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

```
z5369144@vx13:~/Downloads/comp3331/week3$ dig www.princeton.edu A

; <<>> DiG 9.18.24-1-Debian <<>> www.princeton.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38644
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4763a6af9026f6f80100000065e822048e1f32dfca1c6a6b (good)
;; QUESTION SECTION:
;www.princeton.edu.             IN      A

;; ANSWER SECTION:
www.princeton.edu.      3578    IN      CNAME   www.princeton.edu.cdn.cloudflare.net.
www.princeton.edu.cdn.cloudflare.net. 82 IN A   104.18.5.101
www.princeton.edu.cdn.cloudflare.net. 82 IN A   104.18.4.101

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Wed Mar 06 18:57:56 AEDT 2024
;; MSG SIZE  rcvd: 156
```

Question 1. What is the IP address of **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**)? Suggest a reason for having an alias for this server.

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?

```
z5369144@vx13:~/Downloads/comp3331/week3$ cat /etc/resolv.conf
domain orchestra.cse.unsw.EDU.AU
search orchestra.cse.unsw.EDU.AU cse.unsw.edu.au.
nameserver 129.94.242.2
nameserver 129.94.242.45
nameserver 129.94.242.33
```

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 . 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?

```
z5369144@vx13:~/Downloads/comp3331/week3$ dig princeton.edu NS

; <<>> DiG 9.18.24-1-Debian <<>> princeton.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23636
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 14

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2cbd23f4f6bb2f430100000065e82718aca799cd579c85a5 (good)
;; QUESTION SECTION:
;princeton.edu.                 IN      NS

;; ANSWER SECTION:
princeton.edu.          14831   IN      NS      a20-65.akam.net.
princeton.edu.          14831   IN      NS      a6-64.akam.net.
princeton.edu.          14831   IN      NS      ns6.dnsmadeeasy.com.
princeton.edu.          14831   IN      NS      ns7.dnsmadeeasy.com.
princeton.edu.          14831   IN      NS      a24-66.akam.net.
princeton.edu.          14831   IN      NS      a3-67.akam.net.
princeton.edu.          14831   IN      NS      ns5.dnsmadeeasy.com.
princeton.edu.          14831   IN      NS      a7-65.akam.net.
princeton.edu.          14831   IN      NS      a1-158.akam.net.

;; ADDITIONAL SECTION:
ns5.dnsmadeeasy.com.    38122   IN      A       208.94.148.13
ns6.dnsmadeeasy.com.    79028   IN      A       208.80.124.13
ns7.dnsmadeeasy.com.    79783   IN      A       208.80.126.13
a3-67.akam.net.         70141   IN      A       96.7.49.67
a7-65.akam.net.         70379   IN      A       23.61.199.65
a1-158.akam.net.        49505   IN      A       193.108.91.158
a20-65.akam.net.        33184   IN      A       95.100.175.65
a24-66.akam.net.        1041    IN      A       2.16.130.66
ns6.dnsmadeeasy.com.    75447   IN      AAAA    2600:1801:6::1
ns7.dnsmadeeasy.com.    64359   IN      AAAA    2600:1802:7::1
a3-67.akam.net.         72316   IN      AAAA    2600:1408:1c::43
a7-65.akam.net.         15354   IN      AAAA    2600:1406:32::41
a24-66.akam.net.        85576   IN      AAAA    2600:1480:9800::42

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Wed Mar 06 19:19:36 AEDT 2024
;; MSG SIZE  rcvd: 538
```

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?

```
z5369144@vx13:~/Downloads/comp3331/week3$ dig -x 198.54.223.213

; <<>> DiG 9.18.24-1-Debian <<>> -x 198.54.223.213
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54399
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d3666f139c6e7b7c0100000065e82e8079dbf48e95c2705b (good)
;; QUESTION SECTION:
;213.223.54.198.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
213.223.54.198.in-addr.arpa. 85243 IN   PTR     cput.ac.za.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Wed Mar 06 19:51:12 AEDT 2024
;; MSG SIZE  rcvd: 108
```

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). 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)

```
z5369144@vx13:~/Downloads/comp3331/week3$ dig @129.94.242.2 google.com MX

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.242.2 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44162
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 141b4e6473497cc90100000065e8303b2d4c3a62c6c921ea (good)
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; Query time: 12 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Wed Mar 06 19:58:35 AEDT 2024
;; MSG SIZE  rcvd: 88
```

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?

```
z5369144@vx13:~/Downloads/comp3331/week3$ dig @2.16.130.66 google.com MX

; <<>> DiG 9.18.24-1-Debian <<>> @2.16.130.66 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47443
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      MX

;; AUTHORITY SECTION:
google.com.             7200    IN      SOA     a18-66.akam.net. hostmaster.akamai.com. 1473132463

;; Query time: 16 msec
;; SERVER: 2.16.130.66#53(2.16.130.66) (UDP)
;; WHEN: Wed Mar 06 20:06:44 AEDT 2024
;; MSG SIZE  rcvd: 108
```

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)

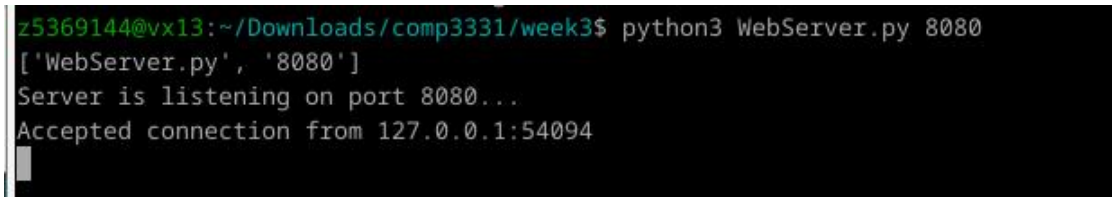
Question 10. In this exercise, you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). If you are using VLAB then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, flute00.cse.unsw.edu.au or flute01.cse.unsw.edu.au. 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?

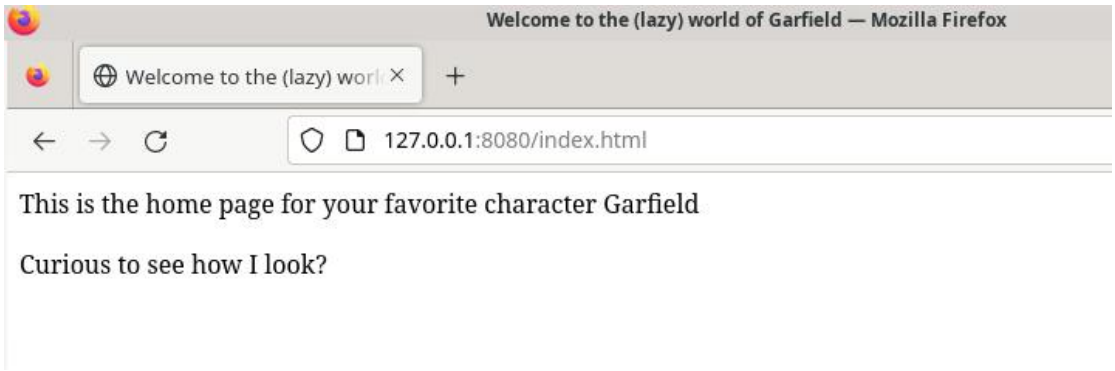
5

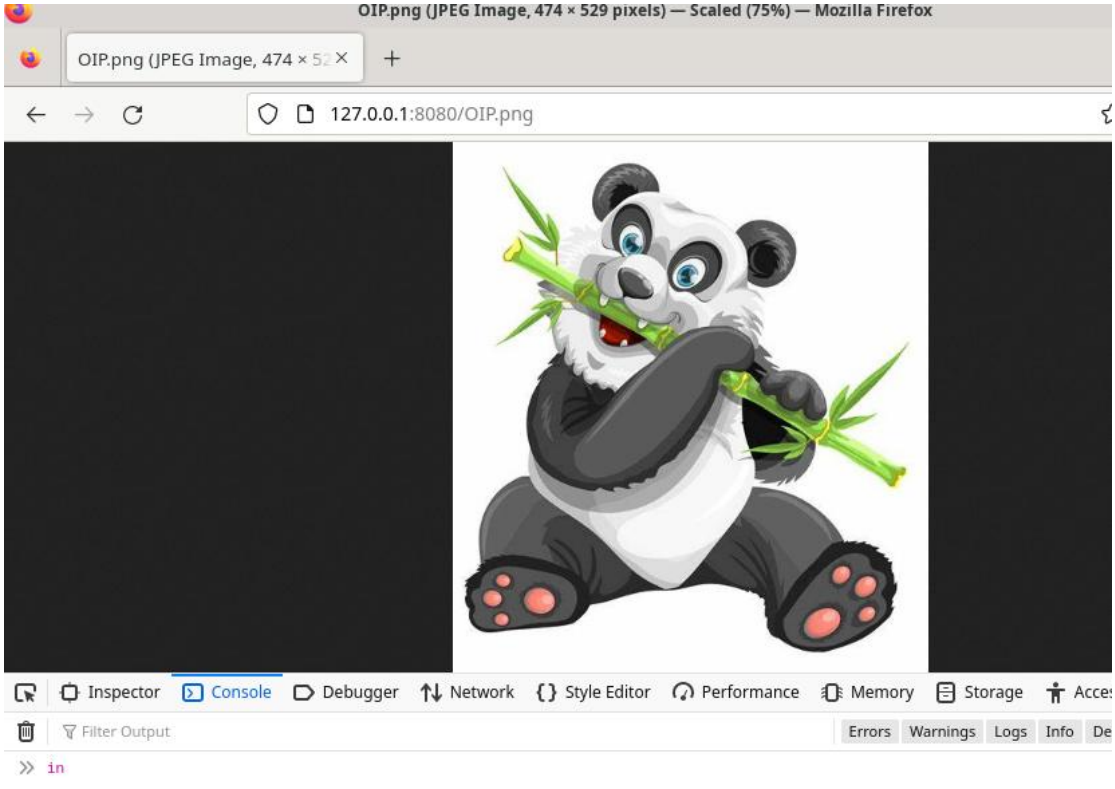
Question 11. Can one physical machine have several names and/or IP addresses associated with it?

Yes

Exercise 4
Run python3 WebServer.py 8080
Input 127.0.0.1:8080/(resource_name) in website.






OIP.png (JPEG Image, 474 × 529 pixels) — Scaled (75%) — Mozilla Firefox
OIP.png (JPEG Image, 474 ×
127.0.0.1:8080/OIP.png
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Filter Output
Errors
Warnings
Logs
Info
in