Amrita Viswa Vidyapeetham
Amrita School of Engineering
Dept of Computer Science & Engineering
Computer Networks Lab

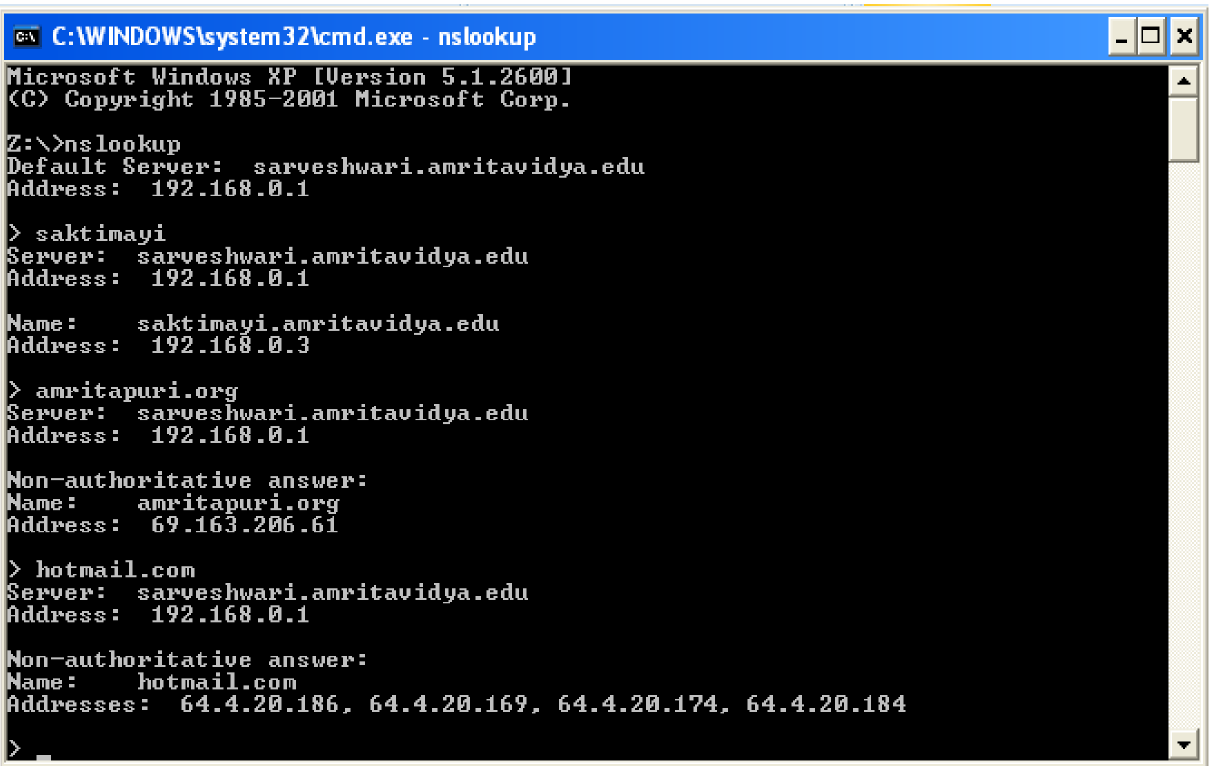
LabSheet3 - Understand how DNS works using the Wireshark

Name: Vinayak V Thayil
Roll No: AM.EN.U4CSE21161

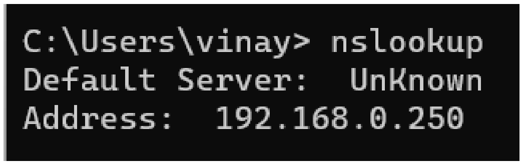
1. nslookup

In this lab, we'll make extensive use of the *nslookup* tool, which is available in most Linux/Unix and Microsoft platforms today. To run *nslookup* in Linux/Unix, you just type the *nslookup* command on the command line. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.

- In it is most basic operation, *nslookup* tool allows the host running the tool to query 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 (see the textbook for definitions of these terms).
- To accomplish this task, *nslookup* sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\>nslookup
Default Server:  sarveshwari.amritavidya.edu
Address:  192.168.0.1

> saktimayi
Server:  sarveshwari.amritavidya.edu
Address:  192.168.0.1

Name:    saktimayi.amritavidya.edu
Address:  192.168.0.3

> amritapuri.org
Server:  sarveshwari.amritavidya.edu
Address:  192.168.0.1

Non-authoritative answer:
Name:    amritapuri.org
Address:  69.163.206.61

> hotmail.com
Server:  sarveshwari.amritavidya.edu
Address:  192.168.0.1

Non-authoritative answer:
Name:    hotmail.com
Addresses:  64.4.20.186, 64.4.20.169, 64.4.20.174, 64.4.20.184

> _
```



```
C:\Users\vinay> nslookup
Default Server:  UnKnown
Address:  192.168.0.250
```

2. ipconfig

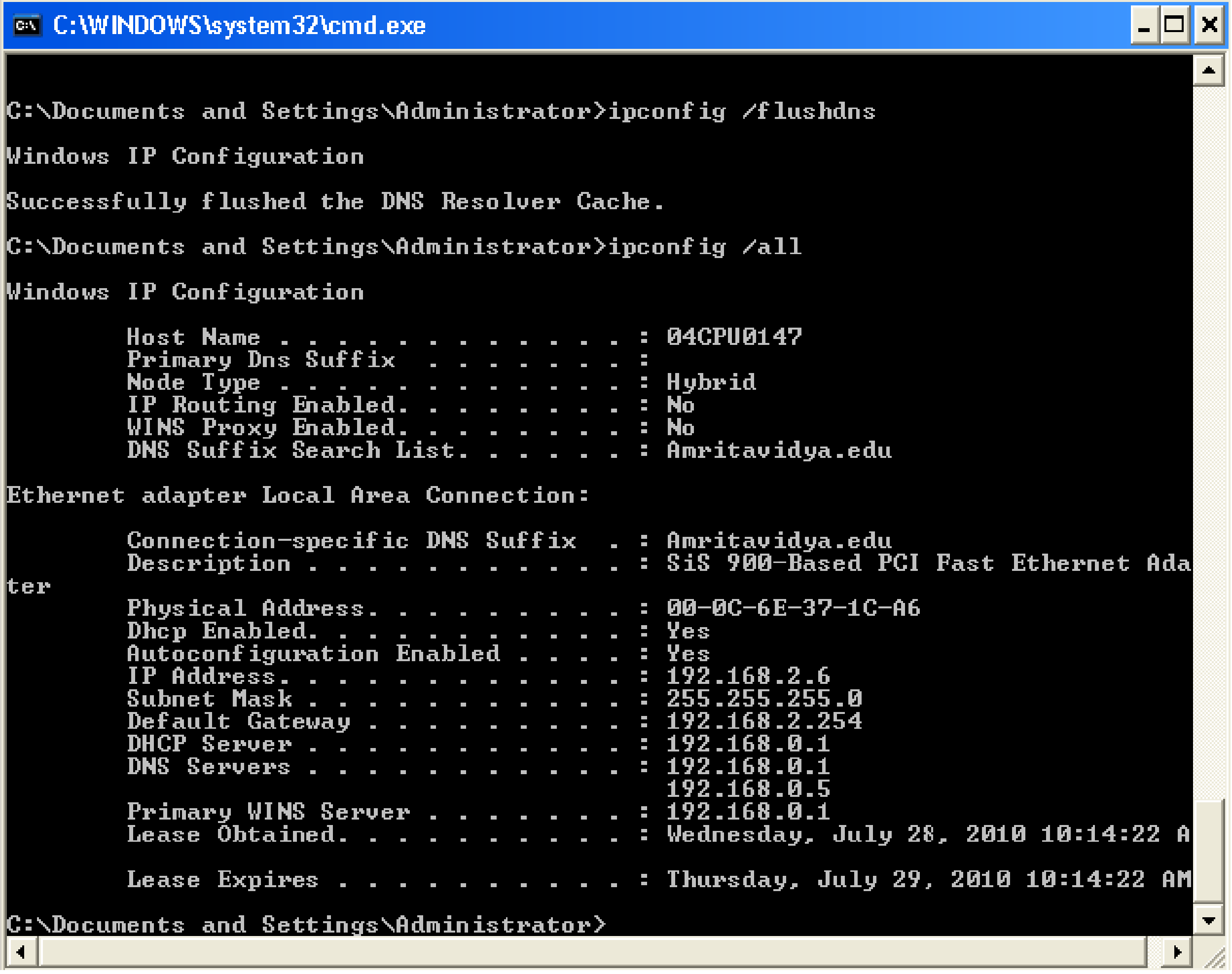
ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues.
Here we'll only describe ipconfig, although the Linux/Unix ifconfig is very similar.

LabSheet3 - Understand how DNS works using the Wireshark

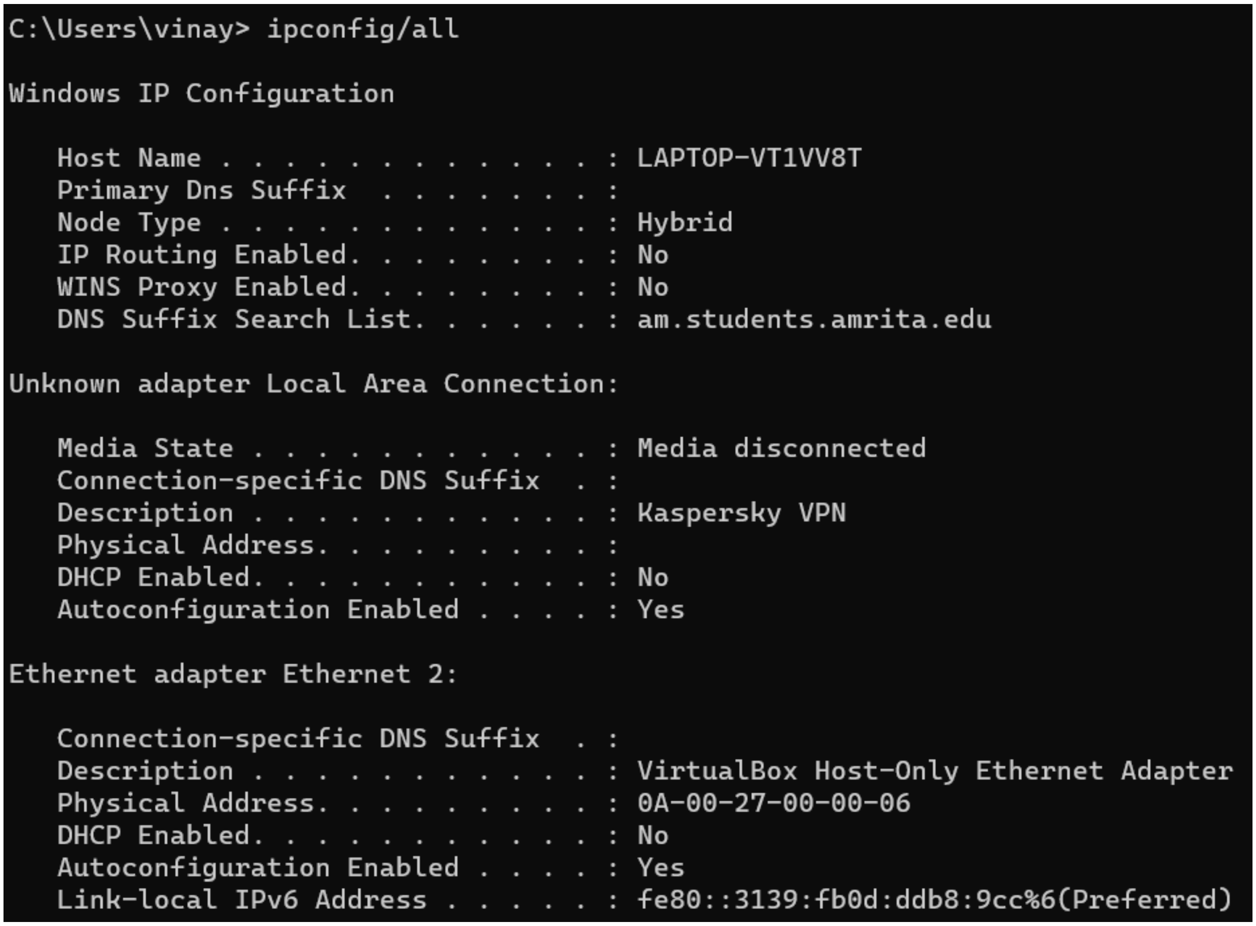
ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you want to see all this information about your host, simply enter:

```
ipconfig /all
```

into the Command Prompt, as shown in the following screenshot.



```
C:\Documents and Settings\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : 04CPU0147
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : Amritavidya.edu

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : Amritavidya.edu
        Description . . . . . . . . . . . : SiS 900-Based PCI Fast Ethernet Ada
pter
        Physical Address. . . . . . . . . : 00-0C-6E-37-1C-A6
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.2.6
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.254
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 192.168.0.1
                                            192.168.0.5
        Primary WINS Server . . . . . . . : 192.168.0.1
        Lease Obtained. . . . . . . . . . : Wednesday, July 28, 2010 10:14:22 A

        Lease Expires . . . . . . . . . . : Thursday, July 29, 2010 10:14:22 AM

C:\Documents and Settings\Administrator>
```



```
C:\Users\vinay> ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-VT1VV8T
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : am.students.amrita.edu

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Kaspersky VPN
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-06
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::3139:fb0d:ddb8:9cc%6(Preferred)
```

- *ipconfig* is also very useful for managing the DNS information stored in your host.
- We have learned that a host can cache DNS records it recently obtained.
- To see these cached records, after the prompt provide the following command: **ipconfig /displaydns**

Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter

ipconfig /flushdns

Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

3. Tracing DNS with Wireshark

Now that we are familiar with nslookup and ipconfig, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web surfing activity.

• Use ipconfig to empty the DNS cache in your host.

• Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)

• Open Wireshark and enter "ip.addr == your_IP_address" into the filter, where you obtain your_IP_address (the IP address for the computer on which you are running Wireshark) with ipconfig. This filter removes all packets that neither originate nor are destined to your host.

• With your browser, visit Web pages in internet.
• Stop packet capture.

1. Explain the working of the DNS protocol[DNS Request Query and DNS Response message] briefly with typed answers and answer highlighted screenshots for the above capture

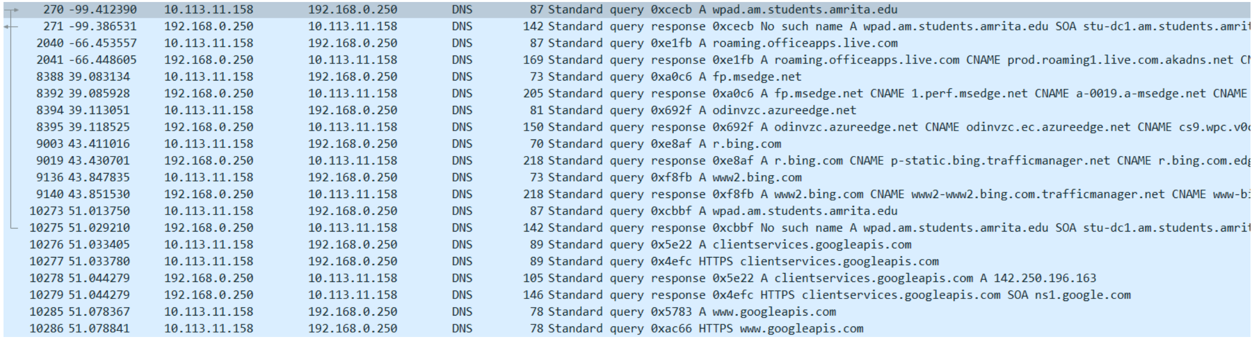
Amrita Viswa Vidyapeetham
Amrita School of Engineering
Dept of Computer Science & Engineering
Computer Networks Lab

LabSheet3 - Understand how DNS works using the Wireshark

DNS is a protocol used for translating domain names into IP addresses.
Working Explained in the following steps:

a. A client sends a DNS query to the local DNS resolver.
b. The local DNS resolver checks its cache to see if it has the requested information. If the information is present, it returns the IP address to the client.
c. If the information is not present in the cache, the resolver forwards the query to the root DNS server.
d. The root DNS server responds with the IP address of the top-level domain server responsible for the requested domain.
e. The resolver then sends a query to the top-level domain server.
f. The top-level domain server responds with the IP address of the authoritative name server responsible for the requested domain.

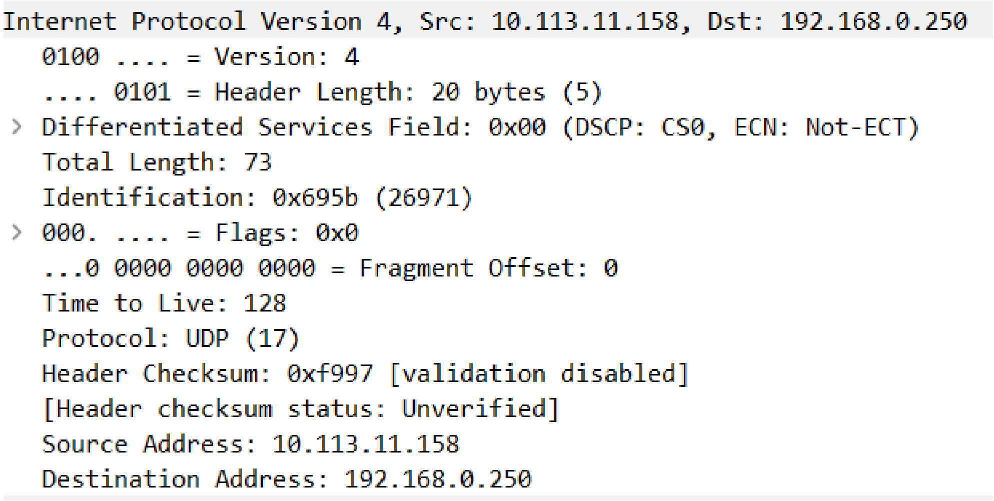
a. Locate the DNS query and response messages. Are they sent over UDP or TCP?



```
  270 -99.412390  10.113.11.158  192.168.0.250  DNS   87 Standard query 0xcecb A wpad.am.students.amrita.edu
  271 -99.386531  192.168.0.250  10.113.11.158  DNS  142 Standard query response 0xcecb No such name A wpad.am.students.amrita.edu SOA stu-dc1.am.students.amri
 2040 -66.453557  10.113.11.158  192.168.0.250  DNS   87 Standard query 0xe1fb A roaming.officeapps.live.com
 2041 -66.448605  192.168.0.250  10.113.11.158  DNS  169 Standard query response 0xe1fb A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net C
 8388 39.083134   10.113.11.158  192.168.0.250  DNS   73 Standard query 0xa0c6 A fp.msedge.net
 8392 39.085928   192.168.0.250  10.113.11.158  DNS  205 Standard query response 0xa0c6 A fp.msedge.net CNAME 1.perf.msedge.net CNAME a-0019.a-msedge.net CNAME
 8394 39.113051   10.113.11.158  192.168.0.250  DNS   81 Standard query 0x692f A odinvzc.azureedge.net
 8395 39.118525   192.168.0.250  10.113.11.158  DNS  150 Standard query response 0x692f A odinvzc.azureedge.net CNAME odinvzc.ec.azureedge.net CNAME cs9.wpc.v0
 9003 43.411016   10.113.11.158  192.168.0.250  DNS   70 Standard query 0xe8af A r.bing.com
 9019 43.430701   192.168.0.250  10.113.11.158  DNS  218 Standard query response 0xe8af A r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.ed
 9136 43.847835   10.113.11.158  192.168.0.250  DNS   73 Standard query 0xf8fb A www2.bing.com
 9140 43.851530   192.168.0.250  10.113.11.158  DNS  218 Standard query response 0xf8fb A www2.bing.com CNAME www2-www2.bing.com.trafficmanager.net CNAME www-b
10273 51.013750   10.113.11.158  192.168.0.250  DNS   87 Standard query 0xcbbf A wpad.am.students.amrita.edu
10275 51.029210   192.168.0.250  10.113.11.158  DNS  142 Standard query response 0xcbbf No such name A wpad.am.students.amrita.edu SOA stu-dc1.am.students.amri
10276 51.033405   10.113.11.158  192.168.0.250  DNS   89 Standard query 0x5e22 A clientservices.googleapis.com
10277 51.033780   10.113.11.158  192.168.0.250  DNS   89 Standard query 0x4efc HTTPS clientservices.googleapis.com
10278 51.044279   192.168.0.250  10.113.11.158  DNS  105 Standard query response 0x5e22 A clientservices.googleapis.com A 142.250.196.163
10279 51.044279   192.168.0.250  10.113.11.158  DNS  146 Standard query response 0x4efc HTTPS clientservices.googleapis.com SOA ns1.google.com
10285 51.078367   10.113.11.158  192.168.0.250  DNS   78 Standard query 0x5783 A www.googleapis.com
10286 51.078841   10.113.11.158  192.168.0.250  DNS   78 Standard query 0xac66 HTTPS www.googleapis.com
```

LabSheet3 - Understand how DNS works using the Wireshark

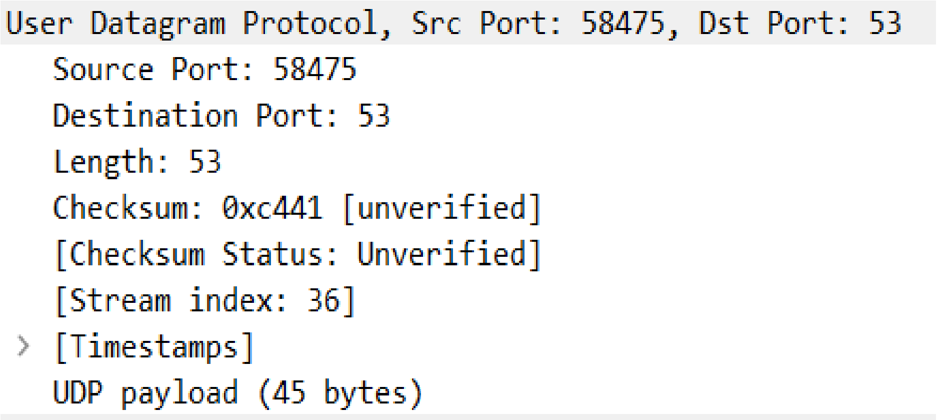
UDP Sent



```
Internet Protocol Version 4, Src: 10.113.11.158, Dst: 192.168.0.250
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 73
   Identification: 0x695b (26971)
 > 000. .... = Flags: 0x0
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: UDP (17)
   Header Checksum: 0xf997 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 10.113.11.158
   Destination Address: 192.168.0.250
```

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

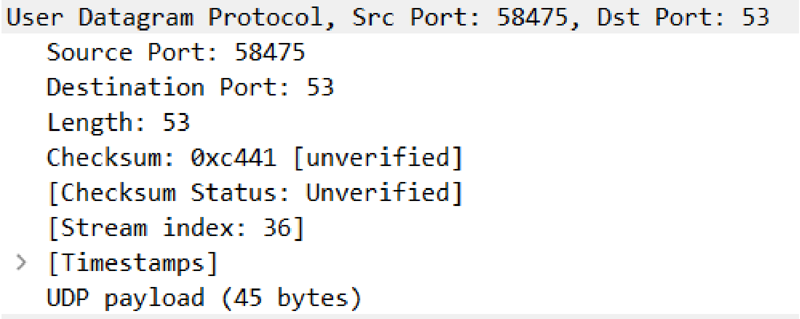
Source port of DNS response message is 53



```
User Datagram Protocol, Src Port: 58475, Dst Port: 53
   Source Port: 58475
   Destination Port: 53
   Length: 53
   Checksum: 0xc441 [unverified]
   [Checksum Status: Unverified]
   [Stream index: 36]
 > [Timestamps]
   UDP payload (45 bytes)
```

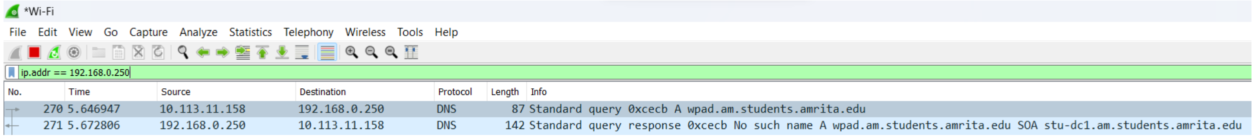
LabSheet3 - Understand how DNS works using the Wireshark

Source port of DNS response message is 53



```
User Datagram Protocol, Src Port: 58475, Dst Port: 53
    Source Port: 58475
    Destination Port: 53
    Length: 53
    Checksum: 0xc441 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 36]
  > [Timestamps]
    UDP payload (45 bytes)
```

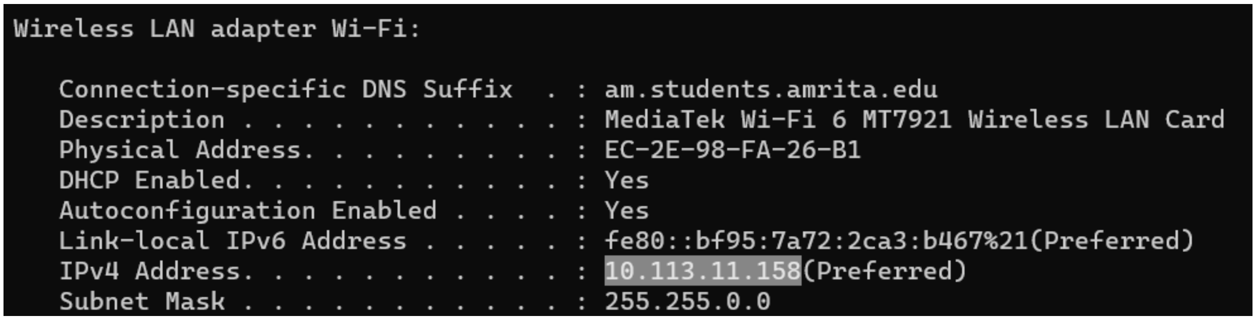
c. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.250

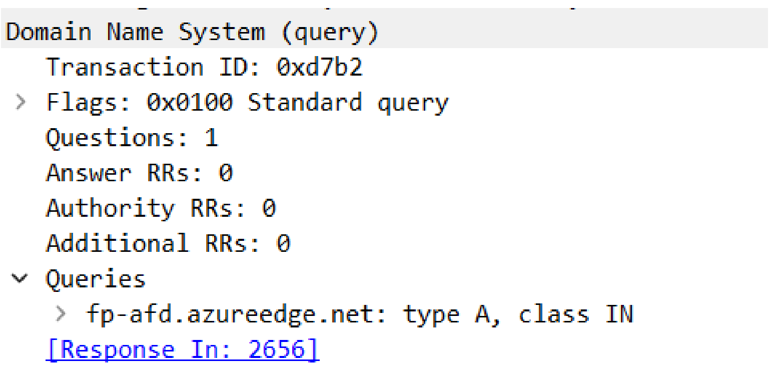
```
No.   Time      Source          Destination     Protocol  Length  Info
  270 5.646947  10.113.11.158   192.168.0.250   DNS           87  Standard query 0xcecb A wpad.am.students.amrita.edu
  271 5.672806  192.168.0.250   10.113.11.158   DNS          142  Standard query response 0xcecb No such name A wpad.am.students.amrita.edu SOA stu-dc1.am.students.amrita.edu
```



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : am.students.amrita.edu
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Physical Address. . . . . . . . . : EC-2E-98-FA-26-B1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::bf95:7a72:2ca3:b467%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.113.11.158(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
```

Both IP addresses are same.

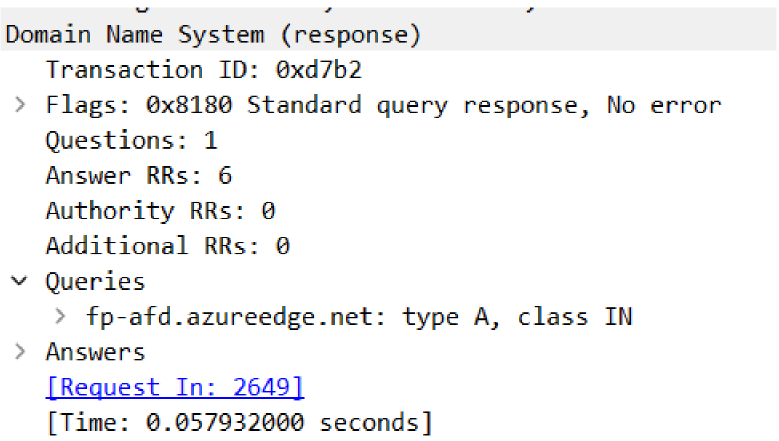
d. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
Domain Name System (query)
   Transaction ID: 0xd7b2
 > Flags: 0x0100 Standard query
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 v Queries
    > fp-afd.azureedge.net: type A, class IN
   [Response In: 2656]
```

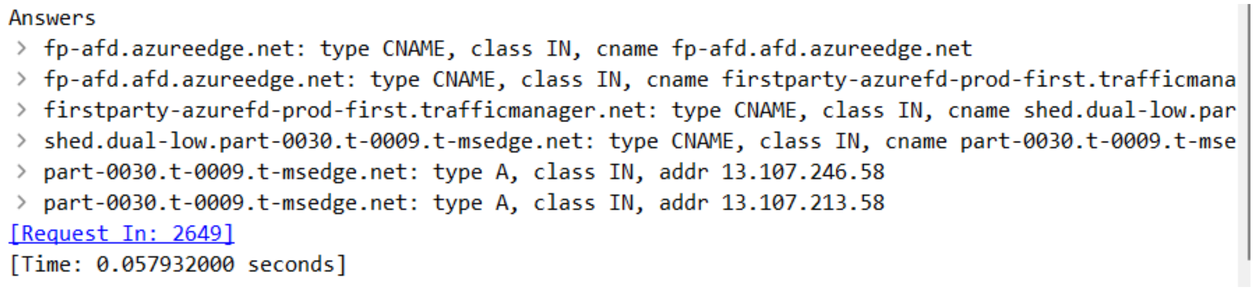
“Type” of DNS query is A.
NO. query message does not contain any “answers”

e. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?



```
Domain Name System (response)
   Transaction ID: 0xd7b2
 > Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 6
   Authority RRs: 0
   Additional RRs: 0
 v Queries
    > fp-afd.azureedge.net: type A, class IN
 > Answers
   [Request In: 2649]
   [Time: 0.057932000 seconds]
```

6 Answers



```
Answers
 > fp-afd.azureedge.net: type CNAME, class IN, cname fp-afd.afd.azureedge.net
 > fp-afd.afd.azureedge.net: type CNAME, class IN, cname firstparty-azurefd-prod-first.trafficmana
 > firstparty-azurefd-prod-first.trafficmanager.net: type CNAME, class IN, cname shed.dual-low.par
 > shed.dual-low.part-0030.t-0009.t-msedge.net: type CNAME, class IN, cname part-0030.t-0009.t-mse
 > part-0030.t-0009.t-msedge.net: type A, class IN, addr 13.107.246.58
 > part-0030.t-0009.t-msedge.net: type A, class IN, addr 13.107.213.58
[Request In: 2649]
[Time: 0.057932000 seconds]
```

f. Before retrieving each image/object in your web page, does your host issue new DNS queries?

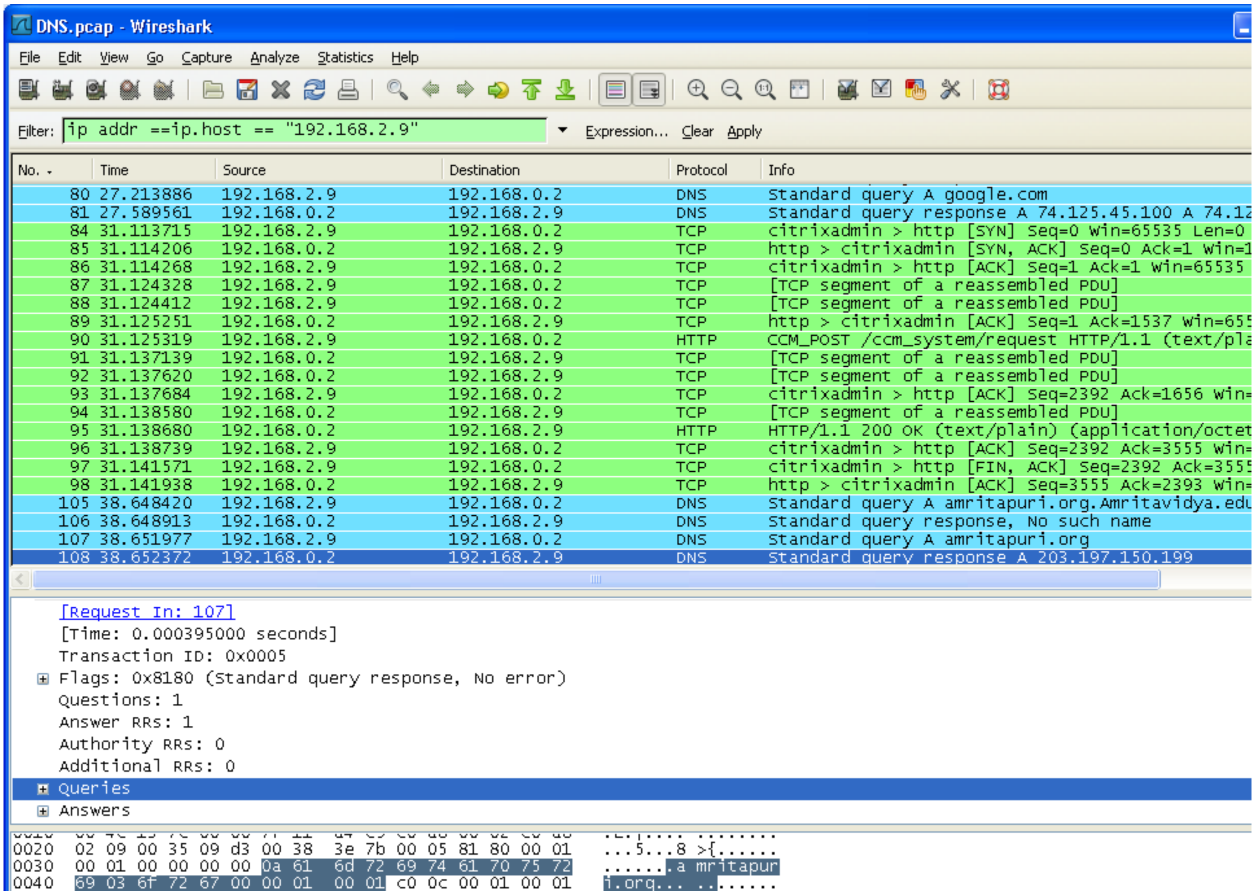
   When a user visits a web page, their browser typically caches the DNS responses for a period of time therefore subsequent requests for resources from the same domain, including images and other objects, will not require a new DNS query as long as the cached record is still valid.

2. Now let’s play with nslookup.

- Start packet capture.
- Do an nslookup on amritapuri.org, google.com etc.
- Stop packet capture.

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

LabSheet3 - Understand how DNS works using the Wireshark



Filter: ip addr ==ip.host == "192.168.2.9"

```
No. .   Time        Source          Destination     Protocol  Info
     80 27.213886   192.168.2.9     192.168.0.2     DNS       Standard query A google.com
     81 27.589561   192.168.0.2     192.168.2.9     DNS       Standard query response A 74.125.45.100 A 74.12
     84 31.113715   192.168.2.9     192.168.0.2     TCP       citrixadmin > http [SYN] Seq=0 Win=65535 Len=0
     85 31.114206   192.168.0.2     192.168.2.9     TCP       http > citrixadmin [SYN, ACK] Seq=0 Ack=1 Win=1
     86 31.114268   192.168.2.9     192.168.0.2     TCP       citrixadmin > http [ACK] Seq=1 Ack=1 Win=65535
     87 31.124328   192.168.2.9     192.168.0.2     TCP       [TCP segment of a reassembled PDU]
     88 31.124412   192.168.2.9     192.168.0.2     TCP       [TCP segment of a reassembled PDU]
     89 31.125251   192.168.0.2     192.168.2.9     TCP       http > citrixadmin [ACK] Seq=1 Ack=1537 Win=655
     90 31.125319   192.168.2.9     192.168.0.2     HTTP      CCM_POST /ccm_system/request HTTP/1.1 (text/pla
     91 31.137139   192.168.0.2     192.168.2.9     TCP       [TCP segment of a reassembled PDU]
     92 31.137620   192.168.0.2     192.168.2.9     TCP       [TCP segment of a reassembled PDU]
     93 31.137684   192.168.2.9     192.168.0.2     TCP       citrixadmin > http [ACK] Seq=2392 Ack=1656 Win=
     94 31.138580   192.168.0.2     192.168.2.9     TCP       [TCP segment of a reassembled PDU]
     95 31.138680   192.168.0.2     192.168.2.9     HTTP      HTTP/1.1 200 OK (text/plain) (application/octet
     96 31.138739   192.168.2.9     192.168.0.2     TCP       citrixadmin > http [ACK] Seq=2392 Ack=3555 Win=
     97 31.141571   192.168.2.9     192.168.0.2     TCP       citrixadmin > http [FIN, ACK] Seq=2392 Ack=3555
     98 31.141938   192.168.0.2     192.168.2.9     TCP       http > citrixadmin [ACK] Seq=3555 Ack=2393 Win=
    105 38.648420   192.168.2.9     192.168.0.2     DNS       Standard query A amritapuri.org.Amritavidya.edu
    106 38.648913   192.168.0.2     192.168.2.9     DNS       Standard query response, No such name
    107 38.651977   192.168.2.9     192.168.0.2     DNS       Standard query A amritapuri.org
    108 38.652372   192.168.0.2     192.168.2.9     DNS       Standard query response A 203.197.150.199
```

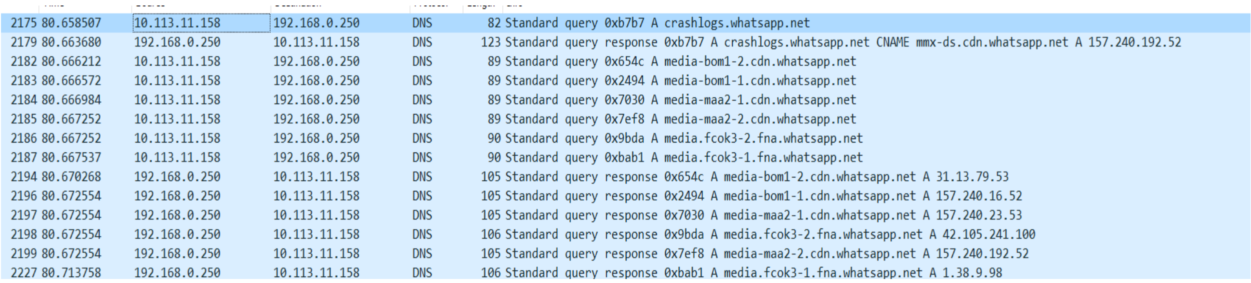
```
    [Request In: 107]
    [Time: 0.000395000 seconds]
    Transaction ID: 0x0005
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
  ⊞ Answers
```

```
0020  02 09 00 35 09 d3 00 38  3e 7b 00 05 81 80 00 01   ...5...8 >{......
0030  00 01 00 00 00 00 0a 61  6d 72 69 74 61 70 75 72   .......a mritapur
0040  69 03 6f 72 67 00 00 01  00 01 c0 0c 00 01 00 01   i.org... ........
```

We see from the above screenshot that *nslookup* actually sent two/three DNS queries and received two/three DNS responses.

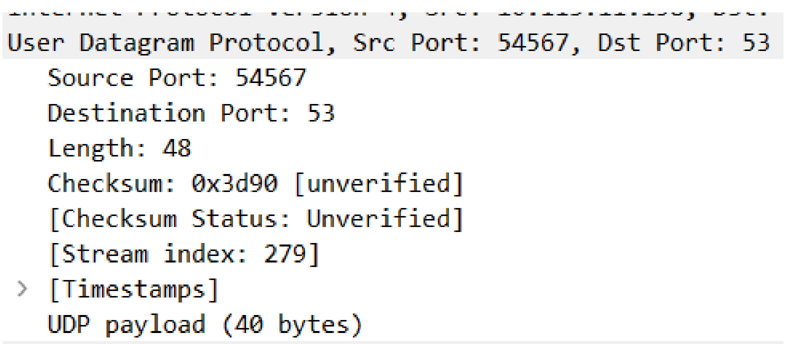
For the purpose of this assignment, in answering the following questions ignore the first one/two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications.

You should instead focus on the last query and response messages. Again, answer the following questions for this capture of frames.

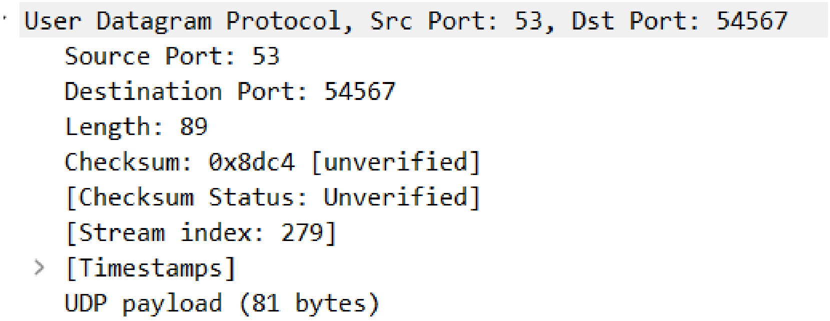


```
2175 80.658507   10.113.11.158   192.168.0.250   DNS    82 Standard query 0xb7b7 A crashlogs.whatsapp.net
2179 80.663680   192.168.0.250   10.113.11.158   DNS   123 Standard query response 0xb7b7 A crashlogs.whatsapp.net CNAME mmx-ds.cdn.whatsapp.net A 157.240.192.52
2182 80.666212   10.113.11.158   192.168.0.250   DNS    89 Standard query 0x654c A media-bom1-2.cdn.whatsapp.net
2183 80.666572   10.113.11.158   192.168.0.250   DNS    89 Standard query 0x2494 A media-bom1-1.cdn.whatsapp.net
2184 80.666984   10.113.11.158   192.168.0.250   DNS    89 Standard query 0x7030 A media-maa2-1.cdn.whatsapp.net
2185 80.667252   10.113.11.158   192.168.0.250   DNS    89 Standard query 0x7ef8 A media-maa2-2.cdn.whatsapp.net
2186 80.667252   10.113.11.158   192.168.0.250   DNS    90 Standard query 0x9bda A media.fcok3-2.fna.whatsapp.net
2187 80.667537   10.113.11.158   192.168.0.250   DNS    90 Standard query 0xbab1 A media.fcok3-1.fna.whatsapp.net
2194 80.670268   192.168.0.250   10.113.11.158   DNS   105 Standard query response 0x654c A media-bom1-2.cdn.whatsapp.net A 31.13.79.53
2196 80.672554   192.168.0.250   10.113.11.158   DNS   105 Standard query response 0x2494 A media-bom1-1.cdn.whatsapp.net A 157.240.16.52
2197 80.672554   192.168.0.250   10.113.11.158   DNS   105 Standard query response 0x7030 A media-maa2-1.cdn.whatsapp.net A 157.240.23.53
2198 80.672554   192.168.0.250   10.113.11.158   DNS   106 Standard query response 0x9bda A media.fcok3-2.fna.whatsapp.net A 42.105.241.100
2199 80.672554   192.168.0.250   10.113.11.158   DNS   105 Standard query response 0x7ef8 A media-maa2-2.cdn.whatsapp.net A 157.240.192.52
2227 80.713758   192.168.0.250   10.113.11.158   DNS   106 Standard query response 0xbab1 A media.fcok3-1.fna.whatsapp.net A 1.38.9.98
```

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



```
Internet Protocol Version 4, Src: 10.113.11.158, Dst:
User Datagram Protocol, Src Port: 54567, Dst Port: 53
    Source Port: 54567
    Destination Port: 53
    Length: 48
    Checksum: 0x3d90 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 279]
  > [Timestamps]
    UDP payload (40 bytes)
```



```
User Datagram Protocol, Src Port: 53, Dst Port: 54567
    Source Port: 53
    Destination Port: 54567
    Length: 89
    Checksum: 0x8dc4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 279]
  > [Timestamps]
    UDP payload (81 bytes)
```

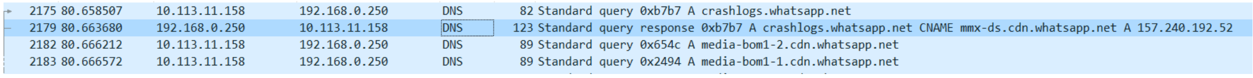
Destination port for the DNS query message is 53

Source port of DNS response message is 53

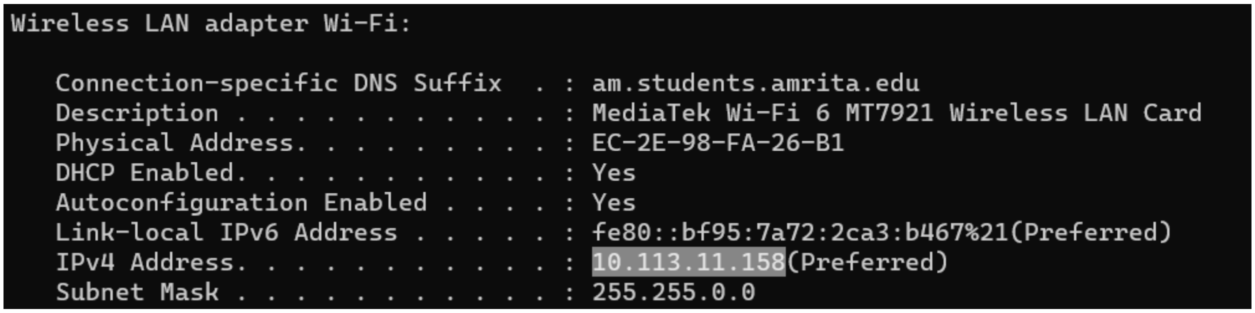
LabSheet3 - Understand how DNS works using the Wireshark

b. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Yes



```
2175 80.658507  10.113.11.158  192.168.0.250  DNS   82 Standard query 0xb7b7 A crashlogs.whatsapp.net
2179 80.663680  192.168.0.250  10.113.11.158  DNS  123 Standard query response 0xb7b7 A crashlogs.whatsapp.net CNAME mmx-ds.cdn.whatsapp.net A 157.240.192.52
2182 80.666212  10.113.11.158  192.168.0.250  DNS   89 Standard query 0x654c A media-bom1-2.cdn.whatsapp.net
2183 80.666572  10.113.11.158  192.168.0.250  DNS   89 Standard query 0x2494 A media-bom1-1.cdn.whatsapp.net
```

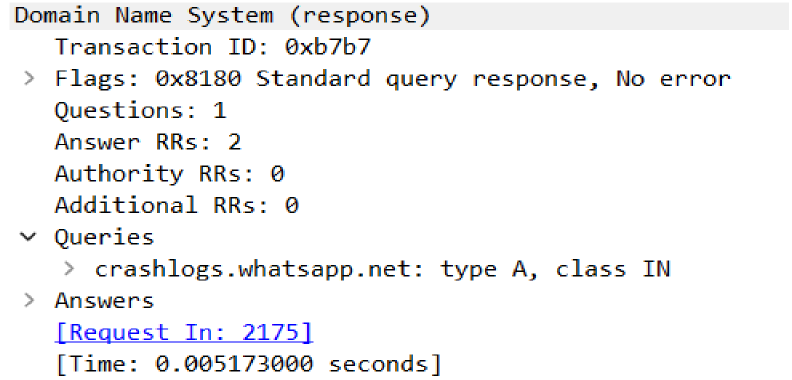


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : am.students.amrita.edu
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Physical Address. . . . . . . . . : EC-2E-98-FA-26-B1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::bf95:7a72:2ca3:b467%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.113.11.158(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
```

c. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

"Type" of DNS query is A.

NO, the query message does not contain any "answers"

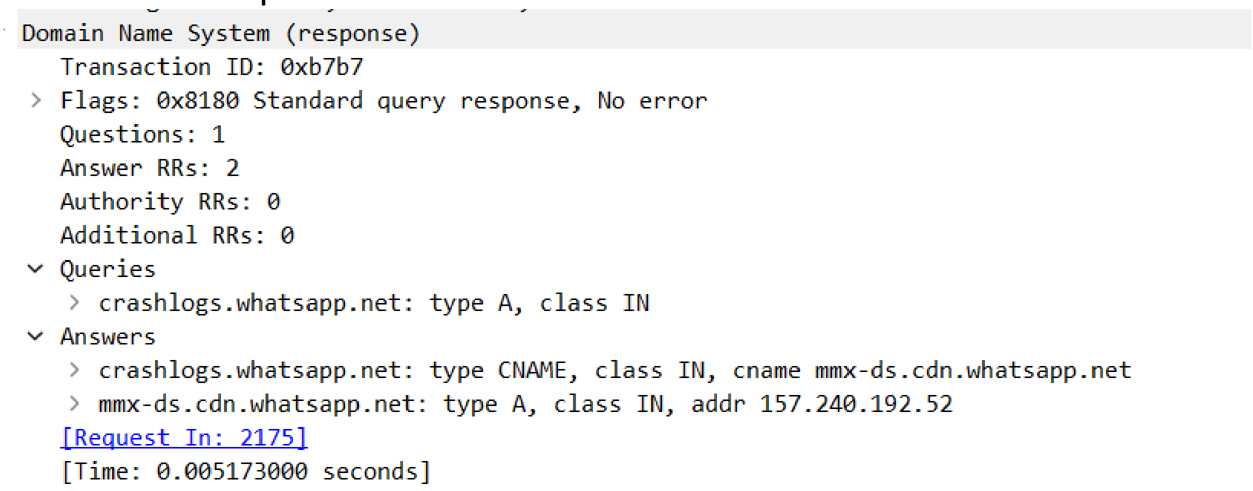


```
Domain Name System (response)
   Transaction ID: 0xb7b7
 > Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 2
   Authority RRs: 0
   Additional RRs: 0
 v Queries
   > crashlogs.whatsapp.net: type A, class IN
 > Answers
   [Request In: 2175]
   [Time: 0.005173000 seconds]
```

LabSheet3 - Understand how DNS works using the Wireshark

d. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

2 "answers" is provided.



```
Domain Name System (response)
    Transaction ID: 0xb7b7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
      > crashlogs.whatsapp.net: type A, class IN
  v Answers
      > crashlogs.whatsapp.net: type CNAME, class IN, cname mmx-ds.cdn.whatsapp.net
      > mmx-ds.cdn.whatsapp.net: type A, class IN, addr 157.240.192.52
    [Request In: 2175]
    [Time: 0.005173000 seconds]
```