Exercise 3

A computer screen shot of a black screen

Description automatically generated

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

 In the ANSWER SECTION, The IP address of [www.hi.is](http://www.hi.is/)  is 130.208.165.186.

 We can find the type of DNS query under QUESTION SECTION, which is type A DNS

Question 2. What is the canonical name for the webserver (i.e., [www.hi.is](http://www.hi.is/))? Suggest a reason for having an alias for this server.

In the ANSWER SECTION, the canonical name for [www.hi.is](http://www.hi.is/) is web-lb.rhi.hi.is.

Reason: Aliases are easy for human to recall compared to the IP address, additionally it can also maintain when the IP address of a server change.

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))?

flags: Give us summary of the response.

Cookies: Record the cookie the sent by the server.

The section at the bottom gave us brief information from the query sender, query time, sender IP address, time of query sent and the message size.

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

129.94.208.2

Question 5. What are the DNS nameservers for the " **hi.is**” domain (note: the domain name is **hi.is**and not [www.hi.is](http://www.hi.is/). 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?

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedNS DNS query type is used to obtain the nameserver and A DNS query type is used to obtain the IP address. The nameservers are:  dvalinn.rhnet.is(130.208.16.21) , borg.rhi.hi.is(130.208.165.54) and info.rhi.hi.is(130.208.143.33).

Question 6. What is the DNS name associated with the IP address 18.67.93.67 ? Which DNS query type is used to obtain this information?

A computer screen shot of a black screen

Description automatically generated

DNS query type PTR is used to track the DNS name of a specific IP address. The DNS name is server-18-67-93-67.syd62.r.cloudfront.net

Question 7. Run, dig and query the CSE nameserver (129.94.242.2) for the mail servers for outlook.com (again, the domain name is outlook.com, not [www.outlook.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)

A screenshot of a computer

Description automatically generated

No, I didn't get an authoritative answer, since the flags doesn't contain aa.

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

A screenshot of a computer

Description automatically generated

Didn’t get a response with borg.rhi.hi.is to outlook.com. The status is REFUSED.

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

A screenshot of a computer

Description automatically generated

Then I pick nse13.o365filtering.com as the nameserver

A screenshot of a computer

Description automatically generated

We use type MX DNS query to obtain this information.

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?

A screenshot of a computer screen

Description automatically generated

I pick a.root-servers.net(198.41.0.4)

A screenshot of a computer screen

Description automatically generated

We are now referred to .au nameserver Then I pick a.au(58.65.254.1).

A screenshot of a computer

Description automatically generated

Then we are referred to edu.au, the IP didn’t change, we still use t.au to do next step

nA screenshot of a computer screen

Description automatically generated

Now we are referred to unsw.edu.au. nameserver. I choose ns1.unsw.edu.au(129.94.9.192)

A computer screen shot of a black screen

Description automatically generated

Now we are referred to the CSE nameserver, we now send type A DNS query.

A computer screen shot of a black screen

Description automatically generated

The IP address of lyre00.cse.unsw.edu.au is 129.94.210.20.

We query 5 DNS servers for an authoritative answer.

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

Yes, it can have multiple names and IP addresses associated with it since it can have multiple network interfaces.

Exercise 4:

To achieve persistent, I set timeout to each connection, when connection is closed, it have to build connection again.