Catalina Cisneros

**Lab: Wireshark DNS v9.0**

**1. nslookup**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Questions**

1. Run nslookup to obtain the IP address of the web server for the IndianInstitute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of [www.iitb.ac.in](http://www.iitb.ac.in)

🡪 The IP Address is 103.21.124.133

A black and white rectangular sign with white text

AI-generated content may be incorrect.

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

🡪 The IP Address from the DNS server is 2001:558:feed::1



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

🡪 Non authoritative server

A close-up of a black and white logo

AI-generated content may be incorrect.

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 servers: dns2.iitb.ac.in, dns3.iitb.ac.in, dns1.iitb.ac.in   
🡪 First one listed: dns2.iitb.ac.in

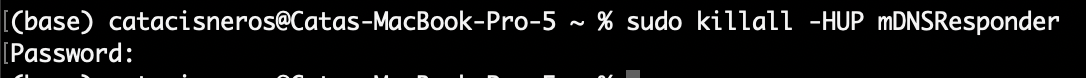
A computer screen with white text

AI-generated content may be incorrect.  
🡪 To find its IP: nslookup dns2.iitb.ac.in

A black screen with white text

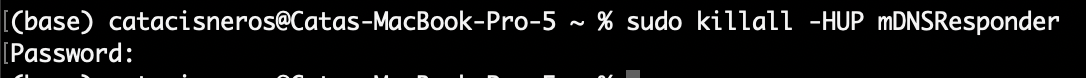
AI-generated content may be incorrect.

1. **The DNS Cache on your computer**



1. **Tracing DNS with wireshark**

* Clear the DNS cache in the host



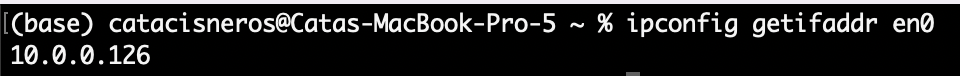
* Open browser and clear cache

A screenshot of a browser window

AI-generated content may be incorrect.

* Open wireshark and enter my IP address

🡪 My IP Address: 10.0.0.126



🡪 Enter it in Wireshark

A screenshot of a computer

AI-generated content may be incorrect.

* Start packet capture

A screenshot of a computer

AI-generated content may be incorrect.

* Visit <http://gaia.cs.umass.edu/kurose_ross/>

A screenshot of a computer

AI-generated content may be incorrect.

* Stop packet capture

A screenshot of a computer

AI-generated content may be incorrect.

**Questions**

5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number6 in the trace for the DNS query message? Is this query message sent over UDP or TCP?

🡪 The first DNS query that resolved gaia.cs.umass.edu was packet 1605, using the UDP protocol.

A screenshot of a computer

AI-generated content may be incorrect.

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?

🡪 The matching DNS response appeared in packet 1615, using UDP

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The DNS query was sent to destination port 53, and the response came from source port 53.

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The destination IP address of the DNS query was 2001:558:feed::1, which is the DNS resolver.

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The DNS query contained 1 question and 0 answers.

A screenshot of a computer

AI-generated content may be incorrect.

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?

🡪 The DNS response contained 1 question and 0 answers, with 1 authority record indicating a referral instead of a direct IP.

A screenshot of a computer error

AI-generated content may be incorrect.

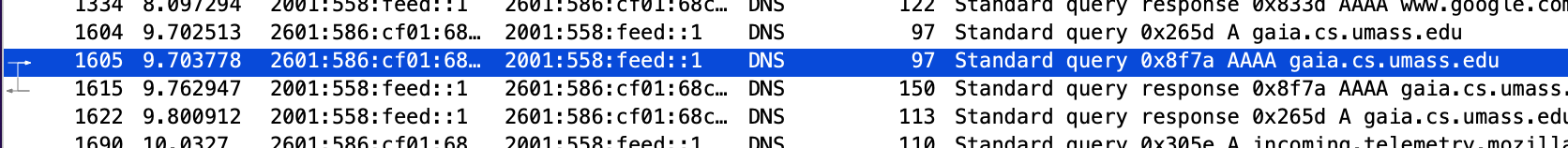
11. The web page for the base file http://gaia.cs.umass.edu/kurose\_ross/ references the image object http://gaia.cs.umass.edu/kurose\_ross/header\_graphic\_book\_8E\_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request 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.

🡪 The initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose\_ross/ occurred in packet 1637.

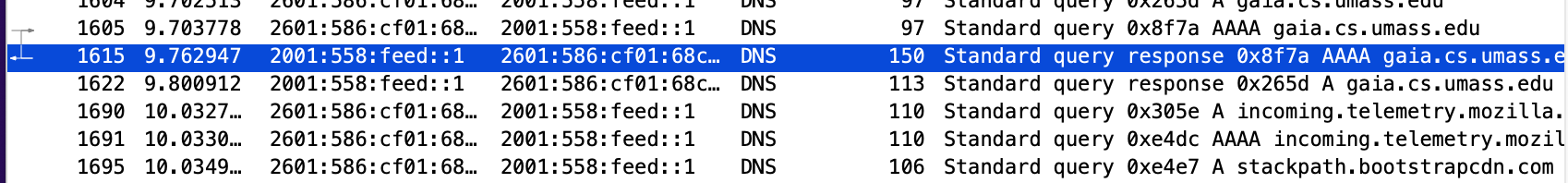
A screenshot of a computer

AI-generated content may be incorrect.

🡪The DNS query that resolved gaia.cs.umass.edu so the GET could be sent was packet 1605.



🡪 The DNS response providing the server address was packet 1615.



🡪 The HTTP GET request for the image header\_graphic\_book\_9E\_1.jpg was packet 1920.

A screenshot of a computer

AI-generated content may be incorrect.

🡪 No new DNS query was made before this second GET; the browser reused the cached DNS result from the earlier lookup since the hostname was already resolved and still valid.

* Start packet capture

A screenshot of a computer

AI-generated content may be incorrect.

* Do an nslookup on [www.cs.umass.edu](http://www.cs.umass.edu)

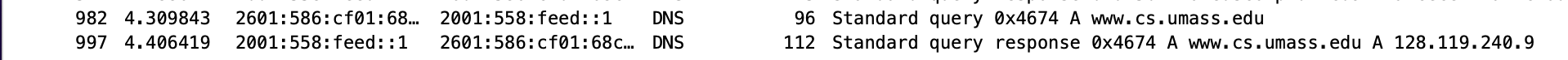
A computer screen with white text

AI-generated content may be incorrect.

* Stop capture

A screenshot of a computer

AI-generated content may be incorrect.

* Results

**Questions**

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

🡪 The DNS query used destination port 53 (standard DNS port)

A screenshot of a computer

AI-generated content may be incorrect.

🡪 The DNS response came from source port 53.

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The DNS query was sent to 2001:558:feed::1, which is the same IP address of my default local DNS server

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The DNS query type is A (host address) — requesting the IPv4 address of www.cs.umass.edu.

🡪 The query message contained 1 question and 0 answers.

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The DNS response message contained 1 question and 1 answer, returning the IP address 128.119.240.9 for www.cs.umass.edu.

A screenshot of a computer

AI-generated content may be incorrect.

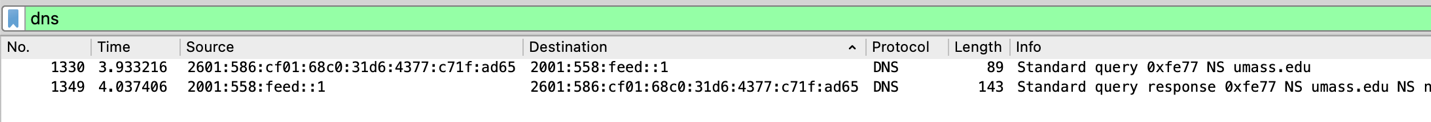
Last, let’s use nslookup to issue a command that will return a type NS DNS record, Enter the following command: nslookup –type=NS umass.edu and then answer the following questions:

A computer screen with white text

AI-generated content may be incorrect.

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

🡪The DNS query was sent to 2001:558:feed::1, which is the default local DNS server



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

🡪 The query message contains 1 question and 0 answers. It requests an NS (name server) record for umass.edu.

A screenshot of a computer

AI-generated content may be incorrect.

18. Examine the DNS response message (in particular the DNS response message that has type “NS”). 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 (if additional information is returned)?

🡪The DNS response contains 1 question and 3 answers.

🡪 The answers list the authoritative name servers for umass.edu:

* ns3.umass.edu
* ns1.umass.edu
* ns2.umass.edu.

🡪There are no additional resource records in this response.

A screenshot of a computer

AI-generated content may be incorrect.