Domain Name System

In this exercise, you will be observing different DNS resource records through **`nslookup`** and inspecting DNS packets to explore their content and relate these to the protocol specifications defined in the DNS RFC.

1. Ensure that your PC has connectivity to a DNS server.

   i. To check your DNS server setting, open up the command line terminal on the PC and input the command:

   `ipconfig /all`

   Look for the DNS server setting under your Ethernet/WLAN adapter connection and copy the IP address here:

10.160.41.211

   ii. Ping the DNS server IP address and ensure that you can contact it. Attach the screenshot.

```
C:\Users\danie>ping 10.160.41.211

Pinging 10.160.41.211 with 32 bytes of data:
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128

Ping statistics for 10.160.41.211:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\danie>
```

2. On the PC command line, start the nslookup tool by entering the command.

   `nslookup`

   The prompt should change to “>”

3. Determine the administrative zone of the server by querying for Start of Authority (SOA) records:

   i. Enter the following commands:

```
set type=SOA
delta.dlsu.edu.ph
```

   ii. From the output, identify the domain name administered by this server:

delta.manila.dlsu.edu.ph

   What other information about a domain can you get from an SOA record?

responsible mail address, serial number, refresh in seconds, retry in seconds, expire in seconds, default TTL in seconds.

4. Try to trace the DNS tree structure up to the root server for the branch where your DNS server belongs. Query for the DNS servers of the domains listed below. You may input the domain name directly. No need to set the record type again.

Domain	Primary DNS server name or IP address
dlsu.edu.ph	delta.manila.dlsu.edu.ph
edu.ph	gomez.ph.net
ph	ph-tld-ns.dot.ph
.	a.root-servers.net

5. Determine the name servers of a domain querying for name server (NS) records: Set 'NS' as the record type to be queried using the command

```
set type=NS
```

6. Query the following domains and fill in the number of name servers serving each of them.

Domain	Number of DNS servers
dlsu.edu.ph	3
edu.ph	4
ph	4
.	13

Why would there be a need for multiple name servers for a domain?

There would be a need for multiple name servers for a domain because it helps domains remain available and perform well under all conditions.

Why would a DNS server need to contain NS type of resource records?

A DNS server needs to contain NS type of resource records to ensure the proper delegation and management of the domain name system hierarchy.

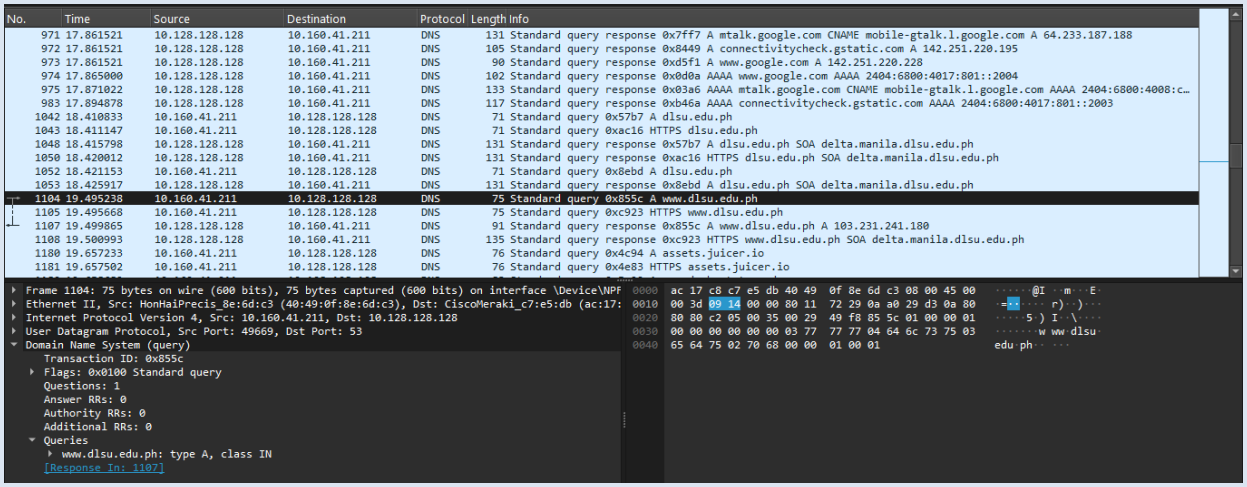
7. Run Wireshark and set it to capture on your Ethernet/WLAN connection. Set the filter to capture only DNS (UDP port 53)
8. Get DNS host records by setting query type to 'A', then query for the host www.dlsu.edu.ph.

   What is the response of the server?

   Answer RRs: 0

9. Go to Wireshark and check captured packets, there should be a query and reply packet for www.dlsu.edu.ph
   i. Look for the DNS query packet of the client then expand the DNS message details. Observe the data within the query

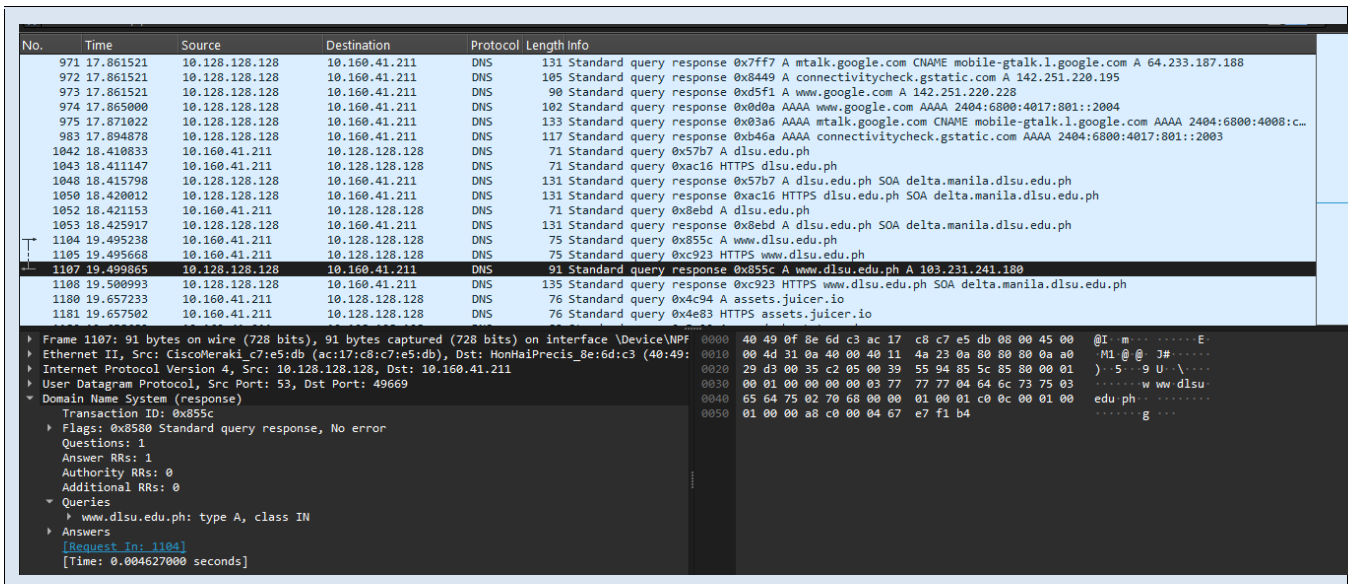
      How many questions are included in the message? Attach the screenshot of the captured packet.



1 question

ii. Look for the DNS reply packet of the server then expand the DNS message details. Observe the flag values and data within the query

How many answers are included in the message? Based on the flag value, is the answer considered authoritative? Attach the screenshot of the captured packet.



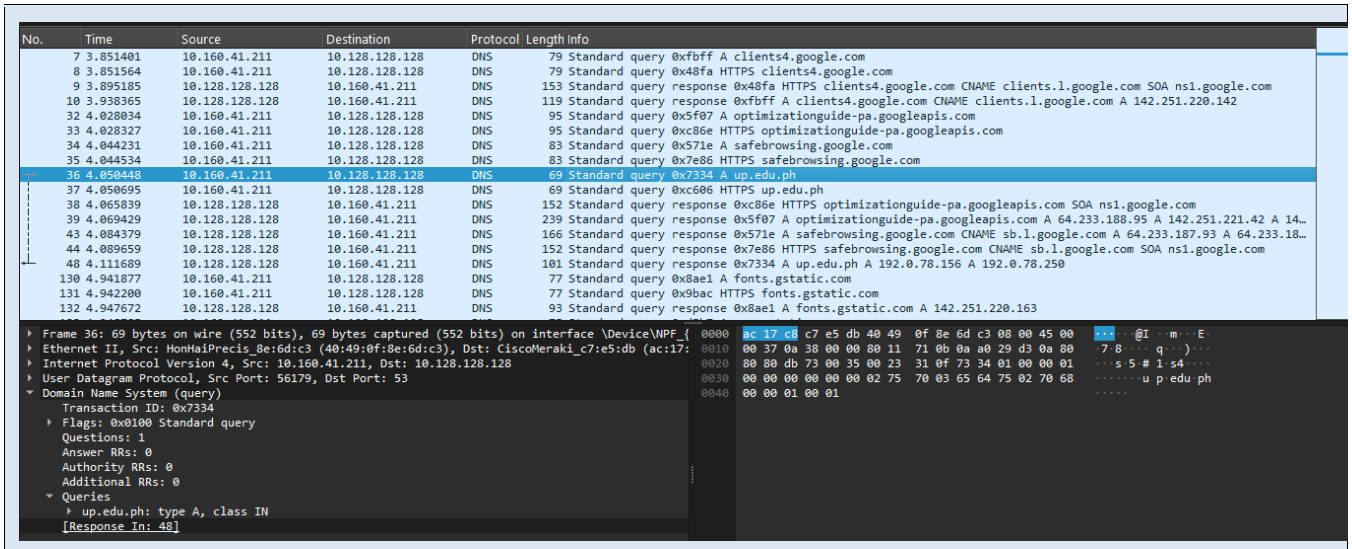
The answer is not authoritative.

What does it mean if the server returns an authoritative answer in the DNS response?

it means that the DNS server providing the response has the original records of the domain because it is directly responsible for that domain

10. Using nslookup, query for ‘www.up.edu.ph’ this time then check Wireshark for the server reply for ‘www.up.edu.ph’.

    What is the value of the ‘Authoritative’ flag? Attach the screenshot of the captured packet.



0

Why is the authoritative flag different for this response?

The authoritative flag is same because it uses the same DNS query.

11. Stop the packet capture on Wireshark.
12. Try querying for ‘dlsu.instructure.com’, which is the URL for Animospace. Notice that the result includes a different name. This is an indication that the name is an alias rather than the real name of the server.
13. Set the nslookup query type to ‘cname’ to query the DNS for canonical names.

    Query for ‘dlsu.instructure.com’. What is its canonical name? Attach a screenshot.

```
> dlsu.instructure.com
Server:  UnKnown
Address:  10.128.128.128

Non-authoritative answer:
dlsu.instructure.com    canonical name = cluster396.instructure.com
```

14. Query for the canonical name of the result obtained in #13.

    What is its canonical name? Attach a screenshot.

```
Non-authoritative answer:
dlsu.instructure.com    canonical name = cluster396.instructure.com
cluster396.instructure.com      canonical name = canvas-sin-prod-c396-1782718951.ap-southeast-1.elb.amazonaws.com
>
```

Based on the result, which provider do you think is hosting Animospace?

Amazon Web Services

15. Get mail exchange records by setting query type to ‘MX’, then query for the domain dlsu.edu.ph.

    How many mail servers are used by DLSU?

```
*** Can't find address for server dlsu.edu.ph: Non-authoritative answer
> set type=mx
> dlsu.edu.ph
Server:  UnKnown
Address:  10.128.128.128

dlsu.edu.ph     MX preference = 2, mail exchanger = aspmx.l.google.com
aspmx.l.google.com      internet address = 108.177.97.27
aspmx.l.google.com      AAAA IPv6 address = 2404:6800:4008:c19::1b
```

2 mail servers

Based on the results, which provider is hosting the mail services for DLSU?

Google