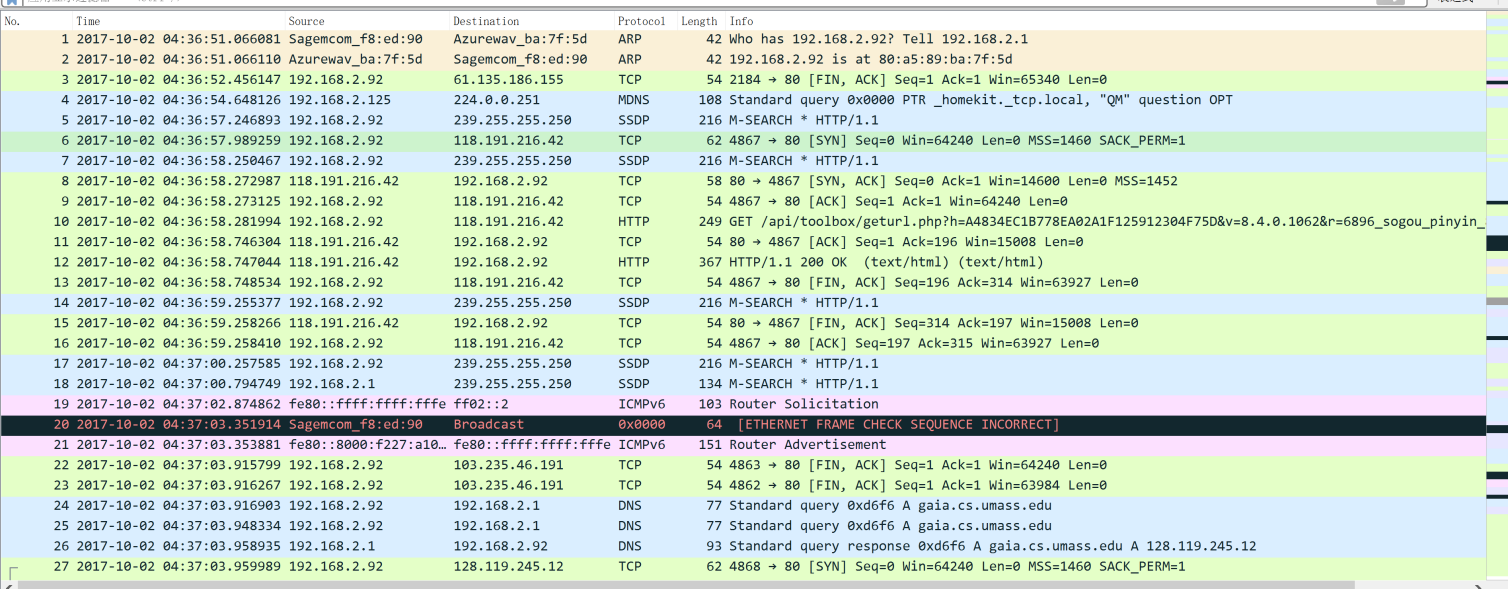
The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you’ve been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

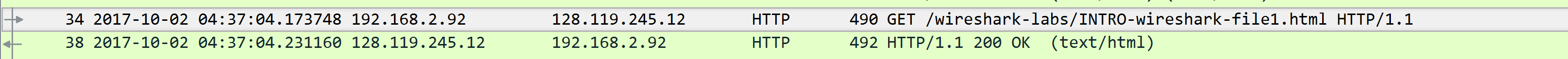
1. **List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**

The result in wiresharp is as follow:



Answer: The protocols listed in the picture include **ARP, TCP MDNS, SSDP and ICMP**

2**. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)**



Answer: According to the picture, the time from the HTTP GET message was sent to the OK reply was received is about 0.07s.

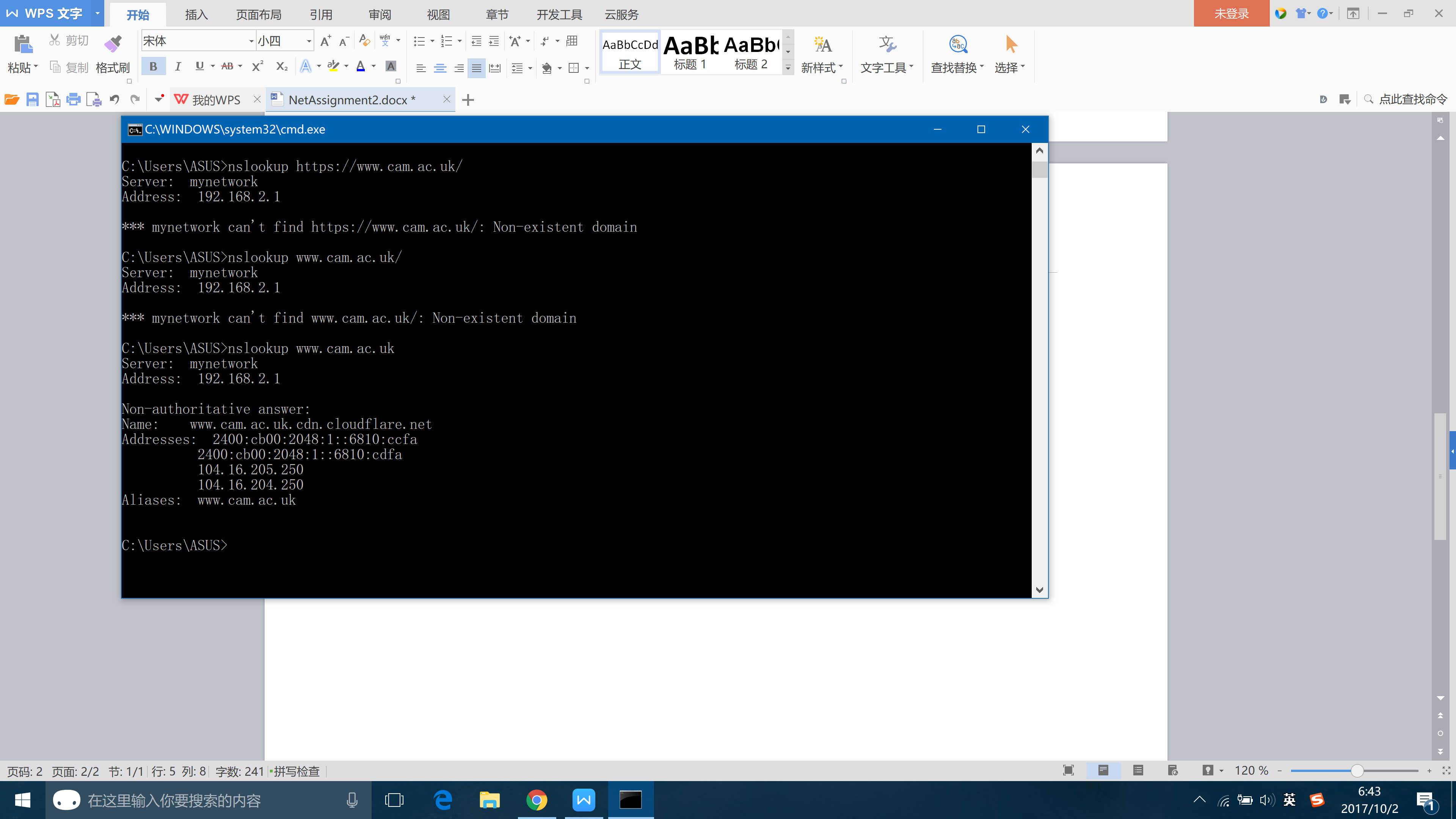
1. **What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?**

Answer: As the picture above, the Internet address for gaia.cs.umass.edu is 128.119.245.12 and the Internet address for my computer 192.168.2.92.

**Nslookup:**

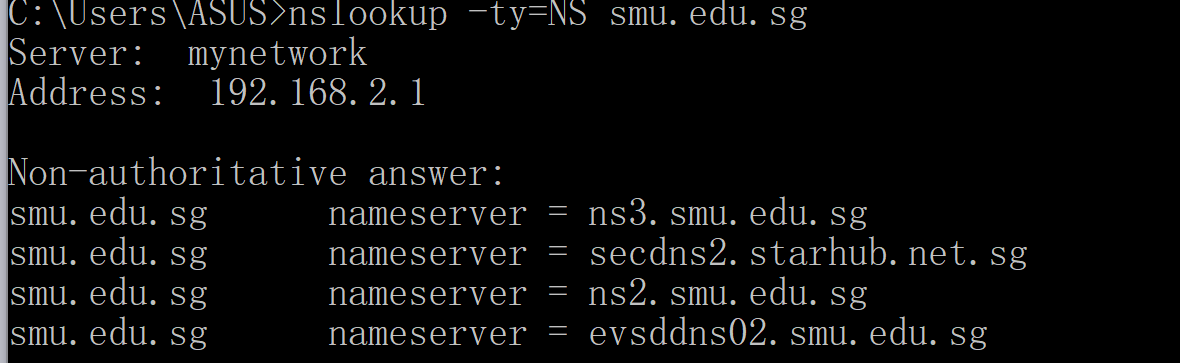
1. **Run nslookup to obtain the IP address of a Web server in UK. What is the IP address of that server? (3 Marks)**

**Answer:The screenshot of the CMD is as follow:**



The ip address for the website of the Cambridge University is **104.16.205.250**

1. **Run nslookup to determine the authoritative DNS servers for a university in Singapore. (3 Marks)**



Answer: The authoritative DNS server of National University of Singapore is ns3.smu.edu.sg

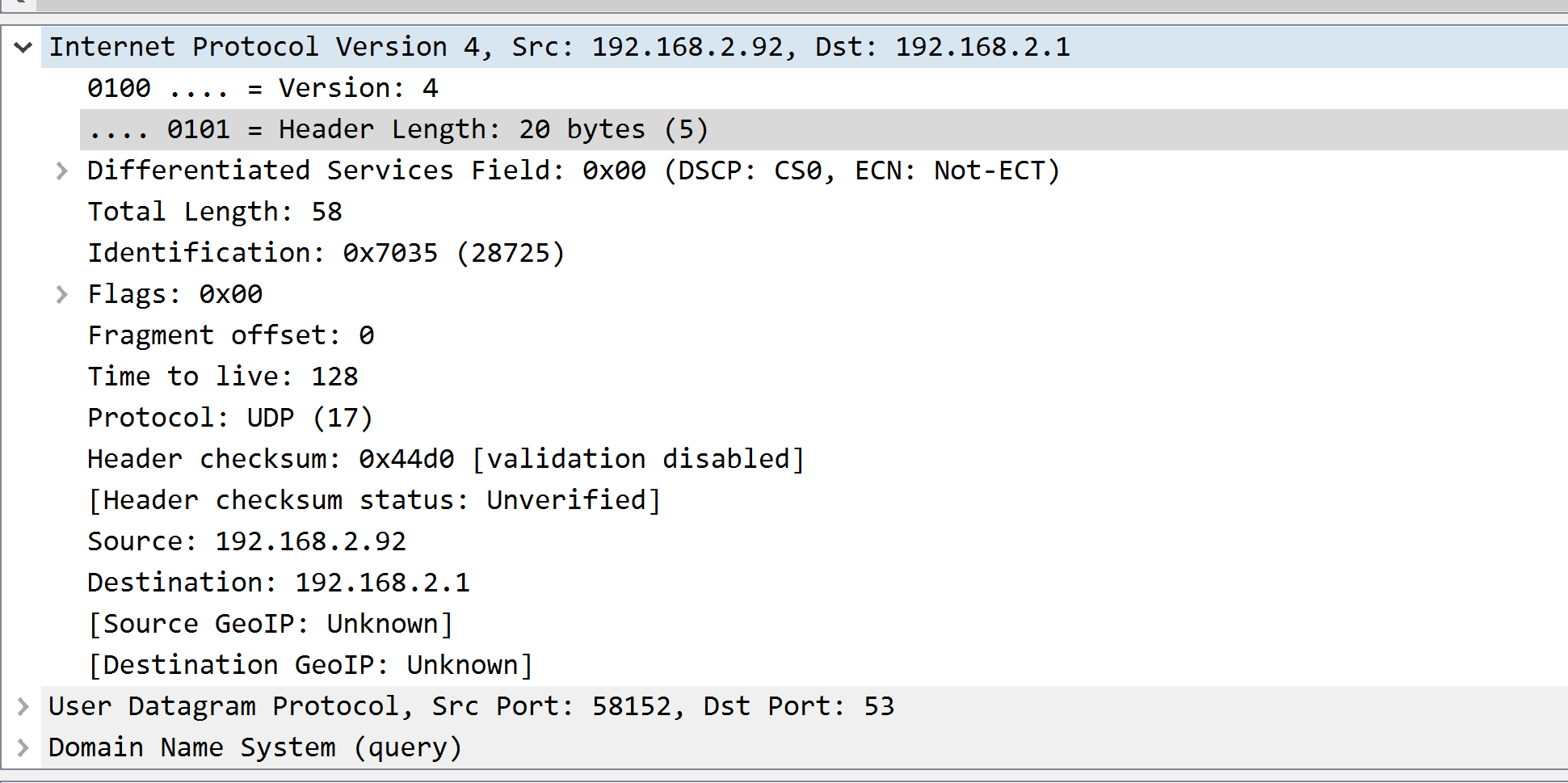
1. **Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for ProntoMail. What is its IP address? (3 Marks)**

**Answer:**



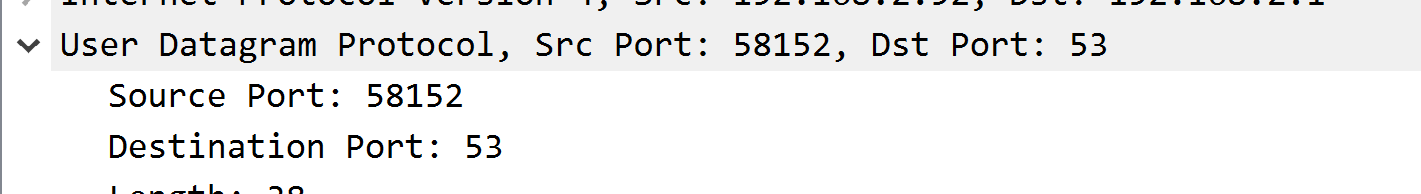
**The ip address of prontomail is 69.20.39.2**

**4. Locate the DNS query and response messages. Are then sent over UDP or TCP? *(3 Marks)***



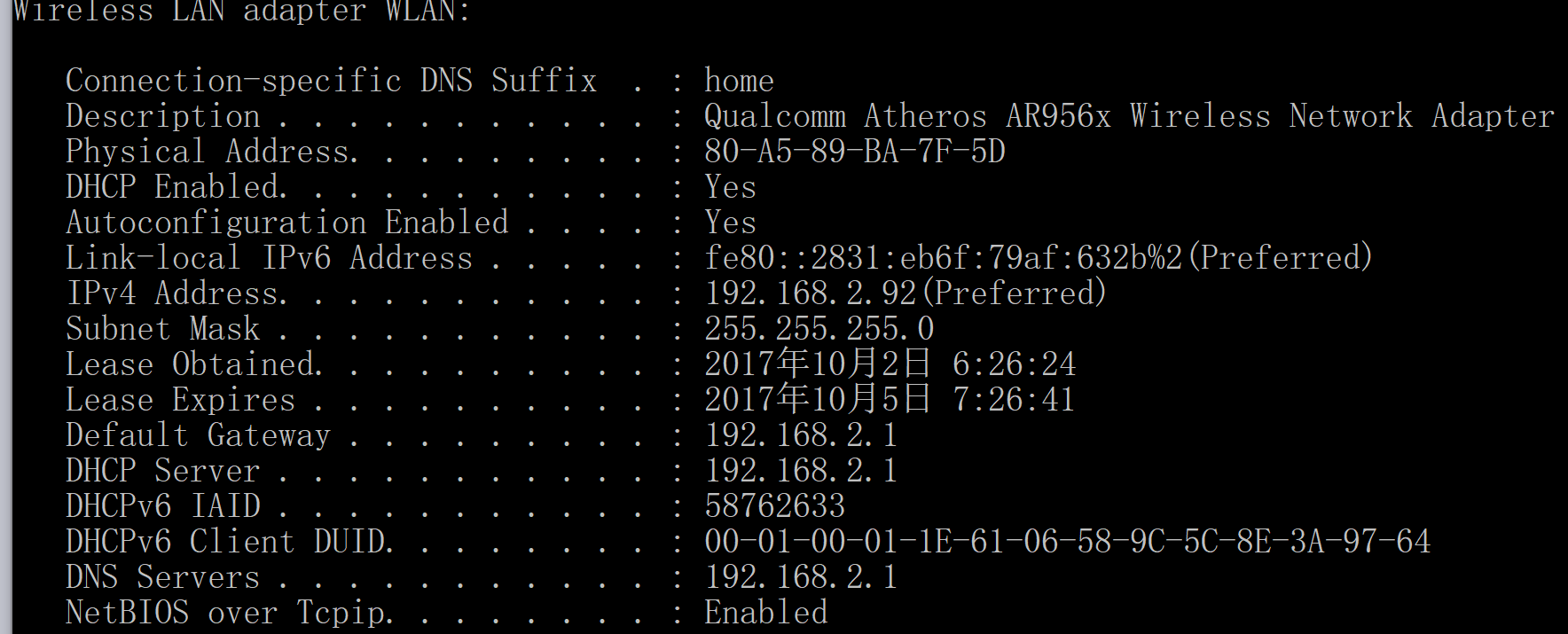
Answer: As the wiresharp shows, the DNS is sent over UPD protocol.

1. **What is the destination port for the DNS query message (3 Marks)? What is the source port of DNS response message? (3 Marks)**



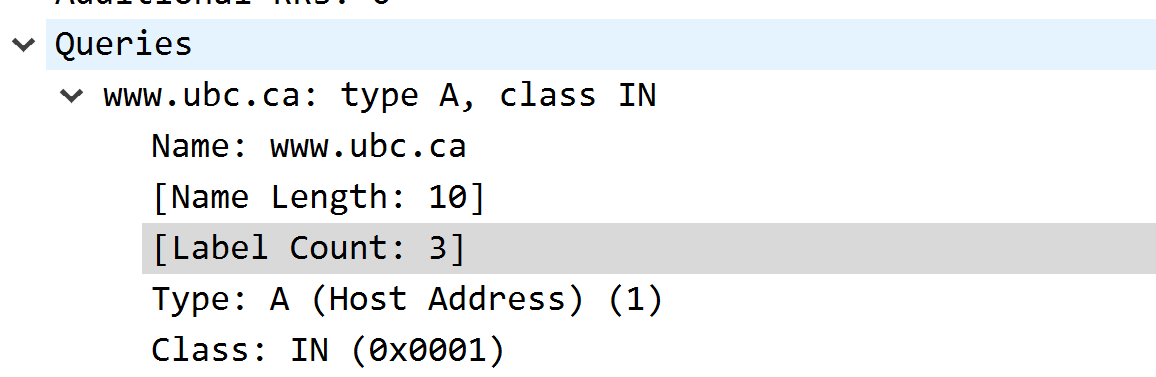
**Answer: The destination port is 53, and the source port is 58152.**

**6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server *(3 Marks)*? Are these two IP addresses the same? *(3 Marks)***



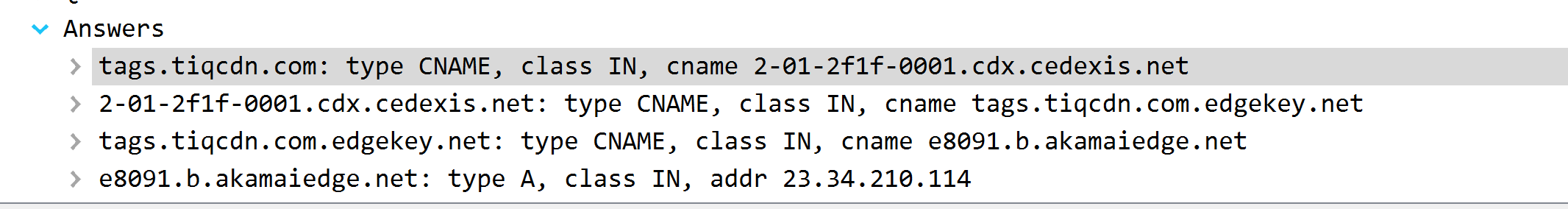
**Answer: The ip address The DNS query sent is 192.168.2.1. My DNS Server is 192.168.2.1. They are the same.**

1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? *(4 Marks)***



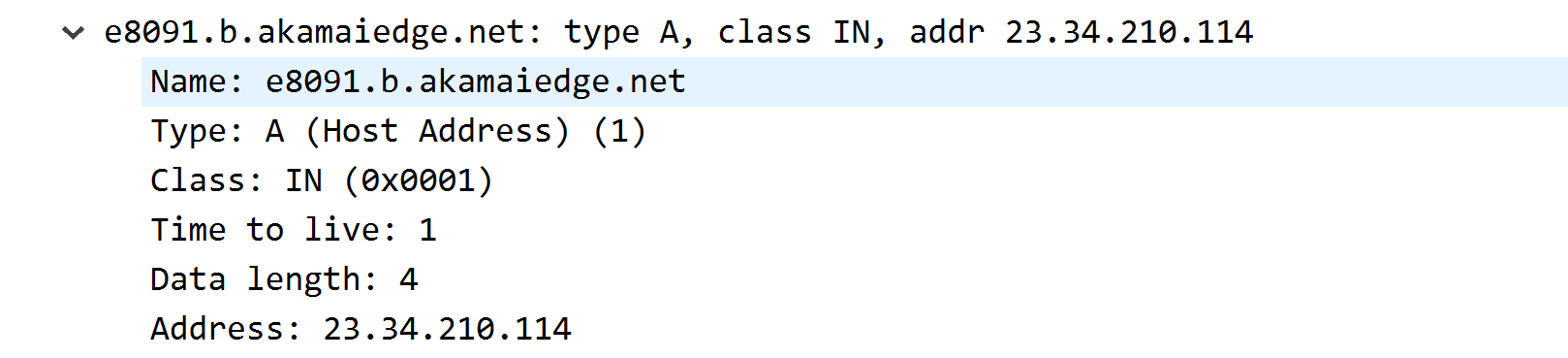
Answer: The DNS query shows the DNS query is a type ‘A’ query.No answer is provided.

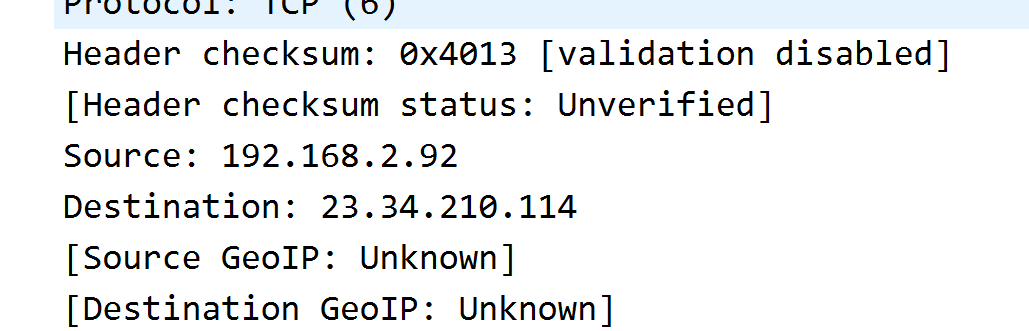
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? *(4 Marks)*



**Answer: There are 4 answers are provided. The answers contain *name, type,class time to live, data length*** *and the* ***cname****.*

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? *(3 Marks)*

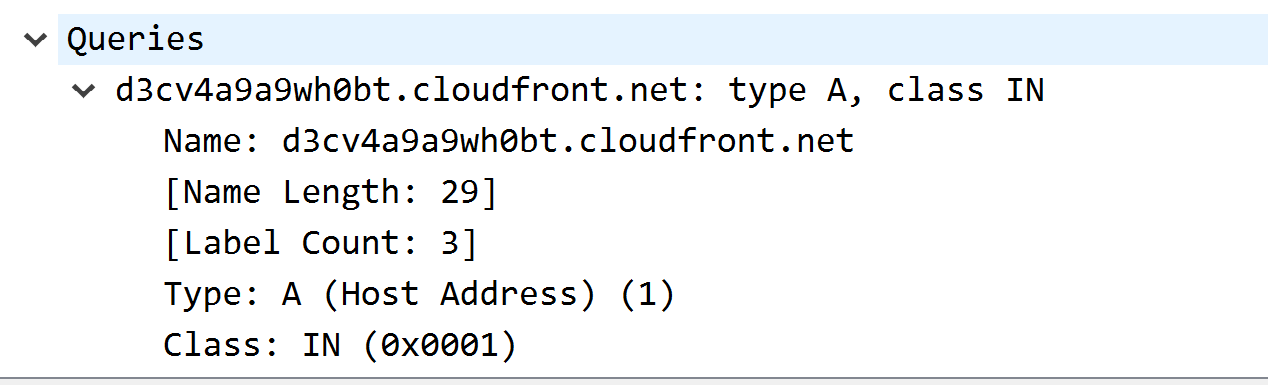




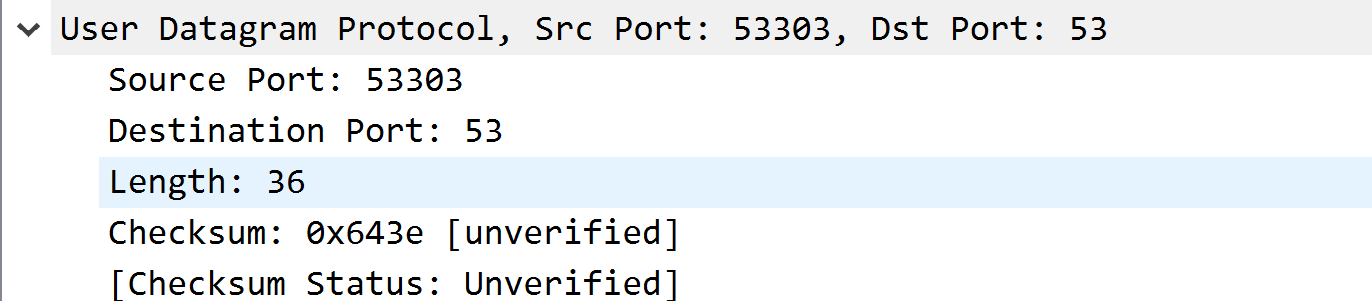
**Answer: The DNS response message provides the IP address that the SYNC packet sent to.**

1. **This web page contains images. Before retrieving each image, does your host issue new DNS queries? *(3 Marks)***

***Answer: Yes. Host will send request to the DNS server for the address of the images.***



1. What is the destination port for the DNS query message? What is the source port of DNS response message? *(3 Marks)*

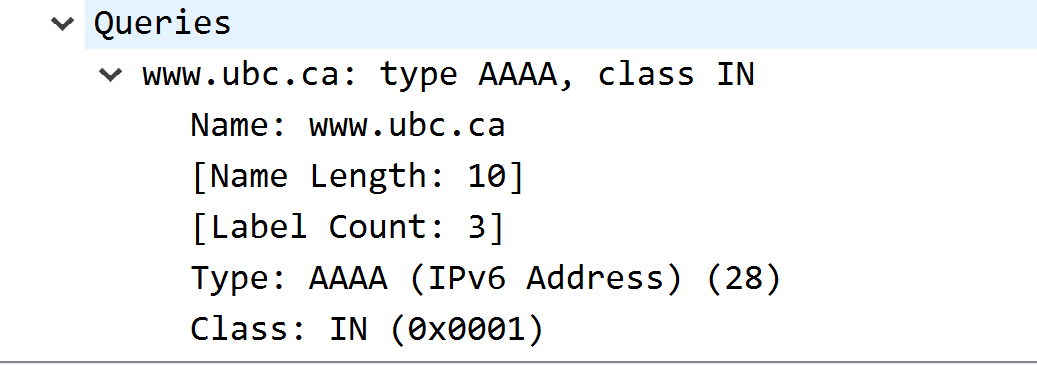


Answer: The destination port is 53, the source port is 53303.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? *(4 Marks)*

*Answer: The IP address the DNS query message sent is 192.168.2.1. It is the same as 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”? *(4 Marks)*

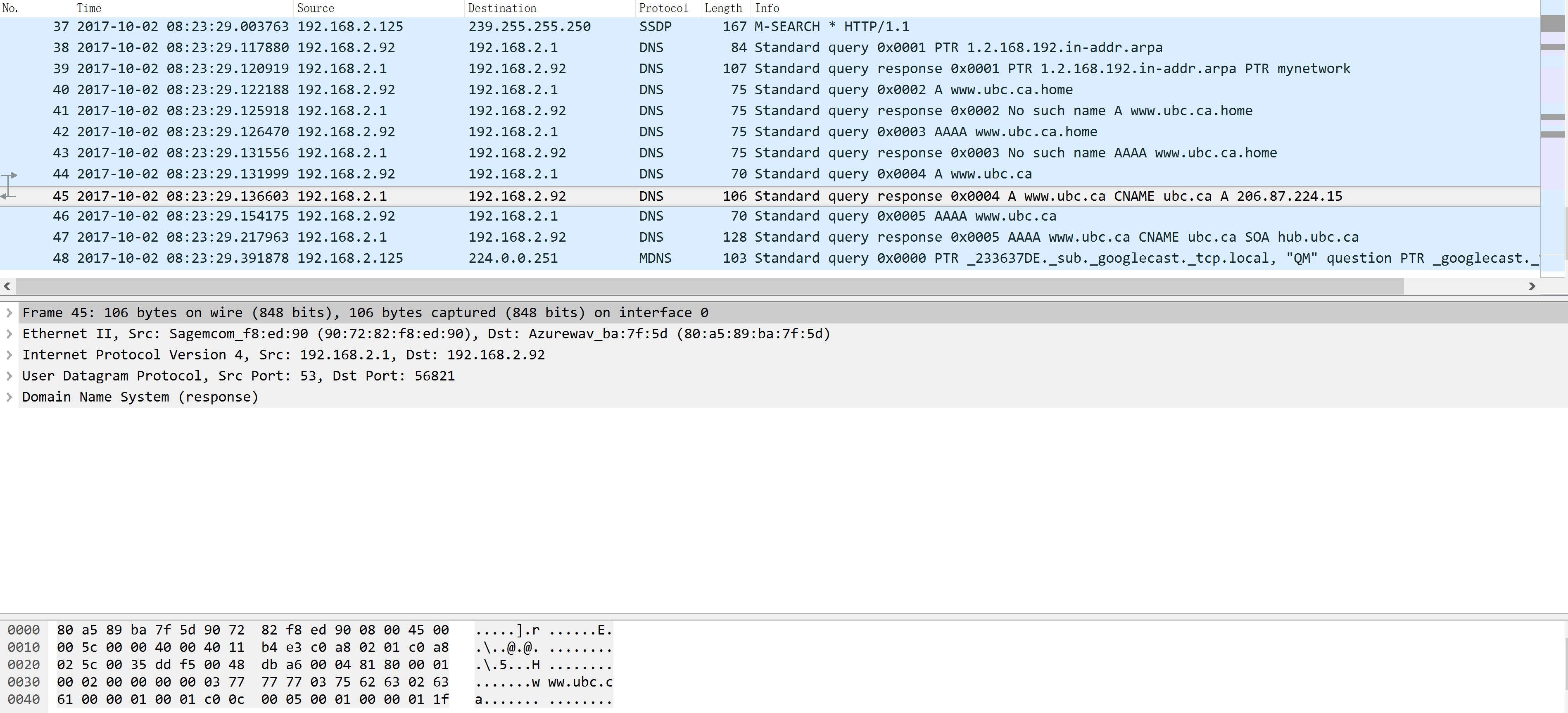


Answer : The DNS query message showed the type of the DNS query is Type **“AAAA”**. No ‘**answers’** is provided.

1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? *(4 Marks)*

*Answer: Only* ***1*** *answer is provided. The answer includes* ***Name, Type, Class, Time to Live, Data length and CNAME***

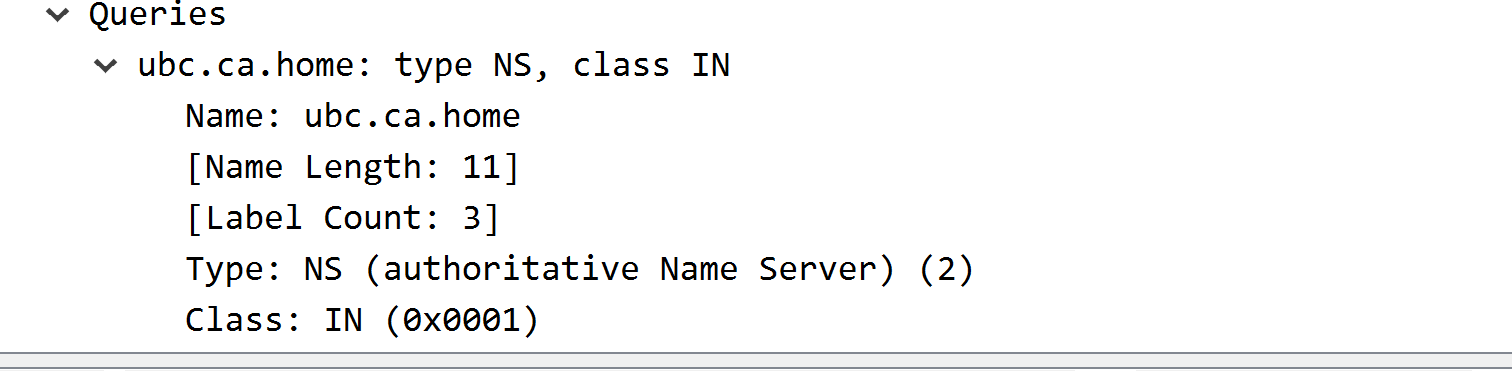
1. **Provide a screenshot. (7 Marks)**



1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? *(4 Marks)*

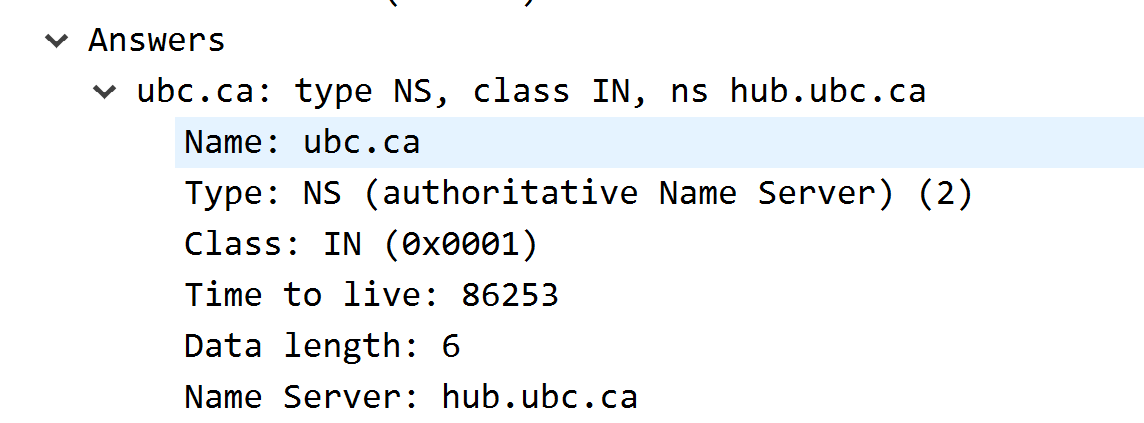
*Answer:The IP address sent is 192.168.2.1.It is the same as my local DNS server.*

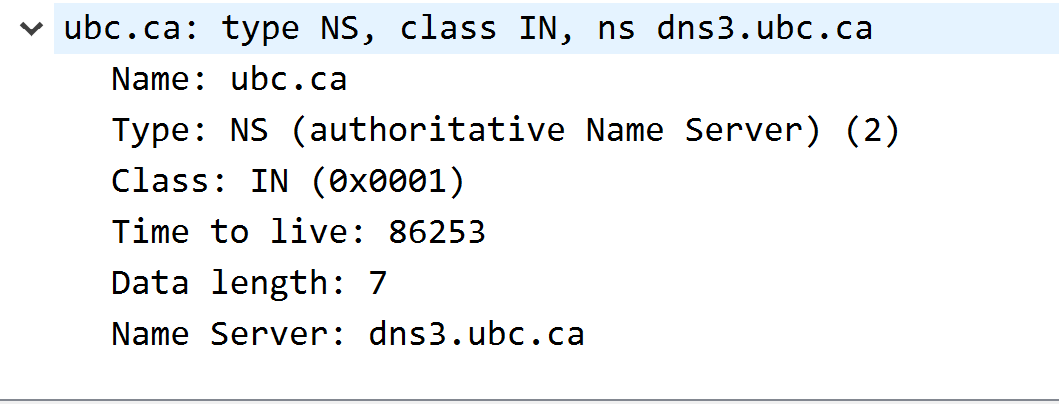
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? *(4 Marks)*



*Answer: The Type of the query is* ***“NS”****. No ‘answers’ is provided.*

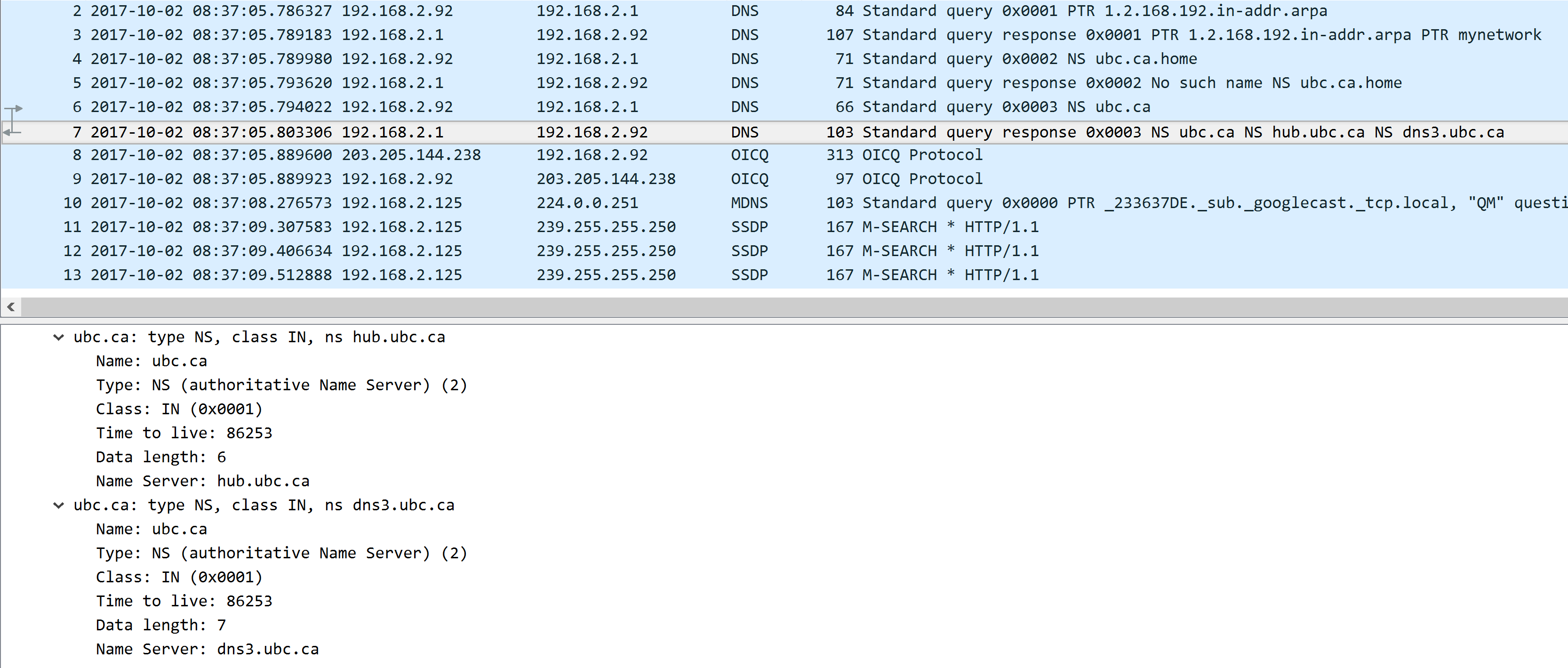
18. Examine the DNS response message. What UBC nameservers does the response message provide? Does this response message also provide the IP addresses of the UBC namesers? *(5 Marks)*



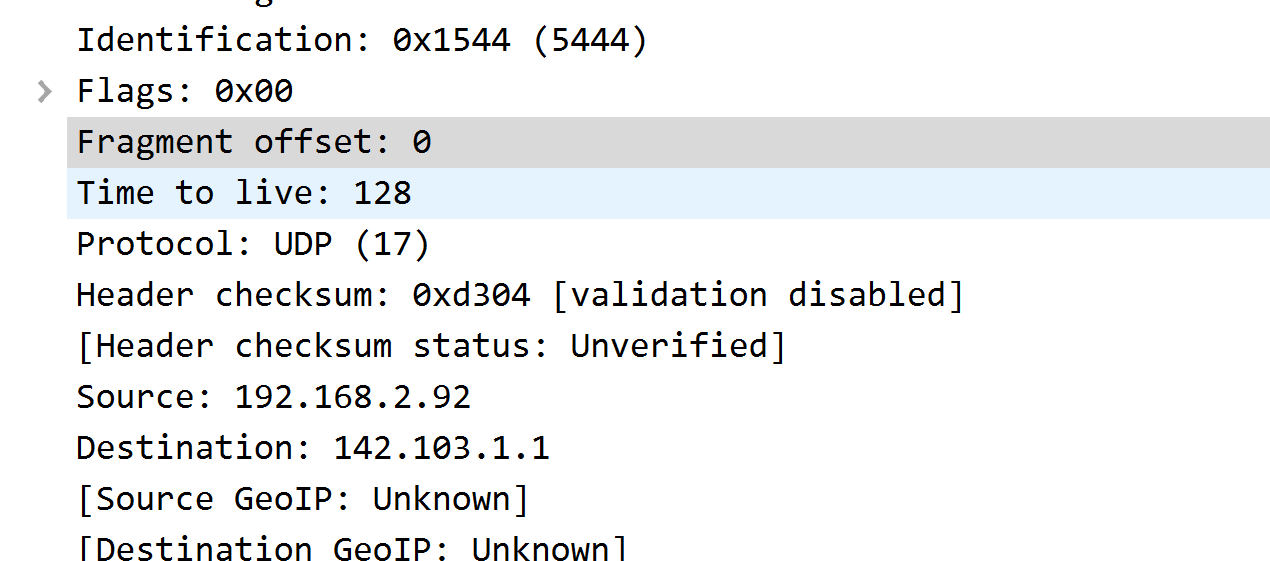


**Answer: The nameserver is hub.ubc.ca and dns3.ubc.ca. The response message didn’t provde IP addresses.**

1. Provide a screenshot. *(7 Marks)*

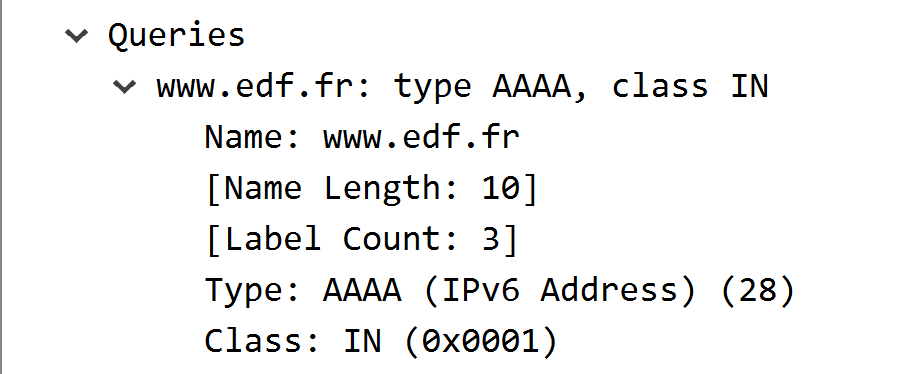


1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to? (5 Marks)



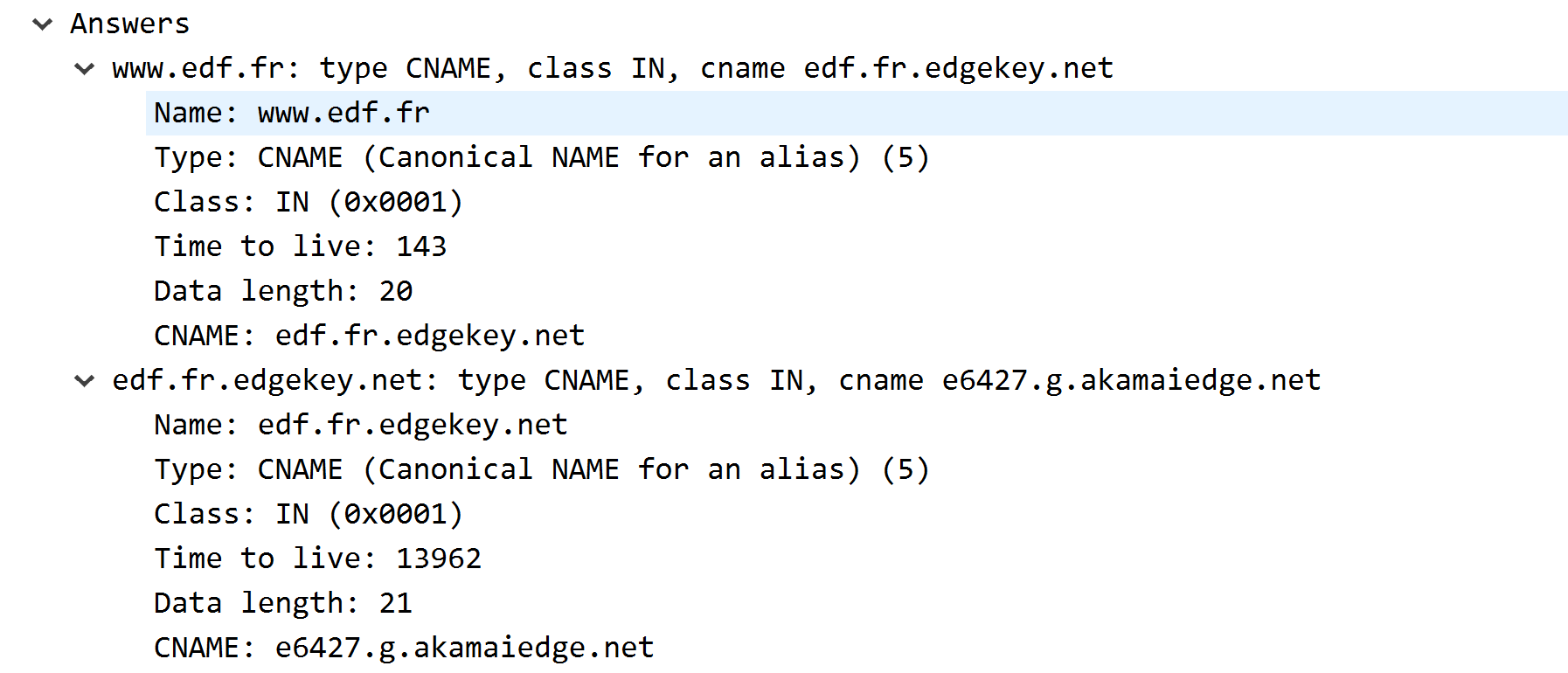
*Answer:The IP address sent is* ***142.103.1.1****. It is not the same as my local DNS server* ***192.168.2.1****.*

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? *(4 Marks)*



*Answer: The type of the DNS query message is type ‘****AAAA’****. It* ***didn’t*** *contain any answer.*

1. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain? *(4 Marks)*



*Answer: Two answers are provided. It contains the* ***name, type,class time to live, data length*** *and the* ***cname****.*

23. Provide a screenshot. *(7 Marks)*

