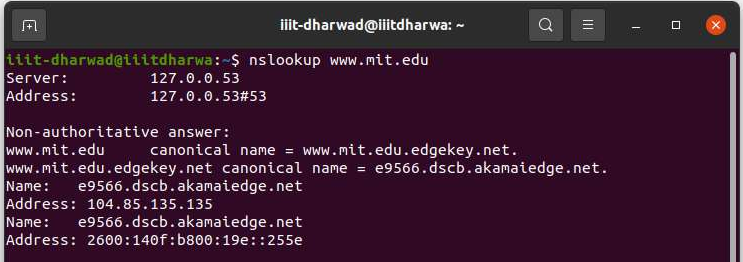
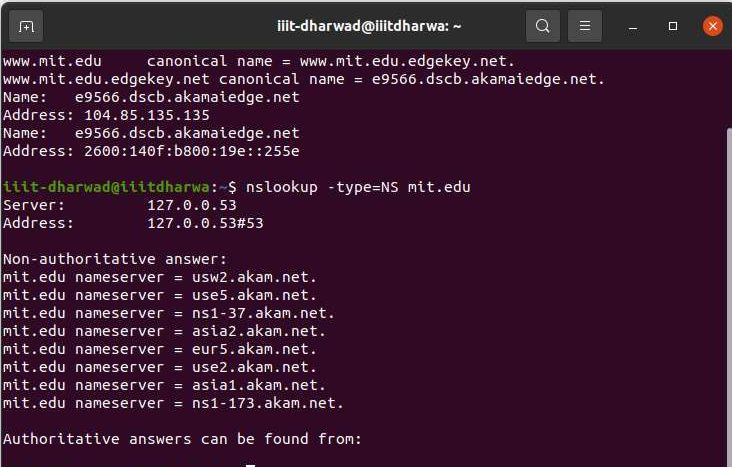
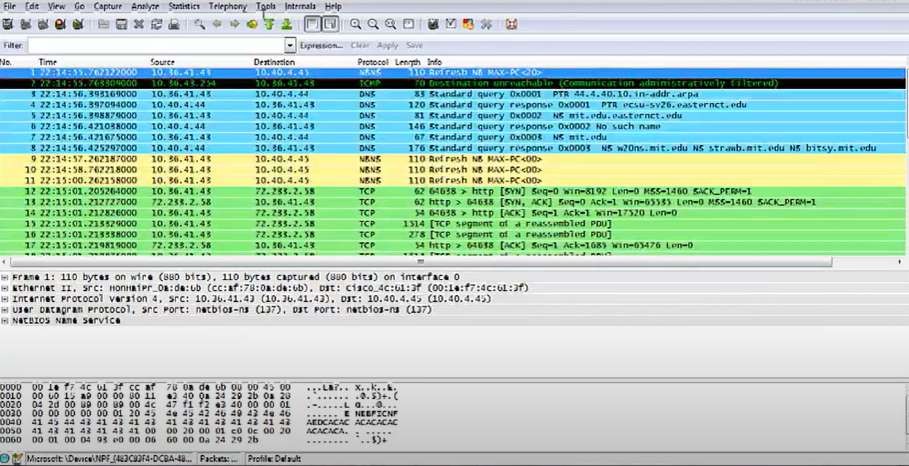
# Lab 4

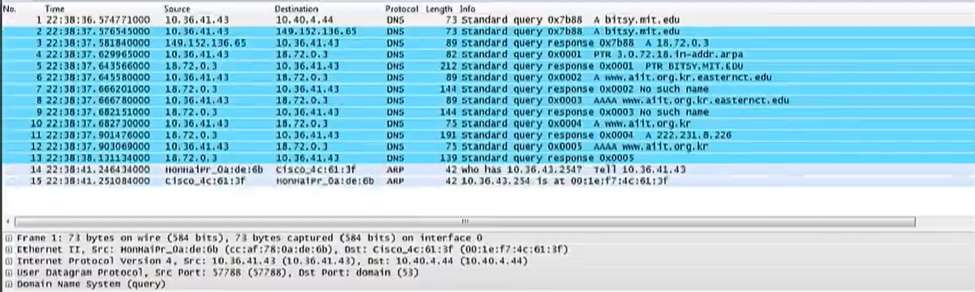
1. nslookup



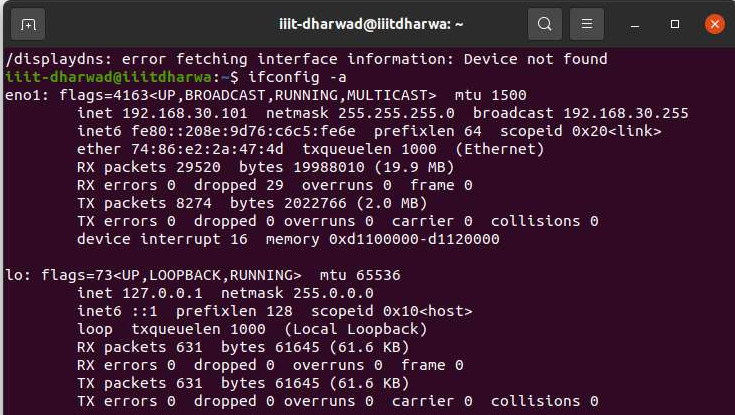
*nslookup –type=NS mit.edu*



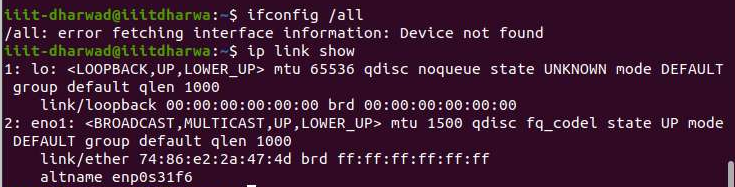


nslookup [www.aiit.or.kr](http://www.aiit.or.kr/) bitsy.mit.edu

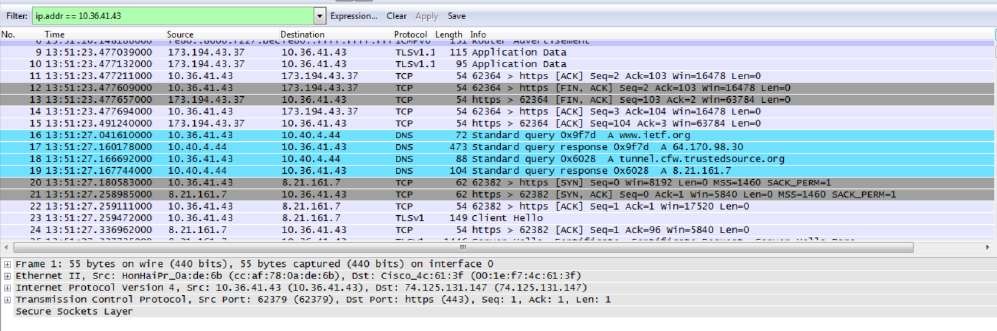
1. ipconfig



ipconfig \all



ipconfig /flushdns

1. Tracing DNS with Wireshark
2. Locate the DNS query and response messages. Are then sent over UDP or TCP? The DNS query and response messages are sent over UDP
3. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port is 53. The source port is 50133.

1. 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?

The DNS query was sent to IP address 10.40.4.44. Yes it is the same IP address as that of my local DNS server.

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

The query message was a type “A” query, but the message did not contain any “answers.”

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

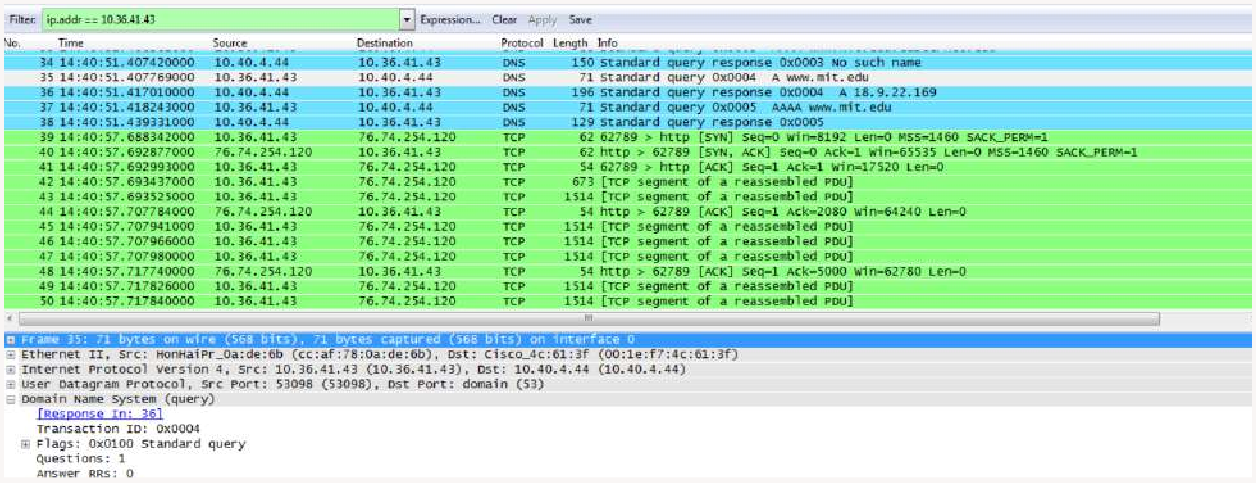
The response message contained one answer to the query which was the sites address [64.170.98.30]. Although it also provided 6 authoritative nameservers, and 11 other responses containing additional information.

1. 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?

The destination of the SYN packet is 64.170.98.30, the same address that was provided in the DNS response message as the type “A” address of the webpage.

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

Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made.



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

Destination Port: 53. Source Port: 53098.

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

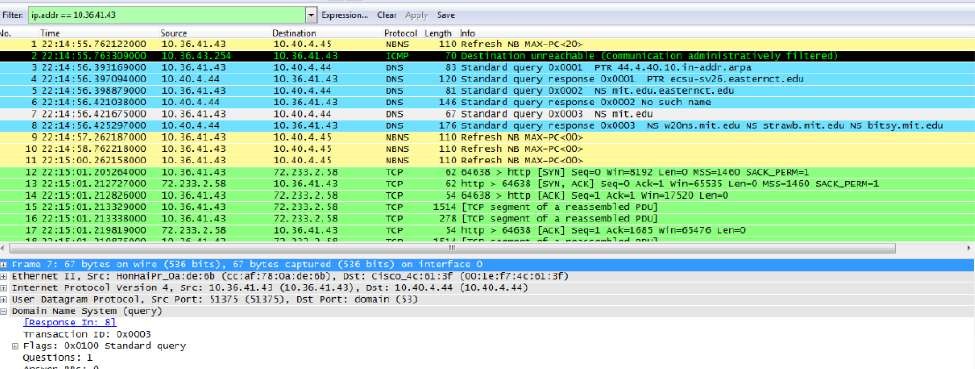
The DNS query message is sent to IP address 10.40.4.44, the same address as my default local DNS server.

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

The DNS query message is a type “A” query, containing only one question and not containing any answers.

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

The response message contains one answer to the aformentioned query which is the type “A” address of [**http://www.mit.edu**](http://www.mit.edu/)or 18.9.22.169. It also contained information on 3 authoritative nameservers and 3 additional records



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

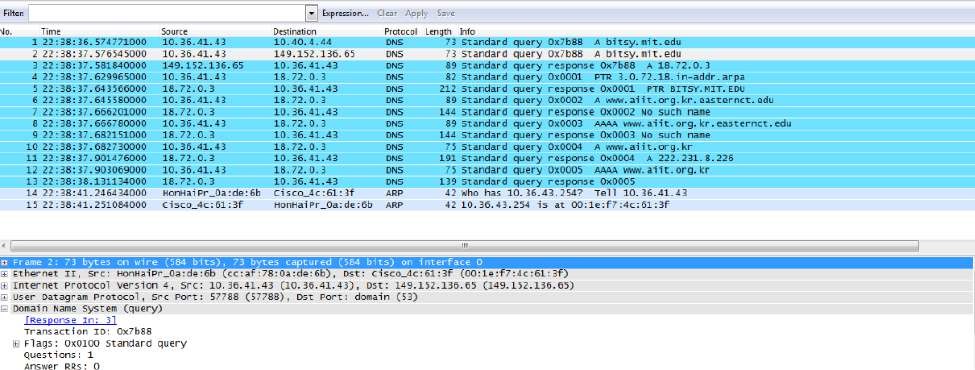
The query is sent to 10.40.4.44, the same IP address as that of my default local DNS server.

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

The DNS query is a type “NS” message including one question. The query message did not contain any answers.

1. 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 namesers?

The response message provides 3 MIT nameservers: w20ns.mit.edu[18.70.0.160], strawb.mit.edu[18.71.0.150], and bitsy.mit.edu[18.72.0.3]. The IP addresses for the nameservers was included under the additional records category sent back as part of the response message.



1. 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?

This DNS query message is sent to 149.152.136.65 which is the IP address of the MIT DNS response sender.

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

This DNS query is a type “A” query. The message does not contain any answers.

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

It only provided one “answer” containing the servers IP address, however, the server also returned a flag that stated that it could complete a recursive query.