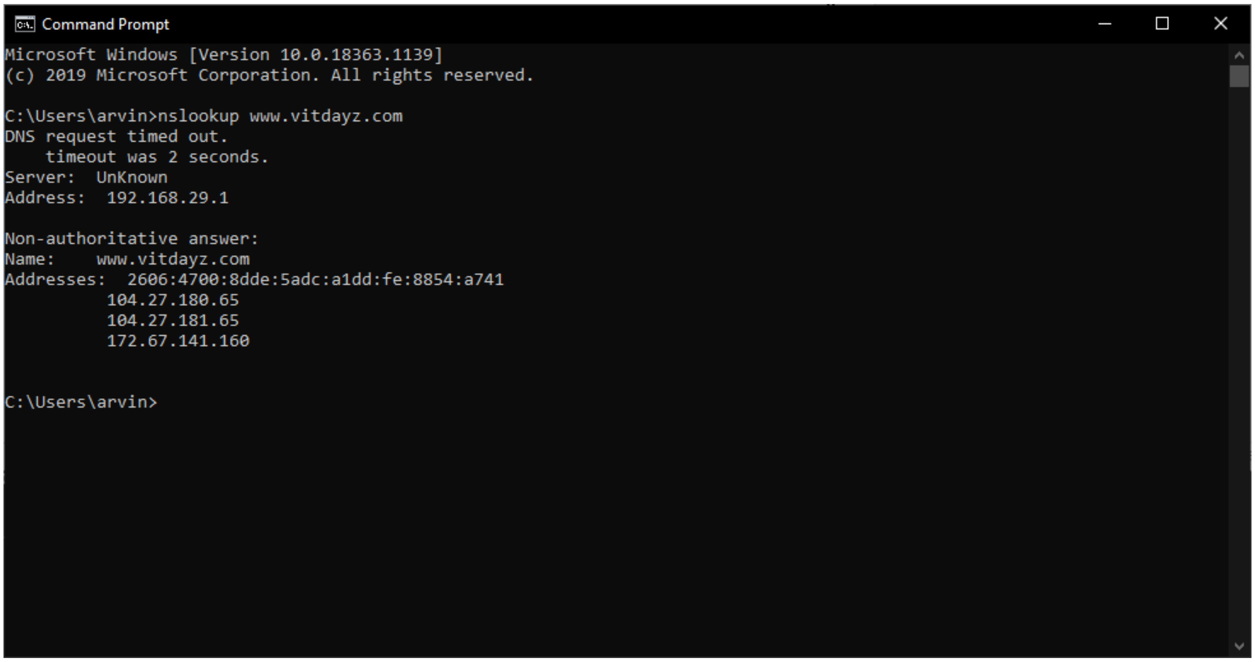
CSE1004 – LAB SUBMISSION 11B – 21/10/2020
Done by: ARVIND C B 19BCE1221
Faculty: Dr. Kanchana Devi V

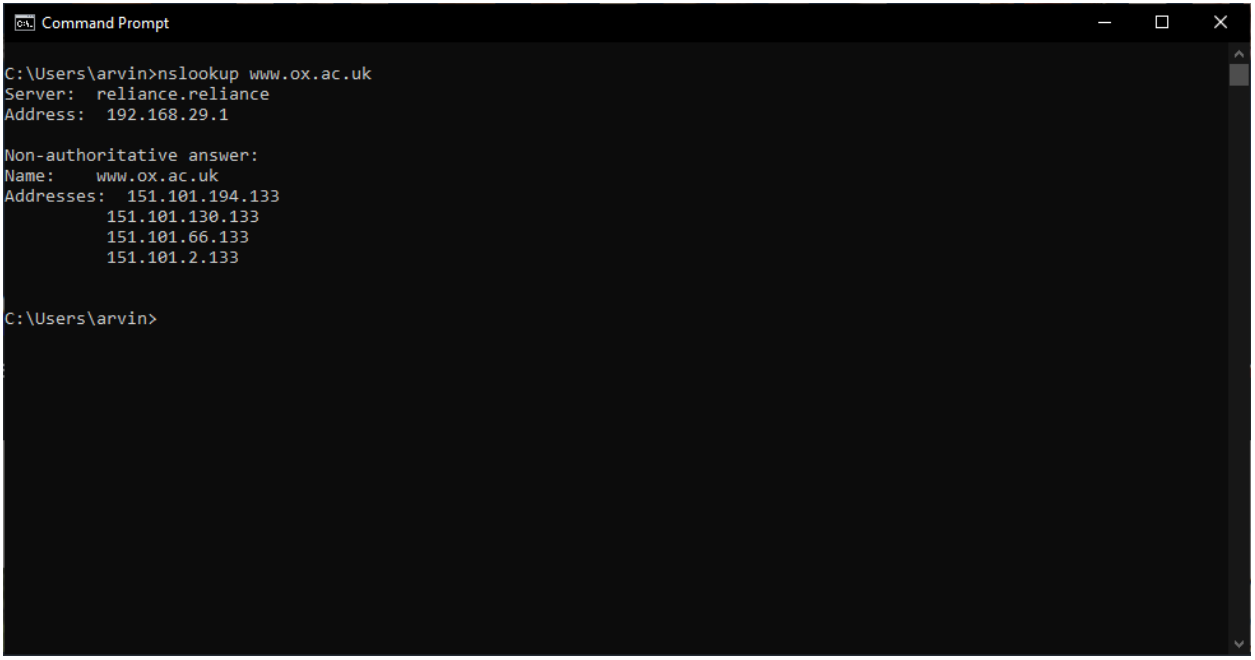
For questions with websites, as instructed I have used the website I am working with (www.vitdayz.com). For a few questions I have used chennai.vit.ac.in and vit.ac.in

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?



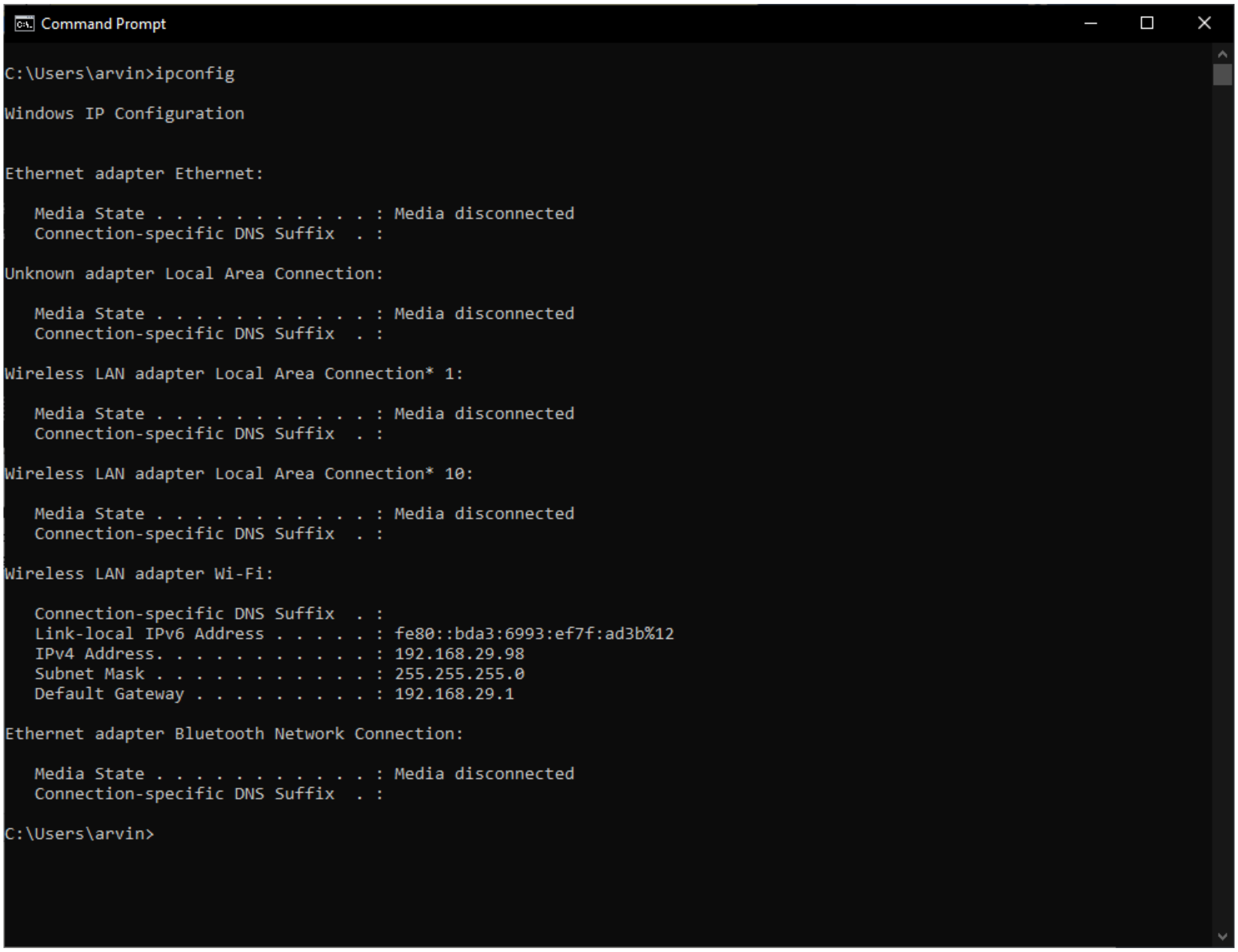
```
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\arvin>nslookup www.vitdayz.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.29.1

Non-authoritative answer:
Name:    www.vitdayz.com
Addresses:  2606:4700:8dde:5adc:a1dd:fe:8854:a741
          104.27.180.65
          104.27.181.65
          172.67.141.160


C:\Users\arvin>
```

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.



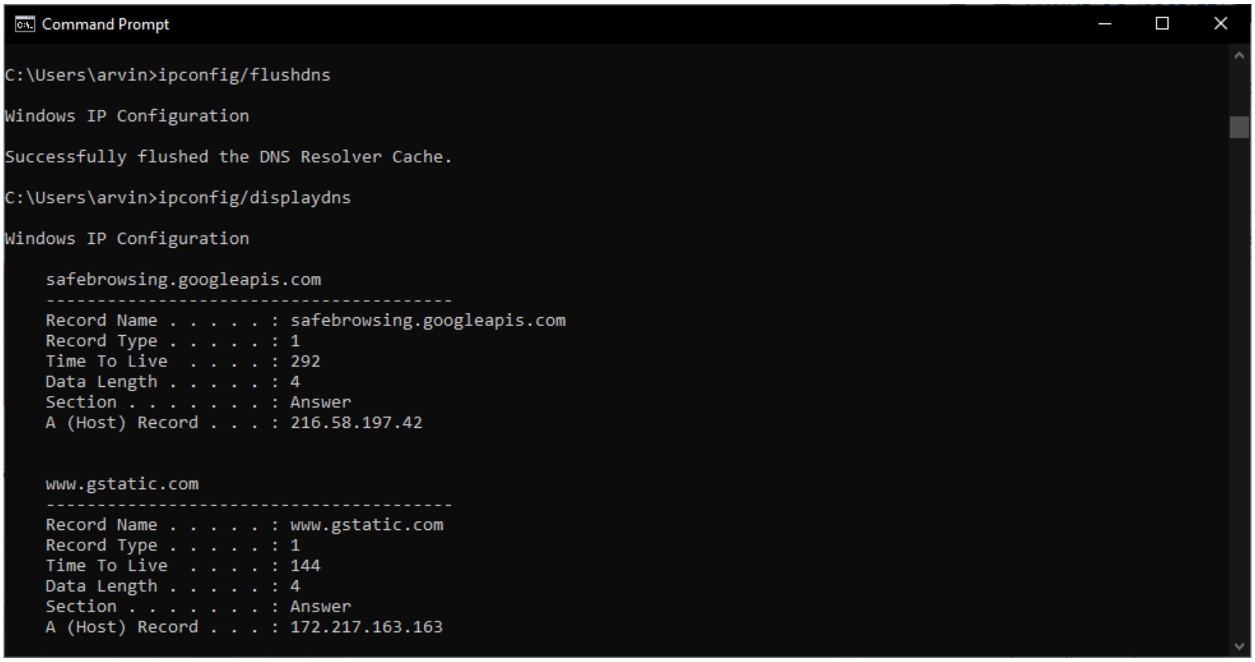
```
C:\Users\arvin>nslookup www.ox.ac.uk
Server:  reliance.reliance
Address:  192.168.29.1

Non-authoritative answer:
Name:    www.ox.ac.uk
Addresses:  151.101.194.133
          151.101.130.133
          151.101.66.133
          151.101.2.133


C:\Users\arvin>
```

ipconfig



```
C:\Users\arvin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bda3:6993:ef7f:ad3b%12
   IPv4 Address. . . . . . . . . . . : 192.168.29.98
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.29.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\arvin>
```

ipconfig/flushdns and ipconfig/displaydns



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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\arvin>ipconfig/displaydns

Windows IP Configuration

    safebrowsing.googleapis.com
    ----------------------------------------
    Record Name . . . . . : safebrowsing.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 292
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 216.58.197.42


    www.gstatic.com
    ----------------------------------------
    Record Name . . . . . : www.gstatic.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 144
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 172.217.163.163
```

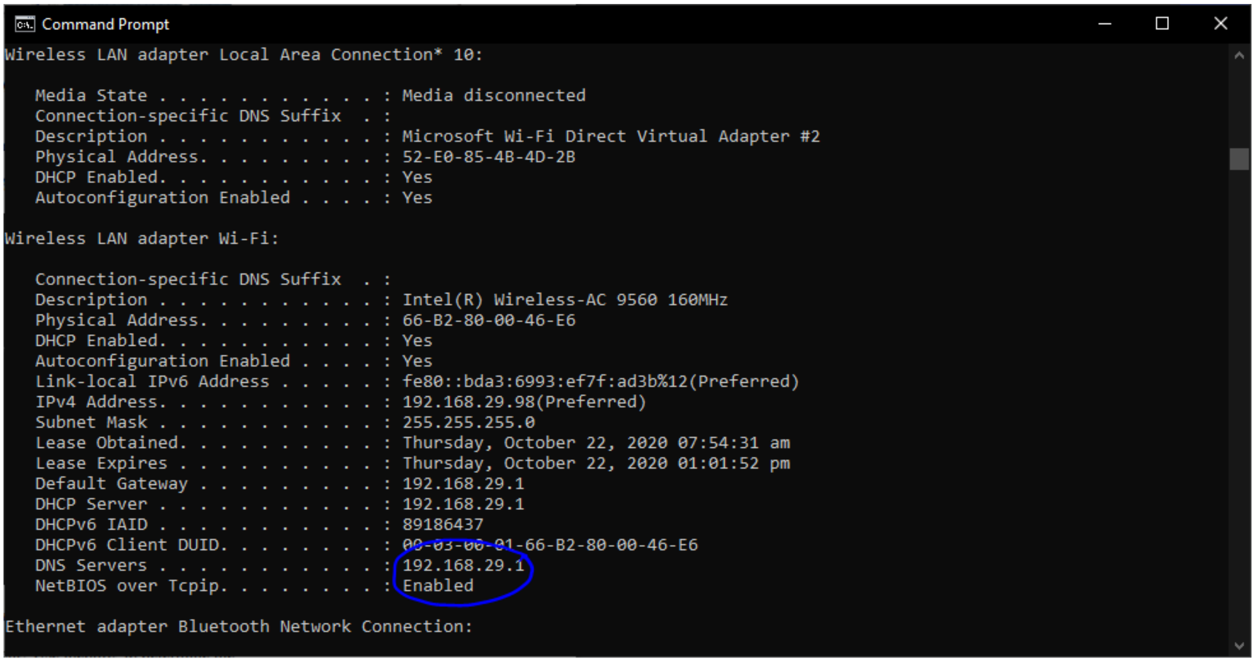
3. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Ans. They are sent over UDP

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

Ans. The destination port for the DNS query is 53 and the source port of the DNS response is 53.

5. 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?



```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 52-E0-85-4B-4D-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 66-B2-80-00-46-E6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::bda3:6993:ef7f:ad3b%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.29.98(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, October 22, 2020 07:54:31 am
   Lease Expires . . . . . . . . . . : Thursday, October 22, 2020 01:01:52 pm
   Default Gateway . . . . . . . . . : 192.168.29.1
   DHCP Server . . . . . . . . . . . : 192.168.29.1
   DHCPv6 IAID . . . . . . . . . . . : 89186437
   DHCPv6 Client DUID. . . . . . . . : 00-03-00-01-66-B2-80-00-46-E6
   DNS Servers . . . . . . . . . . . : 192.168.29.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
```

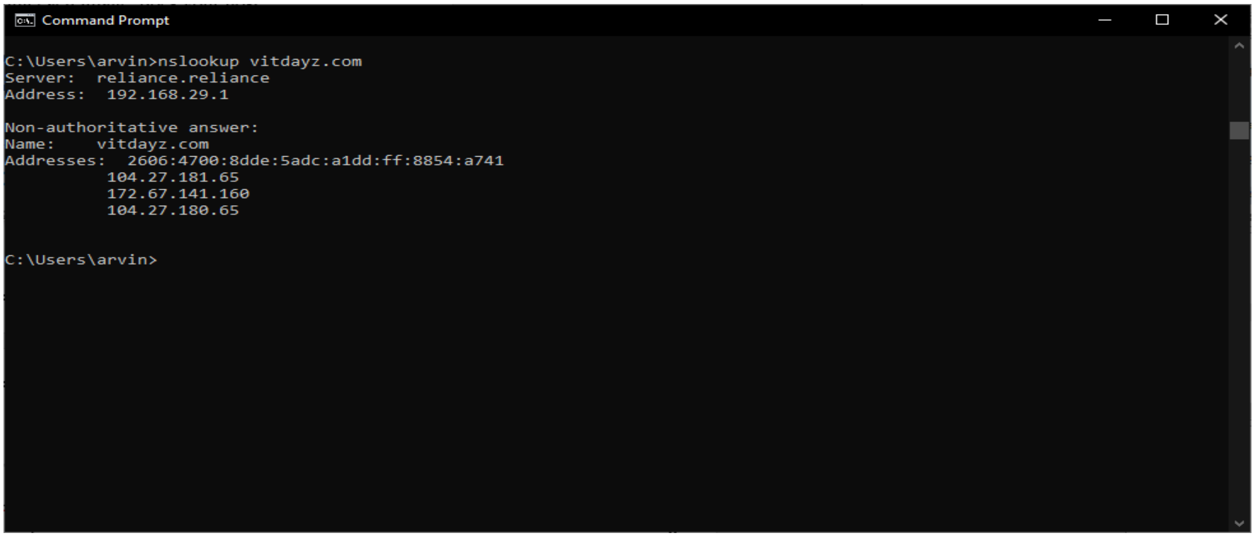
DNS Server = 192.168.29.1

The DNS Server is 192.168.29.1

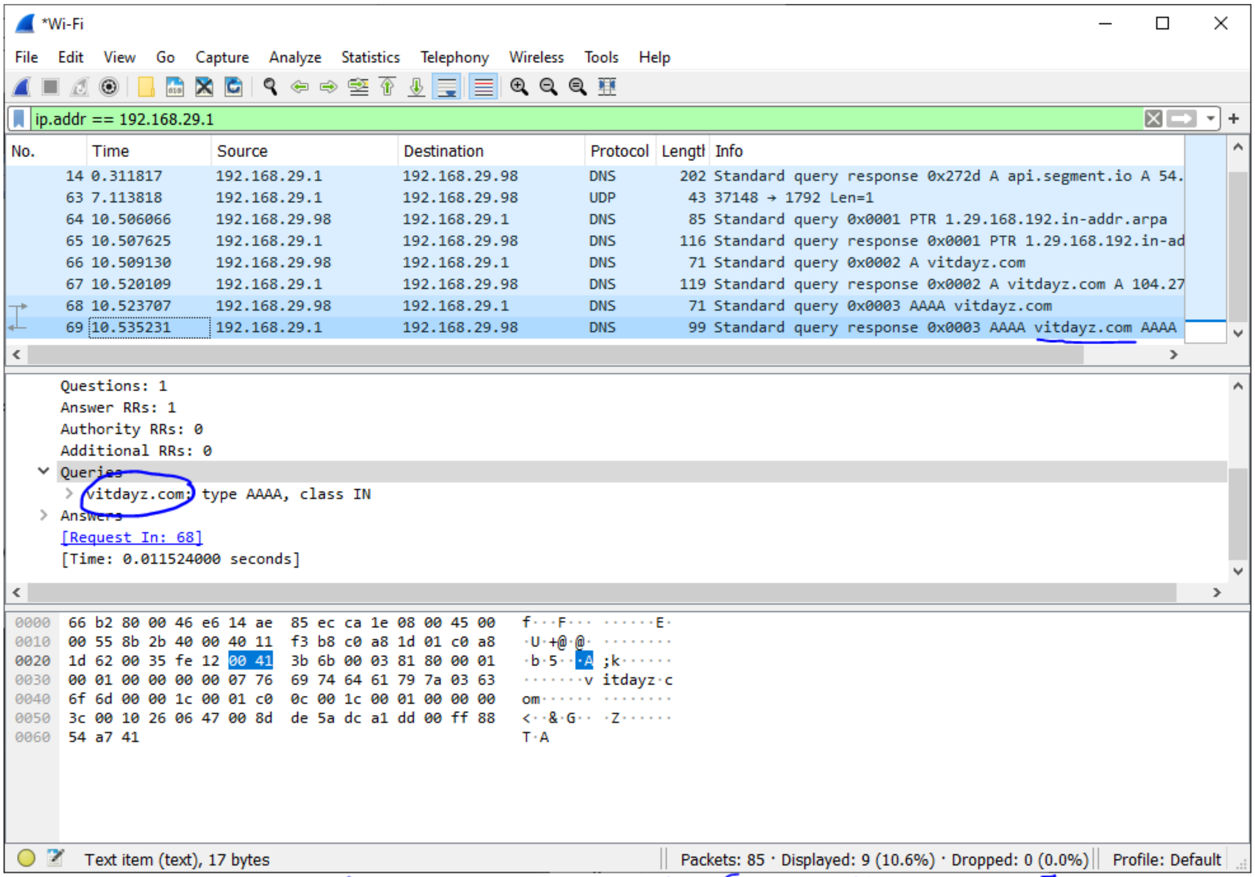
6. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Ans. Type A, does not contain answers

- Start packet capture.
- Do an nslookup on www.mit.edu
- Stop packet capture.



```
C:\Users\arvin>nslookup vitdayz.com
Server:  reliance.reliance
Address:  192.168.29.1

Non-authoritative answer:
Name:    vitdayz.com
Addresses:  2606:4700:8dde:5adc:a1dd:ff:8854:a741
          104.27.181.65
          172.67.141.160
          104.27.180.65


C:\Users\arvin>
```



ip.addr == 192.168.29.1

No.	Time	Source	Destination	Protocol	Lengtl	Info
14	0.311817	192.168.29.1	192.168.29.98	DNS	202	Standard query response 0x272d A api.segment.io A 54.
63	7.113818	192.168.29.1	192.168.29.98	UDP	43	37148 → 1792 Len=1
64	10.506066	192.168.29.98	192.168.29.1	DNS	85	Standard query 0x0001 PTR 1.29.168.192.in-addr.arpa
65	10.507625	192.168.29.1	192.168.29.98	DNS	116	Standard query response 0x0001 PTR 1.29.168.192.in-ad
66	10.509130	192.168.29.98	192.168.29.1	DNS	71	Standard query 0x0002 A vitdayz.com
67	10.520109	192.168.29.1	192.168.29.98	DNS	119	Standard query response 0x0002 A vitdayz.com A 104.27
68	10.523707	192.168.29.98	192.168.29.1	DNS	71	Standard query 0x0003 AAAA vitdayz.com
69	10.535231	192.168.29.1	192.168.29.98	DNS	99	Standard query response 0x0003 AAAA vitdayz.com AAAA

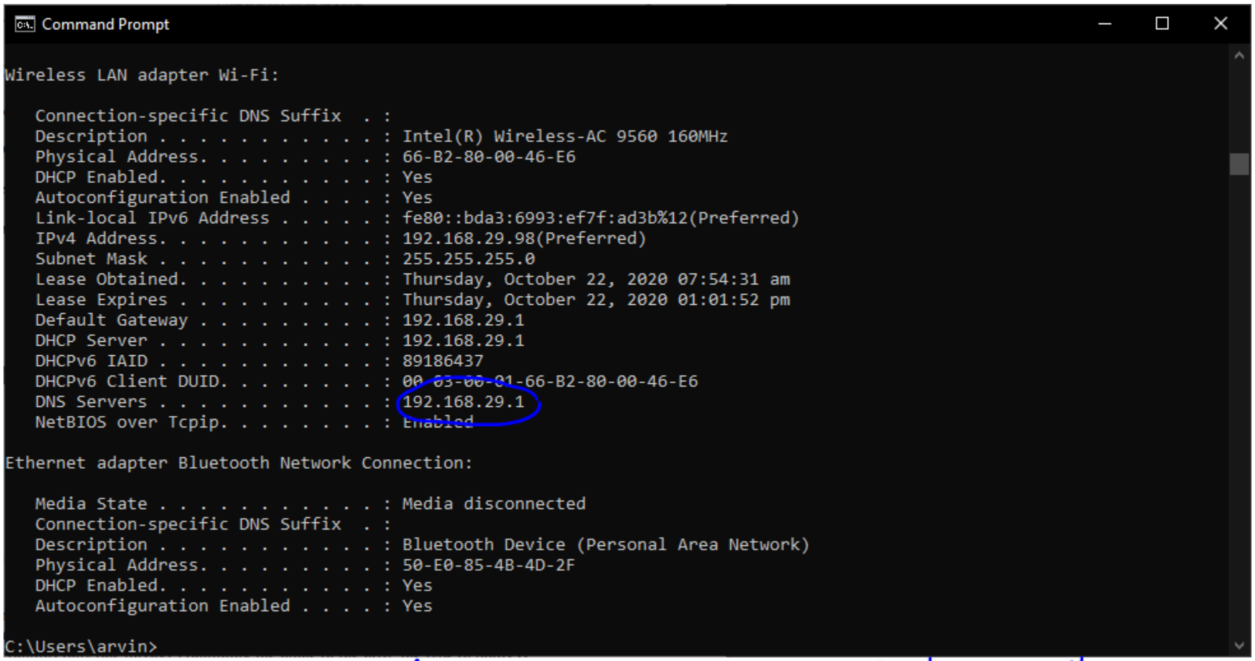
```
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ∨ Queries
    > vitdayz.com: type AAAA, class IN
  > Answers
    [Request In: 68]
    [Time: 0.011524000 seconds]
```

```
0000  66 b2 80 00 46 e6 14 ae  85 ec ca 1e 08 00 45 00   f···F··· ······E·
0010  00 55 8b 2b 40 00 40 11  f3 b8 c0 a8 1d 01 c0 a8   ·U·+@·@· ········
0020  1d 62 00 35 fe 12 00 41  3b 6b 00 03 81 80 00 01   ·b·5···A ;k······
0030  00 01 00 00 00 00 07 76  69 74 64 61 79 7a 03 63   ·······v itdayz·c
0040  6f 6d 00 00 1c 00 01 c0  0c 00 1c 00 01 00 00 00   om······ ········
0050  3c 00 10 26 06 47 00 8d  de 5a dc a1 dd 00 ff 88   <··&·G·· ·Z······
0060  54 a7 41                                           T·A
```

Text item (text), 17 bytes || Packets: 85 · Displayed: 9 (10.6%) · Dropped: 0 (0.0%) || Profile: Default

After nslookup in Command prompt. [www.vitdayz.com]

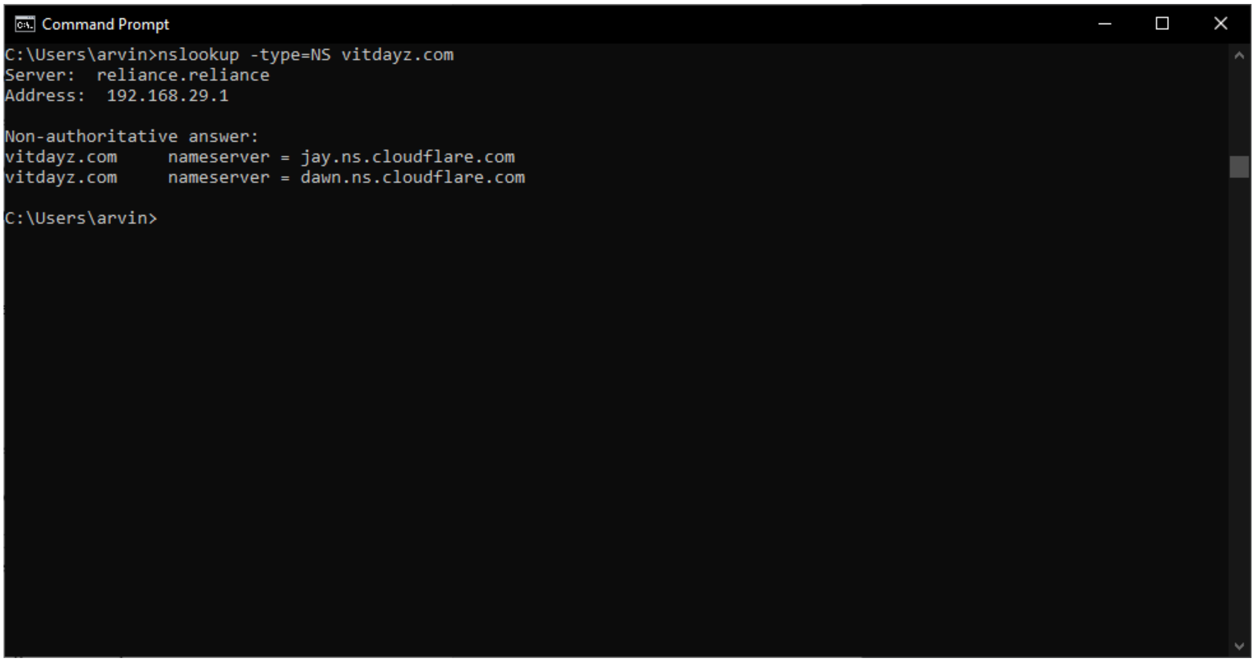
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 66-B2-80-00-46-E6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::bda3:6993:ef7f:ad3b%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.29.98(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, October 22, 2020 07:54:31 am
   Lease Expires . . . . . . . . . . : Thursday, October 22, 2020 01:01:52 pm
   Default Gateway . . . . . . . . . : 192.168.29.1
   DHCP Server . . . . . . . . . . . : 192.168.29.1
   DHCPv6 IAID . . . . . . . . . . . : 89186437
   DHCPv6 Client DUID. . . . . . . . : 00-03-00-01-66-B2-80-00-46-E6
   DNS Servers . . . . . . . . . . . : 192.168.29.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 50-E0-85-4B-4D-2F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\arvin>
```

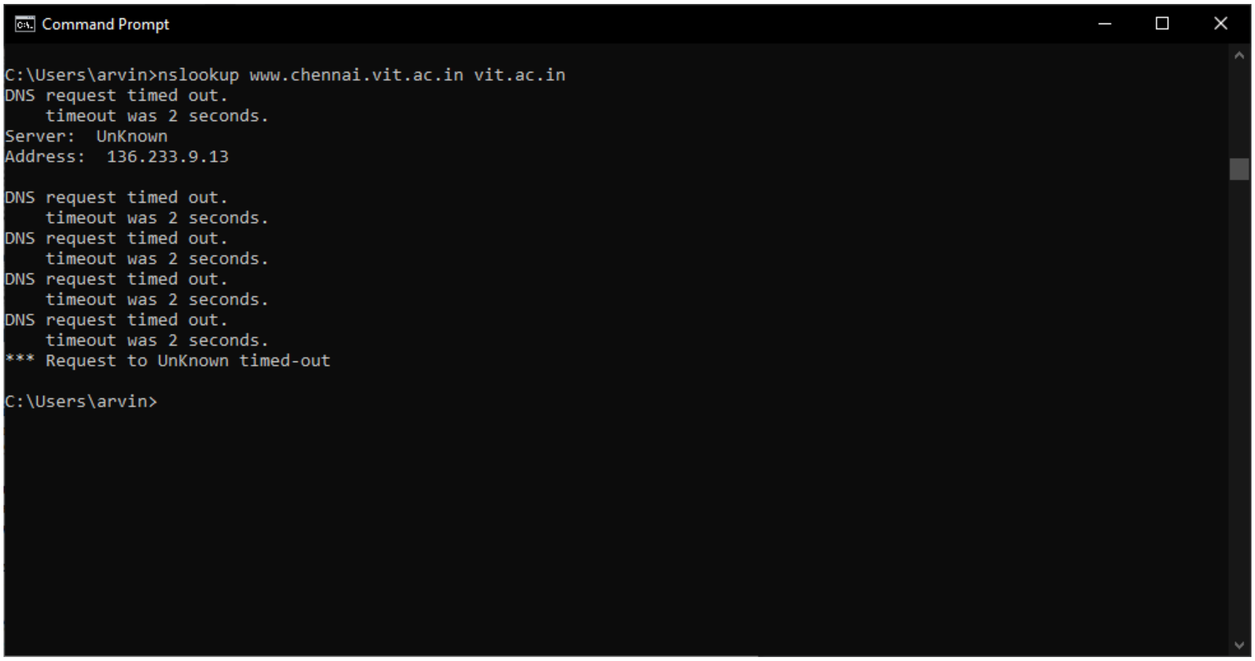
The IP address to which DNS Query will be Sent : 192.168.29.1

nslookup -type=NS vitdayz.com



```
C:\Users\arvin>nslookup -type=NS vitdayz.com
Server:  reliance.reliance
Address:  192.168.29.1

Non-authoritative answer:
vitdayz.com     nameserver = jay.ns.cloudflare.com
vitdayz.com     nameserver = dawn.ns.cloudflare.com

C:\Users\arvin>
```

```
nslookup www.chennai.vit.ac.in vit.ac.in
```



```
C:\Users\arvin>nslookup www.chennai.vit.ac.in vit.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  136.233.9.13

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\arvin>
```