SIT202: Computer Networks and Communication

Leaning Evidence for Active Class Task 3

Name: Kenisha Corera
Student ID: C23020001

Members in this group activity task:

Nishad	– C23110001
Kenisha	– C23020001
Shekaina	– C23110002
Raaid	– C23020004
Pavithran	– C22060015

Activity 1

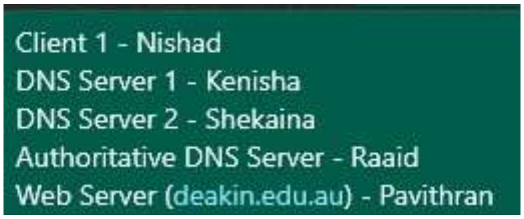
1. What is the core Internet function provided by DNS?
    - Domain Name System (DNS) translates human – readable domain names into IP addresses which are used by computers to identify each other in a network.

2. Why do we need DNS?
    - DNS is essential because it simplifies the process of accessing websites and other resources on the internet.

3. What is the layer that DNS belong to?
    - DNS protocol belongs and operates in the Application Layer in the TCP/IP model.

4. Do you think a single DNS server is enough to support the entire network? Justify your answer. Provide alternate solution if we have any
    - A singe DNS server is not sufficient to support the entire network due to the sheer volume of request and the need for redundancy. A distributed system of DNS servers is used to handle the load, provide faster response times and to ensure reliability. Alternatives could include using either Top – Level Domain (TLD) and authoritative name servers.

5. Discuss the steps involved in your browser to send a HTTP request message to the Web server, deakin.edu.au. Assume that this is the first time you access this webpage. You can continue the discussion as a role play.
    a. One group member can act as the web server, another as DNS servers (you need to decide how many DNS serves will be involved), and the remaining members can be the clients.

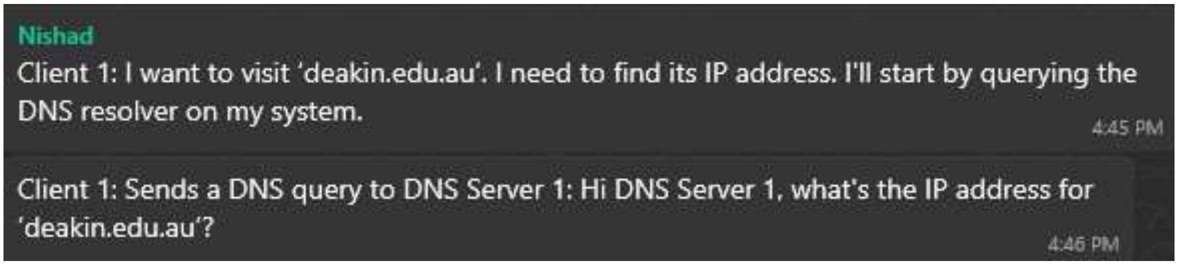


Client 1 - Nishad
DNS Server 1 - Kenisha
DNS Server 2 - Shekaina
Authoritative DNS Server - Raaid
Web Server (deakin.edu.au) - Pavithran

b. First, Client 1 needs to view deakin.edu.au and initiate the conversation saying the right message to the right device (to the person who is acting as the right device). Use your knowledge about web browsing that we covered in Module 1 and the first part of Module 2. Assume that there is no DNS caching available.

c. All the devices need to respond to each other with the correct messages in the right sequence. Make sure you record all the steps as you will need those notes to complete the activity 2.

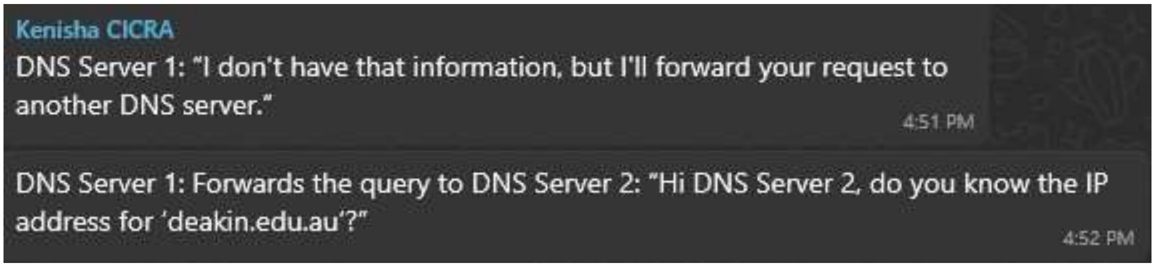
Part 1: Client 1 Accessing deakin.edu.au



Nishad

Client 1: I want to visit ‘deakin.edu.au’. I need to find its IP address. I'll start by querying the DNS resolver on my system. 4:45 PM

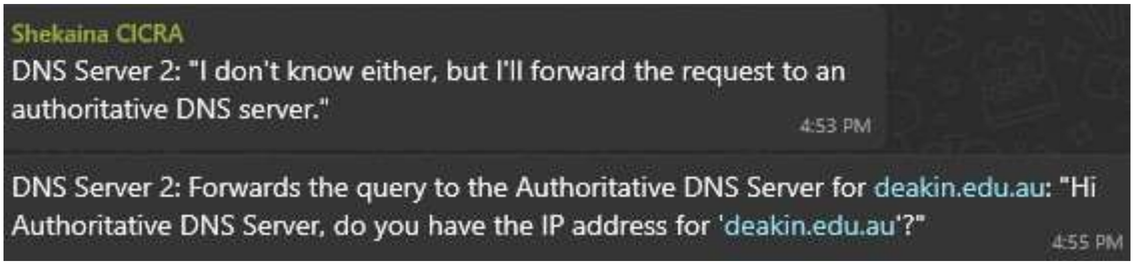
Client 1: Sends a DNS query to DNS Server 1: Hi DNS Server 1, what's the IP address for ‘deakin.edu.au’? 4:46 PM



Kenisha CICRA

DNS Server 1: “I don't have that information, but I'll forward your request to another DNS server.” 4:51 PM

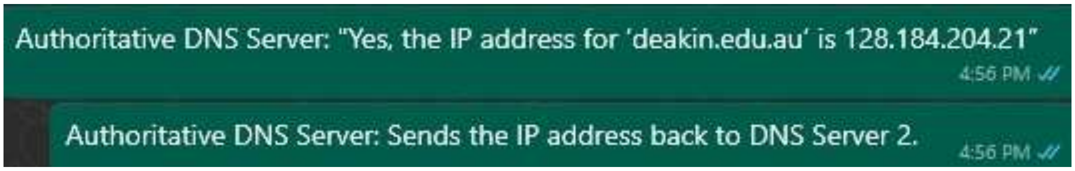
DNS Server 1: Forwards the query to DNS Server 2: “Hi DNS Server 2, do you know the IP address for ‘deakin.edu.au’?” 4:52 PM



Shekaina CICRA

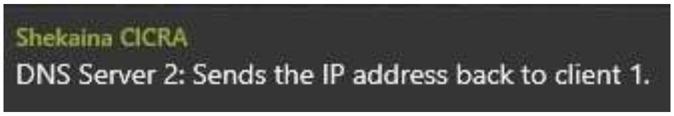
DNS Server 2: "I don't know either, but I'll forward the request to an authoritative DNS server." 4:53 PM

DNS Server 2: Forwards the query to the Authoritative DNS Server for deakin.edu.au: "Hi Authoritative DNS Server, do you have the IP address for 'deakin.edu.au'?" 4:55 PM



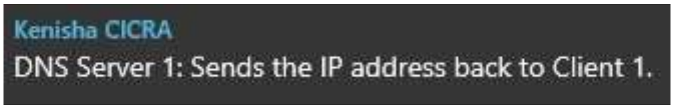
Authoritative DNS Server: "Yes, the IP address for 'deakin.edu.au' is 128.184.204.21” 4:56 PM

Authoritative DNS Server: Sends the IP address back to DNS Server 2. 4:56 PM



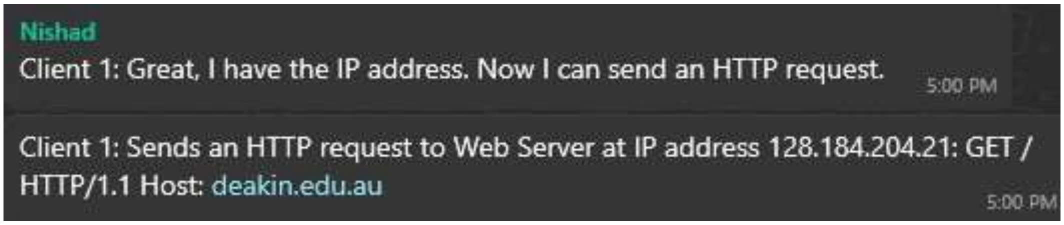
Shekaina CICRA

DNS Server 2: Sends the IP address back to client 1.



Kenisha CICRA

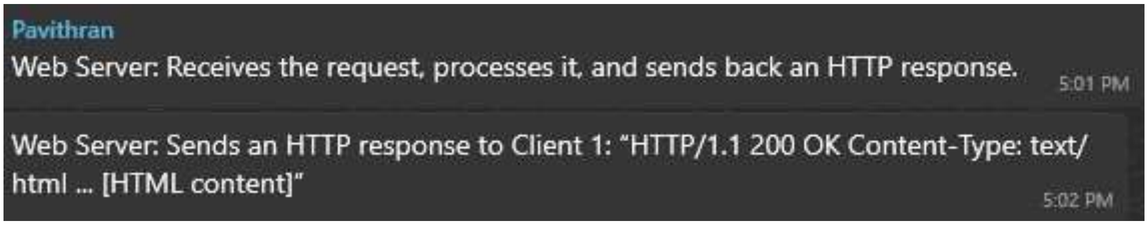
DNS Server 1: Sends the IP address back to Client 1.



Nishad

Client 1: Great, I have the IP address. Now I can send an HTTP request. 5:00 PM

Client 1: Sends an HTTP request to Web Server at IP address 128.184.204.21: GET / HTTP/1.1 Host: deakin.edu.au 5:00 PM

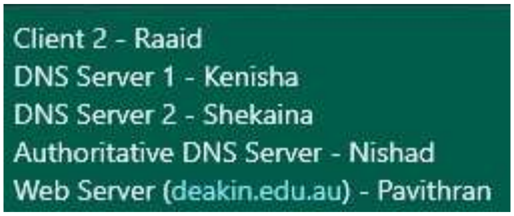


Pavithran

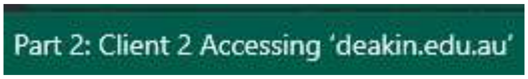
Web Server: Receives the request, processes it, and sends back an HTTP response. 5:01 PM

Web Server: Sends an HTTP response to Client 1: "HTTP/1.1 200 OK Content-Type: text/ html ... [HTML content]" 5:02 PM

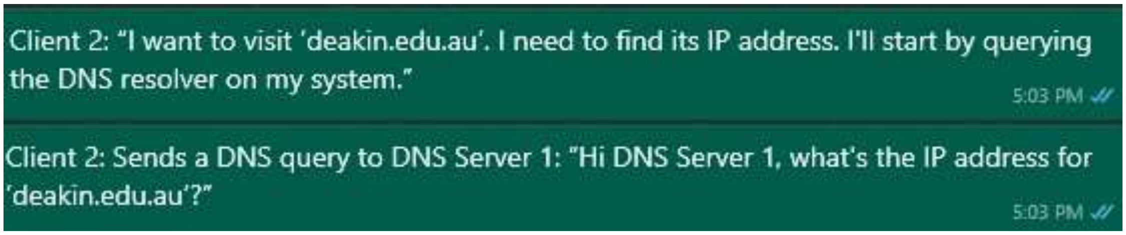
d. Now, after Client 1 accessed deakin.edu.au, Client 2 also needs to view deakin.edu.au. Discuss the steps involved in Client 2's web browser to be able to send a HTTP request message to the Web server.



Client 2 - Raaid
DNS Server 1 - Kenisha
DNS Server 2 - Shekaina
Authoritative DNS Server - Nishad
Web Server (deakin.edu.au) - Pavithran

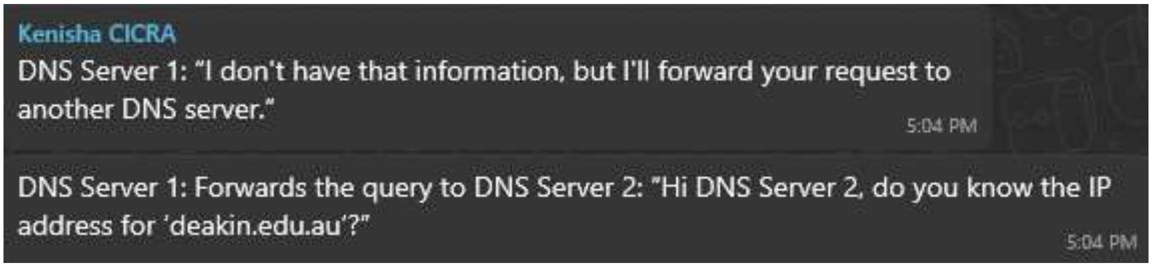


Part 2: Client 2 Accessing 'deakin.edu.au'



Client 2: "I want to visit 'deakin.edu.au'. I need to find its IP address. I'll start by querying the DNS resolver on my system." 5:03 PM

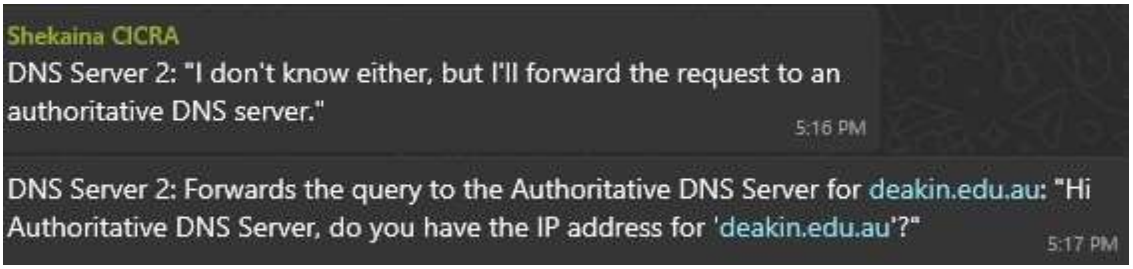
Client 2: Sends a DNS query to DNS Server 1: "Hi DNS Server 1, what's the IP address for 'deakin.edu.au'?" 5:03 PM



Kenisha CICRA

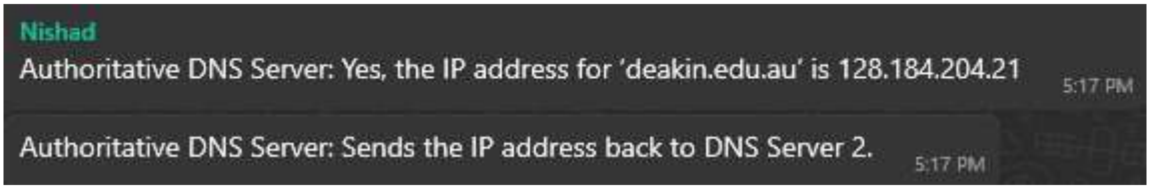
DNS Server 1: "I don't have that information, but I'll forward your request to another DNS server." 5:04 PM

DNS Server 1: Forwards the query to DNS Server 2: "Hi DNS Server 2, do you know the IP address for 'deakin.edu.au'?" 5:04 PM


Shekaina CICRA

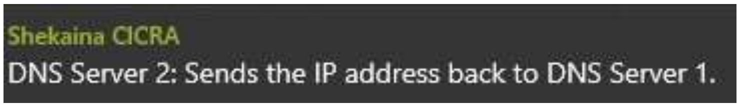
DNS Server 2: "I don't know either, but I'll forward the request to an authoritative DNS server." 5:16 PM

DNS Server 2: Forwards the query to the Authoritative DNS Server for deakin.edu.au: "Hi Authoritative DNS Server, do you have the IP address for 'deakin.edu.au'?" 5:17 PM

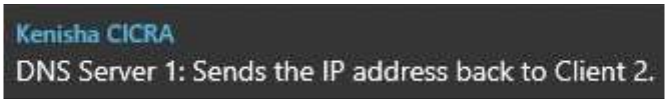

Nishad

Authoritative DNS Server: Yes, the IP address for 'deakin.edu.au' is 128.184.204.21 5:17 PM

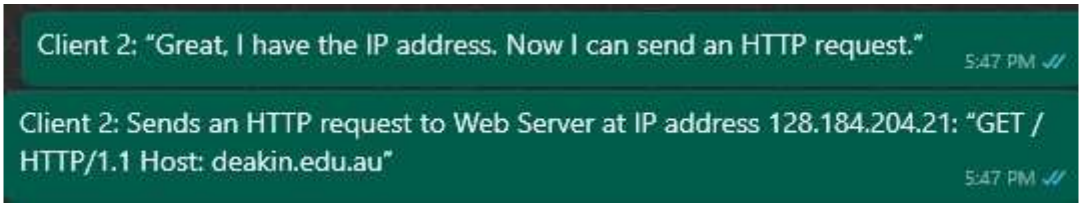
Authoritative DNS Server: Sends the IP address back to DNS Server 2. 5:17 PM


Shekaina CICRA

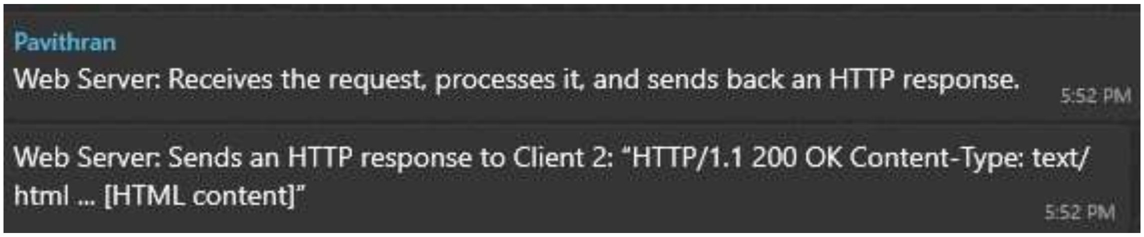
DNS Server 2: Sends the IP address back to DNS Server 1.


Kenisha CICRA

DNS Server 1: Sends the IP address back to Client 2.


Client 2: "Great, I have the IP address. Now I can send an HTTP request." 5:47 PM

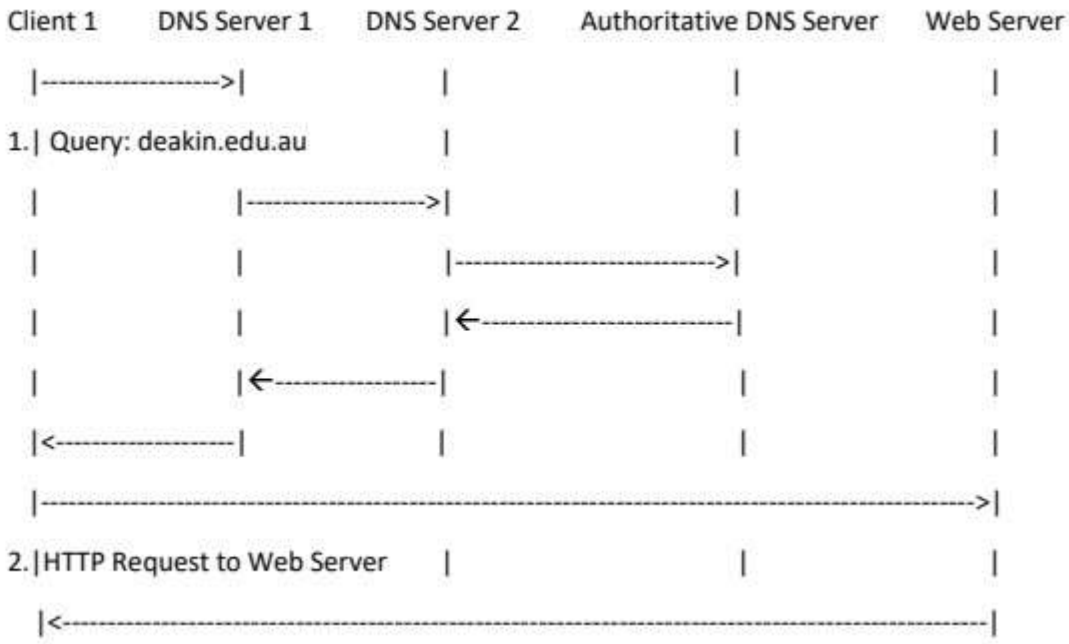
Client 2: Sends an HTTP request to Web Server at IP address 128.184.204.21: "GET / HTTP/1.1 Host: deakin.edu.au" 5:47 PM


Pavithran

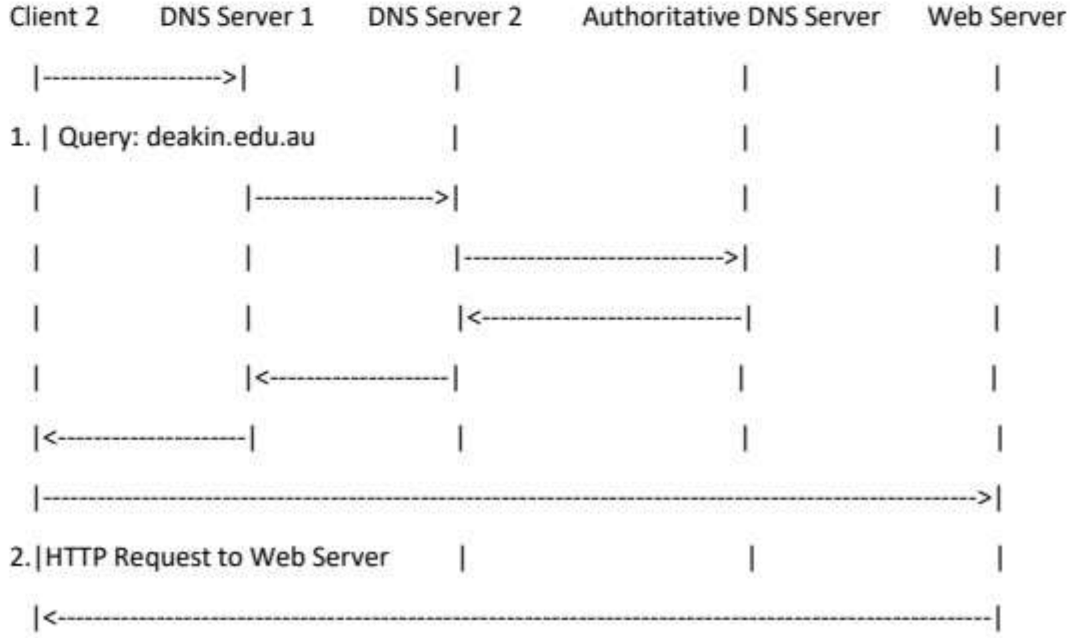
Web Server: Receives the request, processes it, and sends back an HTTP response. 5:52 PM

Web Server: Sends an HTTP response to Client 2: "HTTP/1.1 200 OK Content-Type: text/html ... [HTML content]" 5:52 PM

e. You can show all the steps in a timing diagram with the end systems and numbering the sequence of steps (similar to the activity you did in Active Class 1).



```
Client 1      DNS Server 1      DNS Server 2      Authoritative DNS Server      Web Server
  |------------------->|               |                     |                        |
1.| Query: deakin.edu.au               |                     |                        |
  |                    |------------------>|                 |                        |
  |                    |               |--------------------------->|                 |
  |                    |               |←---------------------------|                 |
  |                    |←-----------------|                  |                        |
  |<-------------------|               |                     |                        |
  |-------------------------------------------------------------------------------------->|
2.|HTTP Request to Web Server          |                     |                        |
  |<--------------------------------------------------------------------------------------|
```



```
Client 2      DNS Server 1      DNS Server 2      Authoritative DNS Server      Web Server
  |------------------->|               |                     |                        |
1. | Query: deakin.edu.au              |                     |                        |
  |                    |------------------>|                 |                        |
  |                    |               |--------------------------->|                 |
  |                    |               |<---------------------------|                 |
  |                    |<-------------------|                |                        |
  |<--------------------|              |                     |                        |
  |-------------------------------------------------------------------------------------->|
2.|HTTP Request to Web Server          |                     |                        |
  |<--------------------------------------------------------------------------------------|
```

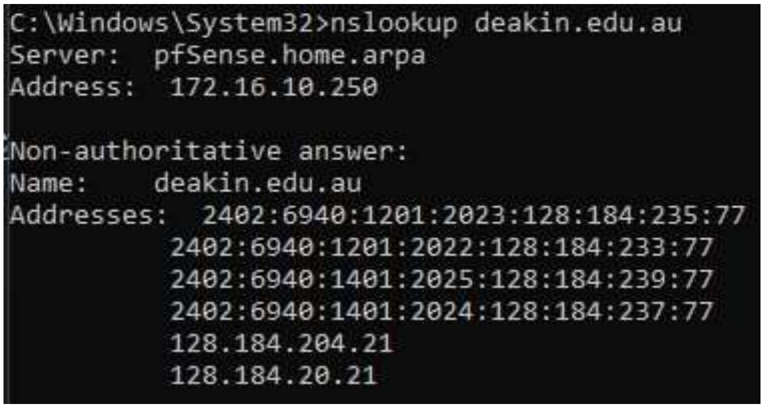
Activity 2

1. You can send a DNS query message directly to some DNS servers. For this, we use “nslookup”

2. First use “nslookup” in command prompt in Windows or terminal in MacOS to identify the IP address of a Web server deakin.edu.au (in Australia). Note down the webserver and the IP address of that server.

- Webserver: pfSense.home.arpa
  IP Address: 172.16.10.250 and 128.184.20.21

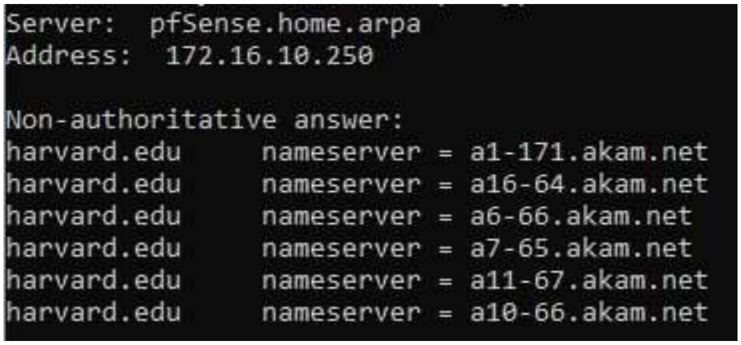
3. What are the answers you received from nslookup?



```
C:\Windows\System32>nslookup deakin.edu.au
Server:  pfSense.home.arpa
Address:  172.16.10.250

Non-authoritative answer:
Name:    deakin.edu.au
Addresses:  2402:6940:1201:2023:128:184:235:77
          2402:6940:1201:2022:128:184:233:77
          2402:6940:1401:2025:128:184:239:77
          2402:6940:1401:2024:128:184:237:77
          128.184.204.21
          128.184.20.21
```

4. What are the authoritative and non-authoritative answers?
   - An authoritative answer comes from a nameserver that is considered authoritative(main) for the domain where as a non-authoritative answer is when the answer is not fetched from the authoritative DNS sever.

5. Use nslookup to identify the authoritative DNS servers for a webserver of a university in USA.

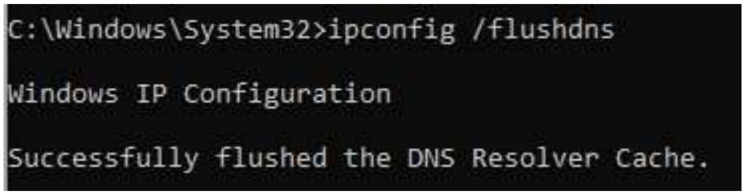


```
Server:  pfSense.home.arpa
Address:  172.16.10.250

Non-authoritative answer:
harvard.edu     nameserver = a1-171.akam.net
harvard.edu     nameserver = a16-64.akam.net
harvard.edu     nameserver = a6-66.akam.net
harvard.edu     nameserver = a7-65.akam.net
harvard.edu     nameserver = a11-67.akam.net
harvard.edu     nameserver = a10-66.akam.net
```

6. Compare the answers in 2 and 5.
   - The nslookup command provides the authoritave DNS servers for Harvard University’s domain whilst the nslookup command in question 2 provides both IPv6 and IPv4 addresses for Deakin University’s domain. So, whilst Harvard university provides the DNS servers that are authoritative for the ‘harvard.edu’ domain, Deakin Universities output displays the list of IP addresses that can be used to access the ‘deakin.edu.au’ web server.

7. Let’s trace DNS in Wireshark now. First,

a. Use ipconfig in your command prompt/ terminal to empty the DNS cache in your host ipconfig /flushdns. (MacOS Mojave use: sudo killall -HUP mDNSResponder)

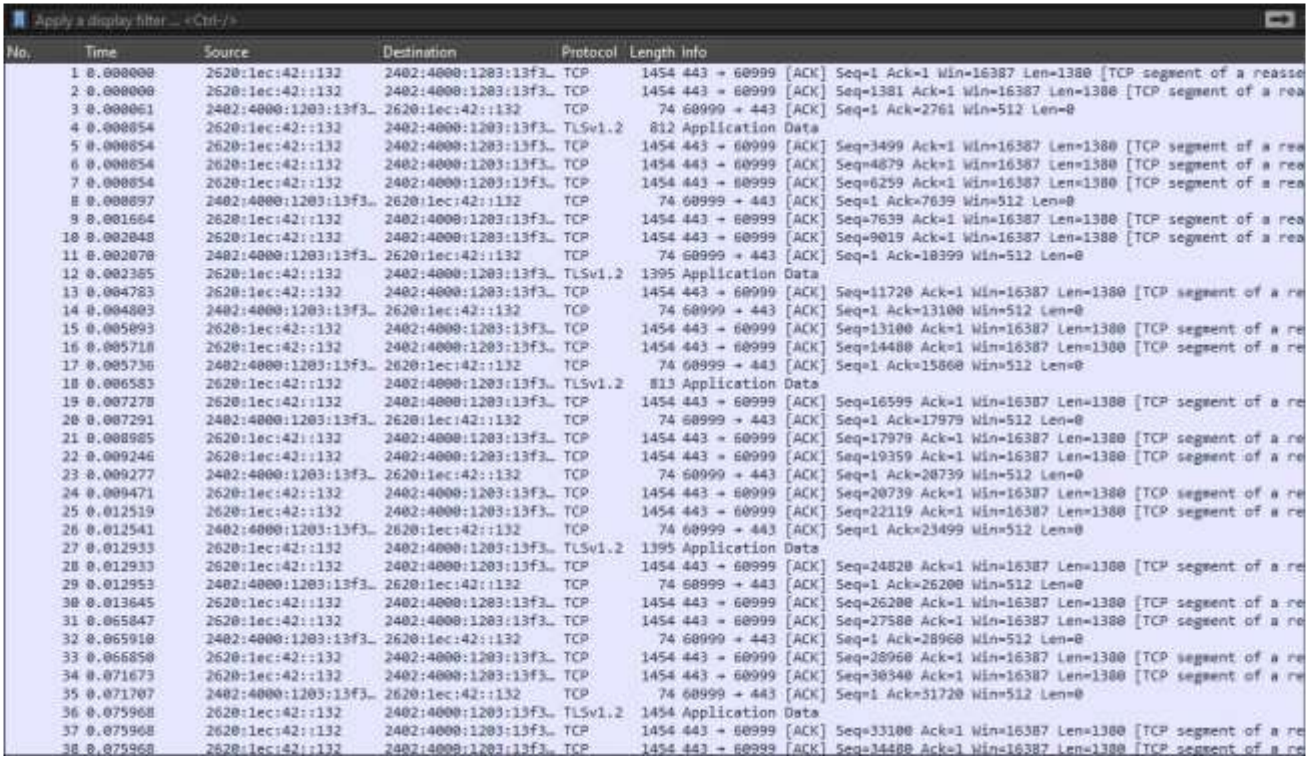


```
C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

b. Open google chrome and empty your browser cache.

Browser cache emptied.

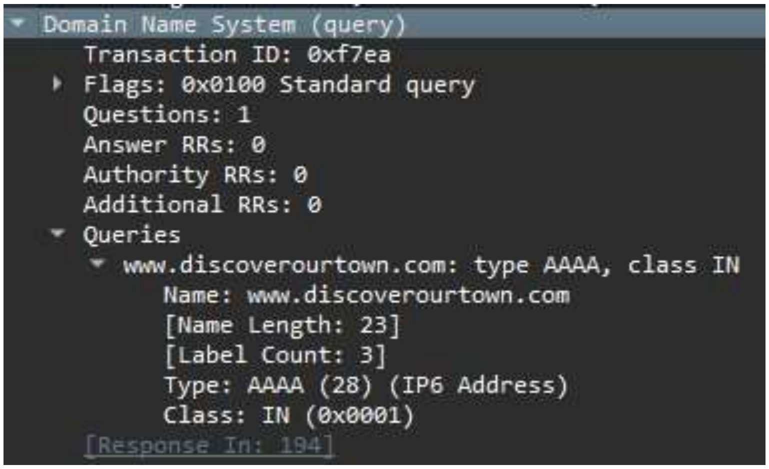
c. Open Wireshark and start packet capture. Then, visit the Web page: http://www.discoverourtown.com in your browser and stop packet capture.



```
No.  Time       Source                Destination           Protocol Length Info
   1 0.000000   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=1 Ack=1 Win=16387 Len=1380 [TCP segment of a reasse
   2 0.000000   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=1381 Ack=1 Win=16387 Len=1380 [TCP segment of a rea
   3 0.000061   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=2761 Win=512 Len=0
   4 0.000854   2620:1ec:42::132      2402:4000:1203:13f3…  TLSv1.2   812 Application Data
   5 0.000854   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=3499 Ack=1 Win=16387 Len=1380 [TCP segment of a rea
   6 0.000854   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=4879 Ack=1 Win=16387 Len=1380 [TCP segment of a rea
   7 0.000854   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=6259 Ack=1 Win=16387 Len=1380 [TCP segment of a rea
   8 0.000897   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=7639 Win=512 Len=0
   9 0.001664   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=7639 Ack=1 Win=16387 Len=1380 [TCP segment of a rea
  10 0.002048   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=9019 Ack=1 Win=16387 Len=1380 [TCP segment of a rea
  11 0.002070   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=10399 Win=512 Len=0
  12 0.002385   2620:1ec:42::132      2402:4000:1203:13f3…  TLSv1.2  1395 Application Data
  13 0.004783   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=11720 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  14 0.004803   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=13100 Win=512 Len=0
  15 0.005093   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=13100 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  16 0.005718   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=14480 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  17 0.005736   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=15860 Win=512 Len=0
  18 0.006583   2620:1ec:42::132      2402:4000:1203:13f3…  TLSv1.2   813 Application Data
  19 0.007278   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=16599 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  20 0.007291   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=17979 Win=512 Len=0
  21 0.008985   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=17979 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  22 0.009246   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=19359 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  23 0.009277   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=20739 Win=512 Len=0
  24 0.009471   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=20739 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  25 0.012519   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=22119 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  26 0.012541   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=23499 Win=512 Len=0
  27 0.012933   2620:1ec:42::132      2402:4000:1203:13f3…  TLSv1.2  1395 Application Data
  28 0.012933   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=24820 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  29 0.012953   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=26200 Win=512 Len=0
  30 0.013645   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=26200 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  31 0.065847   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=27580 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  32 0.065910   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=28960 Win=512 Len=0
  33 0.066850   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=28960 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  34 0.071673   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=30340 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  35 0.071707   2402:4000:1203:13f3…  2620:1ec:42::132      TCP        74 60999 → 443 [ACK] Seq=1 Ack=31720 Win=512 Len=0
  36 0.075968   2620:1ec:42::132      2402:4000:1203:13f3…  TLSv1.2  1454 Application Data
  37 0.075968   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=33100 Ack=1 Win=16387 Len=1380 [TCP segment of a re
  38 0.075968   2620:1ec:42::132      2402:4000:1203:13f3…  TCP      1454 443 → 60999 [ACK] Seq=34480 Ack=1 Win=16387 Len=1380 [TCP segment of a re
```

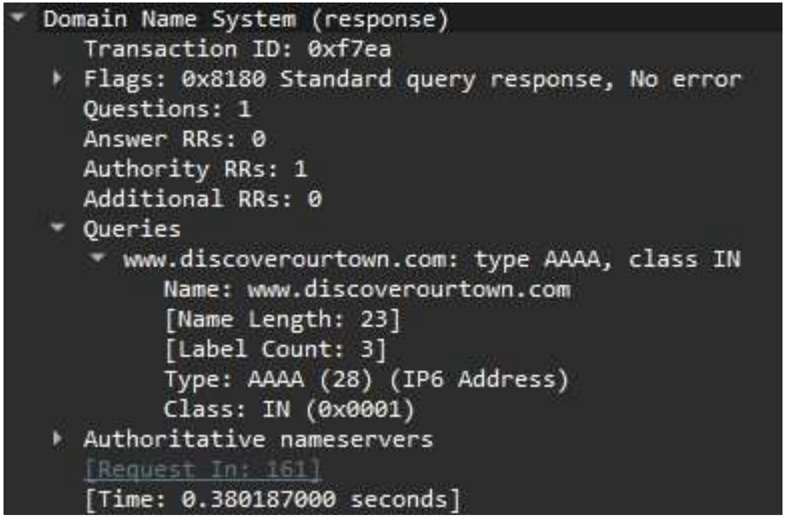
8. Now you are ready to analyze what you captured in Wireshark and explore more about DNS. Use the following questions as a guide for your analysis.

   a. Find the DNS query and response messages. Which transport layer protocol they have used? UDP or TCP?



```
Domain Name System (query)
    Transaction ID: 0xf7ea
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.discoverourtown.com: type AAAA, class IN
        Name: www.discoverourtown.com
        [Name Length: 23]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
    [Response In: 194]
```

DNS Query



```
Domain Name System (response)
    Transaction ID: 0xf7ea
  Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  Queries
    www.discoverourtown.com: type AAAA, class IN
        Name: www.discoverourtown.com
        [Name Length: 23]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  Authoritative nameservers
    [Request In: 161]
    [Time: 0.380187000 seconds]
```

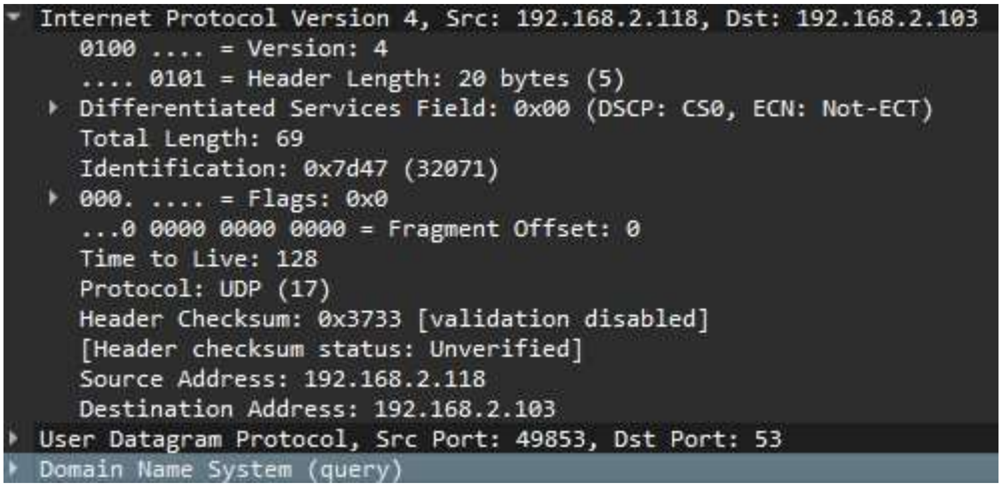
DNS Response

They both use UDP.

b. What are the destination port of the DNS query message and the source port of DNS response message?

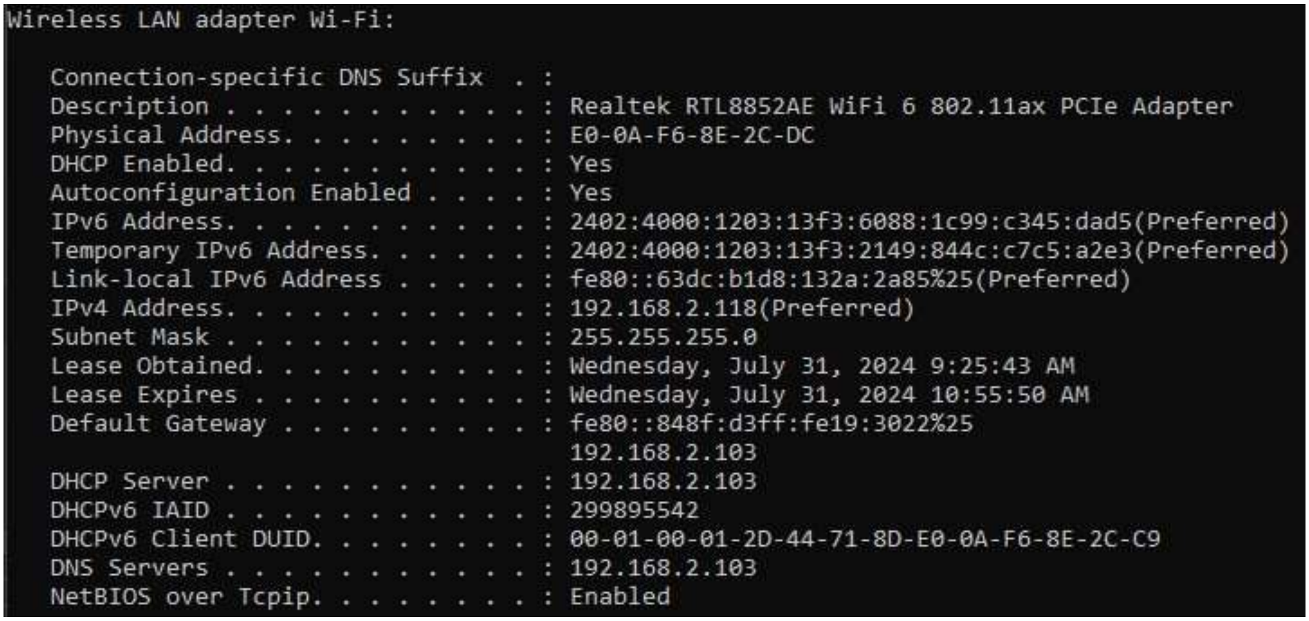
The destination port of query port and and source port of response messages are both 53 because DNS queries are sent through UDP port number 53.

c. What is the IP address that the DNS query message was sent?



```
▾ Internet Protocol Version 4, Src: 192.168.2.118, Dst: 192.168.2.103
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 69
     Identification: 0x7d47 (32071)
   ▸ 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 128
     Protocol: UDP (17)
     Header Checksum: 0x3733 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.2.118
     Destination Address: 192.168.2.103
▸ User Datagram Protocol, Src Port: 49853, Dst Port: 53
▸ Domain Name System (query)
```

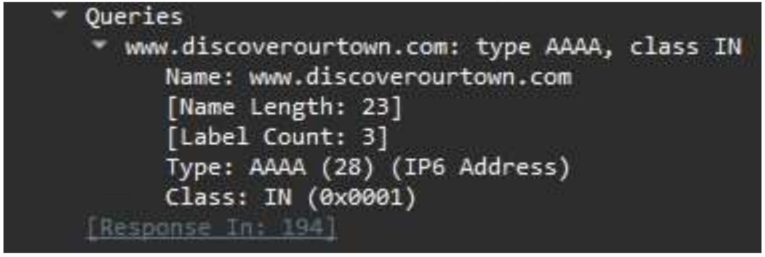
d. Identify the IP address of your local DNS server using the terminal/command prompt. Are these two IP addresses identified in c and d the same?



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
   Physical Address. . . . . . . . . : E0-0A-F6-8E-2C-DC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2402:4000:1203:13f3:6088:1c99:c345:dad5(Preferred)
   Temporary IPv6 Address. . . . . . : 2402:4000:1203:13f3:2149:844c:c7c5:a2e3(Preferred)
   Link-local IPv6 Address . . . . . : fe80::63dc:b1d8:132a:2a85%25(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.118(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 31, 2024 9:25:43 AM
   Lease Expires . . . . . . . . . . : Wednesday, July 31, 2024 10:55:50 AM
   Default Gateway . . . . . . . . . : fe80::848f:d3ff:fe19:3022%25
                                       192.168.2.103
   DHCP Server . . . . . . . . . . . : 192.168.2.103
   DHCPv6 IAID . . . . . . . . . . . : 299895542
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-44-71-8D-E0-0A-F6-8E-2C-C9
   DNS Servers . . . . . . . . . . . : 192.168.2.103
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

They have the same IP address

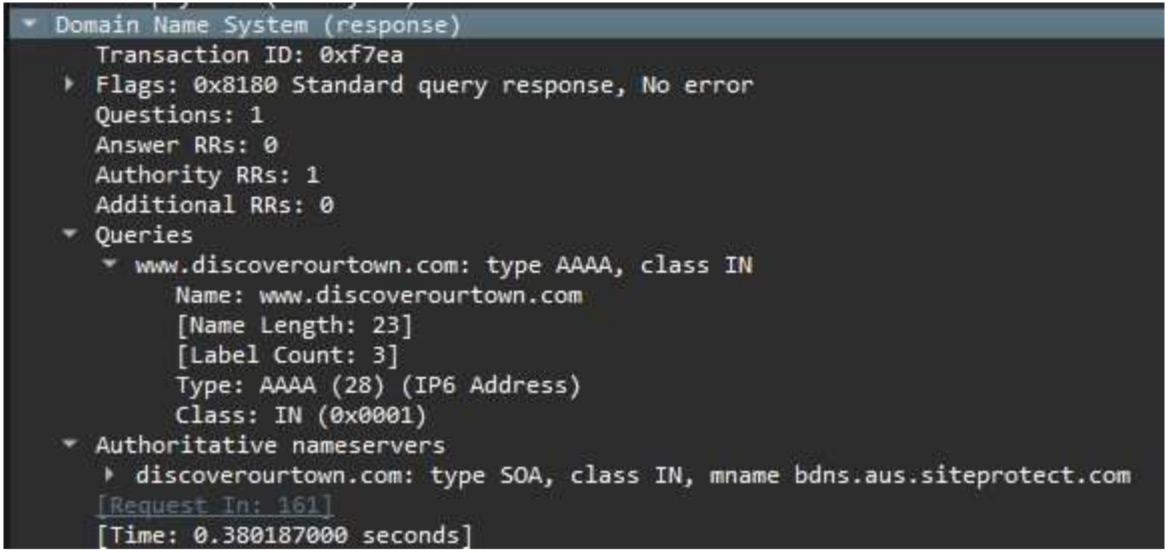
e. You can further explore the DNS query message. Can you identify the "Type" of DNS query? What does the query message contain?



```
▾ Queries
   ▾ www.discoverourtown.com: type AAAA, class IN
        Name: www.discoverourtown.com
        [Name Length: 23]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  [Response In: 194]
```

The DNS query message can be seen above and its type is AAAA

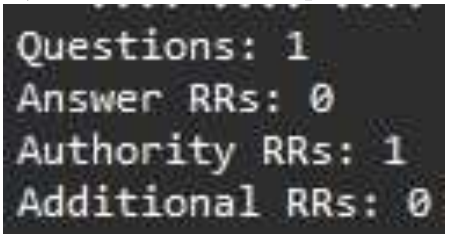
f. You can further explore the DNS response message. Can you identify the “Type” of DNS response?



```
▾ Domain Name System (response)
    Transaction ID: 0xf7ea
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  ▾ Queries
    ▾ www.discoverourtown.com: type AAAA, class IN
        Name: www.discoverourtown.com
        [Name Length: 23]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▾ Authoritative nameservers
    ▸ discoverourtown.com: type SOA, class IN, mname bdns.aus.siteprotect.com
    [Request In: 161]
    [Time: 0.380187000 seconds]
```

The DNS response message can be seen above and its type is AAAA

g. Are there any “answers” in the response message? If so, what are these answers?



```
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
```

As you can see there are no answers in the response message.

h. The web page that you have accessed contains a couple of images. Does the host request new DNS queries to access each image? Explain your answer.

The host does not need to necessarily request new DNS queries for images that are located in the same domain as is the case for this webpage.

Above and Beyond Tasks

- Explain E-mail (another popular application) o What is the principal application layer protocol used in e-mails?
    - ▪ The protocol followed in application layer for emails is Simple Mail Transfer Protocol (SMTP)

- o What is the underlaying architecture and transport layer protocol used in e-mail application layer protocol?
    - ✦ The underlying architecture of the SMTP protocol is the Client – Server model, where Email clients communicate with email servers to send, receive and store emails. The Transport Layer protocol used in this instance is TCP

- o Can you list down the basic steps involve in sending an e-mail from user A to B?
    - ✦ User A – Writes an email using an email client
    - ✦ The email client sends the email to the user's email server (SMTP server) using SMTP.
    - ✦ The email client establishes a connection with the SMTP server on port 25 and then the SMTP server authenticates User A after conluding the SMTP Handshake.
    - ✦ The SMTP server checks the domain of User B's email address so if User B's domain is different from User A's, the SMTP server looks up the destination domains Mail exchange record using DNS to find the receiver's mail server.
    - ✦ The SMTP server sends the email to User B's mail server.
    - ✦ User B's mail server receives and stores the email in User B's mailbox.
    - ✦ User B opens their email client, which connects to the mail server using either POP3 or IMAP (where the email is retrieved and stored).
    - ✦ User B reads the email.