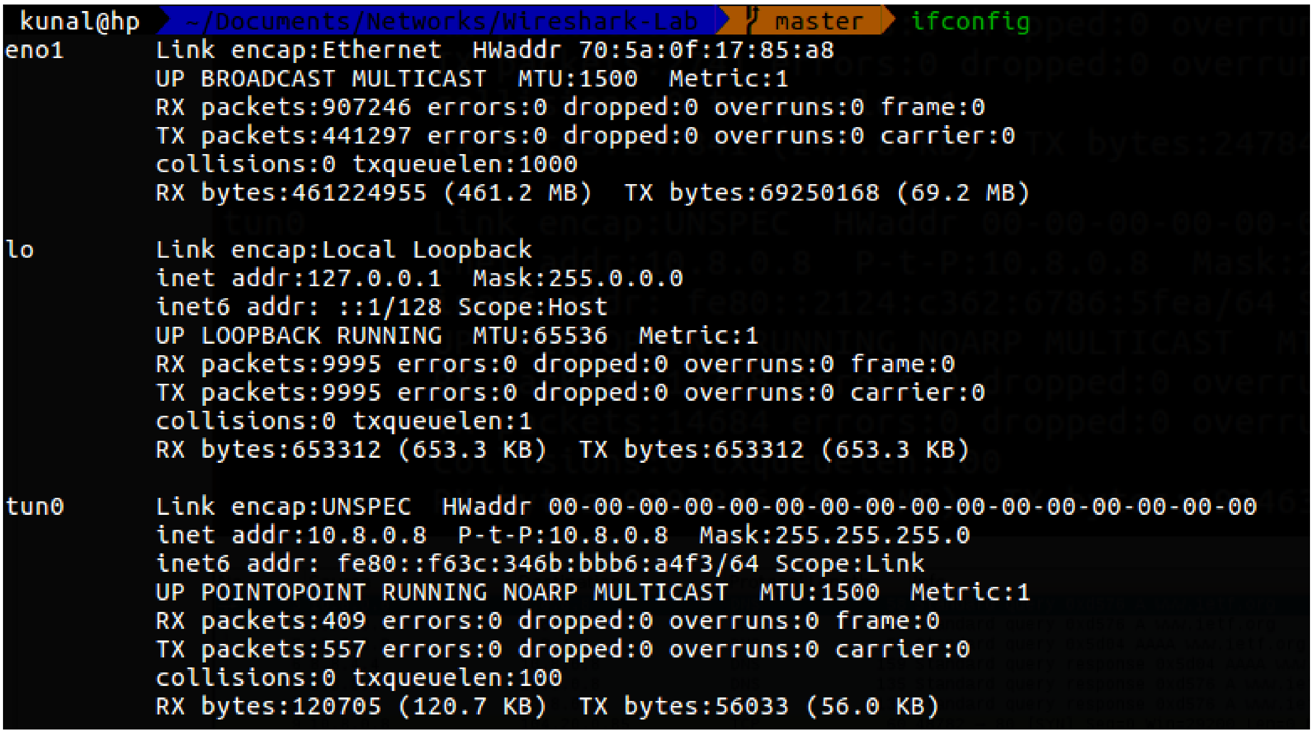
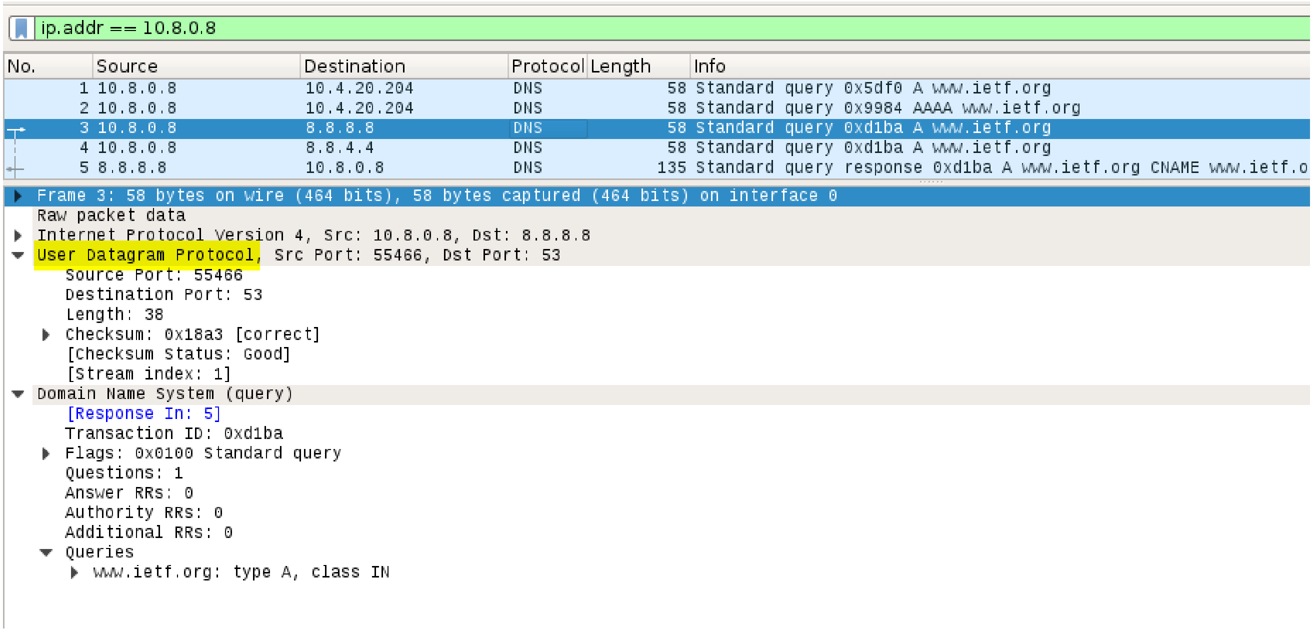
DNS

A. Tracing DNS with Wireshark



```
 kunal@hp  ~/Documents/Networks/Wireshark-Lab  master  ifconfig
eno1      Link encap:Ethernet  HWaddr 70:5a:0f:17:85:a8
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:907246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:441297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:461224955 (461.2 MB)  TX bytes:69250168 (69.2 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:9995 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9995 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:653312 (653.3 KB)  TX bytes:653312 (653.3 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.8  P-t-P:10.8.0.8  Mask:255.255.255.0
          inet6 addr: fe80::f63c:346b:bbb6:a4f3/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:409 errors:0 dropped:0 overruns:0 frame:0
          TX packets:557 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:120705 (120.7 KB)  TX bytes:56033 (56.0 KB)
```

Figure 1: Output of ifconfig, ip address is 10.8.0.8

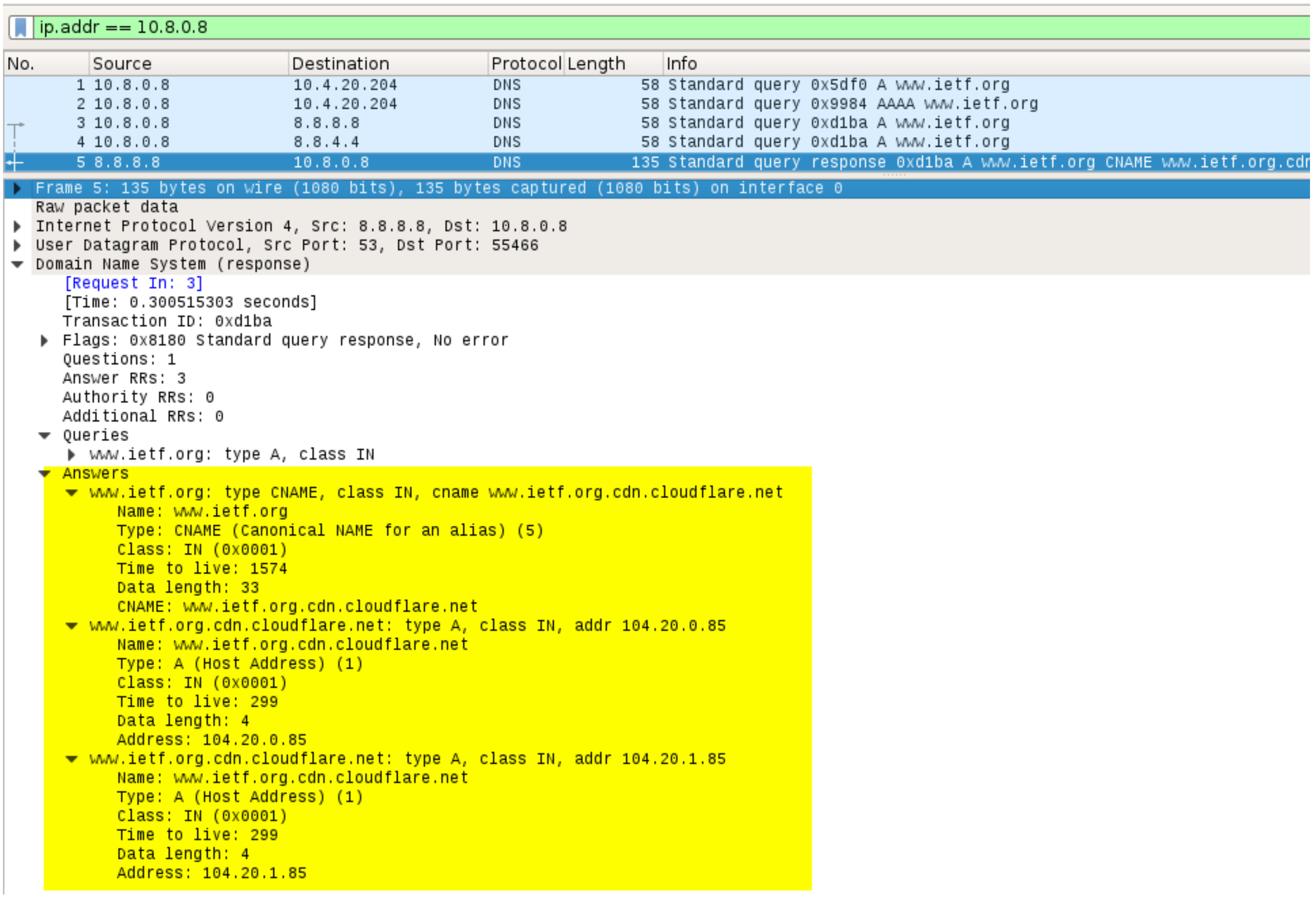


```
ip.addr == 10.8.0.8

No.  Source      Destination   Protocol Length Info
   1 10.8.0.8    10.4.20.204   DNS          58 Standard query 0x5df0 A www.ietf.org
   2 10.8.0.8    10.4.20.204   DNS          58 Standard query 0x9984 AAAA www.ietf.org
   3 10.8.0.8    8.8.8.8       DNS          58 Standard query 0xd1ba A www.ietf.org
   4 10.8.0.8    8.8.4.4       DNS          58 Standard query 0xd1ba A www.ietf.org
   5 8.8.8.8     10.8.0.8      DNS         135 Standard query response 0xd1ba A www.ietf.org CNAME www.ietf.o

Frame 3: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
Raw packet data
Internet Protocol Version 4, Src: 10.8.0.8, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 55466, Dst Port: 53
    Source Port: 55466
    Destination Port: 53
    Length: 38
    Checksum: 0x18a3 [correct]
    [Checksum Status: Good]
    [Stream index: 1]
Domain Name System (query)
    [Response In: 5]
    Transaction ID: 0xd1ba
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
```

Figure 2: DNS Query message to http://www.ietf.org

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

   Answer : They are sent over **UDP**.

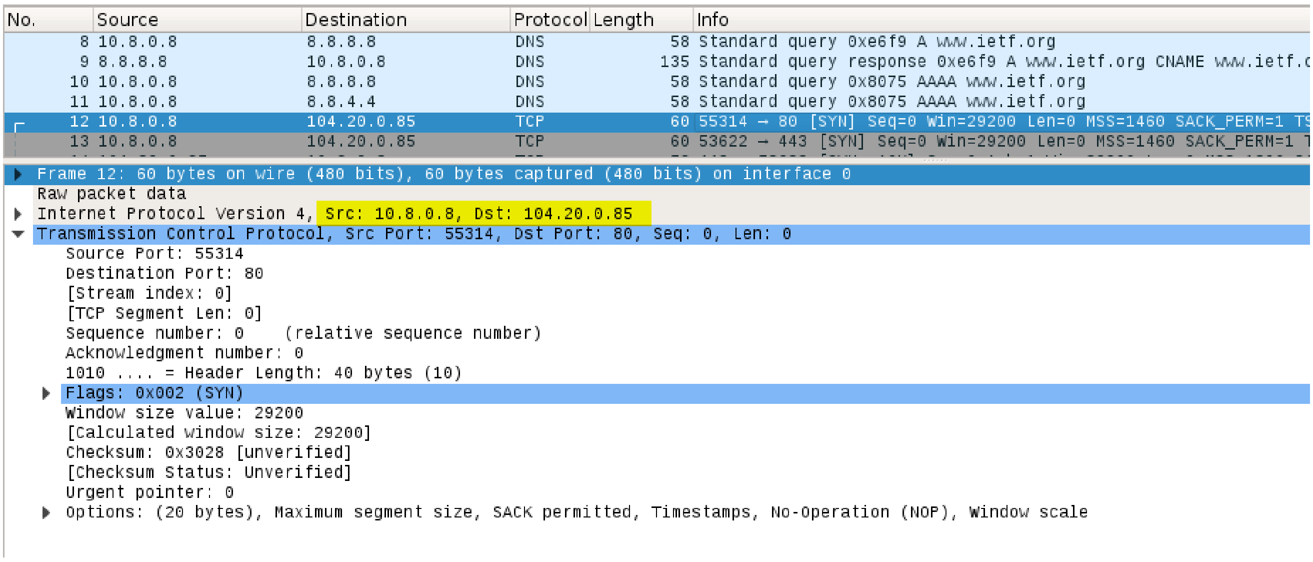


```
ip.addr == 10.8.0.8

No.     Source          Destination     Protocol Length Info
      1 10.8.0.8        10.4.20.204     DNS          58 Standard query 0x5df0 A www.ietf.org
      2 10.8.0.8        10.4.20.204     DNS          58 Standard query 0x9984 AAAA www.ietf.org
      3 10.8.0.8        8.8.8.8         DNS          58 Standard query 0xd1ba A www.ietf.org
      4 10.8.0.8        8.8.4.4         DNS          58 Standard query 0xd1ba A www.ietf.org
      5 8.8.8.8         10.8.0.8        DNS         135 Standard query response 0xd1ba A www.ietf.org CNAME www.ietf.org.cdr

Frame 5: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
Raw packet data
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.8.0.8
User Datagram Protocol, Src Port: 53, Dst Port: 55466
Domain Name System (response)
    [Request In: 3]
    [Time: 0.300515303 seconds]
    Transaction ID: 0xd1ba
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
    Answers
        www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
            Name: www.ietf.org
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 1574
            Data length: 33
            CNAME: www.ietf.org.cdn.cloudflare.net
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
            Name: www.ietf.org.cdn.cloudflare.net
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 299
            Data length: 4
            Address: 104.20.0.85
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
            Name: www.ietf.org.cdn.cloudflare.net
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 299
            Data length: 4
            Address: 104.20.1.85
```

Figure 3: DNS response message from http://www.ietf.org

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

   Answer : There were **3 answers** containing information about the **name of the host, the type of address, class, the TTL, the data length and the IP address**.



```
No.     Source          Destination     Protocol Length Info
      8 10.8.0.8        8.8.8.8         DNS          58 Standard query 0xe6f9 A www.ietf.org
      9 8.8.8.8         10.8.0.8        DNS         135 Standard query response 0xe6f9 A www.ietf.org CNAME www.ietf.c
     10 10.8.0.8        8.8.8.8         DNS          58 Standard query 0x8075 AAAA www.ietf.org
     11 10.8.0.8        8.8.4.4         DNS          58 Standard query 0x8075 AAAA www.ietf.org
     12 10.8.0.8        104.20.0.85     TCP          60 55314 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
     13 10.8.0.8        104.20.0.85     TCP          60 53622 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 T

Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Raw packet data
Internet Protocol Version 4, Src: 10.8.0.8, Dst: 104.20.0.85
Transmission Control Protocol, Src Port: 55314, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 55314
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
    Flags: 0x002 (SYN)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x3028 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

Figure 4: TCP SYN packet sent by my host

3. **Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

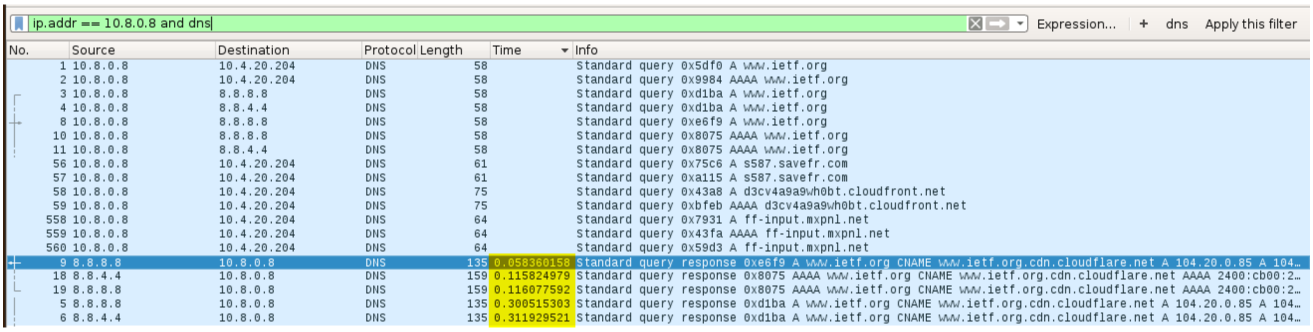
Answer : The first SYN packet was sent to **104.20.0.85** which corresponds to the first IP address provided in the DNS response message.

4. **This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

   Answer : No, host doesn't issue queries for each image, it issues mutiple DNS requests.

5. **Sort the queries according to their DNS response time. Attach screenshot along with it.**

   Answer :

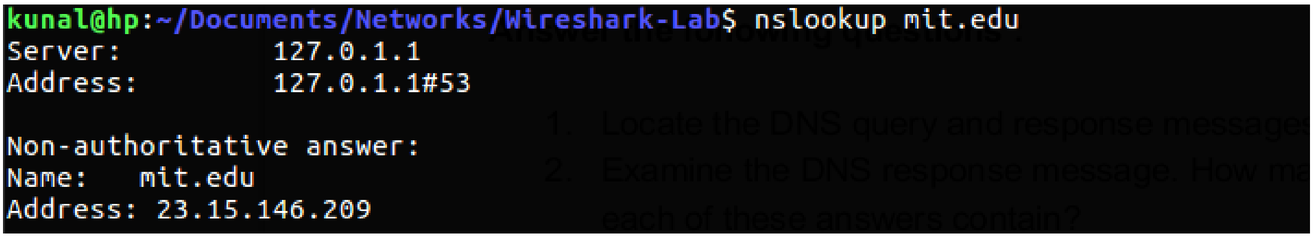


ip.addr == 10.8.0.8 and dns

No.	Source	Destination	Protocol	Length	Time	Info
1	10.8.0.8	10.4.20.204	DNS	58		Standard query 0x5df0 A www.ietf.org
2	10.8.0.8	10.4.20.204	DNS	58		Standard query 0x9984 AAAA www.ietf.org
3	10.8.0.8	8.8.8.8	DNS	58		Standard query 0xd1ba A www.ietf.org
4	10.8.0.8	8.8.4.4	DNS	58		Standard query 0xd1ba A www.ietf.org
8	10.8.0.8	8.8.8.8	DNS	58		Standard query 0xe6f9 A www.ietf.org
10	10.8.0.8	8.8.8.8	DNS	58		Standard query 0x8075 AAAA www.ietf.org
11	10.8.0.8	8.8.4.4	DNS	58		Standard query 0x8075 AAAA www.ietf.org
56	10.8.0.8	10.4.20.204	DNS	61		Standard query 0x75c6 A s587.savefr.com
57	10.8.0.8	10.4.20.204	DNS	61		Standard query 0xa115 A s587.savefr.com
58	10.8.0.8	10.4.20.204	DNS	75		Standard query 0x43a8 A d3cv4a9a9wh0bt.cloudfront.net
59	10.8.0.8	10.4.20.204	DNS	75		Standard query 0xbfeb AAAA d3cv4a9a9wh0bt.cloudfront.net
558	10.8.0.8	10.4.20.204	DNS	64		Standard query 0x7931 A ff-input.mxpnl.net
559	10.8.0.8	10.4.20.204	DNS	64		Standard query 0x43fa AAAA ff-input.mxpnl.net
560	10.8.0.8	10.4.20.204	DNS	64		Standard query 0x59d3 A ff-input.mxpnl.net
9	8.8.8.8	10.8.0.8	DNS	135	0.058360158	Standard query response 0xe6f9 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104…
18	8.8.4.4	10.8.0.8	DNS	159	0.115824979	Standard query response 0x8075 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2400:cb00:2…
19	8.8.8.8	10.8.0.8	DNS	159	0.116077592	Standard query response 0x8075 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2400:cb00:2…
5	8.8.8.8	10.8.0.8	DNS	135	0.300515303	Standard query response 0xd1ba A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104…
6	8.8.4.4	10.8.0.8	DNS	135	0.311929521	Standard query response 0xd1ba A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104…

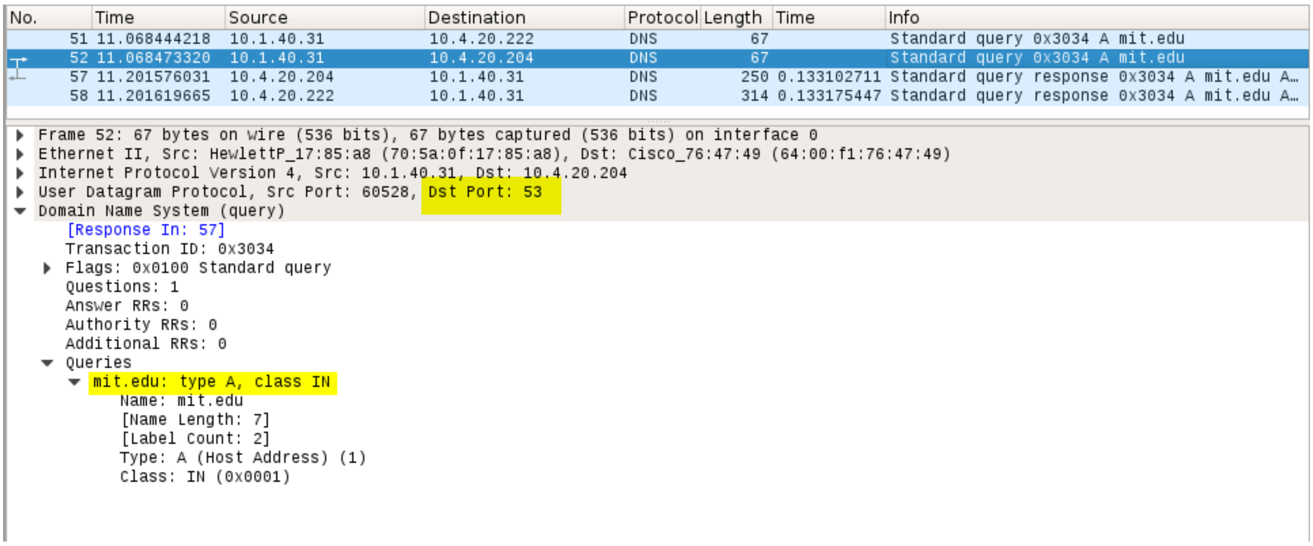
Figure 5: Sorted queries according to their DNS response time

B. Tracing DNS with nslookup



```
kunal@hp:~/Documents/Networks/Wireshark-Lab$ nslookup mit.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   mit.edu
Address: 23.15.146.209
```

Figure 6: nslookup Output



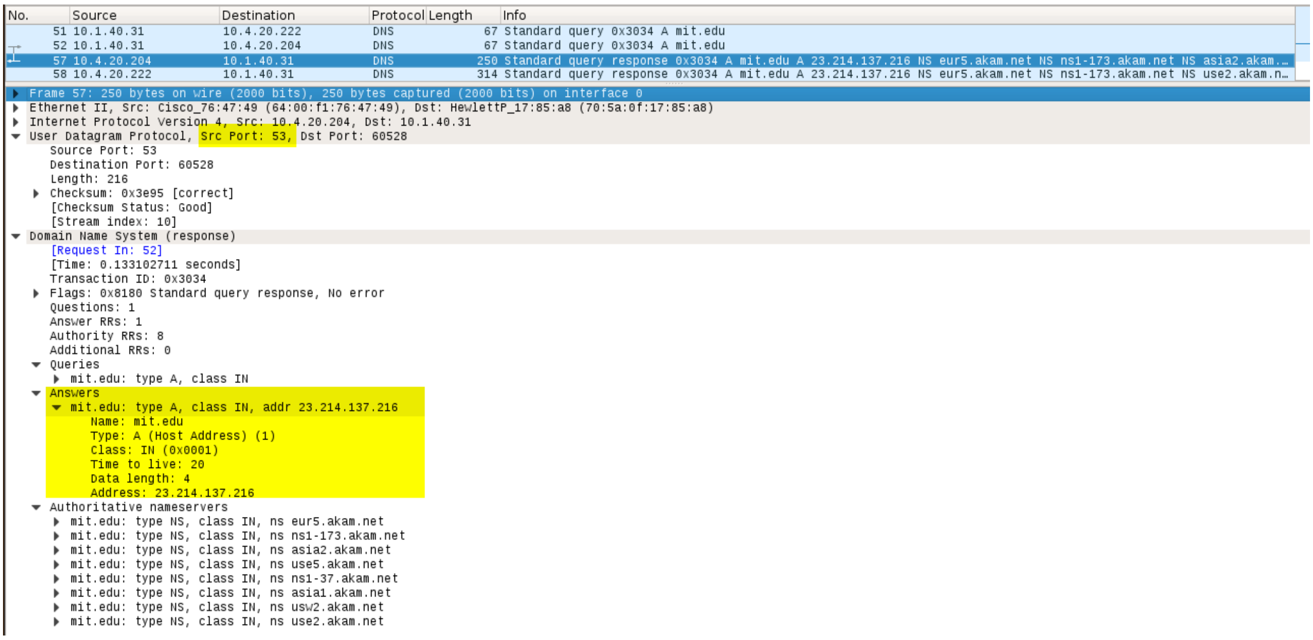
No.	Time	Source	Destination	Protocol	Length	Time	Info
51	11.068444218	10.1.40.31	10.4.20.222	DNS	67		Standard query 0x3034 A mit.edu
52	11.068473320	10.1.40.31	10.4.20.204	DNS	67		Standard query 0x3034 A mit.edu
57	11.201576031	10.4.20.204	10.1.40.31	DNS	250	0.133102711	Standard query response 0x3034 A mit.edu A…
58	11.201619665	10.4.20.222	10.1.40.31	DNS	314	0.133175447	Standard query response 0x3034 A mit.edu A…

```
▶ Frame 52: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶ Ethernet II, Src: HewlettP_17:85:a8 (70:5a:0f:17:85:a8), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)
▶ Internet Protocol Version 4, Src: 10.1.40.31, Dst: 10.4.20.204
▶ User Datagram Protocol, Src Port: 60528, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 57]
    Transaction ID: 0x3034
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type A, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Figure 7: DNS Query Message

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

   Answer : The destination port of the DNS query is 53 and the source port of the DNS response is 53.



```
No.   Source          Destination     Protocol Length  Info
   51 10.1.40.31      10.4.20.222     DNS          67 Standard query 0x3034 A mit.edu
   52 10.1.40.31      10.4.20.204     DNS          67 Standard query 0x3034 A mit.edu
   57 10.4.20.204     10.1.40.31      DNS         250 Standard query response 0x3034 A mit.edu A 23.214.137.216 NS eur5.akam.net NS ns1-173.akam.net NS asia2.akam.…
   58 10.4.20.222     10.1.40.31      DNS         314 Standard query response 0x3034 A mit.edu A 23.214.137.216 NS eur5.akam.net NS ns1-173.akam.net NS use2.akam.n…
▶ Frame 57: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) on interface 0
▶ Ethernet II, Src: Cisco_76:47:49 (64:00:f1:76:47:49), Dst: HewlettP_17:85:a8 (70:5a:0f:17:85:a8)
▶ Internet Protocol Version 4, Src: 10.4.20.204, Dst: 10.1.40.31
▼ User Datagram Protocol, Src Port: 53, Dst Port: 60528
     Source Port: 53
     Destination Port: 60528
     Length: 216
   ▶ Checksum: 0x3e95 [correct]
     [Checksum Status: Good]
     [Stream index: 10]
▼ Domain Name System (response)
     [Request In: 52]
     [Time: 0.133102711 seconds]
     Transaction ID: 0x3034
   ▶ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 1
     Authority RRs: 8
     Additional RRs: 0
   ▼ Queries
     ▶ mit.edu: type A, class IN
   ▼ Answers
     ▼ mit.edu: type A, class IN, addr 23.214.137.216
           Name: mit.edu
           Type: A (Host Address) (1)
           Class: IN (0x0001)
           Time to live: 20
           Data length: 4
           Address: 23.214.137.216
   ▼ Authoritative nameservers
     ▶ mit.edu: type NS, class IN, ns eur5.akam.net
     ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
     ▶ mit.edu: type NS, class IN, ns asia2.akam.net
     ▶ mit.edu: type NS, class IN, ns use5.akam.net
     ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
     ▶ mit.edu: type NS, class IN, ns asia1.akam.net
     ▶ mit.edu: type NS, class IN, ns usw2.akam.net
     ▶ mit.edu: type NS, class IN, ns use2.akam.net
```

Figure 8: DNS Response Message

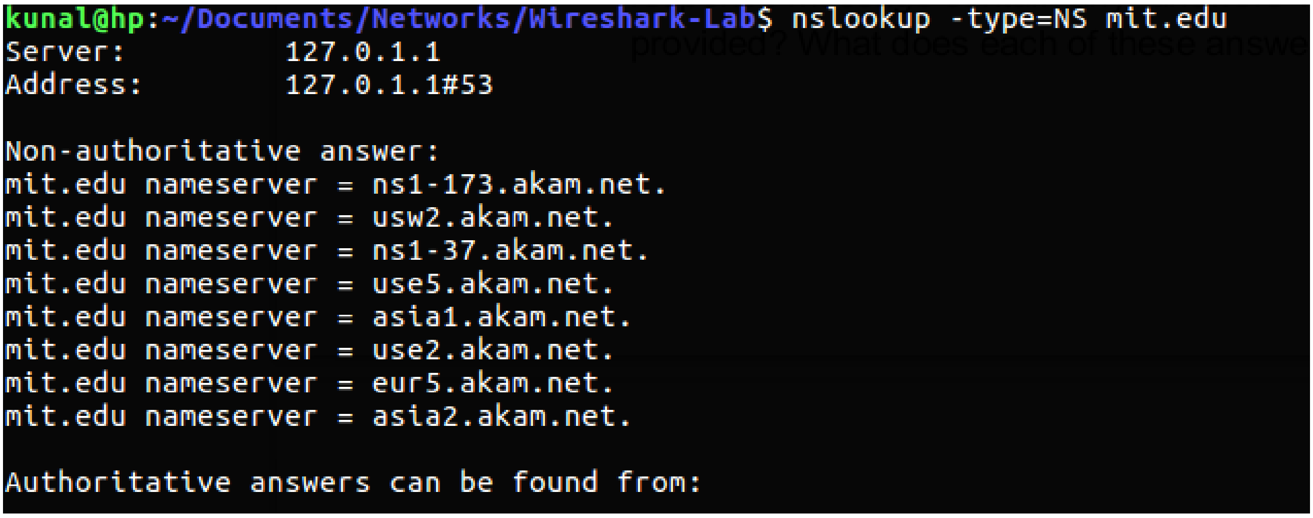
7. **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? If yes, then how many "answers" are provided? What does each of these answers contain?**

   Answer : The query is of **type A**. **No**, it doesn't contain any answers.

8. **Examine the DNS response message. What "Type" of DNS query is it? Does the response message contain any "answers"? If yes, then how many "answers" are provided? What does each of these answers contain?**

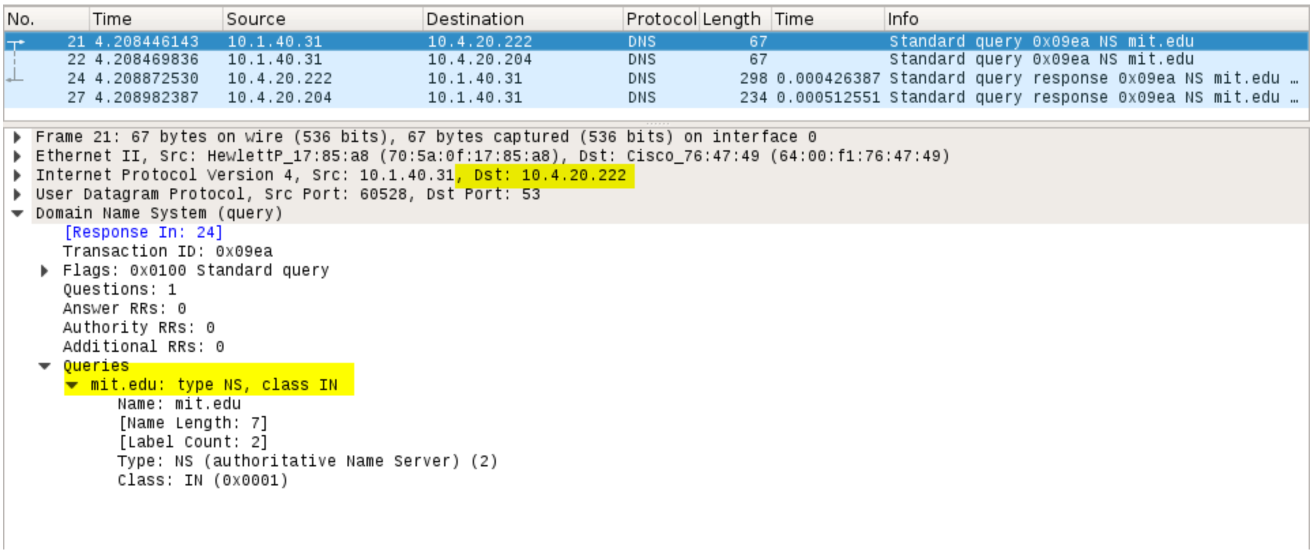
   Answer : The query is of **type A**. **Yes**, the response DNS message contains **one answer** containing the **name of the host, the type of address, the class, TTL, data length and the IP address**.

C. Tracing DNS with nslookup –type=NS



```
kunal@hp:~/Documents/Networks/Wireshark-Lab$ nslookup -type=NS mit.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = asia2.akam.net.

Authoritative answers can be found from:
```

Figure 9: nslookup –type=NS mit.edu Output

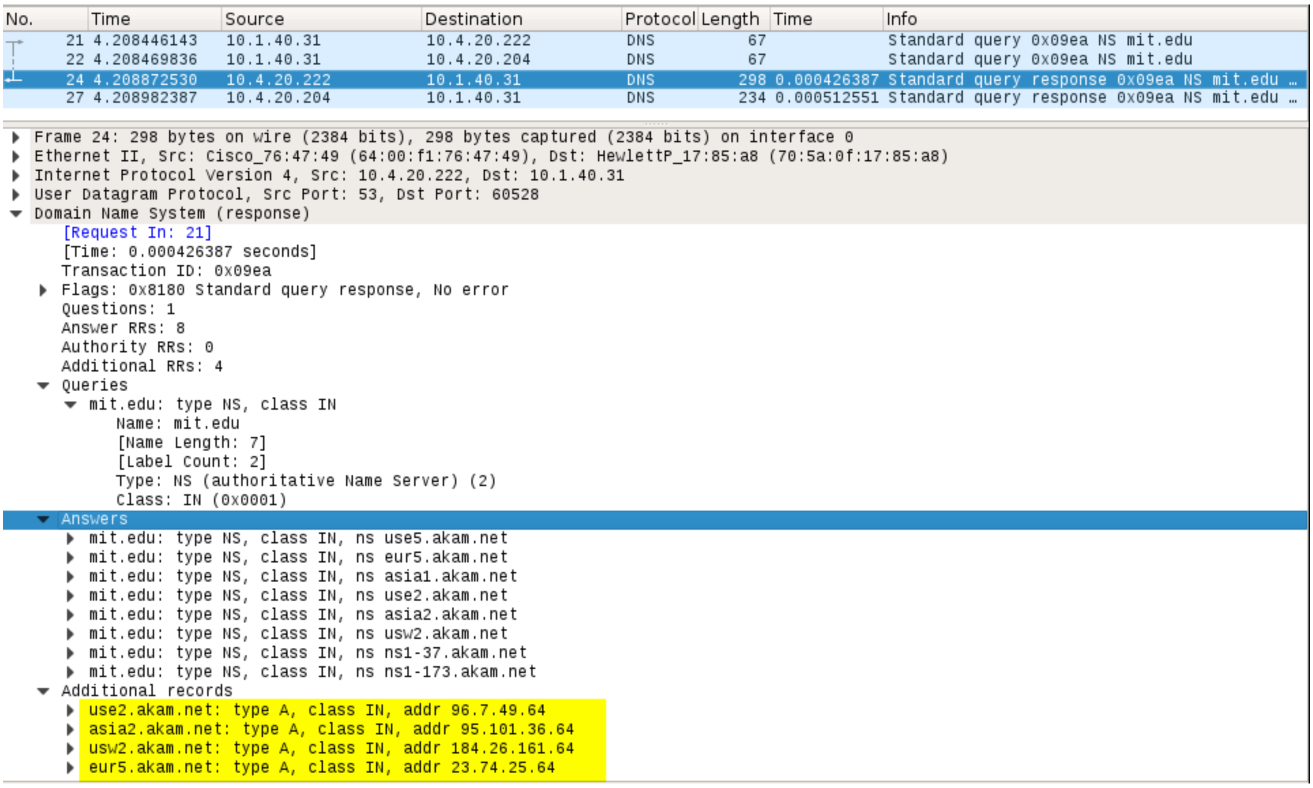


```
No.   Time          Source        Destination   Protocol Length Time         Info
   21 4.208446143   10.1.40.31    10.4.20.222   DNS         67              Standard query 0x09ea NS mit.edu
   22 4.208469836   10.1.40.31    10.4.20.204   DNS         67              Standard query 0x09ea NS mit.edu
   24 4.208872530   10.4.20.222   10.1.40.31    DNS        298 0.000426387  Standard query response 0x09ea NS mit.edu …
   27 4.208982387   10.4.20.204   10.1.40.31    DNS        234 0.000512551  Standard query response 0x09ea NS mit.edu …

▶ Frame 21: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶ Ethernet II, Src: HewlettP_17:85:a8 (70:5a:0f:17:85:a8), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)
▶ Internet Protocol Version 4, Src: 10.1.40.31, Dst: 10.4.20.222
▶ User Datagram Protocol, Src Port: 60528, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 24]
    Transaction ID: 0x09ea
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```

Figure 10: DNS Query Message

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

   Answer : It was sent to 10.4.20.222 which is my default DNS server.



```
No.   Time          Source        Destination   Protocol Length Time         Info
   21 4.208446143   10.1.40.31    10.4.20.222   DNS         67              Standard query 0x09ea NS mit.edu
   22 4.208469836   10.1.40.31    10.4.20.204   DNS         67              Standard query 0x09ea NS mit.edu
   24 4.208872530   10.4.20.222   10.1.40.31    DNS        298 0.000426387  Standard query response 0x09ea NS mit.edu …
   27 4.208982387   10.4.20.204   10.1.40.31    DNS        234 0.000512551  Standard query response 0x09ea NS mit.edu …

▶ Frame 24: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface 0
▶ Ethernet II, Src: Cisco_76:47:49 (64:00:f1:76:47:49), Dst: HewlettP_17:85:a8 (70:5a:0f:17:85:a8)
▶ Internet Protocol Version 4, Src: 10.4.20.222, Dst: 10.1.40.31
▶ User Datagram Protocol, Src Port: 53, Dst Port: 60528
▼ Domain Name System (response)
    [Request In: 21]
    [Time: 0.000426387 seconds]
    Transaction ID: 0x09ea
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 4
  ▼ Queries
    ▼ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ▼ Answers
    ▶ mit.edu: type NS, class IN, ns use5.akam.net
    ▶ mit.edu: type NS, class IN, ns eur5.akam.net
    ▶ mit.edu: type NS, class IN, ns asia1.akam.net
    ▶ mit.edu: type NS, class IN, ns use2.akam.net
    ▶ mit.edu: type NS, class IN, ns asia2.akam.net
    ▶ mit.edu: type NS, class IN, ns usw2.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
  ▼ Additional records
    ▶ use2.akam.net: type A, class IN, addr 96.7.49.64
    ▶ asia2.akam.net: type A, class IN, addr 95.101.36.64
    ▶ usw2.akam.net: type A, class IN, addr 184.26.161.64
    ▶ eur5.akam.net: type A, class IN, addr 23.74.25.64
```

Figure 11: DNS Response Message

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

    Answer : It’s a **type NS** DNS query. **No**, it doesn’t contain any answers.

11. **Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?**

Answer : The nameservers are **use2, asia2, usw2 and eur5**. **Yes**, we can find their IP addresses if we expand the Additional records field in Wireshark as seen above.