Exercise 3: Digging into DNS

3.1

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

The IP address is 150.203.161.98

The type of DNS query is a recursive query since there is a RD set in the dig query header



3.2

What is the canonical name for the CECS ANU web server? Suggest a reason for having an alias for this server.

The canonical name is rproxy.cecs.anu.edu.au.

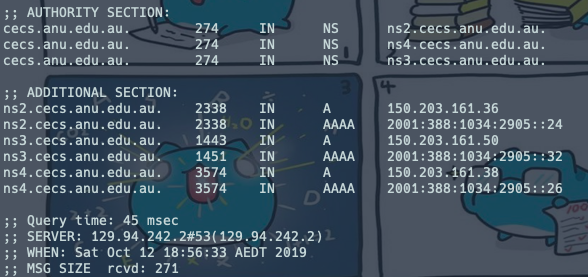
IP aliasing can be used to provide multiple network addresses on a single physical interface, it’s like having multiple front doors to a location, can have more than one domain names that takes you to a single site.

3.3

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

In the Authority section there are 3 DNS servers which are responsible for the domain.

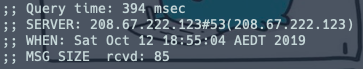
In the Additional section contains A and AAAA records, which are IPv4 and IPv6 address.



3.4

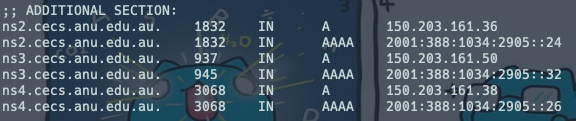
What is the IP address of the local nameserver for your machine?

\*did not ssh to cse machine but my machine



3.5

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.cecs.anu.edu.au))? Find out their IP addresses? What type of DNS query is sent to obtain this information?

The DNS query is > dig [www.cecs.anu.edu.au](http://www.cecs.anu.edu.au) (I ssh into cse machine)

3.6

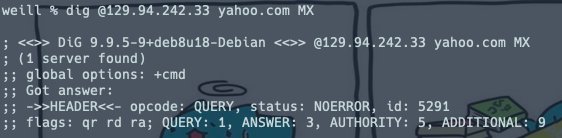
What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?



3.7

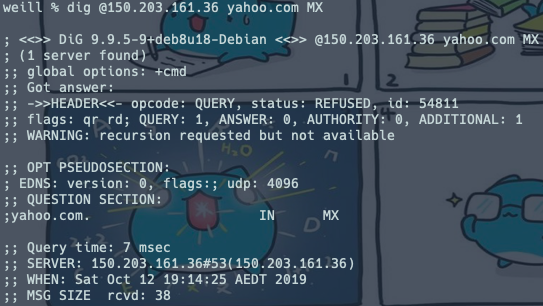
Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not [www.yahoo.com](http://www.yahoo.com)). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS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

Non authoritative because there is no aa(authoritative answer) flag, and CSE nameserver has no authority on yahoo.com



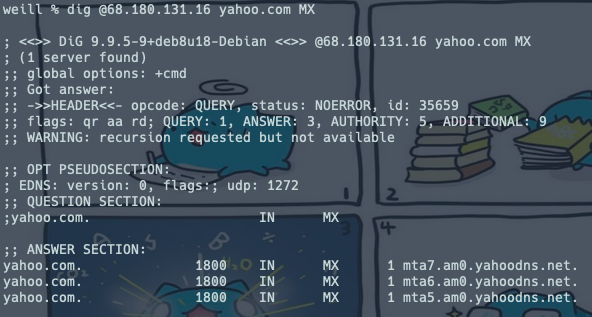
3.8

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



3.9

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

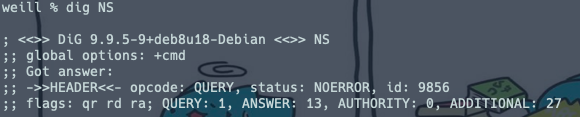


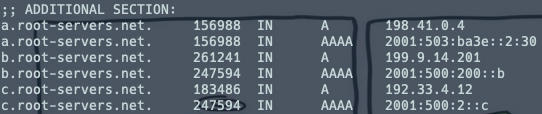
3.10

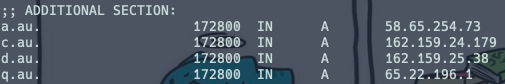
In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this 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?

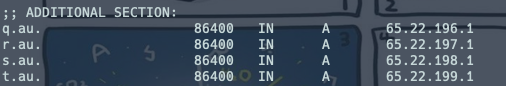
5 DNS servers to get an authoritative answer for lyre00.cse.unsw.edu.au

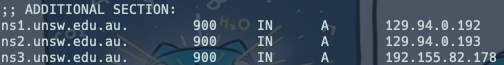
* a.root-servers.net.
* a.au.
* q.au.
* ns1.unsw.edu.au.
* beethoven.orchestra.cse.unsw.edu.au.

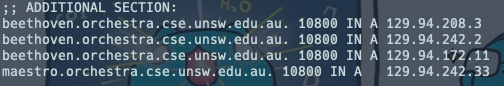














3.11

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

Yes, based on the evidences above an IP address can have multiple names(alias which refers to one canonical name) associated with it.