CS315: Lab Assignment 4

B Siddharth Prabhu
200010003@iitdh.ac.in

24 January 2023

1 Exploring nslookup

The following are screenshots of commands that have been run related to nslookup, which is a command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address, or other DNS records. Below them, we will answer a few questions regarding the same:

```
siddharth@DESKTOP-5490SID-LINUX:~$ nslookup www.iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

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

siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 1: Output when querying IP address of `www.iitdh.ac.in`

```
siddharth@DESKTOP-5490SID-LINUX:~$ nslookup -type=NS iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
iitdh.ac.in     nameserver = dns1.iitdh.ac.in.
iitdh.ac.in     nameserver = dns2.iitdh.ac.in.

Authoritative answers can be found from:

siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 2: Output when querying for a type-NS record to default local DNS server

```
siddharth@DESKTOP-5490SID-LINUX:~$ nslookup google.com ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   google.com
Address: 142.250.205.238
Name:   google.com
Address: 2404:6800:4007:82d::200e

siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 3: Output when querying IP address of `google.com` from specific DNS server

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

As seen in Figure (1), there are 2 IP addresses for the IITDh web server, which are `14.139.150.68` and `203.129.219.164` . The reason for having multiple such IP addresses may be load balancing.

(2) Run nslookup to determine the DNS servers for `www.google.com` .

From Figure (4), we can observe that the DNS servers for `www.google.com` are as follows:

- `ns1.google.com`
- `ns2.google.com`
- `ns3.google.com`
- `ns4.google.com`

The IP addresses of the same (IPv4 and IPv6) are also listed.

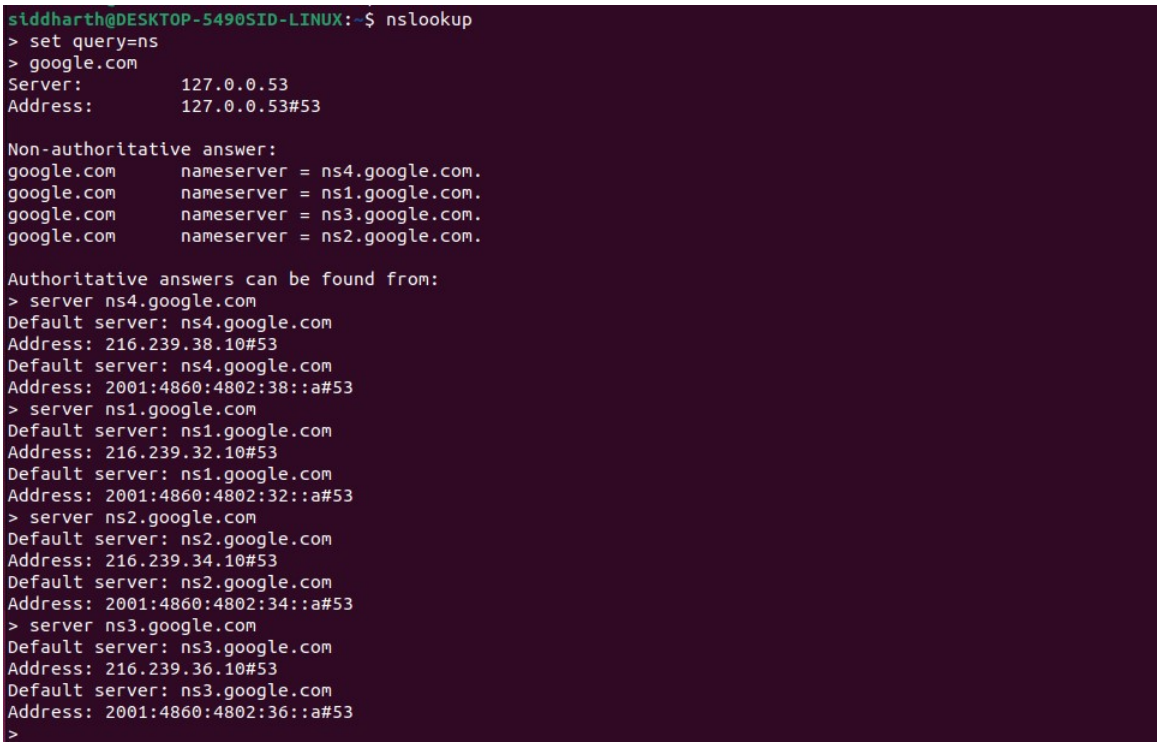

Figure 4: Output when determining DNS servers of `google.com`

(3) Run nslookup so that one of the DNS servers obtained in Question 2 is queried for `gmail.com` . What is its IP address?

From Figure (5), we can observe that the IP address for `gmail.com` is `142.250.67.197` (IPv4) and also `2404:6800:4009:813::2005` (IPv6).

```
siddharth@DESKTOP-5490SID-LINUX:~$ nslookup gmail.com ns4.google.com
Server:         ns4.google.com
Address:        216.239.38.10#53

Name:   gmail.com
Address: 142.250.67.197
Name:   gmail.com
Address: 2404:6800:4009:813::2005

siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 5: Output when querying for the IP address of `gmail.com`

2 DNS Cache Clearing

Here, we will explicitly clear the contents of the system's DNS cache. This just means that the computer will need to invoke the distributed DNS service next time it needs to use the DNS name resolution service, since it will find no records in the cache. Note that the `systemd-resolve` command is not present by default, so we use `resolvectl` instead. This does the same thing.

```
siddharth@DESKTOP-5490SID-LINUX:~$ sudo systemd-resolve --flush-caches
[sudo] password for siddharth:
sudo: systemd-resolve: command not found
siddharth@DESKTOP-5490SID-LINUX:~$ sudo resolvectl flush-caches
siddharth@DESKTOP-5490SID-LINUX:~$
```

Figure 6: Clearing DNS Cache of the system

3 DNS Tracing with Wireshark

We shall first capture the DNS packets that are generated by ordinary Web-surfing activity, then answer some questions regarding the same. The screenshot of the relevant DNS entries is below:

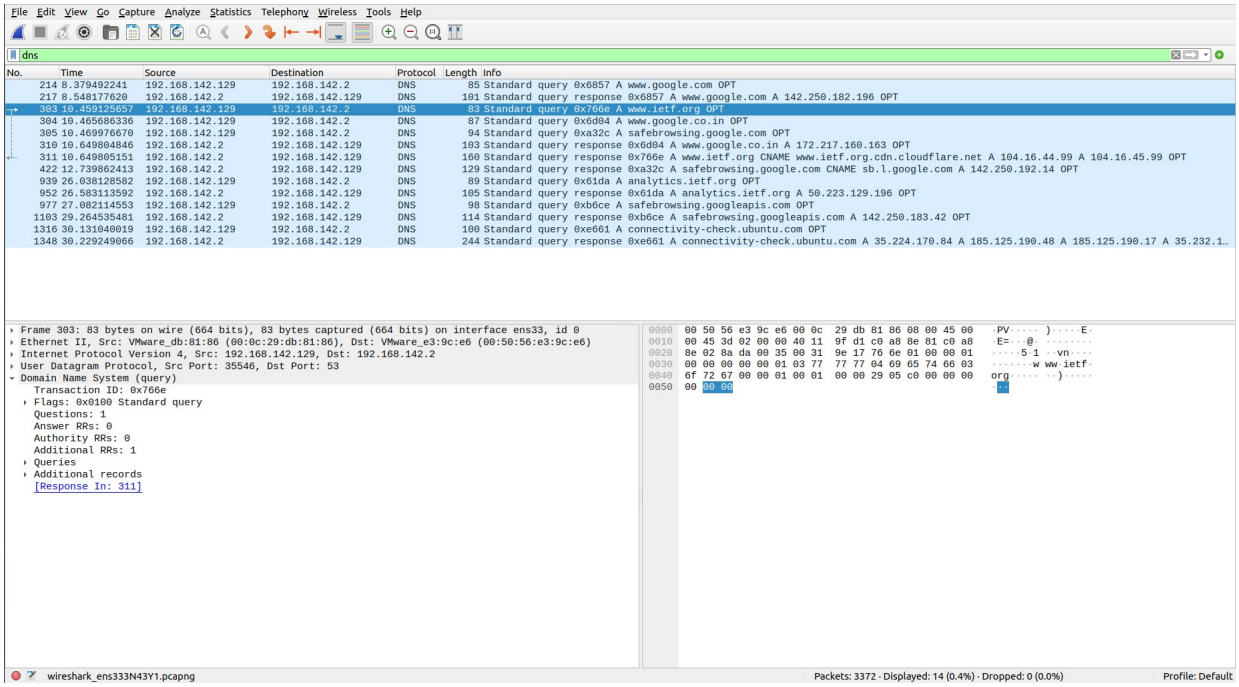

Figure 7: DNS Trace on Wireshark

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

We observe in the Packet Details Pane of Figure (7) that DNS queries and responses are sent over **UDP (User Datagram Protocol)**, since the size of a DNS query/response is small enough to be encapsulated in a single datagram. The same over TCP may be more reliable, although with substantial connection/disconnection overhead.

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

It is visible in the Packet Details Pane of Figure (7) that the destination port for the DNS query message is **port 53**. Also, the source port of DNS response messages is **port 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?

As seen in Figure (7), the DNS query message is sent to `192.168.142.2`. The IP address of the local DNS server is `127.0.0.53`. These two addresses are **not the same**. Ths implies that the local DNS server does not have the record necessary to resolve the domain entered.

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

As seen in Figure (7), the DNS query message is of **Type A Standard**, and it **doesn't** contain any answers.

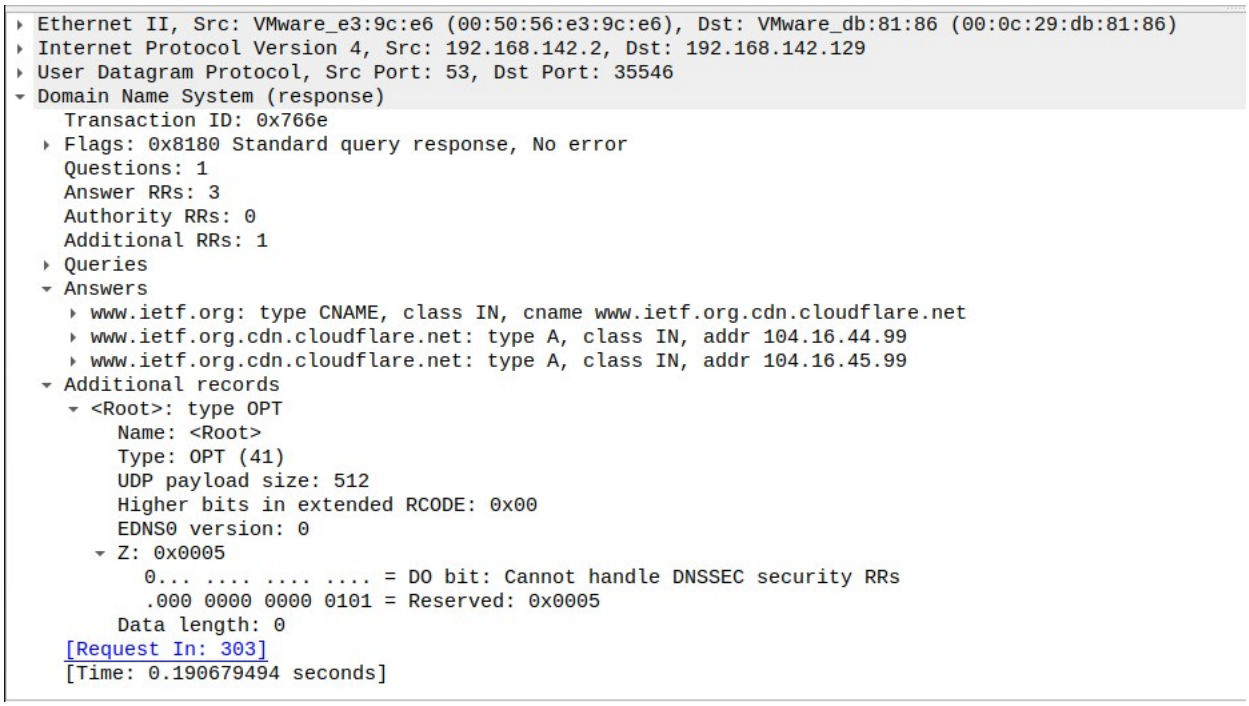

Figure 8: Details of DNS Response Message

(5) Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

As seen in Figure (8), the DNS response message contains **3 answers**. Each of these answers contain the following information:

- Name of the Host
- Type of address class
- TTL (Time To Live)
- Data length
- IP address

The same can be seen in the expanded view of the list of answers in Figure (9).

```
▾ 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: 5 (5 seconds)
      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: 5 (5 seconds)
      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: 5 (5 seconds)
      Data length: 4
      Address: 104.16.45.99
```

Figure 9: Details of DNS Response Message

(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?

We observe that the subsequent TCP SYN packet, as shown in Figure (10) on the next page, has a destination address of `104.16.44.99` . This is also present in the answers of the DNS response message, and is located in the second "answer" of Figure (9).

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

No, the host **does not** issue new DNS queries for retrieving each image. This may be due to all of the images being on the same server; and hence not requiring resolution of another domain name.

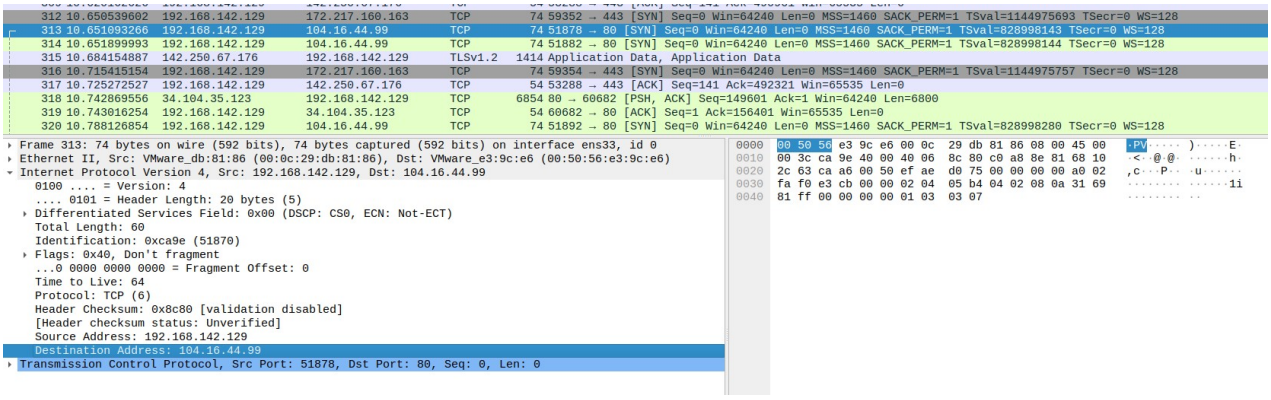

Figure 10: Details of subsequent TCP SYN packet

4 Wireshark and nslookup

We shall capture packets during an `nslookup` call, and analyze the trace obtained. First, let's do `nslookup www.mit.edu` . We will answer five questions that analyze parts of the trace, which are in the screenshots below:

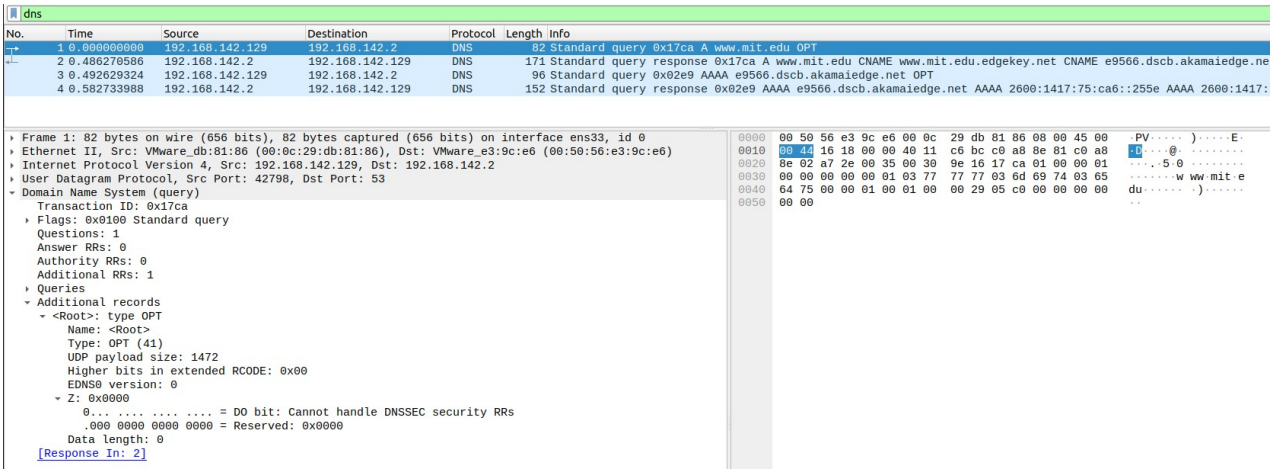

Figure 11: Details of DNS query message

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

It is visible in the Packet Details Pane of Figure (11) that the destination port for the DNS query message is **port 53**. Also, the source port of DNS response messages is **port 53**, as seen in Figure (12).

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

We observe in Figure (11) that the DNS query message is sent to IP address `192.168.142.2` . The local DNS server has IP address `127.0.0.53` . These are not the same.

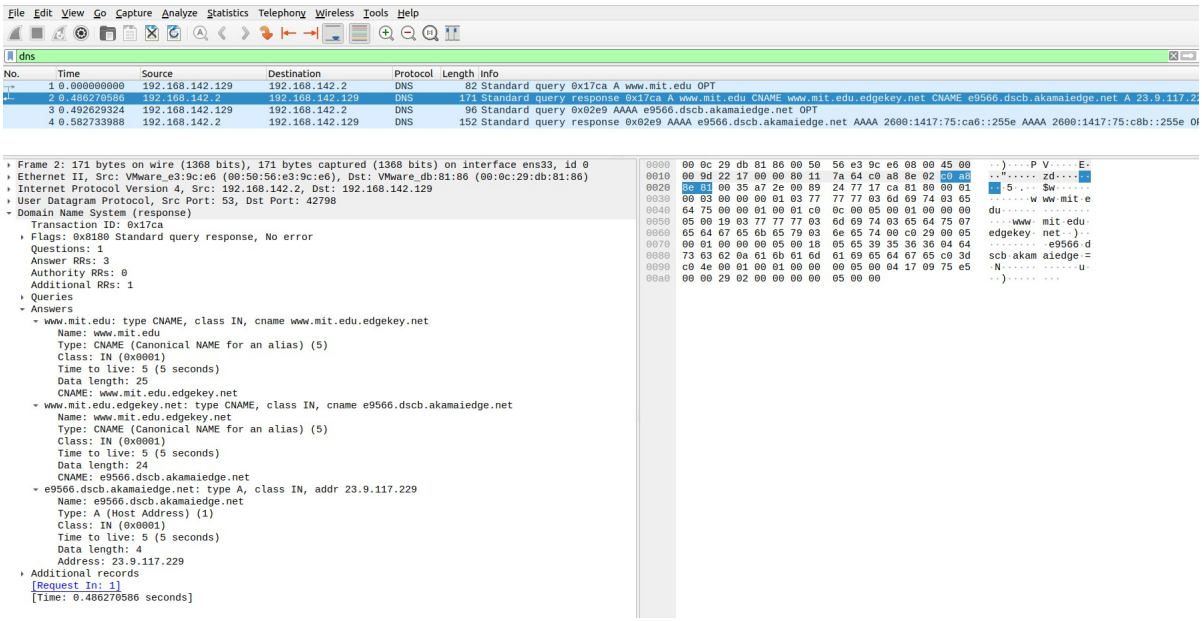

Figure 12: Details of DNS response message

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

As seen in Figure (11), the DNS query message is of **Type A Standard**, 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?

As seen in Figure (12), the DNS response message has **three answers**. The first answer is a canonical record, which is an alias for another domain. Similarly, the second answer is canonical as well. Finally, the third answer is an A record. Each of these answers contain the following information:

- Name of the Host
- of address class
- TTL (Time To Live)
- Data length
- IP address (for the A record)

Note that if we check the details of the second DNS query that is made to the IP address in the A record present in the answers of the first DNS query, then there are 2 answers in the response to *that* second DNS query.

(5) Provide a screenshot.

Refer to Figures (11) and (12).

Next, we shall capture packets while issuing the command `nslookup -=ns mit.edu` . Four questions regarding the same are answered below the screenshots below.

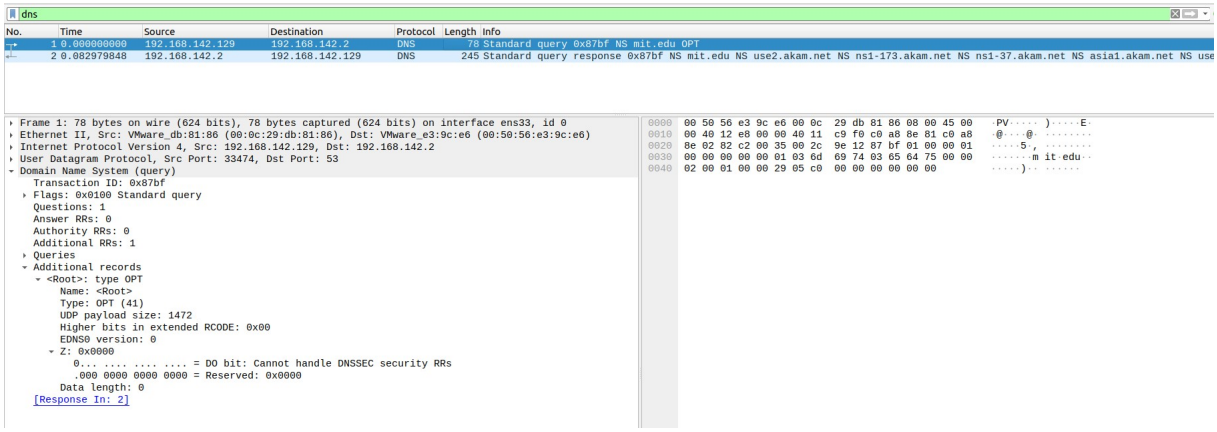

Figure 13: Details of DNS query message

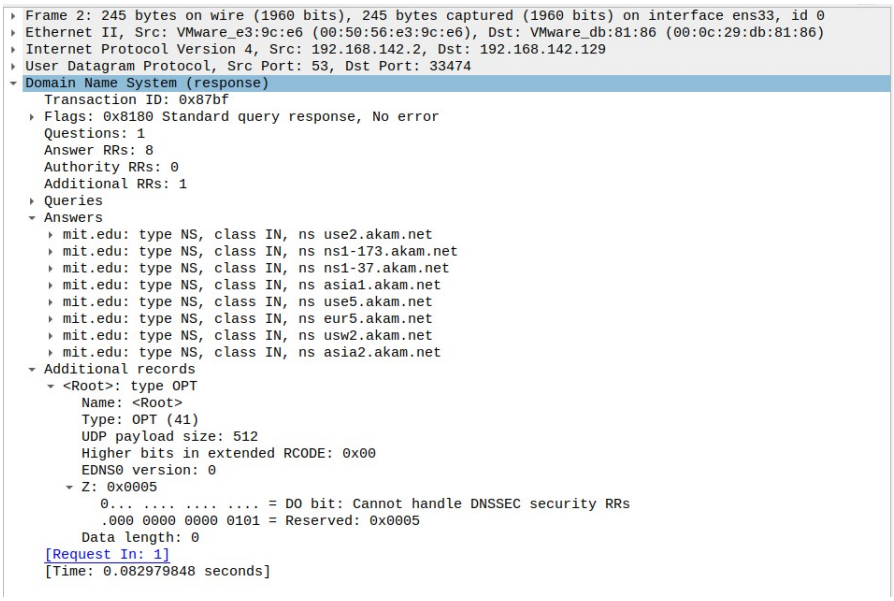

Figure 14: Details of DNS response message

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

We observe in Figure (13) that the DNS query message is sent to IP address `192.168.142.2` . The local DNS server has IP address `127.0.0.53` . These are not the same.

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

As seen in Figure (11), the DNS query message is of **NS Standard**, and it **does not** contain any answers.

(8) 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?

The MIT name servers provided in the response message answers are the 8 ones listed below:

- use2.akam.net
- ns1-173.akam.net
- ns1-37.akam.net
- asia1.akam.net
- use5.akam.net
- eur5.akam.net
- usw2.akam.net
- asia2.akam.net

Also, this response message **does not** provide the IP addresses of the MIT name servers. To find this, we would need to do additional nslookup operations.

(9) Provide a screenshot.

Refer to Figures (13) and (14).

Next, we repeat the same experiment, but for an instance where we query a particular name server for a domain. Here, we run `nslookup gmail.com ns3.google.com` . Below are screenshots of the DNS request and response messages, following which we will answer four questions regarding the same.

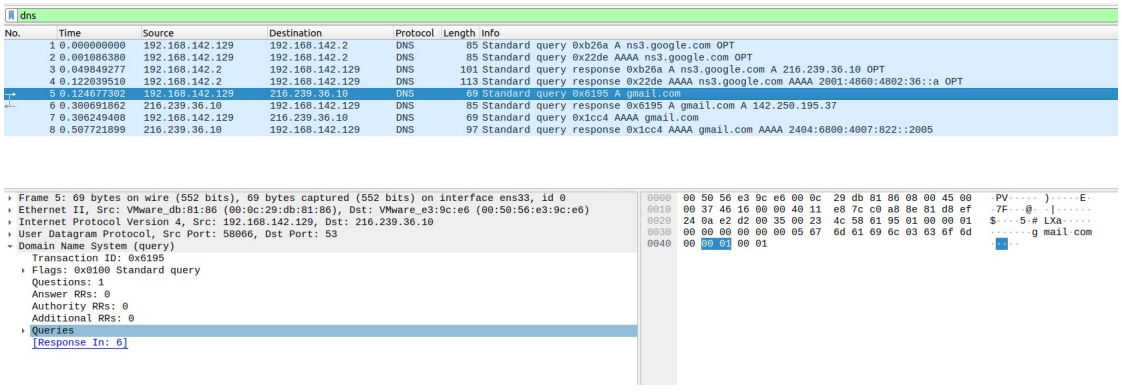

Figure 15: Details of DNS query message

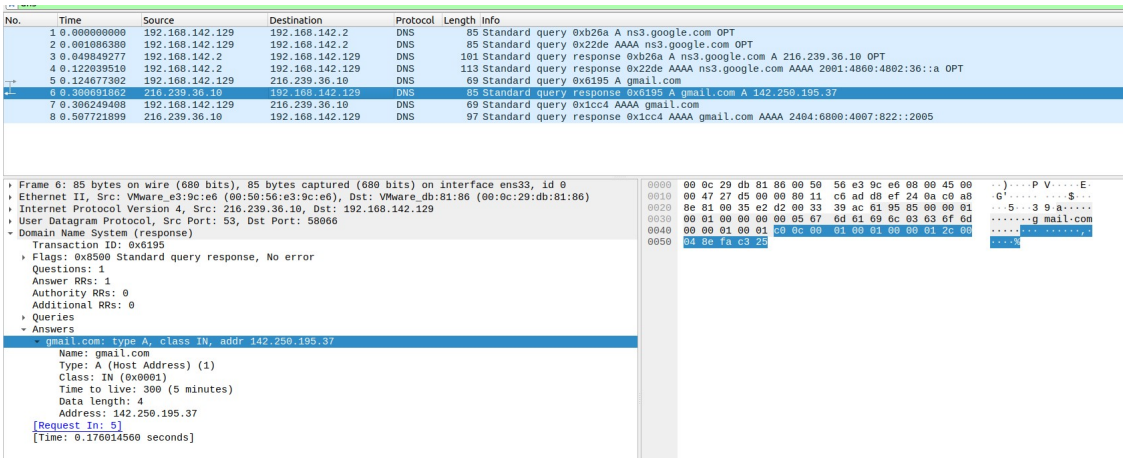

Figure 16: Details of DNS response message

(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?

We observe in Figure (15) that the DNS query message is sent to IP address `216.239.36.10`. The local DNS server has IP address `127.0.0.53`. These are not the same. The reason for this is that we specifically queried the DNS server `ns3.google.com`. The obtained IP address would be that of this specific DNS server.

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

As seen in Figure (15), the DNS query message is of **Type A Standard**, and it **does not** contain any answers.

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

As seen in Figure (16), the DNS response message has **one answer**. This contains the following information:

- Name of the Host
- Type of record
- Class
- TTL (Time To Live)
- Data length
- IP address

(13) Provide a screenshot.

Refer to Figures (15) and (16).