

# 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: lexis.nitk.ac.in

Address: 10.9.0.10

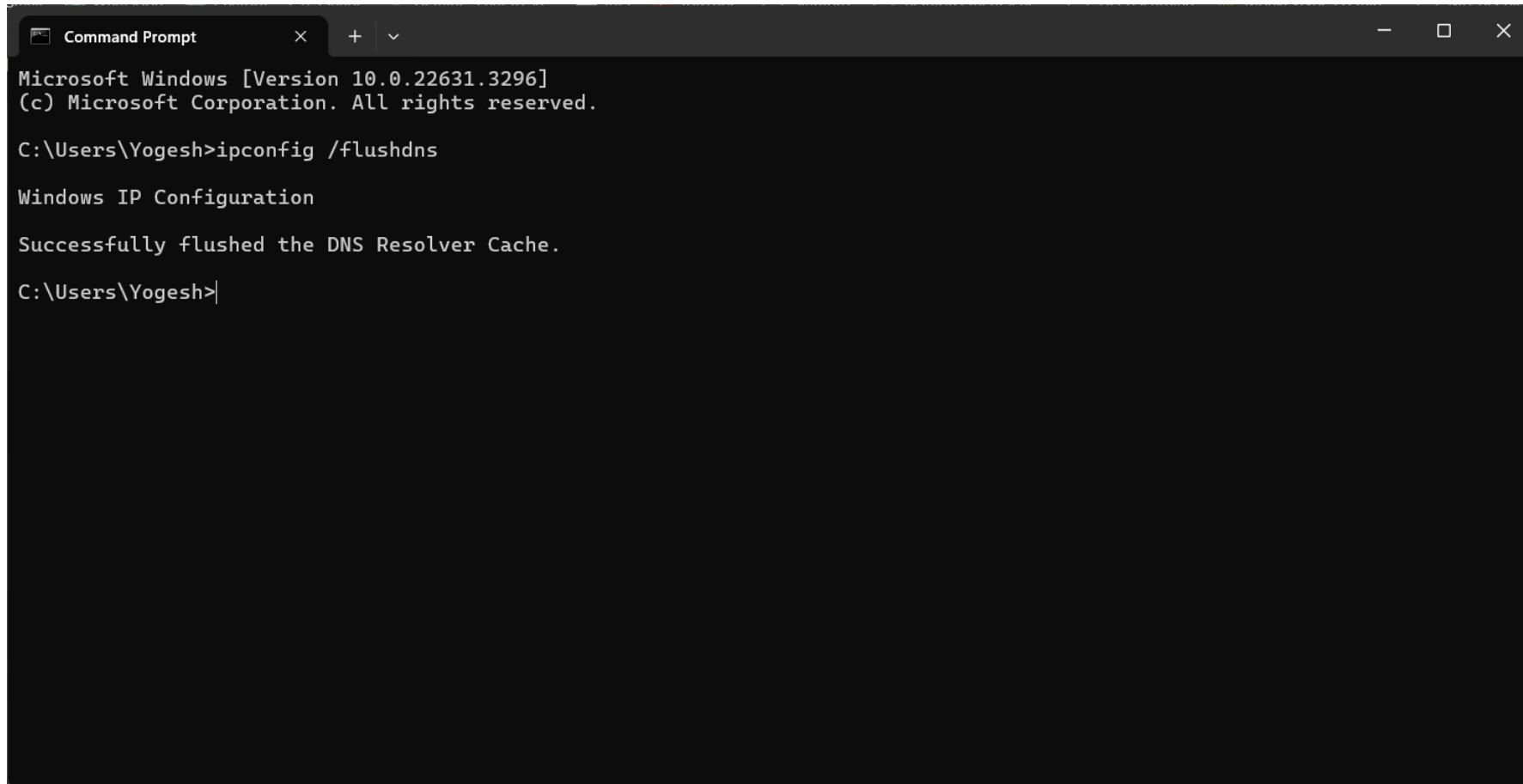
3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

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

The image shows a Wireshark packet capture window titled "\*Wi-Fi". The filter bar at the top is set to "ip.addr==10.53.76.103". The packet list on the left shows several packets, with packet 9823 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS Standard query (transaction ID 0x6da5) for "gaia.cs.umass.edu". The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9823	21.539441	10.53.76.103	10.20.1.21	DNS	77	Standard query 0x6da5 A gaia.cs.umass.edu
9824	21.539725	10.53.76.103	10.20.1.21	DNS	77	Standard query 0x8576 HTTPS gaia.cs.umass.edu
9826	21.544518	10.20.1.21	10.53.76.103	DNS	93	Standard query response 0x6da5 A gaia.cs.umass.edu A 128.119.245.12
9835	21.550451	10.53.76.103	128.119.245.12	TCP	66	15387 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9837	21.552375	10.53.76.103	10.20.1.21	DNS	77	Standard query 0x283c A gaia.cs.umass.edu
9851	21.587018	10.53.76.103	128.119.245.12	TCP	66	15388 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9859	21.609152	10.53.76.103	20.189.173.2	TCP	66	15389 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9932	21.720105	10.20.1.21	10.53.76.103	DNS	93	Standard query response 0x283c A gaia.cs.umass.edu A 128.119.245.12
9954	21.803133	10.53.76.103	128.119.245.12	TCP	66	15390 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9980	21.865593	10.53.76.103	20.189.173.2	TCP	66	15391 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10022	21.941530	20.189.173.2	10.53.76.103	TCP	66	443 → 15389 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
10023	21.941753	10.53.76.103	20.189.173.2	TCP	54	15389 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
10025	21.942166	10.53.76.103	20.189.173.2	TLSv1.3	760	Client Hello (SNI=browser.events.data.msn.com)

Frame 9823: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF\_{FB8D562D-4600-450... Ethernet II, Src: ChongqingFug\_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet\_e5:45:1c (04:d5:90:e5:45:1c) Internet Protocol Version 4, Src: 10.53.76.103, Dst: 10.20.1.21 User Datagram Protocol, Src Port: 56400, Dst Port: 53

**Domain Name System (query)**

Transaction ID: 0x6da5

Flags: 0x0100 Standard query

- 0... .. = Response: Message is a query
- .000 0... .. = Opcode: Standard query (0)
- .... ..0. .... = Truncated: Message is not truncated
- .... ..1 .... = Recursion desired: Do query recursively
- .... ..0.. .... = Z: reserved (0)
- .... ..0 .... = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

**Queries**

- gaia.cs.umass.edu: type A, class IN

[Response In: 9826]

Domain Name System (dns), 35 bytes

Packets: 49111 · Displayed: 1684 (3.4%) · Dropped: 0 (0.0%) Profile: Default

# Standard response

The image shows a Wireshark packet capture window titled "\*Wi-Fi". The filter bar at the top is set to "ip.addr==10.53.76.103". The packet list on the left shows several packets, with packet 9826 selected. The packet details pane on the right shows the structure of the selected packet, which is a Domain Name System (DNS) standard query response. The packet is 93 bytes on wire (744 bits) and 93 bytes captured (744 bits) on interface \\Device\\NPF\_{FB8D562D-4600-4500-0000-5c3a45b05347}. The packet is an Ethernet II frame from Fortinet\_e5:45:1c (04:d5:90:e5:45:1c) to ChongqingFug\_b0:53:47 (5c:3a:45:b0:53:47). The Internet Protocol Version 4 header shows the source as 10.20.1.21 and the destination as 10.53.76.103. The User Datagram Protocol header shows the source port as 53 and the destination port as 56400. The Domain Name System (response) section shows the transaction ID as 0x6da5, flags as 0x8180 (Standard query response, No error), and the response message. The response message includes the following fields: Opcode: Standard query (0), Authoritative: Server is not an authority for domain, Truncated: Message is not truncated, Recursion desired: Do query recursively, Recursion available: Server can do recursive queries, Z: reserved (0), Answer authenticated: Answer/authority portion was not authenticated by the server, Non-authenticated data: Unacceptable, and Reply code: No error (0). The response also includes one question and one answer. The question is for gaia.cs.umass.edu: type A, class IN. The answer is for gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12. The packet is 51 bytes long and is a Domain Name System (dns) packet.

No.	Time	Source	Destination	Protocol	Length	Info
9823	21.539441	10.53.76.103	10.20.1.21	DNS	77	Standard query 0x6da5 A gaia.cs.umass.edu
9824	21.539725	10.53.76.103	10.20.1.21	DNS	77	Standard query 0x8576 HTTPS gaia.cs.umass.edu
9826	21.544518	10.20.1.21	10.53.76.103	DNS	93	Standard query response 0x6da5 A gaia.cs.umass.edu A 128.119.245.12
9835	21.550451	10.53.76.103	128.119.245.12	TCP	66	15387 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9837	21.552375	10.53.76.103	10.20.1.21	DNS	77	Standard query 0x283c A gaia.cs.umass.edu
9851	21.587018	10.53.76.103	128.119.245.12	TCP	66	15388 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9859	21.609152	10.53.76.103	20.189.173.2	TCP	66	15389 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9932	21.720105	10.20.1.21	10.53.76.103	DNS	93	Standard query response 0x283c A gaia.cs.umass.edu A 128.119.245.12
9954	21.803133	10.53.76.103	128.119.245.12	TCP	66	15390 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9980	21.865593	10.53.76.103	20.189.173.2	TCP	66	15391 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10022	21.941530	20.189.173.2	10.53.76.103	TCP	66	443 → 15389 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
10023	21.941753	10.53.76.103	20.189.173.2	TCP	54	15389 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
10025	21.942166	10.53.76.103	20.189.173.2	TLSv1.3	760	Client Hello (SNI=browser.events.data.msn.com)

Frame 9826: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \\Device\\NPF\_{FB8D562D-4600-4500-0000-5c3a45b05347}

Ethernet II, Src: Fortinet\_e5:45:1c (04:d5:90:e5:45:1c), Dst: ChongqingFug\_b0:53:47 (5c:3a:45:b0:53:47)

Internet Protocol Version 4, Src: 10.20.1.21, Dst: 10.53.76.103

User Datagram Protocol, Src Port: 53, Dst Port: 56400

Domain Name System (response)

Transaction ID: 0x6da5

Flags: 0x8180 Standard query response, No error

1... .. = Response: Message is a response

.000 0... .. = Opcode: Standard query (0)

... .. = Authoritative: Server is not an authority for domain

... .. = Truncated: Message is not truncated

... .. = Recursion desired: Do query recursively

... .. 1... .. = Recursion available: Server can do recursive queries

... .. 0... .. = Z: reserved (0)

... .. 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server

... .. 0... .. = Non-authenticated data: Unacceptable

... .. 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

gaia.cs.umass.edu: type A, class IN

Answers

gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12

[Request In: 9823]

[Time: 0.005077000 seconds]

Domain Name System (dns), 51 bytes

Packets: 49111 · Displayed: 1684 (3.4%) · Dropped: 0 (0.0%)

Profile: Default



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

The image displays a Wireshark packet capture window titled "\*Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A filter bar at the top shows "ip.addr==10.53.76.103". The packet list pane shows several packets, with packet 10074 selected, which is an HTTP GET request. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet.

ip.addr==10.53.76.103

No.	Time	Source	Destination	Protocol	Length	Info
10067	22.024167	10.20.1.21	10.53.76.103	DNS	130	Standard query response 0x8576 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu
10068	22.024190	10.53.76.103	10.20.1.21	ICMP	158	Destination unreachable (Port unreachable)
10072	22.025056	128.119.245.12	10.53.76.103	TCP	66	80 → 15387 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
10073	22.025156	10.53.76.103	128.119.245.12	TCP	54	15387 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
10074	22.025463	10.53.76.103	128.119.245.12	HTTP	541	GET /kurose_ross/index.php HTTP/1.1
10190	22.223622	10.53.76.103	20.189.173.2	TCP	66	15392 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10191	22.224392	128.119.245.12	10.53.76.103	TCP	66	80 → 15388 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
10192	22.224392	128.119.245.12	10.53.76.103	TCP	66	80 → 15390 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
10193	22.224493	10.53.76.103	128.119.245.12	TCP	54	15388 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
10194	22.224532	10.53.76.103	128.119.245.12	TCP	54	15390 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
10199	22.229773	128.119.245.12	10.53.76.103	TCP	54	80 → 15387 [ACK] Seq=1 Ack=488 Win=3737088 Len=0
10324	22.446662	20.189.173.2	10.53.76.103	TCP	66	443 → 15391 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
10325	22.446743	10.53.76.103	20.189.173.2	TCP	54	15391 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0

Frame 10074: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF\_{FB8D562D-460-0000-0000-000000000000} on 0  
Ethernet II, Src: ChongqingFug\_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet\_e5:45:1c (04:d5:90:e5:45:1c)  
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 15387, Dst Port: 80, Seq: 1, Ack: 1, Len: 487  
Hypertext Transfer Protocol  
GET /kurose\_ross/index.php HTTP/1.1  
Host: gaia.cs.umass.edu  
Connection: keep-alive  
DNT: 1  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/123.0.0.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9,en-AU;q=0.8  
[Full request URI: http://gaia.cs.umass.edu/kurose\_ross/index.php]  
[HTTP request 1/2]  
[Response in frame: 10591]  
[Next request in frame: 10701]

0000 04 d5 90 e5 45 1c 5c 3a 45 b0 53 47 08 00 00 00 ... E \: E SG : E  
0010 02 0f ae 1d 40 00 80 06 7e ab 0a 35 4c 67 80 77 ... @ : ~ 5Lg.w  
0020 f5 0c 3c 1b 00 50 52 aa 90 6d 1c fa 4d 33 50 18 ... < PR : m .M3P  
0030 02 01 60 9a 00 00 47 45 54 20 2f 6b 75 72 6f 73 ... GE T /kuros  
0040 65 5f 72 6f 73 73 2f 69 6e 64 65 78 2e 70 68 70 e\_ross/i ndex.php  
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1 Host:  
0060 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 gaia.cs .umass.e  
0070 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 du .Conn ection:  
0080 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 44 e5 54 3a keep-ali ve-DNT:  
0090 20 31 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 1 Upgr ade-Inse  
00a0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1  
00b0 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..User-A gent: Mo  
00c0 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo  
00d0 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 ws NT 10 .0; Win6  
00e0 3a 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4; x64) AppleWeb  
00f0 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d Kit/537. 36 (KHTM  
0100 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 L, like Gecko) C  
0110 68 72 6f 6d 65 2f 31 32 33 2e 30 2e 30 2e 30 20 hrome/12 3.0.0.0  
0120 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64 Safari/5 37.36 Ed  
0130 67 2f 31 32 33 2e 30 2e 30 2e 30 0d 0a 41 63 63 g/123.0. 0.0 Acc  
0140 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 ept: tex t/html,a  
0150 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c pplicati on/xhtml  
0160 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,app lication  
0170 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0 .9,image  
0180 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 /avif,im age/webp  
0190 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b ,image/a png,\*/\*;  
01a0 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f q=0.8,ap plicatio  
01b0 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 n/signed -exchang  
01c0 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 e;v=b3;q =0.7 Ac  
01d0 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g  
01e0 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 zip, def late Ac  
01f0 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Lan guage: e  
0200 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 2c 65 6e n-US,en; q=0.9,en

Wireshark: Wi-FiAMK2.pcapng

Packets: 49111 - Displayed: 1684 (3.4%) - Dropped: 0 (0.0%) Profile: Default

11. The web page for the base file [http://gaia.cs.umass.edu/kurose\\_ross/](http://gaia.cs.umass.edu/kurose_ross/) references the image object [http://gaia.cs.umass.edu/kurose\\_ross/header\\_graphic\\_book\\_8E\\_2.jpg](http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg), which, like the base webpage, is on [gaia.cs.umass.edu](http://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/](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](http://gaia.cs.umass.edu) so that this initial HTTP request can be sent to the [gaia.cs.umass.edu](http://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](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](http://gaia.cs.umass.edu) so that this second HTTP request can be sent to the [gaia.cs.umass.edu](http://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.

The image shows a Wireshark packet capture window titled '\*Wi-Fi'. The filter bar is set to 'dns'. The packet list pane shows several DNS packets. Packet 20700 is selected, showing a standard query for 'www.cs.umass.edu.nitk.ac.in'. The packet details pane shows the following information:

- Frame 20700: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF\_{F88D562D-4600-45...}
- Ethernet II, Src: ChongqingFug\_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet\_e5:45:1c (04:d5:90:e5:45:1c)
- Internet Protocol Version 4, Src: 10.53.76.103, Dst: 10.9.0.10
- User Datagram Protocol, Src Port: 62811, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0x0002
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - [Response In: 20704]

The packet bytes pane shows the raw data of the DNS query, including the transaction ID 0000 and the domain name 'www.cs.umass.edu.nitk.ac.in'.

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

The image shows a Wireshark packet capture window titled "\*Wi-Fi". The packet list pane displays several packets, with the selected packet being a DNS standard query response (packet 7887) from 10.53.76.103 to 10.9.0.10. The packet details pane shows the structure of the domain name system query, including the transaction ID, flags, and the query itself.

No.	Time	Source	Destination	Protocol	Length	Info
44	0.039524	10.9.0.100	10.53.76.103	ICMP	110	Destination unreachable (Port unreachable)
2951	2.988679	10.53.76.103	10.9.0.10	DNS	69	Standard query 0xbd4f A umass.edu
3378	3.368784	10.53.76.103	10.9.0.100	DNS	69	Standard query 0xbd4f A umass.edu
3420	3.418076	10.9.0.100	10.53.76.103	ICMP	97	Destination unreachable (Port unreachable)
3421	3.418239	10.53.76.103	10.20.1.21	DNS	69	Standard query 0xbd4f A umass.edu
3701	3.738028	10.20.1.21	10.53.76.103	DNS	85	Standard query response 0xbd4f A umass.edu A 128.119.8.148
3707	3.741643	10.53.76.103	128.119.8.148	DNS	86	Standard query 0x0001 PTR 148.8.119.128.in-addr.arpa
5933	5.730642	10.53.76.103	128.119.8.148	DNS	79	Standard query 0x0002 A type=NS.nitk.ac.in
6553	6.386828	10.9.0.10	10.53.76.103	DNS	69	Standard query response 0xbd4f Server failure A umass.edu
6554	6.386855	10.53.76.103	10.9.0.10	ICMP	97	Destination unreachable (Port unreachable)
7887	7.731300	10.53.76.103	128.119.8.148	DNS	79	Standard query 0x0003 AAAA type=NS.nitk.ac.in

Frame 44: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF\_{F88D562D-4600-450... Ethernet II, Src: Fortinet\_e5:45:1c (04:d5:90:e5:45:1c), Dst: ChongqingFug\_b0:53:47 (5c:3a:45:b0:53:47) Internet Protocol Version 4, Src: 10.9.0.100, Dst: 10.53.76.103 Internet Control Message Protocol Domain Name System (query) Transaction ID: 0x5abc Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries

Packets: 13660 - Displayed: 11 (0.1%) - Dropped: 0 (0.0%) Profile: Default

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