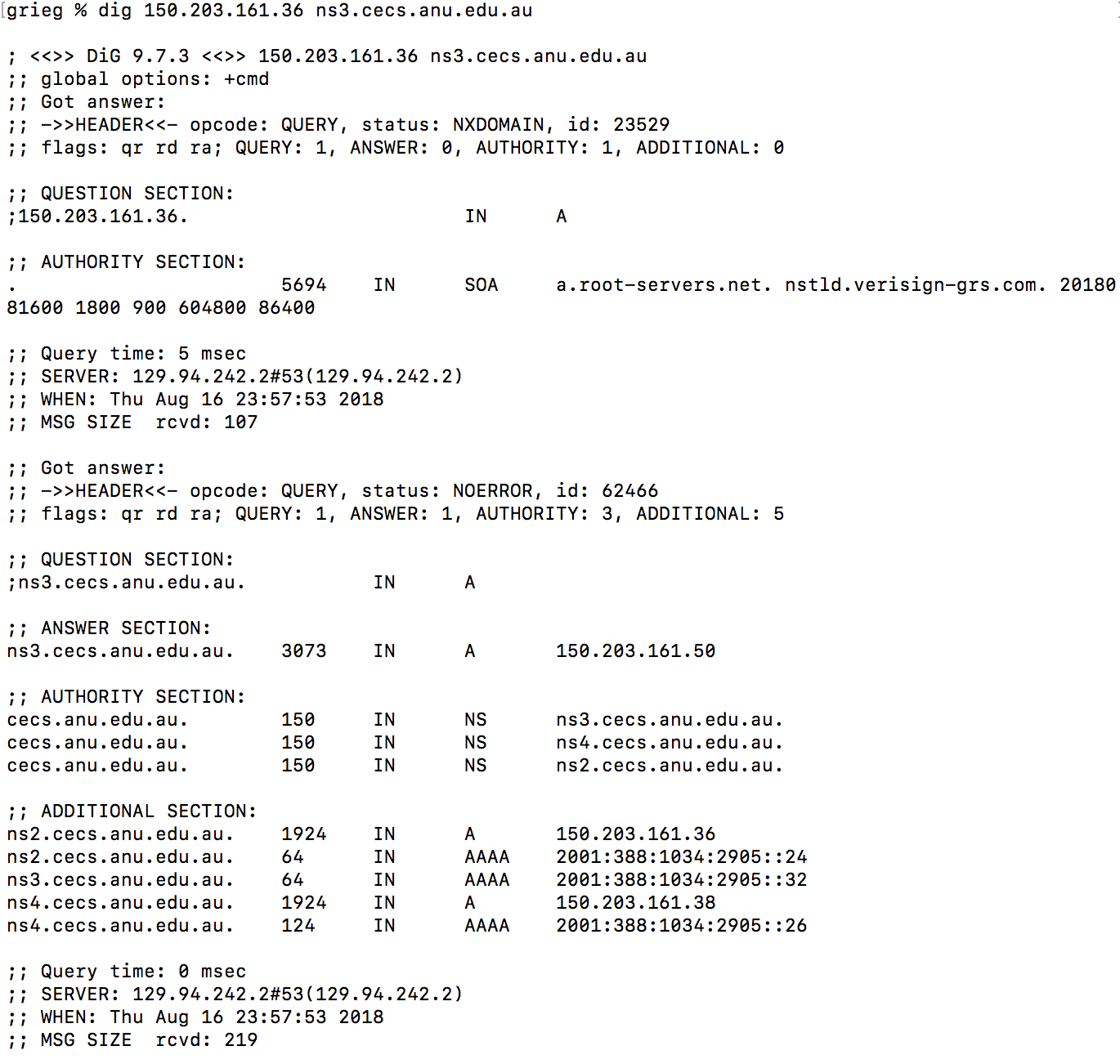
**Type: SOA**

Question 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](http://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)

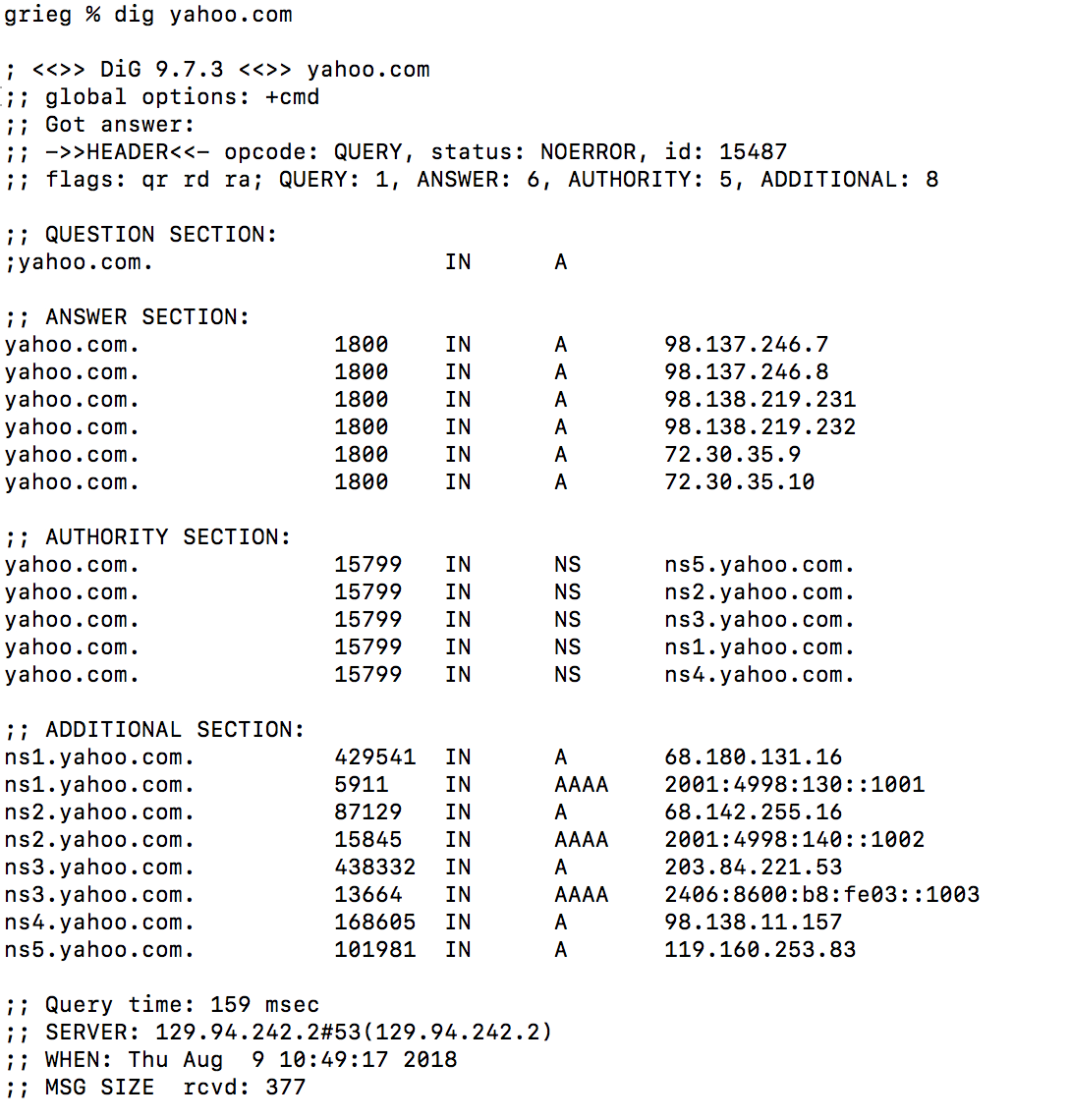


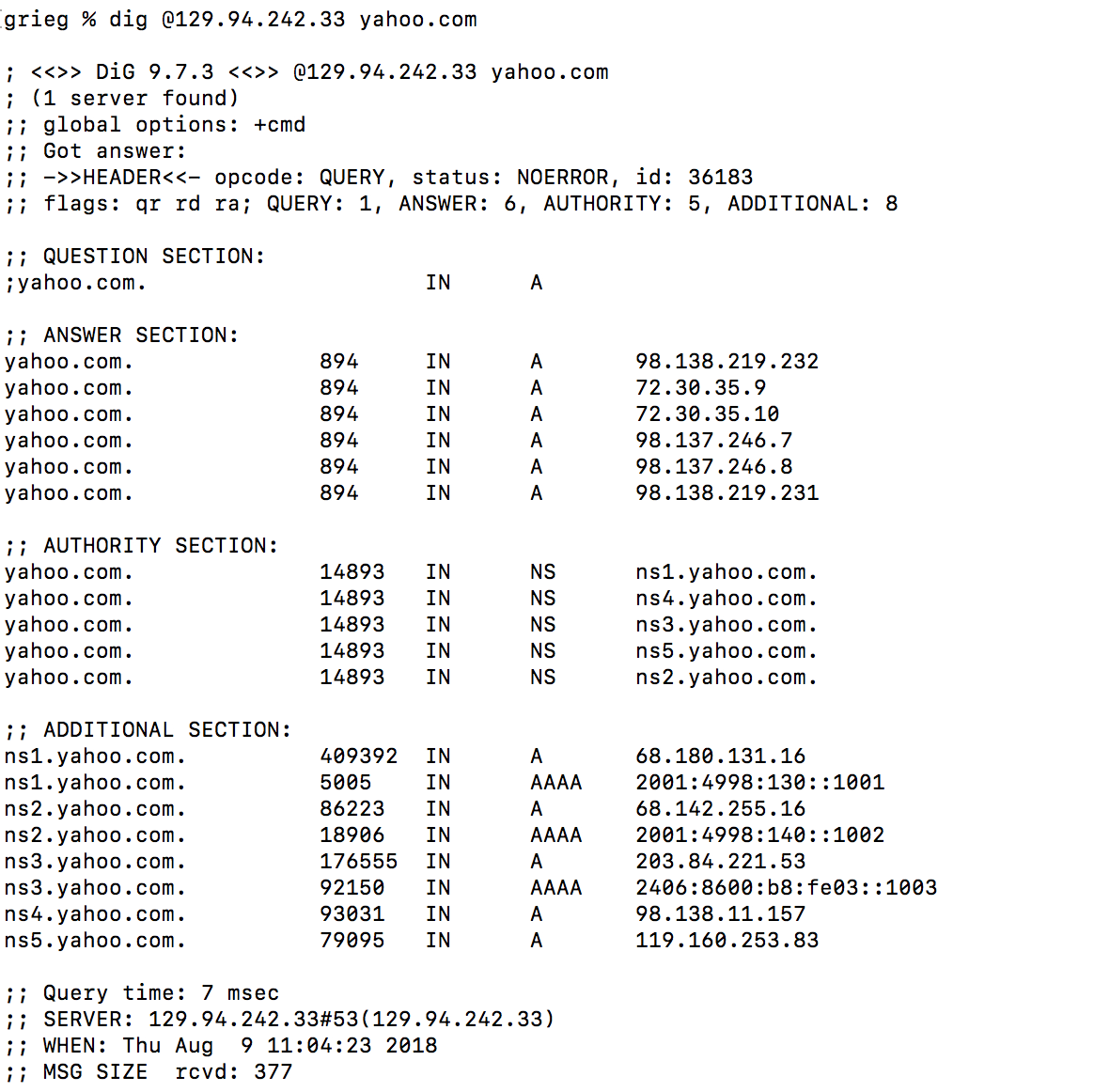
**No, it is not an authoritative answer, because there is not an “aa” flags which means “authoritative answer” in Flags.**

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



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

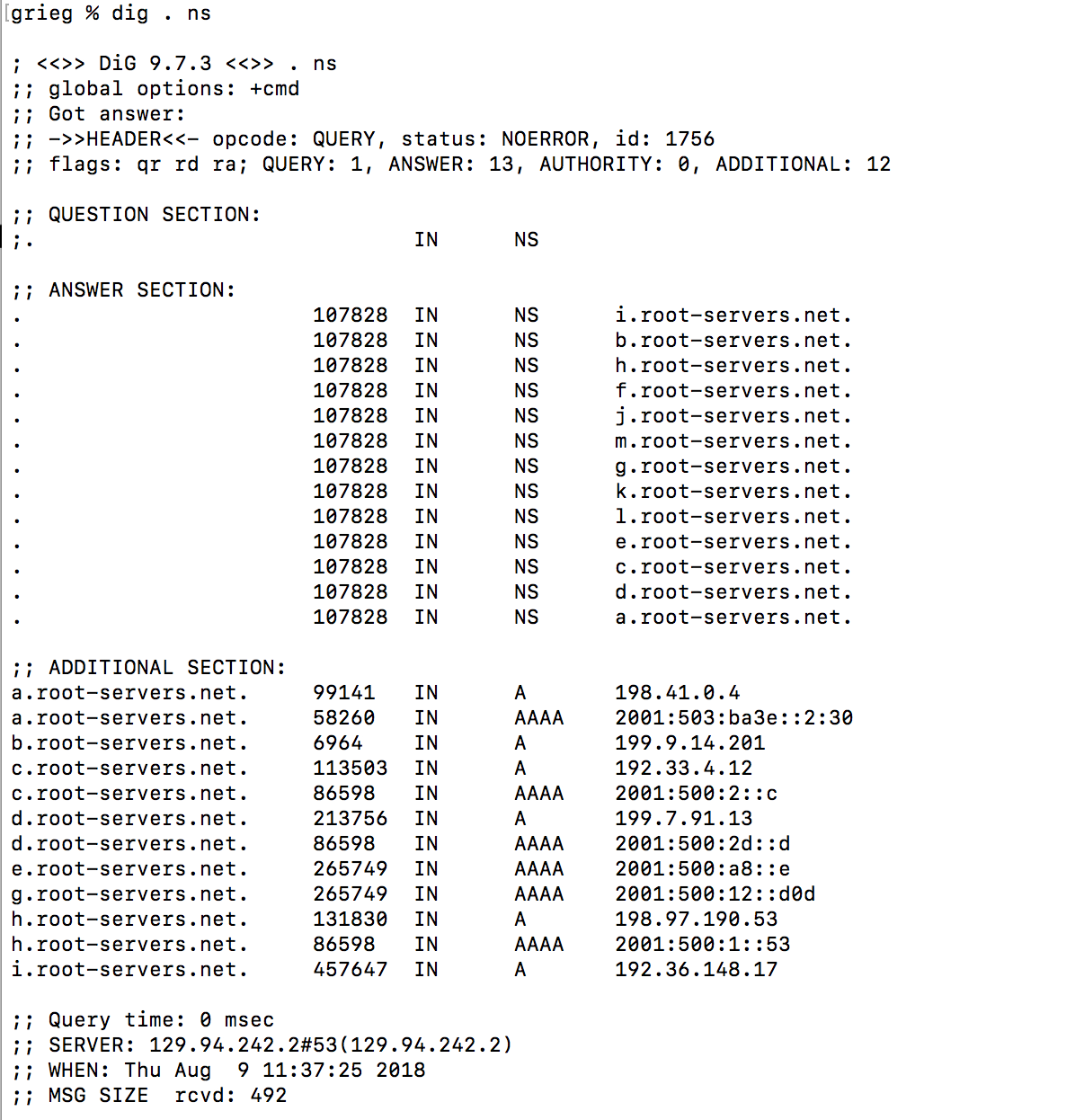




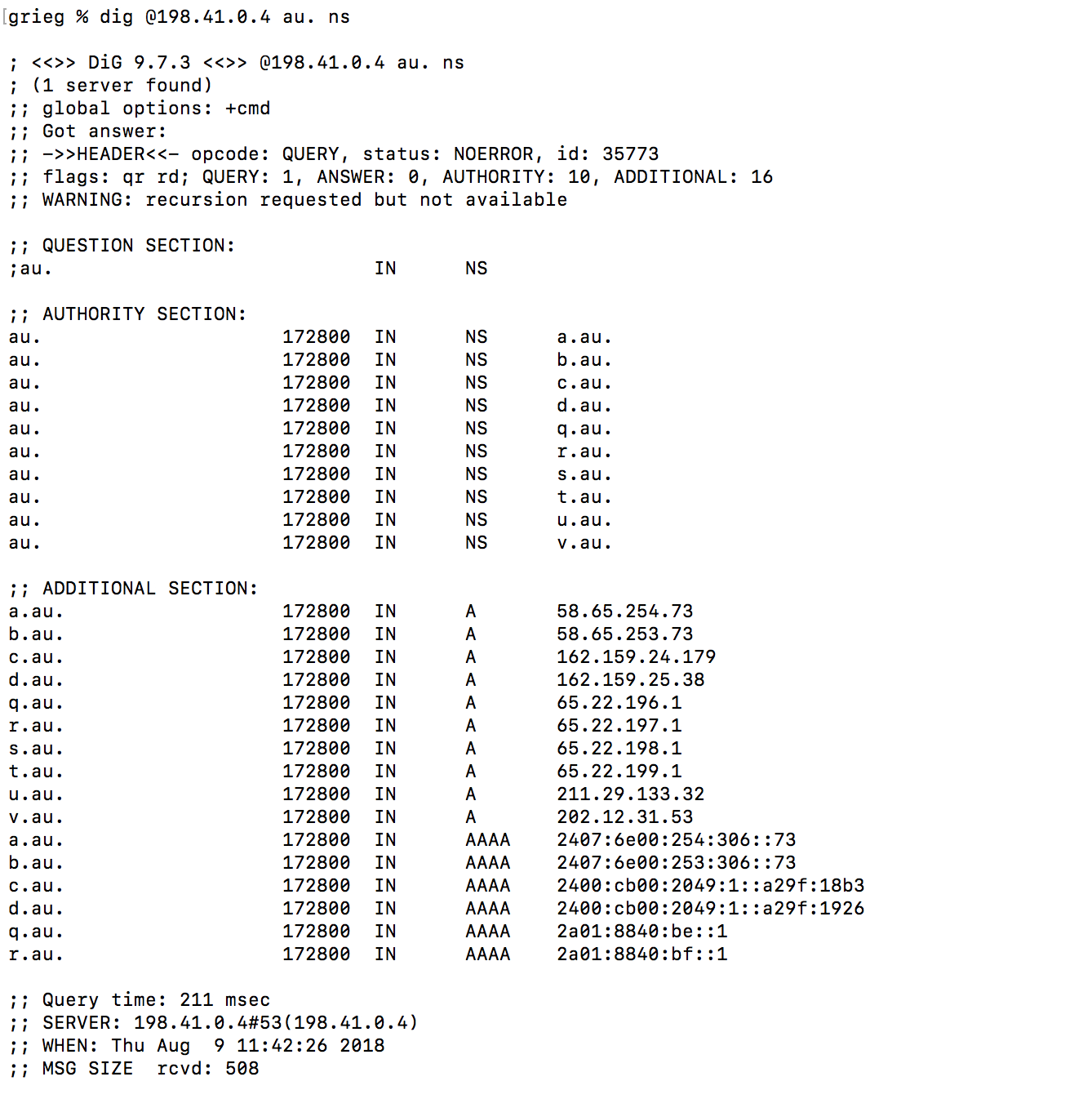
Type: NS

Question 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?

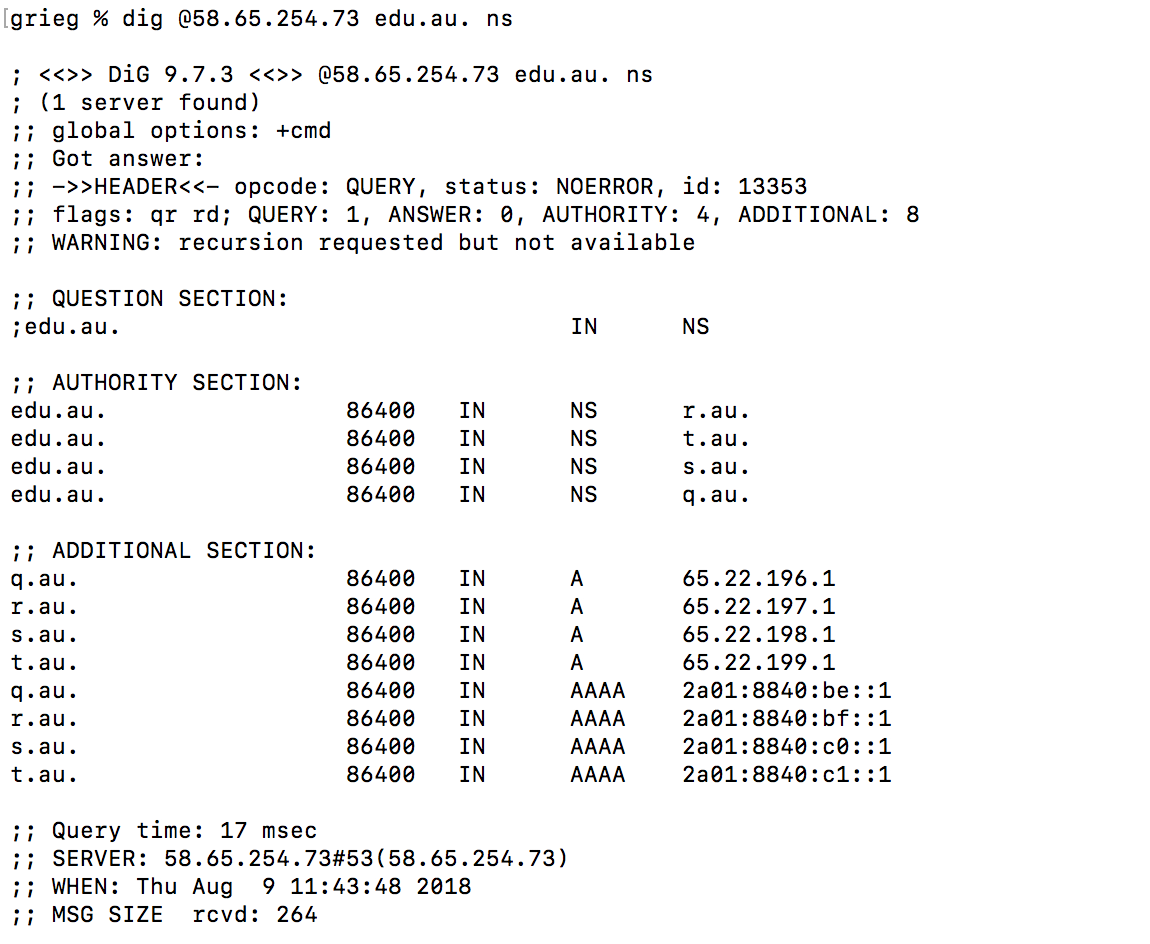
1.



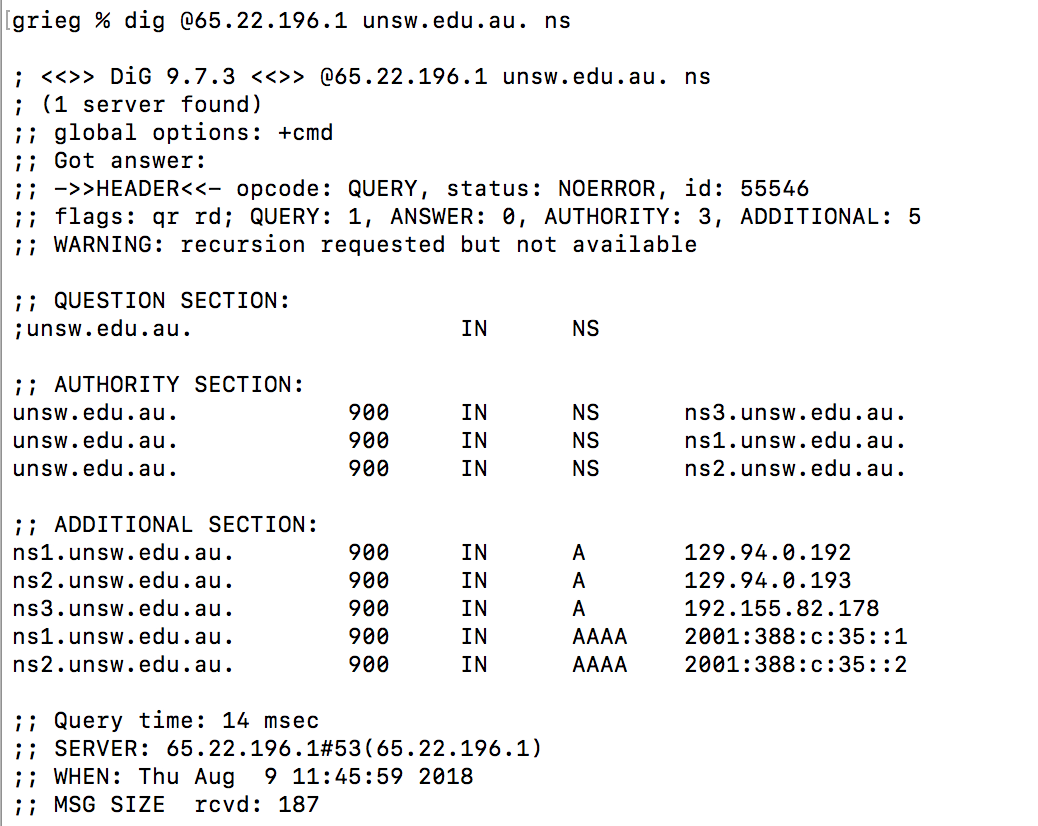
2.



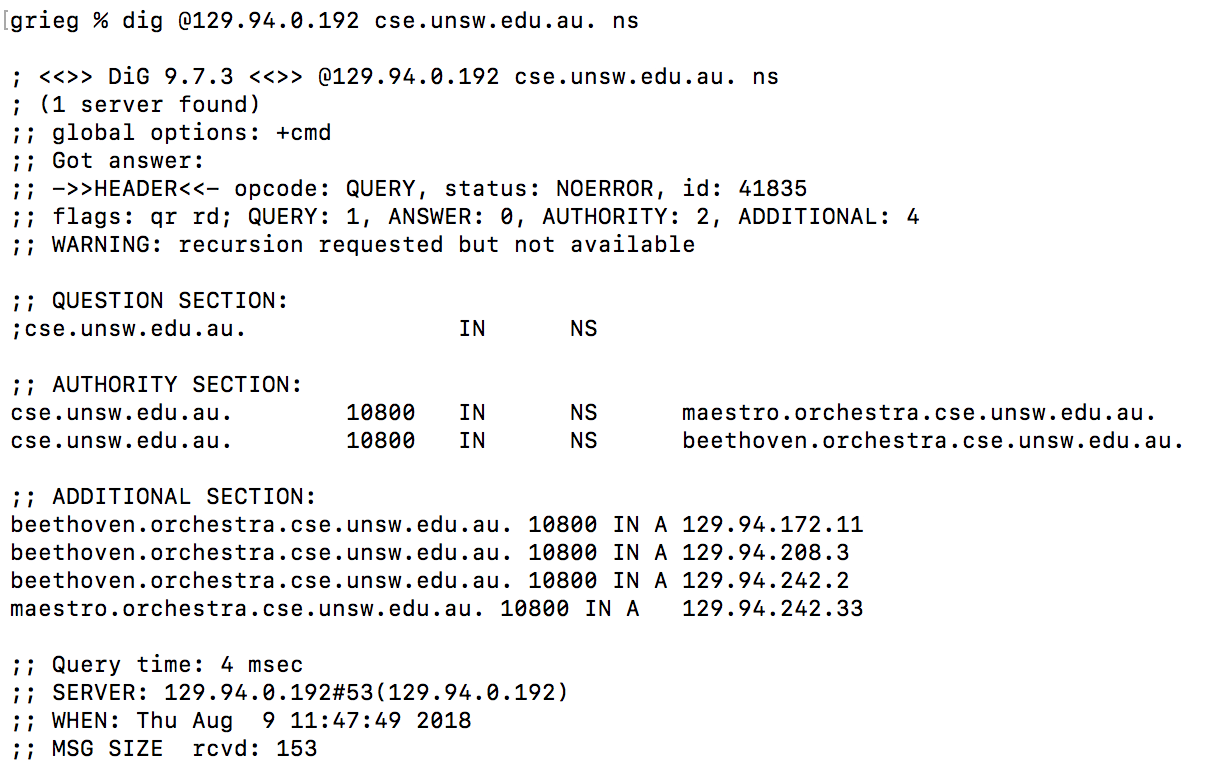
3.



4.



5.



**My machine ip address is 124.94.242.2**

**So there are 5 DNS servers to query to get authoritative answer.**

Question 11. Can one physical machine have several names and/or IP addresses associated with it?

**Yes, a machine may have several network interfaces and a network interface can have several IP address associated with it at any given time. So an IP address may have associated with several names ("aliases").  To obtain the canonical name for the machine, use dig with query type=cname.**