Wireshark Lab: DNS v6.01

Vandré Leal Cândido

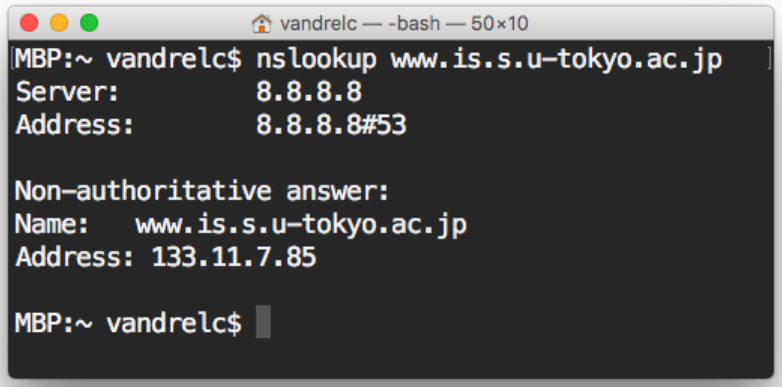
August 27, 2017

1 nslookup

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

  The IP address is 133.11.7.85

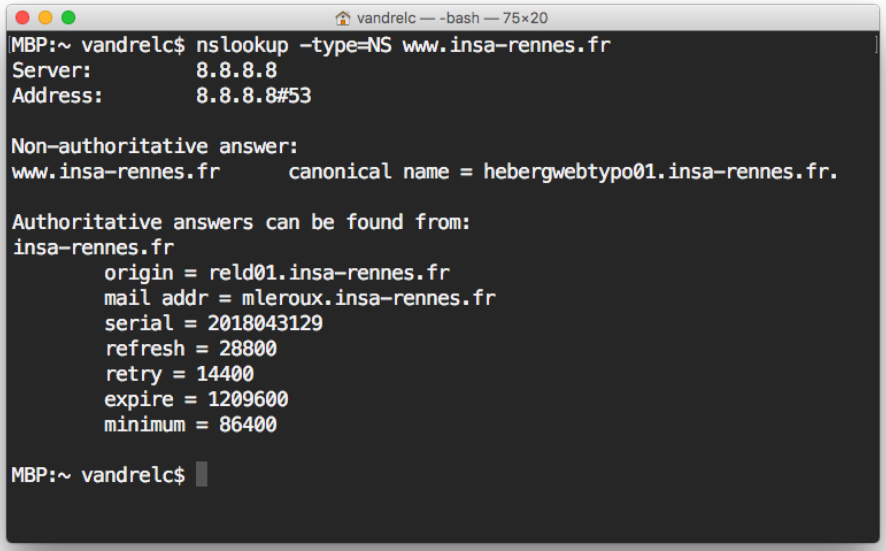
Figure 1: Question 01



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

  The authoritative DNS server is reld01.insa-rennes.fr.

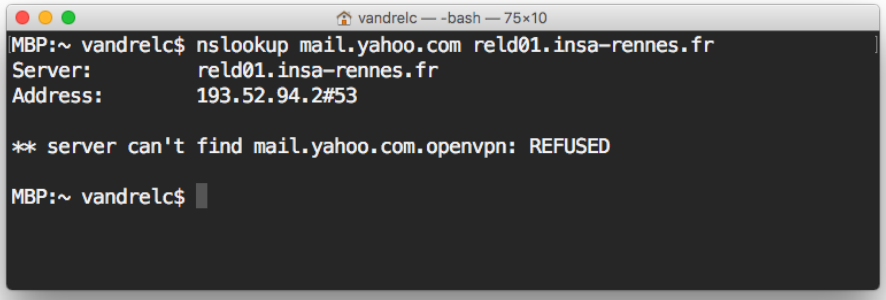
Figure 2: Question 02



- *Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?*

  The IP address is 193.52.94.2.

Figure 3: Question 03



2 Tracing DNS with Wireshark

Figure 4: DNS Query Message

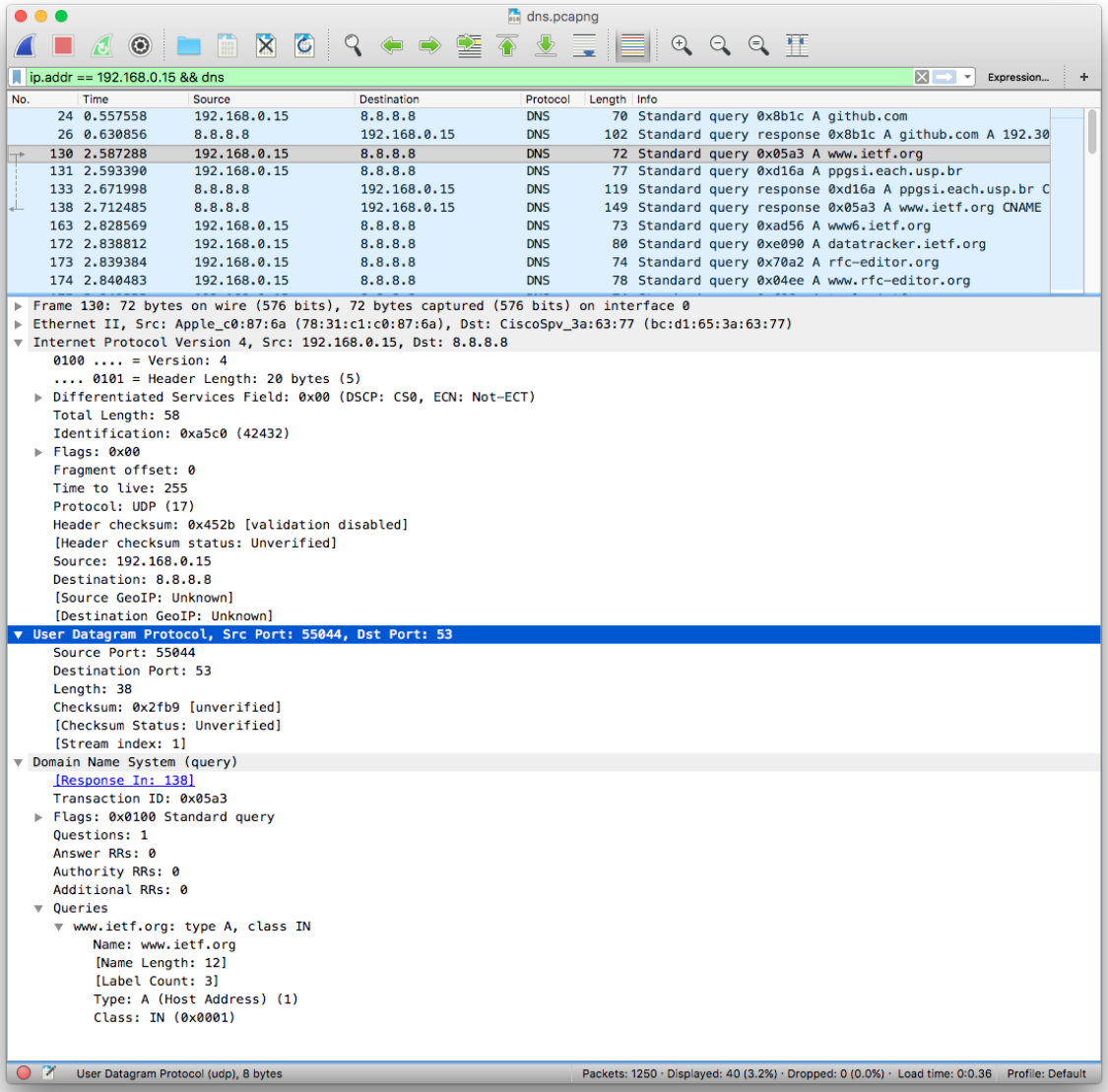
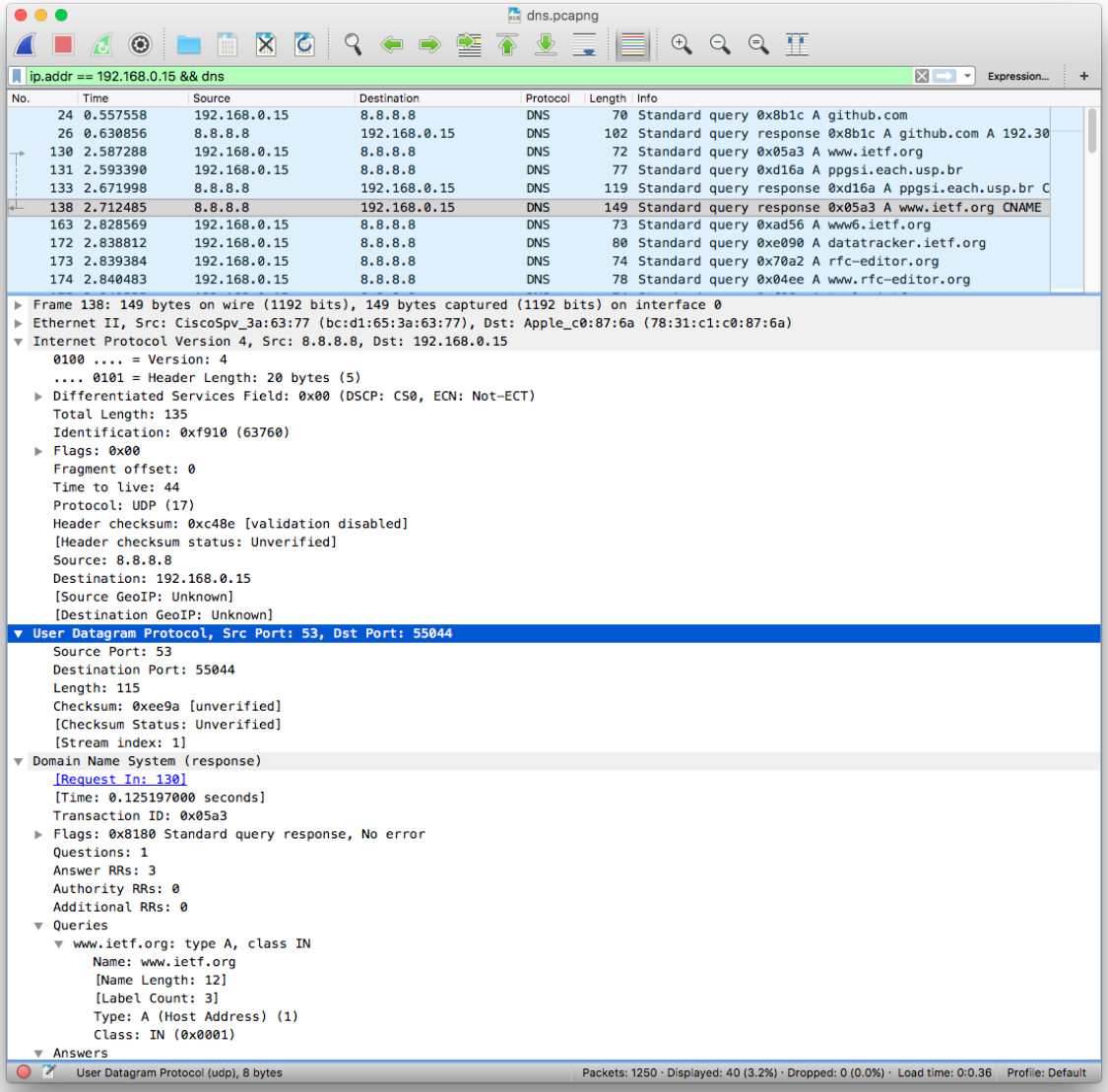


Figure 5: DNS Response Message



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

  Both the query and response messages are sent over UDP.

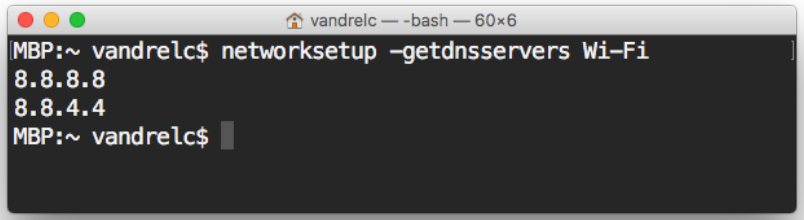
- *What is the destination port for the DNS query message? What is the source port of DNS response message?*

  The destination port of the DNS query message is 53. The source port of the response message is also 53.

- *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 message is sent to 8.8.8.8, which is the IP address of one of the local DNS servers (Google DNS).

Figure 6: Local DNS servers



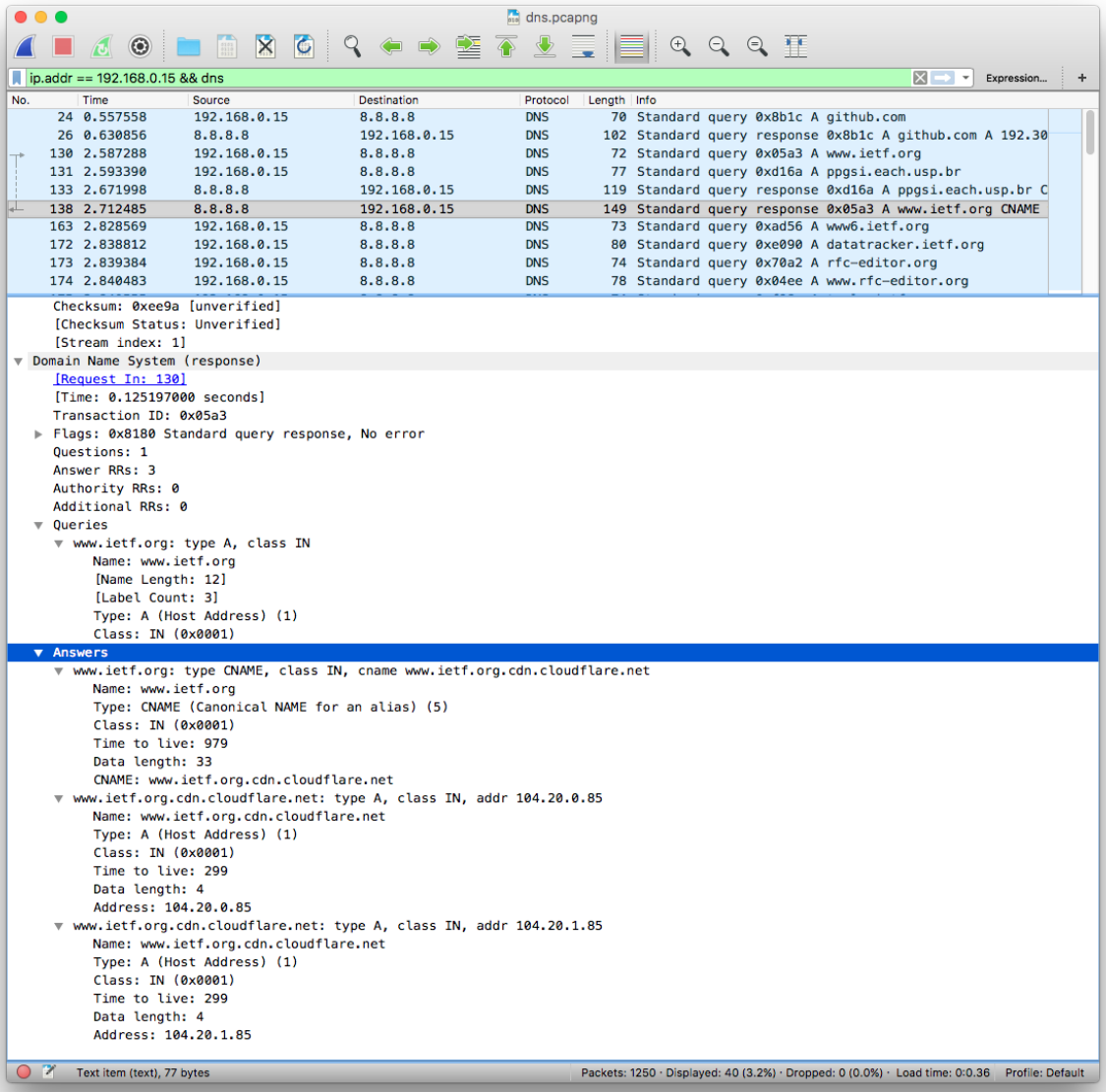
- *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

  It's a standard query (Type A). It doesn't contain any answers.

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

  3 answers were provided. Each answer contains the following information: name of the host, type, class, TTL, data length and IP address.

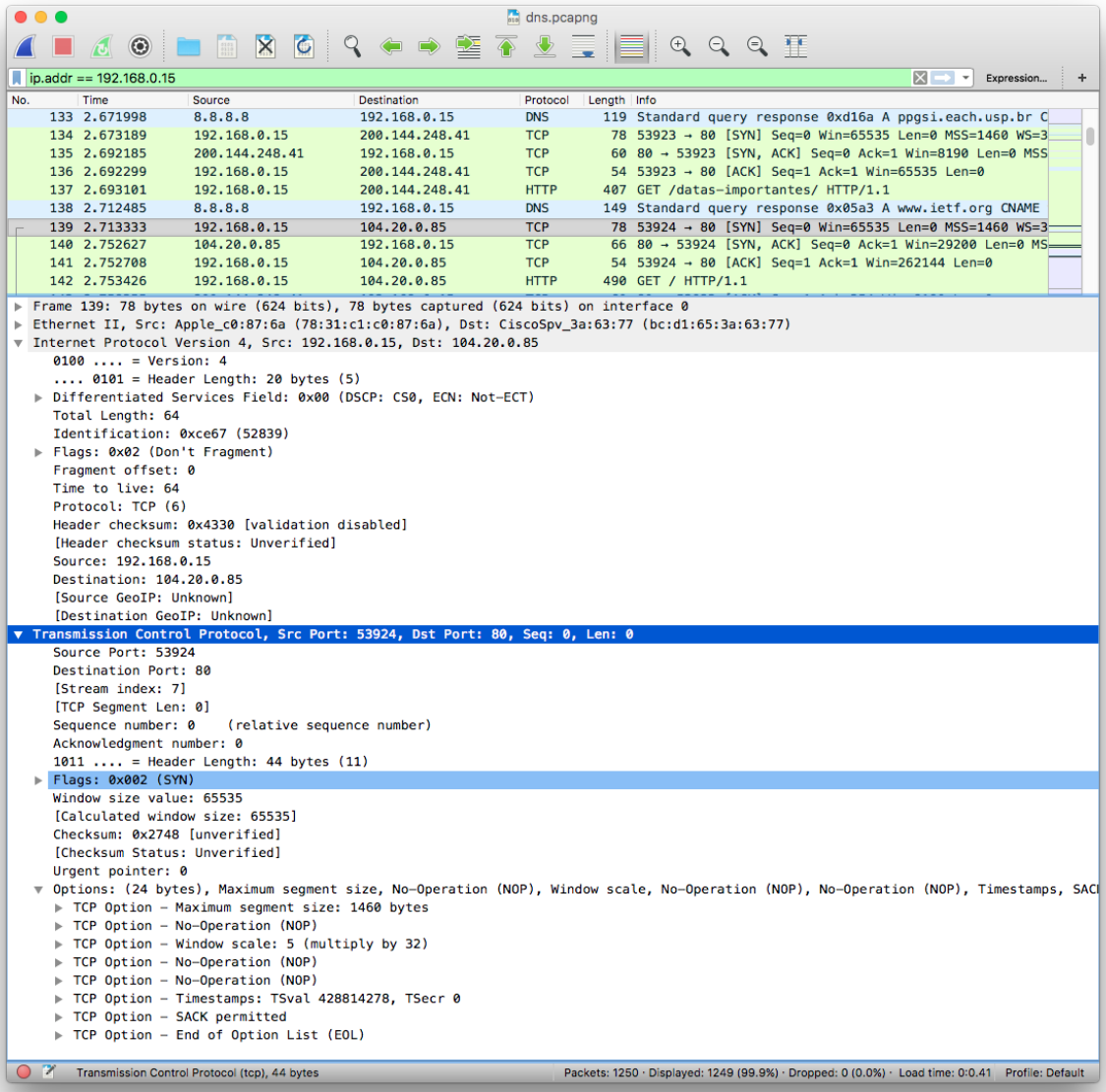
Figure 7: DNS response answers



- *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 first SYN packet was sent to 104.20.0.85 which is one of the IP addresses provided in the DNS response message.

Figure 8: TCP SYN packet



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

  No.

Now let's play with nslookup.

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

Figure 9: nslookup www.mit.edu (DNS Request)

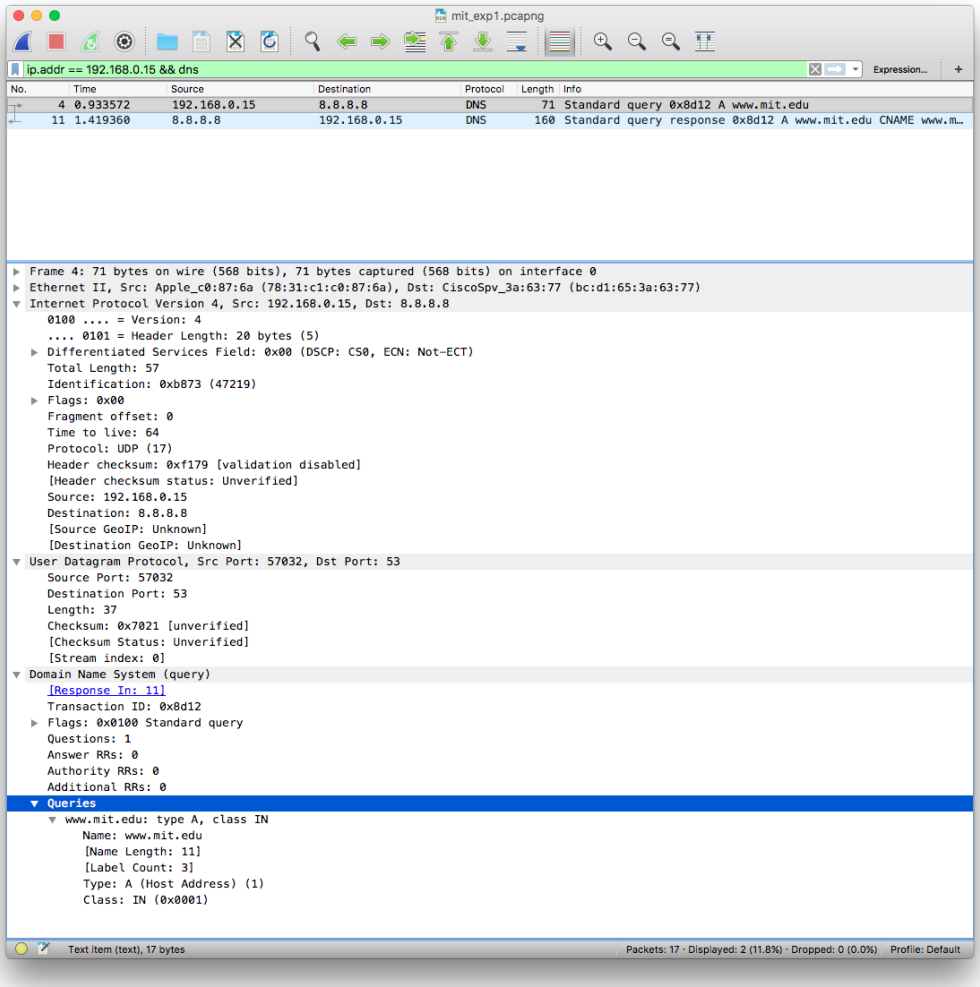
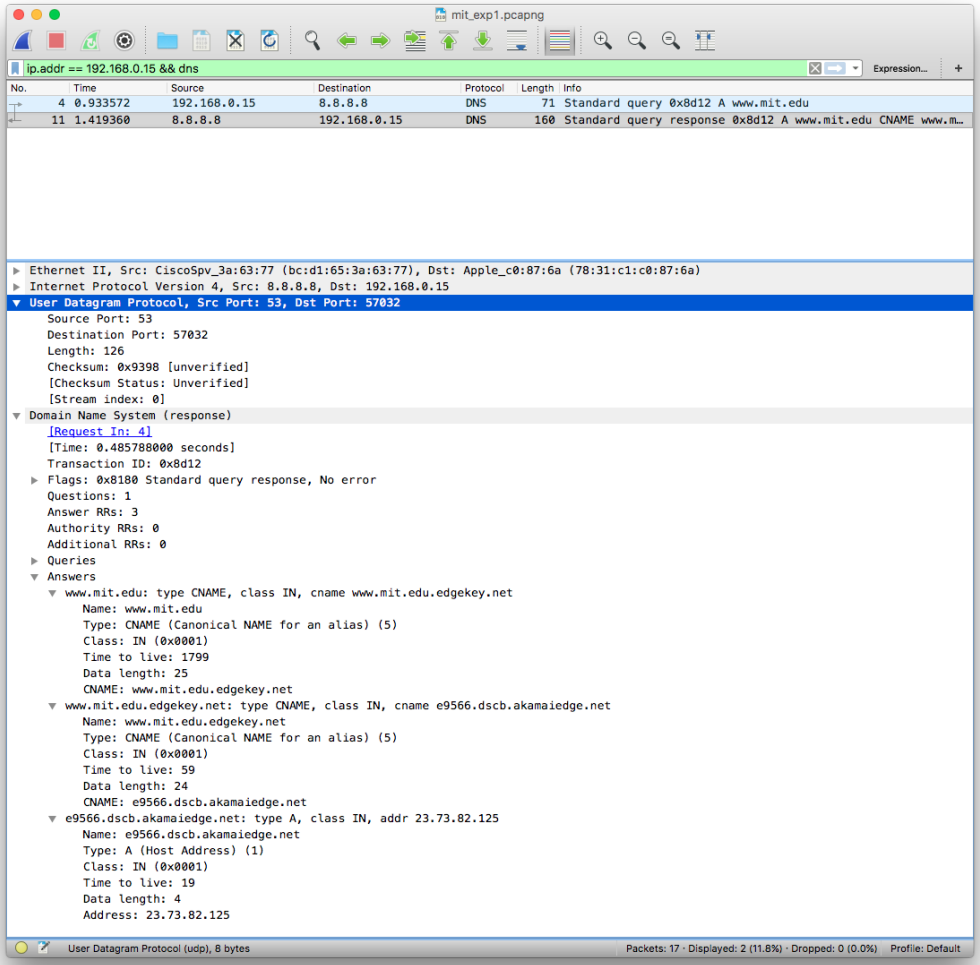


Figure 10: nslookup www.mit.edu (DNS Response)



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

  The destination port of the DNS query message is 53. The source port of the response message is also 53.

- *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 8.8.8.8, which is the IP address of one of the local DNS servers.

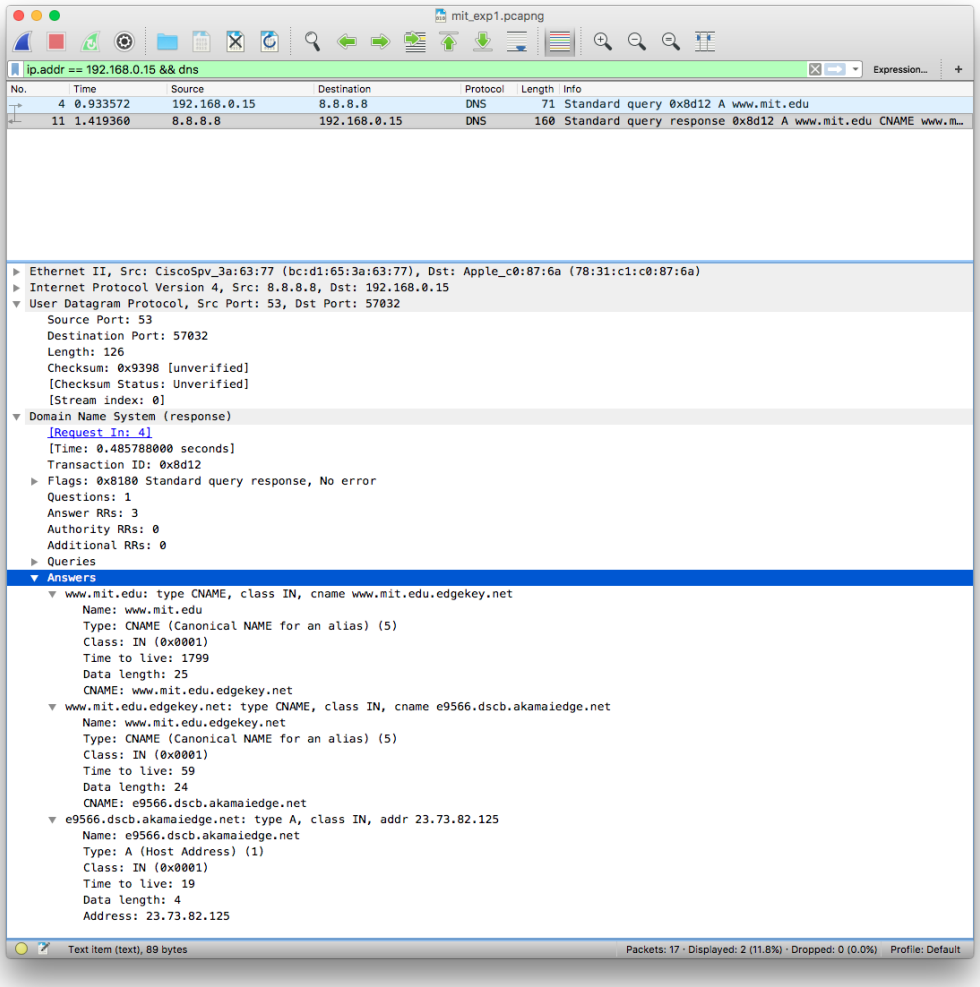
- *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

  Type A. It doesn't contain any answers.

- *Provide a screenshot.*

  Figure 11.

Figure 11: nslookup www.mit.edu (DNS Response Answers)



Now repeat the previous experiment, but instead issue the command:
nslookup –type=NS mit.edu

Figure 12: nslookup –type=NS mit.edu (DNS Request)

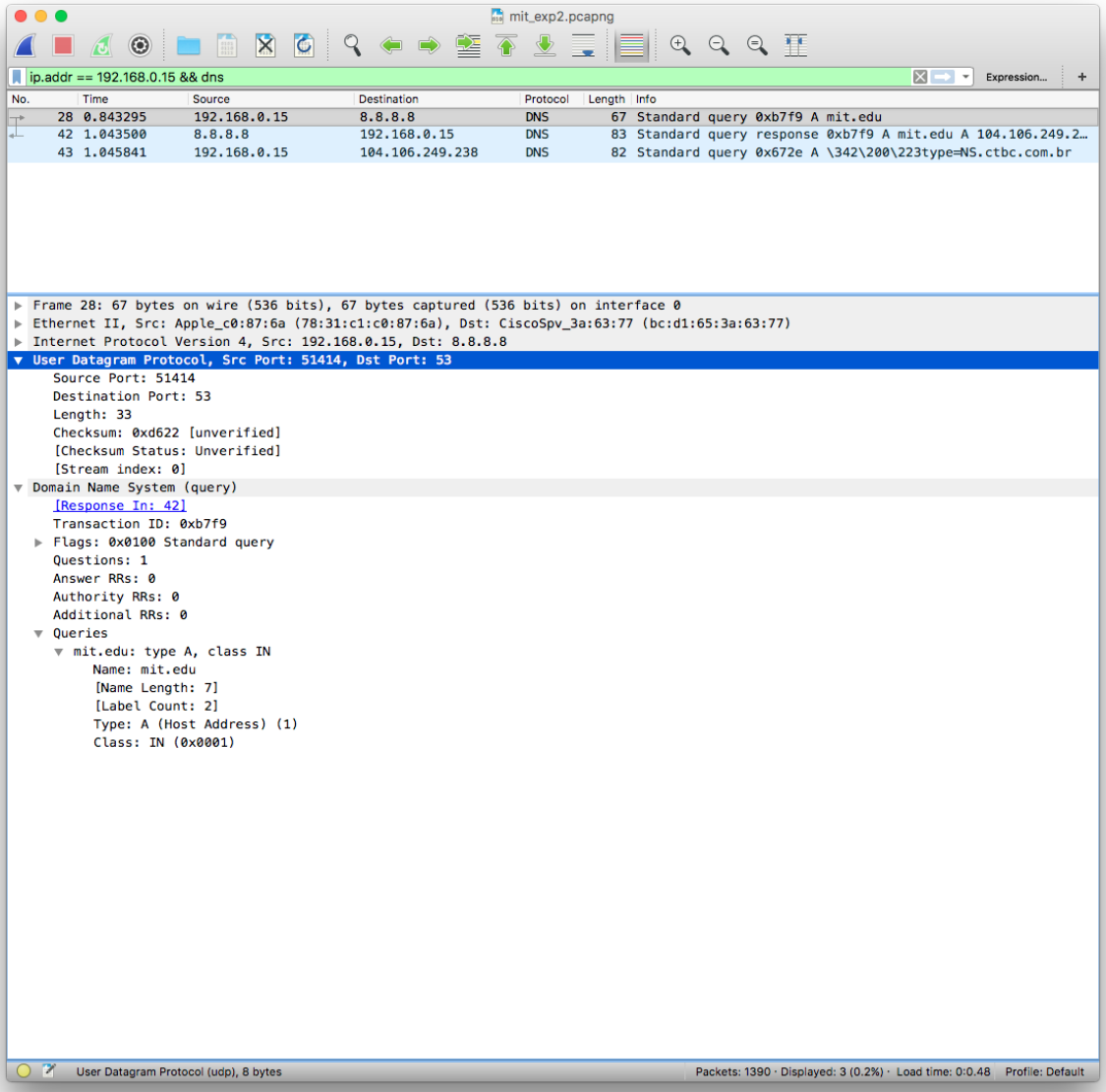
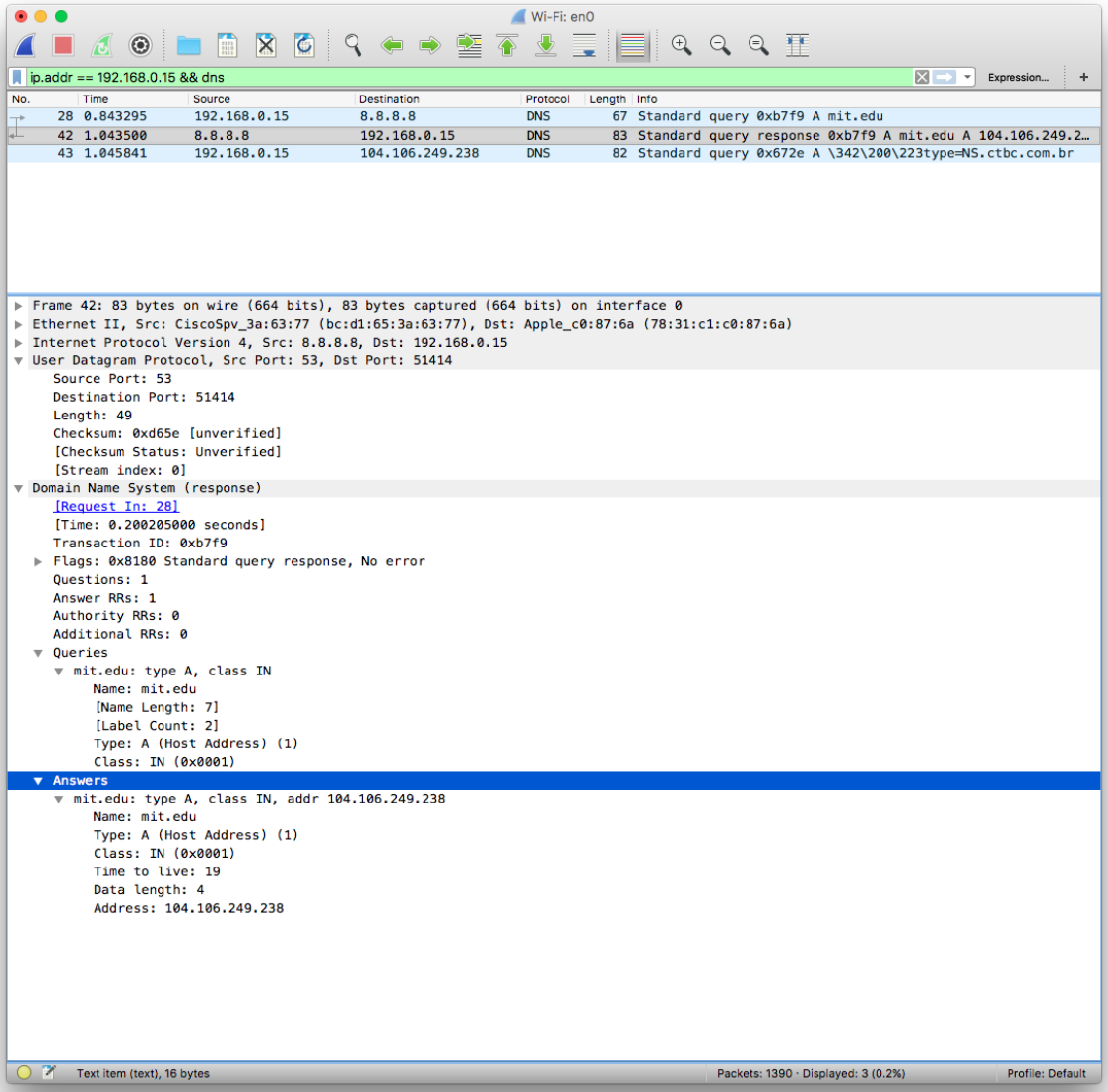


Figure 13: nslookup –type=NS mit.edu (DNS Response)



- *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 8.8.8.8, which is the IP address of one of the local DNS servers.

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

  Type A. It doesn't contain any answers.

- *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?*

  The message provides an unique answer that provides info for the server name 'mit.edu' which address is 104.106.249.238.

- *Provide a screenshot.*

  Figures 12 and 13.

Now repeat the previous experiment, but instead issue the command:
nslookup www.aiit.or.kr bitsy.mit.edu

Figure 14: nslookup www.aiit.or.kr bitsy.mit.edu (DNS Request)

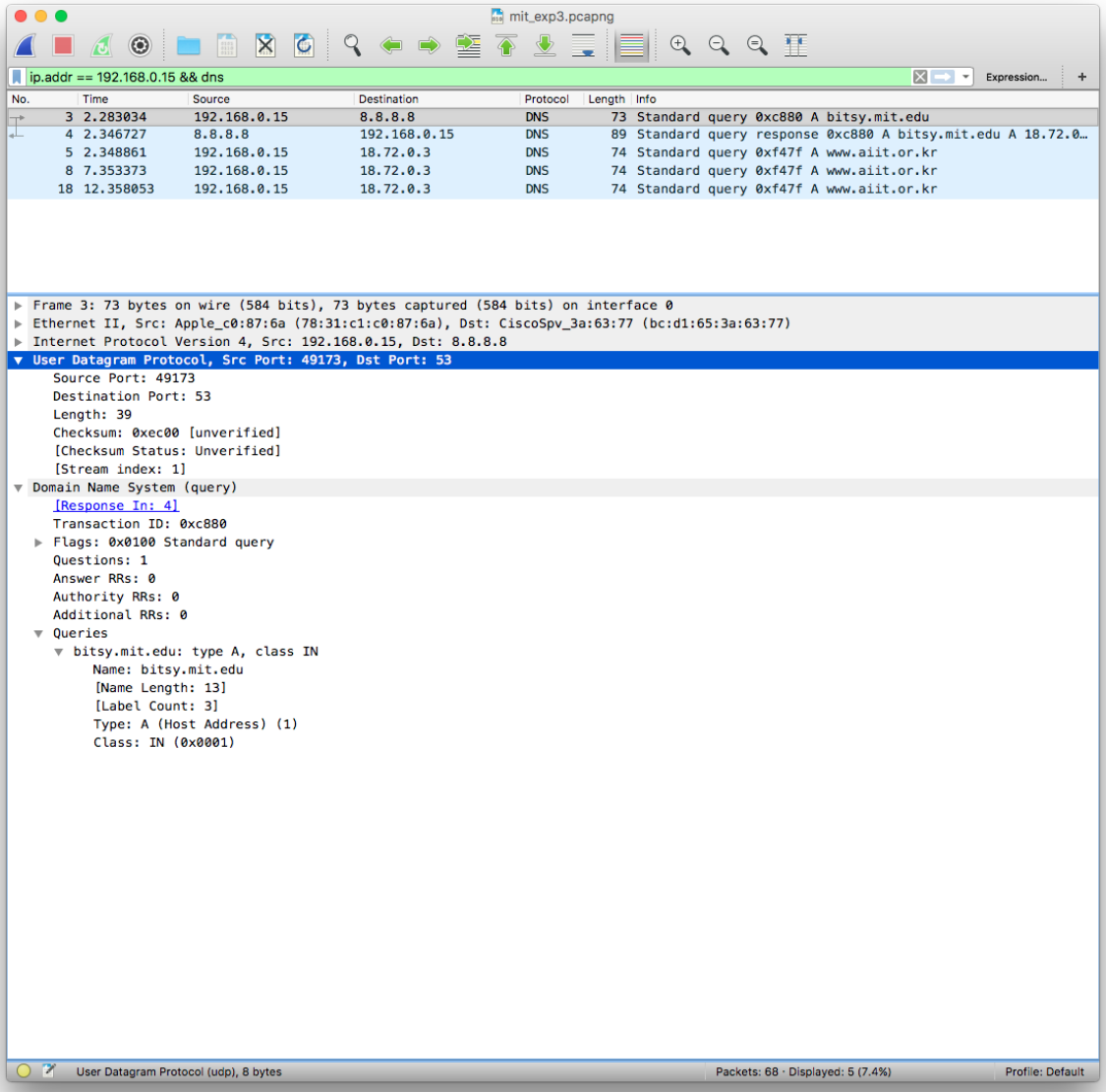
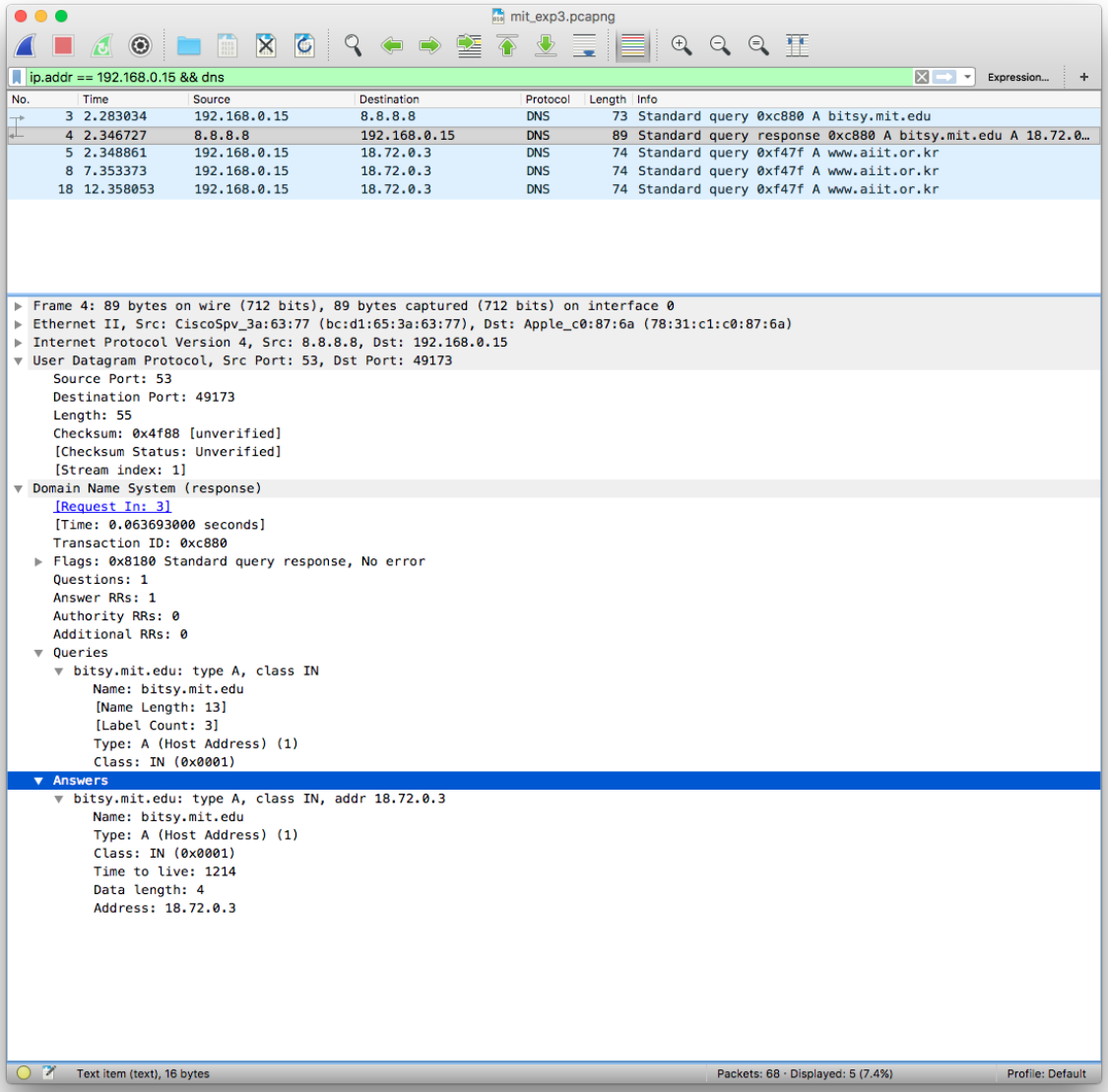


Figure 15: nslookup www.aiit.or.kr bitsy.mit.edu (DNS Response)



- *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?*

  The DNS query message is sent to 8.8.8.8, which is the IP address of one of the local DNS servers.

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

  Type A. It doesn't contain any answers.

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

  Only one answer is provided. The answer contains the following information: name of the host, type, class, TTL, data length and IP address.

- *Provide a screenshot.*

  Figures 14 and 15.