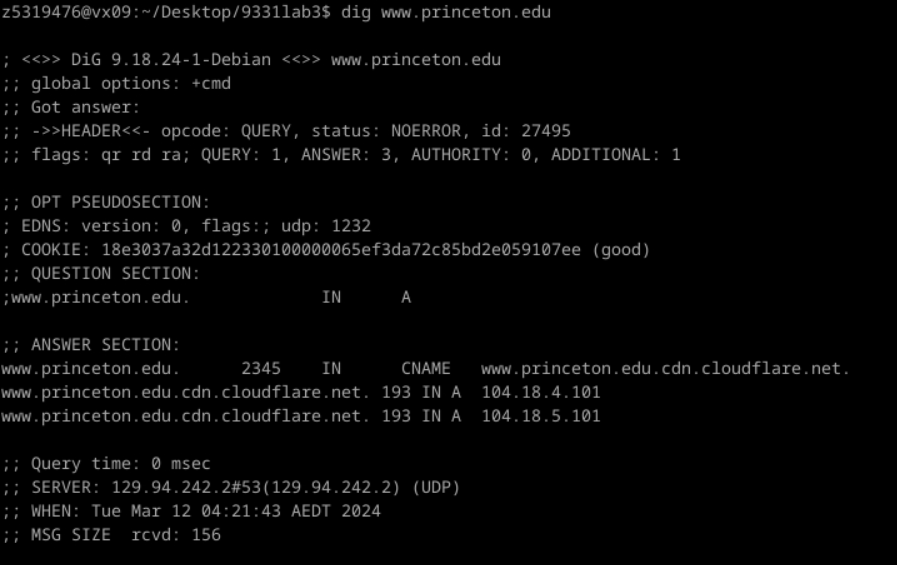
**Comp9331 lab3 answer**

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

**Question 1. What is the IP address of**[**www.princeton.edu**](http://www.princeton.edu/)**? What type of DNS query is sent to get this answer?**



According to the information, The IP addresses are **104.18.4.101** and **104.18.5.101**.

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

**Question 2. What is the canonical name for the Princeton webserver (i.e.,**[**www.princeton.edu**](http://www.oxford.ac.uk/)**)? Suggest a reason for having an alias for this server.**

the canonical name for the Princeton webserver is [www.princeton.edu.cdn.cloudflare.net](http://www.princeton.edu.cdn.cloudflare.net).

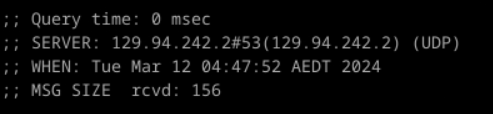
using an alias for a server provides flexibility, scalability, and make it easier to remember.

**Question 3. What can you make of the rest of the response/what is it used for (i.e., the details available in the DNS response (cookies and other fields))?**

Based on the other parts of the dig query results, we can obtain information about EDNS. This section contains information about DNS extensions, such as version number, flags, and UDP packet size. In the query results, version is 0, no special flags are set, and the size of the UDP packet is 1232 bytes.

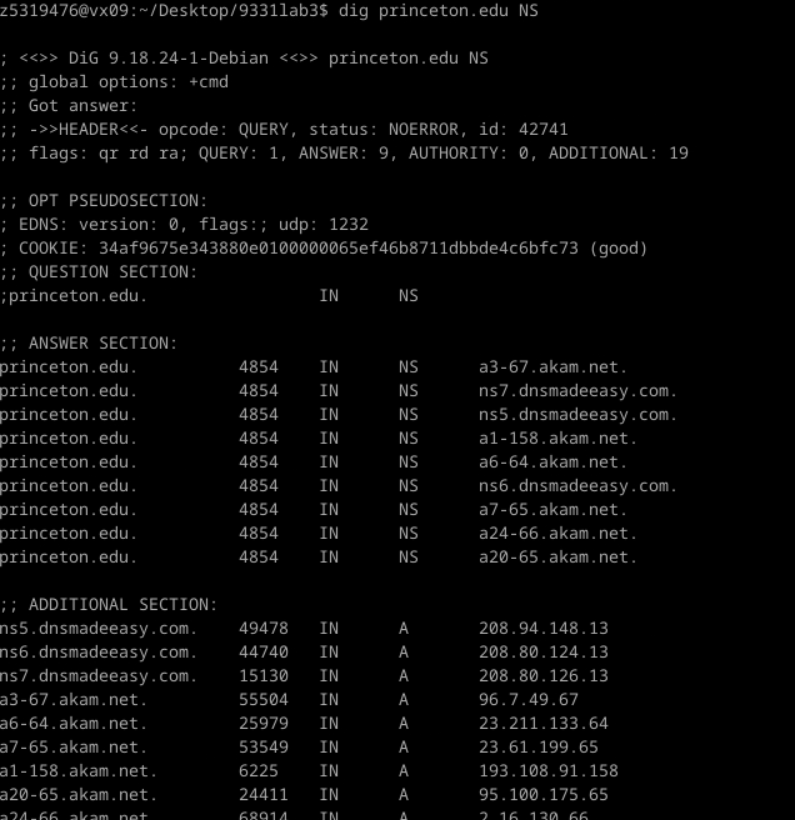
Moreover, COOKIE is typically used to maintain session state or for other purposes, so that the server can recognize and track a user's session. The query result shows that the value of COOKIE is "18e3037a32d122330100000065ef3da72c85bd2e059107ee" and is marked as "good", indicating that COOKIE is valid.

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



The IP address of local nameserver for CSE is 129.94.242.2.

**Question 5. What are the DNS nameservers for the " princeton.edu” domain (note: the domain name is princeton.edu and not**[**www.princeton.edu**](http://www.oxford.ac.uk/)**. This is an example of what is referred to as the apex/naked domain)? Find their IP addresses. Which DNS query type is used to obtain this information?**



the DNS nameservers (answer section):

a3-67.akam.net.

ns7.dnsmadeeasy.com.

ns5.dnsmadeeasy.com.

a1-158.akam.net.

a6-64.akam.net.

ns6.dnsmadeeasy.com.

a7-65.akam.net.

a24-66.akam.net.

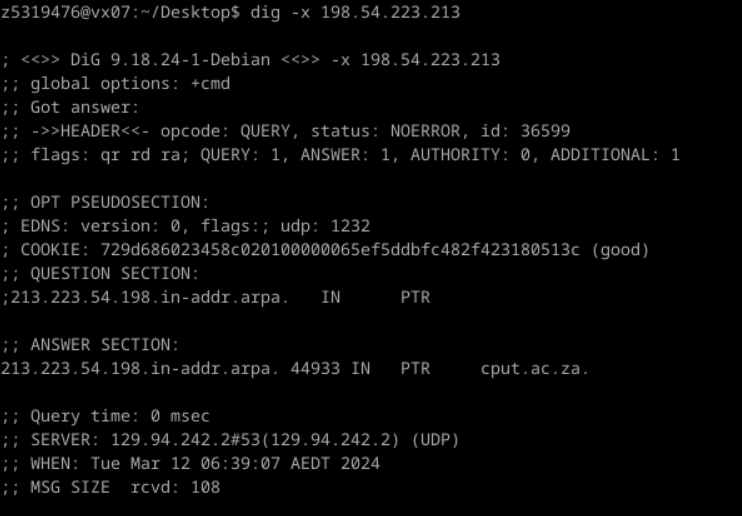
a20-65.akam.net.

IP addresses (additional section):



DNS query type is **NS.**

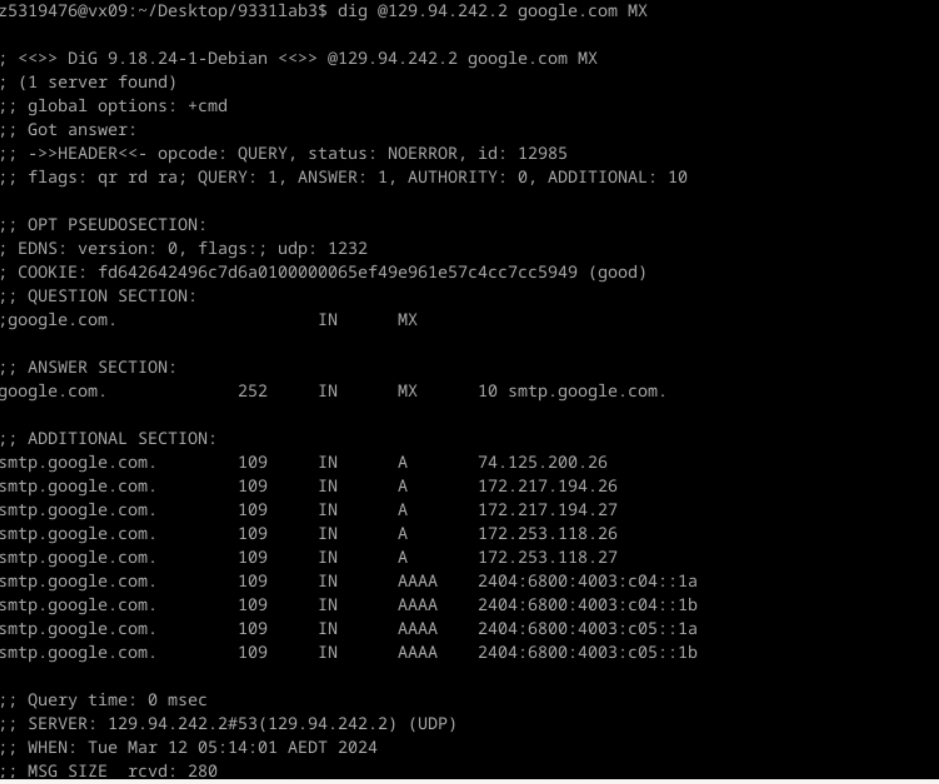
**Question 6. What is the DNS name associated with the IP address 198.54.223.213? Which DNS query type is used to obtain this information?**

****

the DNS name is **cput.ac.za.**

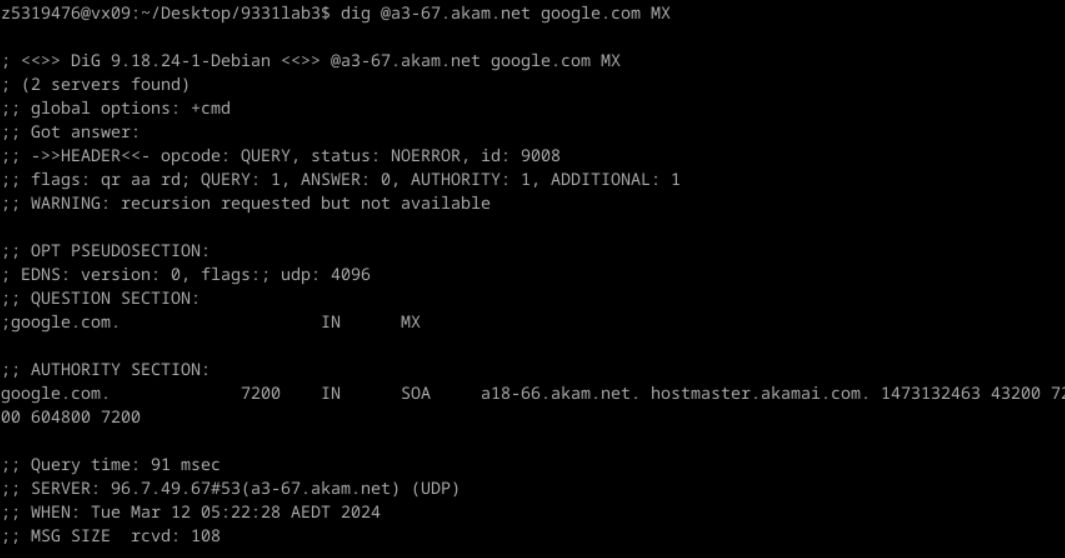
DNS query type is **PTR**.

**Question 7. Run, dig and query the CSE nameserver (129.94.242.2) for the mail servers for google.com (again, the domain name is google.com, not**[**www.google.com**](http://www.google.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 message to determine the answer)**



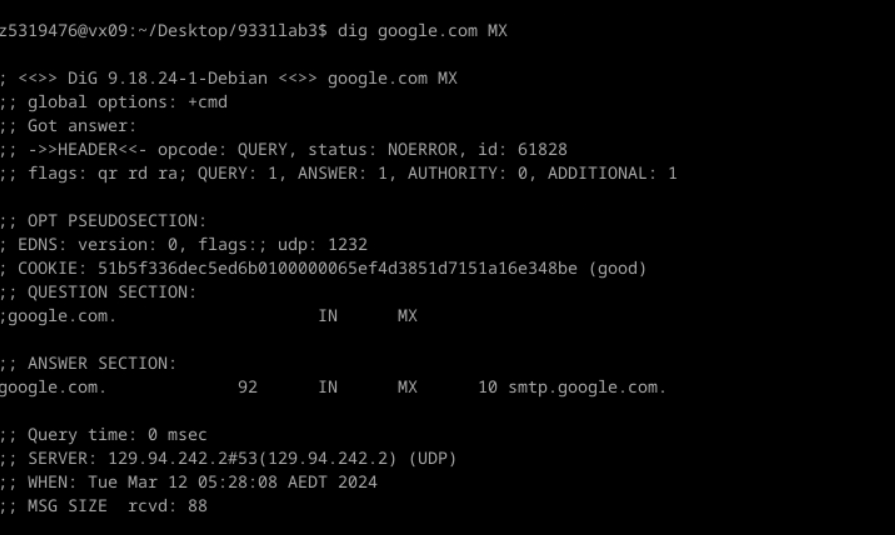
We did not get an authoritative answer. In the dig output, if the flags field in the response contains the AA (Authoritative Answer) flag, it indicates that the response is an authoritative answer from an authoritative domain name server. However, I did not see the AA flag in the output. Therefore, the answer is no.

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



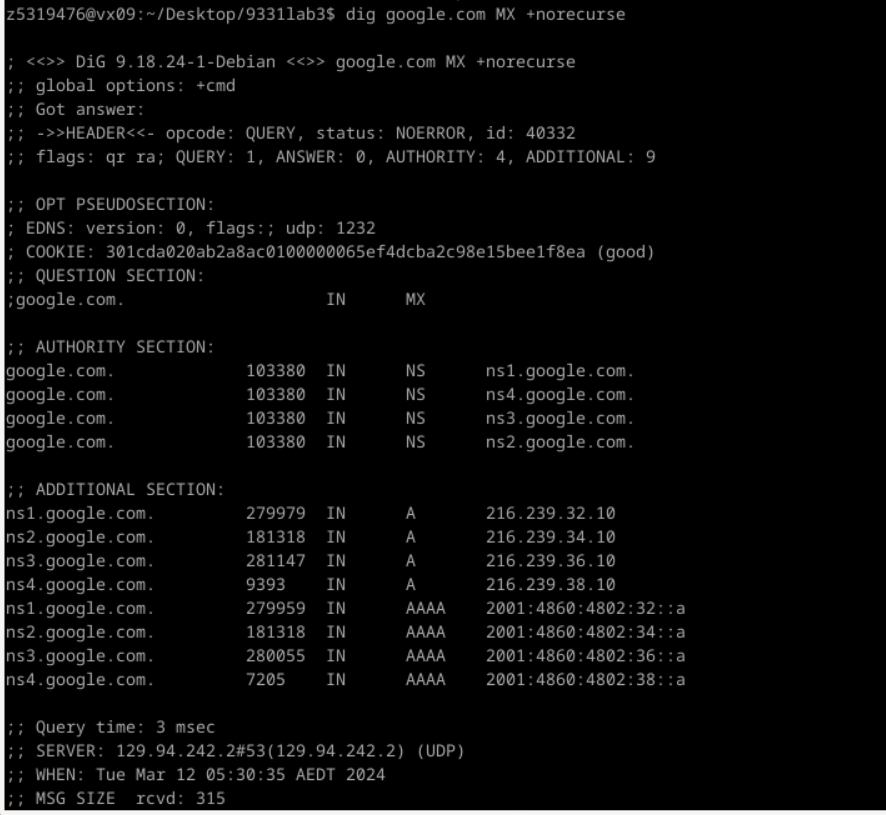
**I did not get a respond when I try the** nameserver **a3-67.akam.net** (no answer section).

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

****

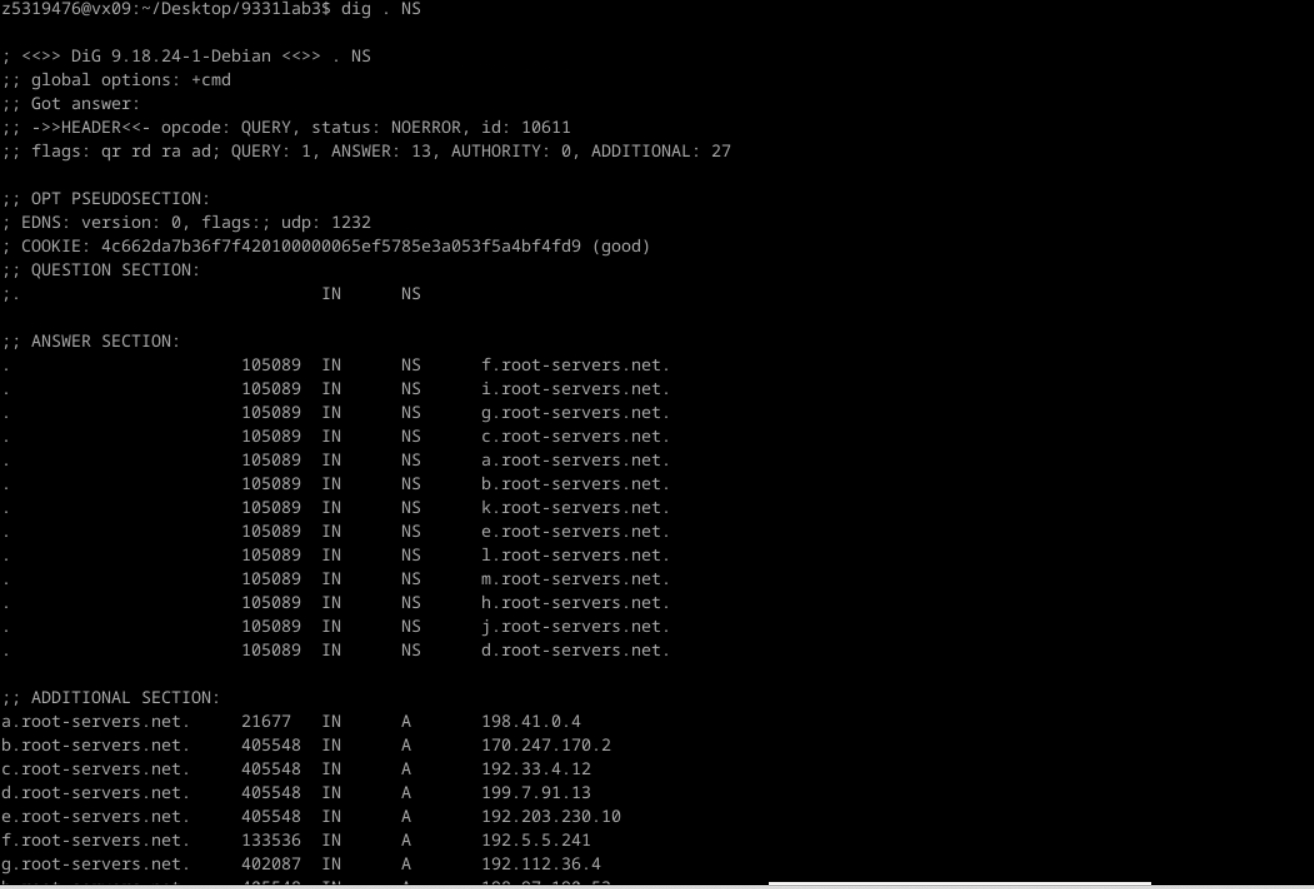
**We can use “dig google.com MX” to** obtain the authoritative answer for the mail servers for google.com.

We can also use “dig google.com MX +norecurse” to obtain more information, such as IP address.

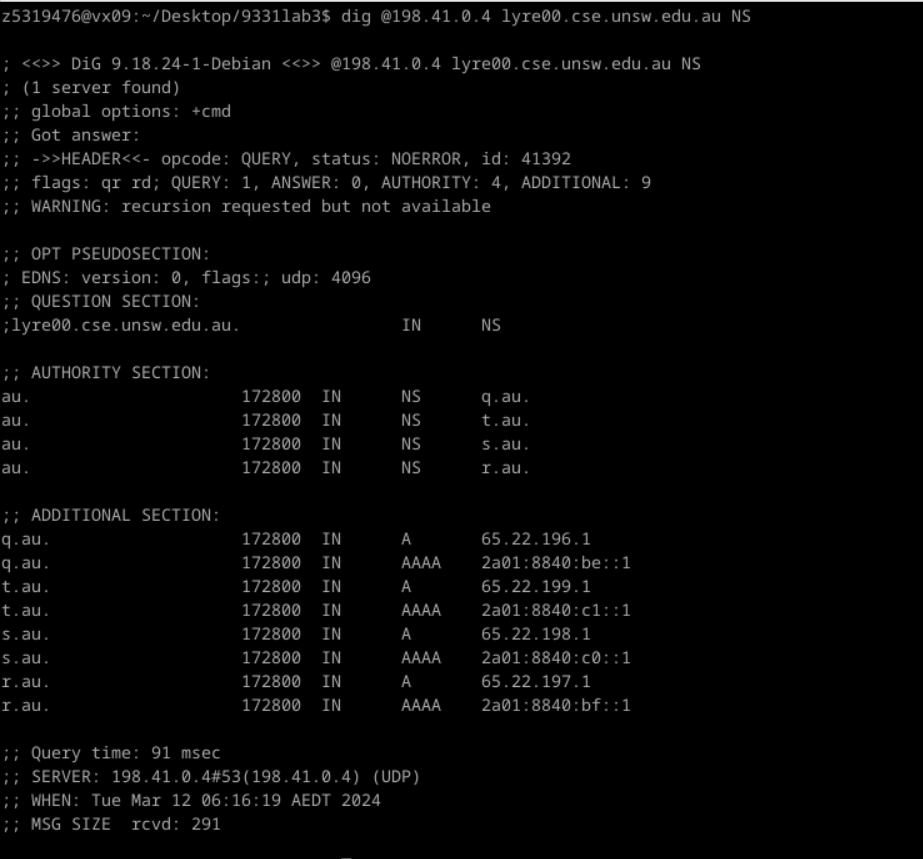
****

**Question 10. find the IP address** **lyre00.cse.unsw.edu.au**

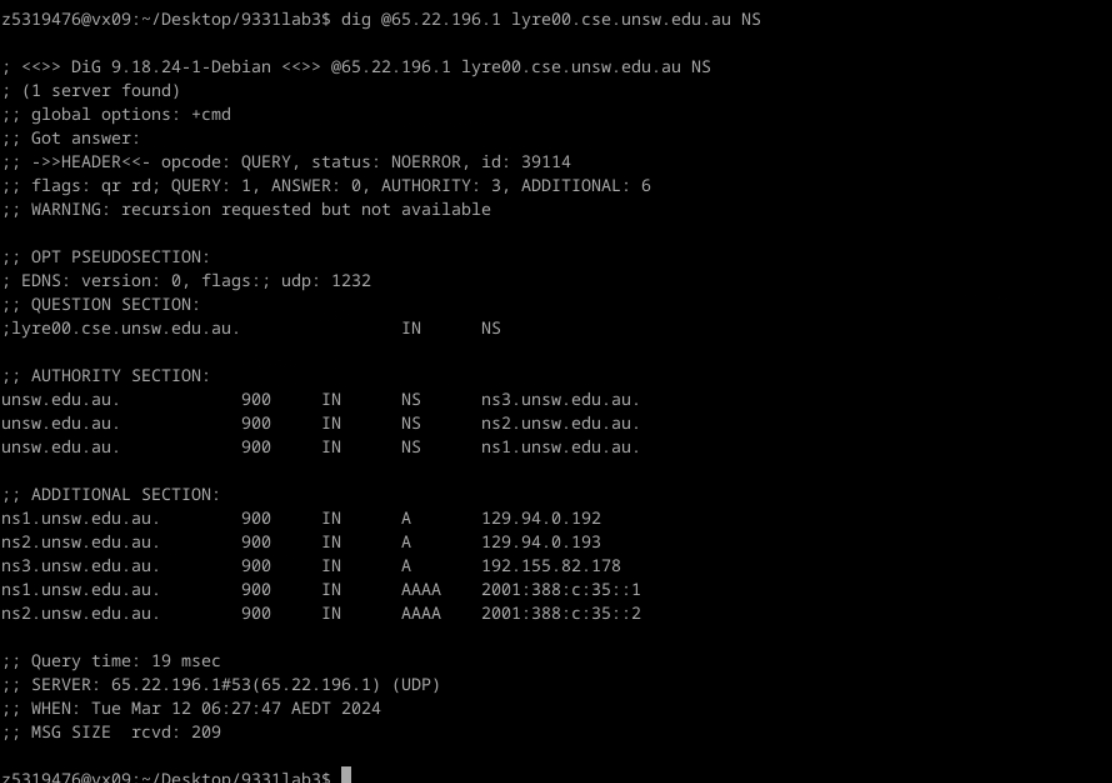
1. Firstly, type “dig . NS” query



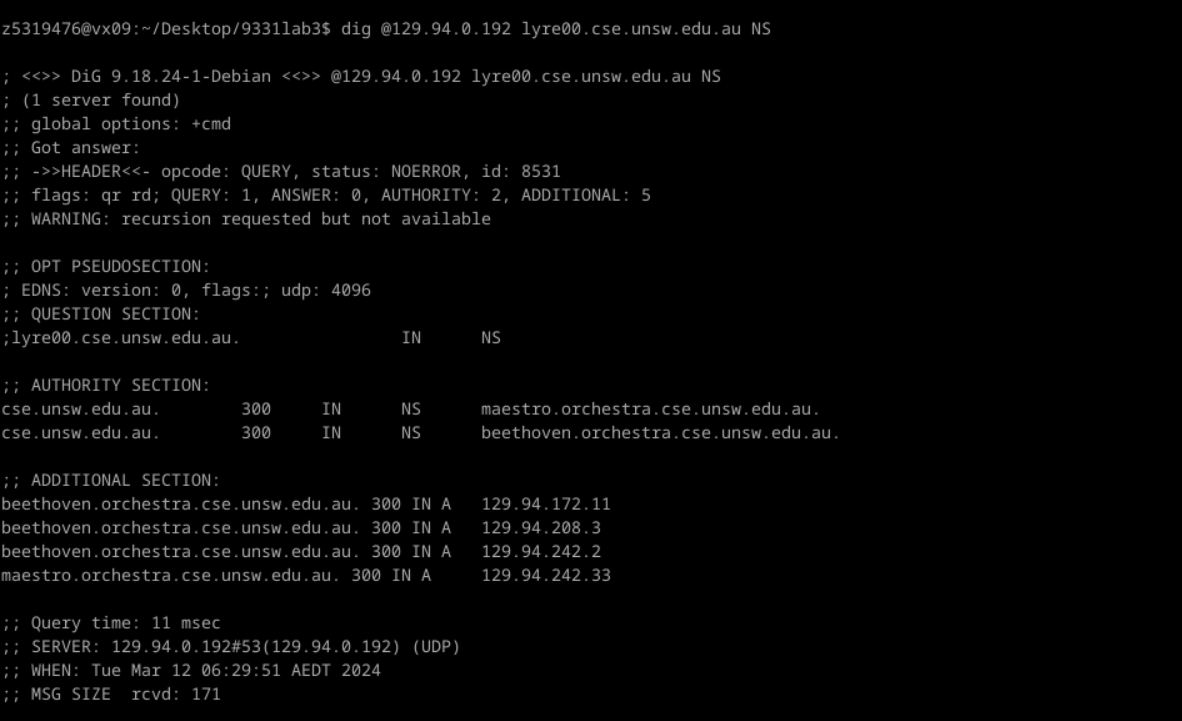
1. Then, use one of the nameservers to query,



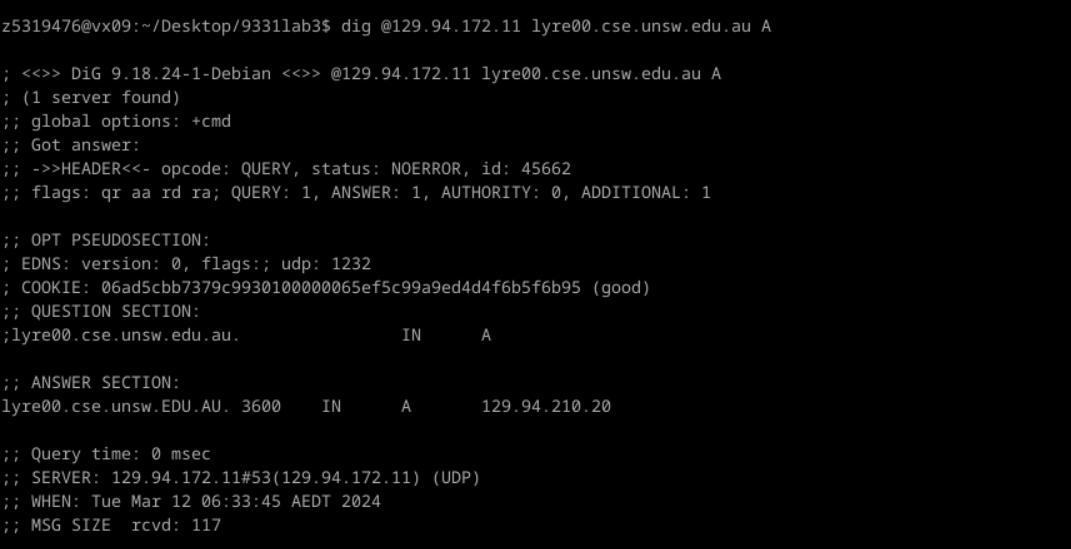
1. Use q.au nameserver to query,



1. Use 129.94.0.192 to query,



1. Use 129.94.172.11 to get the final answer,



the IP address for lyre00.cse.unsw.edu.au is **129.94.210.20**. I used 5 DNS servers to obtain an authoritative answer

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

Yes, a physical machine can have several names and/or IP addresses associated with it. This is often implemented through aliasing, each IP address can have multiple "aliases", which are host names. A single machine can have multiple network interfaces and IP addresses. This allows the machine to be accessed through multiple IP addresses, each of which may serve different purposes or network segments.

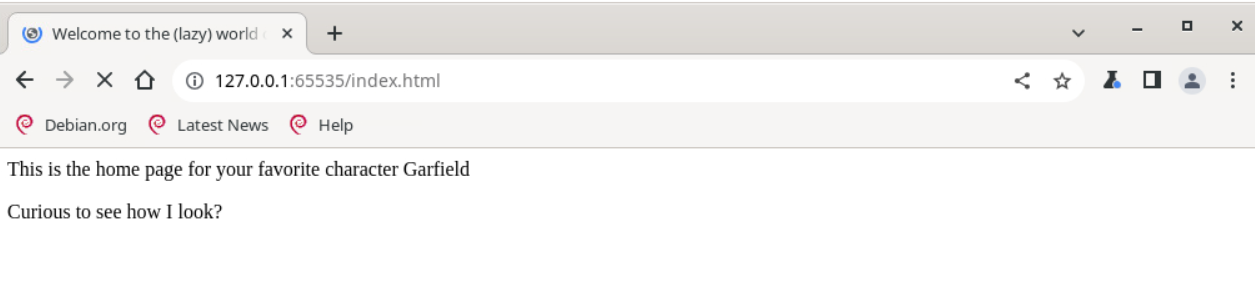
**Exercise 4: A Simple Web Server (Marked, submit your code, 5 Marks)**

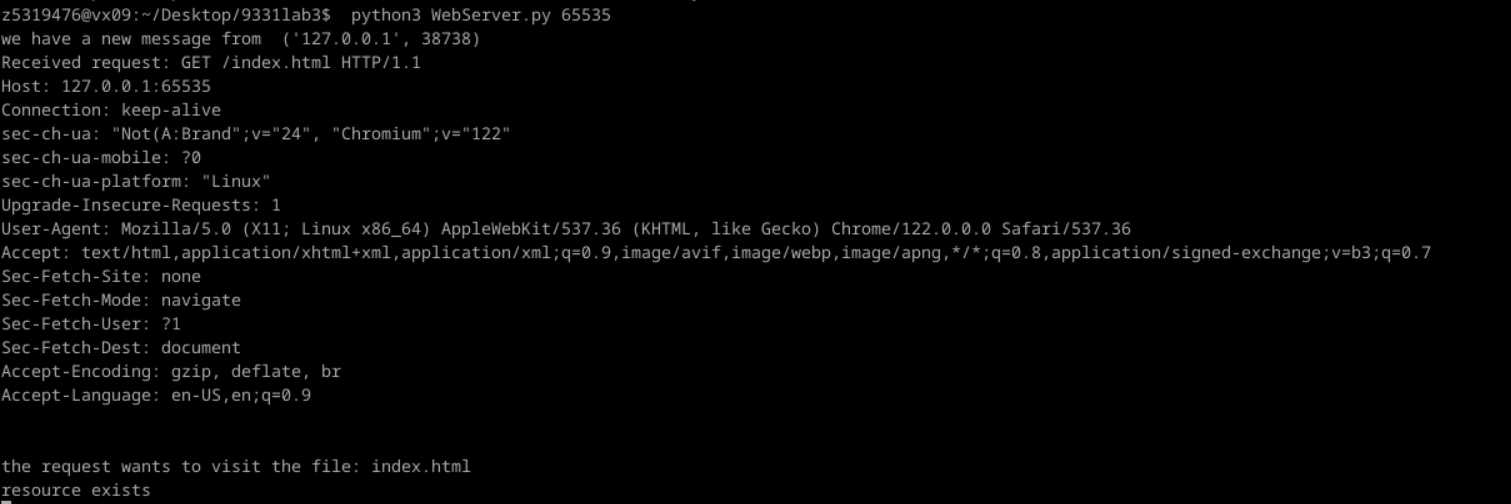
**Environment: python3.10**

**Browser: google**

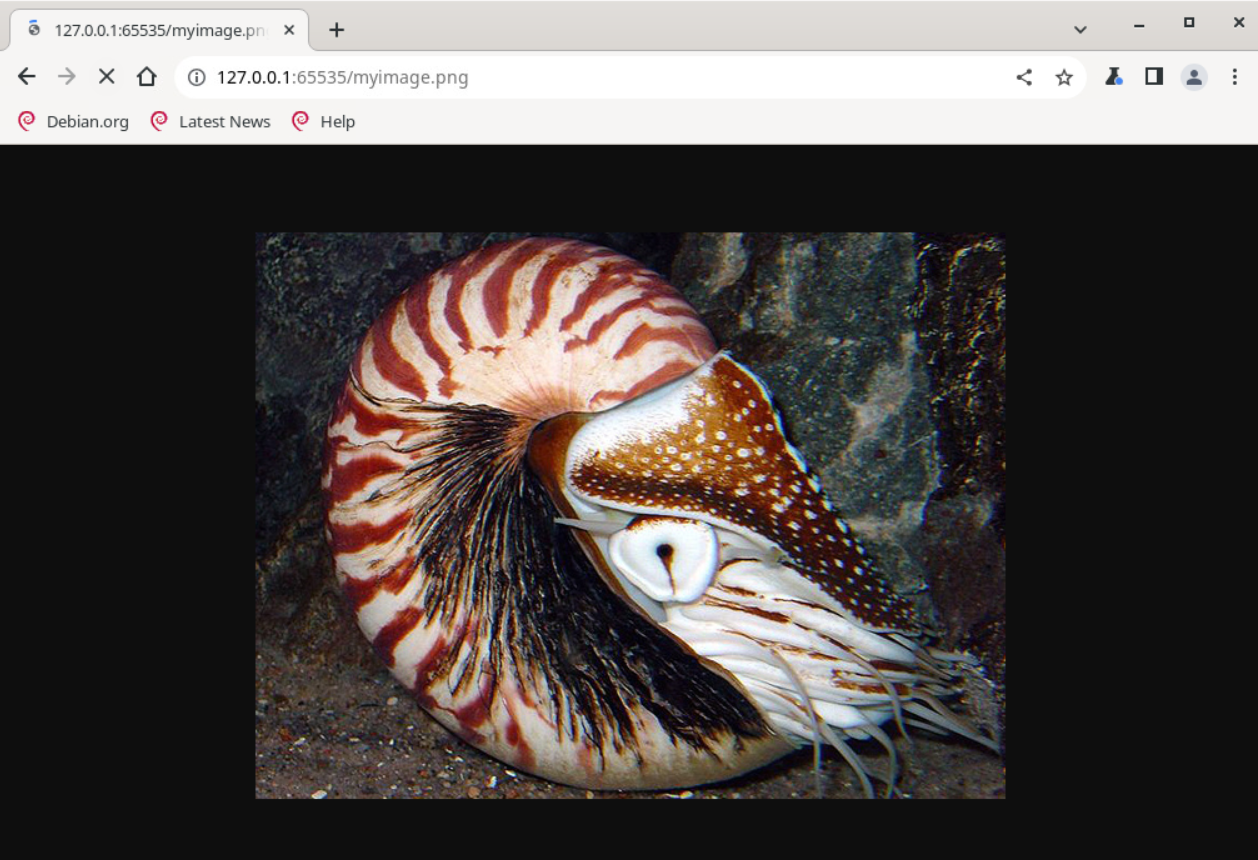
**Result:**

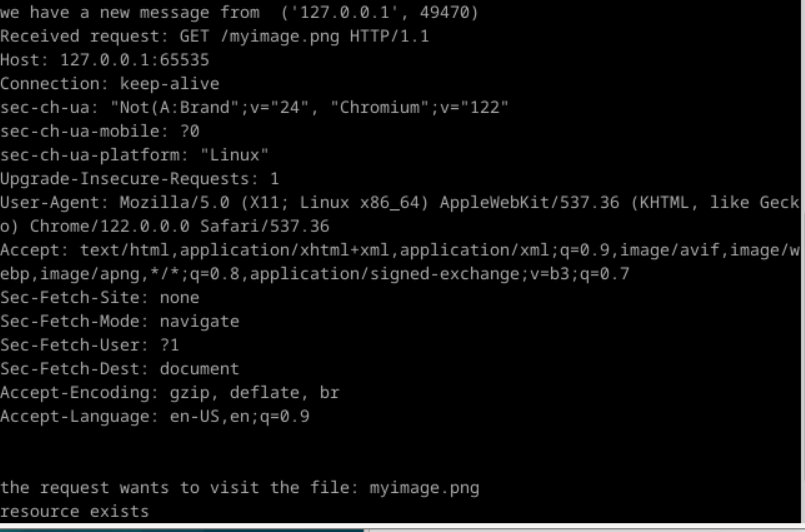
1. http://127.0.0.1:65535/index.html

****

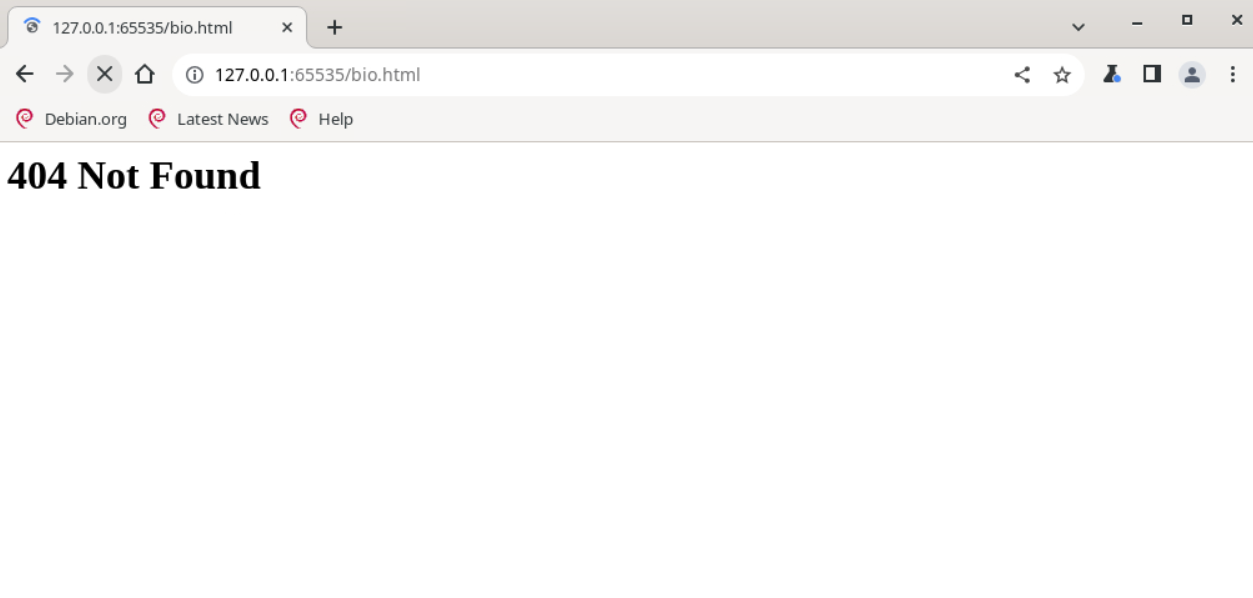
****

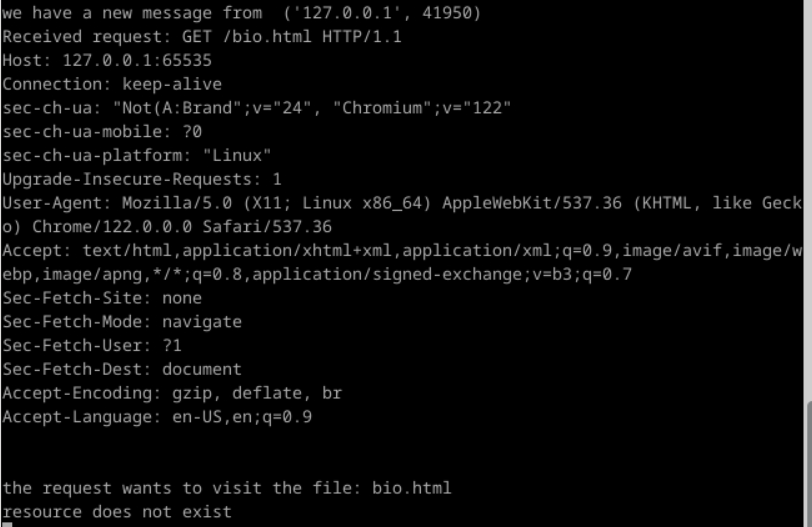
1. http://127.0.0.1:port/index.html

****

****

1. http://127.0.0.1:port/index.html

****

****