

CS315 : Computer Networks Lab

Assignment 4

Sourabh Bhosale (200010004)

January 24, 2023

1 Part-1: nslookup

1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology Dharwad, India: www.iitdh.ac.in. What is the IP address of www.iitdh.ac.in

IP address : 203.129.219.164 or 14.139.150.68

```
~ $ nslookup www.iitdh.ac.in
Server:          192.168.67.111
Address:         192.168.67.111#53

Non-authoritative answer:
Name:   www.iitdh.ac.in
Address: 203.129.219.164
Name:   www.iitdh.ac.in
Address: 14.139.150.68
```

2. Run nslookup to determine the DNS servers for google.com.

ns3.google.com, ns4.google.com, ns1.google.com, ns2.google.com

```
~ $ nslookup -type=NS google.com
Server:          192.168.67.111
Address:         192.168.67.111#53

Non-authoritative answer:
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.

Authoritative answers can be found from:
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
```

3. Run nslookup so that one of the DNS servers obtained in Question2 is queried for gmail.com. What is its IP address?

IP address : 142.250.67.197

```
[~ $ nslookup gmail.com ns3.google.com
Server:          ns3.google.com
Address:         216.239.36.10#53

Name:   gmail.com
Address: 142.250.67.197
```

2 Part-2: The DNS cache on your computer

Clearing DNS resolver cache (for Mac)

```
[~ $ sudo killall -HUP mDNSResponder
[Password:
~ $ █
```

3 Part-3: Tracing DNS with Wireshark

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

They are sent over UDP (User Datagram Protocol).

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

Destination port for DNS query message : 53

Source port for DNS response message : 53

3. To what IP address is the DNS query message sent? Use ipconfig(Windows)/dig(Linux) to determine the IP address of your local DNS server. Are these two IP addresses the same?

IP address is the DNS query message sent : 192.168.67.111

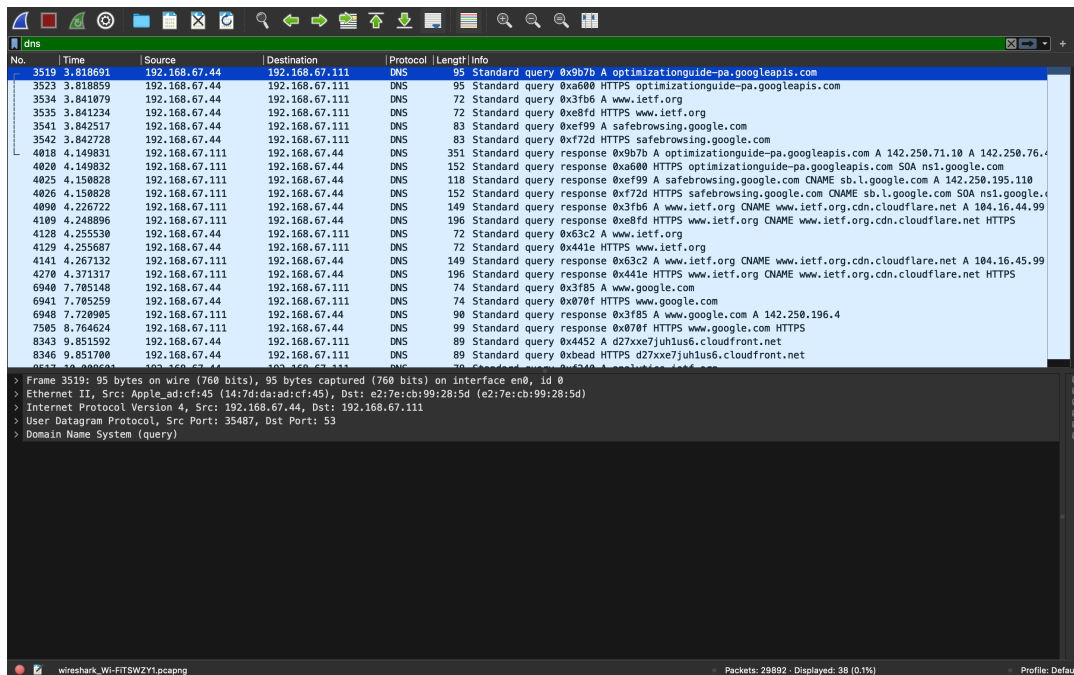
IP address of your local DNS server : 192.168.67.111

Yes, they will be the same.

```
[~] $ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 192.168.67.111
[~] $
```

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

For some of the queries it is a type A Standard Query and for some of them it is HTTPS and it doesn't contain any answers.



The screenshot shows a Wireshark packet capture of DNS traffic. The packet list on the left shows several DNS queries and responses. The packet details pane on the right shows the structure of a DNS query message, including the query type and the query name.

No.	Time	Source	Destination	Protocol	Length	Info
3519	3.818601	192.168.67.44	192.168.67.111	DNS	95	Standard query 0x9b7b A optimizationguide-pa.googleapis.com
3523	3.818859	192.168.67.44	192.168.67.111	DNS	95	Standard query 0xa600 HTTPS optimizationguide-pa.googleapis.com
3534	3.841079	192.168.67.44	192.168.67.111	DNS	72	Standard query 0x3fb6 A www.ietf.org
3535	3.841234	192.168.67.44	192.168.67.111	DNS	72	Standard query 0xe8fd HTTPS www.ietf.org
3541	3.842517	192.168.67.44	192.168.67.111	DNS	83	Standard query 0xef99 A safebrowsing.google.com
3542	3.842728	192.168.67.44	192.168.67.111	DNS	83	Standard query 0xf72d HTTPS safebrowsing.google.com
4018	4.149031	192.168.67.111	192.168.67.44	DNS	351	Standard query response 0x9b7b A optimizationguide-pa.googleapis.com A 142.250.71.10 A 142.250.76.10
4020	4.149832	192.168.67.111	192.168.67.44	DNS	152	Standard query response 0xa600 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
4025	4.150828	192.168.67.111	192.168.67.44	DNS	118	Standard query response 0xef99 A safebrowsing.google.com CNAME sb.l.google.com A 142.250.195.110
4026	4.150828	192.168.67.111	192.168.67.44	DNS	152	Standard query response 0xf72d HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
4090	4.226722	192.168.67.111	192.168.67.44	DNS	149	Standard query response 0x3fb6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99
4109	4.248896	192.168.67.111	192.168.67.44	DNS	196	Standard query response 0xe8fd HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS
4128	4.255530	192.168.67.44	192.168.67.111	DNS	72	Standard query 0x63c2 A www.ietf.org
4129	4.255687	192.168.67.44	192.168.67.111	DNS	72	Standard query 0x441e HTTPS www.ietf.org
4141	4.267132	192.168.67.111	192.168.67.44	DNS	149	Standard query response 0x63c2 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99
4270	4.371317	192.168.67.111	192.168.67.44	DNS	196	Standard query response 0x441e HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS
6940	7.705148	192.168.67.44	192.168.67.111	DNS	74	Standard query 0x3f85 A www.google.com
6941	7.705259	192.168.67.44	192.168.67.111	DNS	74	Standard query 0x070f HTTPS www.google.com
6948	7.726905	192.168.67.111	192.168.67.44	DNS	90	Standard query response 0x3f85 A www.google.com A 142.258.196.4
7505	8.764624	192.168.67.111	192.168.67.44	DNS	99	Standard query response 0x070f HTTPS www.google.com HTTPS
8343	9.851592	192.168.67.44	192.168.67.111	DNS	89	Standard query 0x4452 A d27xxe7juh1u6.cloudfront.net
8346	9.851700	192.168.67.44	192.168.67.111	DNS	89	Standard query 0xbedd HTTPS d27xxe7juh1u6.cloudfront.net

Frame 3519: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface en0, id 0
Ethernet II, Src: Apple-Adcf45 (14:7d:ad:ad:cf:45), Dst: e2:7e:cb:99:28:5d (e2:7e:cb:99:28:5d)
Internet Protocol Version 4, Src: 192.168.67.44, Dst: 192.168.67.111
User Datagram Protocol, Src Port: 35487, Dst Port: 53
Domain Name System (query)

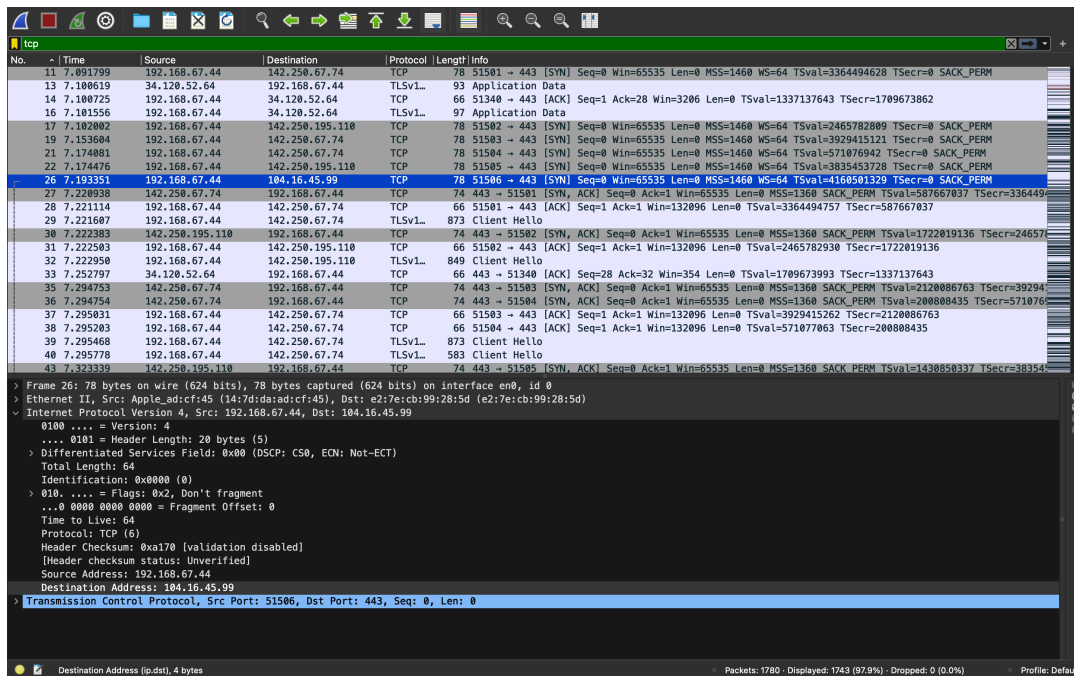
5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There were 3 answers containing information about the name of the host, the type of address, class, time to live, the data length and the IP address. (Screenshot Provided)

6. 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?

Yes, the SYN packet was sent to 104.16.45.99, which corresponds to the destination IP address provided in the DNS response message.

```
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: 1800 (30 minutes)
Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.16.44.99
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.16.45.99
[Request In: 3534]
[Time: 0.385643000 seconds]
```



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

No, it doesn't.

4 Part-4: Wireshark and nslookup

For `nslookup www.mit.edu`

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

Destination port for DNS query message : 53

Source port for DNS response message : 53

```
~ $ nslookup www.mit.edu
Server:      192.168.67.111
Address:     192.168.67.111#53

Non-authoritative answer:
www.mit.edu canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 23.35.92.23

~ $
```

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

IP address is the DNS query message sent : 192.168.67.111

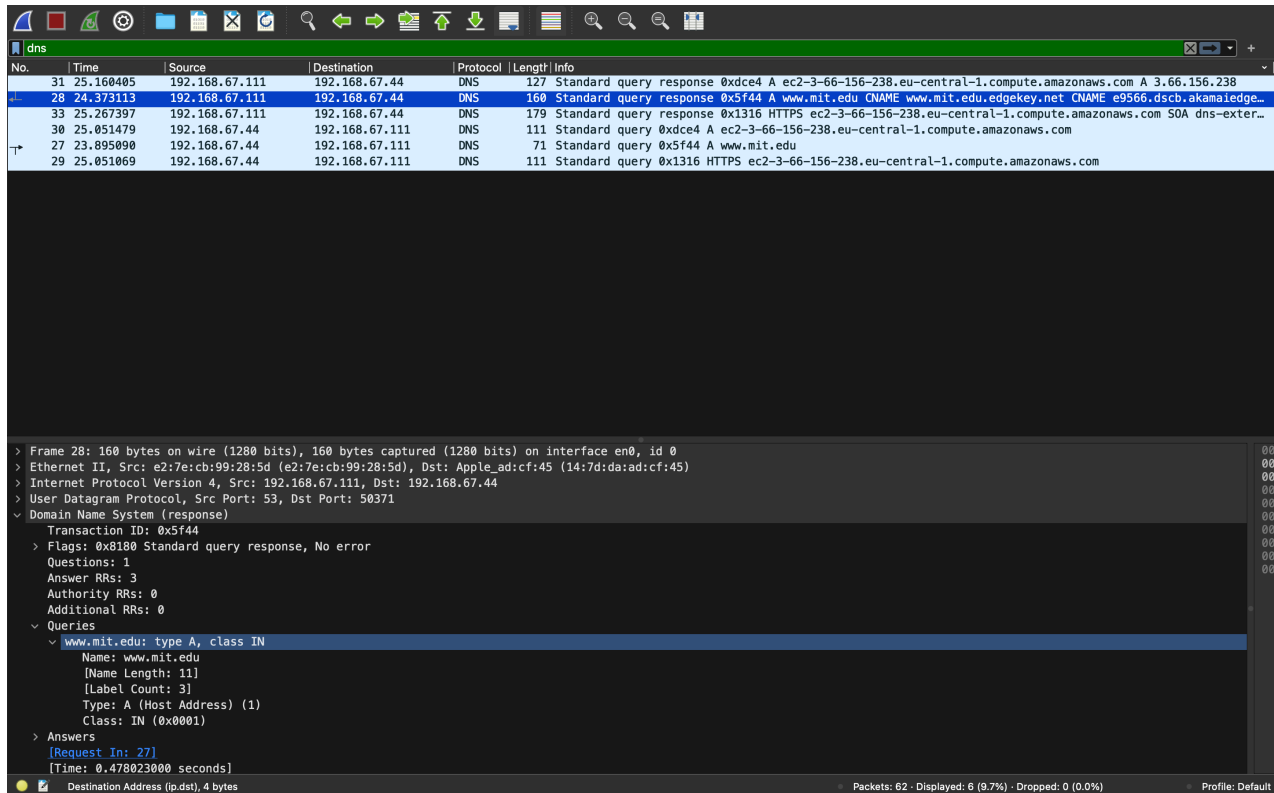
IP address of your local DNS server : 192.168.67.111

Yes, here both will be same.

```
~ $ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 192.168.67.111
~ $
```

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

For some of the queries it is a type A Standard Query and for some of them it is HTTPS and it doesn't contain any answers.



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

There were 3 answers containing information about the name of the host, the type of address, class, time to live, the data length and the IP address.


```

v Answers
  v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 971 (16 minutes, 11 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.35.92.23
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 4
    Address: 23.35.92.23
\[Request In: 27\]
[Time: 0.478023000 seconds]

```

5. Provide a screenshot.

The screenshot shows a Wireshark capture of a DNS transaction. The packet list at the top shows several packets, with packet 27 being the DNS query and packet 28 being the response. The packet details pane for packet 28 shows the response structure, including the transaction ID, flags, and the query details. The query details show the domain name www.mit.edu, the type A, and the class IN. The response details show the CNAME record for www.mit.edu pointing to www.mit.edu.edgekey.net, and the A record for e9566.dscb.akamaiedge.net pointing to 23.35.92.23.

No.	Time	Source	Destination	Protocol	Length	Info
29	25.851069	192.168.67.44	192.168.67.111	DNS	111	Standard query 0x1316 HTTPS ec2-3-66-156-238.eu-central-1.compute.amazonaws.com
27	23.895090	192.168.67.44	192.168.67.111	DNS	71	Standard query 0x5f44 A www.mit.edu
30	25.851479	192.168.67.44	192.168.67.111	DNS	111	Standard query 0xdce4 A ec2-3-66-156-238.eu-central-1.compute.amazonaws.com
33	25.267397	192.168.67.111	192.168.67.44	DNS	179	Standard query response 0x1316 HTTPS ec2-3-66-156-238.eu-central-1.compute.amazonaws.com SOA dns-exte...
28	24.373113	192.168.67.111	192.168.67.44	DNS	160	Standard query response 0x5f44 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge...
31	25.160405	192.168.67.111	192.168.67.44	DNS	127	Standard query response 0xdce4 A ec2-3-66-156-238.eu-central-1.compute.amazonaws.com A 3.66.156.238

Frame 27: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
 Ethernet II, Src: Apple_ad:cf:45 (14:7d:da:ad:cf:45), Dst: e2:7e:cb:99:28:5d (e2:7e:cb:99:28:5d)
 Internet Protocol Version 4, Src: 192.168.67.44, Dst: 192.168.67.111
 User Datagram Protocol, Src Port: 58371, Dst Port: 53
 Domain Name System (query)
 Transaction ID: 0x5f44
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
[\[Response In: 28\]](#)

For `nslookup -type=NS mit.edu`

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

IP address is the DNS query message sent : 192.168.67.111

IP address of your local DNS server : 192.168.67.111

Yes, here both will be same.

```
[~] $ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 192.168.67.111
[~] $
```

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

It's a `type NS` DNS query that doesn't contain any answers.

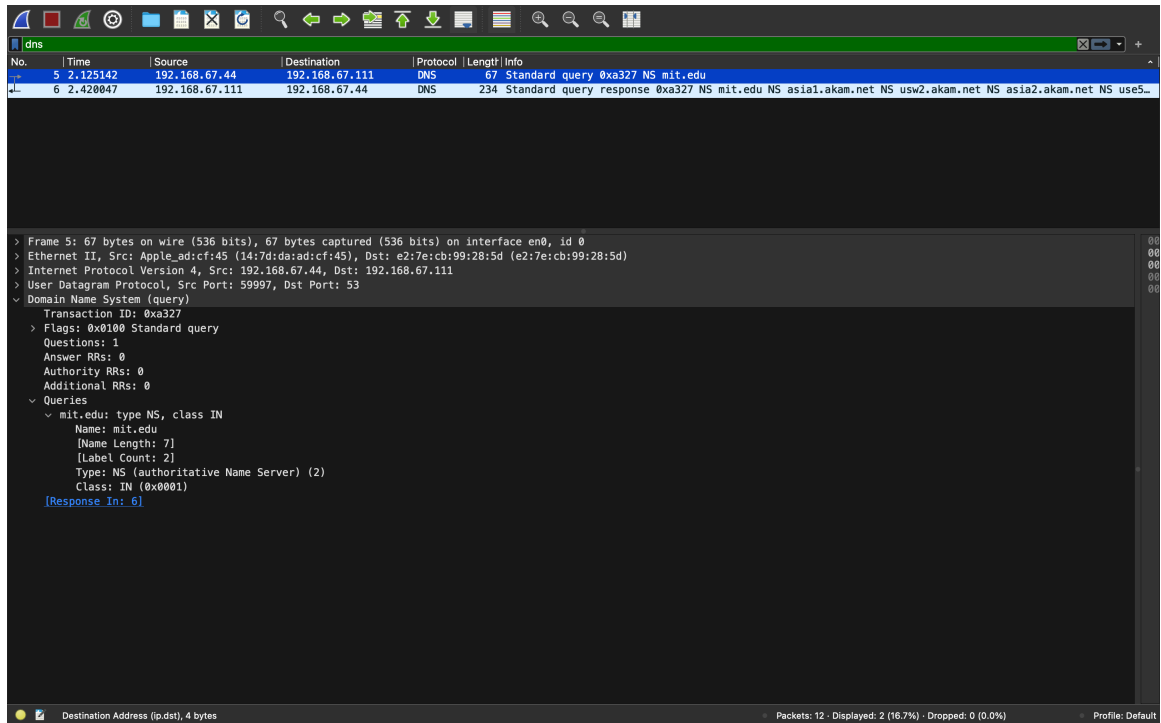
8. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

Following MIT nameservers were provided by response message :

1. asia2.akam.net
2. ns1-37.akam.net
3. use5.akam.net
4. ns1-173.akam.net
5. eur5.akam.net
6. asia1.akam.net
7. use2.akam.net
8. usw2.akam.net

No, the response message doesn't provide the IP addresses of the MIT nameservers. But we can have a look at the IP addresses by using `nplookup` command in terminal.

9. Provide a screenshot.



For `nslookup gmail.com ns3.google.com`

10. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

IP address is the DNS query message sent : 216.239.36.10

IP address of your local DNS server : 192.168.67.111

```
[~ $ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 192.168.67.111
~ $
```

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

It's a `type A` DNS query that doesn't contain any answers.

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

There is 1 answer containing information about the name of the host, the type of address, class, time to live, the data length and the IP address.

```
Domain Name System (response)
  Transaction ID: 0xa095
  > Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > gmail.com: type A, class IN
      Name: gmail.com
      [Name Length: 9]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  > Answers
    > gmail.com: type A, class IN, addr 142.250.67.197
      Name: gmail.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 142.250.67.197
  [Request In: 13]
  [Time: 0.199034000 seconds]
```

13. Provide a screenshot.

