**Computer Networks**

**Lab 2b**

**Wireshark Lab:**

**DNS v8.0**

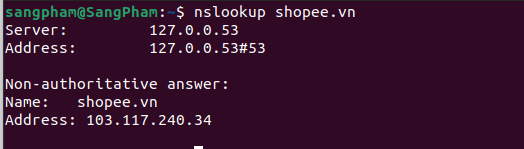
**Student Name: Phạm Ngọc Sang**

**Student No: 1813810**

1. **nslookup**

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

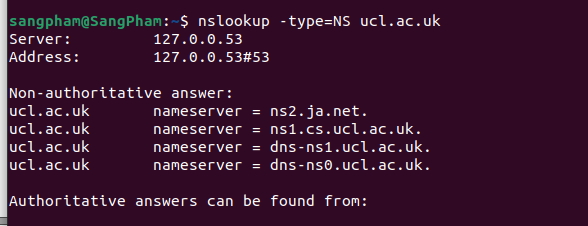
Answer:



The IP address is: 103.117.240.34

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

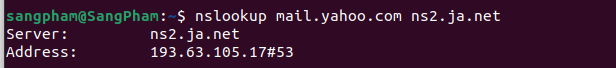
Answer:



The authoritative DNS server for LONDON'S GLOBAL UNIVERSITY is: ns2.ja.net

**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:

****

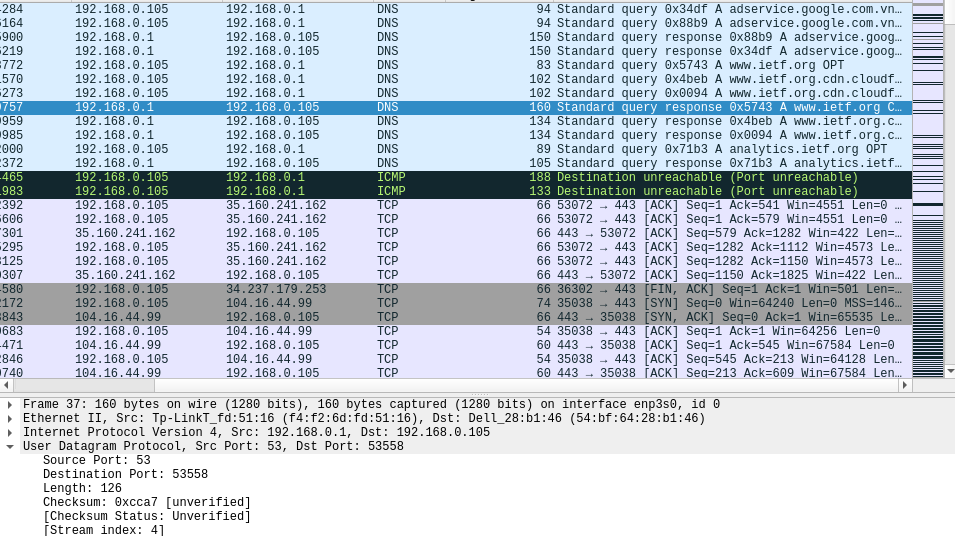
The IP address is: 193.63.105.17

1. **ipconfig**
2. **Tracing DNS with Wireshark**

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

Answer:

The query and response messages are sent via UDP.

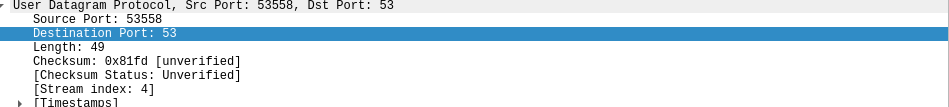


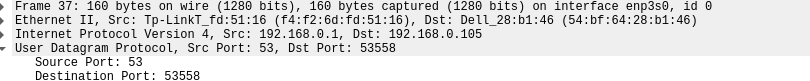
**5. What is the destination port for the DNS query message? What is the source port of the DNS response message?**

Answer:

Destination Port: 53

Source Port: 53





**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:

IP addresses: 192.168.0.1

2 IP are the same

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

Answer:

Type: A Standard Query

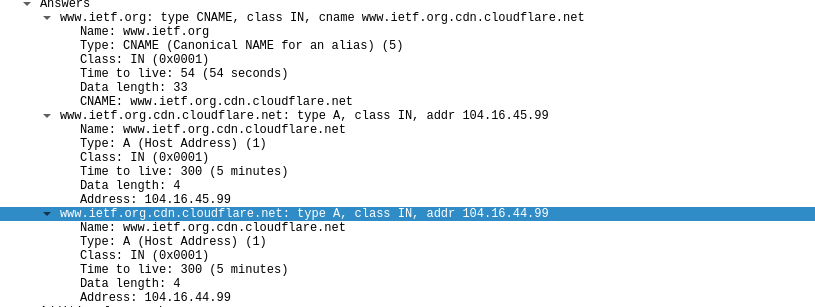
Doesn’t contain any “answers”.

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

Answer:

There are 3 answers.

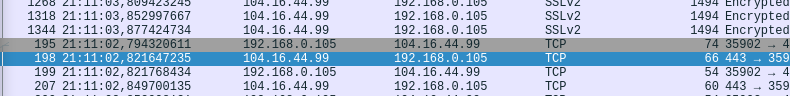
Contain: Name, Type, Class, Time to live, Data length, IP Address



**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 destination IP address of the SYN packet corresponds to the address provided by the DNS response: 104.16.44.99



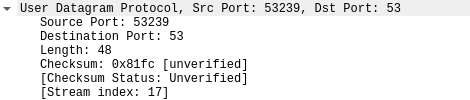
**10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

Answer: No

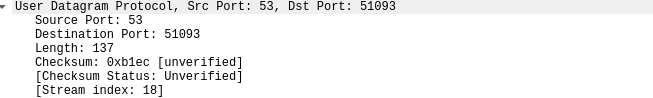
**11. What is the destination port for the DNS query message? What is the source port of the DNS response message?**

Answer:

The destination port for the DNS query message: 53

****

The source port of the DNS response message: 53



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

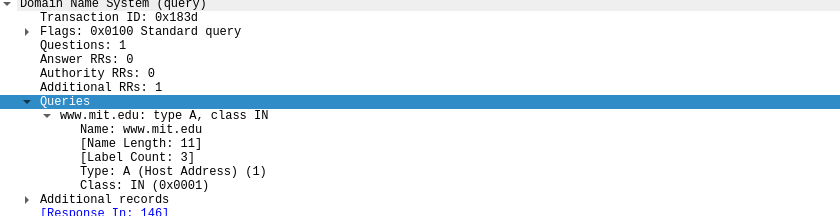
Answer:

IP Address: 192.168.0.1

This is the IP address of my default local DNS server.

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

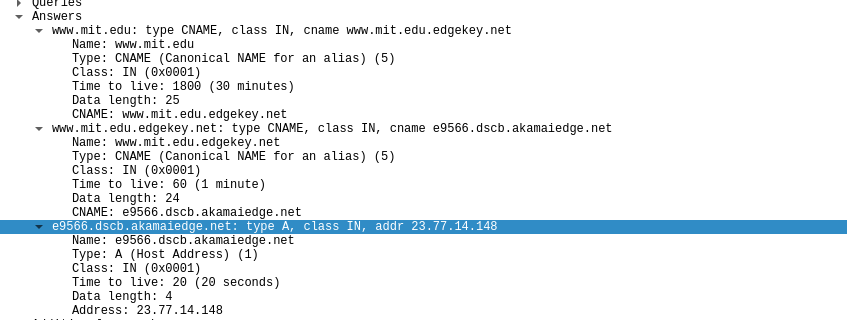
Answer: Type A and doesn't contain answers

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

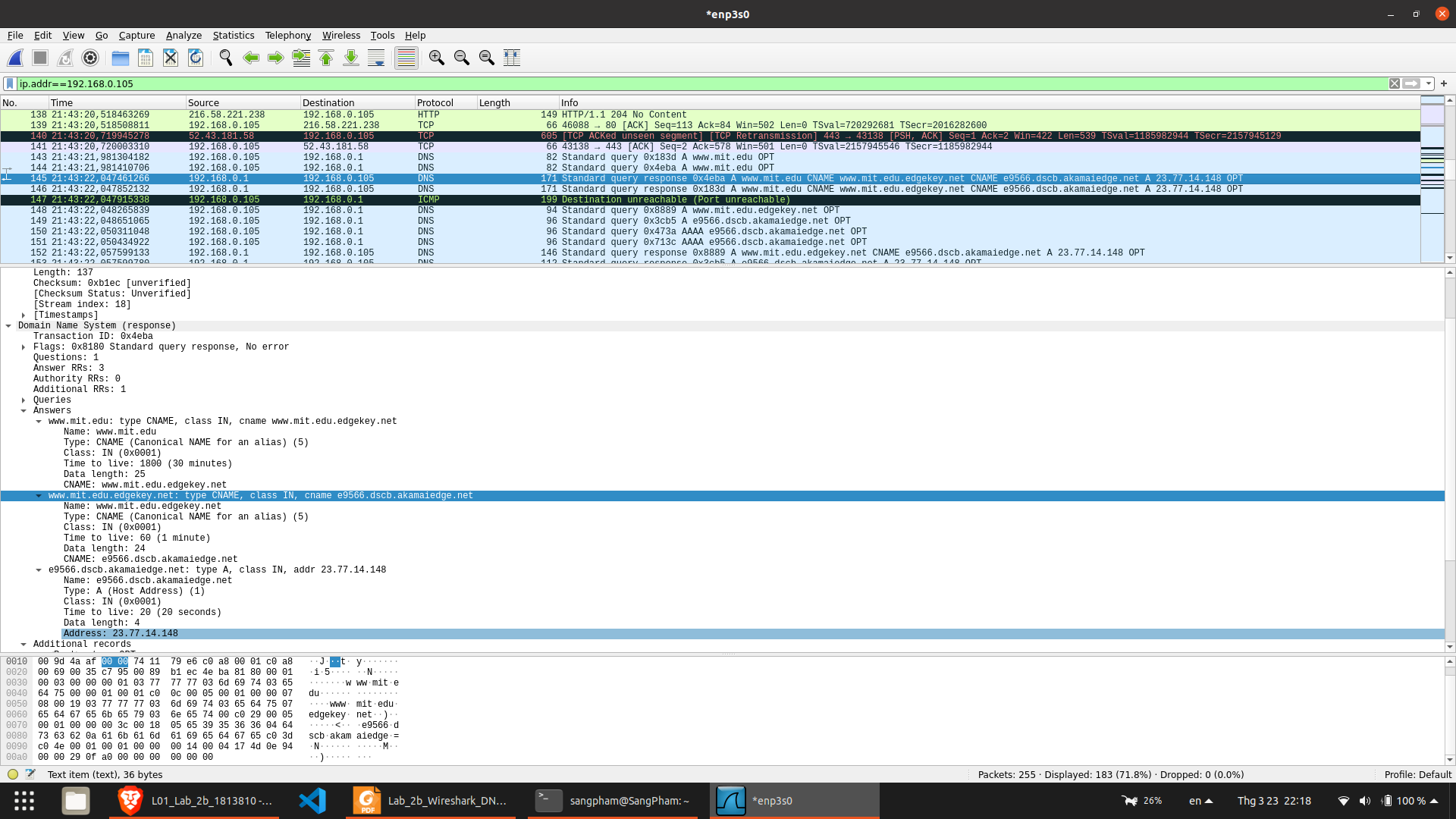
Answer:

There are 3 answers.

Contain: Name, Type, Time to live, Data length, CNAME and IP address



**15. Provide a screenshot.**

****

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

Answer:

IP address: 192.168.0.1

This is the IP address of my default local DNS server.

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

Answer:

Type NS

Doesn’t contain

**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:

Nameservers:

usw2.akam.net

use2.akam.net

eur5.akam.net

use5.akam.net

ns1-173.akam.net

asia2.akam.net

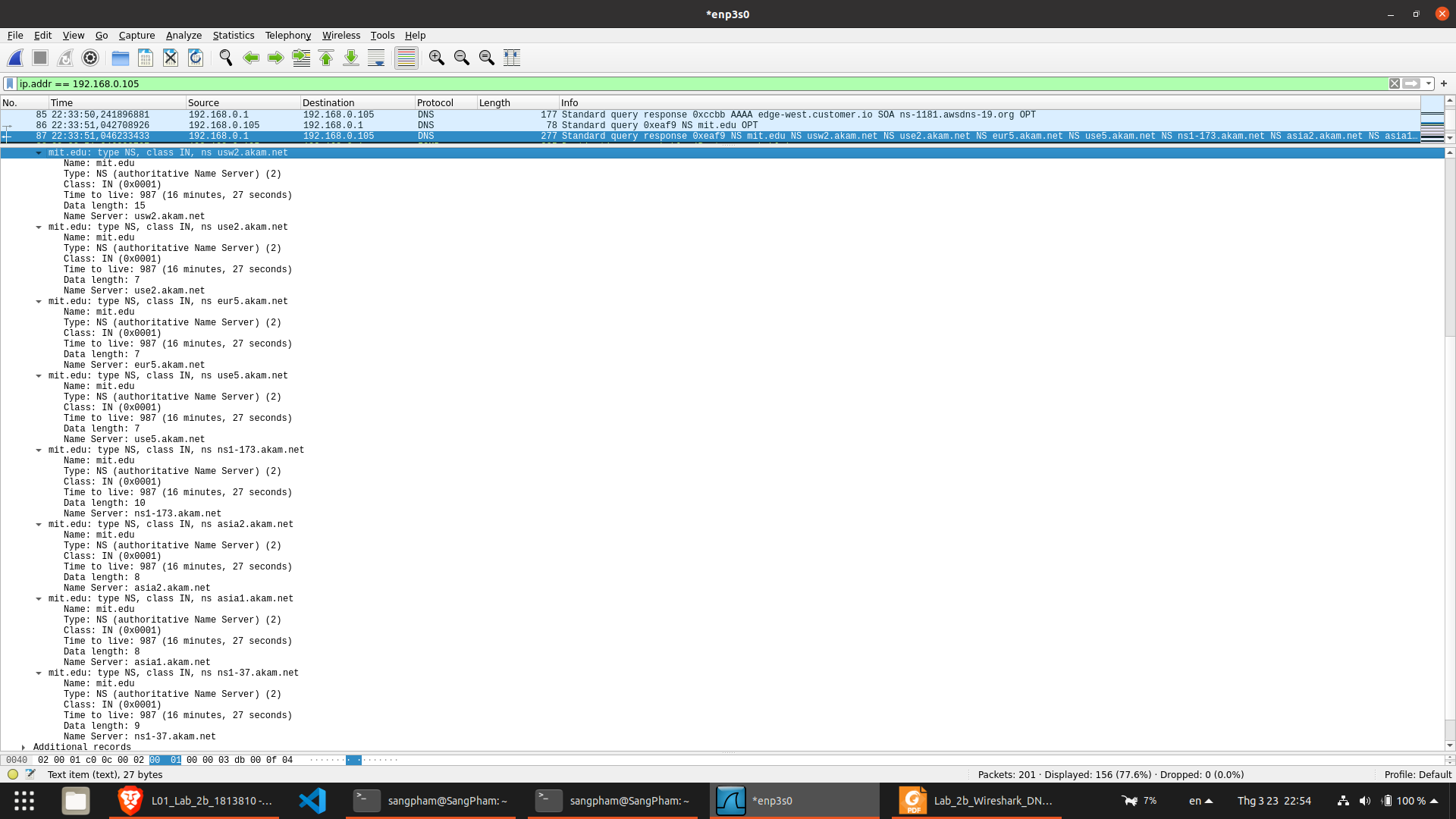
asia1.akam.net

This response message also provides the IP address of the MIT nameservers.

But not all the MIT nameservers (in Additional records)



**19. Provide a screenshot.**

****

**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:

IP address: 18.0.72.3

It isn’t the IP address of my default local DNS server.

This IP address corresponds to www.aiit.or.kr.

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

Answer: Type A and doesn’t contain

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

Answer: no response messages and no answer.

**23. Provide a screenshot.**

