Wireshark Lab:

DNS

v

8

.0

Supplement to

*Computer Networking: A Top*

*-*

*Down*

*Approach,*

*8*

*th*

*ed.*

*,*

J.F. Kurose and K.W. Ross

*“Tell me and I forget. Show me and I remember. Involve me*

*and I understand.”*

Chinese proverb

©

2005

-

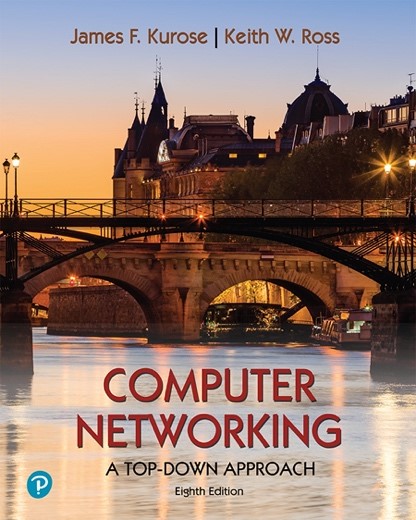
20

20

, J.F Kurose and K.W. Ross, Al

l

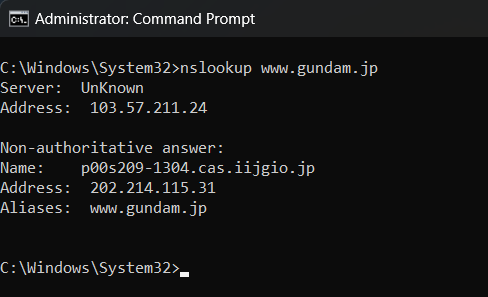
Rights Reserved



Student Name : Nguyễn Hữu Hiếu

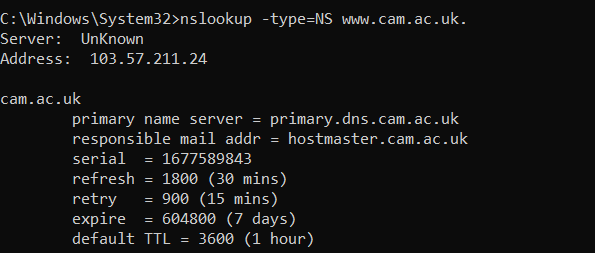
Student ID : 2013149

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



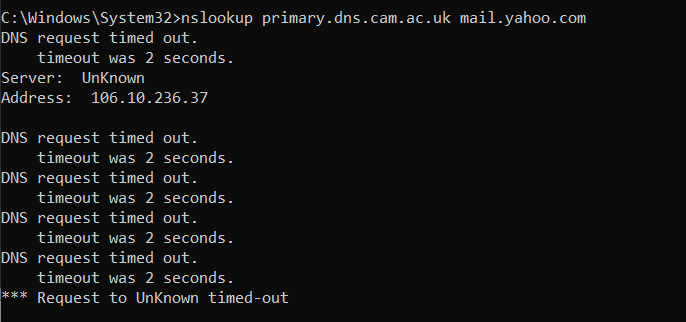
Address: 202.214.115.31

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



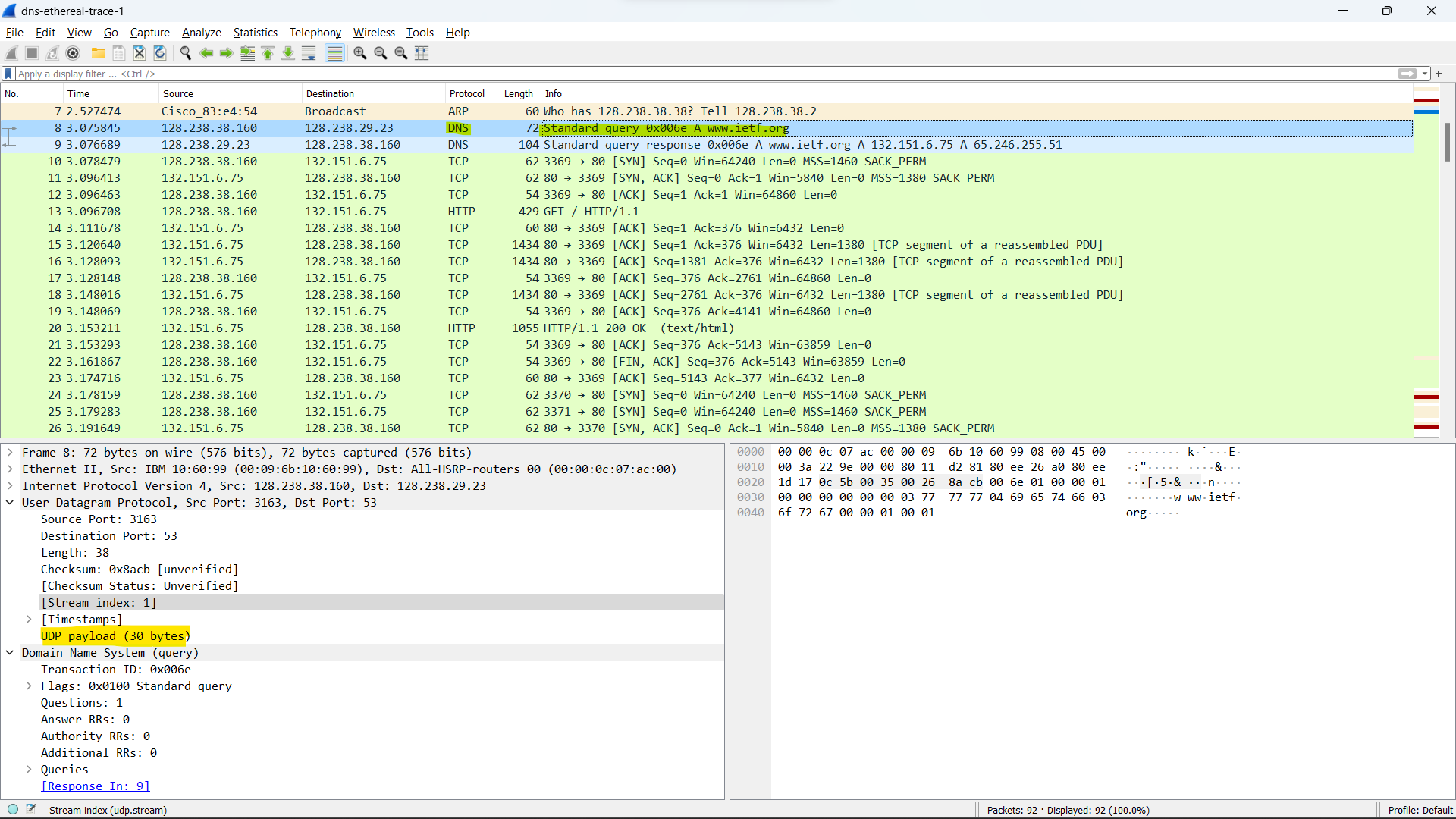
The authoritative DNS server for Cambridge is primary.dns.cam.ac.uk

1. 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 106.10.236.37

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



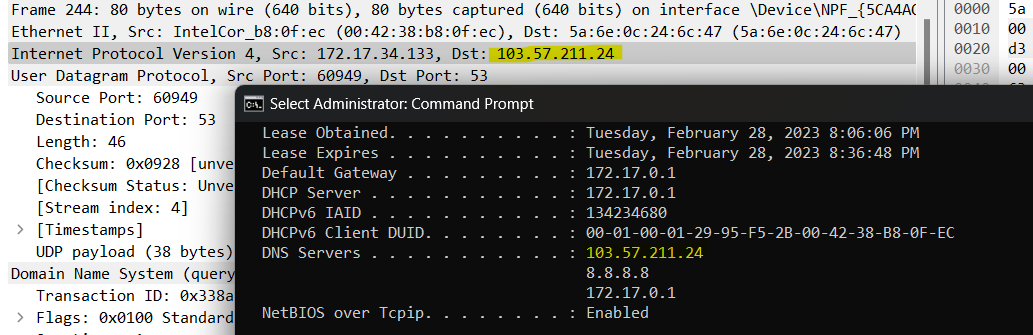
The query and response messages are sent via UDP.

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

Destination Port: 53

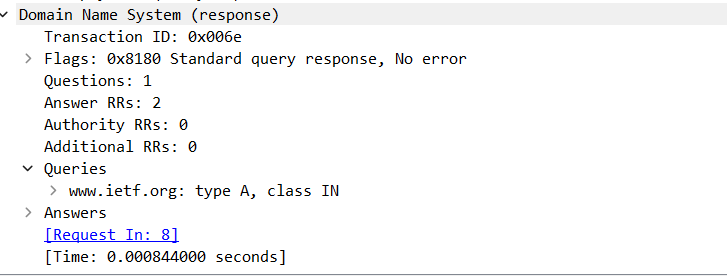
Source Port: 3163

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?



IP addresses is the same

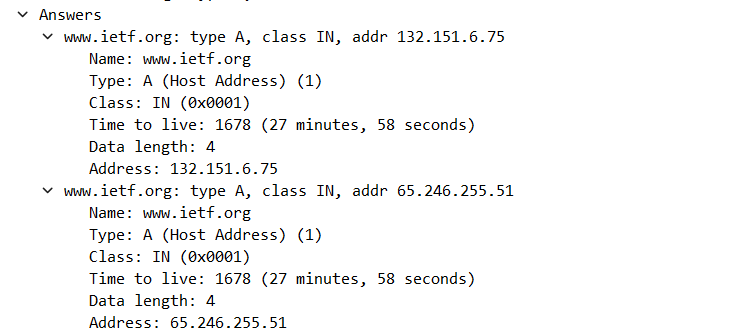
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



Type A

No answer

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

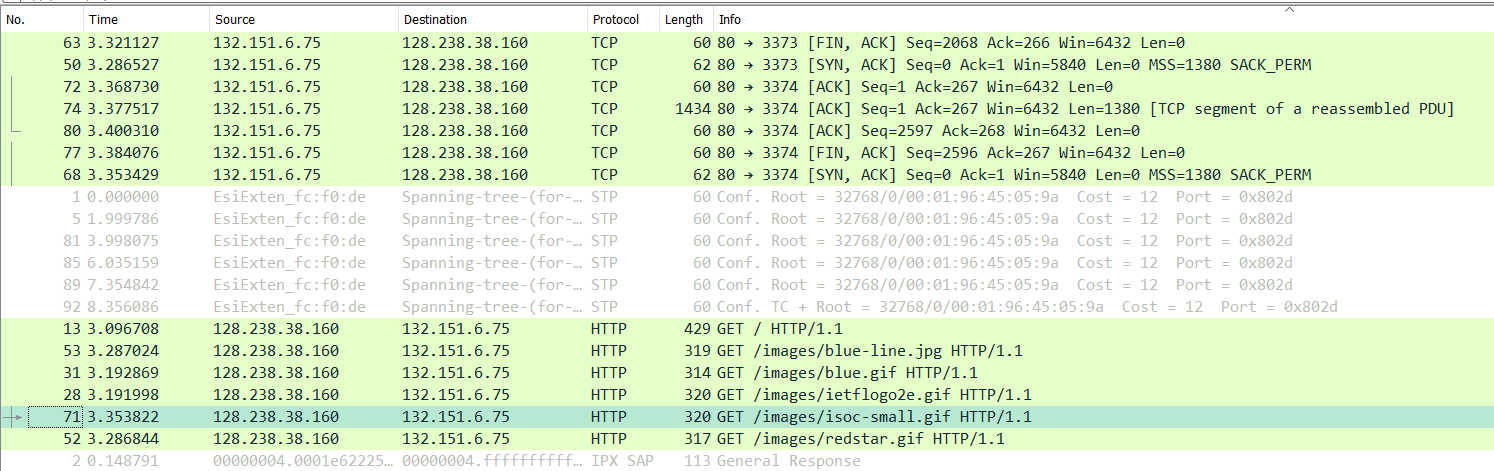


This DNS response message provided two answers. The answers contains the address of the website that it was queried for.

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?

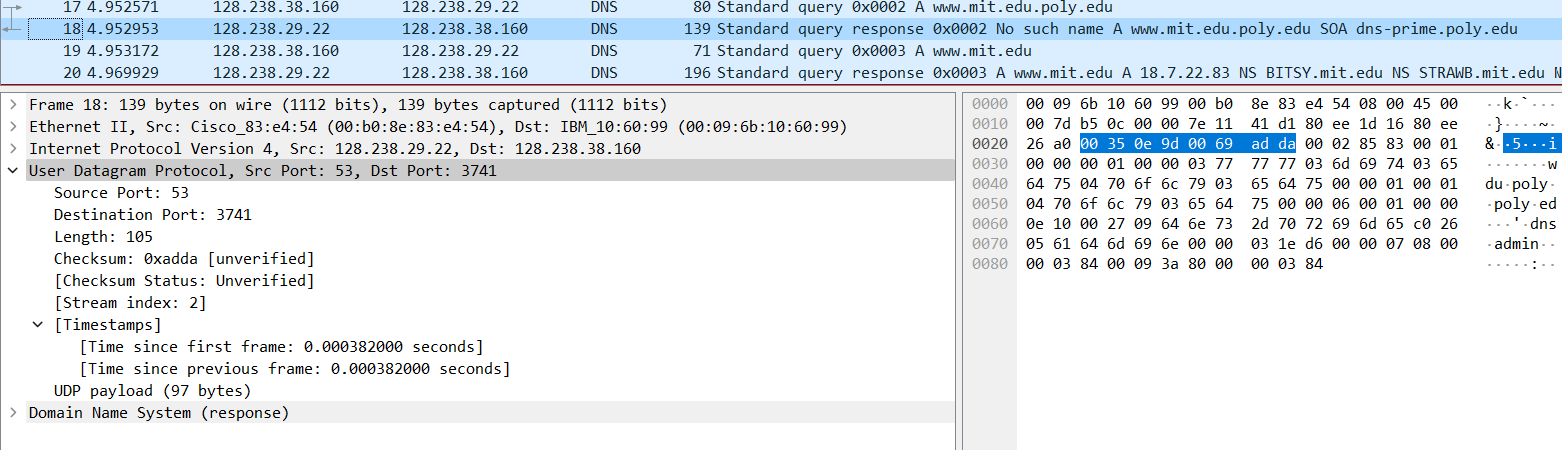
The destination IP address of the SYN packet corresponds to the address provided by the DNS response, 12.22.58.30.

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



Yes, the host issues new DNS queries for each image

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



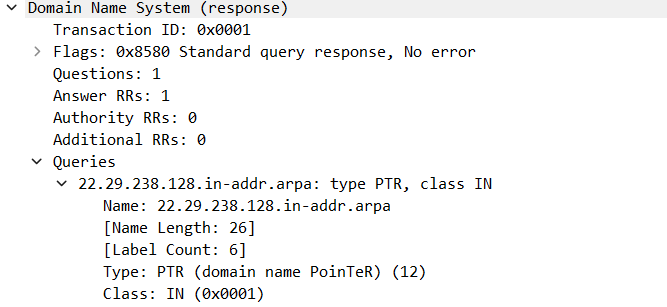
The destination port for the DNS query message is port 53. The source port of the DNS response message is also port 53

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

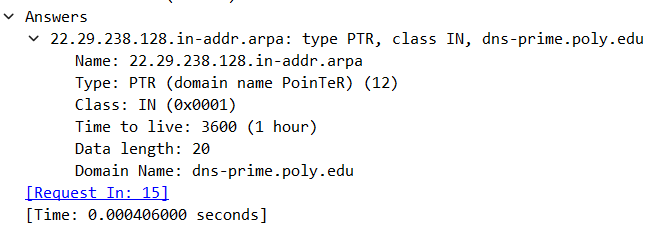
I can’t answer this question because my WireShark is not work.

But I guess Ip address that The DNS query message is the same IP address of local DNS server.

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

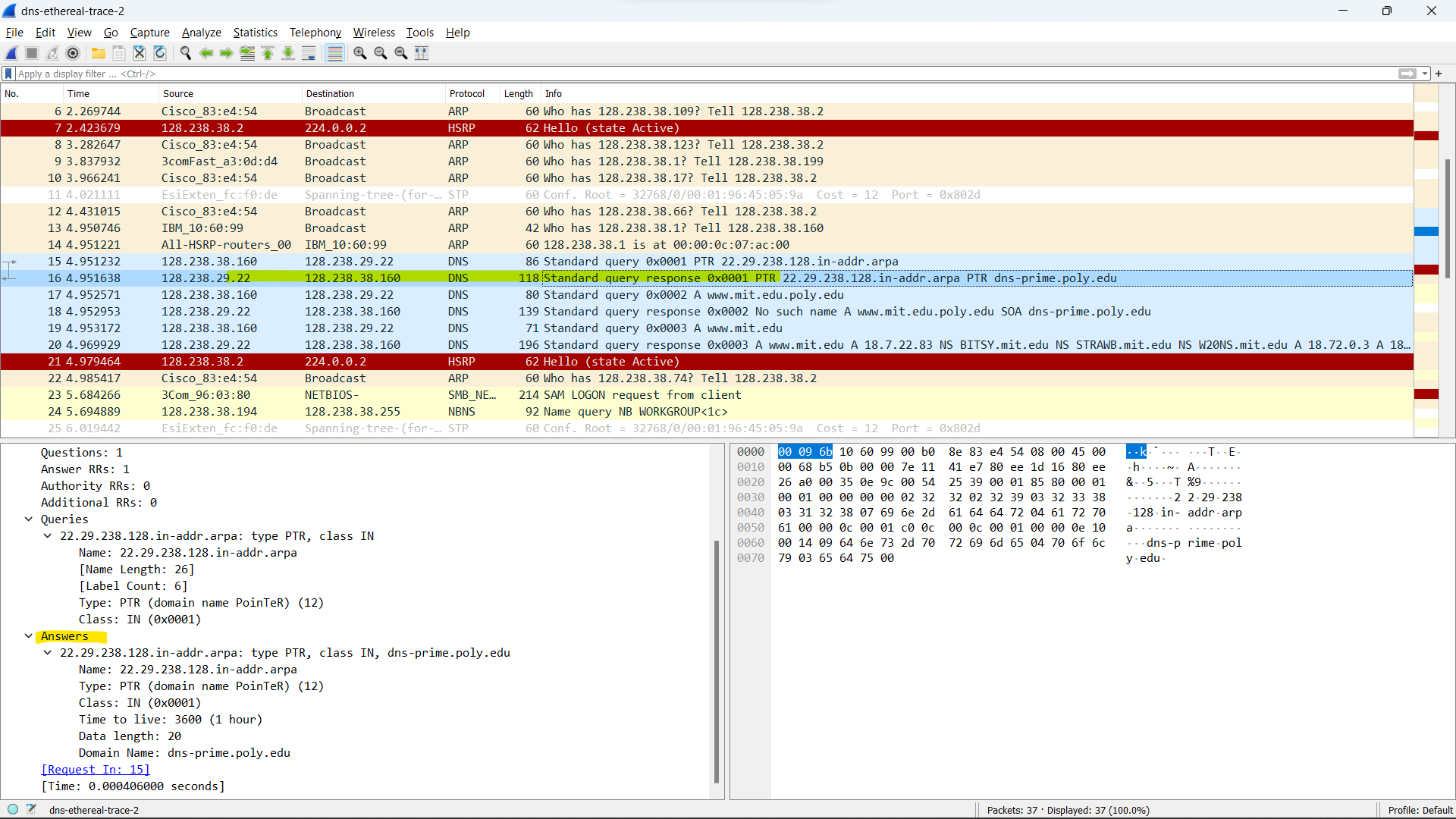
 This message is of type PTR and contains no answers.

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

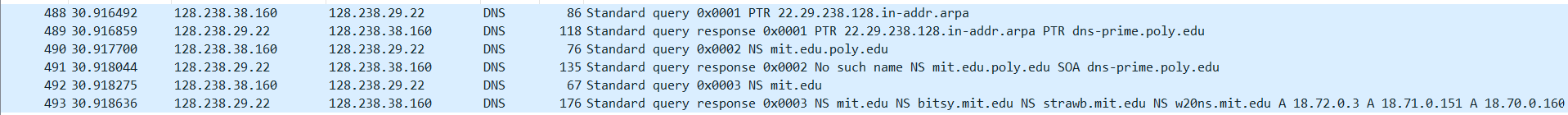


The first DNS response message contains one answer. This answer contains the next DNS server to query en route to <http://www.mit.edu>

1. Provide a screenshot.

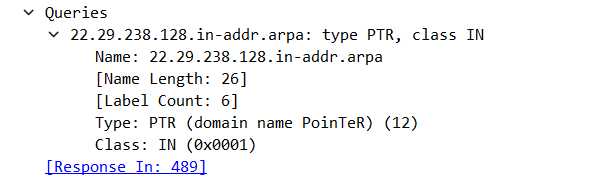


1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



IP address of DNS query message sent is 128.238.38.160

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



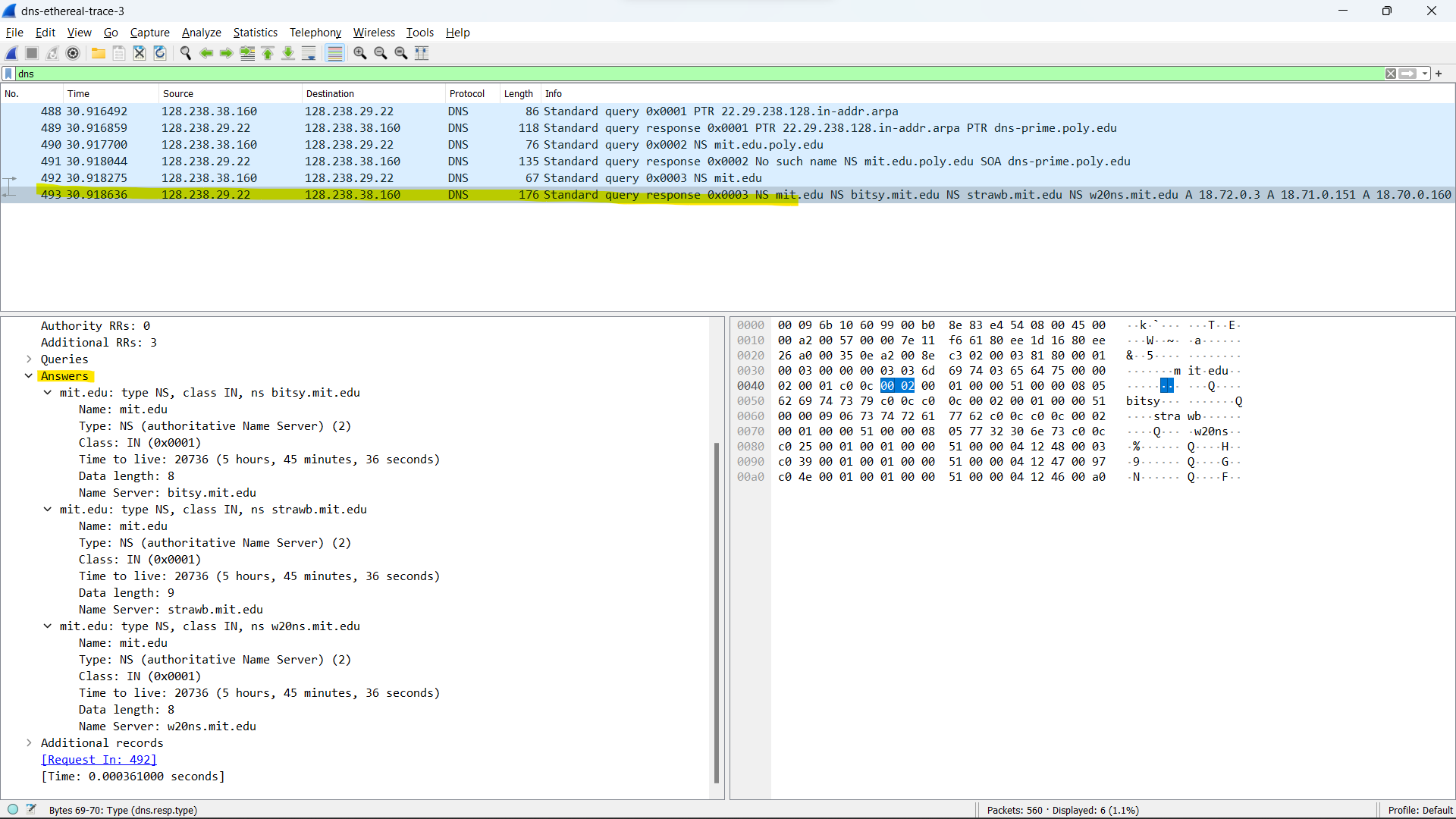
It is a type PTR DNS query that contains no answers.

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?

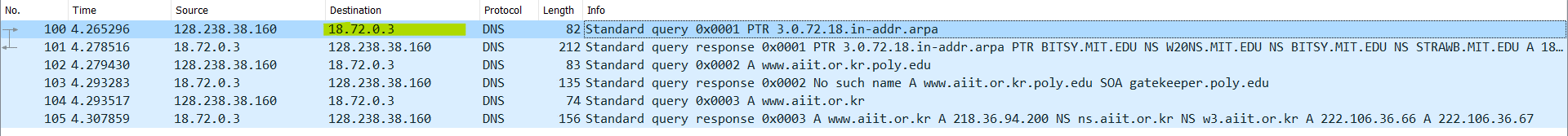
It provides <http://www.mit.edu>

This response message does not include IP addresses

1. Provide a screenshot.

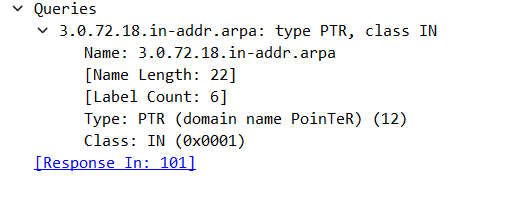


1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?



The DNS query message is sent to 18.72.0.3 which is not the same as my local DNS server. This IP address corresponds to [www.aiit.or.kr](http://www.aiit.or.kr).

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 Domain name pointer, type PTR, and does not contain any answers.

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

It contain the ip address of each of them

1. Provide a screenshot.
2. 