COMP9331 – Lab3

Exercise 3: Digging into DNS (5 Marks)

Question 1. What is the IP address of www.amazon.com.au? What type of DNS query is sent to get this answer?

```
z5484442@vx22:~/9331/lab03$ dig www.amazon.com.au

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.amazon.com.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58300
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3644013e5aed1adf0100000067d69ef402439a4b8a109a46 (good)
;; QUESTION SECTION:
;www.amazon.com.au.             IN      A

;; ANSWER SECTION:
www.amazon.com.au.      979     IN      CNAME   tp.04f01a85e-frontier.amazon.com.au.
tp.04f01a85e-frontier.amazon.com.au. 20 IN CNAME cf.04f01a85e-frontier.amazon.com.au.
cf.04f01a85e-frontier.amazon.com.au. 7 IN A     18.67.104.12

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Sun Mar 16 20:50:44 AEDT 2025
;; MSG SIZE  rcvd: 156
```

Answer: The IP address is *18.67.104.12*. The DNS query sent was an A record query.

Question 2. What is the canonical name for the webserver (i.e., www.amazon.com.au)? Suggest a reason for having an alias for this server.

Answer: The canonical name for www.amazon.com.au are *tp.04f01a85e-frontier.amazon.com.au*, *cf.04f01a85e-frontier.amazon.com.au*. IP aliases can be used to provide multiple network addresses on a single physical interface, which can take you to a single site using multiple domain names.

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)?

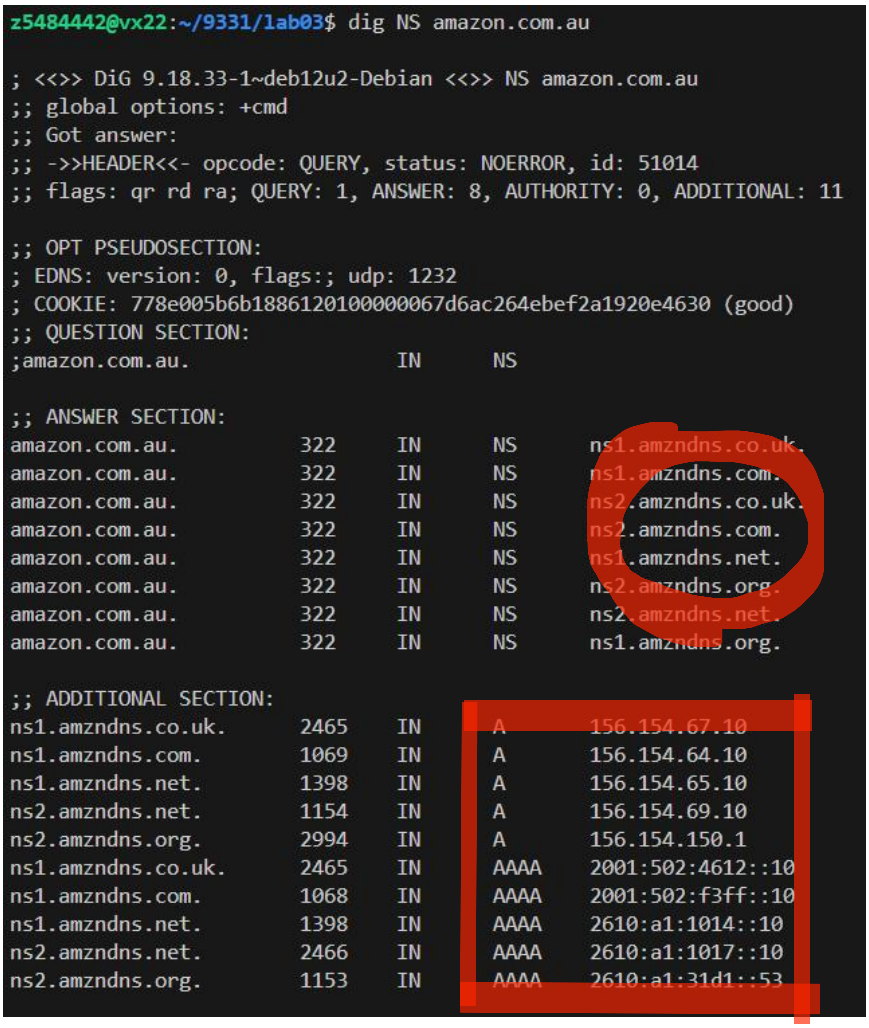
Answer: The EDNS cookie is a security mechanism to prevent DNS attacks. Client Cookie: *3644013e5aed1adf*. Server Cookie: *0100000067d69ef402439a4b8a109a46*. "good" indicates the client validated the server's cookie. Query Time: *0 msec* shows the query was resolved very quickly. Server Information: *129.94.242.2 #53* shows the DNS server responded. The timestamp records the date and time when the query was processed. Message Size shows that the entire DNS response was *156 bytes*.

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

```
PS C:\Users\13512> nslookup example.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  240c::6666
```

Answer: IPv6 DNS Servers: *240c::6666*

Question 5. What are the DNS nameservers for the "amazon.com.au" domain. 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?



```
z5484442@vx22:~/9331/lab03$ dig NS amazon.com.au

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> NS amazon.com.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51014
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 778e005b6b1886120100000067d6ac264ebef2a1920e4630 (good)
;; QUESTION SECTION:
;amazon.com.au.                 IN      NS

;; ANSWER SECTION:
amazon.com.au.          322     IN      NS      ns1.amzndns.co.uk.
amazon.com.au.          322     IN      NS      ns1.amzndns.com.
amazon.com.au.          322     IN      NS      ns2.amzndns.co.uk.
amazon.com.au.          322     IN      NS      ns2.amzndns.com.
amazon.com.au.          322     IN      NS      ns1.amzndns.net.
amazon.com.au.          322     IN      NS      ns2.amzndns.org.
amazon.com.au.          322     IN      NS      ns2.amzndns.net.
amazon.com.au.          322     IN      NS      ns1.amzndns.org.

;; ADDITIONAL SECTION:
ns1.amzndns.co.uk.      2465    IN      A       156.154.67.10
ns1.amzndns.com.        1069    IN      A       156.154.64.10
ns1.amzndns.net.        1398    IN      A       156.154.65.10
ns2.amzndns.net.        1154    IN      A       156.154.69.10
ns2.amzndns.org.        2994    IN      A       156.154.150.1
ns1.amzndns.co.uk.      2465    IN      AAAA    2001:502:4612::10
ns1.amzndns.com.        1068    IN      AAAA    2001:502:f3ff::10
ns1.amzndns.net.        1398    IN      AAAA    2610:a1:1014::10
ns2.amzndns.net.        2466    IN      AAAA    2610:a1:1017::10
ns2.amzndns.org.        1153    IN      AAAA    2610:a1:31d1::53
```

Answer: The query type is NS shows the apex domain amazon.com.au is served by eight nameservers: *ns1.amzndns.co.uk; ns1.amzndns.com; ns2.amzndns.co.uk; ns2.amzndns.com; ns1.amzndns.net; ns2.amzndns.org; ns2.amzndns.net; ns1.amzndns.org.*

IP addresses:

- **ns1.amzndns.co.uk:** IPv4: 156.154.67.10; IPv6: 2001:502:4612::10
- **ns1.amzndns.com:** IPv4: 156.154.64.10; IPv6: 2001:502:f3ff::10

- **ns1.amzndns.net:** IPv4: 156.154.65.10; IPv6: 2610:a1:1014::10
- **ns2.amzndns.net:** IPv4: 156.154.69.10; IPv6: 2610:a1:1017::10
- **ns2.amzndns.org:** IPv4: 156.154.150.1; IPv6: 2610:a1:31d1::53
- **ns2.amzndns.co.uk:** Not provided
- **ns2.amzndns.co.uk:** Not provided

Question 6. What is the DNS name associated with the IP address 9.9.9.9? Which DNS query type is used to obtain this information?

```
z5484442@vx22:~/9331/lab03$ dig -x 9.9.9.9

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> -x 9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50521
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b109034c280b841e0100000067d6b07ba44d2beb4693e2f8 (good)
;; QUESTION SECTION:
;9.9.9.9.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
9.9.9.9.in-addr.arpa.   138441  IN      PTR     dns9.quad9.net.
```

Answer: The DNS name associated with 9.9.9.9 is *dns9.quad9.net*. The type of DNS query is a *PTR* record query.

Question 7. Run, dig and query the CSE nameserver (129.94.242.2) for the mail servers for yahoo.com. Did you get an authoritative answer? Why?

```
z5484442@vx22:~/9331/lab03$ dig @129.94.242.2 yahoo.com MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @129.94.242.2 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12335
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f4ab27703ba9e4630100000067d6b27993e91b9f56a2d61e (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
```

Answer: The response did not come from an authoritative nameserver for yahoo.com. The header flags include *qr, rd, ra* but not *aa*, *AUTHORITY: 0* shows authoritative nameservers are listed. 129.94.242.2 is a recursive resolver rather than an authoritative server for yahoo.com.

Question 8. Repeat the above Q7, use one of the nameservers obtained in Q5 What is the result?

```
z5484442@vx22:~/9331/lab03$ dig 156.154.67.10 yahoo.com MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> 156.154.67.10 yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31801
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d2482179dd1939110100000067d6b5b64a3b39275fead80a (good)
;; QUESTION SECTION:
;156.154.67.10.                 IN      A

;; AUTHORITY SECTION:
.                       9972    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2025031600 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Sun Mar 16 22:27:50 AEDT 2025
;; MSG SIZE  rcvd: 145

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50302
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d2482179dd1939110100000067d6b5b64a3b39275fead80a (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              971     IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              971     IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              971     IN      MX      1 mta7.am0.yahoodns.net.
```

Answer: No *aa* in header flag shows the response is not from an authoritative nameserver for yahoo.com.

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

```
z5484442@vx22:~/9331/lab03$ dig @ns1.yahoo.com yahoo.com MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @ns1.yahoo.com yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27377
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
; COOKIE: aa4f5a636e45b9e772d32e8867d6b810829e71e21b59a81a (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
```

Answer: The query sent is an MX record query. It is directing the query to ns1.yahoo.com, which is an authoritative nameserver for yahoo.com, as shown by *aa* in flag.

Question 10. In this exercise, you simulate the iterative DNS query process to find the IP address of your machine. 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?

```
z5484442@vx22:~/9331/lab03$ dig NS

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30433
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
```

```
;; ADDITIONAL SECTION:
a.root-servers.net.     94519   IN      A       198.41.0.4
b.root-servers.net.     143695  IN      A       170.247.170.2
c.root-servers.net.     143696  IN      A       192.33.4.12
d.root-servers.net.     143696  IN      A       199.7.91.13
e.root-servers.net.     307296  IN      A       192.203.230.10
f.root-servers.net.     126990  IN      A       192.5.5.241
g.root-servers.net.     123208  IN      A       192.112.36.4
h.root-servers.net.     143696  IN      A       198.97.190.53
i.root-servers.net.     143696  IN      A       192.36.148.17
j.root-servers.net.     143696  IN      A       192.58.128.30
k.root-servers.net.     143696  IN      A       193.0.14.129
l.root-servers.net.     143697  IN      A       199.7.83.42
m.root-servers.net.     143695  IN      A       202.12.27.33
a.root-servers.net.     100080  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     143695  IN      AAAA    2801:1b8:10::b
c.root-servers.net.     143696  IN      AAAA    2001:500:2::c
d.root-servers.net.     143696  IN      AAAA    2001:500:2d::d
e.root-servers.net.     124048  IN      AAAA    2001:500:a8::e
f.root-servers.net.     143697  IN      AAAA    2001:500:2f::f
g.root-servers.net.     123208  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     143696  IN      AAAA    2001:500:1::53
i.root-servers.net.     143696  IN      AAAA    2001:7fe::53
j.root-servers.net.     143696  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     143696  IN      AAAA    2001:7fd::1
l.root-servers.net.     143697  IN      AAAA    2001:500:9f::42
m.root-servers.net.     143695  IN      AAAA    2001:dc3::35
```

```
;; ADDITIONAL SECTION:
t.au.                   172800  IN      A       65.22.199.1
t.au.                   172800  IN      AAAA    2a01:8840:c1::1
r.au.                   172800  IN      A       65.22.197.1
r.au.                   172800  IN      AAAA    2a01:8840:bf::1
a.au.                   172800  IN      A       58.65.254.1
a.au.                   172800  IN      AAAA    2407:6e00:254::1
s.au.                   172800  IN      A       65.22.198.1
s.au.                   172800  IN      AAAA    2a01:8840:c0::1
q.au.                   172800  IN      A       65.22.196.1
q.au.                   172800  IN      AAAA    2a01:8840:be::1
```

```
;; ANSWER SECTION:
edu.au.                 3600    IN      NS      a.au.
edu.au.                 3600    IN      NS      q.au.
edu.au.                 3600    IN      NS      r.au.
edu.au.                 3600    IN      NS      s.au.
edu.au.                 3600    IN      NS      t.au.
```

```
;; ADDITIONAL SECTION:
ns1-ext.unsw.edu.au.    3600    IN      A       54.79.80.189
ns1-ext.unsw.edu.au.    3600    IN      AAAA    2001:388:c:35::11
ns2-ext.unsw.edu.au.    3600    IN      A       13.236.238.52
ns2-ext.unsw.edu.au.    3600    IN      AAAA    2001:388:c:35::22
ns3-ext.unsw.edu.au.    3600    IN      A       54.66.99.146
ns3-ext.unsw.edu.au.    3600    IN      AAAA    2001:388:c:35::33
```

```
;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.172.11
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.242.2
maestro.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.242.33
```

```
;; ANSWER SECTION:
lyre01.cse.unsw.EDU.AU. 3600    IN      A       129.94.210.21
```

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

-a.root-servers.net.

-t.au.

-a.au.

-ns1-ext.unsw.edu.au.

-beethoven.orchestra.cse.unsw.edu.au.

IP

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

Answer: Yes, a single physical machine can have multiple names and multiple IP addresses. Because a machine may have more than one network interface and each with its own IP address. A machine can have both an IPv4 address and an IPv6 address. A server with IP can be mapped to multiple domain names.

Exercise 4: A Simple Web Server (5 Marks)

Please submit the source code as a separate file.