Howework 5 (DNS)

Answer the following questions in the space provided. Submit your answers (a modified version of this file) as an attachment to the submission box. Consult the file **2.Wireshark_DNS_v7.0.pdf** if needed.

Concepts

- How DNS is organized?
- What are the **resource records** maintained by each DNS server?
- How to search DNS servers?
- How to use `dig` and `nslookup`.
- How DNS queries and resource recorded are transmitted?

DNS and `dig` Tool

`dig` is a UNIX utility that can interact with DNS servers. We will use `dig` to explore the DNS domain hierarchy. (Read Dig Command Examples for some examples.)

Start `CSC361-VM`. Open a terminal and enter the command:

```
$ dig
```

This will request from your local namer server the list of all **root** name servers.

Q1. How many **root** name servers? What are they?

> *13 root name servers*

> *c.root-servers.net.*
> *m.root-servers.net.*
> *e.root-servers.net.*
> *a.root-servers.net.*
> *j.root-servers.net.*
> *i.root-servers.net.*
> *g.root-servers.net.*
> *h.root-servers.net.*
> *l.root-servers.net.*
> *d.root-servers.net.*
> *b.root-servers.net.*
> *f.root-servers.net.*
> *k.root-servers.net.*

Q2. What is the IP address of the **name server** that provides these answers?

> *142.104.6.1*

Enter the following shell command:

```
$ dig NS ca
```

which requests from your local name server a list of all the name servers responsible for the `.ca` domain.

Q3. How many such name servers? What are they?

> *4 servers*
>
> *any.ca-servers.ca*
>
> *j.ca-servers.ca.*
>
> *c.ca-servers.ca.*
>
> *x.ca-servers.ca.*

Enter the following shell command:

```
$ dig @m.root-servers.net NS ca
```

which requests from one of the **root** name server a list of all the name servers responsible for the `.ca` domain.

Q4. Does this list look exactly the same as the answers in Q3?

> *There no servers*

We are going to **iteratively** investigate all the domain name servers in the DNS hierarchy. Our target hostname is `www.csc.uvic.ca`. There are several domains or subdomains in this hostname, i.e., `.ca`, `.uvic.ca`, `.csc.uvic.ca`.

Enter the following shell command

```
$ dig NS ca
```

which will list all name servers responsible for the `.ca` domain.

Q3. What are they? (The same question as Q3.)

> *any.ca-servers.ca*
>
> *j.ca-servers.ca.*
>
> *c.ca-servers.ca.*
>
> *x.ca-servers.ca.*

Now, take one of those listed name servers and enter:

```
$ dig @<one of the named servers> NS uvic.ca
```

Essentially, we are asking one of the `.ca` root name servers all the namer servers responsible for `.uvic.ca` domain.

Q5. What the registered name servers responsible for `uvic.ca`? How many? What are there?

Now, repeat the command for `csc.uvic.ca` domain by asking one of the name servers in Q5.

```
$ dig @<one of the named servers> NS csc.uvic.ca
```

Q6. What the registered name servers responsible for `csc.uvic.ca`? How many? What are there?

Q7. List all the mail servers for google.com.

Q8. List all DNS record types about "uvic.ca", including A, AAAA, TXT, MX and NS.

DNS and `nslookup` Tool

```
nslookup www.ncu.edu.tw
```

Q9. Run `nslookup` to obtain the IP address of `www.ncu.edu.tw`. What is the IP address of this web server?

> *140.115.17.82*

```
nslookup â€“type=NS ncu.edu.tw
```

Q10. Run `nslookup` to determine the authoritative DNS servers for `ncu.edu.tw`. What are they?

> *140.115.1.33*
>
> *140.115.1.29*

```
nslookup www.ncu.edu.tw <one of the name servers in Q10>
```

Q11. Run `nslookup` to one of the DNS servers obtained in last Question. What are the answers? Compare it against Q9.

> *140.115.17.82 it the same*

```
nslookup -type=MX yahoo.com
```

Q12. Query the mail servers for `yahoo.com` and `yahoo.ca`. What are the results?

> *the same results*
> *68.180.131.16*
> *119.160.253.83*
> *98.138.11.157*
> *203.84.221.53*
> *68.142.255.16*

UDP and DNS

Now, we should use Wireshark to investigate what were sent from your computer when you use `dig` or `nslookup`.

- Start `CSC361-VM`.
- Open a terminal session.
- Flush your DNS cache. (Read How To Flush Your DNS Cache).

- Start Wireshark with a capture filter `ip.addr == your_IP_address`.
- In your terminal, enter the `dig` or `nslookup` commands that you did earlier Q1 to Q3.
- Stop Wireshark but don't close.

Q13. Locate the DNS query and response messages. Are then sent over UDP or TCP?

> *UDP*

Q14. What is the destination port for the DNS query message? What is the source port of DNS response message?

> *Source Port: 50596*
> *Destination Port: 53*

Q15. To what IP address is the DNS query message sent? Compare it to Q1. Are these two IP addresses the same?

> *142.104.6.1 SAME*

Q16. Examine the DNS **query** message. What `Type` of DNS query is it? Does the query message contain any *answers*?

> *Standard query*

Q17. Examine the DNS **response** message. How many *answers* are

provided? What do each of these answers contain? (For example, answers in Q1.)

> *13 answers*