1. nslookup

Yogesh P
201EE138

Command Prompt

```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Yogesh>nslookup -type=NS iitb.ac.in
Server:  UnKnown
Address:  192.168.94.31

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

dns1.iitb.ac.in internet address = 103.21.125.129
dns2.iitb.ac.in internet address = 103.21.126.129
dns3.iitb.ac.in internet address = 103.21.127.129

C:\Users\Yogesh>nslookup dns3.iitb.ac.in
Server:  UnKnown
Address:  192.168.94.31

Non-authoritative answer:
Name:    dns3.iitb.ac.in
Addresses:  64:ff9b::6715:7f81
          103.21.127.129
```

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

A: 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?

A: Server: lexus.nitk.ac.in

Address: 10.9.0.10

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

A: Non- Authoritative

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?

A: Did not receive any authoritative server name, if I had to find ip address of a server id use command like nslookup dns3.iitb.ac.in

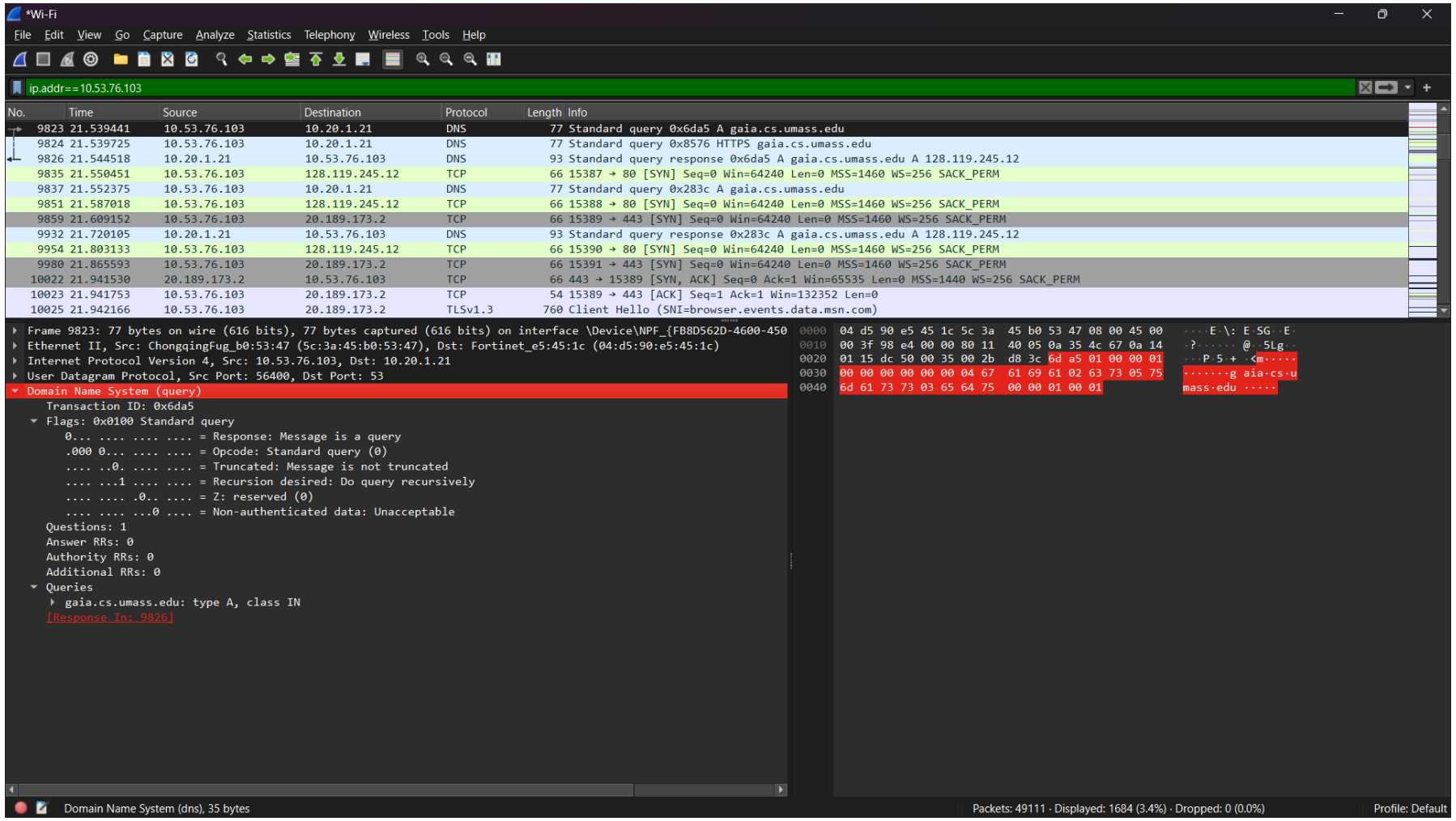
2. The DNS cache on your computer

Command Prompt

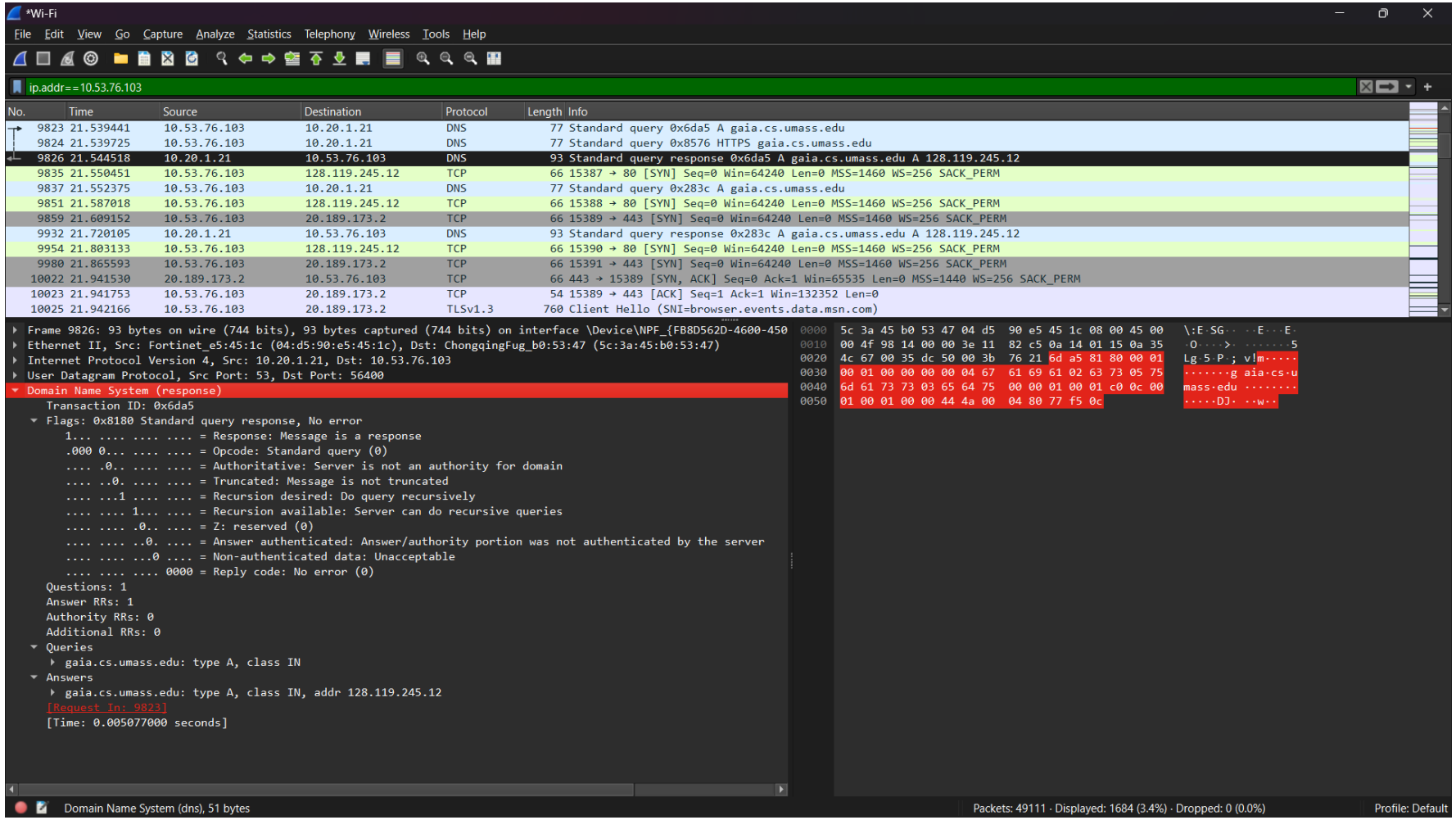
```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Yogesh>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Yogesh>
```

3. Tracing DNS with Wireshark

Standard query



Standard response



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?

A: 9823, 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?

A: 9826, UDP

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

A: 53, 53

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

A: 10.20.1.21

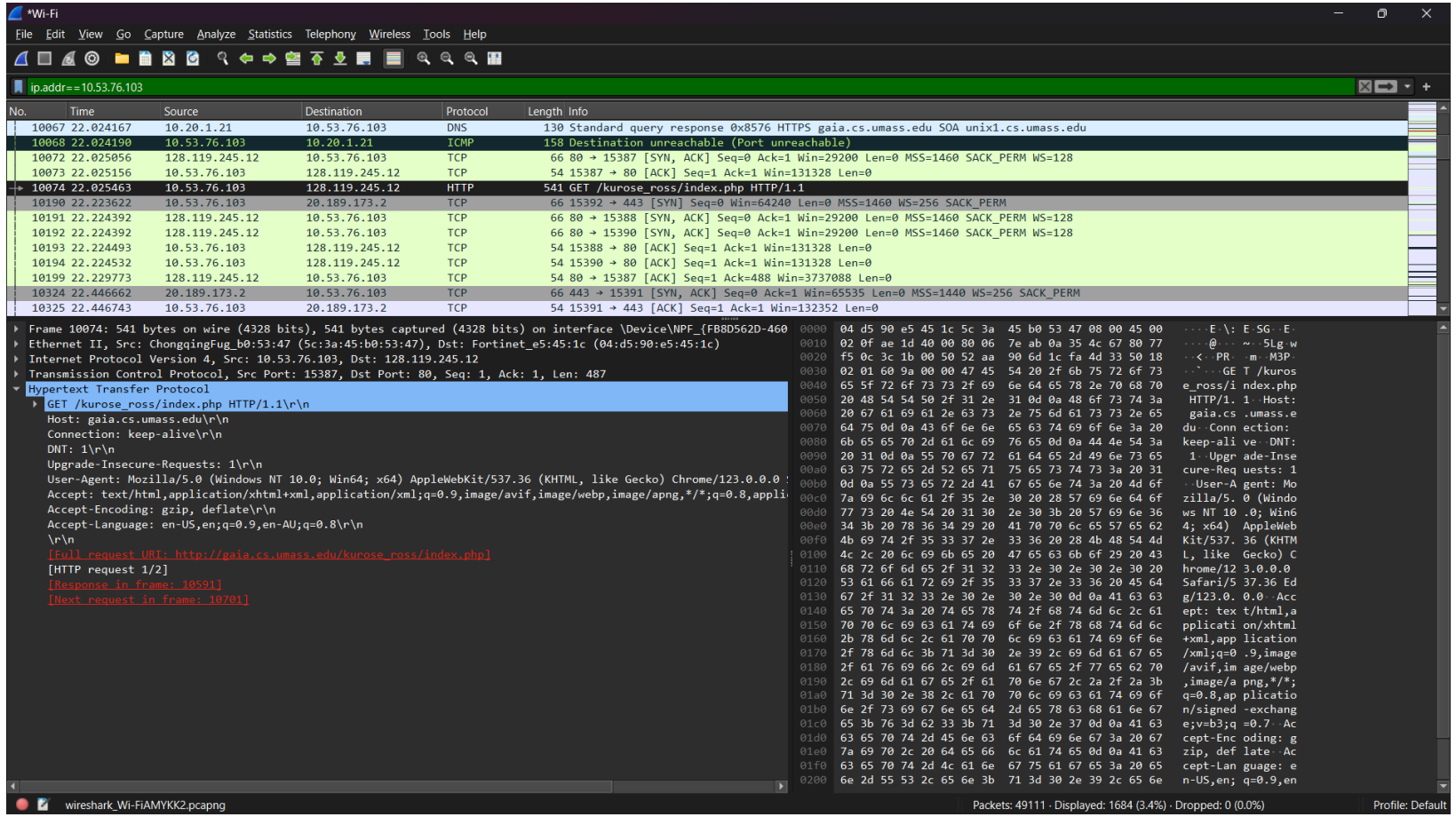
9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

A: 1, 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?

A: 1,1

initial HTTP GET request



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/?

A:

- 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?

A: 10074

- What is the packet number in the trace of the received DNS response?

A: 9932

- 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?

A: 10074

- 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?

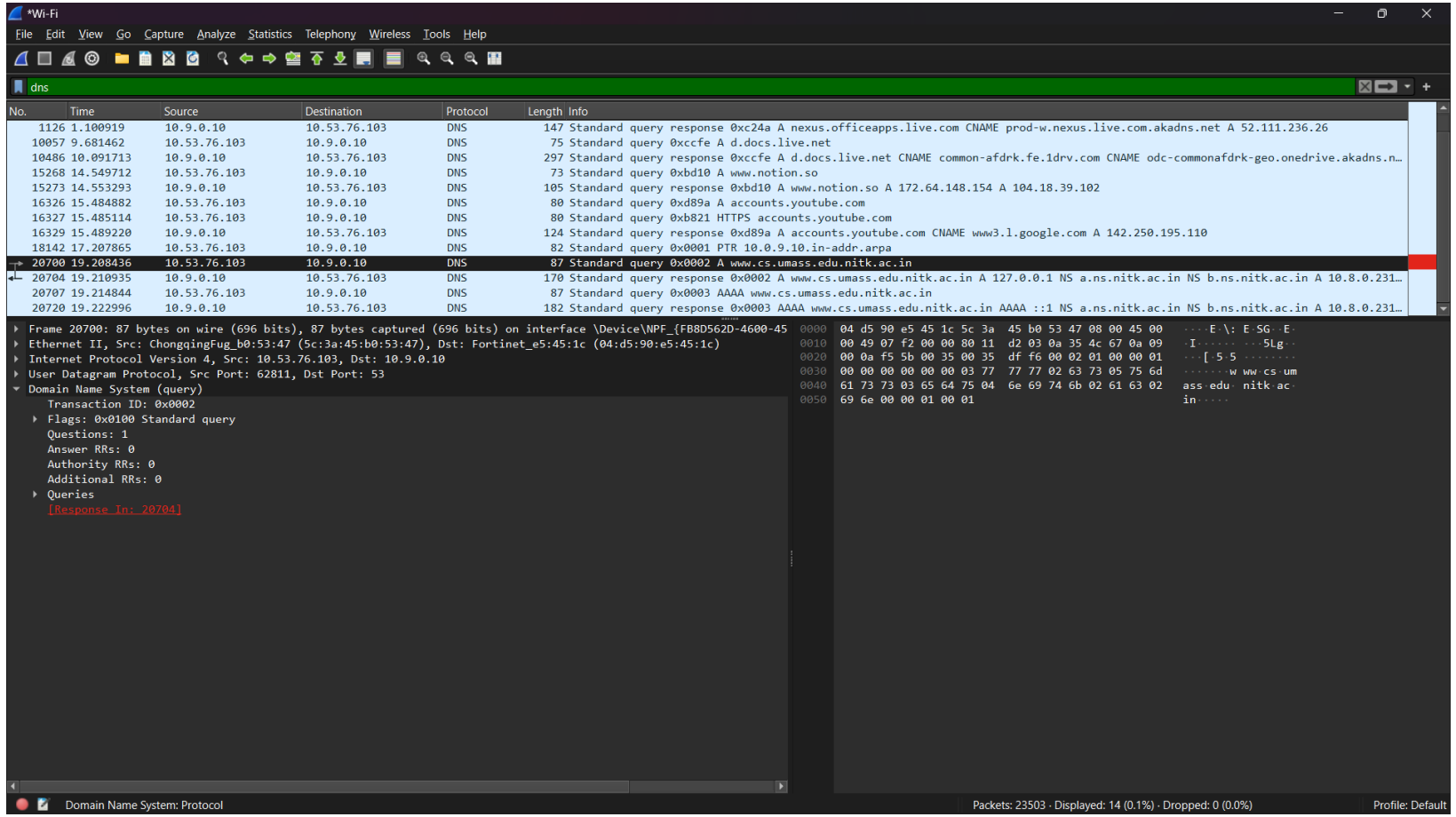
A: 9823

- Discuss how DNS caching affects the answer to this last question.

A: DNS caching reduces the need for repeated DNS queries by storing previously resolved domain names and their corresponding IP addresses, but when cached records expire or are absent, new DNS queries must be made to resolve domain names.

Now let’s play with nslookup7 .

● Start packet capture. ● Do an nslookup on www.cs.umass.edu ● Stop packet capture.



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

A: 53,53

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

A: 10.9.0.10, yes

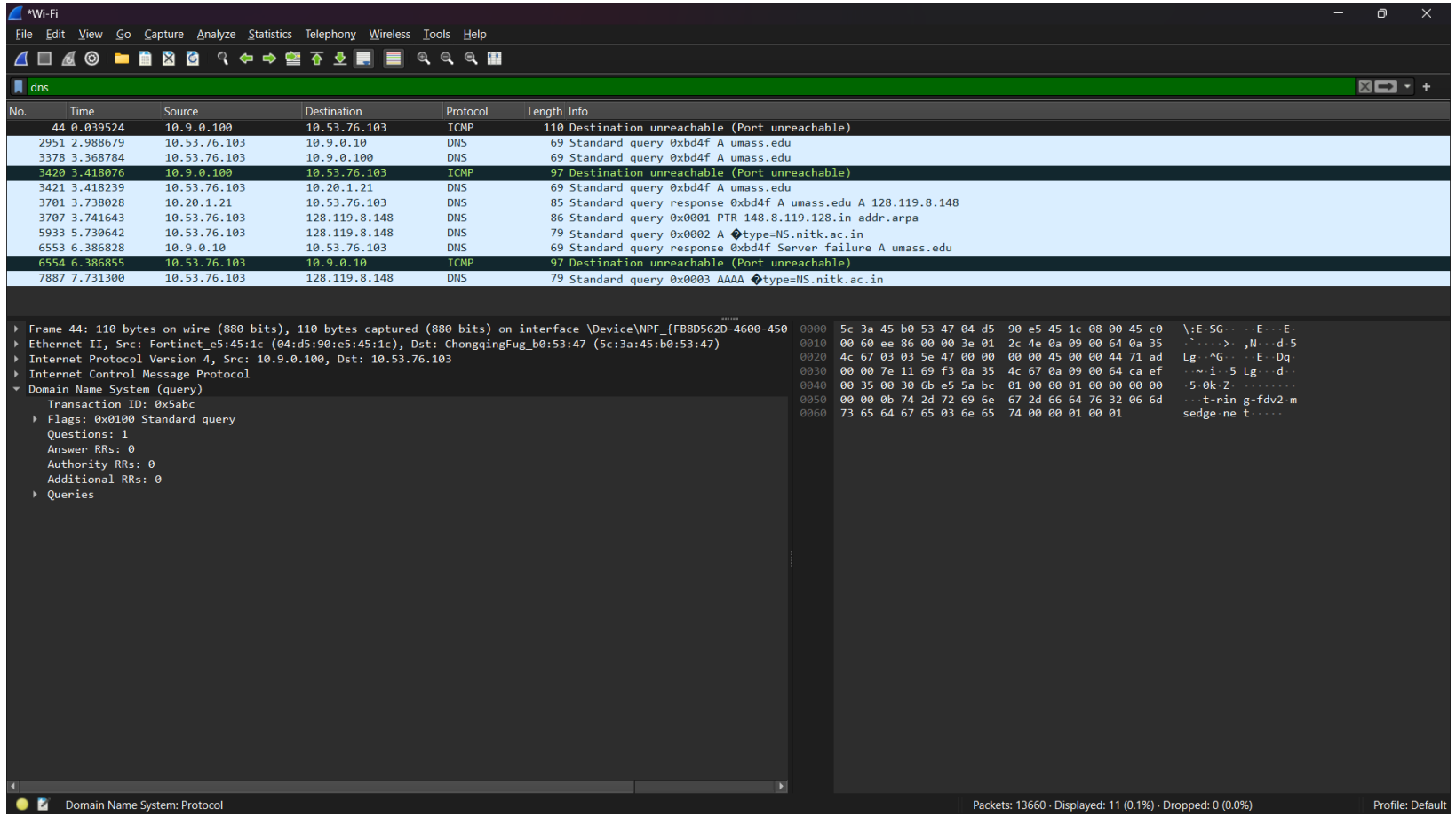
14. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A: Type: A, no

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

A: 1 Question, Answer RRs: 1

Last, let’s use nslookup to issue a command that will return a type NS DNS record, Enter the following command: nslookup –type=NS umass.edu



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

A: 10.20.1.21, no

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

A: 1, no answers

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?

A: 1 answer in one response

umass.edu: type A, class IN, addr 128.119.8.148

umass.edu: type AAAA, class IN, addr 64:ff9b::8077:894

Additional RRs: 0