Họ tên : Lê Bảo Khánh

MSSV : 1911363

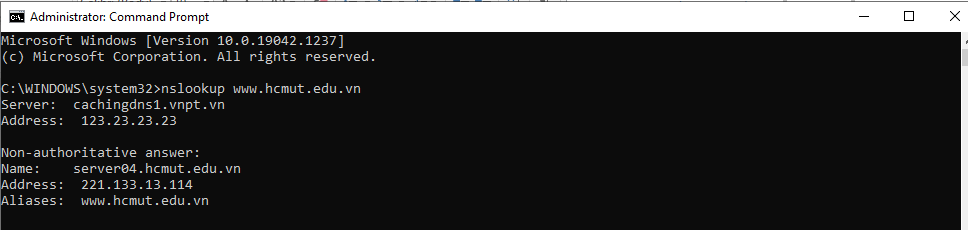
Lớp : L01

**LAB 2b**

**1. nslookup**

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

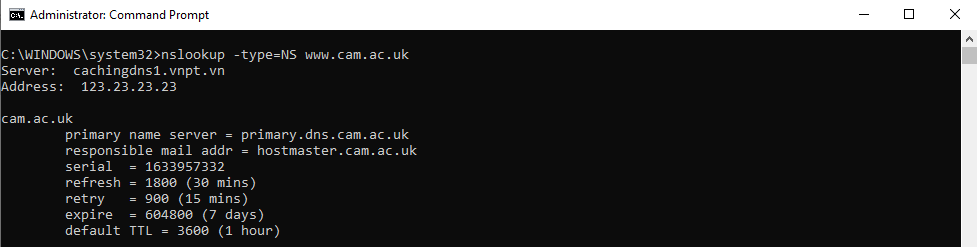
**ANSWER:**



IP address of server: 221.133.13.114

**Question 2:** Run nslookup to determine the authoritative DNS servers for a university in  
Europe.

**ANSWER:**



Authoritative DNS server: primary.dns.cam.ac.uk

**Question 3:** 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?

**ANSWER:**

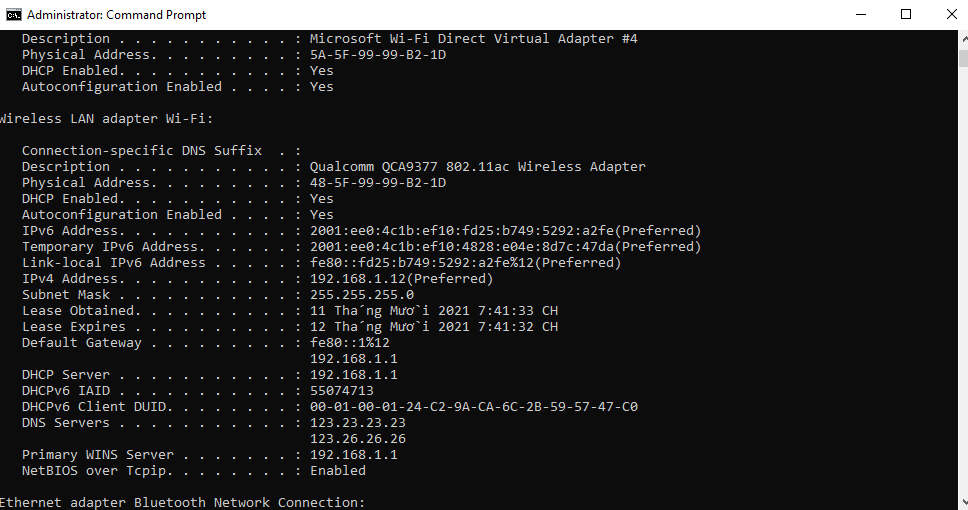


IP address for Yahoo! mail server: 106.10.236.40

**2. ipconfig**

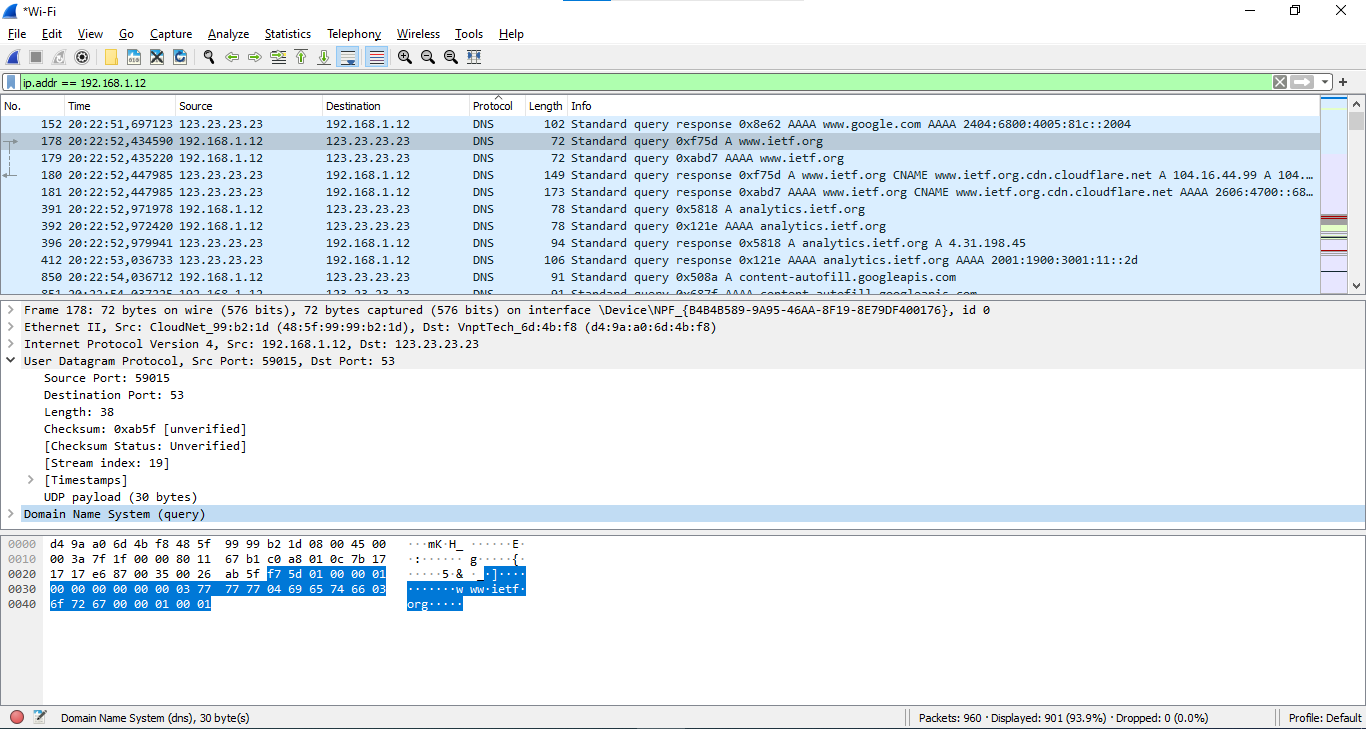
**3. Tracing DNS with Wireshark**

**My IP address: 192.168.1.12**

****

**Question 4**: Locate the DNS query and response messages. Are then sent over UDP or TCP? **ANSWER:**

The DNS query and response message are sent over UDP



**Question 5:** What is the destination port for the DNS query message? What is the source port  
of DNS response message?

**ANSWER:**

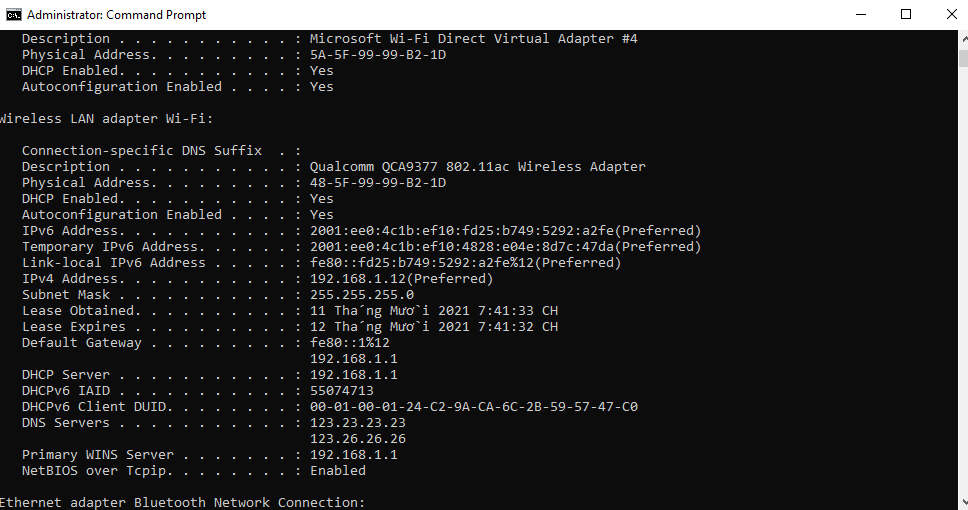
The destination port: 53

The source port: 59015

**Question 6:** 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?

**ANSWER:**

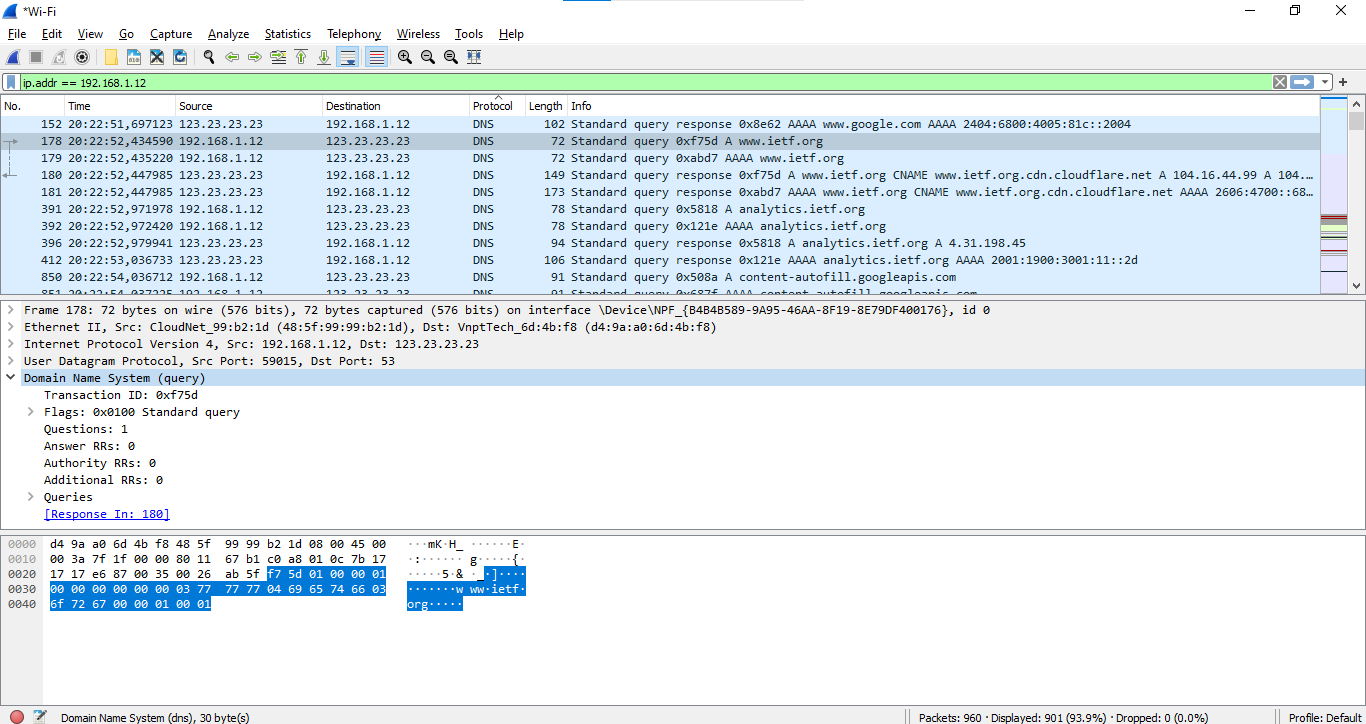
It’s sent to 192.168.1.1,which is the IP address of one of my local DNS servers

****

**Question 7**: Examine the DNS query message. What “Type” of DNS query is it? Does the  
query message contain any “answers”?

**ANSWER:**

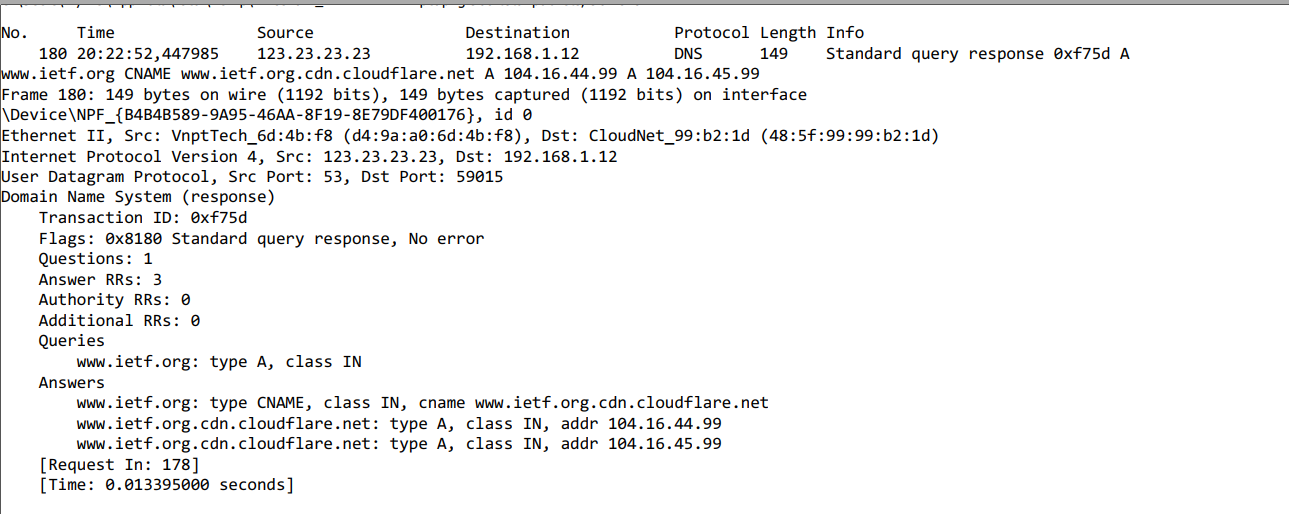
It’s a type A Standard Query and it doesn’t contain any answers.



**Question 8:** Examine the DNS response message. How many “answers” are provided? What  
do each of these answers contain?

**ANSWER:**

There were 3 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address



**Question 9:** 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?

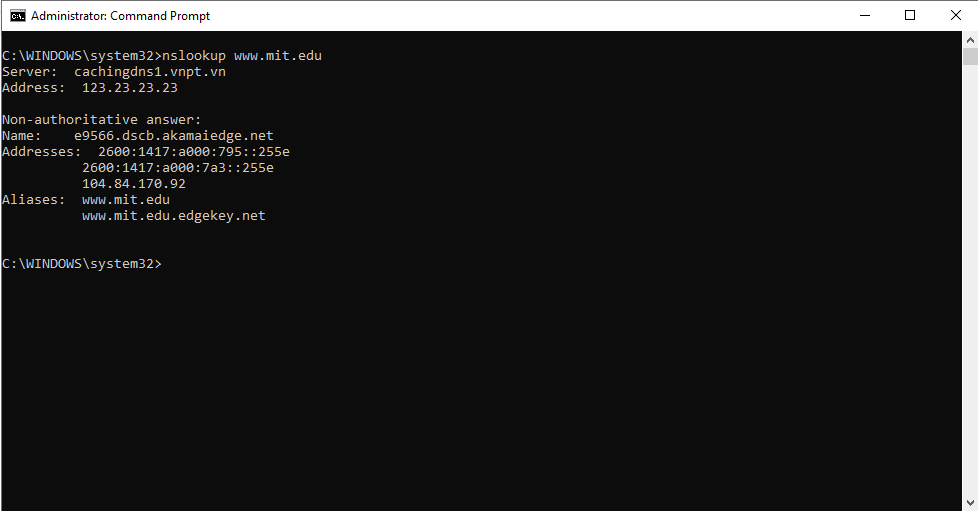
**ANSWER:**

The first SYN packet was sent to 104.16.44.99 which corresponds to the first IP address provided in the DNS response message.

**Question 10:** This web page contains images. Before retrieving each image, does your host  
issue new DNS queries?

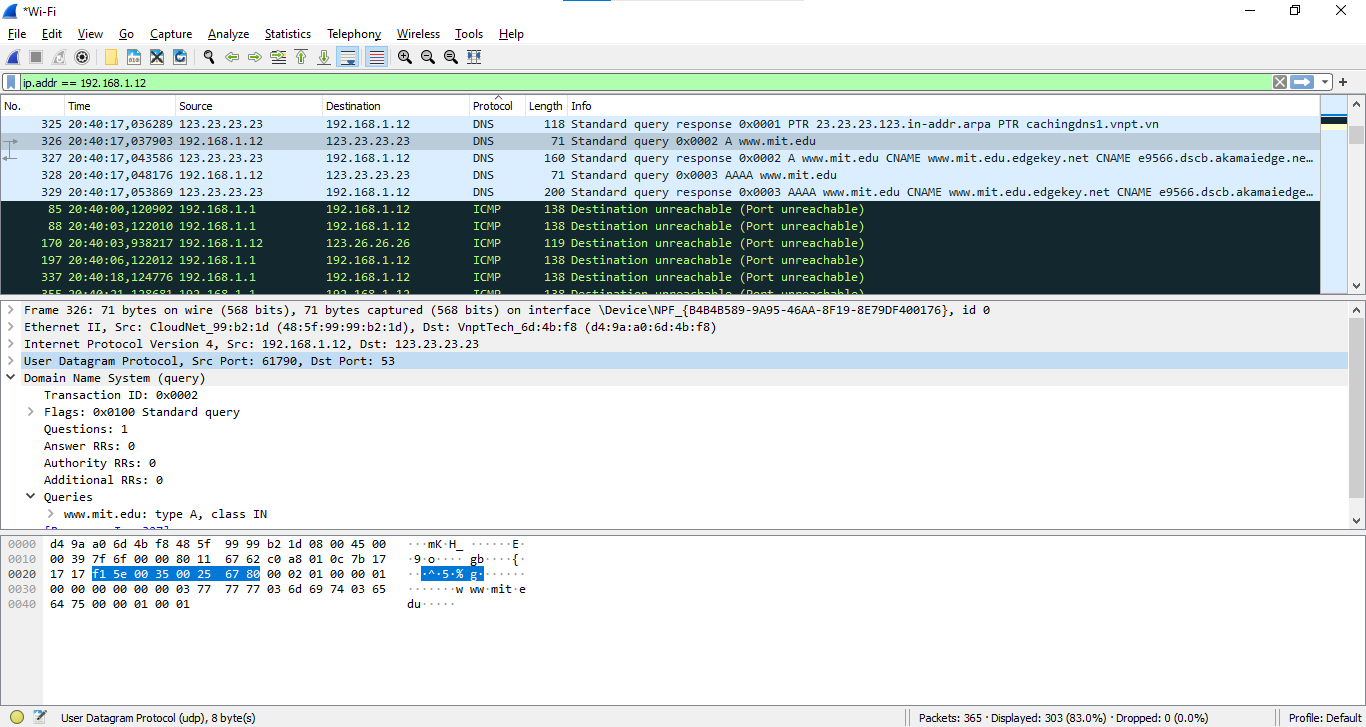
**ANSWER:**

No

****

**Question 11**: What is the destination port for the DNS query message? What is the source port  
of DNS response message?

**ANSWER:**



Destination Port: 53

Source Port: 61790

**Question 12:** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**ANSWER:**

It’s sent to 123.23.23.23,which is the IP address of one of my local DNS servers

**Question 13:** Examine the DNS query message. What “Type” of DNS query is it? Does the  
query message contain any “answers”?

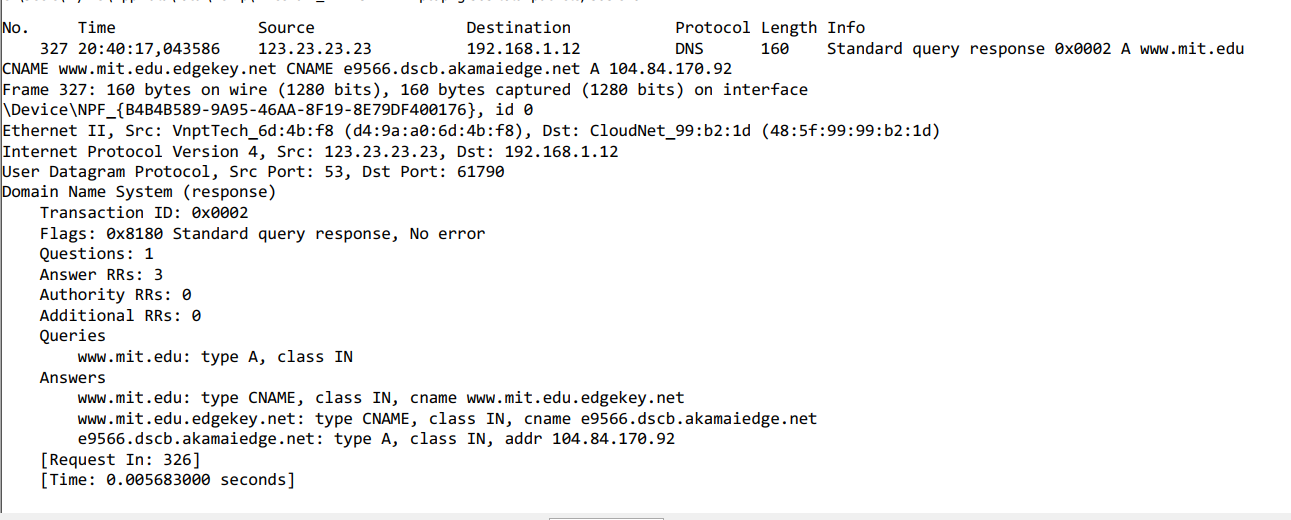
**ANSWER:**

The query is of type A and it doesn’t contain any answers.

**Question 14:** Examine the DNS response message. How many “answers” are provided? What  
do each of these answers contain?

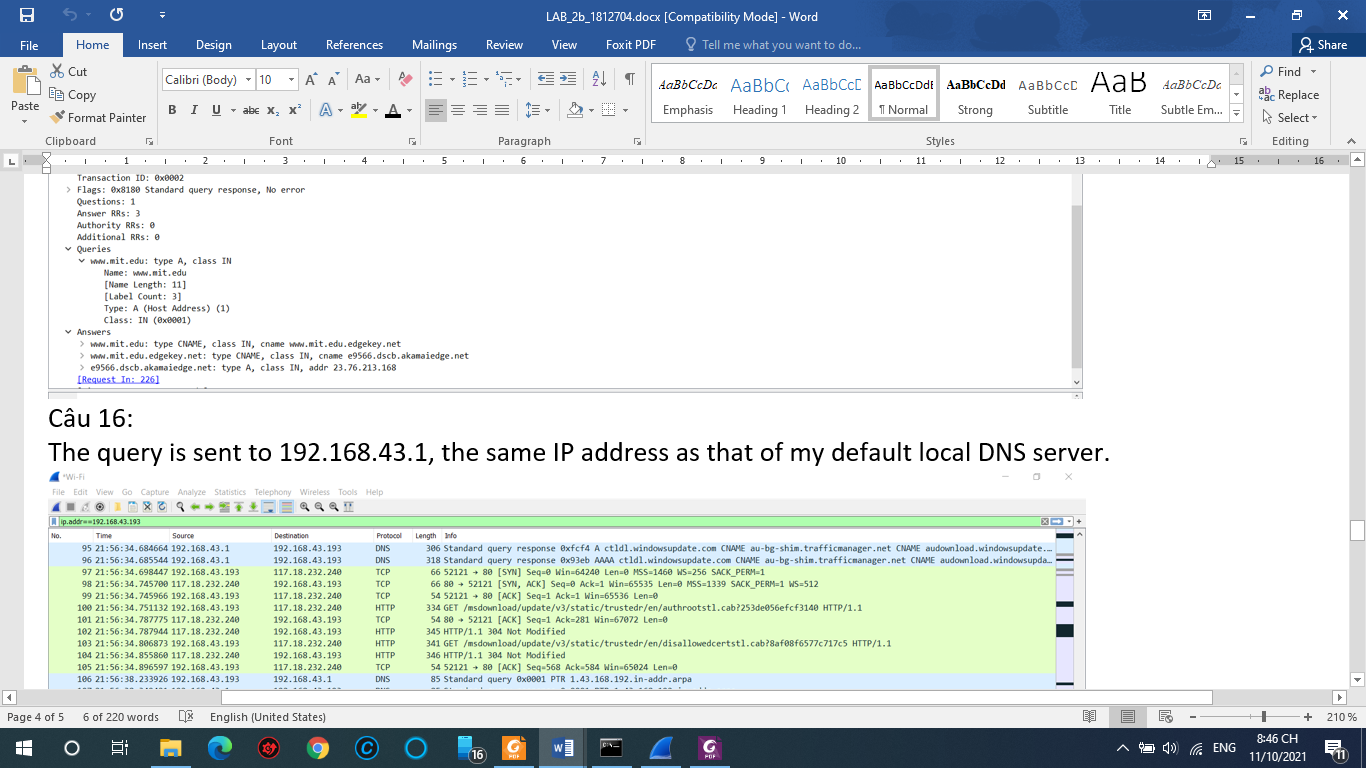
**ANSWER:**

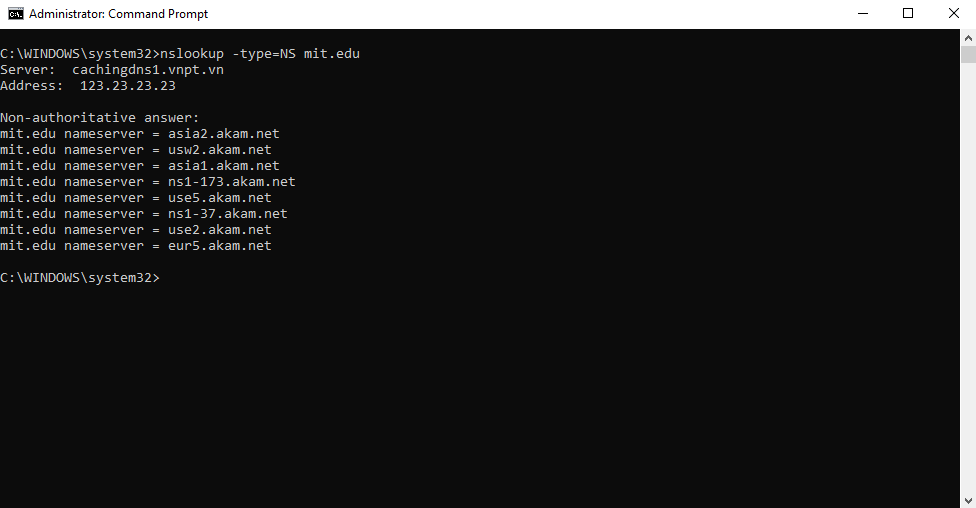
The response DNS message contains 3 answer containing the name of the host, the type of address, the class, and the IP address.

****

**Question 15:** Provide a screenshot.

**ANSWER:**



****

**Question 16:** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

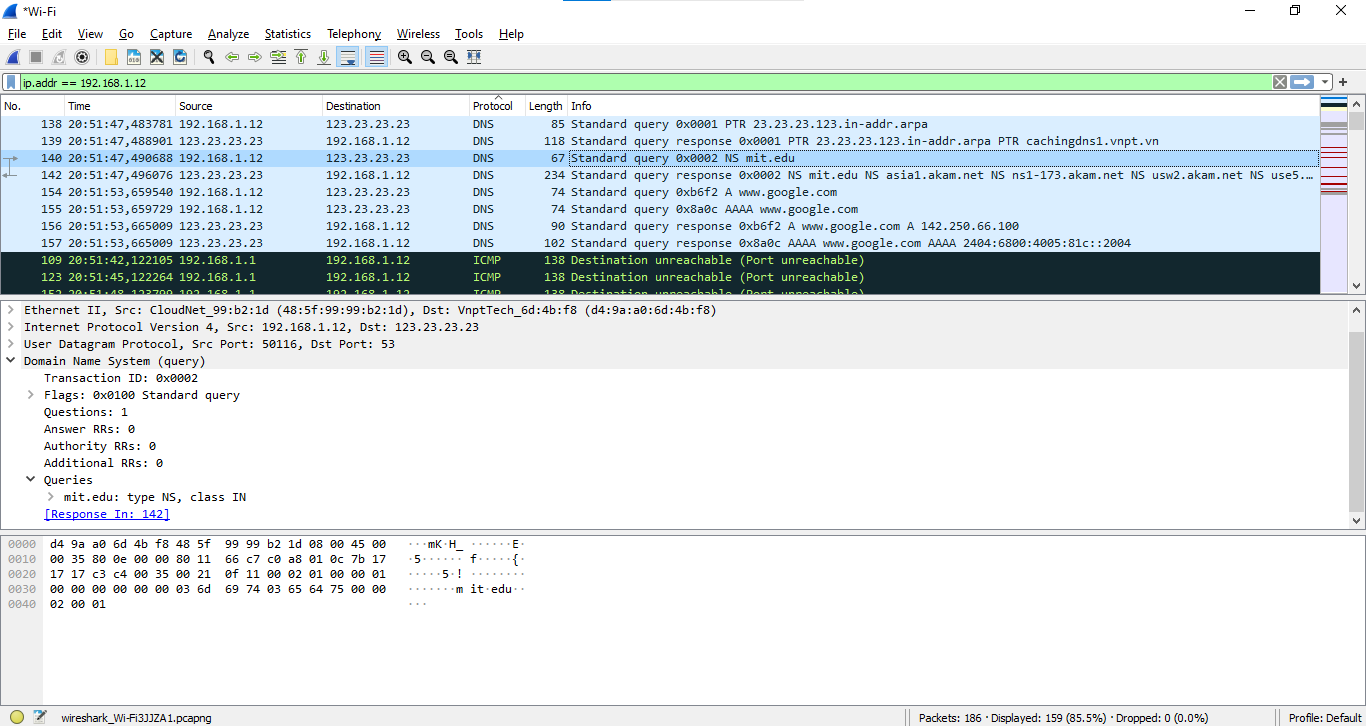
**ANSWER:**

It was sent to 123.23.23.23 which is my default DNS server.

**Question 17:** Examine the DNS query message. What “Type” of DNS query is it? Does the  
query message contain any “answers”?

**ANSWER:**

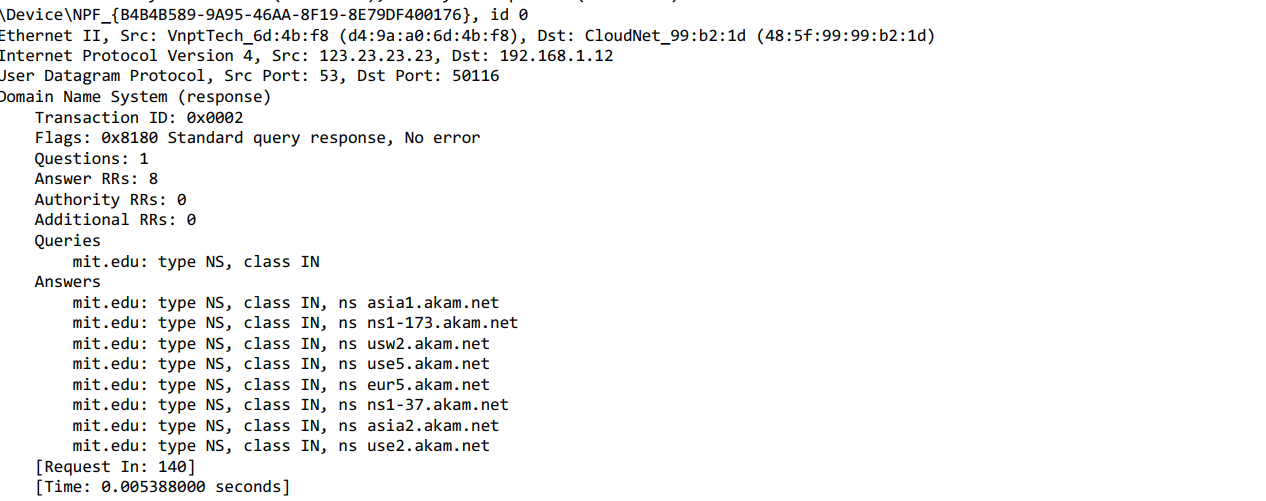
The DNS query is a type “NS” message including one question. The query message did not contain any answers.

****

**Question 18:** 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?

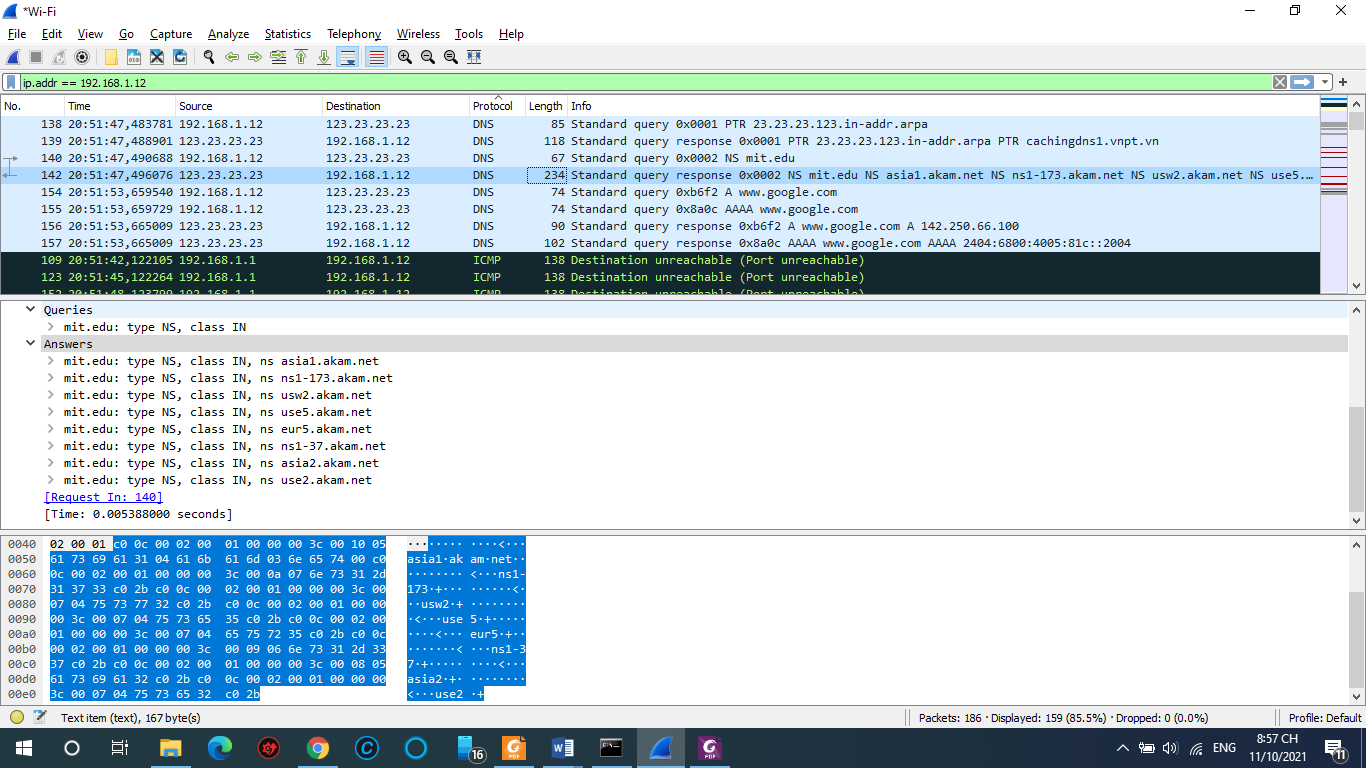
**ANSWER:**

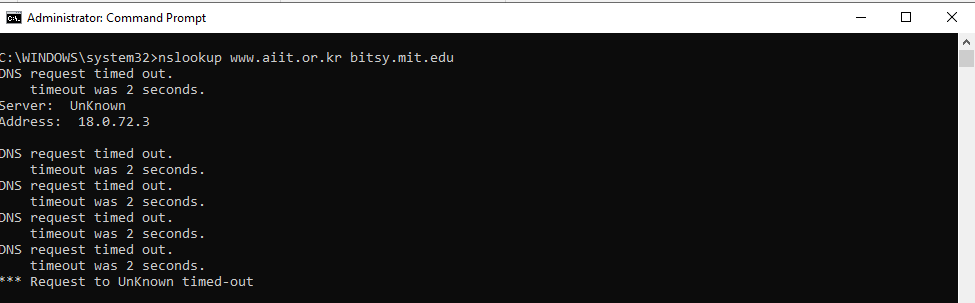
The nameservers are asia1, ns1-173, usw2, use5, eur5, ns1-37, asia2m use2. We can find their IP addresses as seen below.

****

**Question 19:** Provide a screenshot.

**ANSWER:**





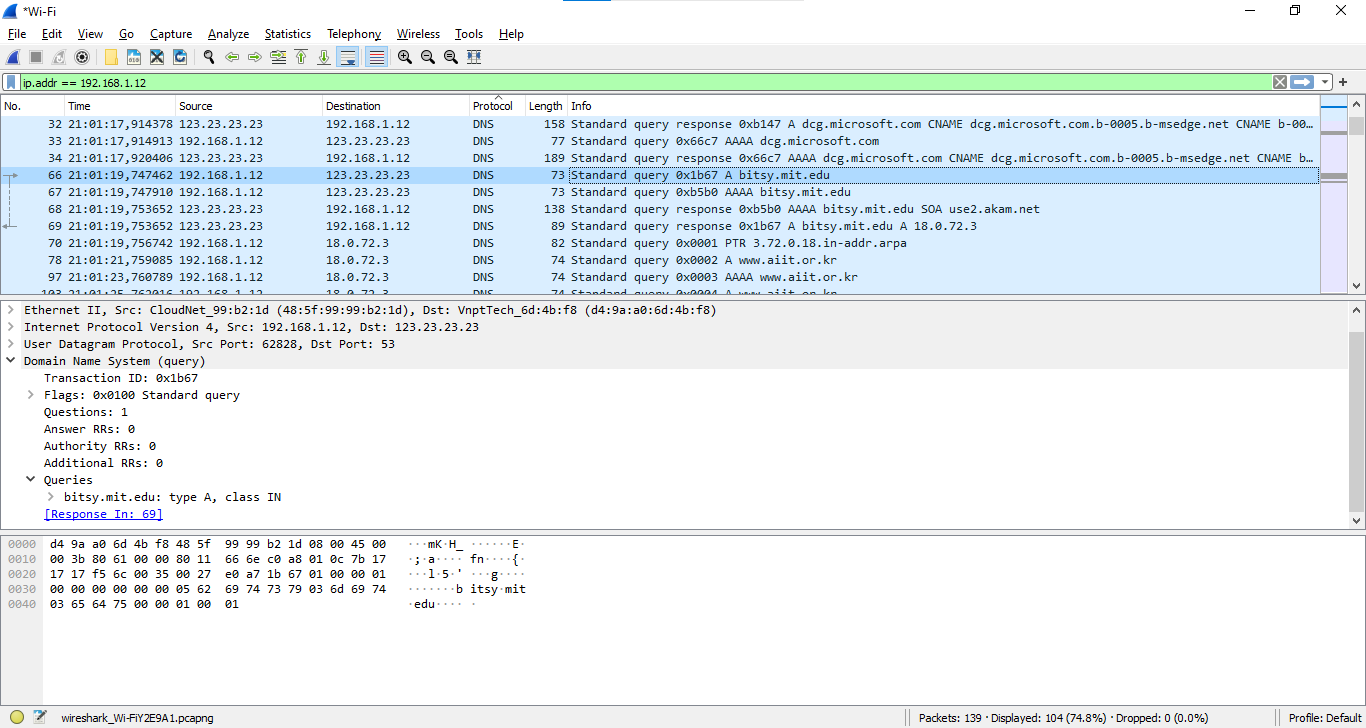
**Question 20:** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

**ANSWER:**

The query is sent to 18.72.0.3 which corresponds tobitsy.mit.edu.

**Question 21:** Examine the DNS query message. What “Type” of DNS query is it? Does the  
query message contain any “answers”?

**ANSWER:**

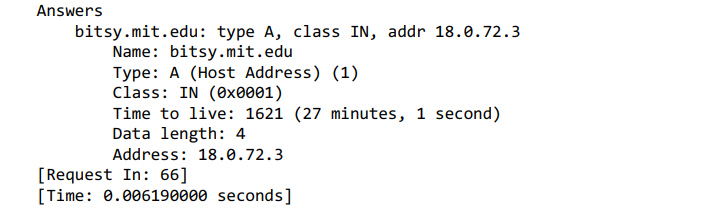
****

It’s a standard type A query that doesn’t contain any answers

**Question 22:** Examine the DNS response message. How many “answers” are provided? What  
does each of these answers contain?

**ANSWER:**

One answer is provided in the DNS response message

****

**Question 23:** Provide a screenshot

**ANSWER:**

