

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 records 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:

```
1 $ dig
```

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

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

|

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

|

Enter the following shell command:

```
1 $ 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?

Enter the following shell command:

```
1 $ 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?

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

```
1 $ dig NS ca
```

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

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

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

```
1 $ dig @<one of the named servers> NS uvic.ca
```

Essentially, we are asking one of the `.ca` root name servers all the name 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.

```
1 $ 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

```
1 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?

```
1 nslookup -type=NS ncu.edu.tw
```

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

```
1 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.

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

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

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?

|

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

|

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

|

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

|

Q17. Examine the DNS **response** message. How many *answers* are provided? What do each of these answers contain? (For example, answers in Q1.)

|