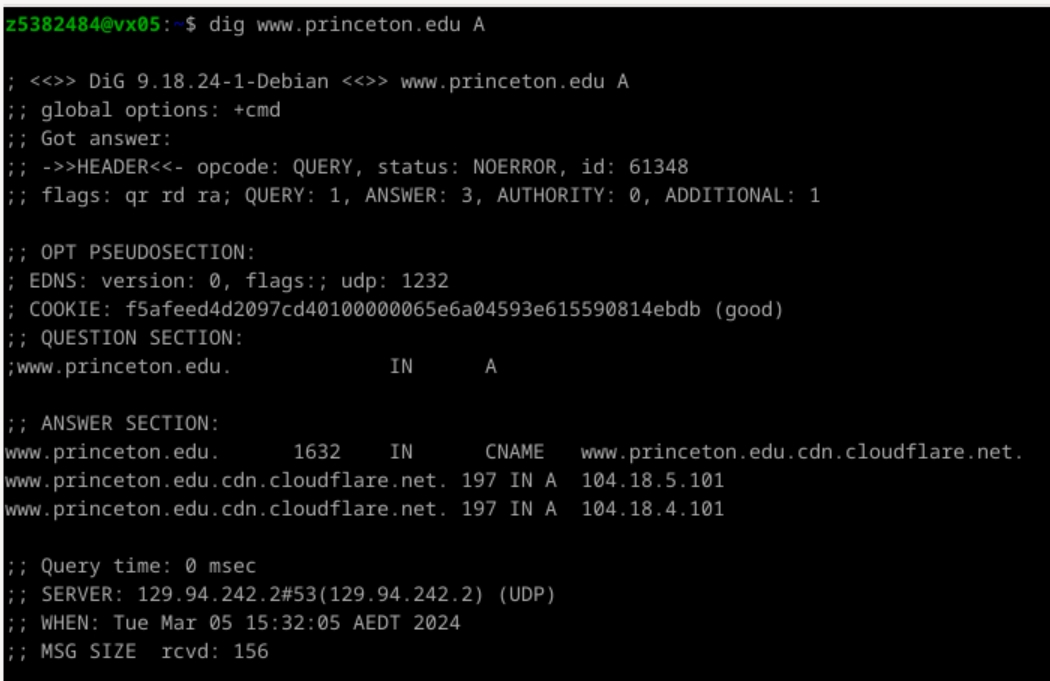
Lab3

LinXing Jia-z5382484

Exercise 3:

Q1:

The IP address of [www.princeton.edu](http://www.princeton.edu) is 104.18.5.101. Type A



Q2:

The canonical name for the Princeton webserver is [www.princeton.edu](http://www.princeton.edu).cdn.cloudflare.net. The reason for setting an alias for the server may be to provide a more concise and easy-to-remember access method. The canonical name is relatively long, which is inconvenient for users to remember and input.

Q3:

In the DNS response, HEADER provides basic information about the response, and OPT PSEUDOSECTION provides some additional extended information. HEADER contains opcode: operation code, status: status code, id: unique identifier, used to identify the association between query and response. , flags: flag bit, QUERY: query quantity, etc.,

OPT PSEUDOSECTION contains:

EDNS: Extended DNS, including the EDNS version and other related information.

COOKIE: Cookie used to verify whether the communication between the server and the client is correct.

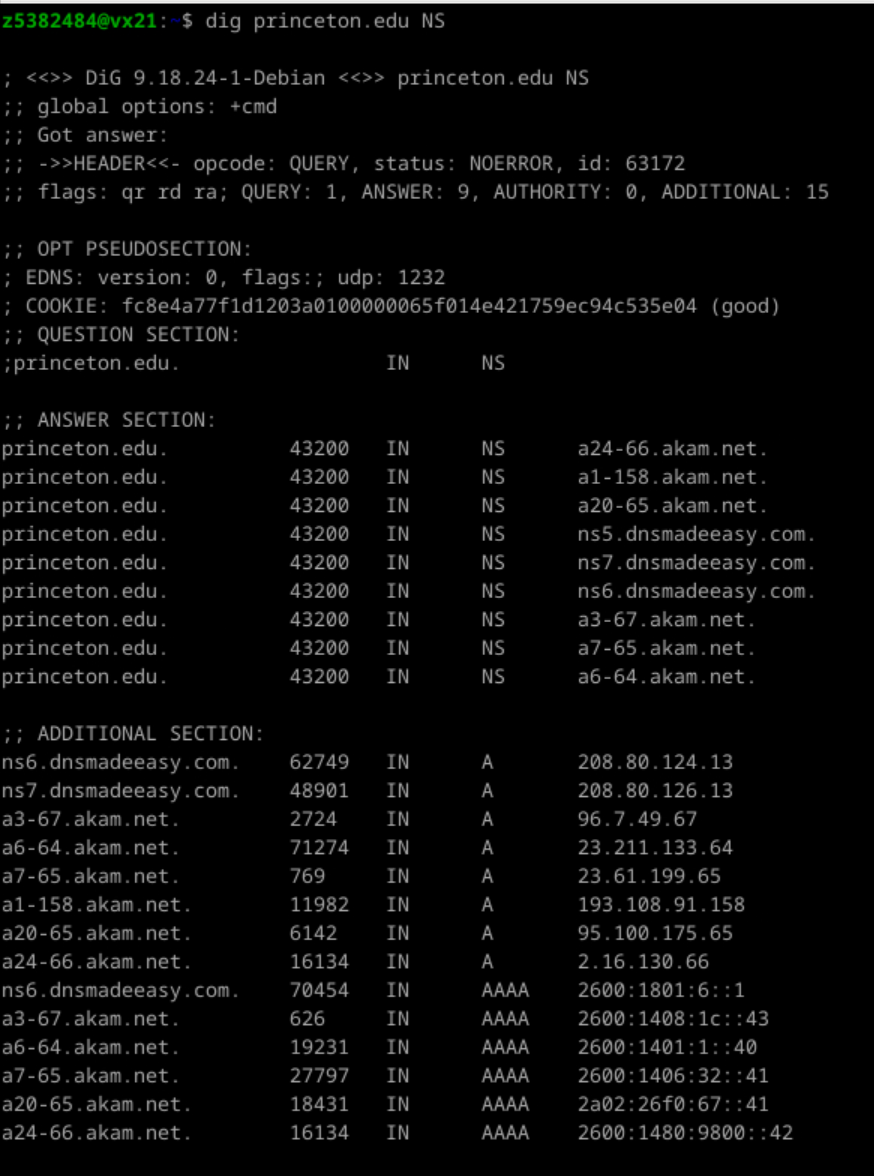
Q4:

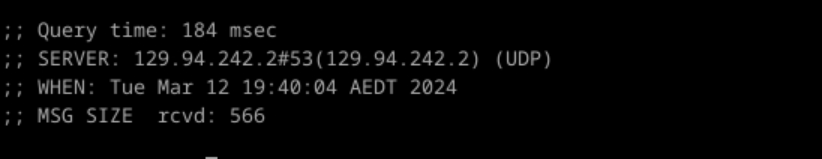
The information about the local nameserver is included at the bottom of the output above, 129.94.242.2. This is the local DNS server for the CSE network.

Q5:

The DNS name server records of the "princeton.edu" domain were queried through the “dig princeton.edu NS”command. Their names and IP addresses are shown in the following table.

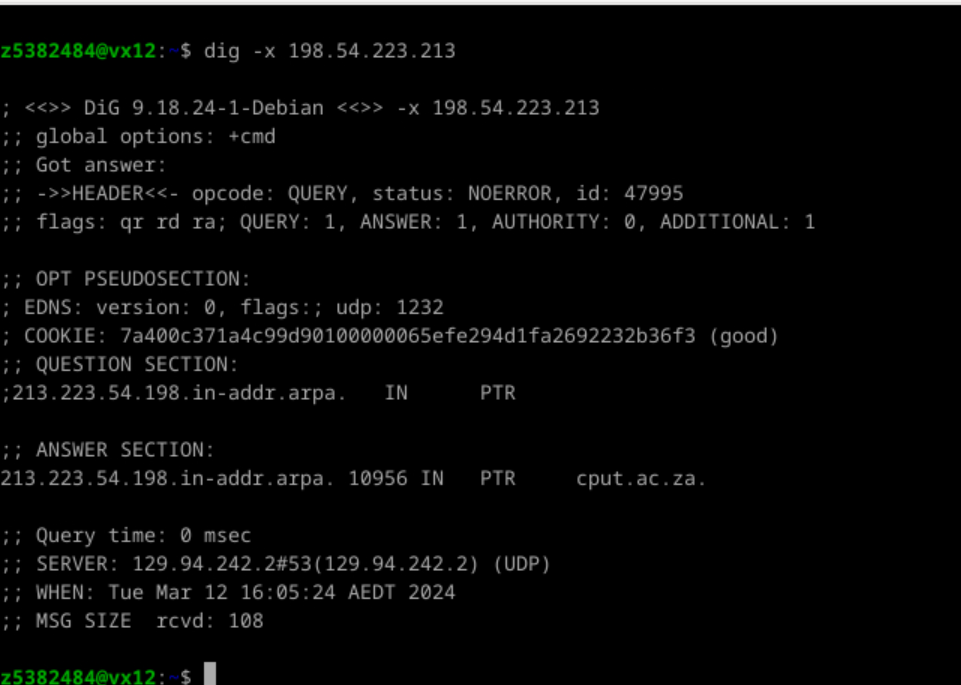
|  |  |
| --- | --- |
| Name Servers | IP address |
| ns6.dnsmadeeasy.com. | 208.80.124.13 |
| ns7.dnsmadeeasy.com. | 208.80.126.13 |
| a3-67.akam.net. | 96.7.49.67 |
| a6-64.akam.net. | 23.211.133.64 |
| a7-65.akam.net. | 23.61.199.65 |
| a1-158.akam.net. | 193.108.91.158 |
| a20-65.akam.net. | 95.100.175.65 |
| a24-66.akam.net. | 2.16.130.66 |





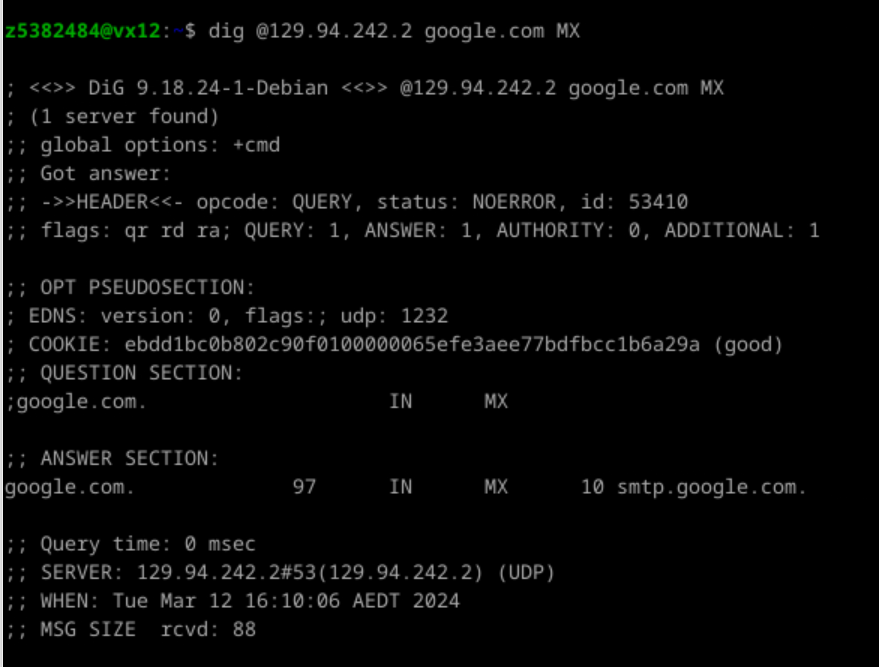
Q6:

The hostname corresponding to 198.54.223.213 is cput.ac.za, The dig -x command can be used to perform reverse DNS queries and find the corresponding domain name through a given IP address.



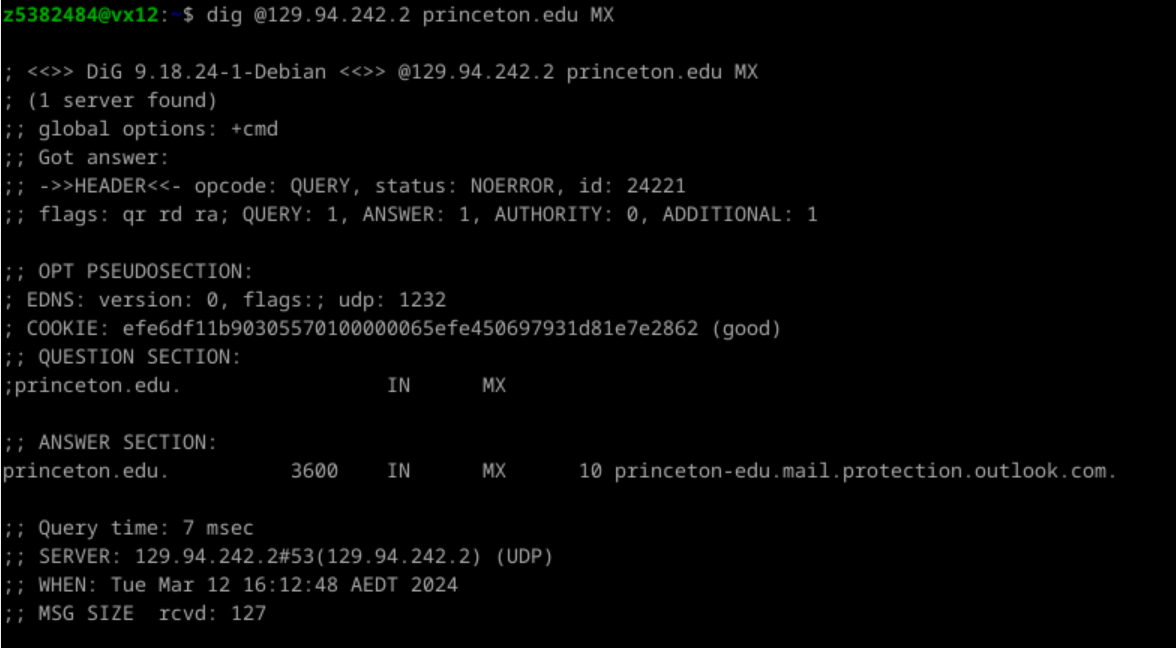
Q7:

We see that the server we queried cannot give us an authoritative answer because “AA” is not included in the flag. This is because it only has permissions on the cse.unsw.edu.au domain, but not on the google domain.



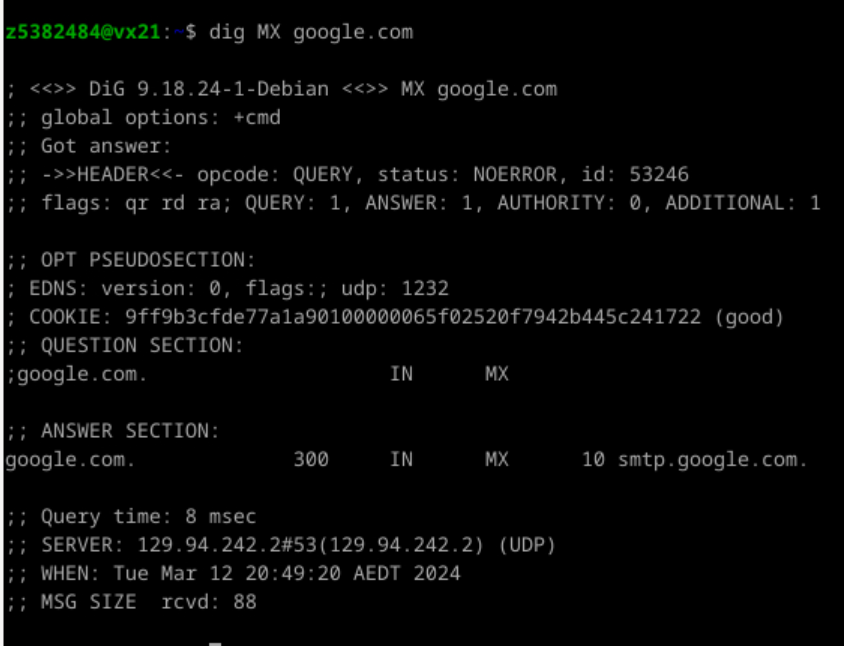
Q8:

Repeated the operation in Q7, but also did not get the authoritative answer.



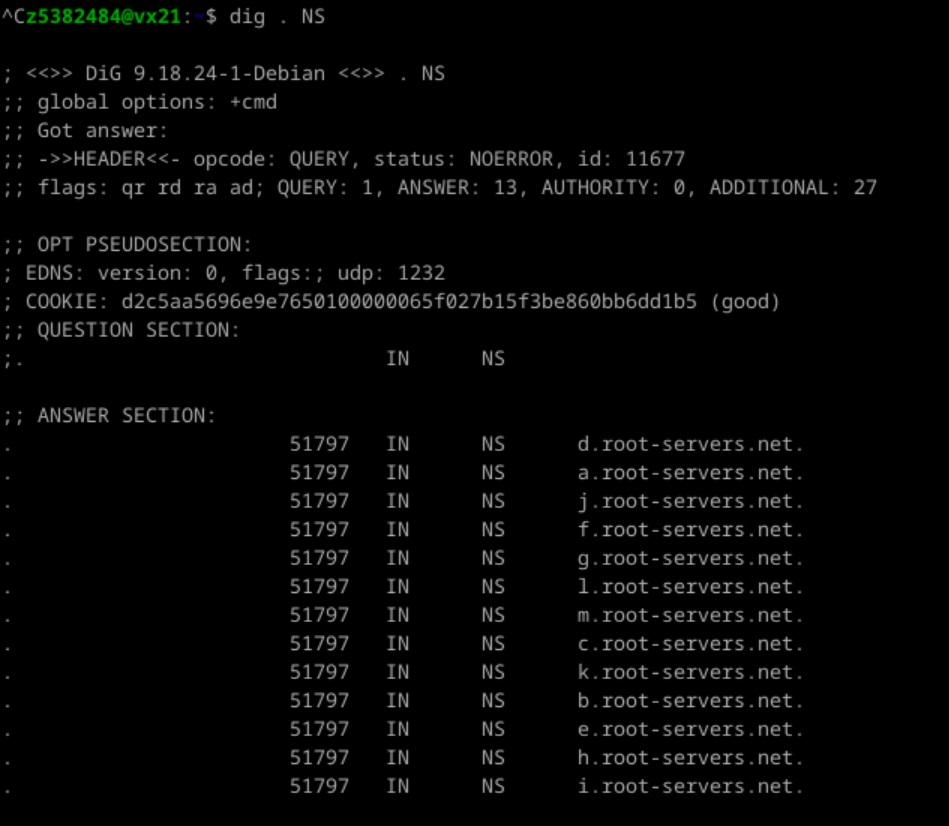
Q9:

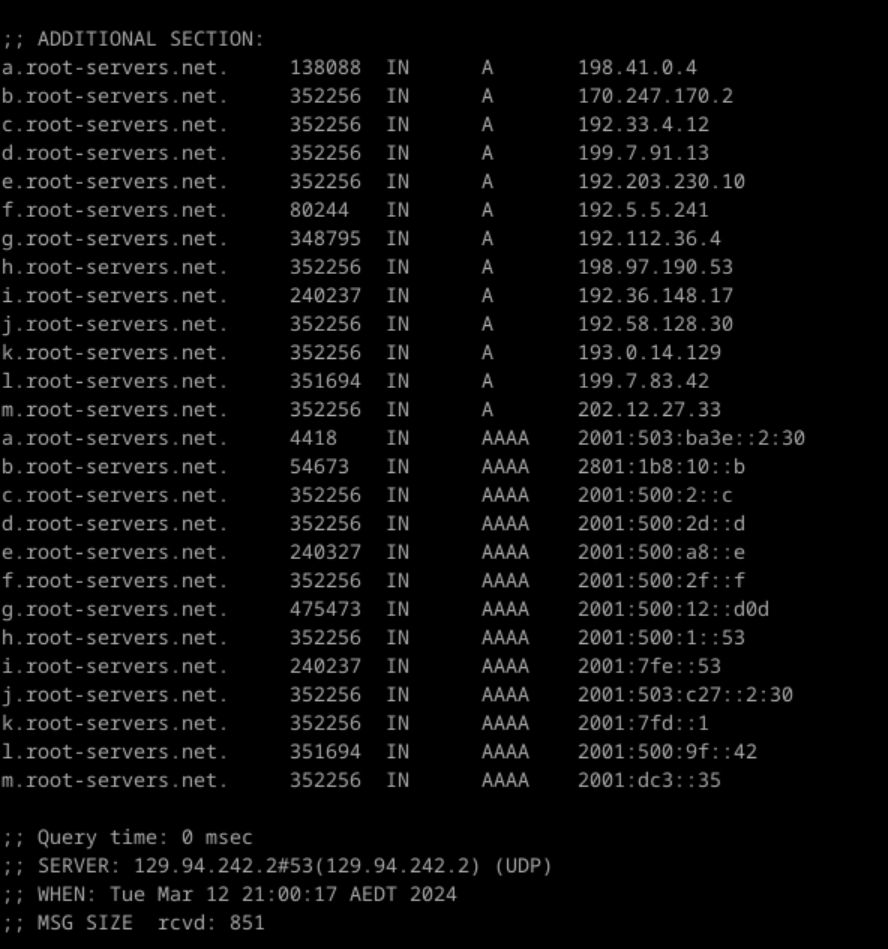
Use dig to send an MX (Mail Exchange) DNS query. This type of DNS query is specifically used to retrieve mail server information for a domain.



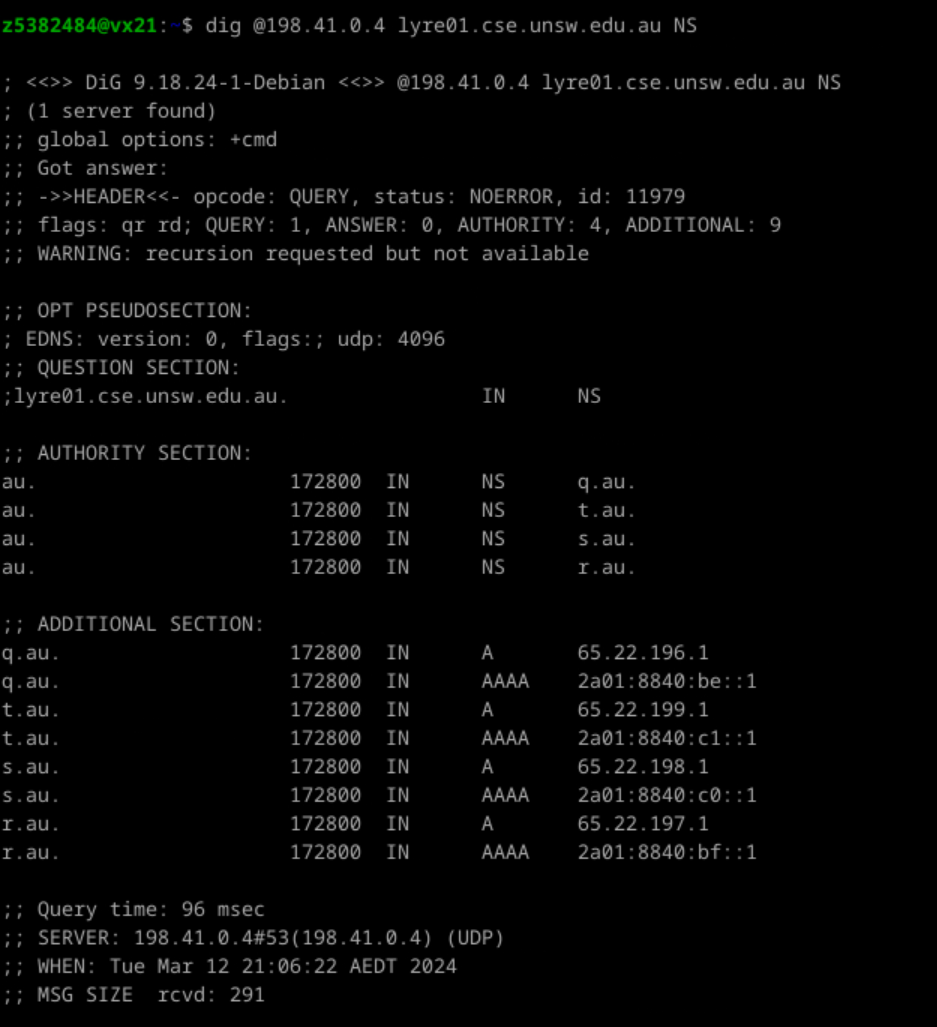
Q10:

Suppose the IP address we want to query is lyre01.cse.unsw.edu.au, first use NS to query the name server (root domain) of the "." domain

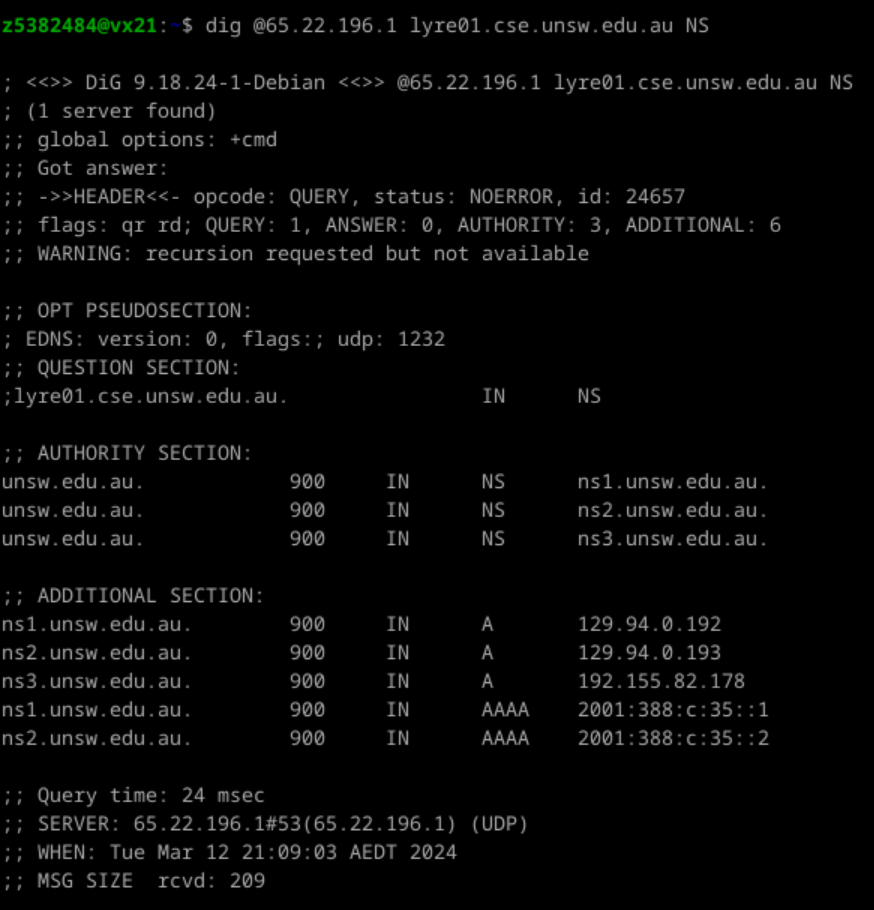




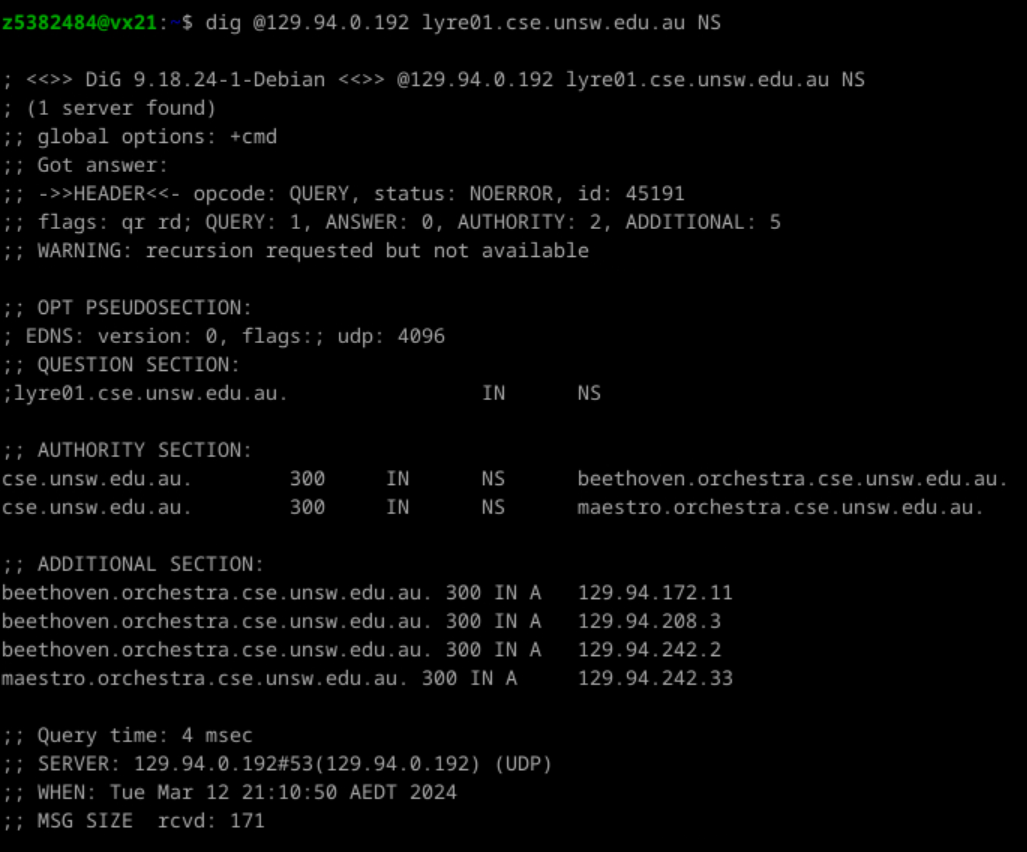
Next query one of the root nameservers as follows:



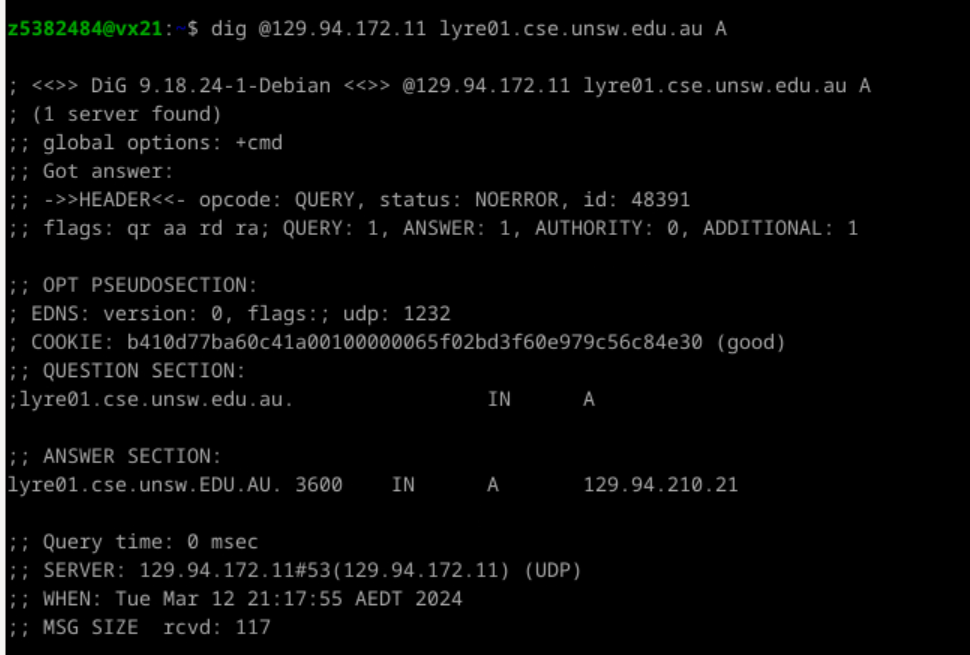
Use one of the IP addresses to query the name servers for the domain "edu.au.":



We can see that the domain name already contains the "unsw.edu.au." field. so query one of them as follows:



We are now referred to the CSE name servers, so we query one of them as follows. (dig A):



The IP address for lyre01.cse.unsw.edu.au is 129.94.210.21. Following the iterative query process starting from the root domain name server, we must query 5 DNS servers.

Q11:

Yes, a physical machine can have multiple names and/or IP addresses associated with it. If a physical machine is connected to multiple networks or subnets, it may be assigned multiple IP addresses, one for each network interface. In addition, a machine may have multiple aliases (also called hostnames) and CNAME records, and these records can be mapped to the same IP address. This allows different names to point to the same physical machine.

Exercise 5:

The running results are as follows:

