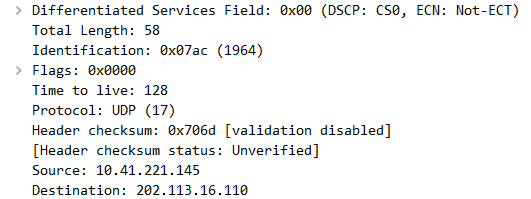
**Lab3 Wireshark\_DNS**

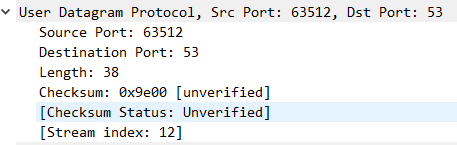
1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

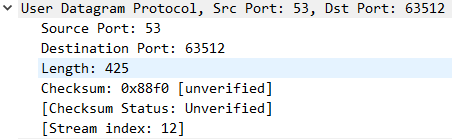
They are sent over UDP.



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

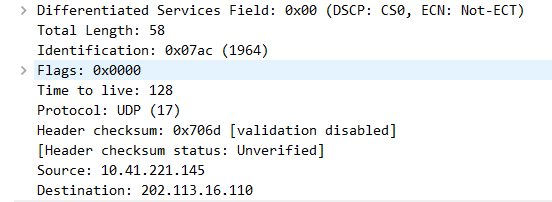
The destination port for the DNS query message is 53, and the source port for the DNS response message is also 53.



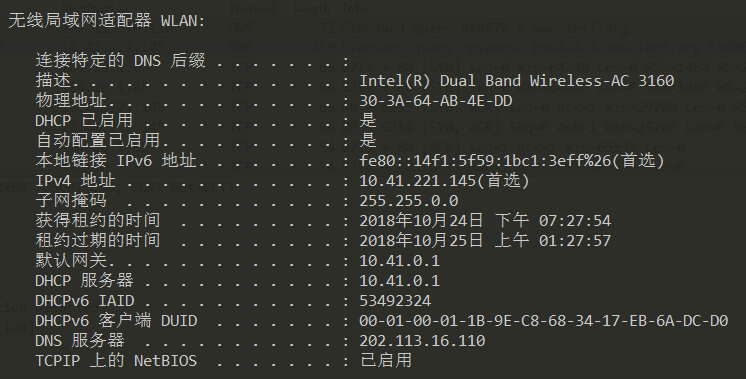


1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query message is sent to 202.113.16.110.



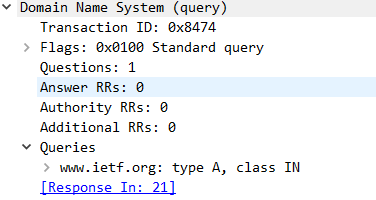
Yes, they are the same.



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

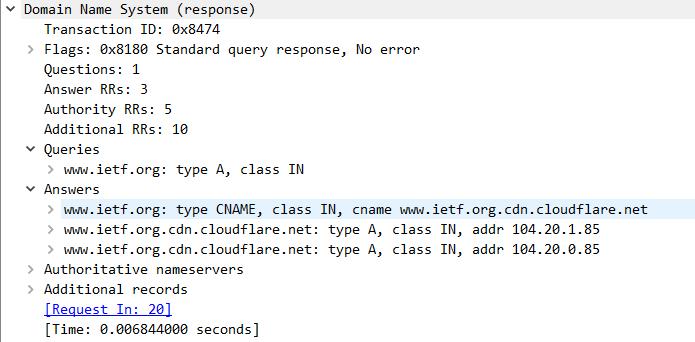
The type of DNS query is A.

No, it doesn’t contain any answers.



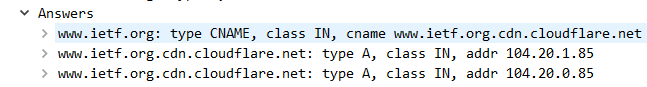
1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

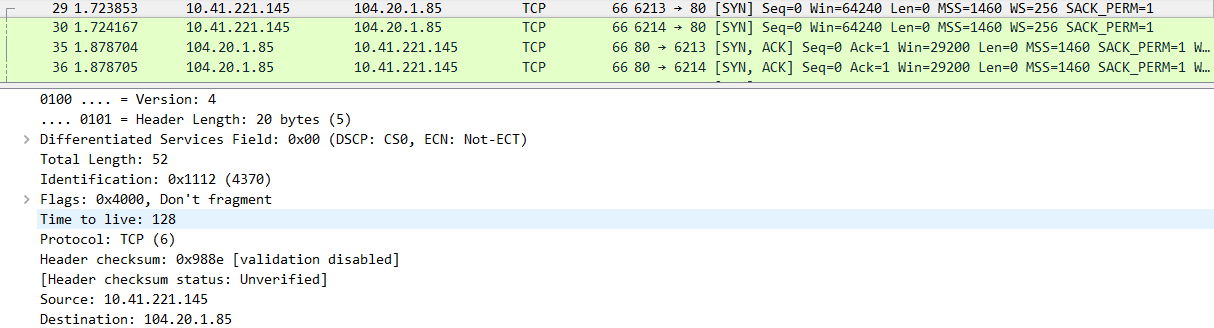
Three answers are provided in the DNS response message.



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?

Yes, it does.



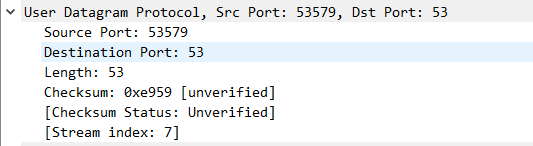


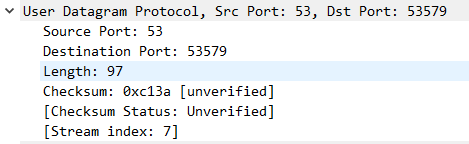
1. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No, my host doesn’t issue new DNS queries.

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

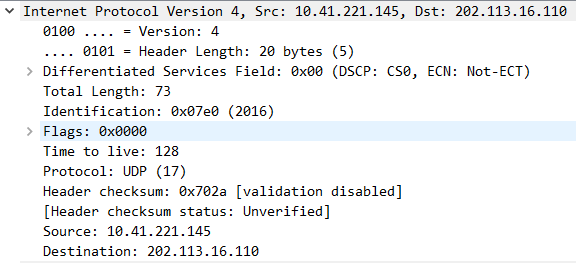
The destination port for the DNS query message is 53, and the source port of DNS response message is also 53.

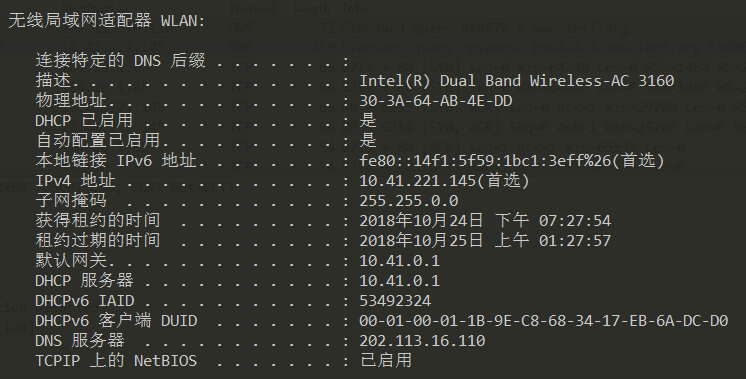




1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

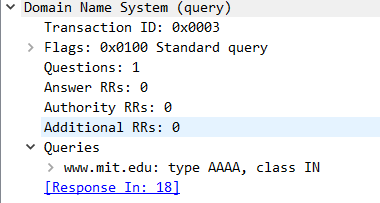
To 202.113.16.110, this is my default local DNS server.



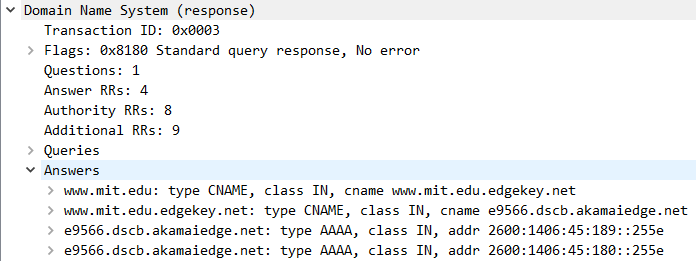


1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The type of DNS query are AAAA, and it doesn’t have any answers in query message.

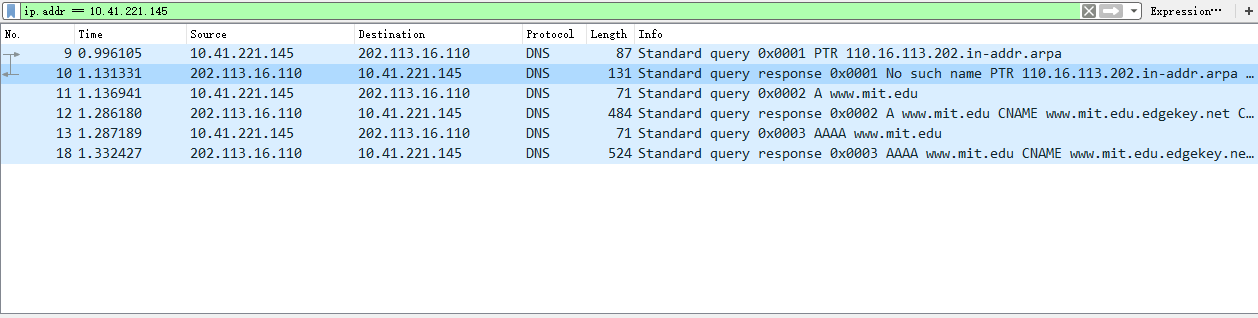


1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



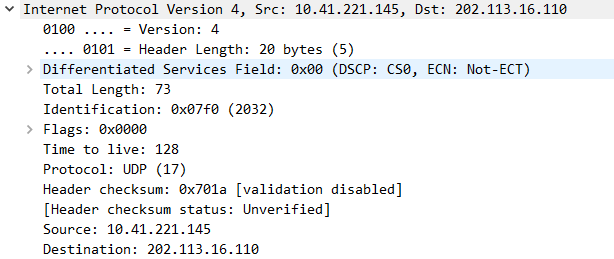
The DNS response has four answers provided.

1. Provide a screenshot.

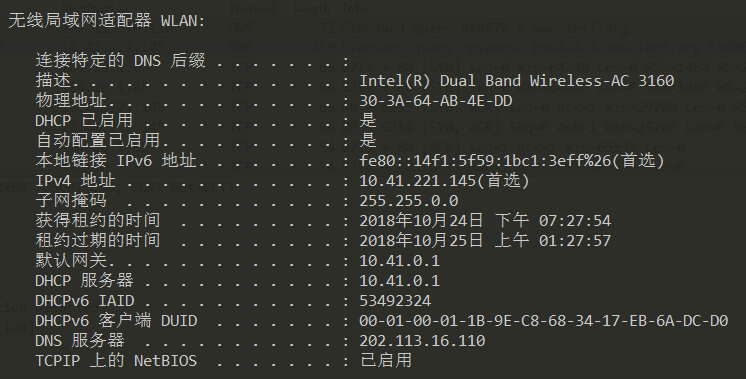


1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS message is sent to 202.113.16.110.

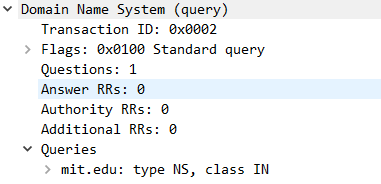


Yes.



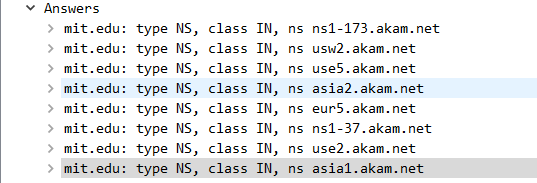
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The type of DNS is NS.

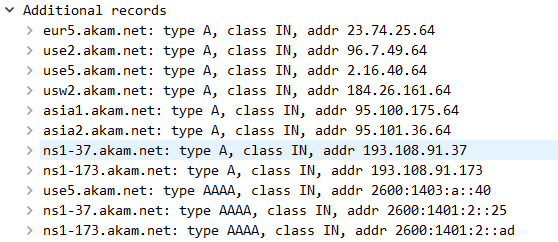


No.

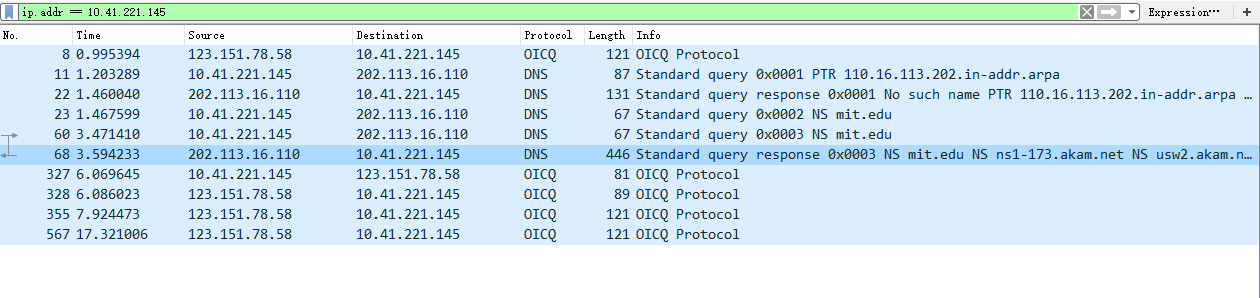
1. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?



Yes, it does.

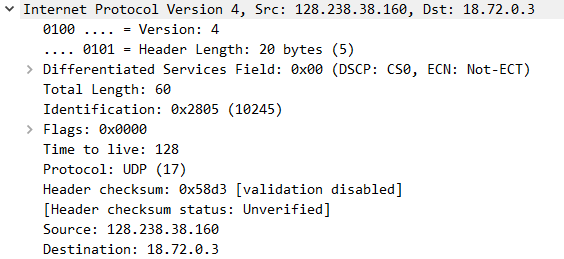


1. Provide a screenshot.



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?

The DNS query message is sent to 18.72.0.3.



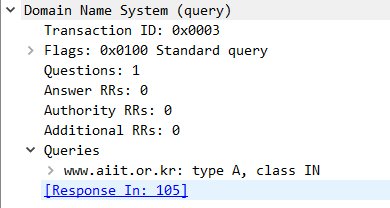
No, it’s not.

It corresponds to the IP address of bitsy.mit.edu.

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

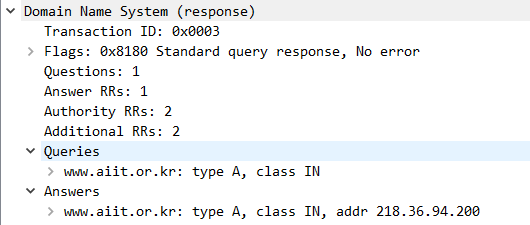
The type of DNS is A.

No, it doesn’t.



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

Only one answer is provided.



1. Provide a screenshot.

