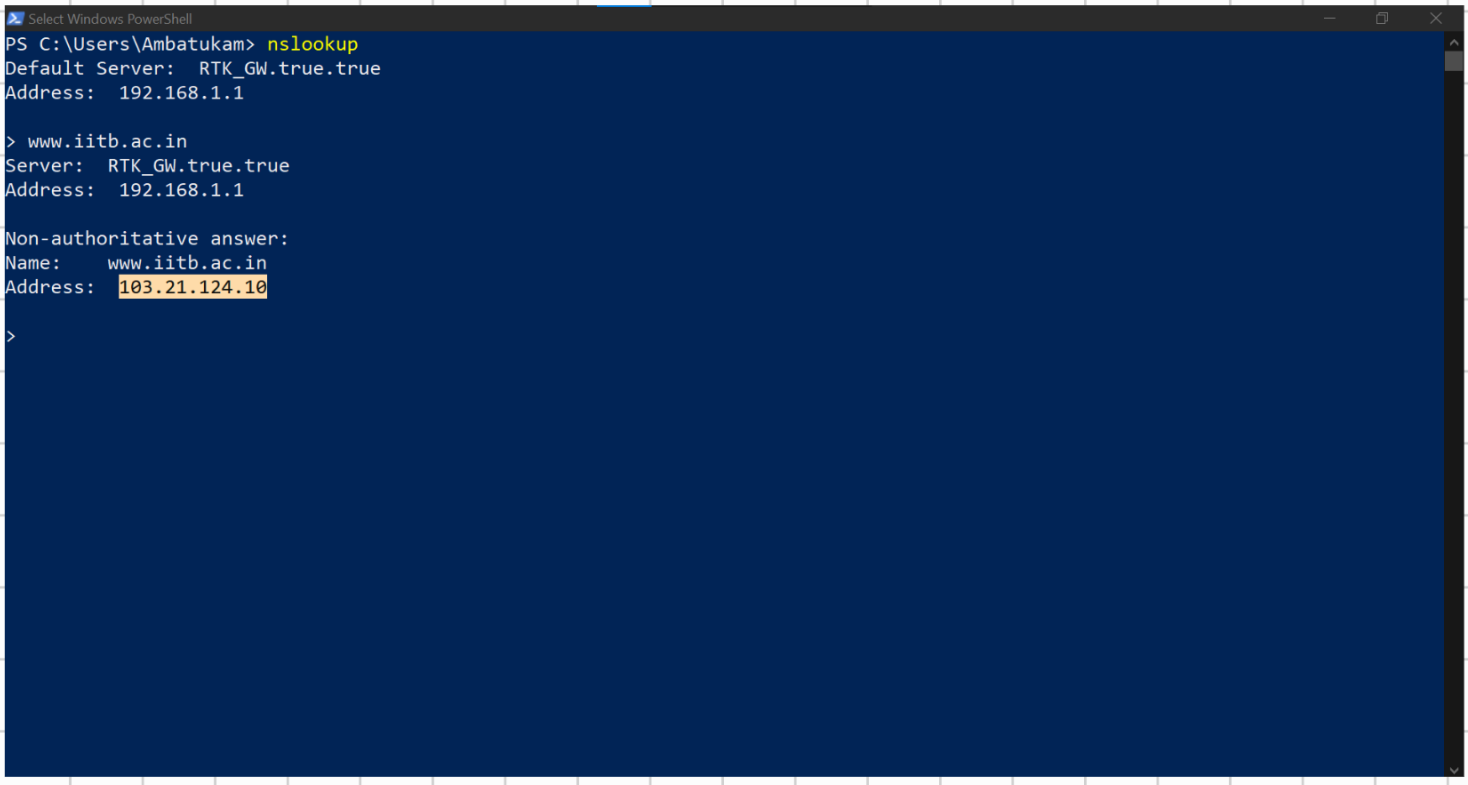
Wireshark Lab 02: DNS

Section 650001

Group ID : G02

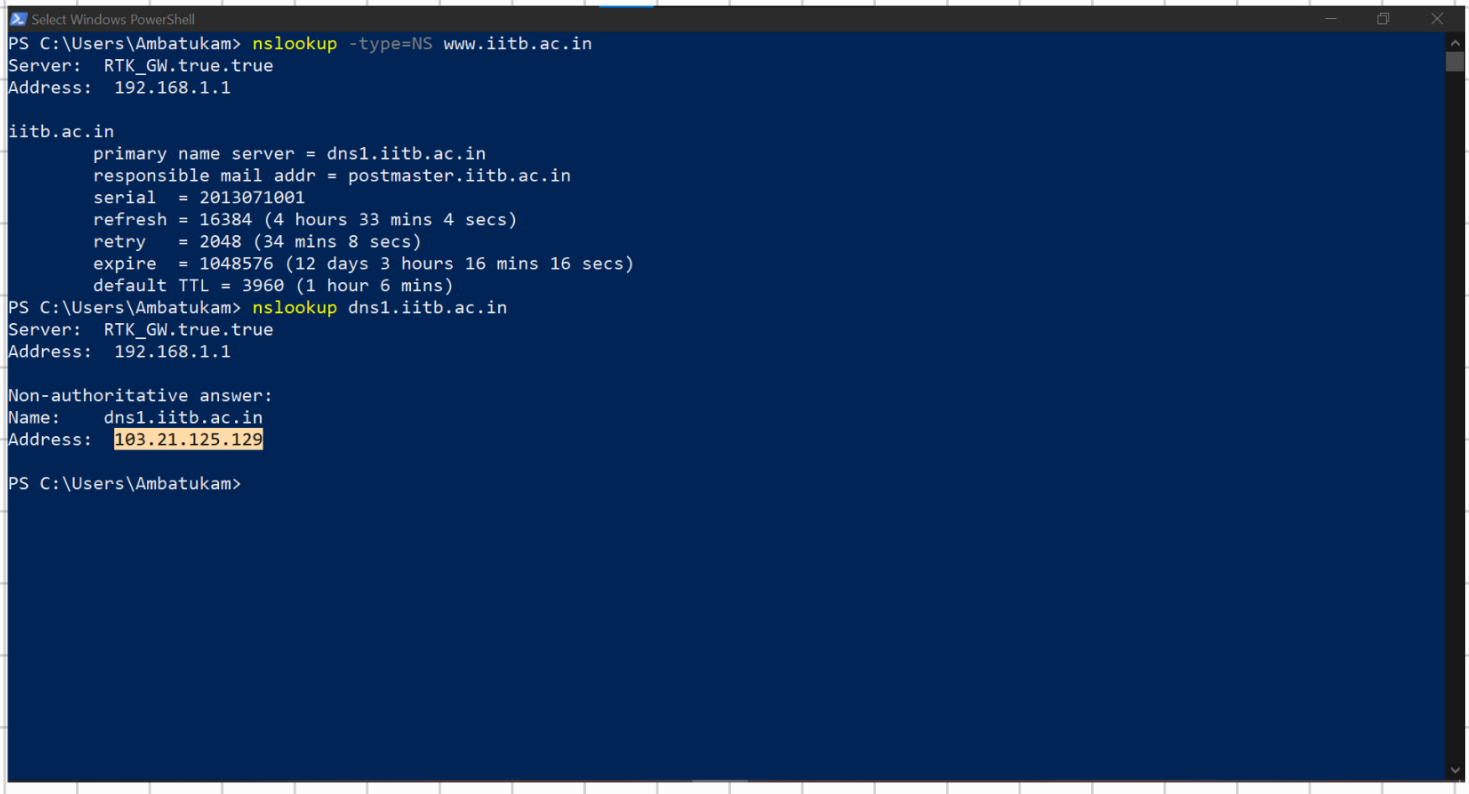
สมาชิกกลุ่ม
นายธีรภัทร เกิดไพบูลย์ 6509650468

1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in



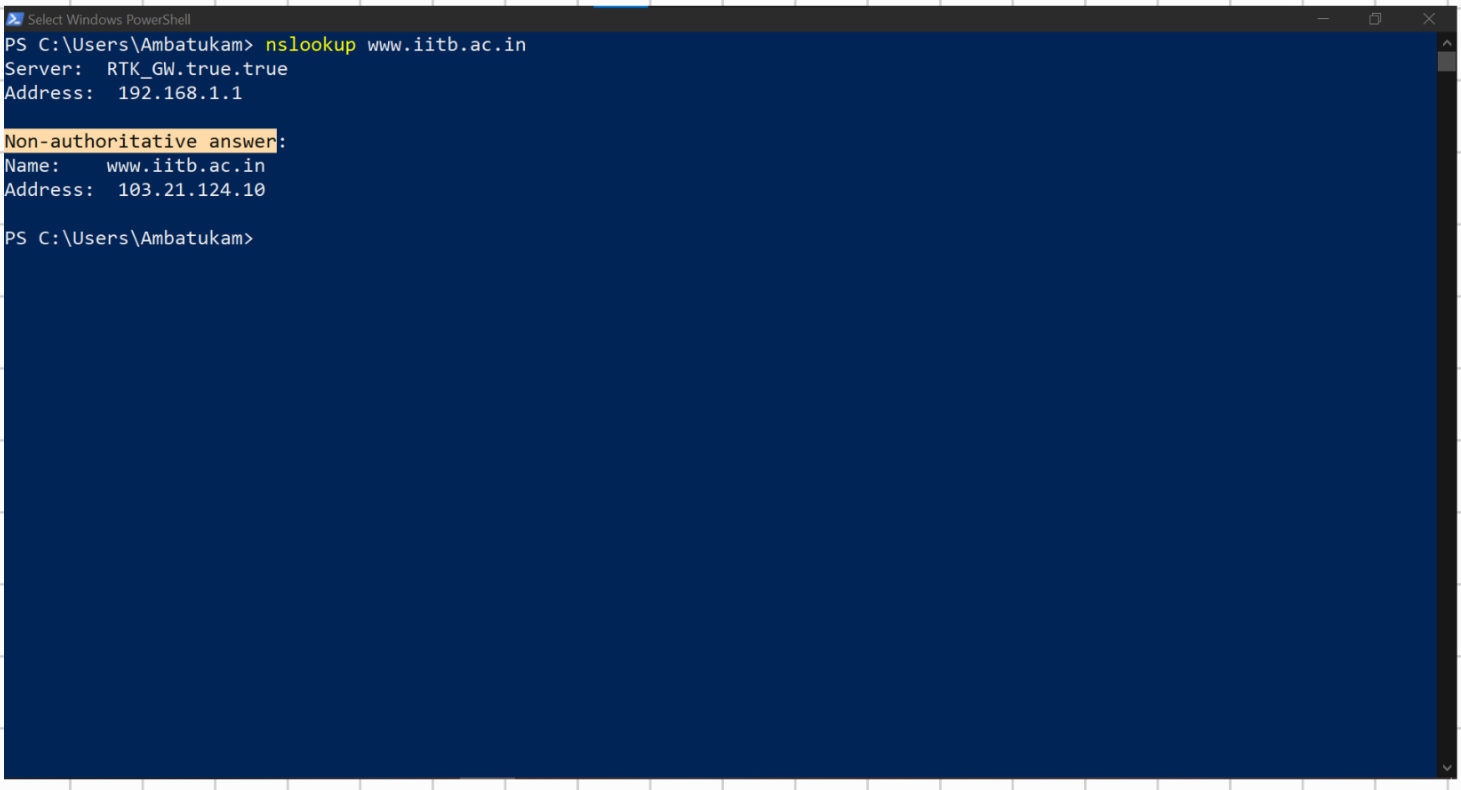
IP Address ของ www.iitb.ac.in คือ 103.21.124.10

2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?



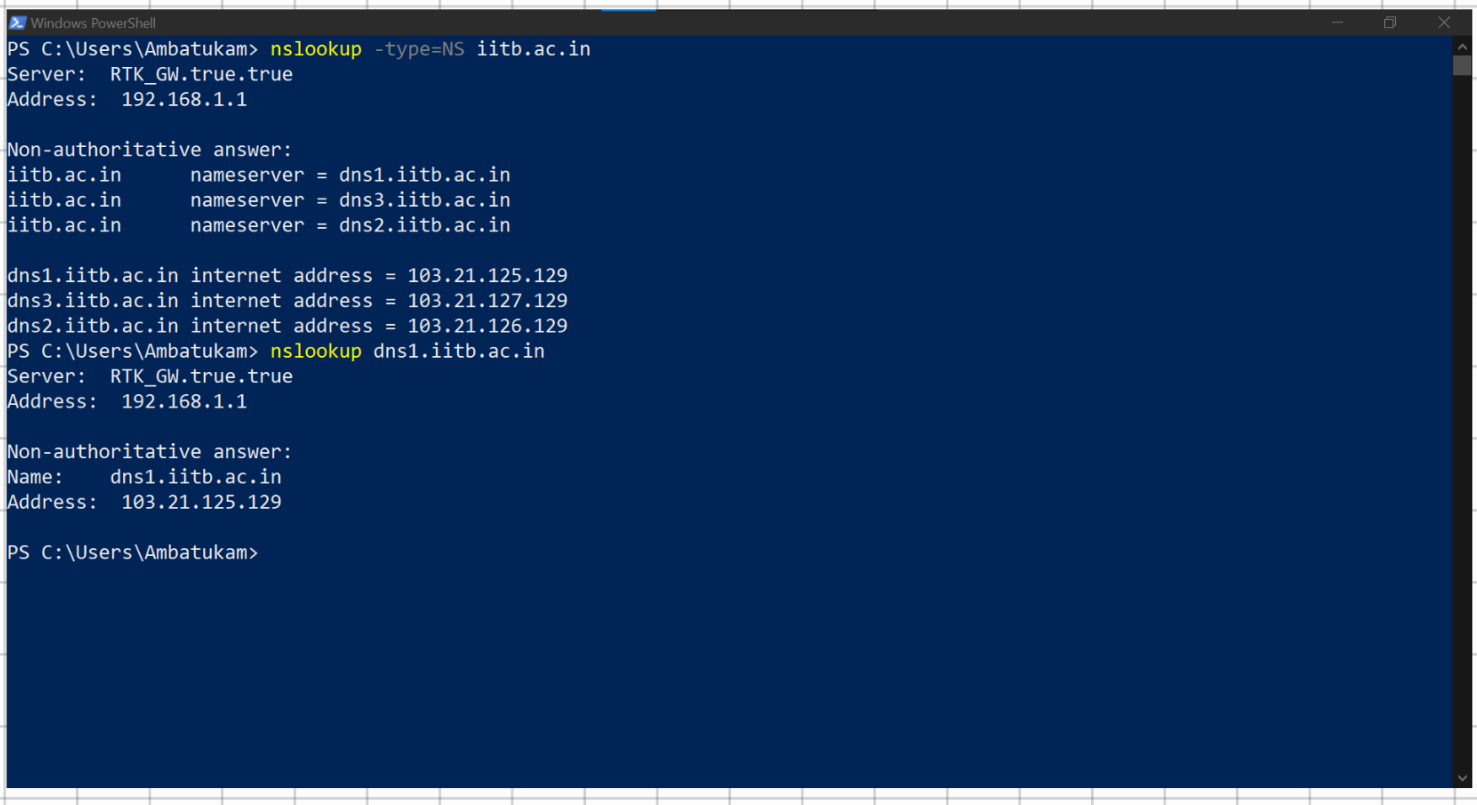
IP address ของ DNS เซิร์ฟเวอร์ dns1.iitb.ac.in คือ 103.21.125.129

3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?



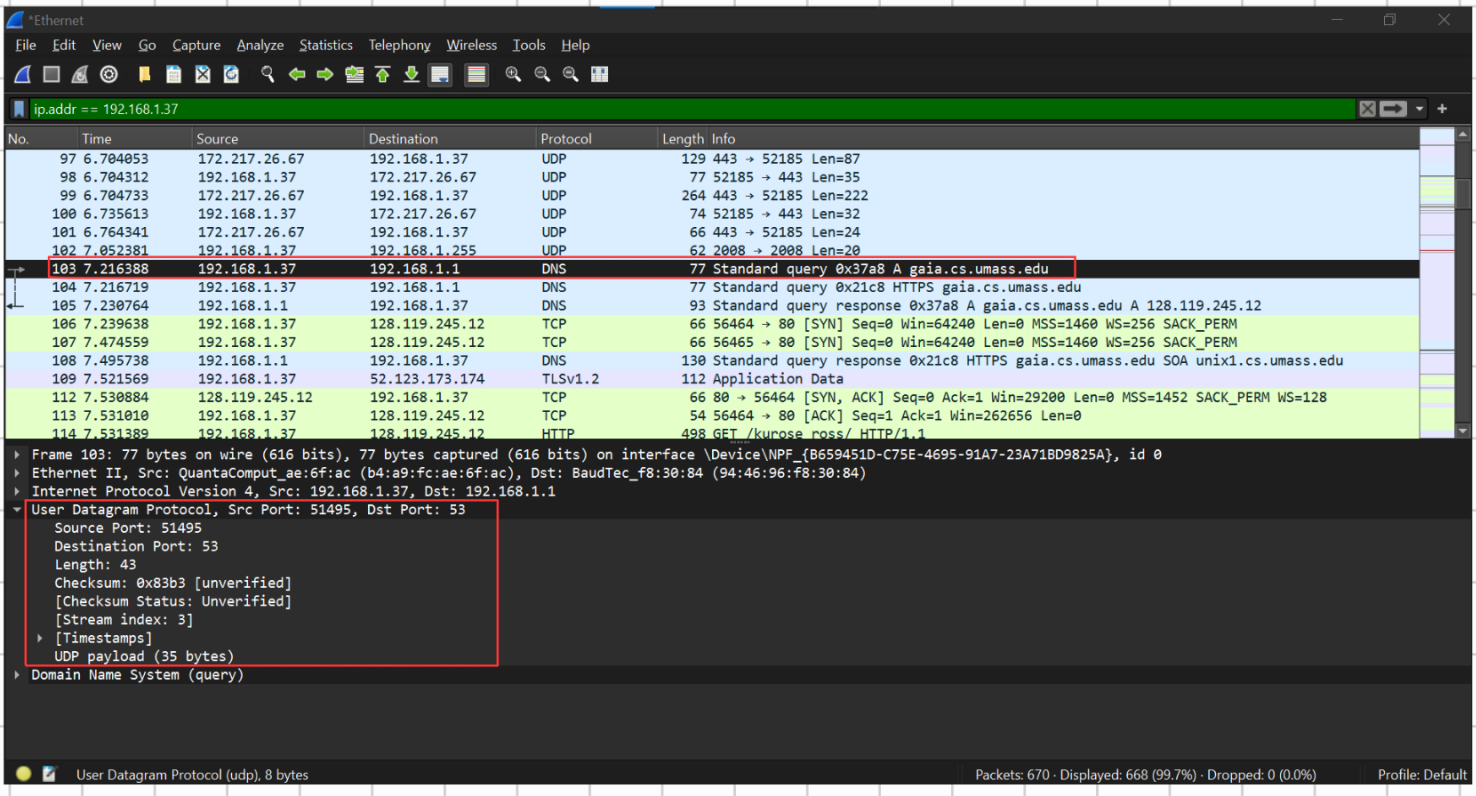
Non-authoritative server

4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?



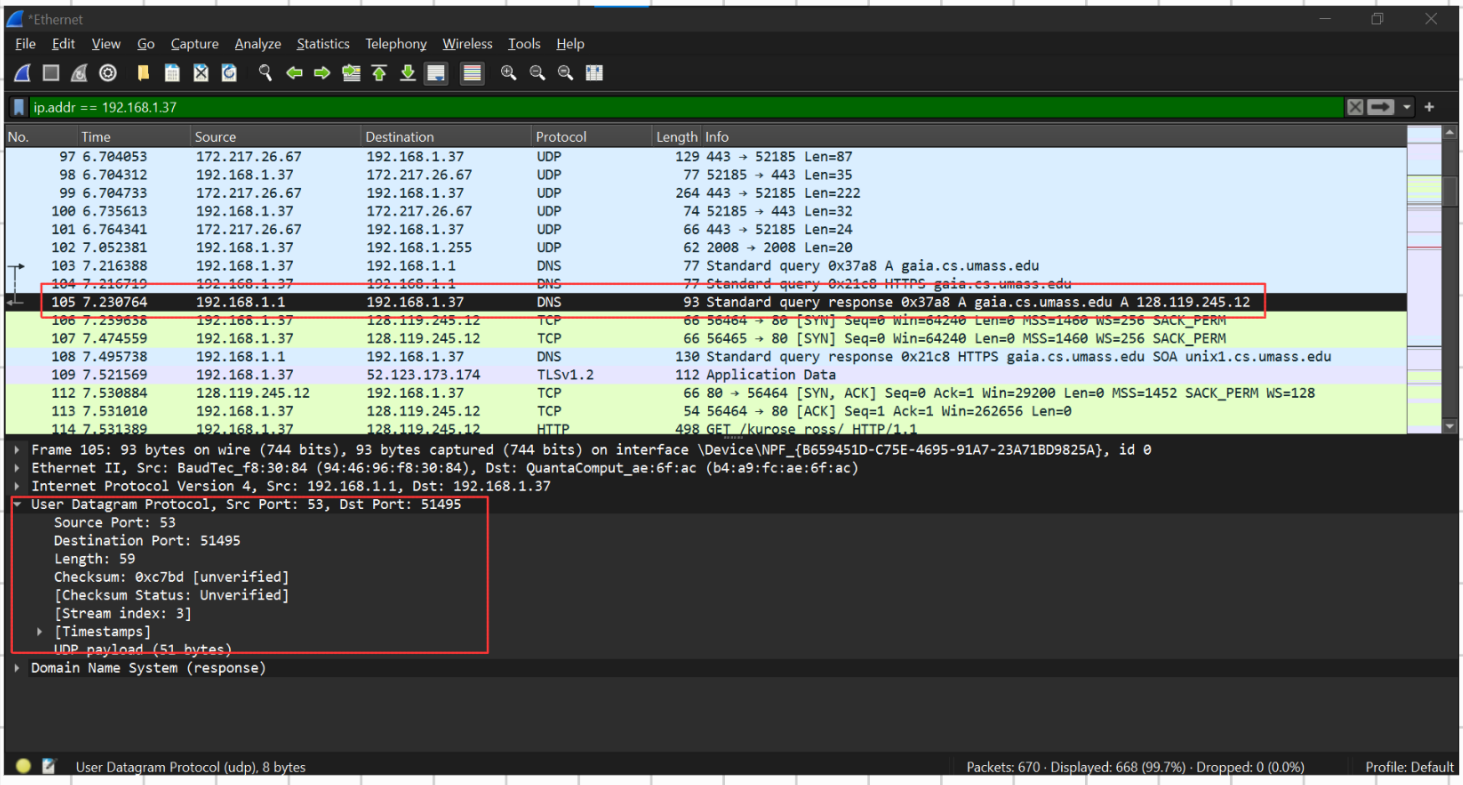
Authoritative name server ที่แสดงเป็นชื่อแรก คือ dns1.iitb.ac.in
ใช้คำสั่ง nslookup ตามด้วย authoritative name server เช่น nslookup dns1.iitb.ac.in

5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?



แพ็กเก็ตหมายเลข 103
ส่งบน UDP

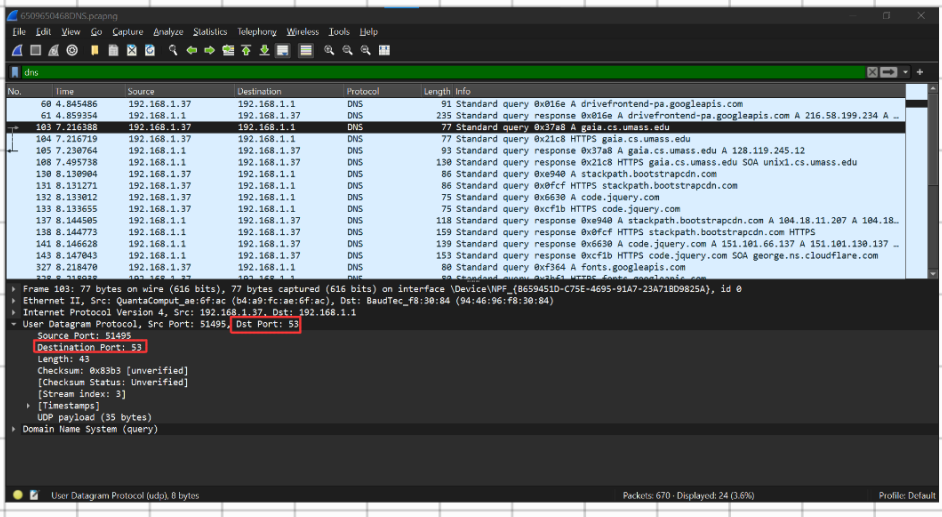
6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?



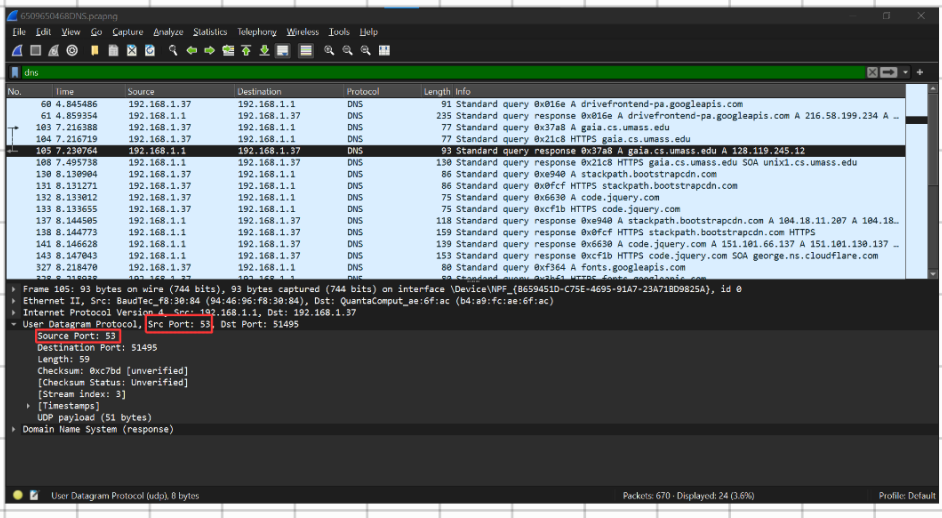
แพ็กเก็ตหมายเลข 105

ส่งบน UDP

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

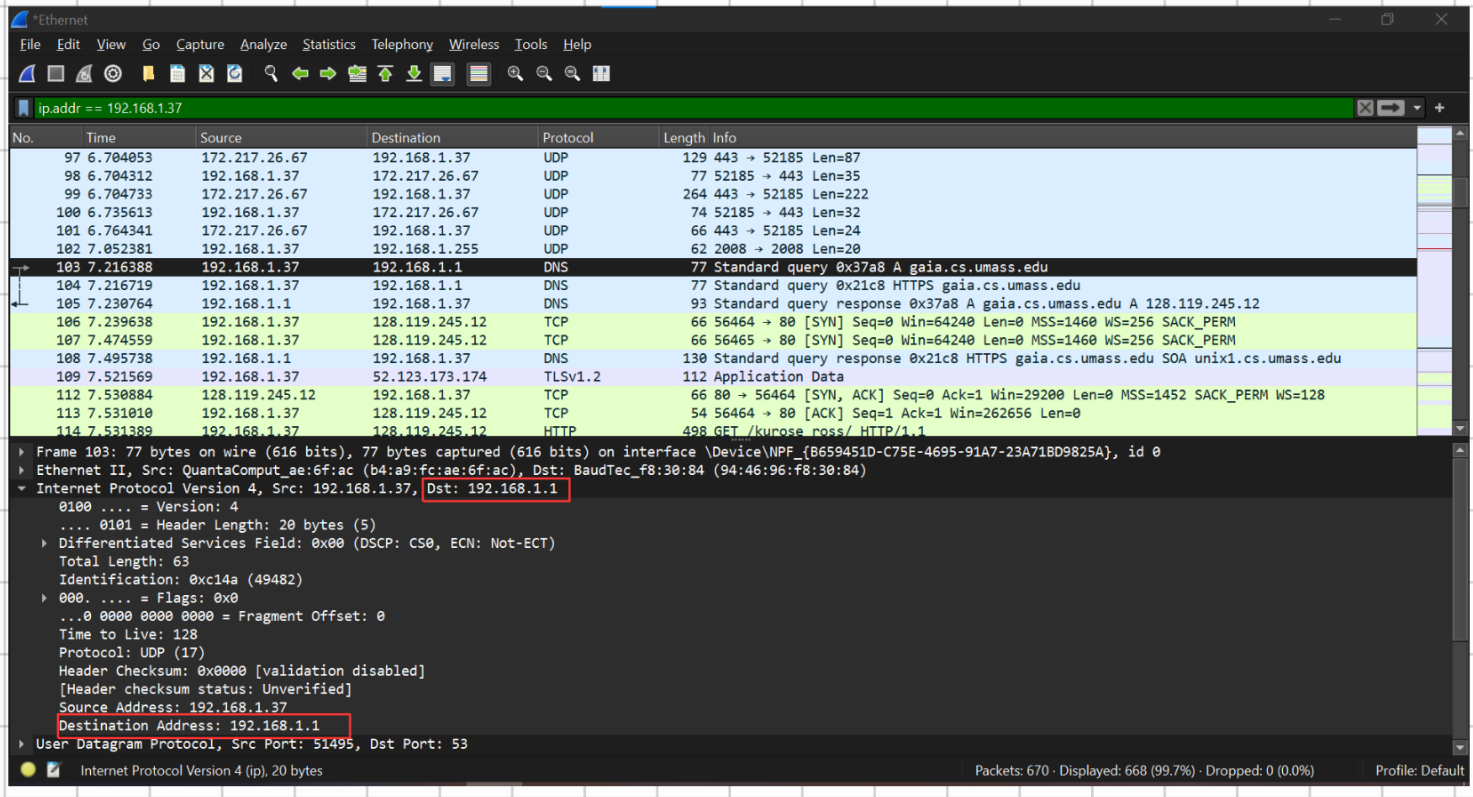


Destination Port of DNS query message: 53



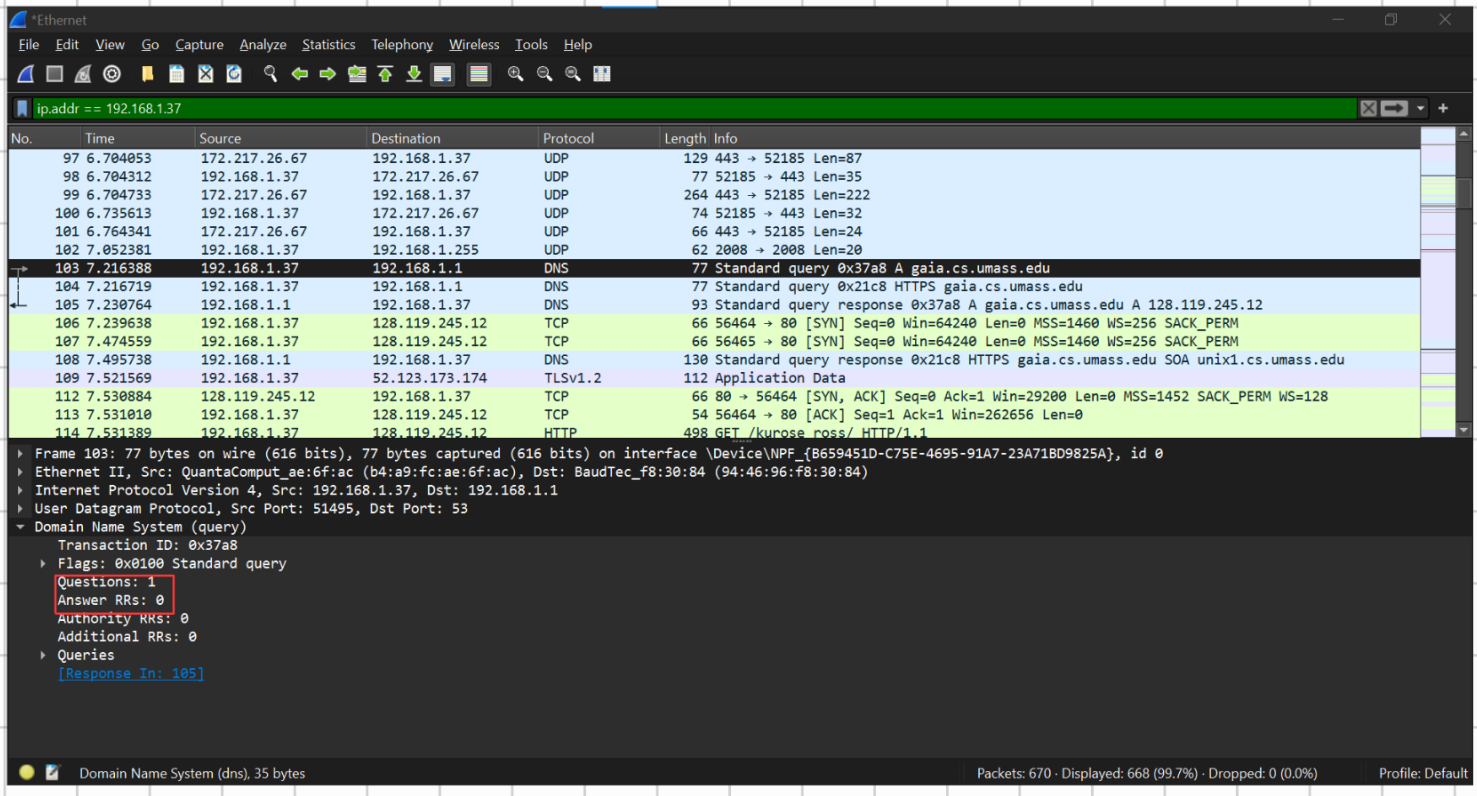
Source Port of the DNS response message: 53

8. To what IP address is the DNS query message sent?



Destination Address: 192.168.1.1

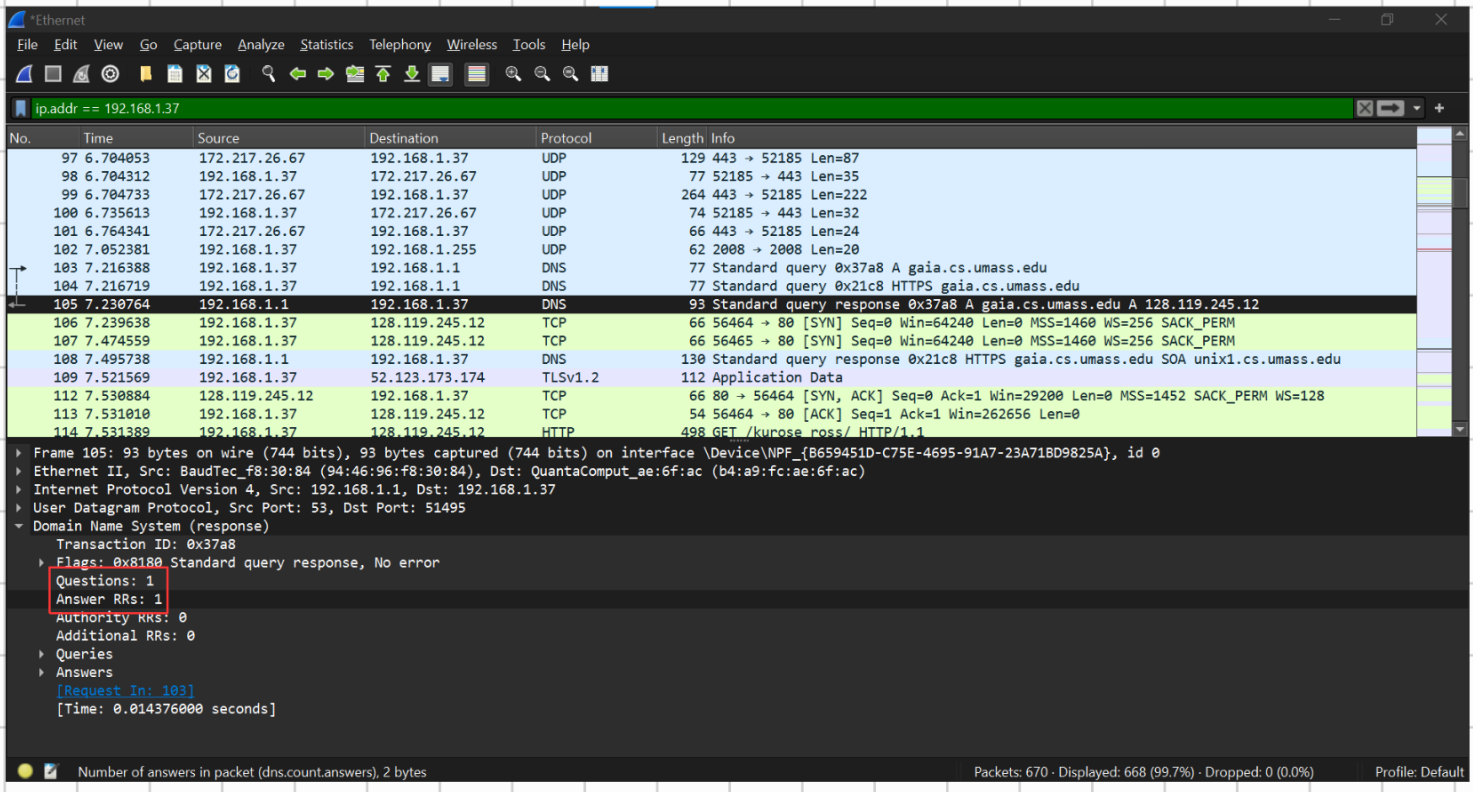
9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?



Questions: 1

Answer RRs: 0

10. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?



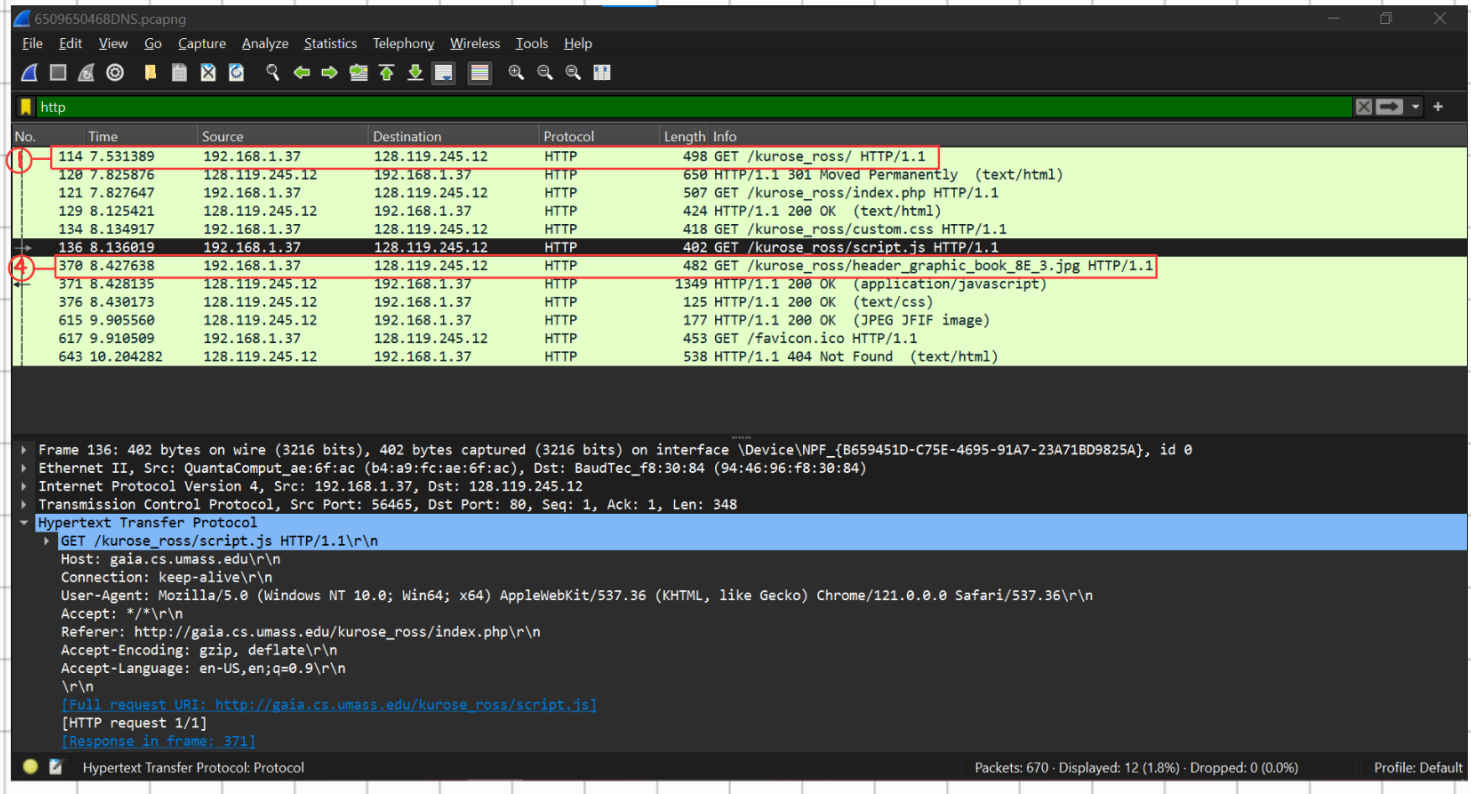
Questions: 1

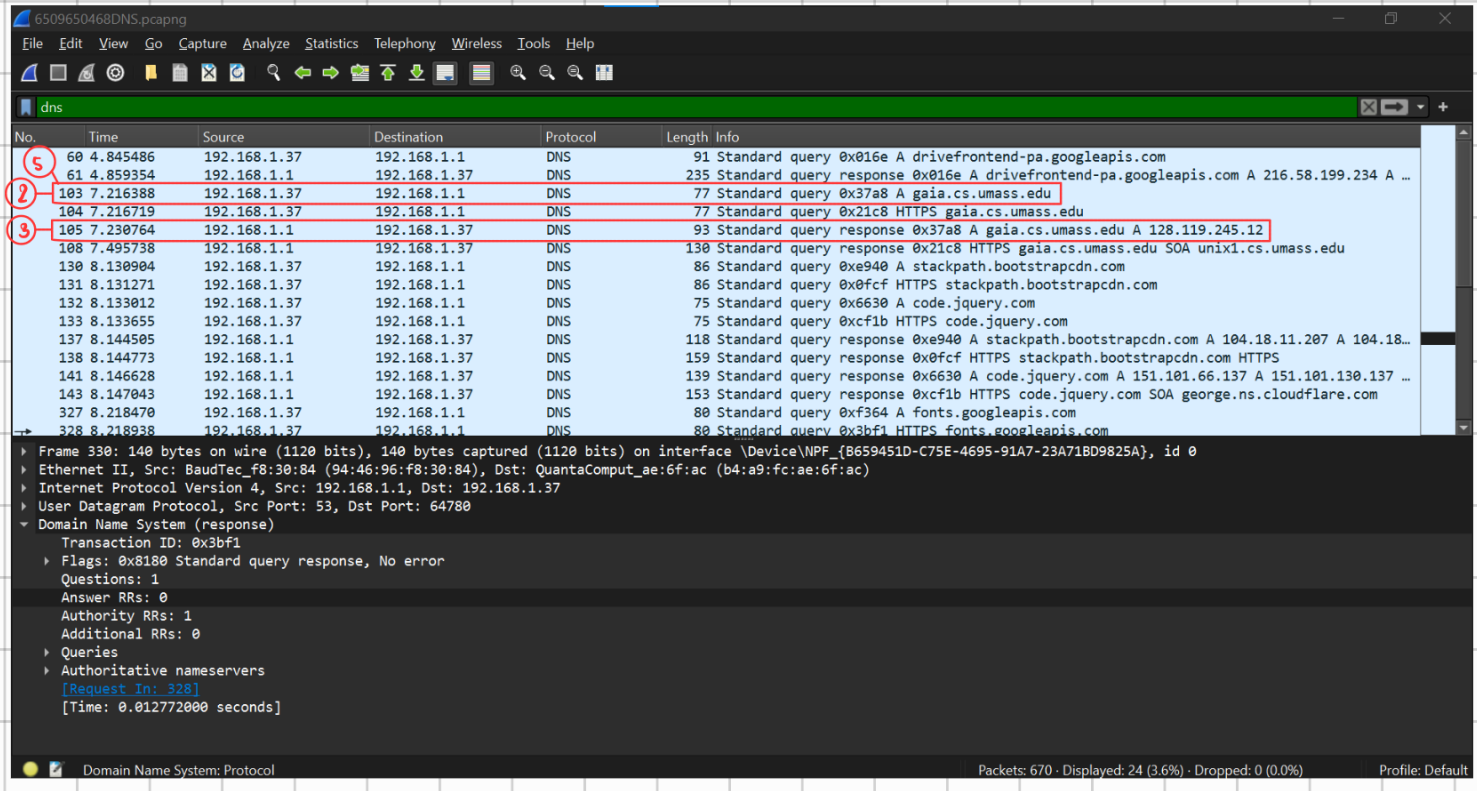
Answers RRs: 1

11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references
the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like
the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/? What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address? What is the packet number in the trace of the received DNS response? What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg? What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address? Discuss how DNS caching affects the answer to this last question.

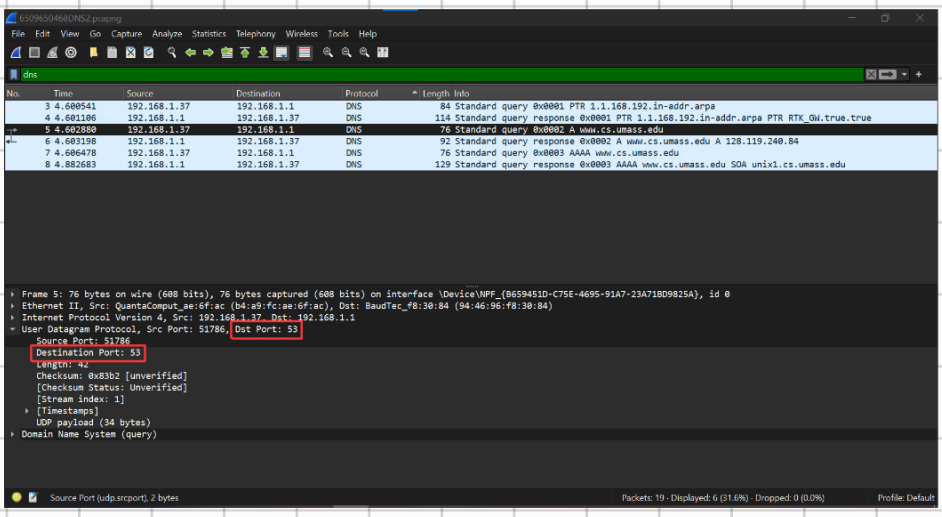
1. หมายเลขแพ็กเก็ตของ HTTP GET Request สำหรับ http://gaia.cs.umass.edu/kurose_ross/ คือ 114
2. หมายเลขแพ็คเก็ตใน DNS query ที่ HTTP Request เริ่มต้นส่งไปยัง IP gaia.cs.umass.edu ได้ คือ 103
3. หมายเลขแพ็คเก็ตใน DNS response คือ 105
4. หมายเลขแพ็คเก็ตของ HTTP GET request สำหรับ image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg คือ 370
5. หมายเลขแพ็คเก็ตใน DNS query ที่ HTTP Request ส่งไปยัง IP gaia.cs.umass.edu ครั้งที่สอง คือ 103

6. เนื่องจากคอมพิวเตอร์เก็บแคชการค้นหา DNS จึงไม่จำเป็นต้องทำการค้นหาเพิ่มเติม ดังนั้นหมายเลขแพ็คเก็ตจึงตรงกับหมายเลขแพ็คเก็ตใน DNS query ของ HTTP Request ครั้งที่หนึ่ง

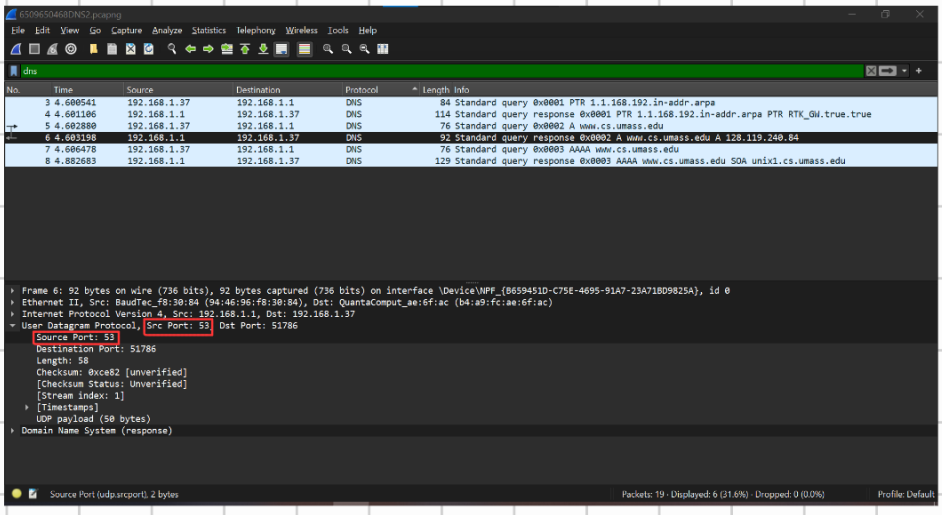




12. What is the destination port for the DNS query message? What is the source port of the DNS response message?

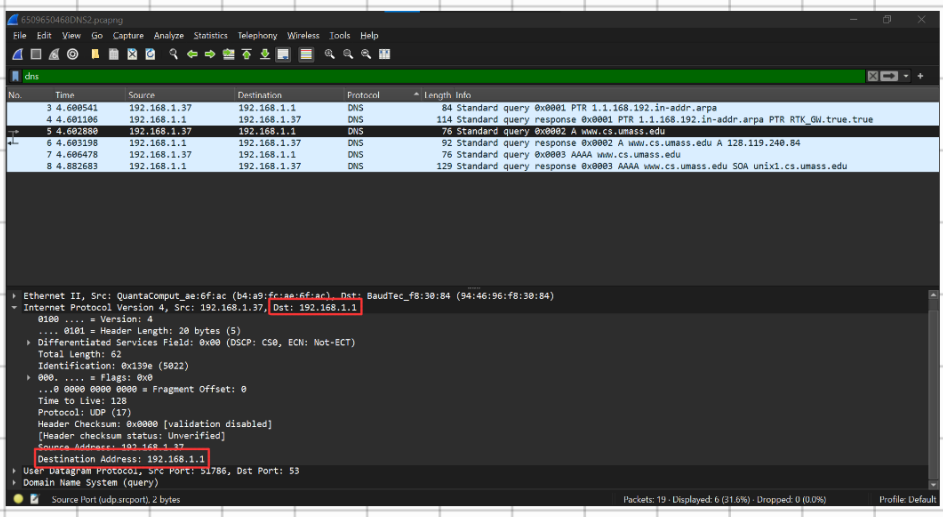


Destination Port of DNS query message: 53

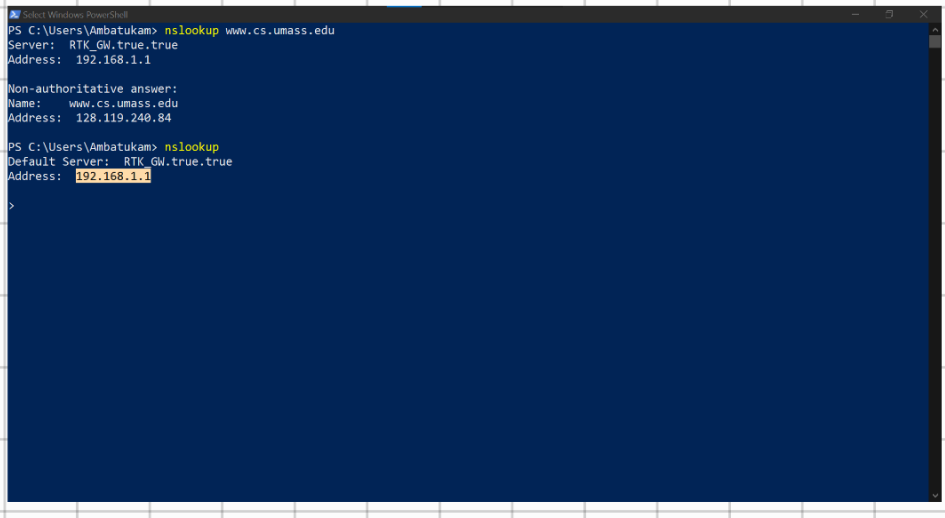


Source Port of the DNS response message: 53

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

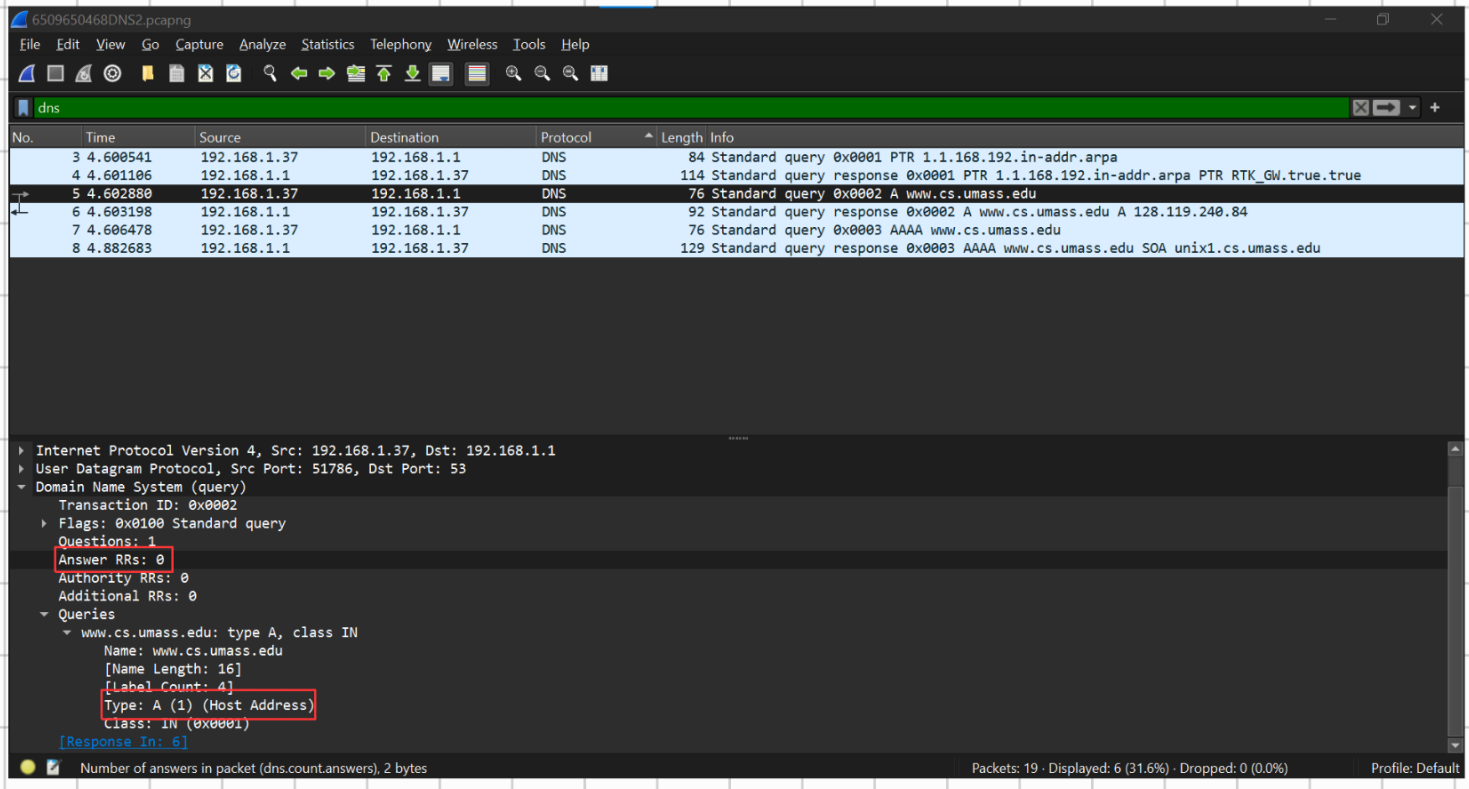


IP address ที่ DNS query message ส่งไป คือ 192.168.1.1



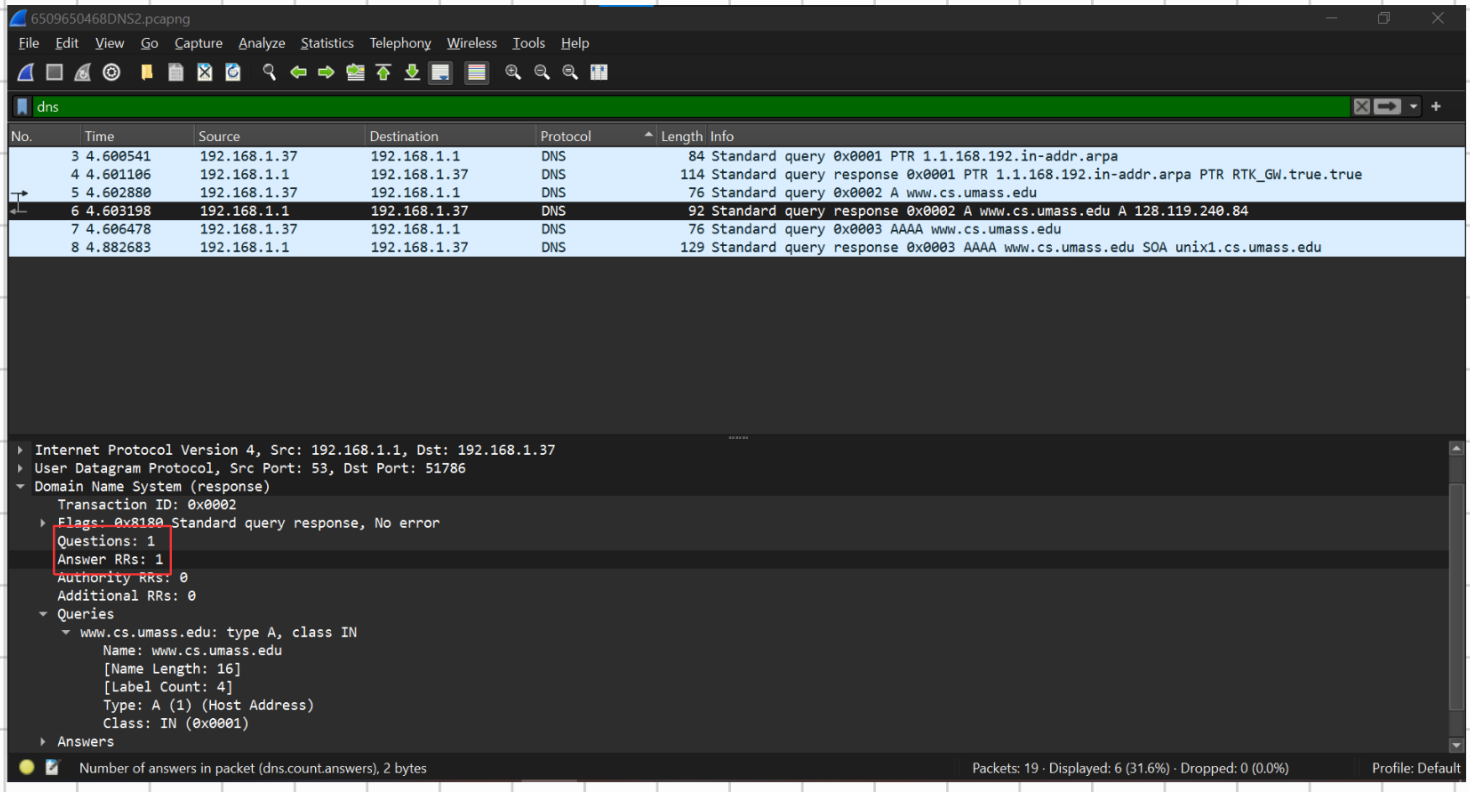
ตรงกับ IP address default local DNS server ของนักศึกษา

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



Type: A (1) (Host Address)
query message ไม่มี “answers”

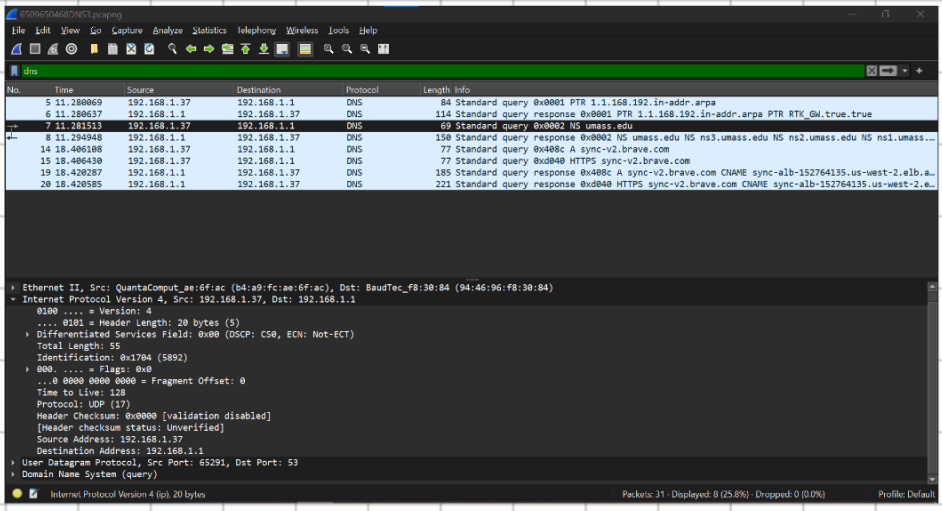
15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?



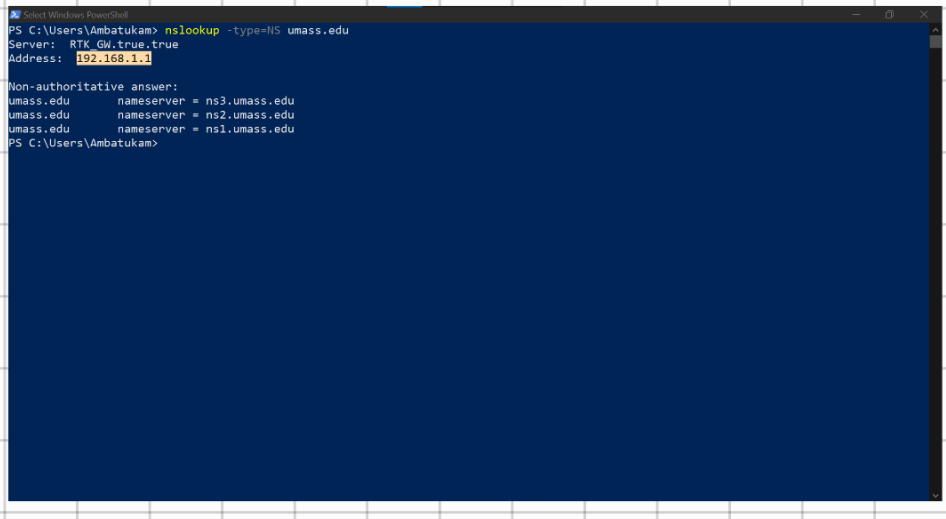
Questions: 1

Answer RRs: 1

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

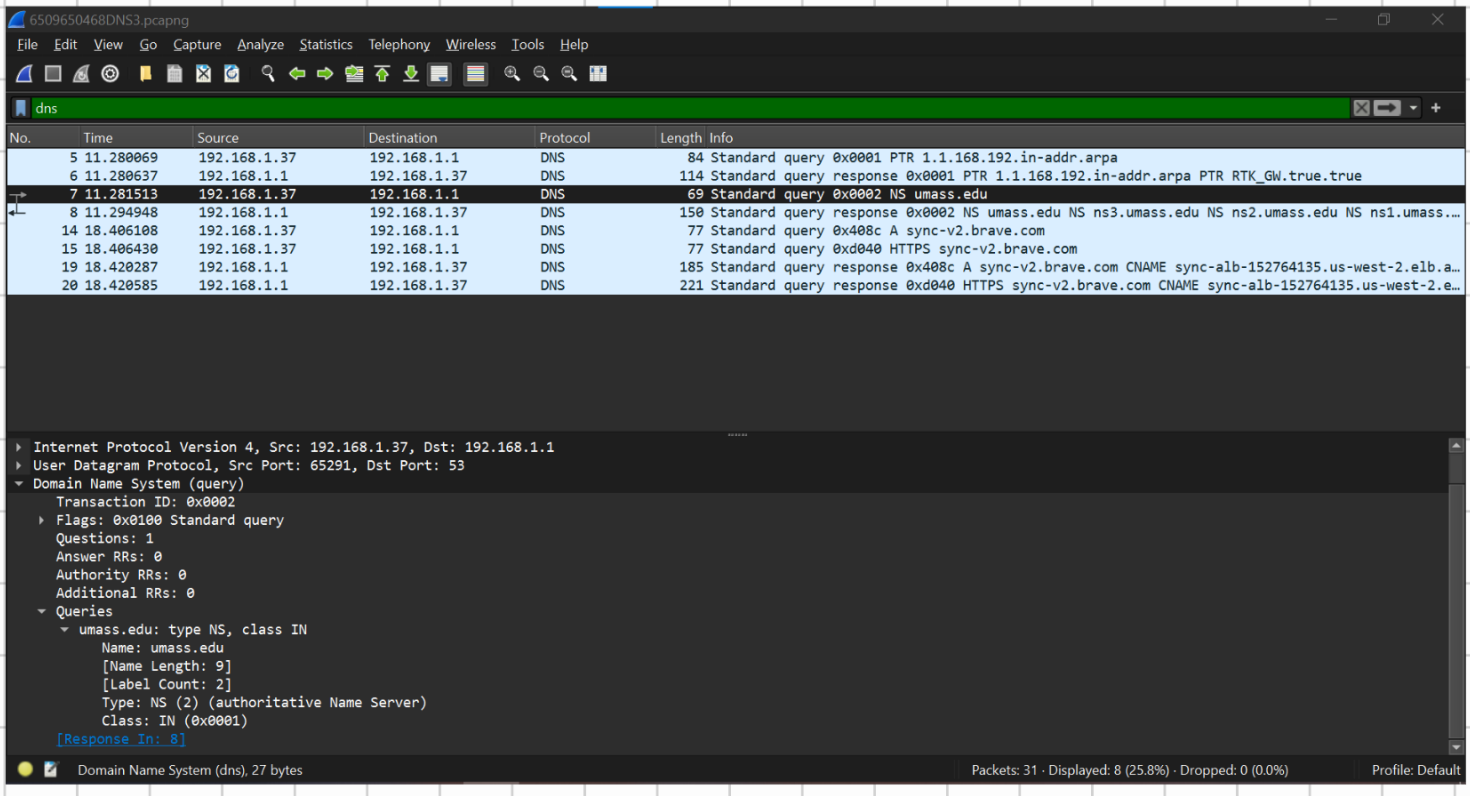


IP address ที่ DNS query message ส่งไป คือ 192.168.1.1



ตรงกับ IP address default local DNS server ของนักศึกษา

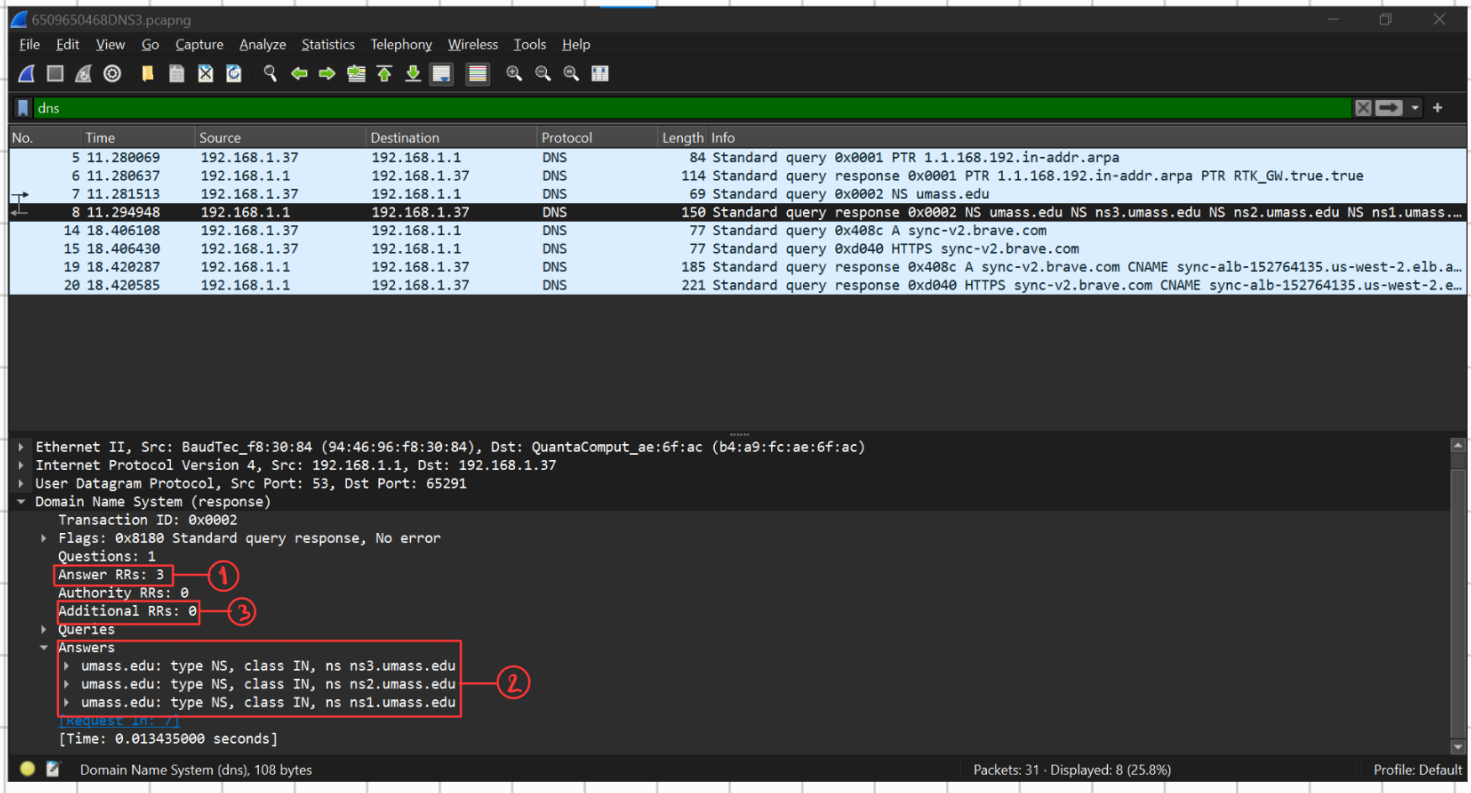
17. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?



Questions: 1

Answer RRs: 0

18. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records?



1. Answer RRs: 3
2. ภายใน Answers มีดังนี้
umass.edu: type NS, class IN, ns ns3.umass.edu
umass.edu: type NS, class IN, ns ns2.umass.edu
umass.edu: type NS, class IN, ns ns1.umass.edu
3. Additional RRs: 0
4. เนื่องจาก Additional RRs เป็น 0 จึงไม่มีข้อมูลใด ๆ ใน Additional RRs