Wireshark Lab: DNS

In our lecture, we have already mentioned the function of the Domain Name System (DNS) in translating hostnames to IP addresses, performing a critical role in the Internet infrastructure. In this lab, we'll look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back.

Nslookup

We will be using the *nslookup* tool, which is available in most Linux/Unix and Microsoft platforms. To run *nslookup* in our Ubuntu lab machines, type **`nslookup`** command on the Terminal. To run it in Windows, type the **`nslookup`** command on Command Prompt.

The nslookup tool queries any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level domain DNS server, an authoritative DNS server, or an intermediate DNS server. To do this, nslookup sends a DNS query to the specified DNS server and then receives a reply from that same DNS server, and displays the result.

The sample run of nslookup below shows the results of three independent nslookup runs.

```
$ nslookup berdugo.upm.edu.ph
Server:         172.16.1.130
Address:        172.16.1.130#53

Name:   berdugo.upm.edu.ph
Address: 202.92.148.162

$ nslookup -type=NS upm.edu.ph
Server:         172.16.1.130
Address:        172.16.1.130#53

upm.edu.ph      nameserver = timog.upm.edu.ph.

$ nslookup www.up.edu.ph
Server:         172.16.1.130
Address:        172.16.1.130#53

Non-authoritative answer:
www.up.edu.ph   canonical name = up.edu.ph.
Name:   up.edu.ph
Address: 104.25.22.19
Name:   up.edu.ph
Address: 104.25.23.19
```

The first command:

```
nslookup berdugo.upm.edu.ph
```

queries the default DNS server for the IP address of berdugo.upm.edu.ph. It's like telling the DNS server "please send me the IP address for the host berdugo.upm.edu.ph". If you look at the response to this command, it provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of berdugo.upm.edu.ph.

Let's look at the second command:

```
nslookup -type=NS upm.edu.ph
```

In this example, the option "-type = NS" causes the nslookup to send a query for a type-NS record to the default local DNS server. It's like asking the DNS server "please send me the host names of the authoritative DNS for upm.edu.ph". (When the –type option is not used, nslookup uses the default, which is to query for type A records.) The answer first indicates the DNS server that is providing the answer along the authoritative DNS server for upm.edu.ph. The IP address of the authoritative DNS server is also returned when the DNS server you have queried is not the authoritative one for the domain name you are querying.

When the reply is non-authoritative, nslookup will indicate the response as non-authoritative answer. See the result of

```
nslookup www.up.edu.ph
```

There are still other options that could be used with nslookup. You can easily search for those other options over the web. Now answer the following questions: (For each answer, include a screenshot showing the nslookup command you have issued and the response it received, which you used as basis for your answer.)

1. What is the IP address of www.upd.edu.ph?
2. What are the authoritative DNS servers for upd.edu.ph?
3. What are the hostname and IP address of the mail servers for @upd.edu.ph?

Dig

A more powerful Linux DNS querying tool is dig. Dig is often used in network troubleshooting due to the many functionalities it can perform. Its output also shows most of the part of a DNS message. Dig can be used to perform DNS lookups, find host addresses, IP address, mail exchanges, CNAMES, and more. It can also be used to verify ISP DNS server and Internet connectivity.

While dig is already available in Ubuntu Linux by default, it is not available in Windows. If you are using a Windows machine, go to ISC's bind site (http://www.isc.org/downloads/bind/) and download bind. Make sure to download the proper binary version (based on your version of Windows). After downloading bind, extract it to a directory. Use command prompt to go to the extracted directory and use can run dig from command line.

To use dig, it is very similar to nslookup.

```
$ dig www.upm.edu.ph
; <<>> DiG 9.9.5-3ubuntu0.4-Ubuntu <<>> www.upm.edu.ph
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54400
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.upm.edu.ph.                        IN      A

;; ANSWER SECTION:
www.upm.edu.ph.         86400   IN      CNAME   habagat.upm.edu.ph.
habagat.upm.edu.ph.     86400   IN      A       202.92.148.134

;; AUTHORITY SECTION:
upm.edu.ph.             86400   IN      NS      timog.upm.edu.ph.

;; ADDITIONAL SECTION:
timog.upm.edu.ph.       86400   IN      A       172.16.1.130
timog.upm.edu.ph.                  86400        IN                  AAAA
2400:b000:300:1:214:5eff:fe69:75ef

;; Query time: 0 msec
;; SERVER: 172.16.1.130#53(172.16.1.130)
;; WHEN: Tue Sep 01 02:06:49 PHT 2015
;; MSG SIZE  rcvd: 145
```

The command **`dig www.upm.edu.ph`** above queries for the IP address of www.upm.edu.ph. As you can see, dig displays lots of information. Let's now look the dig command output:

- The **question section** displays the query type. By default, the query type is for A. In the above example, we wanted to find out the IP address of a hostname. Hence, A is okay with us.
- The **answer section** contains the answer to the query.
- The **authority section** contains the authoritative name server for the domain upm.edu.ph and the **additional section** contains the IP addresses of the authoritative name servers.
- The final section contains the statistics about the query.

To make a specific type of DNS query, we will use the following:

```
dns hostname|IPAddress type
```

where **`type`** could be the following:

- A for an IPv4 address
- AAAA for an IPv6 address
- CNAME for canonical name record
- MX for email server host names
- NS for authoritative name server names
- PTR for pointer to canonical name which is used for reverse DNS lookups

To query for the authoritative name server of upm.edu.ph, we use:

```
$ dig upm.edu.ph NS

; <<>> DiG 9.9.5-3ubuntu0.4-Ubuntu <<>> upm.edu.ph NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32996
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;upm.edu.ph.                    IN      NS

;; ANSWER SECTION:
upm.edu.ph.            86400   IN      NS      timog.upm.edu.ph.

;; ADDITIONAL SECTION:
timog.upm.edu.ph.      86400   IN      A       172.16.1.130
timog.upm.edu.ph.                  86400       IN              AAAA
2400:b000:300:1:214:5eff:fe69:75ef

;; Query time: 7 msec
;; SERVER: 172.16.1.130#53(172.16.1.130)
;; WHEN: Tue Sep 01 02:19:37 PHT 2015
;; MSG SIZE  rcvd: 103
```

To query for the mail servers of upm.edu.ph, we use the following. Note that we use the **`+short`** option to limit the output to only the answers to our query.

```
$ dig +short upm.edu.ph MX
10 aspmx5.googlemail.com.
1 aspmx.l.google.com.
5 alt1.aspmx.l.google.com.
5 alt2.aspmx.l.google.com.
10 aspmx2.googlemail.com.
10 aspmx3.googlemail.com.
10 aspmx4.googlemail.com.
```

To make a reverse DNS lookup, we use the –x option followed by the IP address.

```
$ dig -x 202.92.148.162

; <<>> DiG 9.9.5-3ubuntu0.4-Ubuntu <<>> -x 202.92.148.162
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26142
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;162.148.92.202.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
162.148.92.202.in-addr.arpa. 86400 IN   PTR     berdugo.upm.edu.ph.

;; AUTHORITY SECTION:
148.92.202.in-addr.arpa. 86400  IN      NS      timog.upm.edu.ph.

;; ADDITIONAL SECTION:
timog.upm.edu.ph.       86400   IN      A       172.16.1.130
timog.upm.edu.ph.                  86400        IN                AAAA
2400:b000:300:1:214:5eff:fe69:75ef

;; Query time: 0 msec
;; SERVER: 172.16.1.130#53(172.16.1.130)
;; WHEN: Tue Sep 01 02:25:31 PHT 2015
;; MSG SIZE  rcvd: 152
```

We can force dig to follow the delegation path from the root name servers for the name being looked up.

```
$ dig +trace upd.edu.ph

; <<>> DiG 9.9.5-3ubuntu0.4-Ubuntu <<>> +trace upd.edu.ph
;; global options: +cmd
.                       455642  IN      NS      g.root-servers.net.
.                       455642  IN      NS      a.root-servers.net.
.                       455642  IN      NS      h.root-servers.net.
.                       455642  IN      NS      d.root-servers.net.
.                       455642  IN      NS      k.root-servers.net.
.                       455642  IN      NS      c.root-servers.net.
.                       455642  IN      NS      i.root-servers.net.
.                       455642  IN      NS      b.root-servers.net.
.                       455642  IN      NS      l.root-servers.net.
.                       455642  IN      NS      j.root-servers.net.
.                       455642  IN      NS      f.root-servers.net.
.                       455642  IN      NS      m.root-servers.net.
.                       455642  IN      NS      e.root-servers.net.
.                             455642   IN        RRSIG    NS 8 0 518400
20150909170000            20150830160000           1518           .
Gzngu4elkcCBcNcSMjUfrHF9UR5bDDprnFOOGAzu84ZgymX1B9iNx8Cw
sd+Z2VhQVycOqv3VxEqFSGAcDS93S2cLVSkCB/kT3FWVlvkUIT9e/lko
/G1Ud6ek620X1Oyu+csSlAGlhrReSPKkdzhFXms0IAZGEJQmx8QGVFMR LGs=
;; Received 913 bytes from 172.16.1.130#53(172.16.1.130) in 17 ms

ph.                   172800  IN      NS      ph.cctld.authdns.ripe.net.
ph.                     172800  IN      NS      ph.communitydns.net.
ph.                     172800  IN      NS      ns2.cuhk.edu.hk.
ph.                     172800  IN      NS      sec4.apnic.net.
ph.                     172800  IN      NS      sns-pb.isc.org.
ph.                     86400   IN      NSEC    pharmacy. NS RRSIG NSEC
ph.                          86400    IN        RRSIG    NSEC 8 1 86400
20150910170000             20150831160000              1518             .
eSv0Y6sIC+oisByUwzJrelXk1fO74g4noN8feSgX4ZhKOmrL4pJaiBuD
Fi+cjIy2YdwU/K0+mpwzBfh904xQiilH1/tvq/GxWYDk2w4U46Ea1gPz
/QDdsHNxfV5cVpElVC3CY4rKTODY16rHv4p8URTTzXE4Fwsyv7bMdqtQ ZYI=
;; Received 571 bytes from 2001:7fd::1#53(k.root-servers.net) in 66 ms

edu.ph.                 86400   IN      NS      gabriela.ph.net.
edu.ph.                 86400   IN      NS      ns.skyinet.net.
edu.ph.                 86400   IN      NS      gomez.ph.net.
;;             Received            113            bytes            from
2001:dc0:4001:1:0:1836:0:141#53(sec4.apnic.net) in 341 ms

upd.edu.ph.             86400   IN      NS      ns03.upd.edu.ph.
upd.edu.ph.             86400   IN      NS      ns01.upd.edu.ph.
upd.edu.ph.             86400   IN      NS      ns02.upd.edu.ph.
;; Received 144 bytes from 165.220.3.7#53(gabriela.ph.net) in 23 ms

upd.edu.ph.             86400   IN      A       202.92.128.20
upd.edu.ph.            86400   IN      RRSIG   A 5 3 86400 20150927065017
20150828065017                    31485                        upd.edu.ph.
lfQTm6Xpw4fwhhGDOA10SqLZxvq4gdUxCM3wfeYlPEIFGR9LdaRYZi27
2FgFqsp8Pc61+QqfFYHgNcF00s6cEb57vsArvuWOqyA5HaP5RfX4iQJM
5XQ9hJy8JaoO3EQ2pPkRUGb5QCrxRJrFBM/F826rRKmq1/H4e1diStHw dG0=
upd.edu.ph.             86400   IN      NS      ns02.upd.edu.ph.
upd.edu.ph.             86400   IN      NS      ns01.upd.edu.ph.
upd.edu.ph.             86400   IN      NS      ns03.upd.edu.ph.
upd.edu.ph.            86400   IN      RRSIG   NS 5 3 86400 20150927065017
20150828065017                    31485                        upd.edu.ph.
FxrOpcjidti+TXllGU+ym3yyN01qVz23MwPHYrc4TLLHRI70F35b+O9l
Hf9XTxiQA9IuBErKGZvU+VL+YguJ0iNQcgD6CTMt7TNDABTOiGx3NST6
QVHaPNGOEv7w1bMkv+Ya27jSEYnWa0lBgNGD7mlorsNqyOOJuzFZjJKM wfE=
;; Received 1010 bytes from 202.92.128.249#53(ns02.upd.edu.ph) in 3 ms
```

As mentioned in our lecture, name servers can cache the answers it received to speed up DNS name resolution. How long this can be cached is determined by the TTL value, which is set the authoritative name servers. The TTL is set in seconds. To determine the TTL value of www.upd.edu.ph

```
$ dig +nocmd +noall +answer +ttlid A www.upd.edu.ph
www.upd.edu.ph.         77621   IN      CNAME   upd.edu.ph.
upd.edu.ph.             42874   IN      A       202.92.128.20
```

Answer the following questions by using only 1 dig command. For each of your answer, include a screenshot showing the dig command you have issued and response it received, which you use as basis for your answer.

4. What are the IP addresses of www.yahoo.com?
5. Is www.yahoo.com a canonical name or an alias? If it's an alias, then what is the canonical name?

6. What are the names and IP addresses of the authoritative name servers of yahoo.com?

Tracing DNS with Wireshark

Let’s now trace what is going on in the network as we make DNS queries.

- Open your browser and empty your browser cache.
- Open Wireshark and enter “ip.addr==your_IP_address” into the filter. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark
- With your browser, visit http://dpsm.cas.upm.edu.ph
- Stop the packet capture.

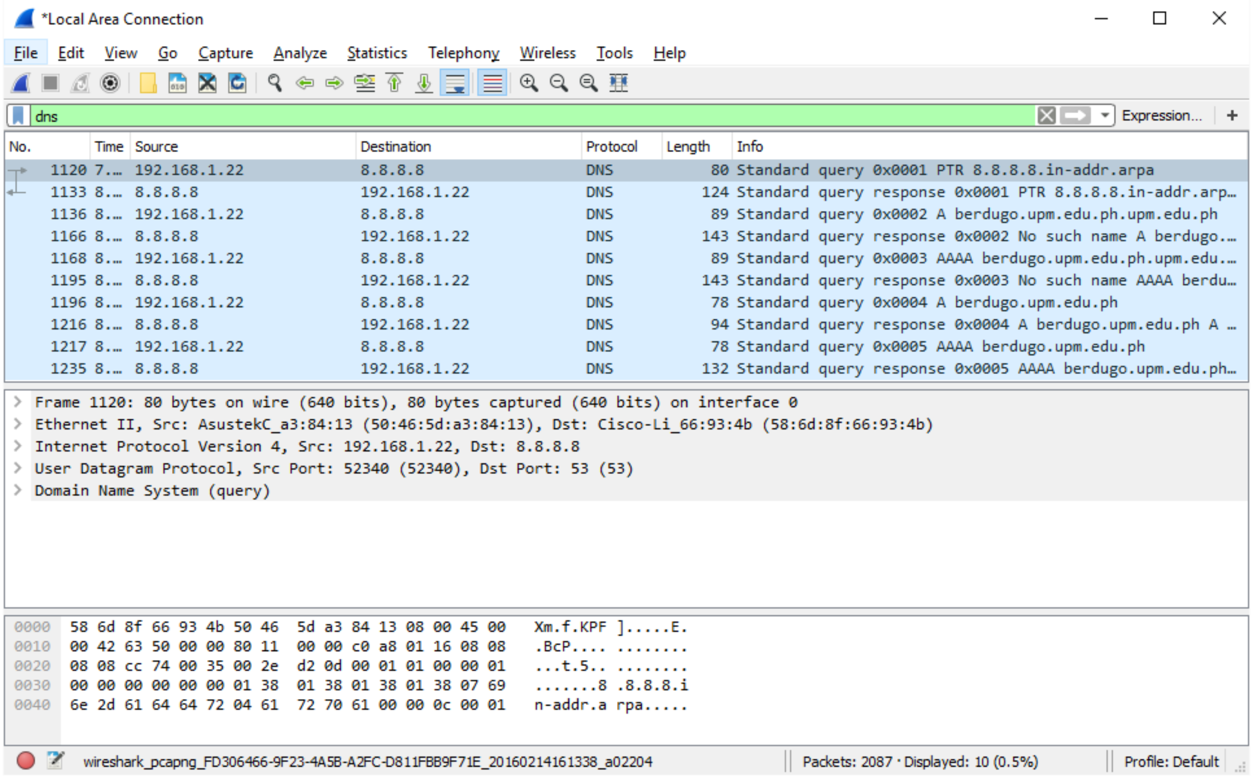
Answer the following questions. For every answer, include a packet trace supporting your answer (similar to what you did in the last lab activity).

7. Locate the DNS query and response messages. Are they sent over UDP or TCP?
8. What is the destination port for the DNS query message? What is the source port of DNS response message?
9. To what IP address is the DNS query message sent? Is this the same as your local DNS server?
    - Linux: You can refer to “Connection Information”, which is next to the volume icon, for your local DNS server (Primary DNS server).
    - Windows: If you can refer to your network details and look at IPv4 DNS servers for your local DNS server.
10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answer”?
11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
12. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
13. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Now let’s trace the packets of nslookup:

- Start packet capture.
- Type “dns” in the filter field.
- Do an nslookup on berdugo.upm.edu.ph.
- Stop packet capture.

You should get a trace that looks something like the following:


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression…
+

No.	Time	Source	Destination	Protocol	Length	Info
1120	7.…	192.168.1.22	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
1133	8.…	8.8.8.8	192.168.1.22	DNS	124	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arp…
1136	8.…	192.168.1.22	8.8.8.8	DNS	89	Standard query 0x0002 A berdugo.upm.edu.ph.upm.edu.ph
1166	8.…	8.8.8.8	192.168.1.22	DNS	143	Standard query response 0x0002 No such name A berdugo.…
1168	8.…	192.168.1.22	8.8.8.8	DNS	89	Standard query 0x0003 AAAA berdugo.upm.edu.ph.upm.edu.…
1195	8.…	8.8.8.8	192.168.1.22	DNS	143	Standard query response 0x0003 No such name AAAA berdu…
1196	8.…	192.168.1.22	8.8.8.8	DNS	78	Standard query 0x0004 A berdugo.upm.edu.ph
1216	8.…	8.8.8.8	192.168.1.22	DNS	94	Standard query response 0x0004 A berdugo.upm.edu.ph A …
1217	8.…	192.168.1.22	8.8.8.8	DNS	78	Standard query 0x0005 AAAA berdugo.upm.edu.ph
1235	8.…	8.8.8.8	192.168.1.22	DNS	132	Standard query response 0x0005 AAAA berdugo.upm.edu.ph…

```
> Frame 1120: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
> Ethernet II, Src: AsustekC_a3:84:13 (50:46:5d:a3:84:13), Dst: Cisco-Li_66:93:4b (58:6d:8f:66:93:4b)
> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52340 (52340), Dst Port: 53 (53)
> Domain Name System (query)
```

```
0000  58 6d 8f 66 93 4b 50 46  5d a3 84 13 08 00 45 00   Xm.f.KPF ].....E.
0010  00 42 63 50 00 00 80 11  00 00 c0 a8 01 16 08 08   .BcP.... ........
0020  08 08 cc 74 00 35 00 2e  d2 0d 00 01 01 00 00 01   ...t.5.. ........
0030  00 00 00 00 00 00 01 38  01 38 01 38 01 38 07 69   .......8 .8.8.8.i
0040  6e 2d 61 64 64 72 04 61  72 70 61 00 00 0c 00 01   n-addr.a rpa.....
```

wireshark_pcapng_FD306466-9F23-4A5B-A2FC-D811FBB9F71E_20160214161338_a02204 | Packets: 2087 · Displayed: 10 (0.5%) | Profile: Default

We see that nslookup actually sent several DNS queries and received several DNS responses. For this activity, in answering the following questions, look only at the query which has a type A and the name is the hostname you used in the nslookup and its corresponding response, as they are specific to nslookup and are not normally generated by standard Internet applications. You should instead focus on the this query and response messages.

14. What is the destination port for the DNS query message? What is the source port of DNS response message?
15. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
16. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
17. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Now repeat the previous steps but instead issue the command:

```
nslookup -type=NS upm.edu.ph
```

Answer the following questions:

18. To what IP address is the DNS query message sent? Is this the IP address of your local DNS server?
19. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contains any “answers”?
20. Examine the DNS response message. What name servers does the response provide?