Wireshark Lab 3

DNS

Suraj Durgesht

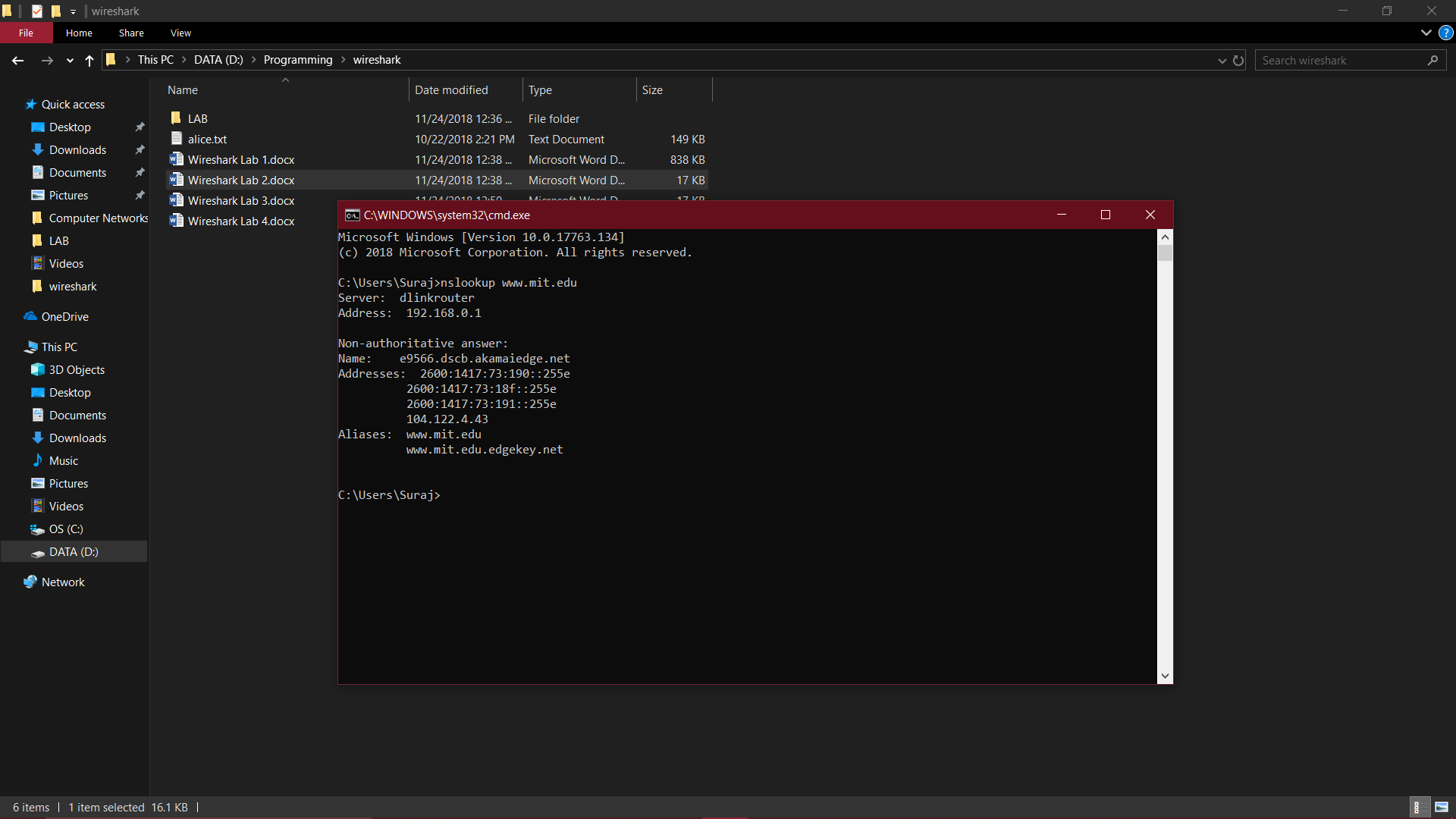
(16EC06)

Instructor: Dr. Rajendra Hegadi

1. nslookup (name server lookup)

Que1. Run nslookupto obtain the IP address of a Web server in Asia. What is the IP address of that server?

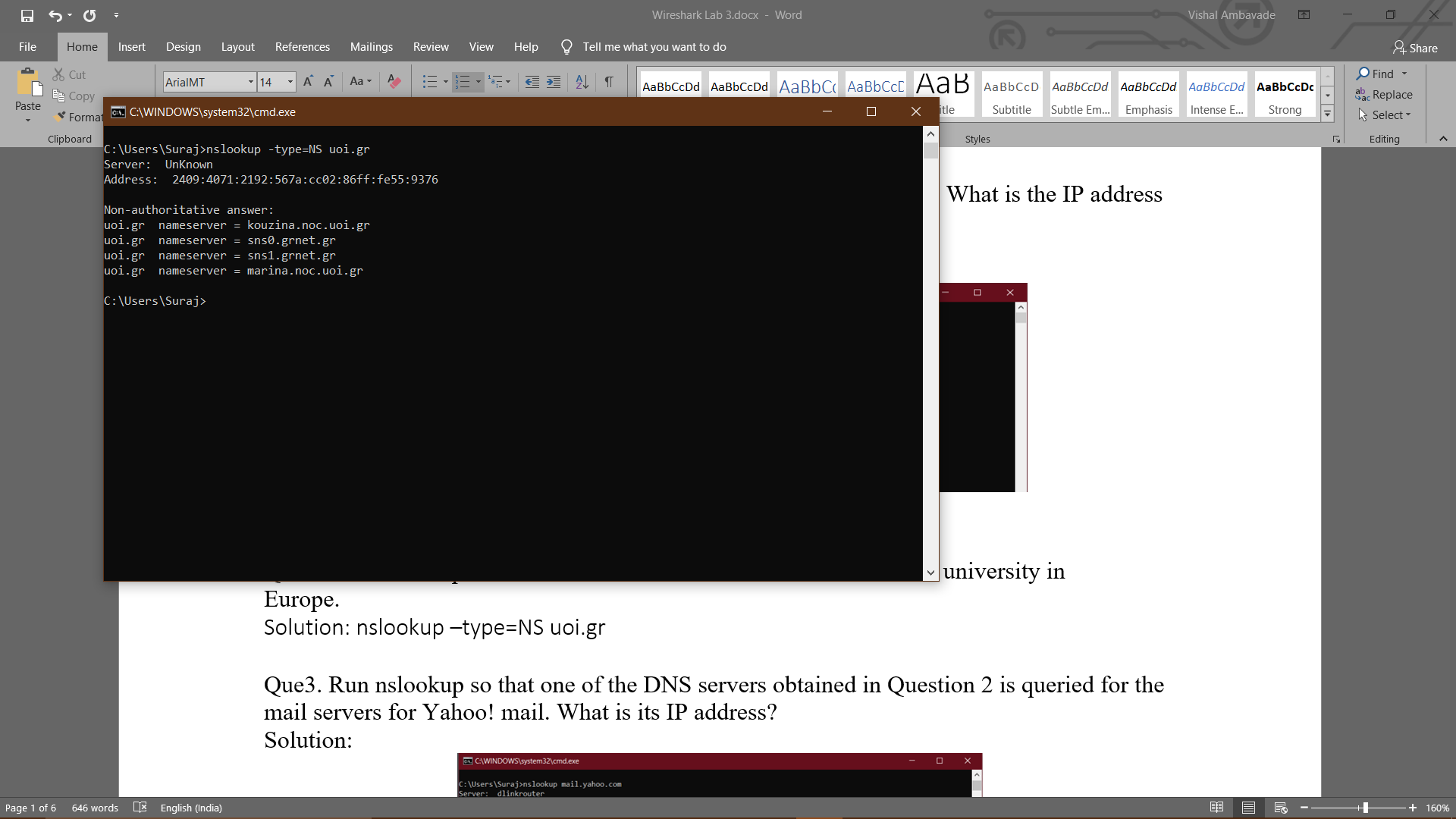
Solution: nslookup www.mit.edu



Que2. Run nslookupto determine the authoritative DNS servers for a university in

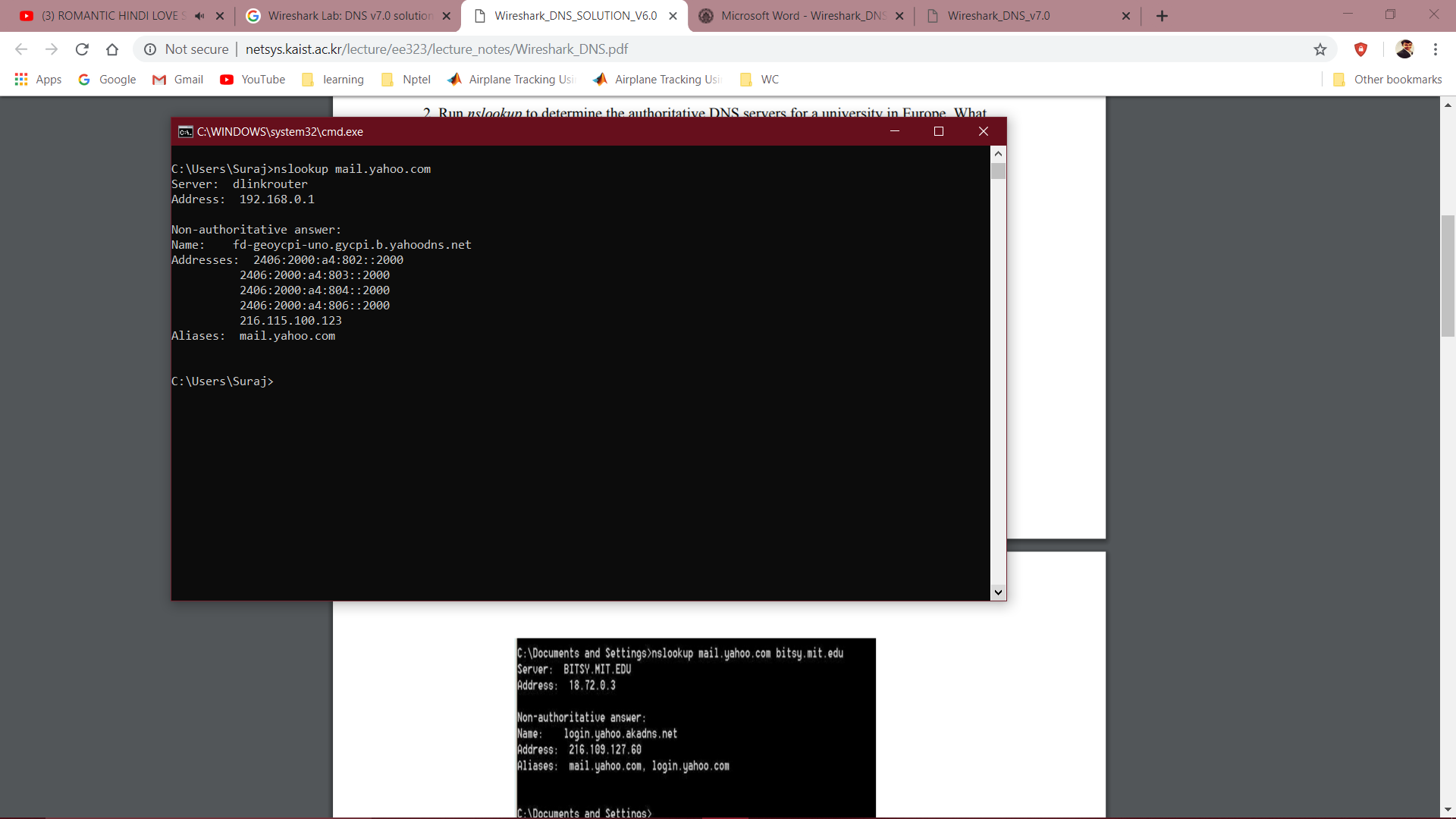
Europe.

Solution: nslookup –type=NS uoi.gr



Que3. Run nslookupso that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Solution:



1. Tracing DNS with Wireshark

Que4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Solution: UDP

Que5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Solution: The destination port for the DNS query is 53 and the source port of the DNS response is 53.

Que6. 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?

Solution:

It’s sent to 192.168.0.1, which is the IP address of one of my local DNS servers.

Que7. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contains any “answers”?

solution:

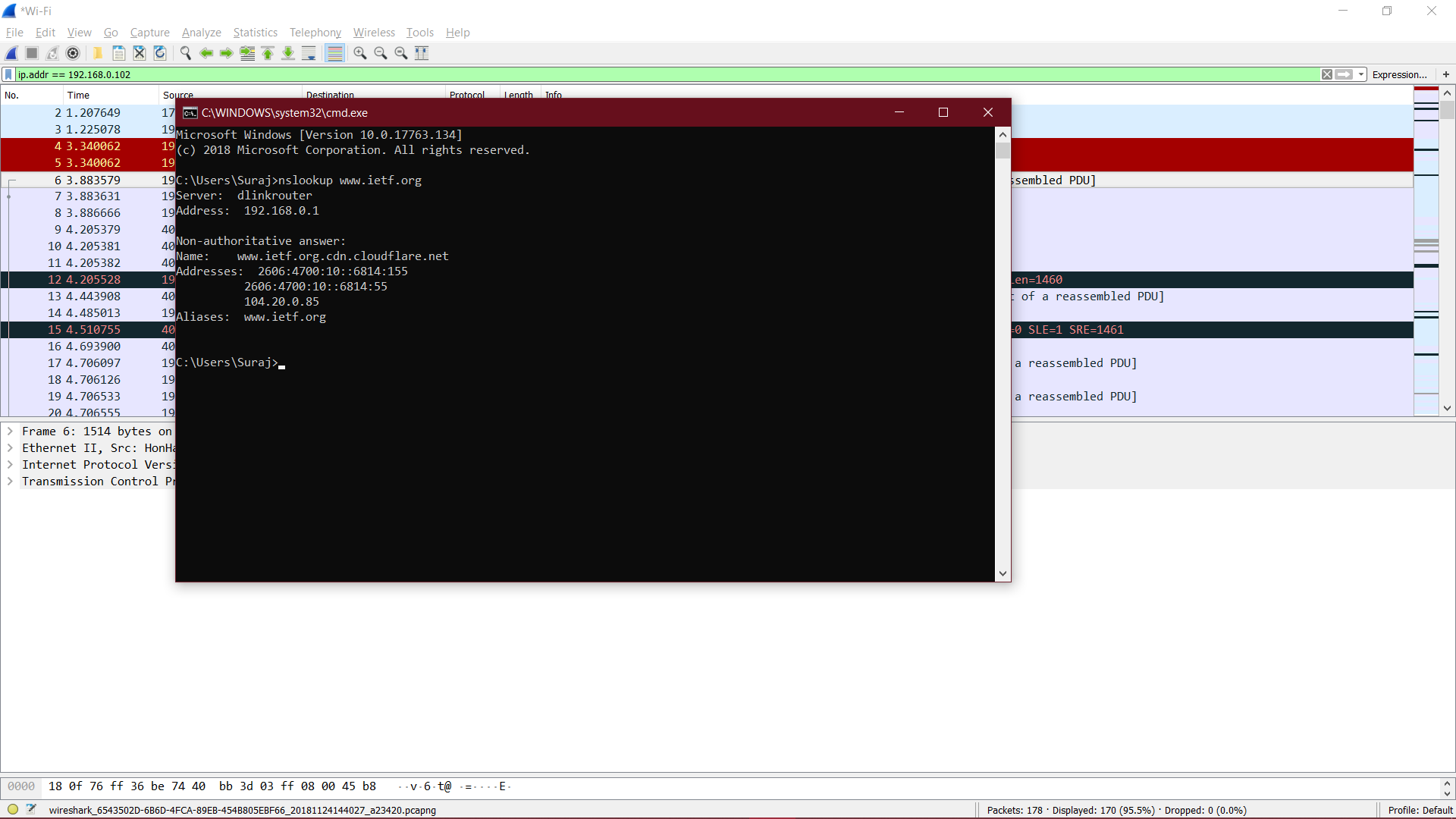
It’s a type A Standard Query and it doesn’t contain any answers.

Que8. Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?

Solution:

There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.



Que9. 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?

Solution:

The first SYN packet was sent to 104.20.0.85 which corresponds to the first IP address provided in the DNS response message.

Que10. This web page contains images. Before retrieving each image, does your host

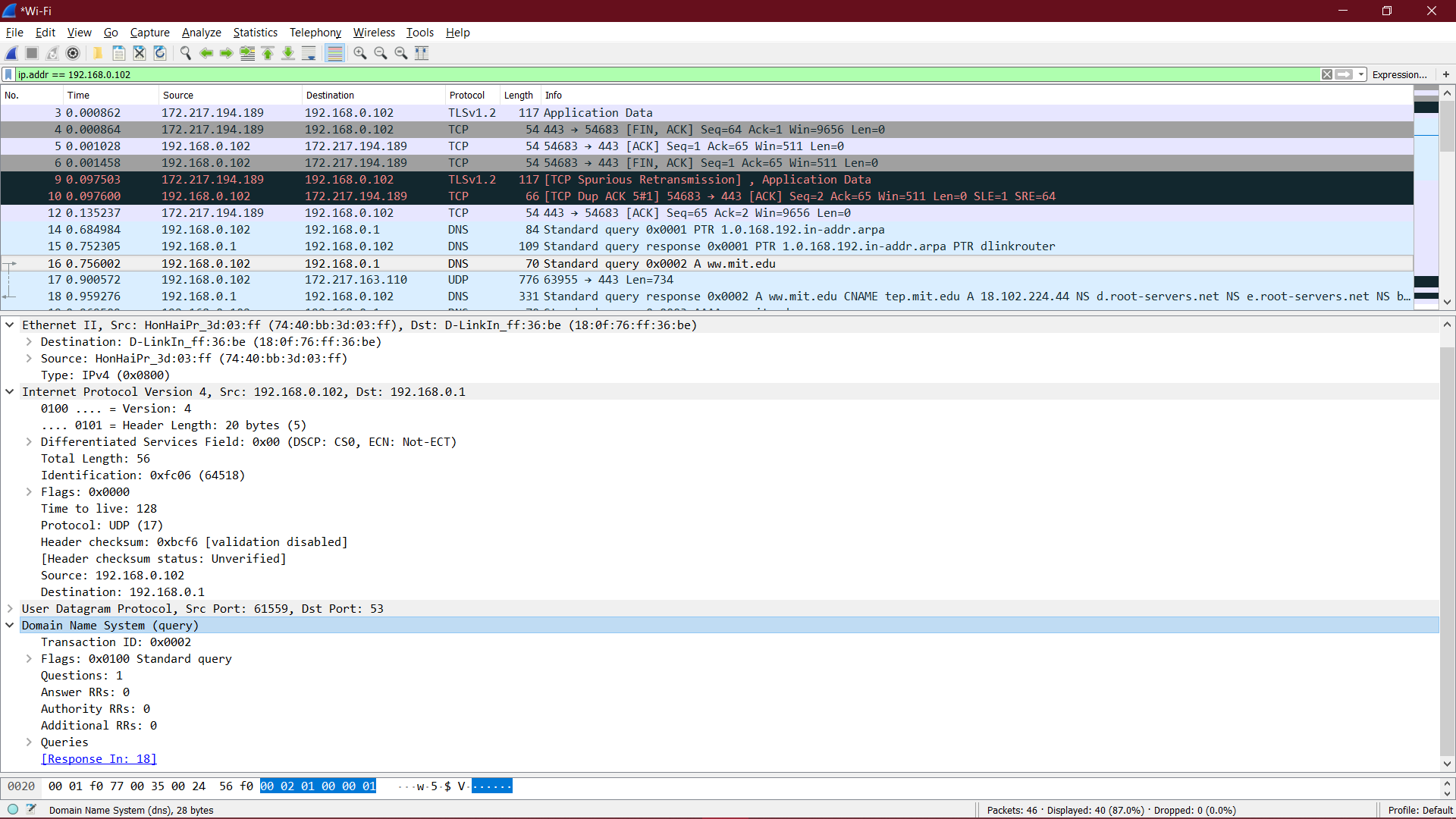
issue new DNS queries?

Solution: No

Que11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Solution:

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



Que12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Solution: 192.168.0.1

Que13. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contains any “answers”?

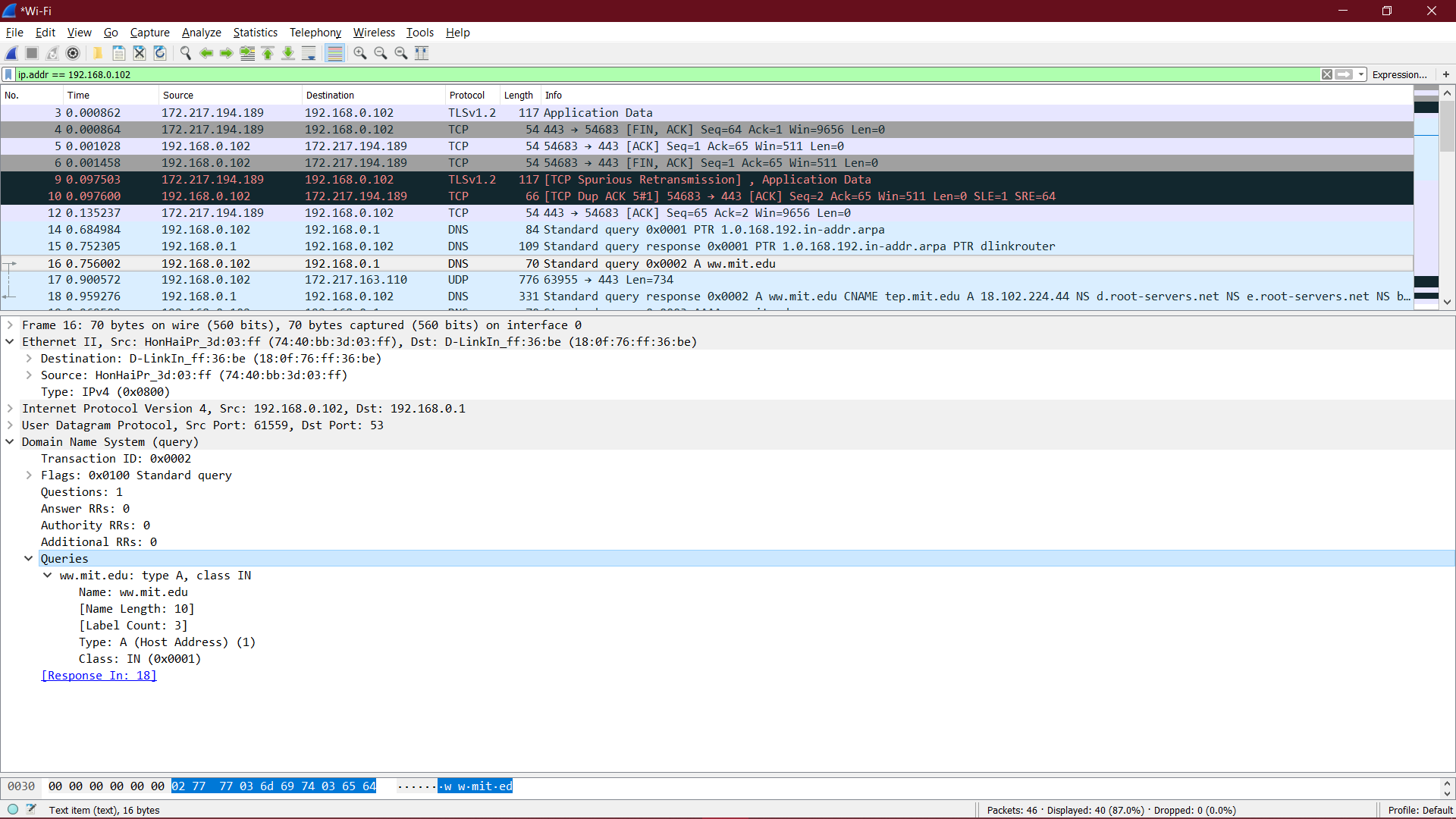
solution:

The query is of type A

Que14. Examine the DNS response message. How many “answers” are provided? What

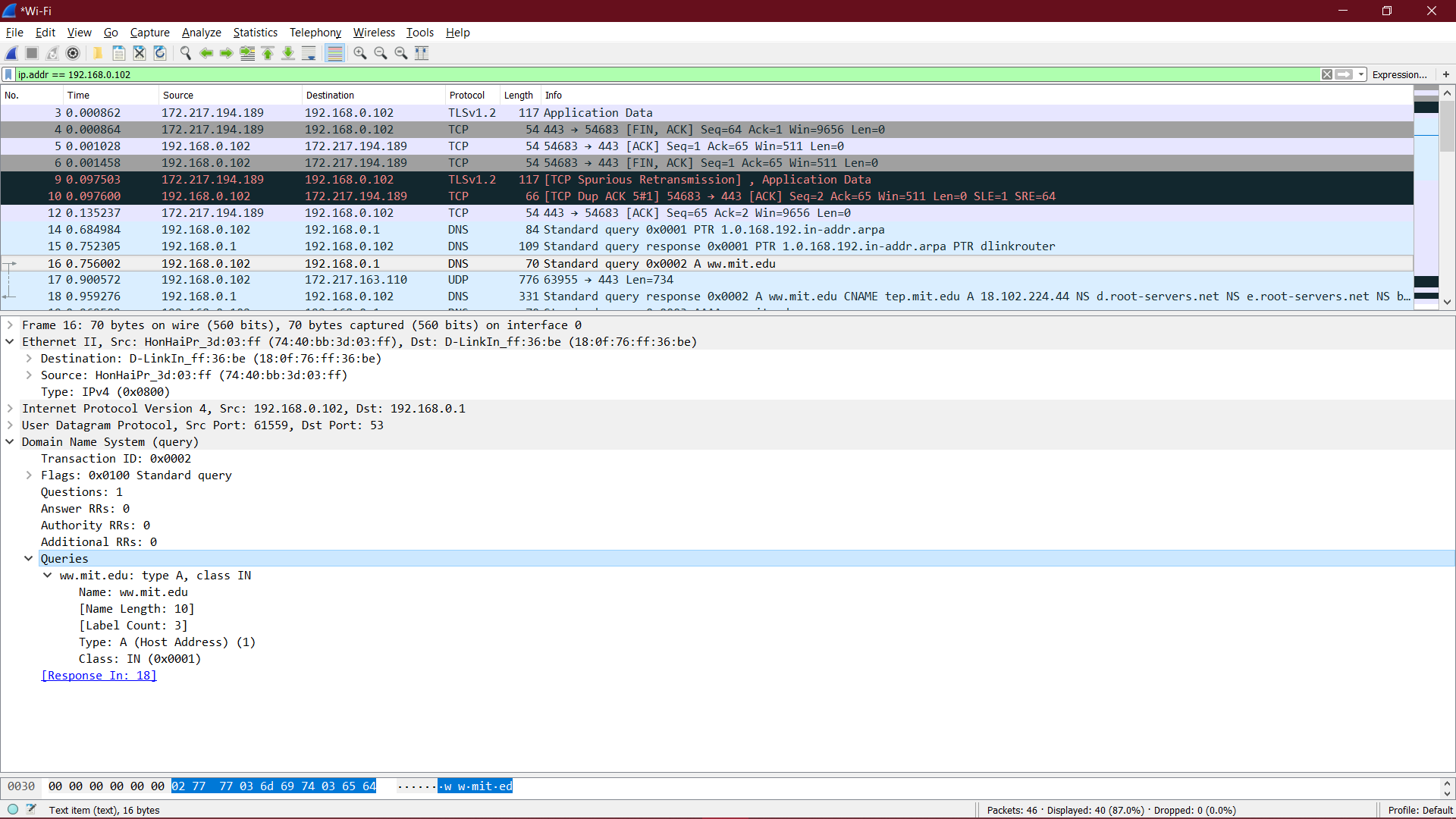
do each of these answers contain?

Solution:



Que15. Provide a screenshot.

Solution:



Que16. To what IP address is the DNS query message sent? Is this the IP address of your

default local DNS server?

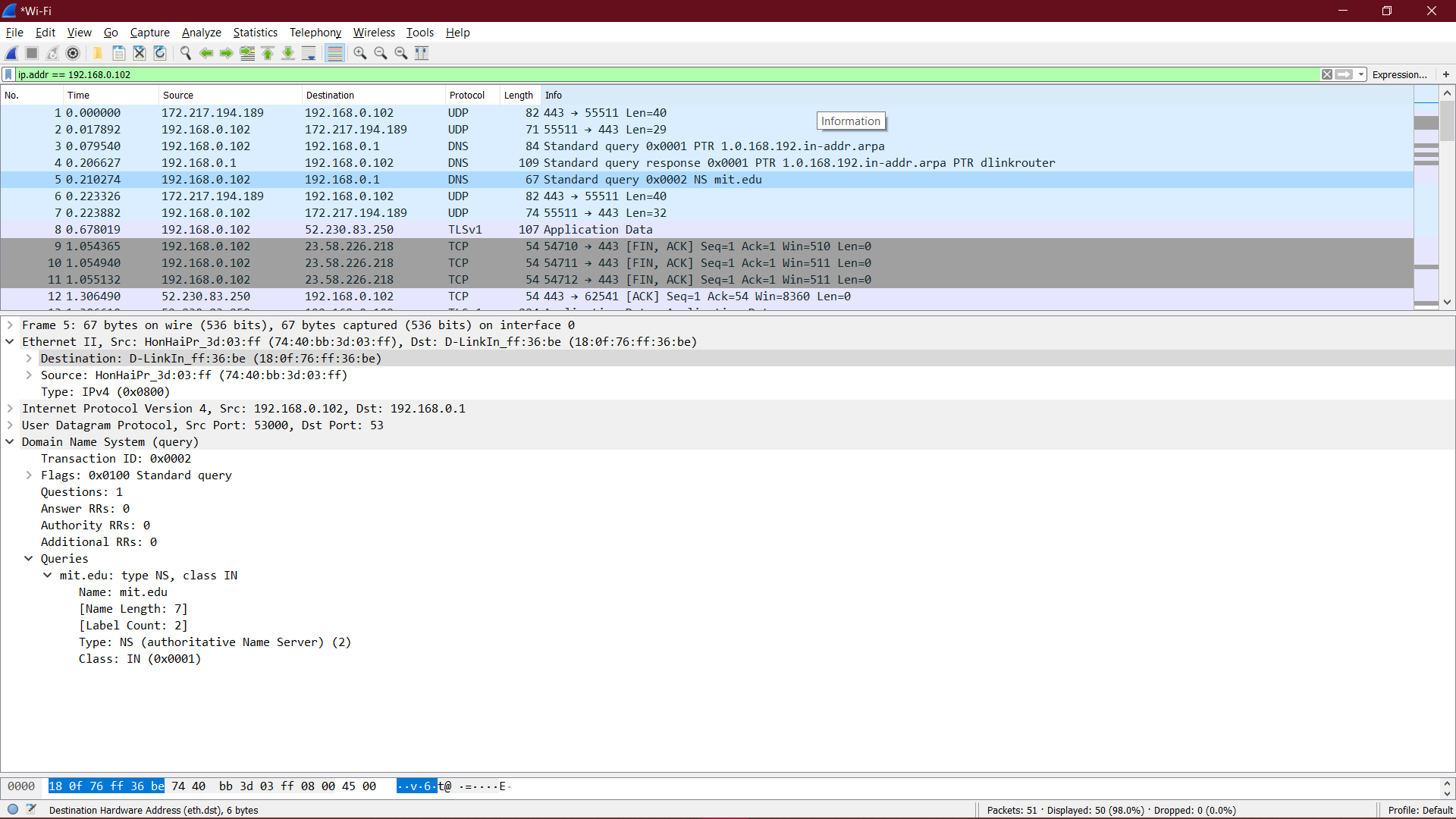
Solution:

It was sent to 192.168.0.1 which is my default DNS server.

Que17. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contains any “answers”?

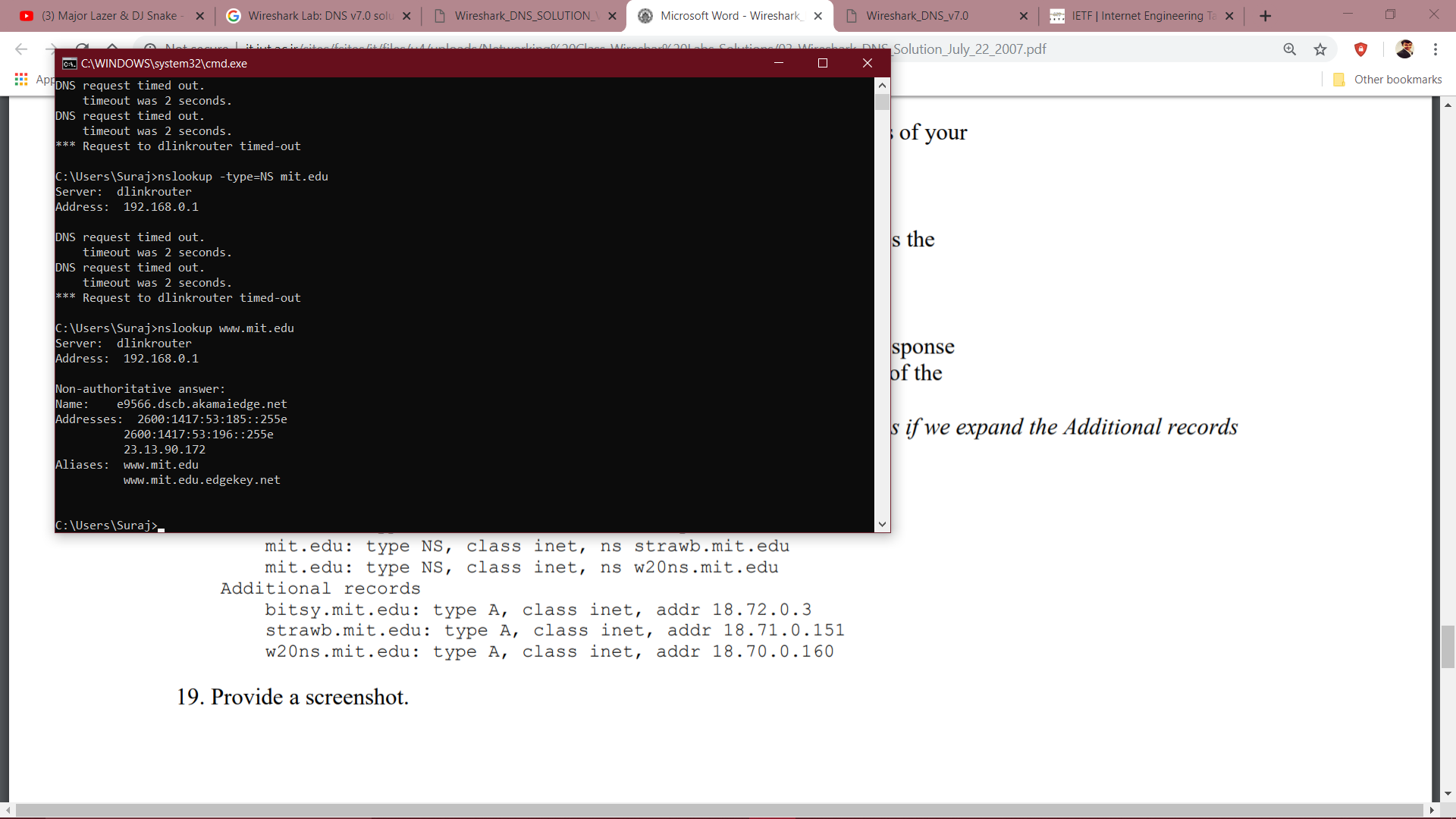
solution:



Que18. Examine the DNS response message. What MIT nameservers does the response

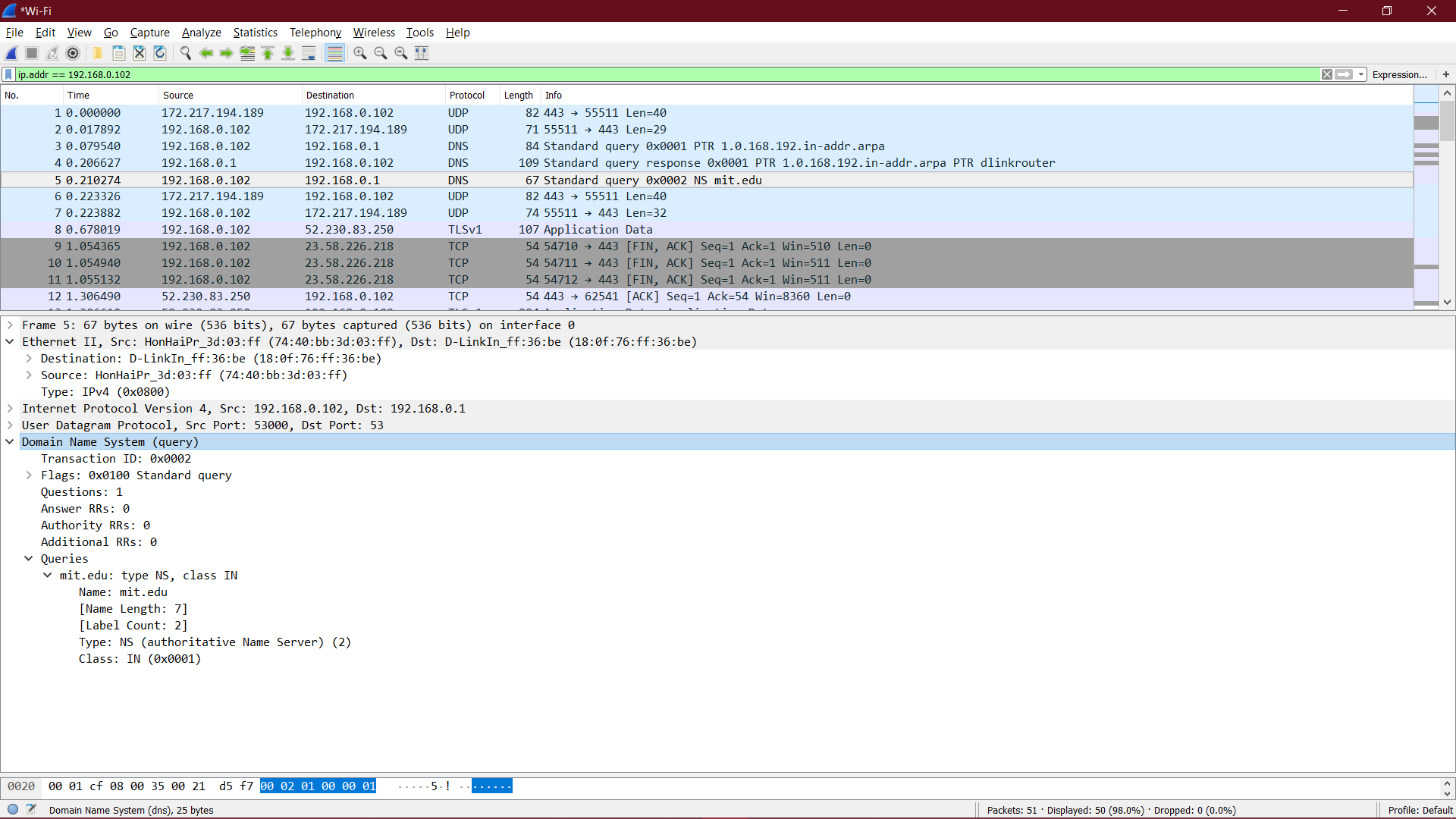
message provides? Does this response message also provide the IP addresses of the MIT name servers?

Solution:



Que19. Provide a screenshot.

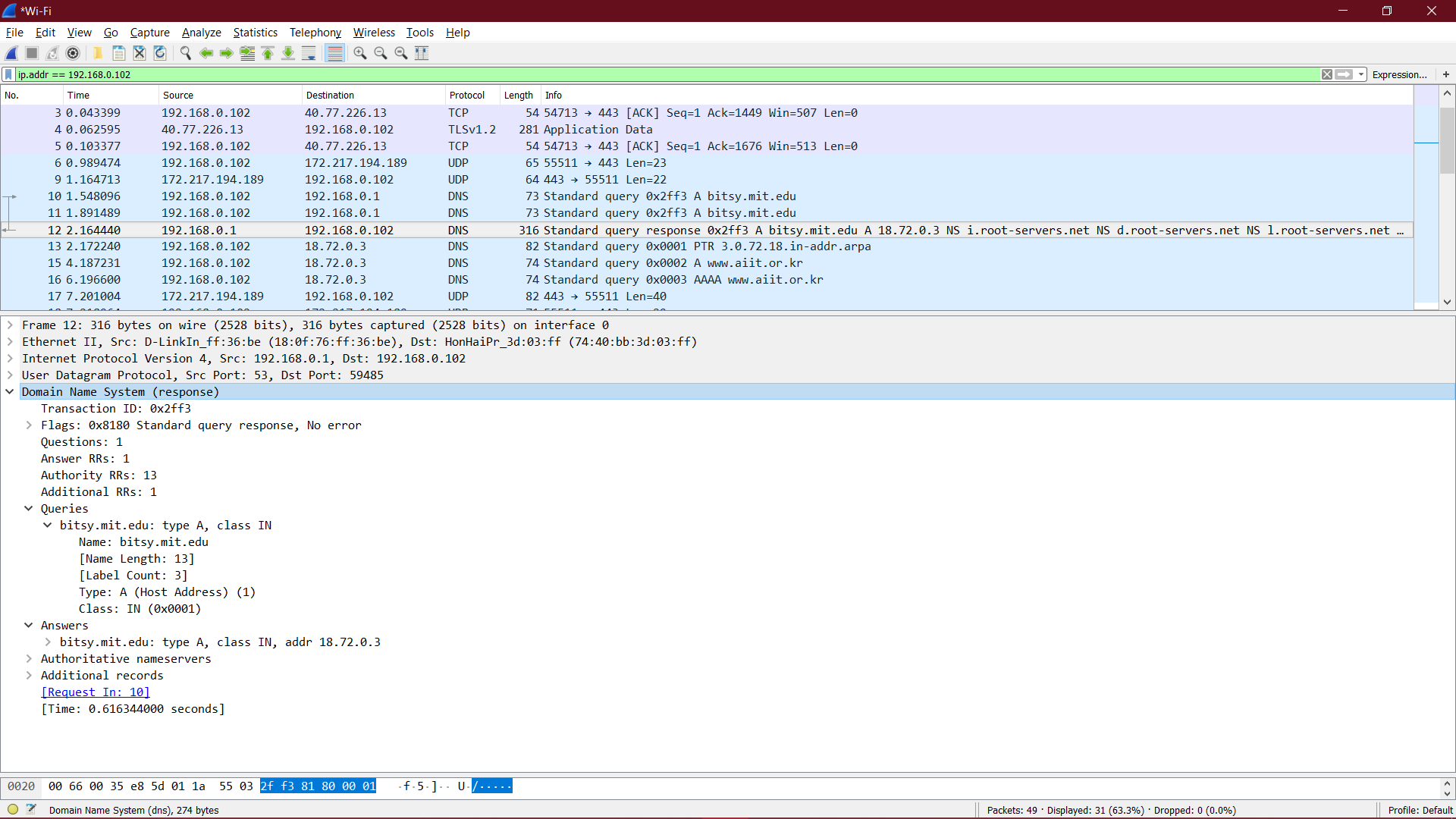
Solution:



Que20. 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?

Solution:

The query is sent to 192.168.0.1 which corresponds to bitsy.mit.edu.



Que21. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contains any “answers”?

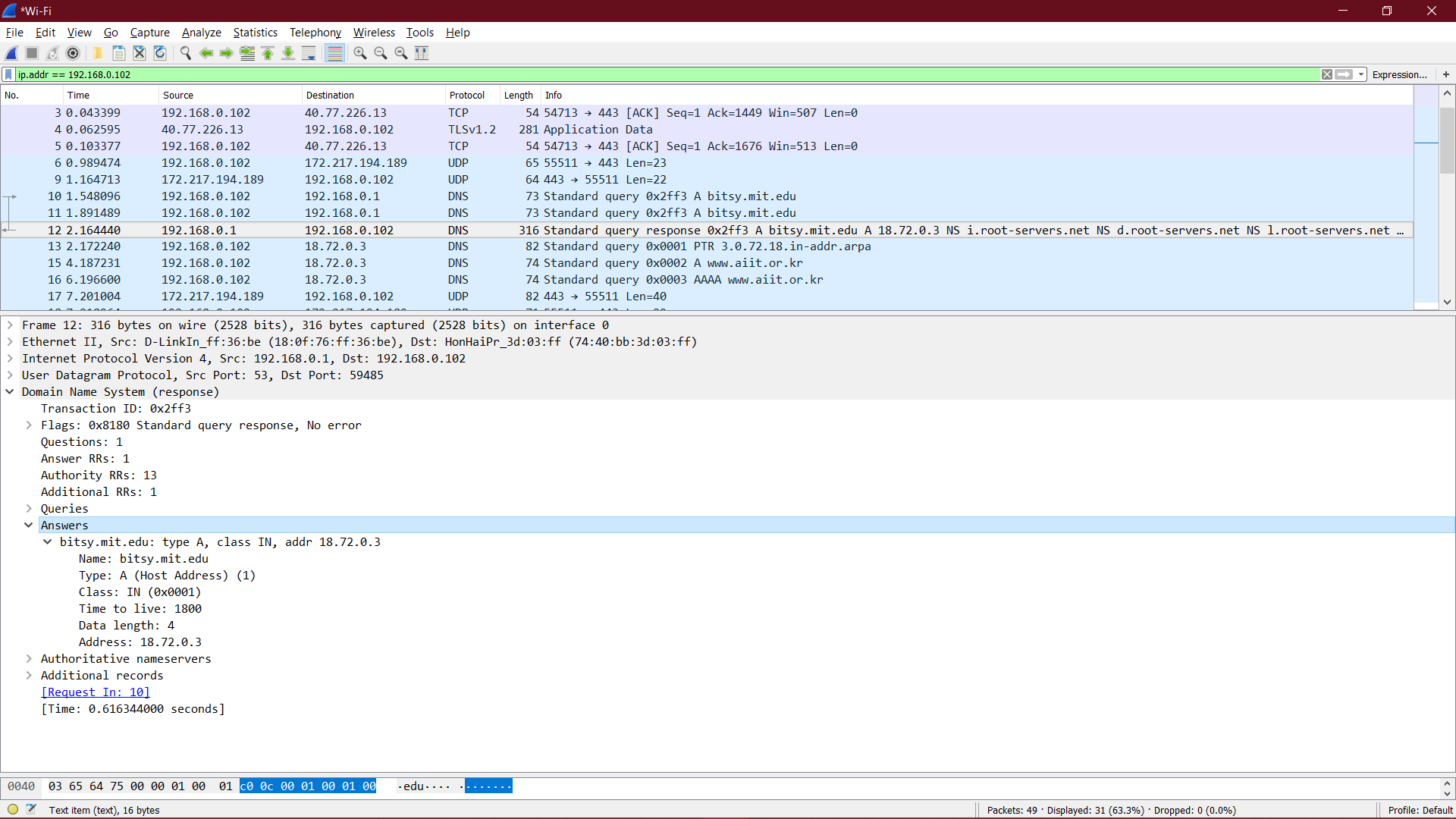
Solution:

It’s a standard type A query.

Que22. Examine the DNS response message. How many “answers” are provided? What

does each of these answers contain?

Solution:



Que23. Provide a screenshot.

Solution:

