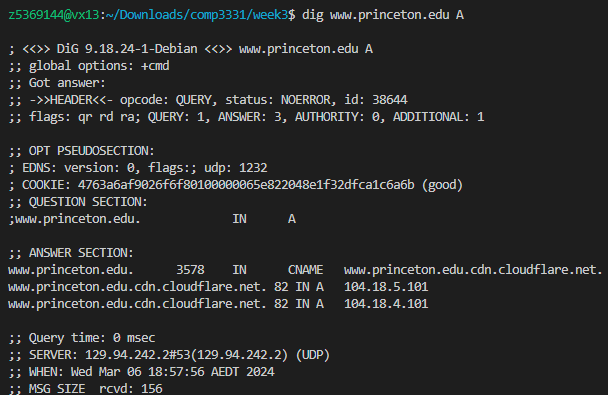
****Exercise 3: Digging into DNS (marked, include in the lab report, 5 Marks)****



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?

104.18.5.101 and 104.18.4.101

A type

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.

[www.princeton.edu.cdn.cloudflare.net](http://www.princeton.edu.cdn.cloudflare.net)

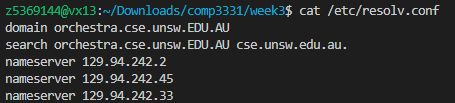
Distribute traffic to different servers to share load and improve performance

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))?

1.Authority Section: If you need to know the authoritative server information about the query domain name, you can check the authoritative section

2.Cookies: Used for authentication and verifying data integrity between DNS queries and responses.

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

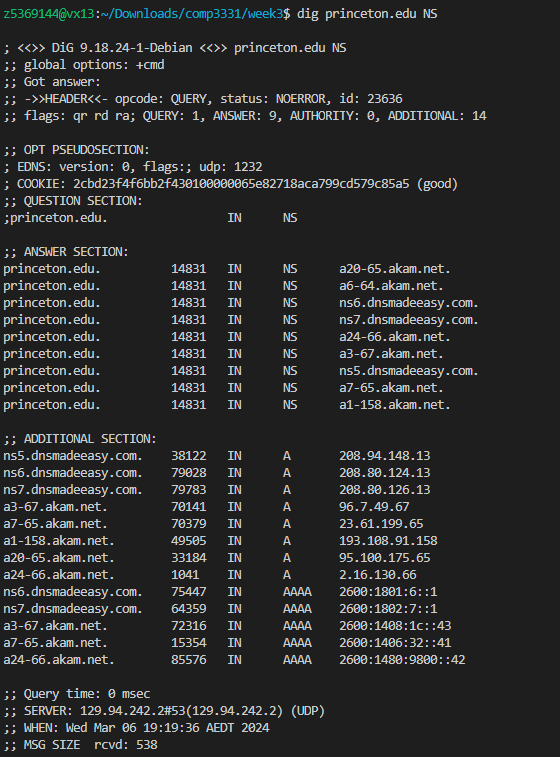


nameserver 129.94.242.2

nameserver 129.94.242.45

nameserver 129.94.242.33

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?



DNS type : NS

a20-65.akam.net. : 95.100.175.65

a6-64.akam.net. : didnt provide

ns6.dnsmadeeasy.com. : 208.80.124.13

ns7.dnsmadeeasy.com. : 208.80.126.13

a24-66.akam.net. : 2.16.130.66

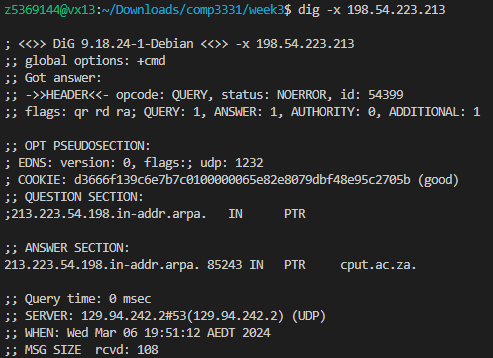
a3-67.akam.net. : 96.7.49.67

ns5.dnsmadeeasy.com. : 208.94.148.13

a7-65.akam.net. : 23.61.199.65

a1-158.akam.net. : 193.108.91.158

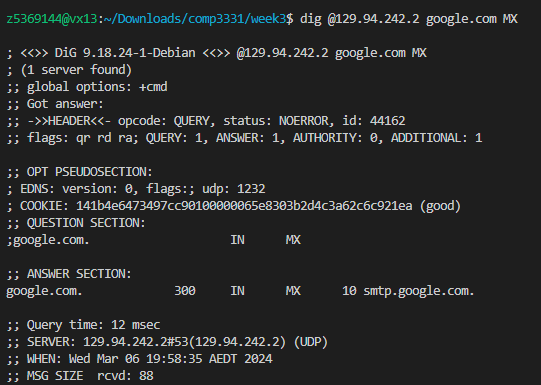
Question 6. What is the DNS name associated with the IP address 198.54.223.213 ? Which DNS query type is used to obtain this information?



cput.ac.za.

DNS query type : 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)



I didnt get authoritative answer because AUTHORITY: 0 is 0

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



I get the Authority answer because AUTHORITY:1

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

SOA(Start of Authority)

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). If you are using VLAB then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, flute00.cse.unsw.edu.au or flute01.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 your host's IP address. How many DNS servers do you have to query for an authoritative answer?

5

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

Yes

Exercise 4

Run python3 WebServer.py 8080

Input 127.0.0.1:8080/(resource\_name) in website.

