

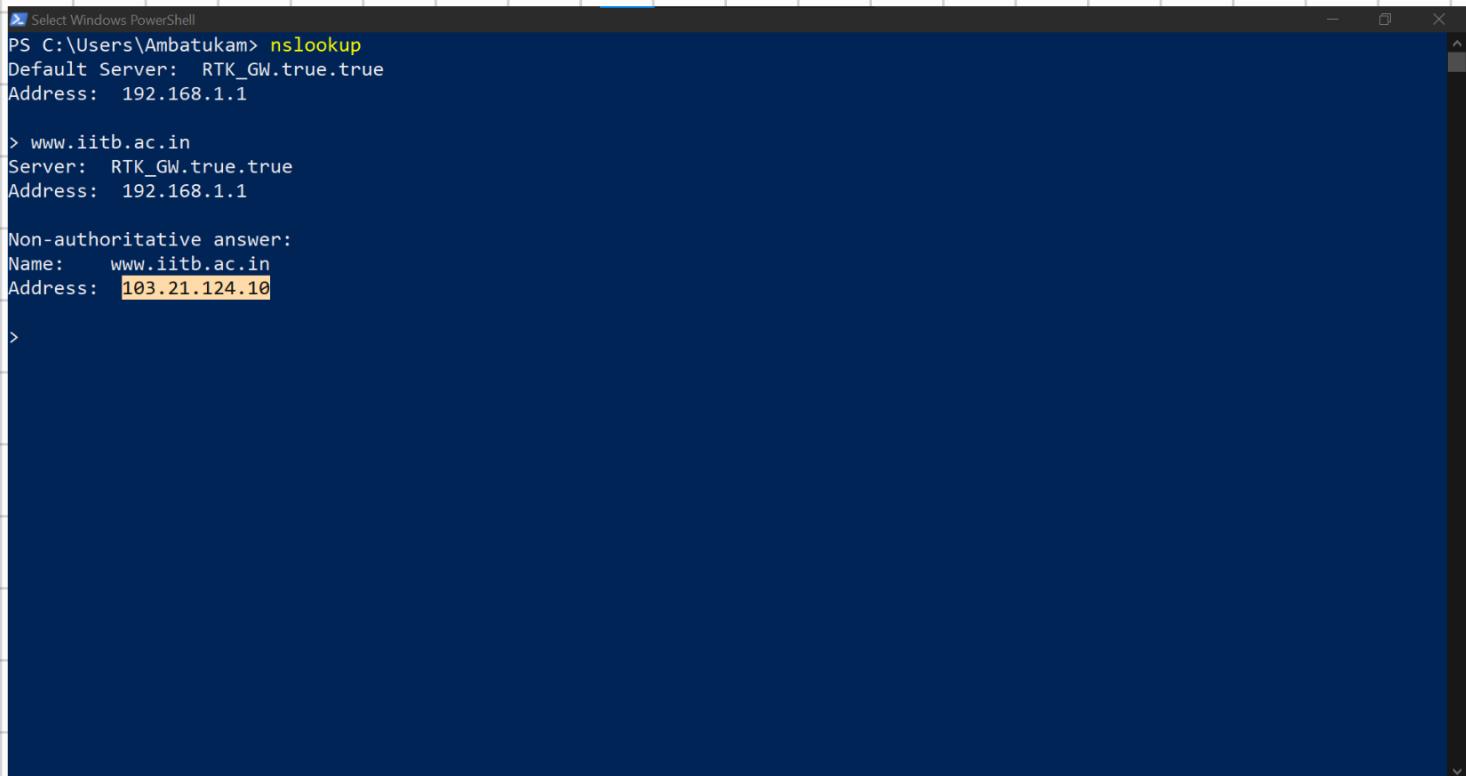
Wireshark Lab 02: DNS

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



```
PS C:\Users\Ambatukam> nslookup
Default Server: RTK_GW.true.true
Address: 192.168.1.1

> www.iitb.ac.in
Server: RTK_GW.true.true
Address: 192.168.1.1

Non-authoritative answer:
Name: www.iitb.ac.in
Address: 103.21.124.10

>
```

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?

```
PS C:\Users\Ambatukam> nslookup -type=NS www.iitb.ac.in
Server:  RTK_GW.true.true
Address:  192.168.1.1

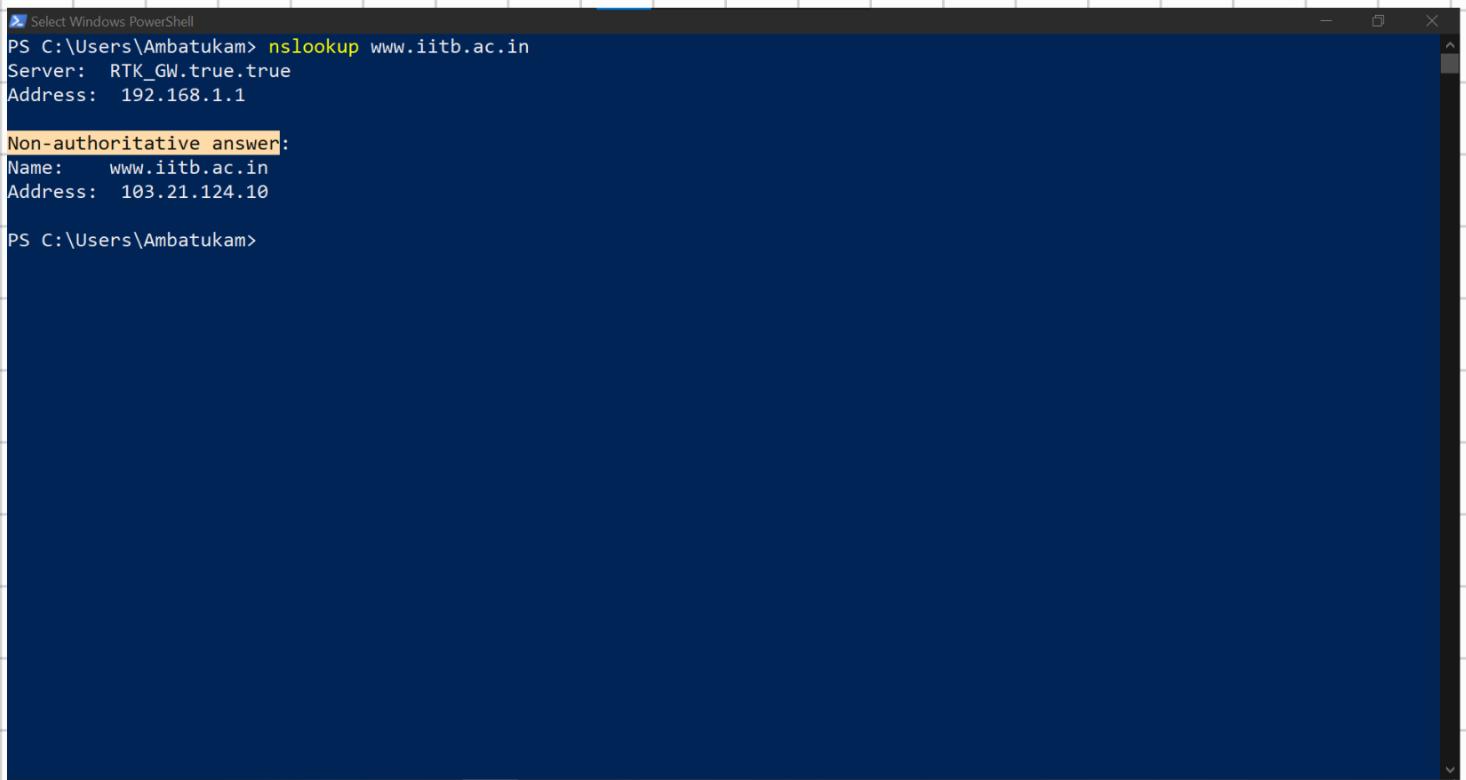
iitb.ac.in
    primary name server = dns1.iitb.ac.in
    responsible mail addr = postmaster.iitb.ac.in
    serial = 2013071001
    refresh = 16384 (4 hours 33 mins 4 secs)
    retry = 2048 (34 mins 8 secs)
    expire = 1048576 (12 days 3 hours 16 mins 16 secs)
    default TTL = 3960 (1 hour 6 mins)
PS C:\Users\Ambatukam> nslookup dns1.iitb.ac.in
Server:  RTK_GW.true.true
Address:  192.168.1.1

Non-authoritative answer:
Name:  dns1.iitb.ac.in
Address: 103.21.125.129

PS C:\Users\Ambatukam>
```

IP address ของ DNS เชิร์ฟเวอร์ 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?



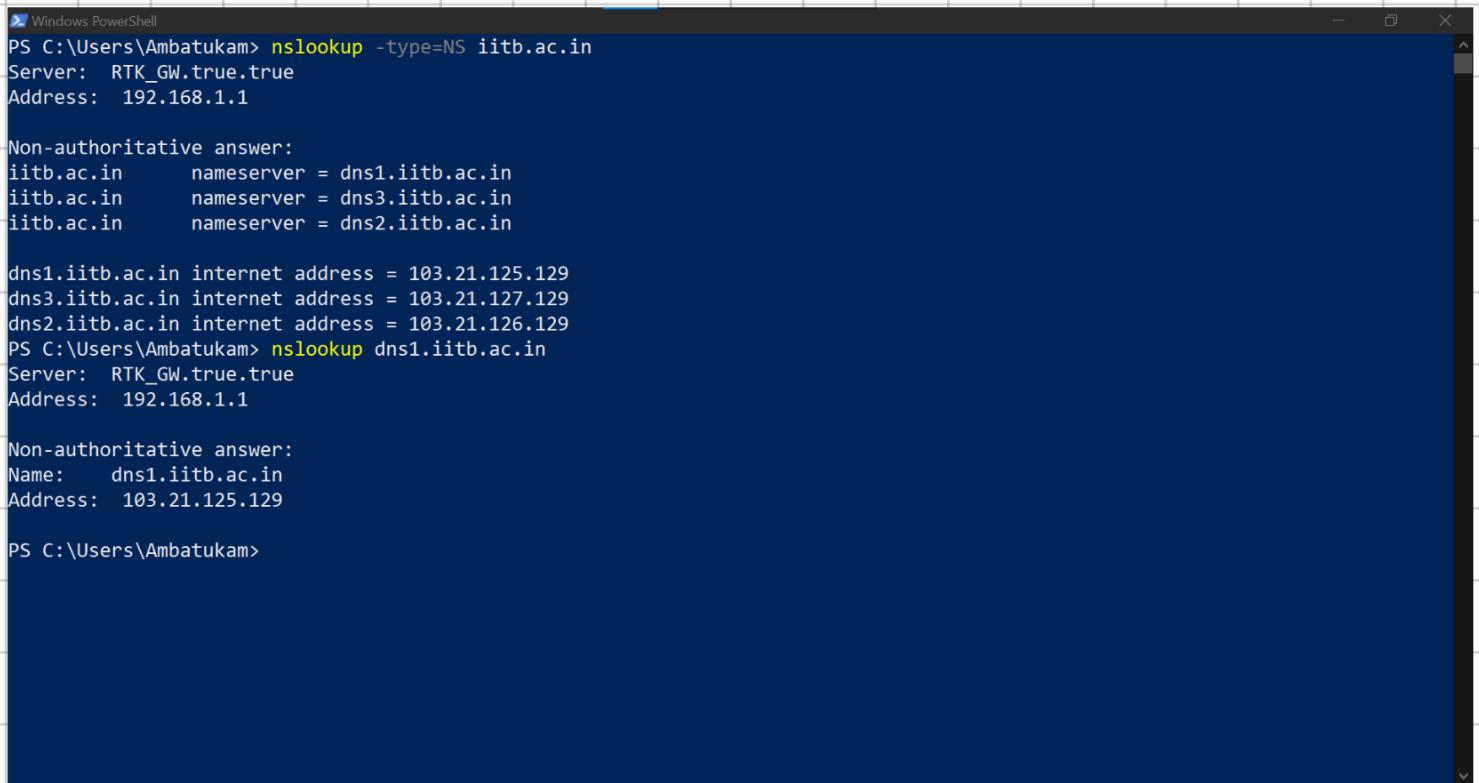
```
PS C:\Users\Ambatukam> nslookup www.iitb.ac.in
Server:  RTK_GW.true.true
Address: 192.168.1.1

Non-authoritative answer:
Name:  www.iitb.ac.in
Address: 103.21.124.10

PS C:\Users\Ambatukam>
```

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?



```
Windows PowerShell
PS C:\Users\Ambatukam> nslookup -type=NS iitb.ac.in
Server:  RTK_GW.true.true
Address: 192.168.1.1

Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in

dns1.iitb.ac.in internet address = 103.21.125.129
dns3.iitb.ac.in internet address = 103.21.127.129
dns2.iitb.ac.in internet address = 103.21.126.129
PS C:\Users\Ambatukam> nslookup dns1.iitb.ac.in
Server:  RTK_GW.true.true
Address: 192.168.1.1

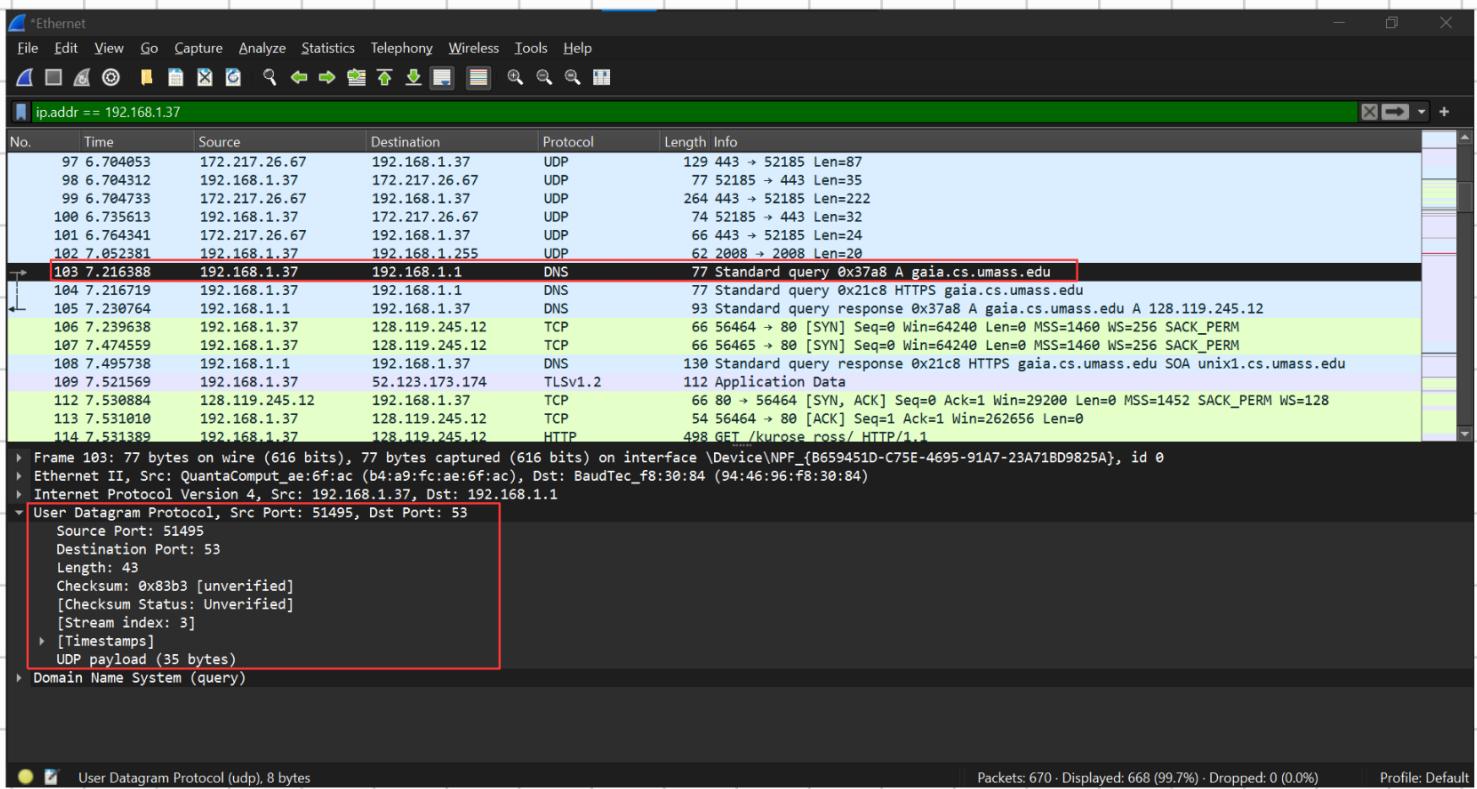
Non-authoritative answer:
Name:  dns1.iitb.ac.in
Address: 103.21.125.129

PS C:\Users\Ambatukam>
```

Authoritative name server ที่แสดงเป็นชื่อแรก คือ
dns1.iitb.ac.in

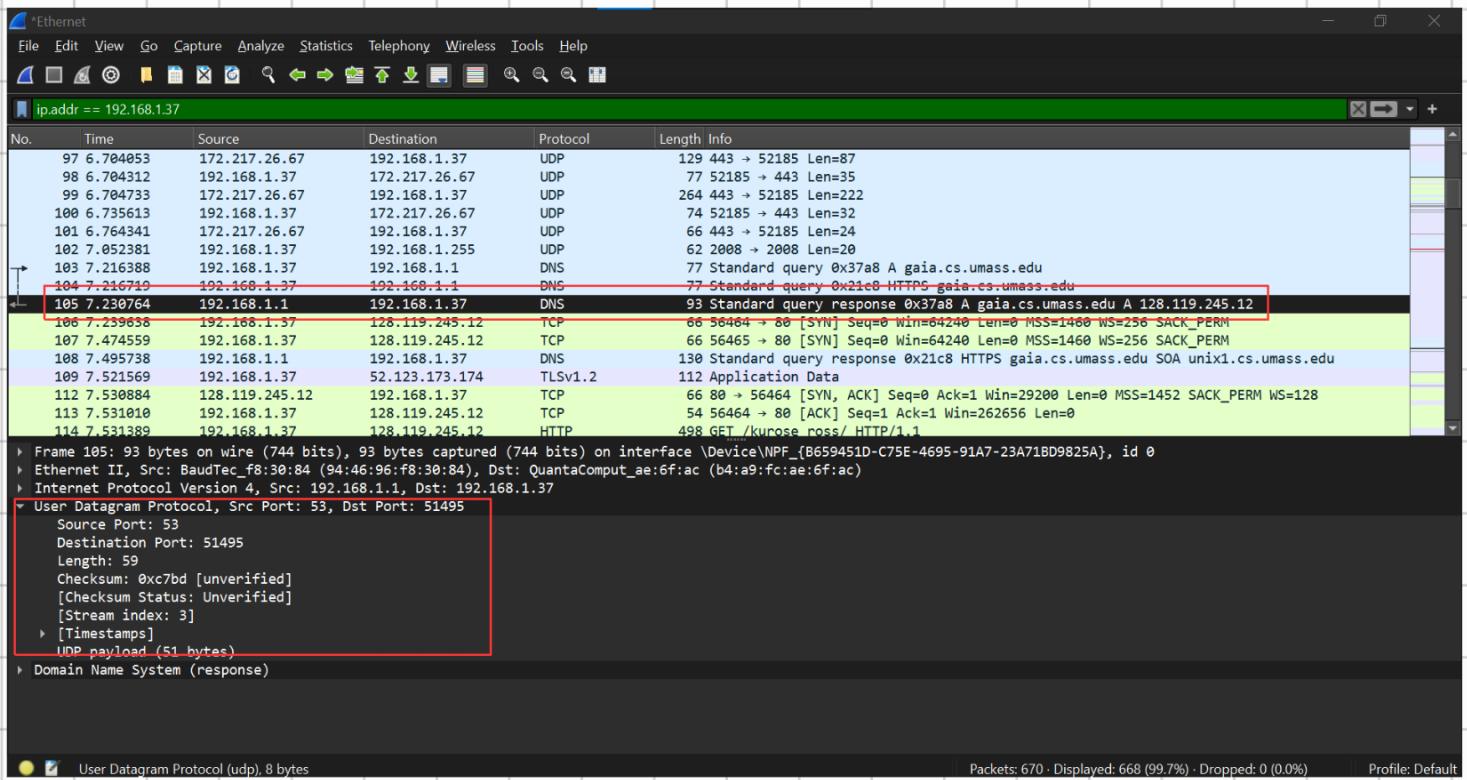
ใช้คำสั่ง nslookup ตามด้วย authoritative name server เช่น
nslookup dns1.iitb.ac.in

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?



ແພັກເກີດໜາຍເລີ່ມ 103
ສົ່ງນິ້ນ UDP

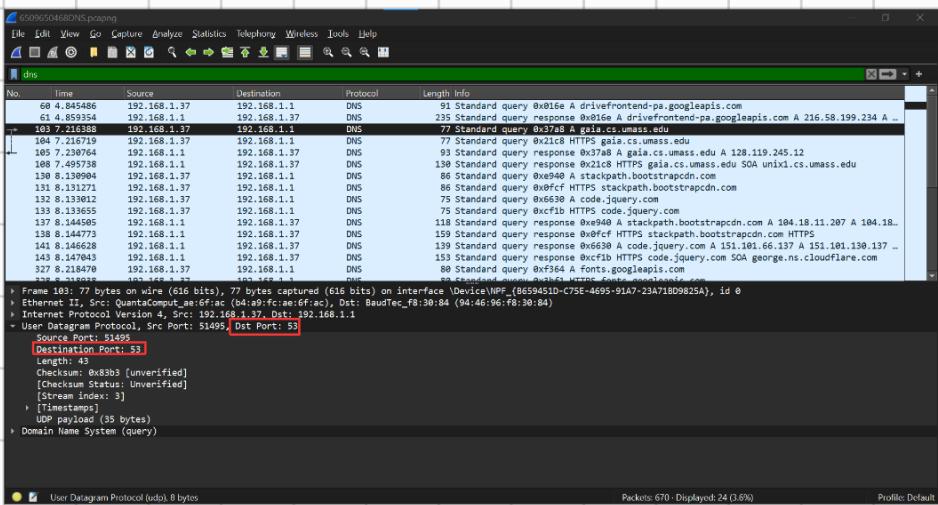
6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?



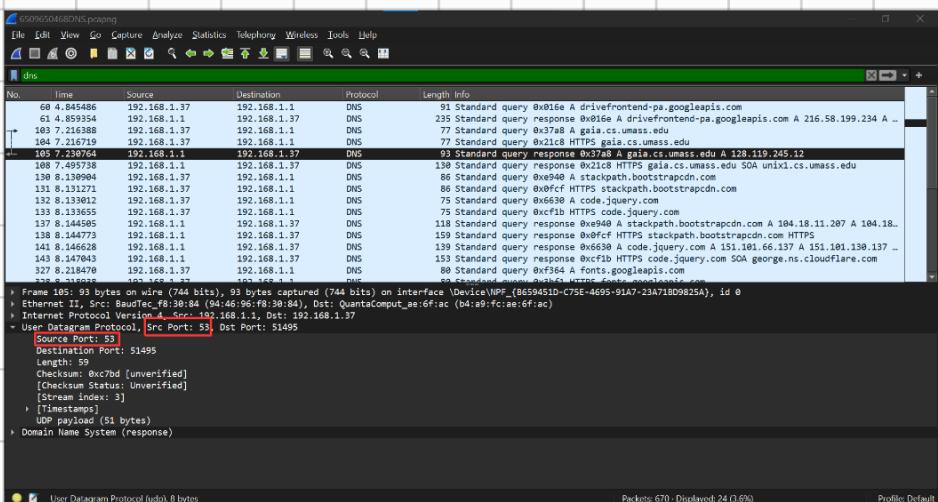
แพ็คเก็ตหมายเลข 105

ส่งบน UDP

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

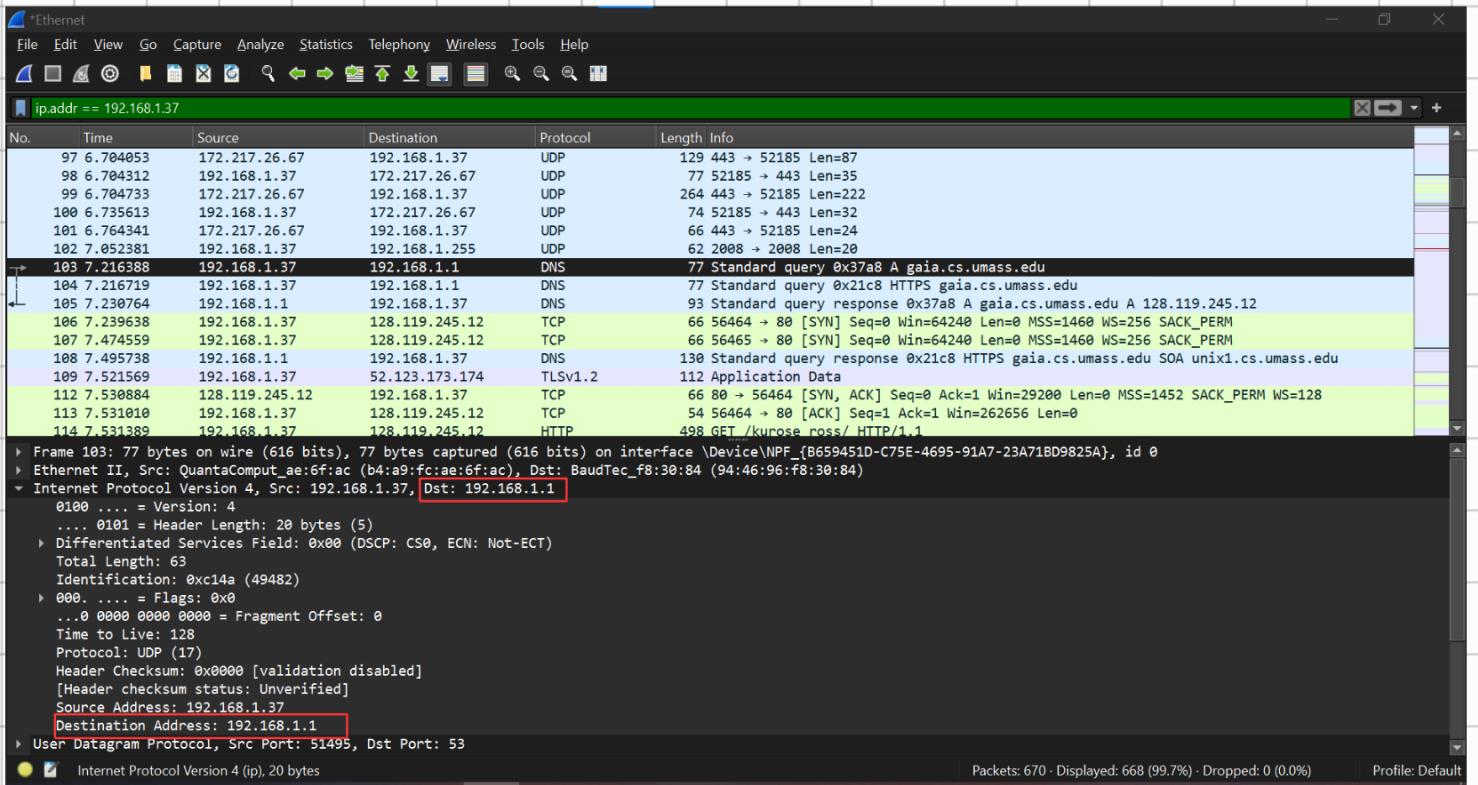


Destination
Port of DNS
query
message: 53



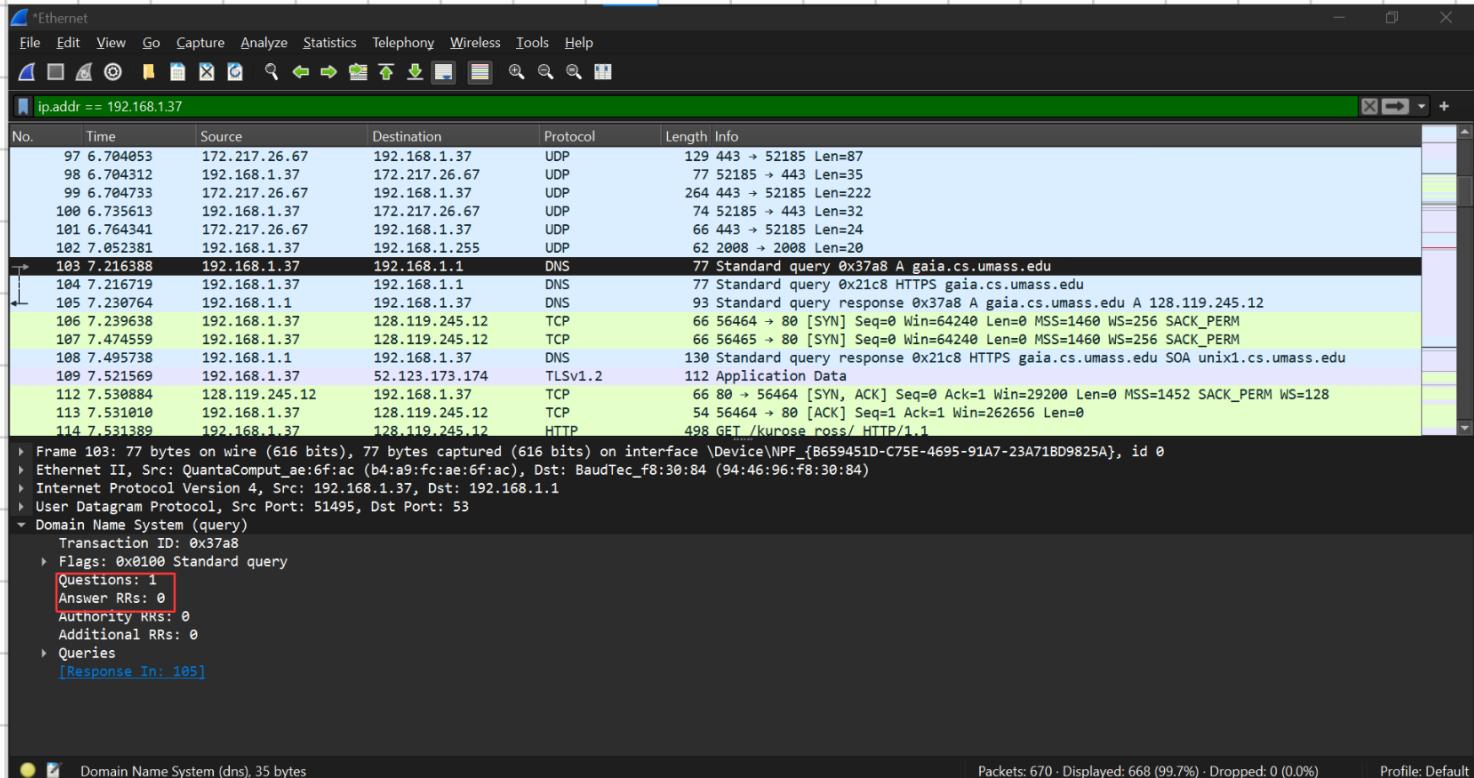
Source Port of
the DNS
response
message: 53

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



Destination Address: 192.168.1.1

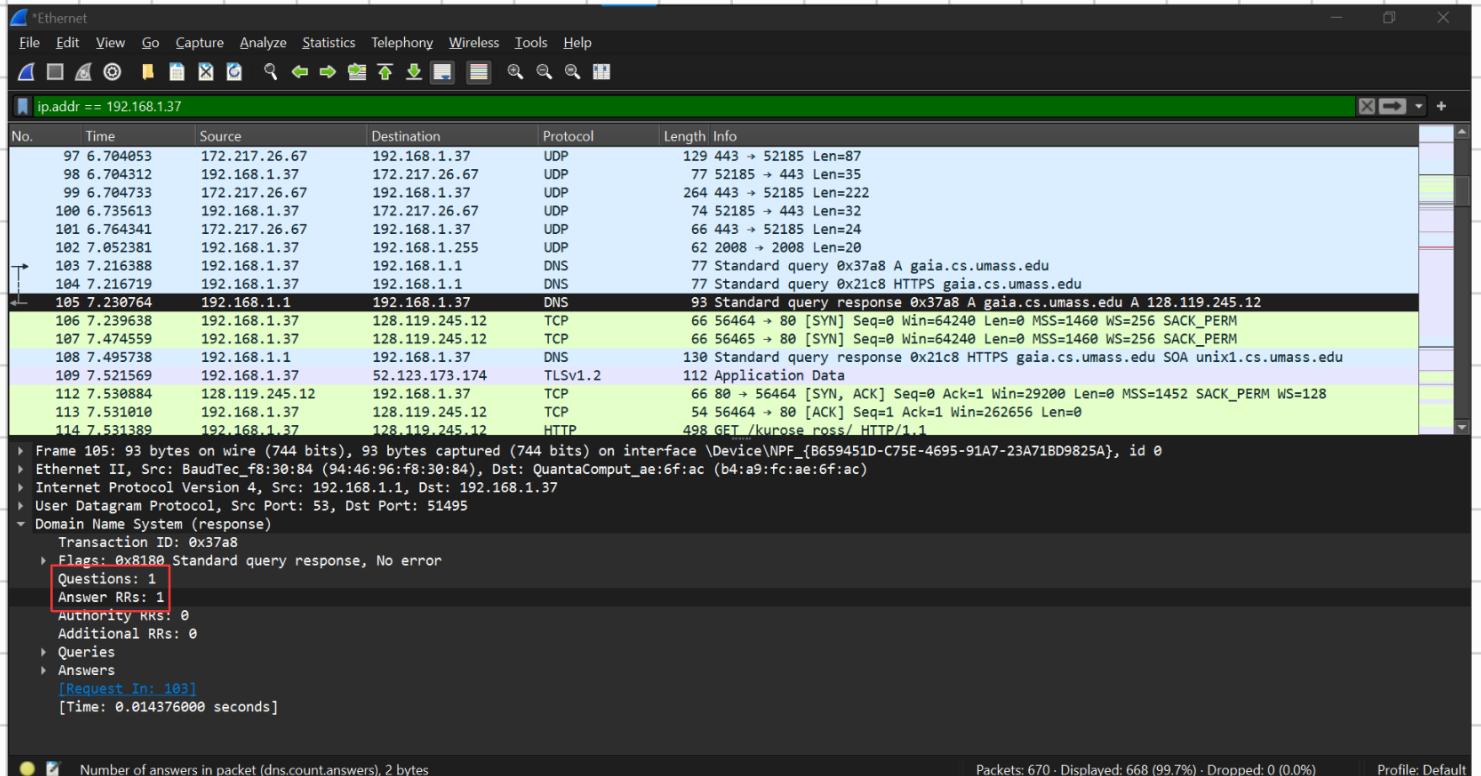
9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?



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. หมายเลขแพ็คเก็ตของ HTTP GET Request สำหรับ http://gaia.cs.umass.edu/kurose_ross/ คือ 114
2. หมายเลขแพ็คเก็ตใน DNS query ที่ HTTP Request เริ่มต้น ส่งไปยัง 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

Screenshot of Wireshark showing an HTTP session between 192.168.1.37 and 192.168.1.37. The session details pane shows the following:

```

> Frame 136: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface \Device\NPF_{B659451D-C75E-4695-91A7-23A71BD9825A}, id 0
> Ethernet II, Src: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac), Dst: BaudTec_f8:30:84 (94:46:96:f8:30:84)
> Internet Protocol Version 4, Src: 192.168.1.37, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56465, Dst Port: 80, Seq: 1, Ack: 1, Len: 348
> Hypertext Transfer Protocol
>   GET /kurose_ross/script.js HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36\r\n
  Accept: */*\r\n
  Referer: http://gaia.cs.umass.edu/kurose_ross/index.php\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
\r\n
  [Full request URI: http://gaia.cs.umass.edu/kurose_ross/script.js]
  [HTTP request 1/1]
  [Response in frame: 371]

```

The packet list shows several requests and responses. The first request (Frame 136) is highlighted with a red circle and labeled '1'. Subsequent responses (Frames 120, 121, 129, 134, 136, 370, 371, 376, 615, 617, 643) are also highlighted with red circles and labeled '2', '3', '4', and '5' respectively. The packet details pane shows the raw HTTP request and its response.

Screenshot of Wireshark showing a DNS session between 192.168.1.37 and 192.168.1.1. The session details pane shows the following:

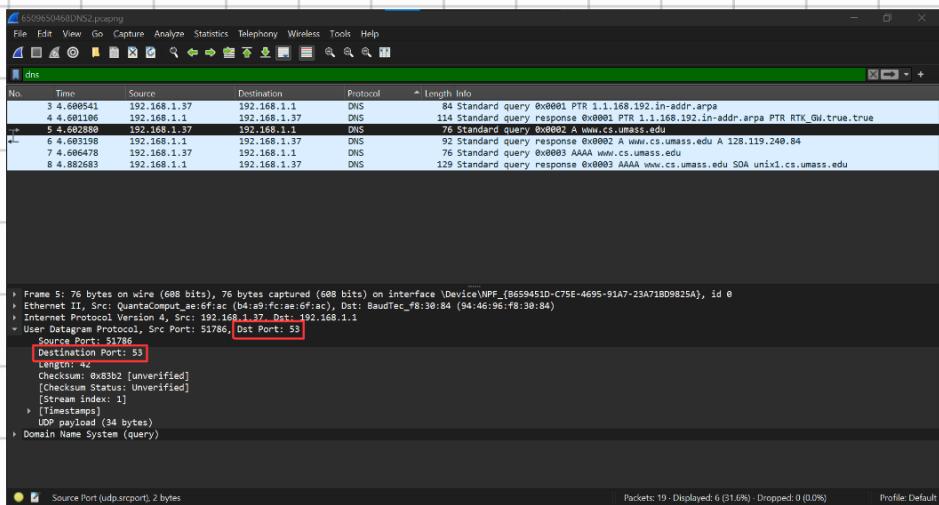
```

> Frame 330: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface \Device\NPF_{B659451D-C75E-4695-91A7-23A71BD9825A}, id 0
> Ethernet II, Src: BaudTec_f8:30:84 (94:46:96:f8:30:84), Dst: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.37
> User Datagram Protocol, Src Port: 53, Dst Port: 64780
> Domain Name System (response)
  Transaction ID: 0x3bf1
  > Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  > Queries
  > Authoritative nameservers
  [Request In: 328]
  [Time: 0.012772000 seconds]

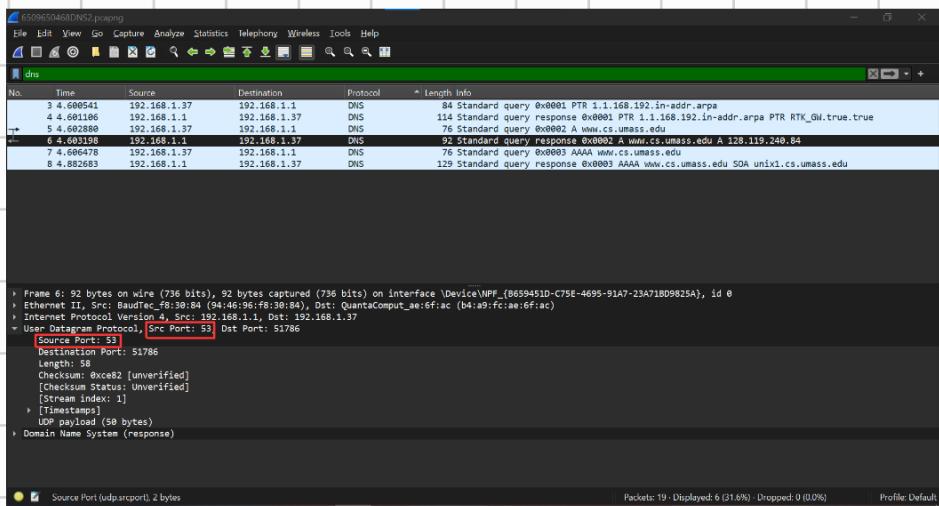
```

The packet list shows several DNS queries and responses. The first query (Frame 60) is highlighted with a red circle and labeled '1'. Subsequent responses (Frames 61, 183, 104, 185, 188, 130, 131, 132, 133, 137, 138, 141, 143, 327, 328) are highlighted with red circles and labeled '2', '3', '4', and '5' respectively. The packet details pane shows the raw DNS query and its response.

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

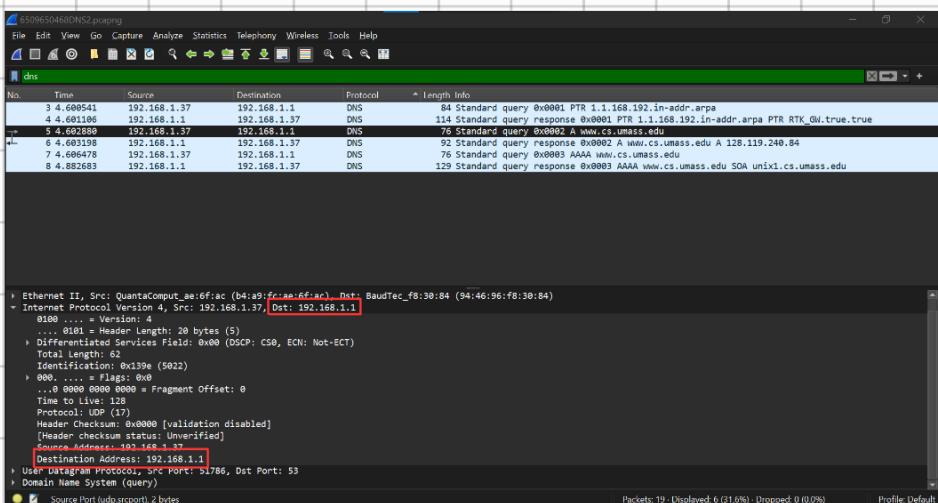


Destination Port
of DNS query
message: 53



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

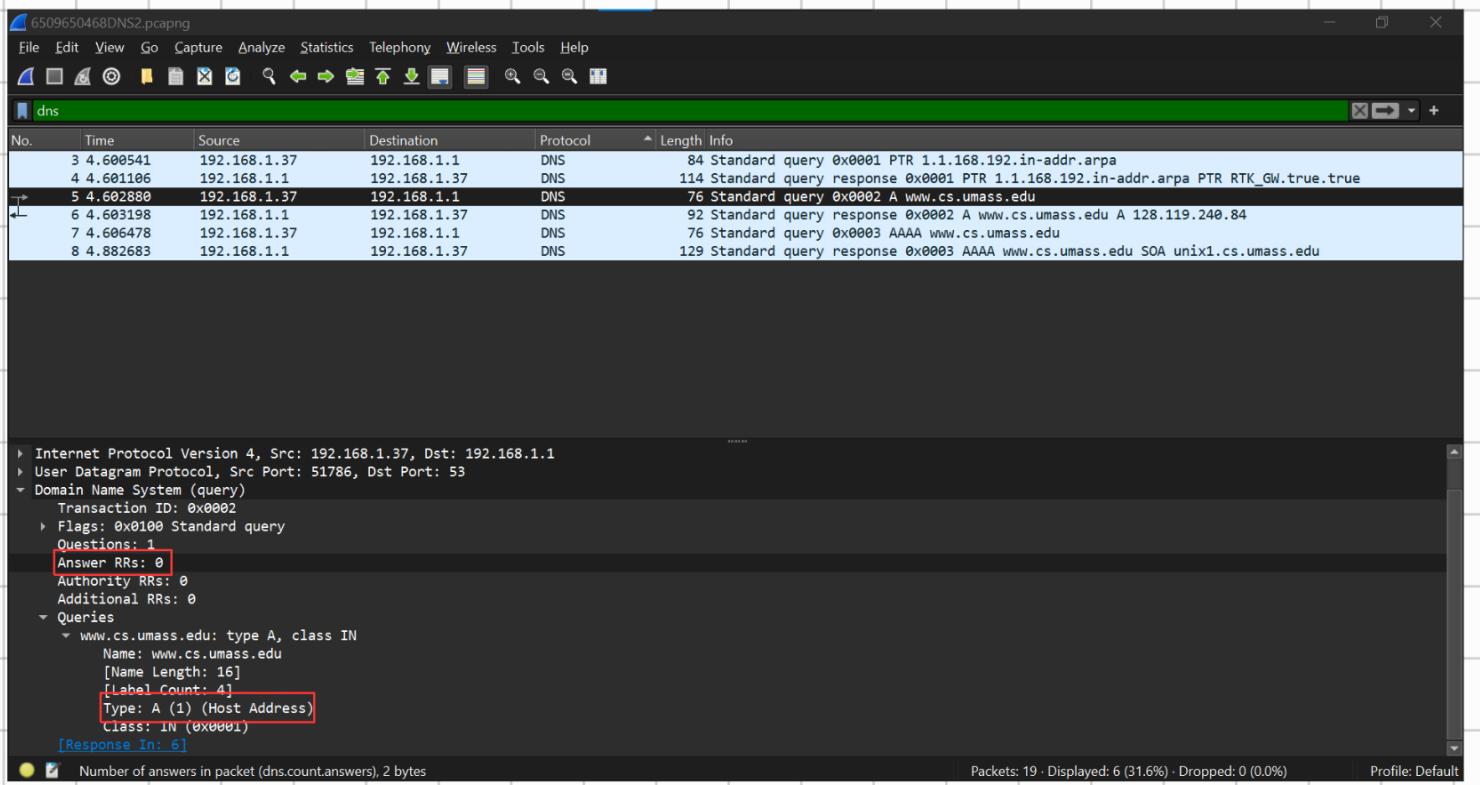
```
PS C:\Users\Ambatukam> nslookup www.cs.umass.edu
Server: RTK_GW.true.true
Address: 192.168.1.1

Non-authoritative answer:
Name: www.cs.umass.edu
Address: 128.119.240.84

PS C:\Users\Ambatukam> nslookup
Default Server: RTK_GW.true.true
Address: 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”?

The screenshot shows a Wireshark capture window titled "6509650468DNS2.pcapng". The packet list pane displays several DNS packets. The selected packet (row 6) is a DNS response from 192.168.1.1 to 192.168.1.37. The details pane shows the DNS header and payload. The payload includes a question section for "www.cs.umass.edu" and an answer section for the IP address 128.119.240.84. The bottom status bar indicates "Packets: 19 · Displayed: 6 (31.6%) · Dropped: 0 (0.0%) · Profile: Default".

No.	Time	Source	Destination	Protocol	Length	Info
3	4.600541	192.168.1.37	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
4	4.601186	192.168.1.1	192.168.1.37	DNS	114	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR RTK_GW.true.true
5	4.602880	192.168.1.37	192.168.1.1	DNS	76	Standard query 0x0002 A www.cs.umass.edu
6	4.603198	192.168.1.1	192.168.1.37	DNS	92	Standard query response 0x0002 A www.cs.umass.edu A 128.119.240.84
7	4.606478	192.168.1.37	192.168.1.1	DNS	76	Standard query 0x0003 AAAA www.cs.umass.edu
8	4.882683	192.168.1.1	192.168.1.37	DNS	129	Standard query response 0x0003 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.37
User Datagram Protocol, Src Port: 53, Dst Port: 51786
Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
www.cs.umass.edu: type A, class IN
Name: www.cs.umass.edu
[Name Length: 16]
[Label Count: 4]
Type: A (1) (Host Address)
Class: IN (0x0001)

Number of answers in packet (dns.count.answers), 2 bytes

Questions: 1

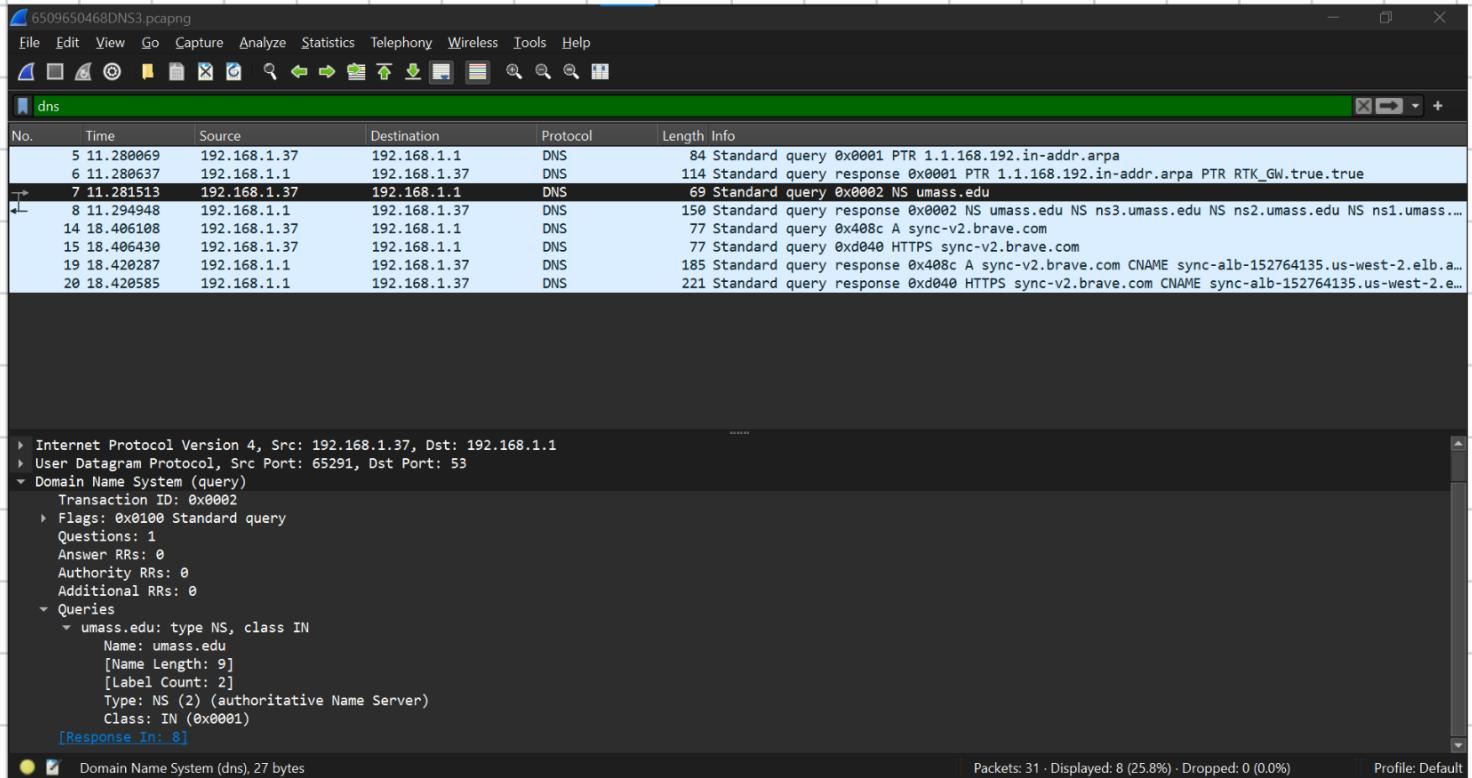
Answer RRs: 1

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 ส่งไปคือ 192.168.1.1

ตรงกับ IP address default local DNS server ของนักศึกษา

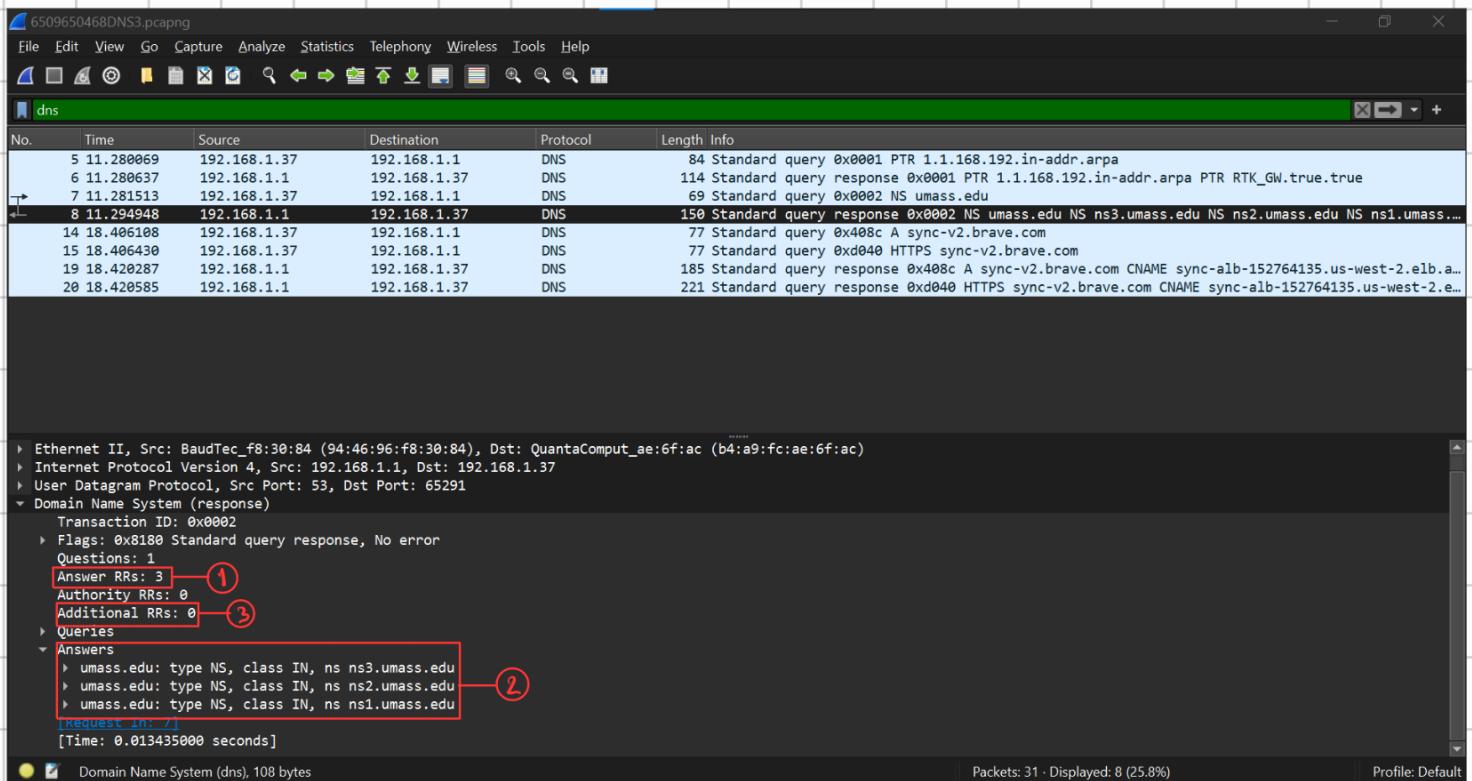
17. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?



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

