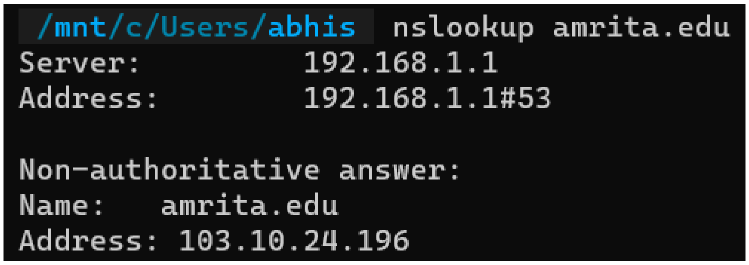
19CSE301

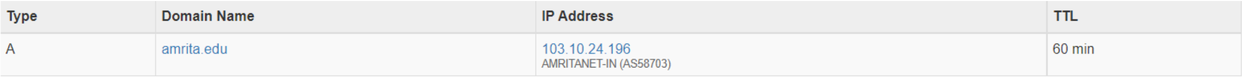
Computer Networks Lab

DNS - Lab Sheet 3

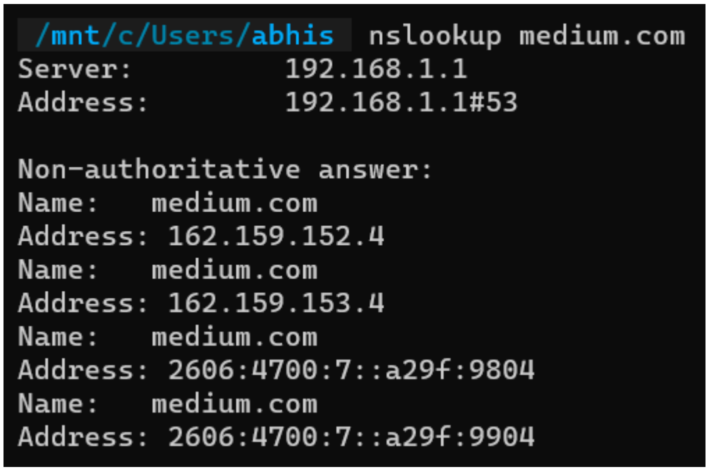
S Abhishek
AM.EN.U4CSE19147



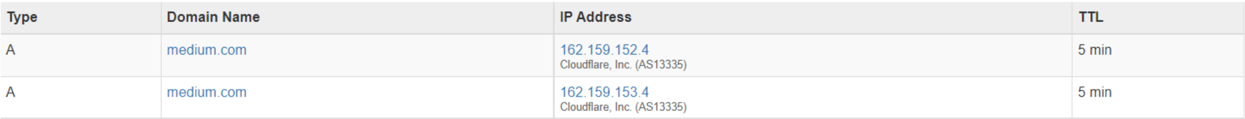
```
 /mnt/c/Users/abhis  nslookup amrita.edu
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   amrita.edu
Address: 103.10.24.196
```



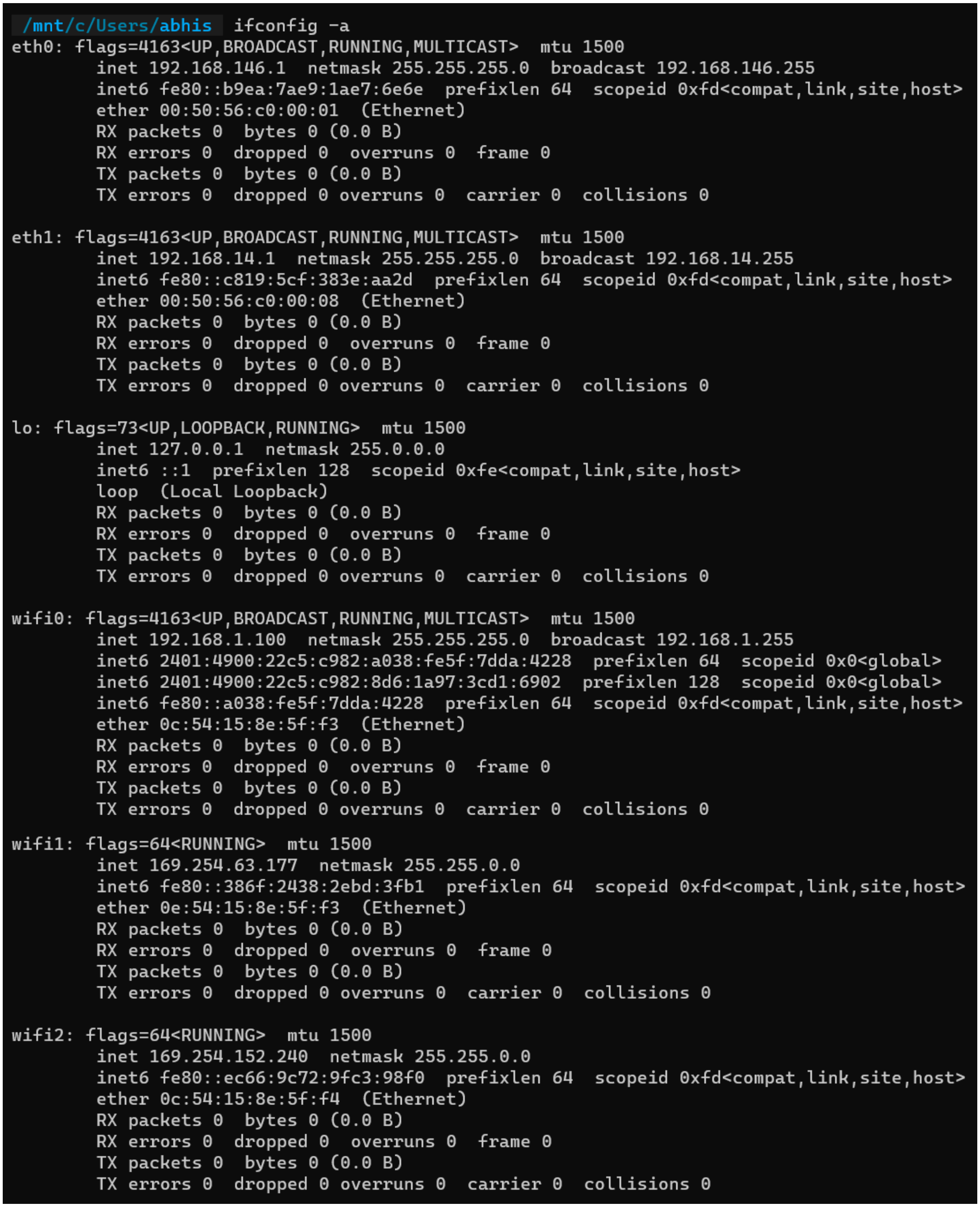
Type	Domain Name	IP Address	TTL
A	amrita.edu	103.10.24.196 AMRITANET-IN (AS58703)	60 min



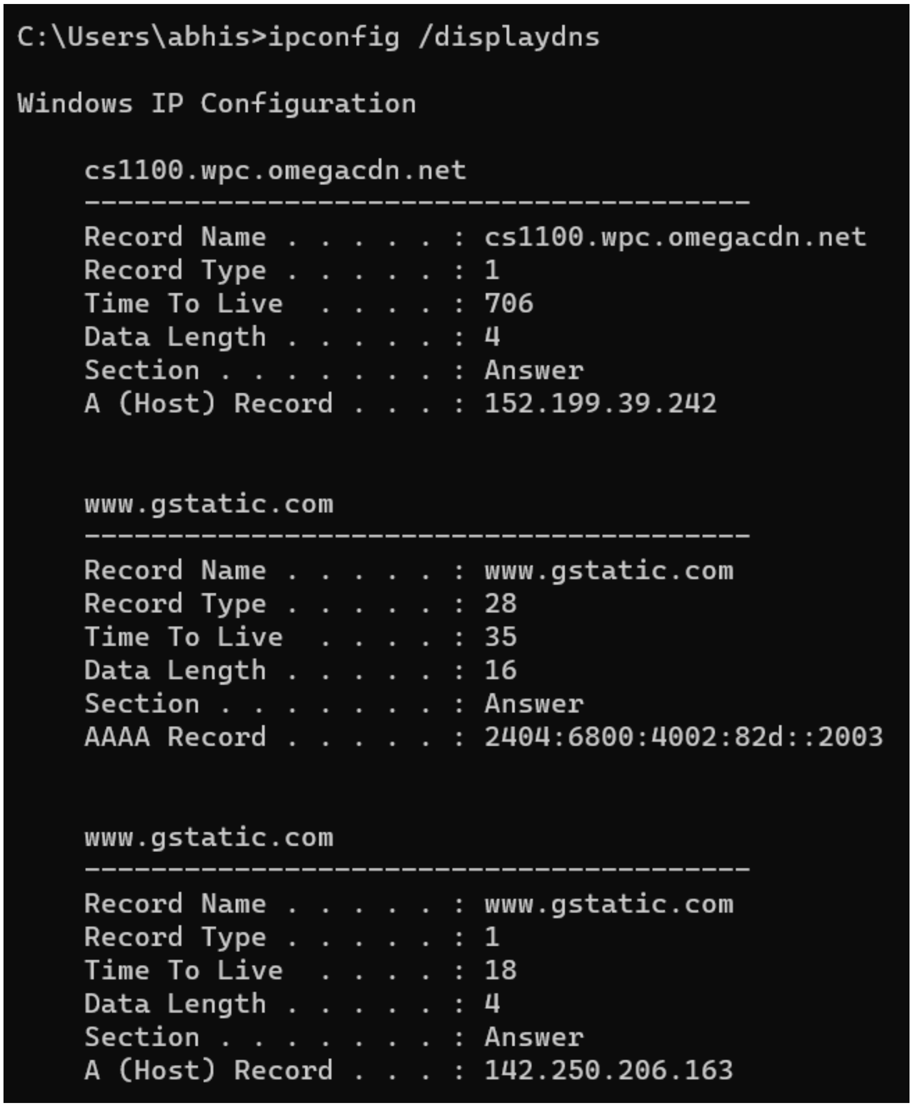
```
 /mnt/c/Users/abhis  nslookup medium.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   medium.com
Address: 162.159.152.4
Name:   medium.com
Address: 162.159.153.4
Name:   medium.com
Address: 2606:4700:7::a29f:9804
Name:   medium.com
Address: 2606:4700:7::a29f:9904
```



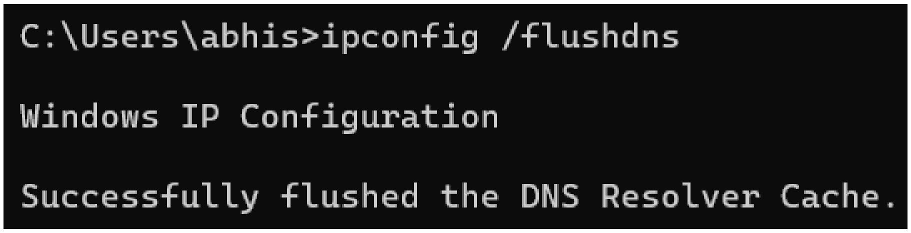
Type	Domain Name	IP Address	TTL
A	medium.com	162.159.152.4 Cloudflare, Inc. (AS13335)	5 min
A	medium.com	162.159.153.4 Cloudflare, Inc. (AS13335)	5 min



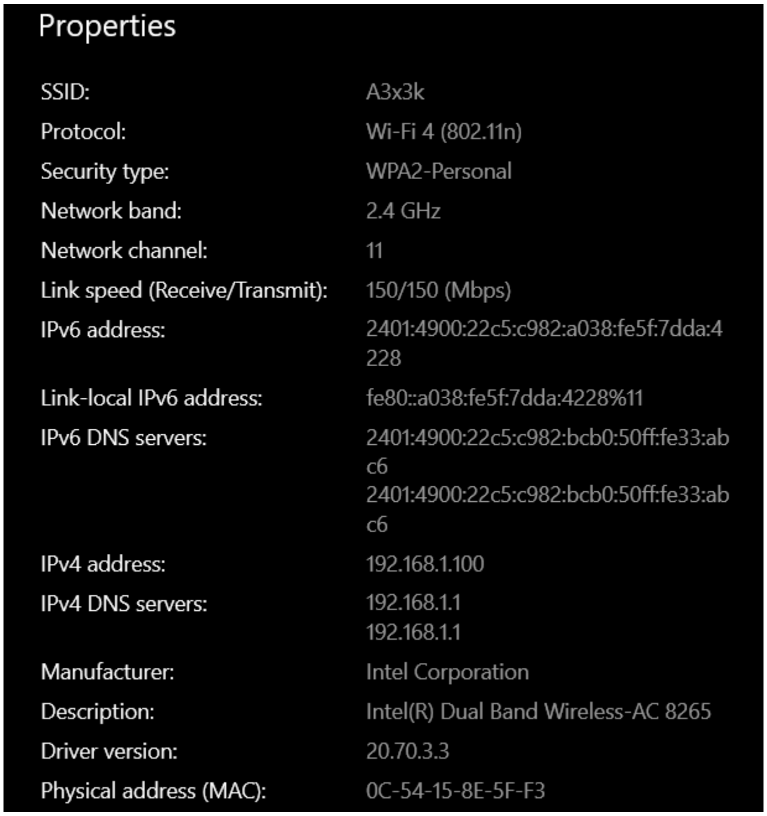
```
 /mnt/c/Users/abhis  ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.146.1  netmask 255.255.255.0  broadcast 192.168.146.255
        inet6 fe80::b9ea:7ae9:1ae7:6e6e  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 00:50:56:c0:00:01  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.14.1  netmask 255.255.255.0  broadcast 192.168.14.255
        inet6 fe80::c819:5cf:383e:aa2d  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 00:50:56:c0:00:08  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 1500
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0xfe<compat,link,site,host>
        loop  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2401:4900:22c5:c982:a038:fe5f:7dda:4228  prefixlen 64  scopeid 0x0<global>
        inet6 2401:4900:22c5:c982:8d6:1a97:3cd1:6902  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::a038:fe5f:7dda:4228  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 0c:54:15:8e:5f:f3  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi1: flags=64<RUNNING>  mtu 1500
        inet 169.254.63.177  netmask 255.255.0.0
        inet6 fe80::386f:2438:2ebd:3fb1  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 0e:54:15:8e:5f:f3  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi2: flags=64<RUNNING>  mtu 1500
        inet 169.254.152.240  netmask 255.255.0.0
        inet6 fe80::ec66:9c72:9fc3:98f0  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 0c:54:15:8e:5f:f4  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
C:\Users\abhis>ipconfig /displaydns

Windows IP Configuration

    cs1100.wpc.omegacdn.net
    ----------------------------------------
    Record Name . . . . . : cs1100.wpc.omegacdn.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 706
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 152.199.39.242


    www.gstatic.com
    ----------------------------------------
    Record Name . . . . . : www.gstatic.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 35
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2404:6800:4002:82d::2003


    www.gstatic.com
    ----------------------------------------
    Record Name . . . . . : www.gstatic.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 18
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.250.206.163
```



```
C:\Users\abhis>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```



Properties

SSID:	A3x3k
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	11
Link speed (Receive/Transmit):	150/150 (Mbps)
IPv6 address:	2401:4900:22c5:c982:a038:fe5f:7dda:4228
Link-local IPv6 address:	fe80::a038:fe5f:7dda:4228%11
IPv6 DNS servers:	2401:4900:22c5:c982:bcb0:50ff:fe33:abc6 2401:4900:22c5:c982:bcb0:50ff:fe33:abc6
IPv4 address:	192.168.1.100
IPv4 DNS servers:	192.168.1.1 192.168.1.1
Manufacturer:	Intel Corporation
Description:	Intel(R) Dual Band Wireless-AC 8265
Driver version:	20.70.3.3
Physical address (MAC):	0C-54-15-8E-5F-F3

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

- DNS provides this same service to the Internet by mapping a domain name to IP Address.

Services provided by DNS:

- Host Resolution
- Mail Server aliasing

Working:

- First, computer looks is its local DNS cache, which stores information that that computer has recently retrieved.
- If computer has recently retrieved your computer doesn't already know the answer, it needs to perform a DNS query to find out
- computer queries Recursive DNS servers which have their own cache, if Recursive DNS servers don't know the answer
- they query Root nameservers
- which look at the first part of domain example.com and direct query to TLD
- Then, we have to go all the way back to the root name servers.
- Then we ask the COM top level domain (TLD) nameservers that handle all the traffic for sites ending in .com
- From here, the .com name servers identify what name servers example.com is a responsible for.
- If TLD nameservers don't have the information we need it directs the query to authoritative nameserver which know all information

about specific domain which are stored in DNS records, then it retrieves “A record”.

DNS Query Message Structure:

- Transaction ID: for matching response to queries
- Flags: specifies the requested operation and a response code
- Questions: count of entries in the queries section
- Answer RRs: count of entries in the answers section (RR stands for “resource record”)
- Authority RRs: count of entries in the authority section
- Additional RRs: count of entries in the additional section
- Queries: queries data
- Questions: 1 means this message has one entry in the Queries.
- Answer RRs: 0 means there are no answers. This is expected as a query message has only questions and no answers.

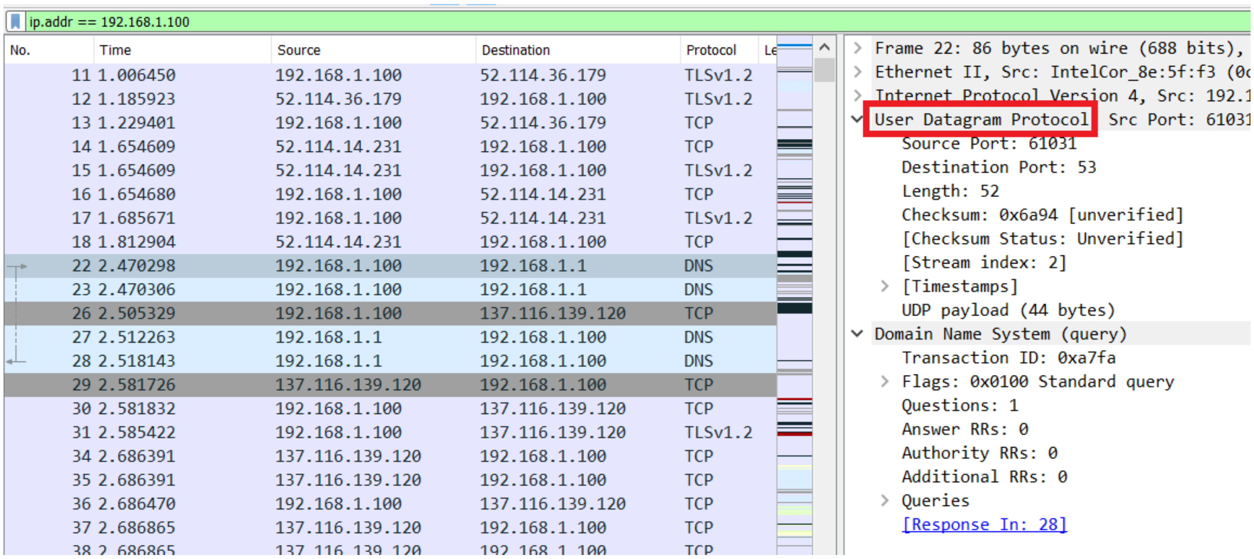
Entry structure of queries:

- Name: the domain name
- Type: DNS record type (e.g., A, CNAME, and MX)
- Class: allows domain names to be used for arbitrary objects

DNS Response:

- A response message shares the same header and Queries with an additional Answers section.
- Besides the same 3 sections found in a query entry, an answer entry has 3 additional pieces.
    - Time to Live (TTL): number of seconds this record can live
    - Data Length: the length of the data
    - Data: the returned data, such as an IP address or CNAME

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



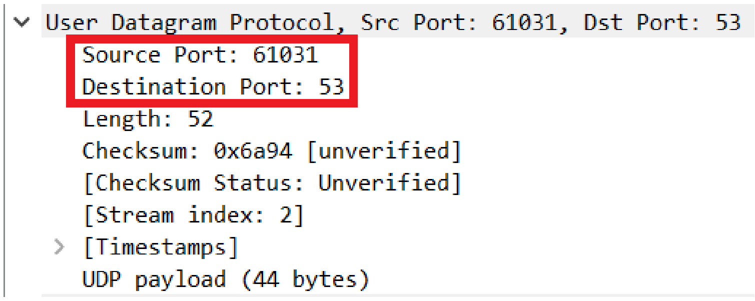
ip.addr == 192.168.1.100

No.	Time	Source	Destination	Protocol	Le
11	1.006450	192.168.1.100	52.114.36.179	TLSv1.2	
12	1.185923	52.114.36.179	192.168.1.100	TLSv1.2	
13	1.229401	192.168.1.100	52.114.36.179	TCP	
14	1.654609	52.114.14.231	192.168.1.100	TCP	
15	1.654609	52.114.14.231	192.168.1.100	TLSv1.2	
16	1.654680	192.168.1.100	52.114.14.231	TCP	
17	1.685671	192.168.1.100	52.114.14.231	TLSv1.2	
18	1.812904	52.114.14.231	192.168.1.100	TCP	
22	2.470298	192.168.1.100	192.168.1.1	DNS	
23	2.470306	192.168.1.100	192.168.1.1	DNS	
26	2.505329	192.168.1.100	137.116.139.120	TCP	
27	2.512263	192.168.1.1	192.168.1.100	DNS	
28	2.518143	192.168.1.1	192.168.1.100	DNS	
29	2.581726	137.116.139.120	192.168.1.100	TCP	
30	2.581832	192.168.1.100	137.116.139.120	TCP	
31	2.585422	192.168.1.100	137.116.139.120	TLSv1.2	
34	2.686391	137.116.139.120	192.168.1.100	TCP	
35	2.686391	137.116.139.120	192.168.1.100	TCP	
36	2.686470	192.168.1.100	137.116.139.120	TCP	
37	2.686865	137.116.139.120	192.168.1.100	TCP	
38	2.686865	137.116.139.120	192.168.1.100	TCP	

```
> Frame 22: 86 bytes on wire (688 bits),
> Ethernet II, Src: IntelCor_8e:5f:f3 (0c
> Internet Protocol Version 4, Src: 192.1
v User Datagram Protocol, Src Port: 61031
    Source Port: 61031
    Destination Port: 53
    Length: 52
    Checksum: 0x6a94 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (44 bytes)
v Domain Name System (query)
    Transaction ID: 0xa7fa
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 28]
```

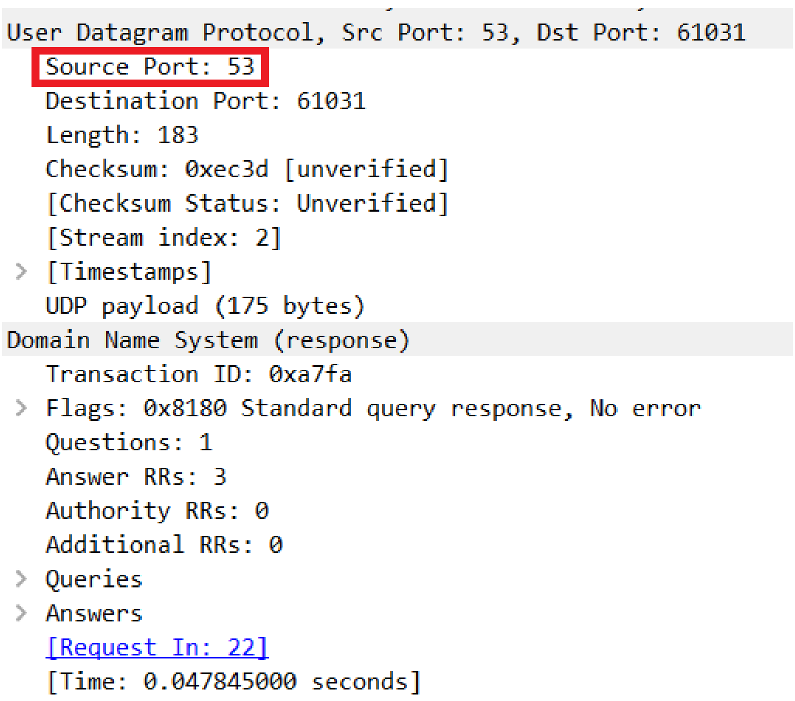
- DNS query and response messages are sent over UDP.

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



```
v User Datagram Protocol, Src Port: 61031, Dst Port: 53
    Source Port: 61031
    Destination Port: 53
    Length: 52
    Checksum: 0x6a94 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (44 bytes)
```

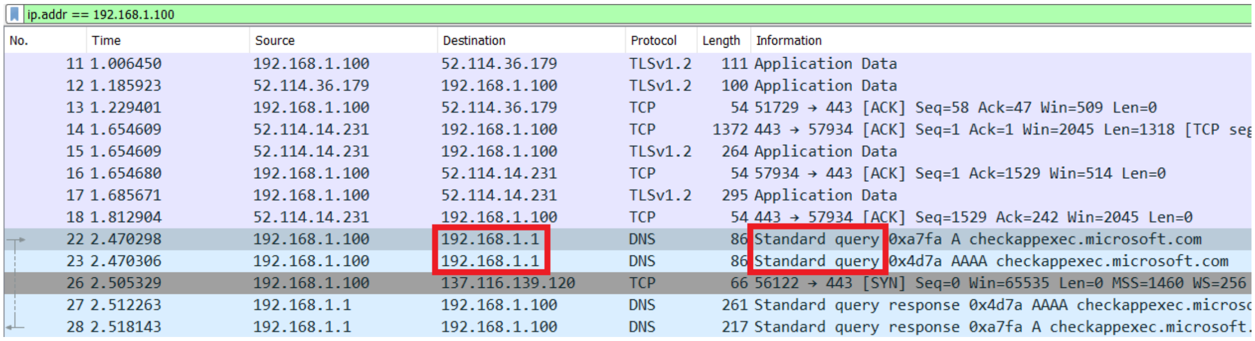
- Source Port : 61031



```
User Datagram Protocol, Src Port: 53, Dst Port: 61031
    Source Port: 53
    Destination Port: 61031
    Length: 183
    Checksum: 0xec3d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (175 bytes)
Domain Name System (response)
    Transaction ID: 0xa7fa
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 22]
    [Time: 0.047845000 seconds]
```

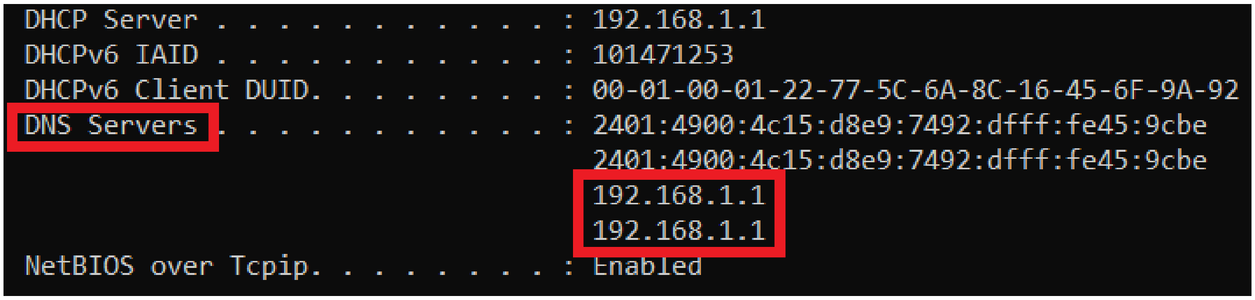
- Source Port : 53

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?



ip.addr == 192.168.1.100

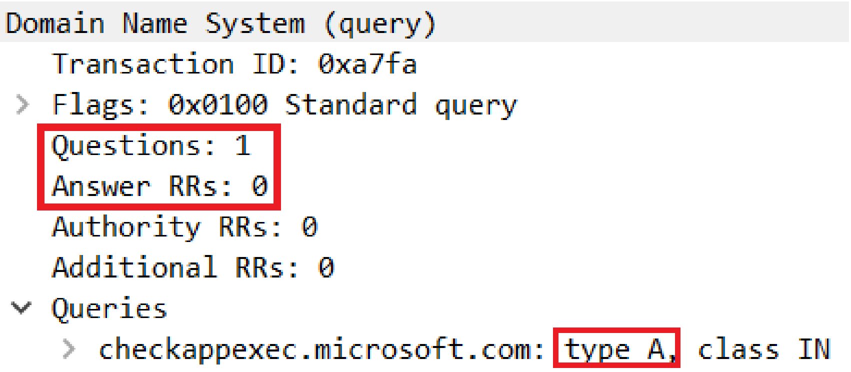
No.	Time	Source	Destination	Protocol	Length	Information
11	1.006450	192.168.1.100	52.114.36.179	TLSv1.2	111	Application Data
12	1.185923	52.114.36.179	192.168.1.100	TLSv1.2	100	Application Data
13	1.229401	192.168.1.100	52.114.36.179	TCP	54	51729 → 443 [ACK] Seq=58 Ack=47 Win=509 Len=0
14	1.654609	52.114.14.231	192.168.1.100	TCP	1372	443 → 57934 [ACK] Seq=1 Ack=1 Win=2045 Len=1318 [TCP seg
15	1.654609	52.114.14.231	192.168.1.100	TLSv1.2	264	Application Data
16	1.654680	192.168.1.100	52.114.14.231	TCP	54	57934 → 443 [ACK] Seq=1 Ack=1529 Win=514 Len=0
17	1.685671	192.168.1.100	52.114.14.231	TLSv1.2	295	Application Data
18	1.812904	52.114.14.231	192.168.1.100	TCP	54	443 → 57934 [ACK] Seq=1529 Ack=242 Win=2045 Len=0
22	2.470298	192.168.1.100	192.168.1.1	DNS	86	Standard query 0xa7fa A checkappexec.microsoft.com
23	2.470306	192.168.1.100	192.168.1.1	DNS	86	Standard query 0x4d7a AAAA checkappexec.microsoft.com
26	2.505329	192.168.1.100	137.116.139.120	TCP	66	56122 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
27	2.512263	192.168.1.1	192.168.1.100	DNS	261	Standard query response 0x4d7a AAAA checkappexec.microsc
28	2.518143	192.168.1.1	192.168.1.100	DNS	217	Standard query response 0xa7fa A checkappexec.microsoft.



```
DHCP Server . . . . . . . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . . . . . . . : 101471253
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-22-77-5C-6A-8C-16-45-6F-9A-92
DNS Servers . . . . . . . . . . . : 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe
                                    2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe
                                    192.168.1.1
                                    192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

- DNS query message is sent to the IP Address 192.168.1.1
- The IP address of the local DNS server determined using ipconfig is **same** as the IP Address to which the DNS query message is sent.

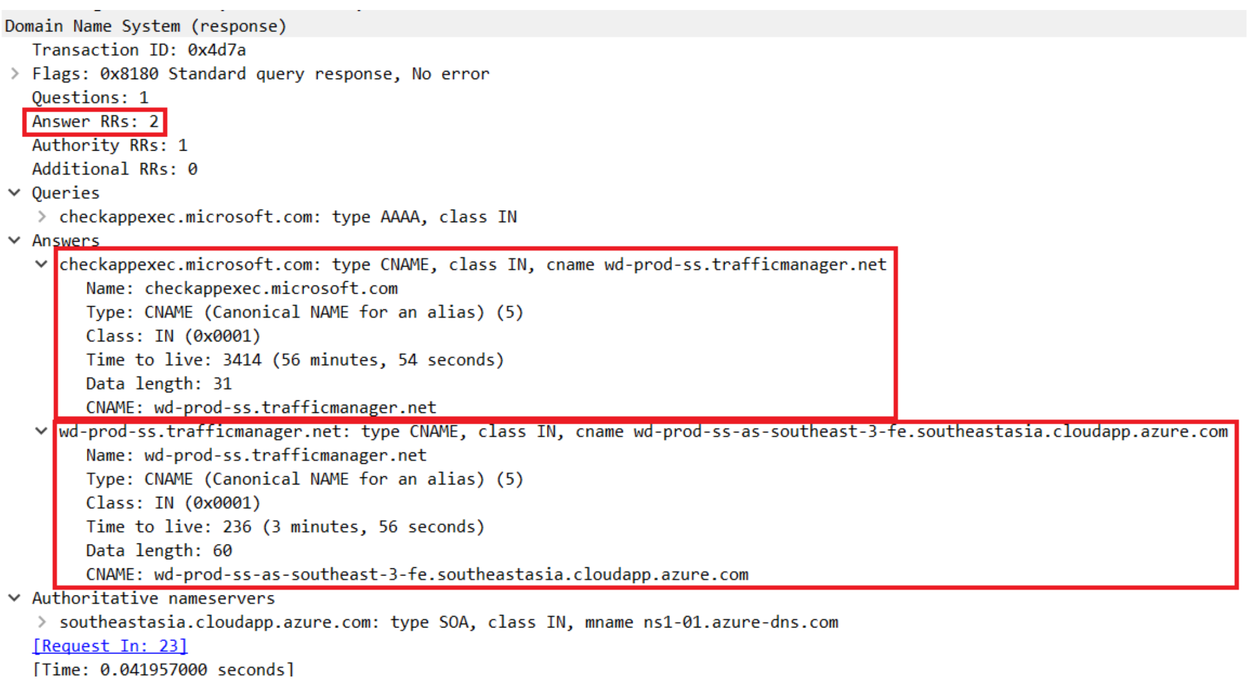
Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



```
Domain Name System (query)
   Transaction ID: 0xa7fa
 > Flags: 0x0100 Standard query
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 v Queries
    > checkappexec.microsoft.com: type A, class IN
```

- Type of DNS query : A
- The query message doesn't contain any answers.

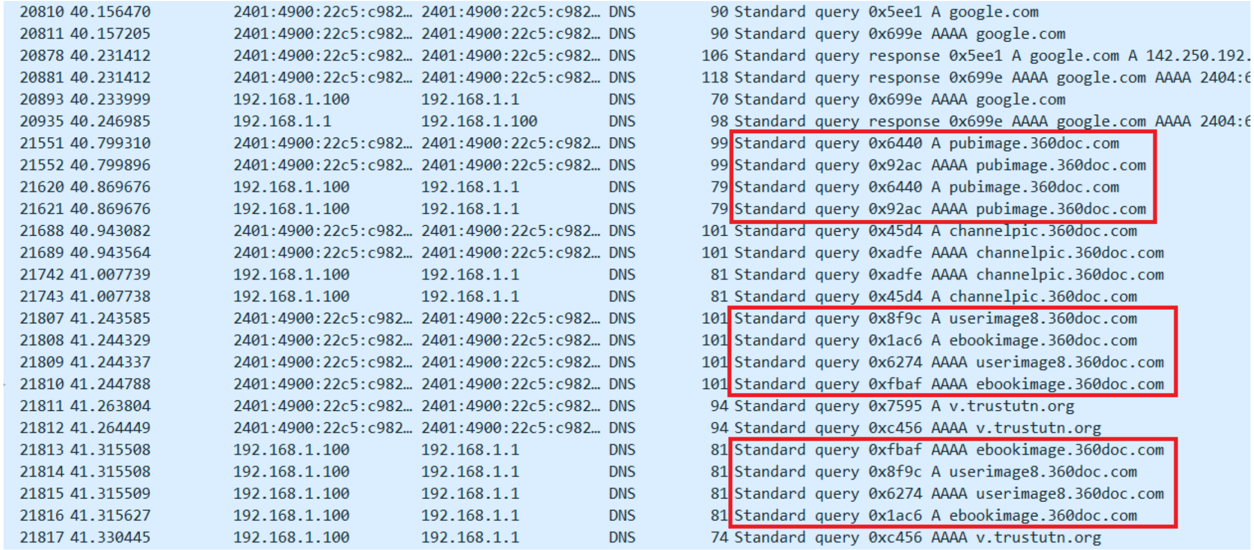
Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?



```
Domain Name System (response)
    Transaction ID: 0x4d7a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 1
    Additional RRs: 0
  ∨ Queries
      > checkappexec.microsoft.com: type AAAA, class IN
  ∨ Answers
      ∨ checkappexec.microsoft.com: type CNAME, class IN, cname wd-prod-ss.trafficmanager.net
            Name: checkappexec.microsoft.com
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 3414 (56 minutes, 54 seconds)
            Data length: 31
            CNAME: wd-prod-ss.trafficmanager.net
      ∨ wd-prod-ss.trafficmanager.net: type CNAME, class IN, cname wd-prod-ss-as-southeast-3-fe.southeastasia.cloudapp.azure.com
            Name: wd-prod-ss.trafficmanager.net
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 236 (3 minutes, 56 seconds)
            Data length: 60
            CNAME: wd-prod-ss-as-southeast-3-fe.southeastasia.cloudapp.azure.com
  ∨ Authoritative nameservers
      > southeastasia.cloudapp.azure.com: type SOA, class IN, mname ns1-01.azure-dns.com
    [Request In: 23]
    [Time: 0.041957000 seconds]
```

- 2 answers are provided with respect to the DNS Query.
- Each of these answers contains information about the,
  - Name of the host
  - Type of address
  - Class
  - Time to Live (TTL)
  - Data length
  - CNAME

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



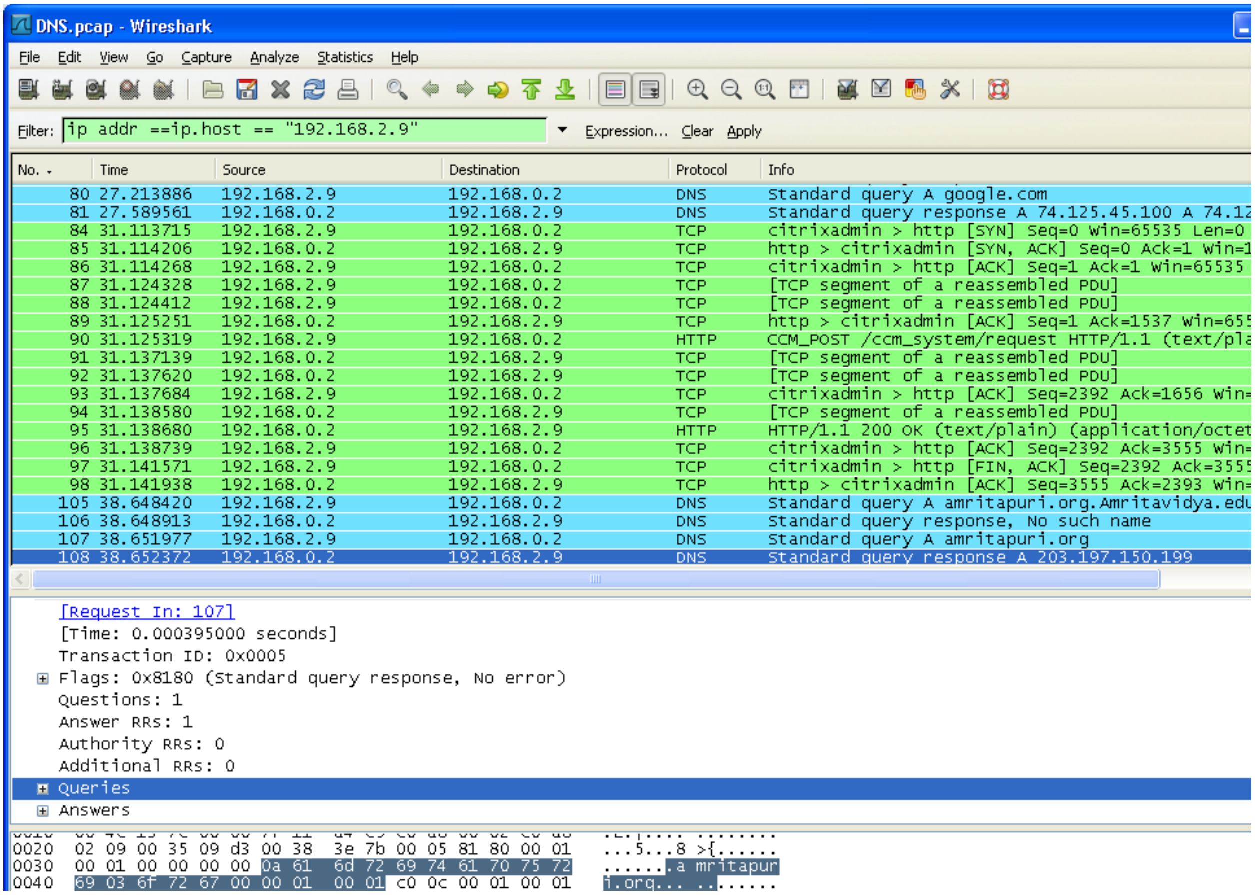
```
20810 40.156470     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS      90 Standard query 0x5ee1 A google.com
20811 40.157205     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS      90 Standard query 0x699e AAAA google.com
20878 40.231412     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     106 Standard query response 0x5ee1 A google.com A 142.250.192.
20881 40.231412     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     118 Standard query response 0x699e AAAA google.com AAAA 2404:6
20893 40.233999     192.168.1.100        192.168.1.1          DNS      70 Standard query 0x699e AAAA google.com
20935 40.246985     192.168.1.1          192.168.1.100        DNS      98 Standard query response 0x699e AAAA google.com AAAA 2404:6
21551 40.799310     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS      99 Standard query 0x6440 A pubimage.360doc.com
21552 40.799896     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS      99 Standard query 0x92ac AAAA pubimage.360doc.com
21620 40.869676     192.168.1.100        192.168.1.1          DNS      79 Standard query 0x6440 A pubimage.360doc.com
21621 40.869676     192.168.1.100        192.168.1.1          DNS      79 Standard query 0x92ac AAAA pubimage.360doc.com
21688 40.943082     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     101 Standard query 0x45d4 A channelpic.360doc.com
21689 40.943564     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     101 Standard query 0xadfe AAAA channelpic.360doc.com
21742 41.007739     192.168.1.100        192.168.1.1          DNS      81 Standard query 0xadfe AAAA channelpic.360doc.com
21743 41.007738     192.168.1.100        192.168.1.1          DNS      81 Standard query 0x45d4 A channelpic.360doc.com
21807 41.243585     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     101 Standard query 0x8f9c A userimage8.360doc.com
21808 41.244329     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     101 Standard query 0x1ac6 A ebookimage.360doc.com
21809 41.244337     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     101 Standard query 0x6274 AAAA userimage8.360doc.com
21810 41.244788     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS     101 Standard query 0xfbaf AAAA ebookimage.360doc.com
21811 41.263804     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS      94 Standard query 0x7595 A v.trustutn.org
21812 41.264449     2401:4900:22c5:c982… 2401:4900:22c5:c982… DNS      94 Standard query 0xc456 AAAA v.trustutn.org
21813 41.315508     192.168.1.100        192.168.1.1          DNS      81 Standard query 0xfbaf AAAA ebookimage.360doc.com
21814 41.315508     192.168.1.100        192.168.1.1          DNS      81 Standard query 0x8f9c A userimage8.360doc.com
21815 41.315509     192.168.1.100        192.168.1.1          DNS      81 Standard query 0x6274 AAAA userimage8.360doc.com
21816 41.315627     192.168.1.100        192.168.1.1          DNS      81 Standard query 0x1ac6 A ebookimage.360doc.com
21817 41.330445     192.168.1.100        192.168.1.1          DNS      74 Standard query 0xc456 AAAA v.trustutn.org
```

- Yes, the host issues new DNS queries for each image since the images are not loaded from the same host.

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:


DNS.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

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
```

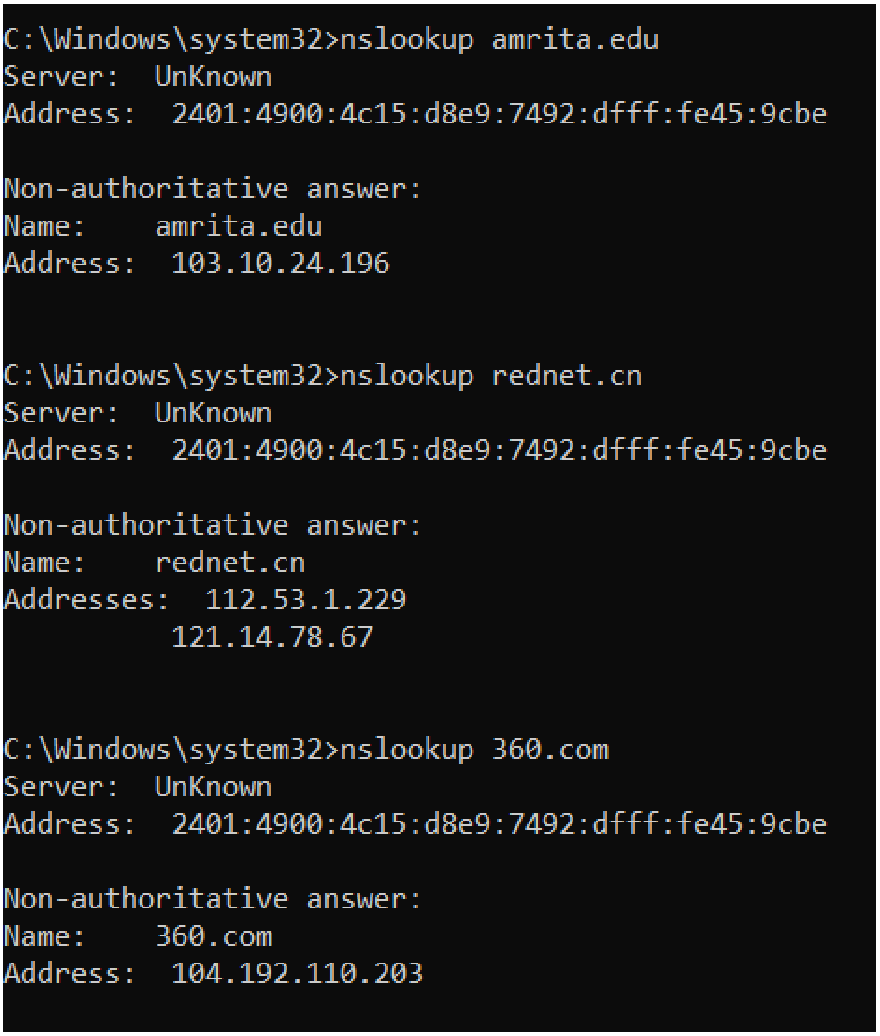
```
    [Request In: 107]
    [Time: 0.000395000 seconds]
    Transaction ID: 0x0005
 ⊞  Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
 ⊞  Queries
 ⊞  Answers
```

```
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... ........
```

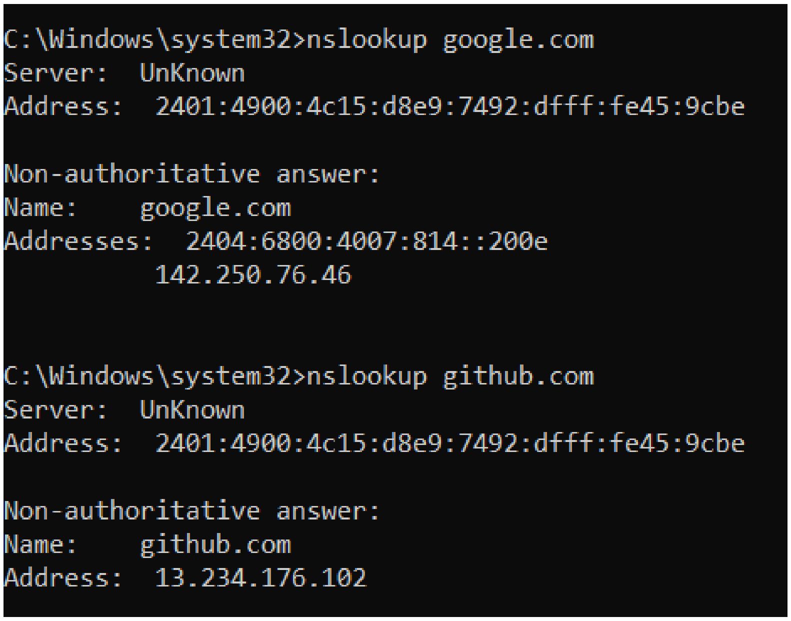
We see from the above screenshot that *nslookup* actually sent two/three DNS queries and received two/three DNS responses.

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.

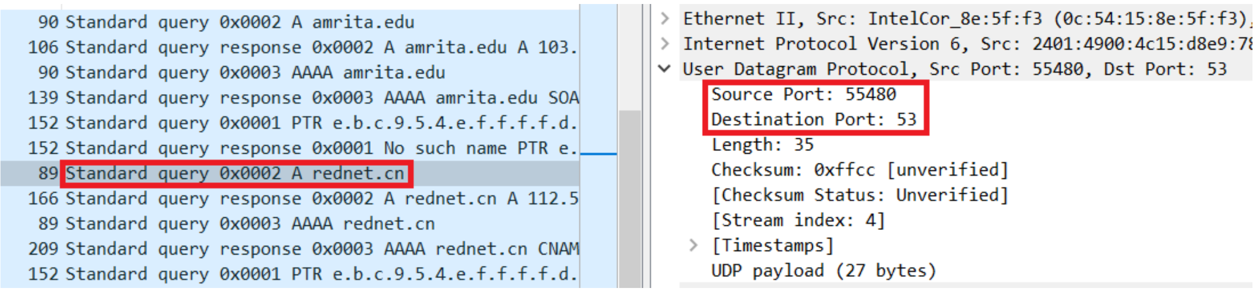


```
C:\Windows\system32>nslookup amrita.edu
Server:  UnKnown
Address:  2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe

Non-authoritative answer:
Name:    amrita.edu
Address:  103.10.24.196


C:\Windows\system32>nslookup rednet.cn
Server:  UnKnown
Address:  2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe

Non-authoritative answer:
Name:    rednet.cn
Addresses:  112.53.1.229
          121.14.78.67


C:\Windows\system32>nslookup 360.com
Server:  UnKnown
Address:  2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe

Non-authoritative answer:
Name:    360.com
Address:  104.192.110.203
```



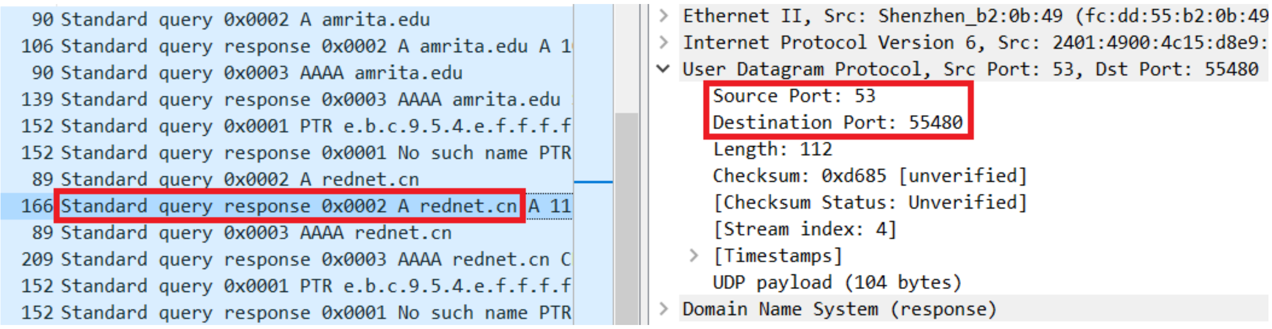
```
C:\Windows\system32>nslookup google.com
Server:  UnKnown
Address:  2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:814::200e
          142.250.76.46


C:\Windows\system32>nslookup github.com
Server:  UnKnown
Address:  2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe

Non-authoritative answer:
Name:    github.com
Address:  13.234.176.102
```

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



```
 90 Standard query 0x0002 A amrita.edu
106 Standard query response 0x0002 A amrita.edu A 103.
 90 Standard query 0x0003 AAAA amrita.edu
139 Standard query response 0x0003 AAAA amrita.edu SOA
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.
152 Standard query response 0x0001 No such name PTR e.
 89 Standard query 0x0002 A rednet.cn
166 Standard query response 0x0002 A rednet.cn A 112.5
 89 Standard query 0x0003 AAAA rednet.cn
209 Standard query response 0x0003 AAAA rednet.cn CNAM
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.
```

```
> Ethernet II, Src: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3),
> Internet Protocol Version 6, Src: 2401:4900:4c15:d8e9:78
v User Datagram Protocol, Src Port: 55480, Dst Port: 53
    Source Port: 55480
    Destination Port: 53
    Length: 35
    Checksum: 0xffcc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (27 bytes)
```

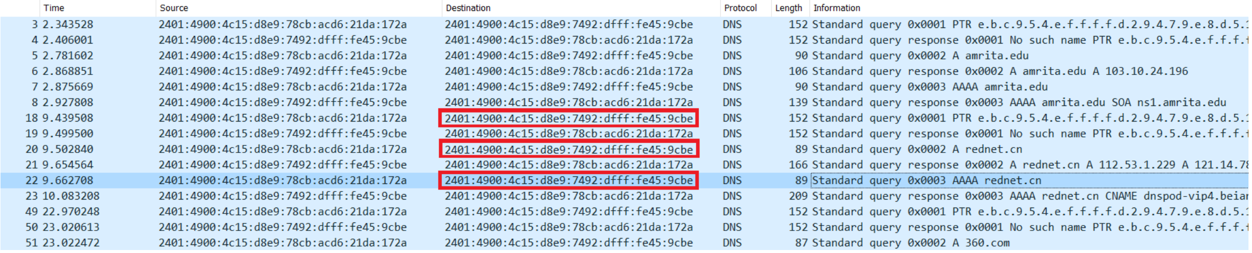


```
 90 Standard query 0x0002 A amrita.edu
106 Standard query response 0x0002 A amrita.edu A 1
 90 Standard query 0x0003 AAAA amrita.edu
139 Standard query response 0x0003 AAAA amrita.edu
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f
152 Standard query response 0x0001 No such name PTR
 89 Standard query 0x0002 A rednet.cn
166 Standard query response 0x0002 A rednet.cn A 11
 89 Standard query 0x0003 AAAA rednet.cn
209 Standard query response 0x0003 AAAA rednet.cn C
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f
152 Standard query response 0x0001 No such name PTR
```

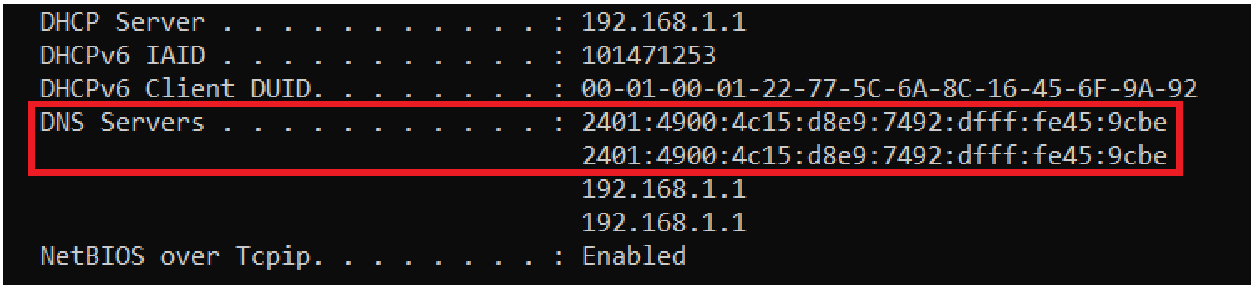
```
> Ethernet II, Src: Shenzhen_b2:0b:49 (fc:dd:55:b2:0b:49
> Internet Protocol Version 6, Src: 2401:4900:4c15:d8e9:
v User Datagram Protocol, Src Port: 53, Dst Port: 55480
    Source Port: 53
    Destination Port: 55480
    Length: 112
    Checksum: 0xd685 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (104 bytes)
> Domain Name System (response)
```

- Destination port of the DNS query message = 53
- Source port of the DNS response message = 53

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



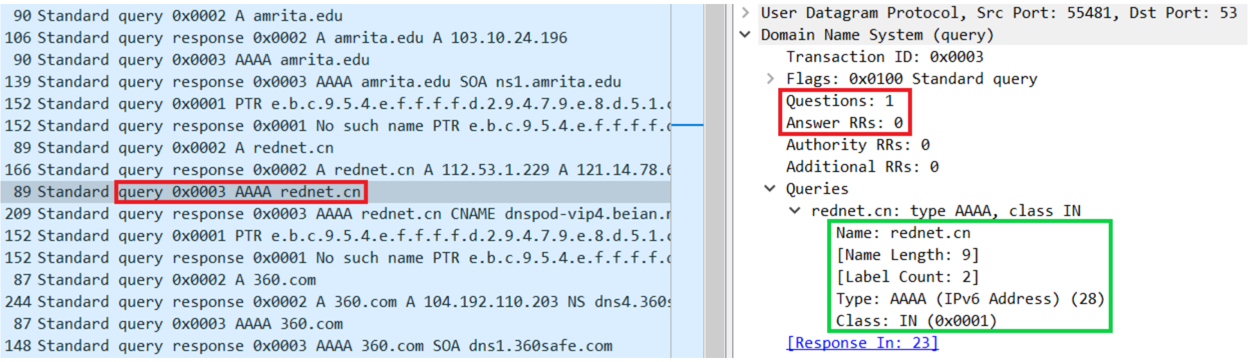
```
    Time       Source                                  Destination                             Protocol  Length Information
 3  2.343528   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS         152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.2.9.4.7.9.e.8.d.5.
 4  2.406001   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         152 Standard query response 0x0001 No such name PTR e.b.c.9.5.4.e.f.f.f.
 5  2.781602   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS          90 Standard query 0x0002 A amrita.edu
 6  2.868851   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         106 Standard query response 0x0002 A amrita.edu A 103.10.24.196
 7  2.875669   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS          90 Standard query 0x0003 AAAA amrita.edu
 8  2.927808   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         139 Standard query response 0x0003 AAAA amrita.edu SOA ns1.amrita.edu
18  9.439508   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS         152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.2.9.4.7.9.e.8.d.5.
19  9.499500   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         152 Standard query response 0x0001 No such name PTR e.b.c.9.5.4.e.f.f.f.
20  9.502840   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS          89 Standard query 0x0002 A rednet.cn
21  9.654564   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         166 Standard query response 0x0002 A rednet.cn A 112.53.1.229 A 121.14.7
22  9.662708   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS          89 Standard query 0x0003 AAAA rednet.cn
23 10.083208   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         209 Standard query response 0x0003 AAAA rednet.cn CNAME dnspod-vip4.beiar
49 22.970248   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS         152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.2.9.4.7.9.e.8.d.5.
50 23.020613   2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe 2401:4900:4c15:d8e9:78cb:acd6:21da:172a DNS         152 Standard query response 0x0001 No such name PTR e.b.c.9.5.4.e.f.f.f.
51 23.022472   2401:4900:4c15:d8e9:78cb:acd6:21da:172a 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe DNS          87 Standard query 0x0002 A 360.com
```



```
 DHCP Server . . . . . . . . . . . . : 192.168.1.1
 DHCPv6 IAID . . . . . . . . . . . . : 101471253
 DHCPv6 Client DUID. . . . . . . . . : 00-01-00-01-22-77-5C-6A-8C-16-45-6F-9A-92
 DNS Servers . . . . . . . . . . . . : 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe
                                       2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe
                                       192.168.1.1
                                       192.168.1.1
 NetBIOS over Tcpip. . . . . . . . . : Enabled
```

- DNS query message is sent to the IP Address 2401:4900:4c15:d8e9:7492:dfff:fe45:9cbe.
- The IP address of the local DNS server determined using ipconfig is **same** as the IP Address to which the DNS query message is sent.

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

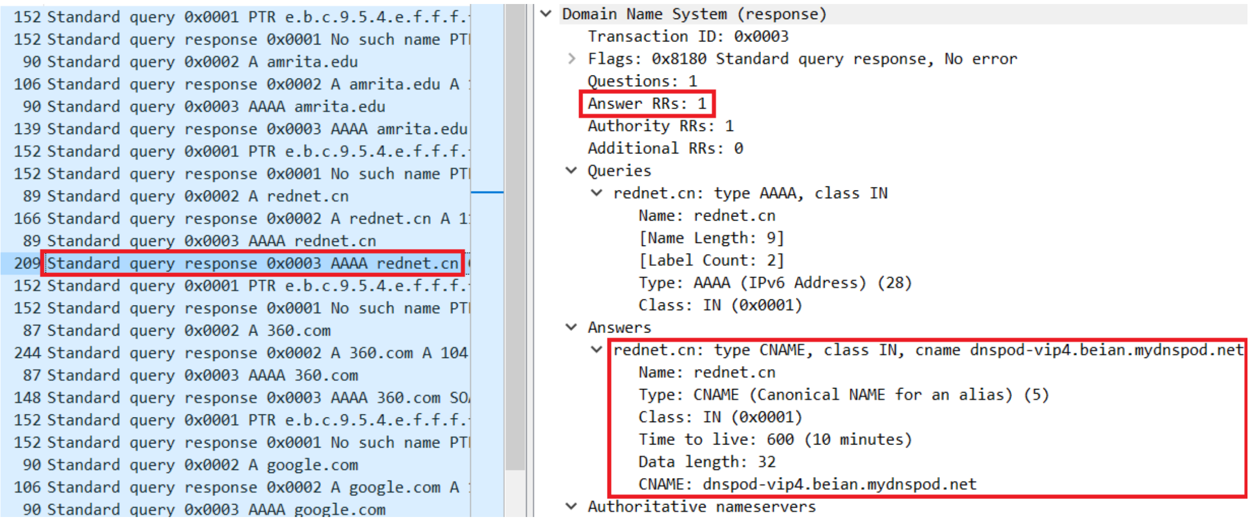


```
 90 Standard query 0x0002 A amrita.edu
106 Standard query response 0x0002 A amrita.edu A 103.10.24.196
 90 Standard query 0x0003 AAAA amrita.edu
139 Standard query response 0x0003 AAAA amrita.edu SOA ns1.amrita.edu
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.2.9.4.7.9.e.8.d.5.1.
152 Standard query response 0x0001 No such name PTR e.b.c.9.5.4.e.f.f.f.f.
 89 Standard query 0x0002 A rednet.cn
166 Standard query response 0x0002 A rednet.cn A 112.53.1.229 A 121.14.78.
 89 Standard query 0x0003 AAAA rednet.cn
209 Standard query response 0x0003 AAAA rednet.cn CNAME dnspod-vip4.beian.
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.f.d.2.9.4.7.9.e.8.d.5.1.
152 Standard query response 0x0001 No such name PTR e.b.c.9.5.4.e.f.f.f.f.
 87 Standard query 0x0002 A 360.com
244 Standard query response 0x0002 A 360.com A 104.192.110.203 NS dns4.360
 87 Standard query 0x0003 AAAA 360.com
148 Standard query response 0x0003 AAAA 360.com SOA dns1.360safe.com
```

```
> User Datagram Protocol, Src Port: 55481, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v rednet.cn: type AAAA, class IN
        Name: rednet.cn
        [Name Length: 9]
        [Label Count: 2]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    [Response In: 23]
```

- Type of DNS query : AAAA
- The query message doesn’t contain any answers.

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



```
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.
152 Standard query response 0x0001 No such name PT
 90 Standard query 0x0002 A amrita.edu
106 Standard query response 0x0002 A amrita.edu A
 90 Standard query 0x0003 AAAA amrita.edu
139 Standard query response 0x0003 AAAA amrita.edu
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.
152 Standard query response 0x0001 No such name PT
 89 Standard query 0x0002 A rednet.cn
166 Standard query response 0x0002 A rednet.cn A 1
 89 Standard query 0x0003 AAAA rednet.cn
209 Standard query response 0x0003 AAAA rednet.cn
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.
152 Standard query response 0x0001 No such name PT
 87 Standard query 0x0002 A 360.com
244 Standard query response 0x0002 A 360.com A 104
 87 Standard query 0x0003 AAAA 360.com
148 Standard query response 0x0003 AAAA 360.com SO
152 Standard query 0x0001 PTR e.b.c.9.5.4.e.f.f.f.
152 Standard query response 0x0001 No such name PT
 90 Standard query 0x0002 A google.com
106 Standard query response 0x0002 A google.com A
 90 Standard query 0x0003 AAAA google.com
```

```
Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  Queries
      rednet.cn: type AAAA, class IN
          Name: rednet.cn
          [Name Length: 9]
          [Label Count: 2]
          Type: AAAA (IPv6 Address) (28)
          Class: IN (0x0001)
  Answers
      rednet.cn: type CNAME, class IN, cname dnspod-vip4.beian.mydnspod.net
          Name: rednet.cn
          Type: CNAME (Canonical NAME for an alias) (5)
          Class: IN (0x0001)
          Time to live: 600 (10 minutes)
          Data length: 32
          CNAME: dnspod-vip4.beian.mydnspod.net
  Authoritative nameservers
```

- 1 answer is provided with respect to the DNS Query.
- Each of the answers contains information about the,
    - Name of the host
    - Type of address
    - Class
    - Time to Live (TTL)
    - Data length
    - CNAME

Thankyou!!