

Lab-2 DNS

```
Last login: Thu Feb 15 09:58:11 on ttys000
zacharybrown@Zacharys-MacBook-Pro-2 ~ % nslookup www.iitb.ac.in
Server:      192.168.0.1
Address:     192.168.0.1#53

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

zacharybrown@Zacharys-MacBook-Pro-2 ~ % nslookup www.iitb.ac.in --type=NS
*** Invalid option: --type=NS
Server:      192.168.0.1
Address:     192.168.0.1#53

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

zacharybrown@Zacharys-MacBook-Pro-2 ~ % nslookup www.iitb.ac.in -type=NS
*** Invalid option: type=NS
Server:      192.168.0.1
Address:     192.168.0.1#53

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

zacharybrown@Zacharys-MacBook-Pro-2 ~ % nslookup www.iitb.ac.in -type=NS
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
*** Can't find www.iitb.ac.in: No answer

Authoritative answers can be found from:
iitb.ac.in
  origin = dns1.iitb.ac.in
  mail addr = postmaster.iitb.ac.in
  serial = 2013071001
  refresh = 16384
  retry = 2048
  expire = 1640576
  minimum = 3000

zacharybrown@Zacharys-MacBook-Pro-2 ~ % nslookup dns1.iitb.ac.in
Server:      192.168.0.1
Address:     192.168.0.1#53

** server can't find dns1.iitb.ac.in: NXDOMAIN

zacharybrown@Zacharys-MacBook-Pro-2 ~ % sudo killall -HUP mDNSResponder
Password:
```

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

Server: 192.168.0.1
Address: 192.168.0.1#53

Non-authoritative answer:
Name: www.iitb.ac.in
Address: 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. 192.168.0.1
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?

Authoritative answers can be found from:

iitb.ac.in

origin = dns1.iitb.ac.in

mail addr = postmaster.iitb.ac.in

serial = 2013071001

refresh = 16384

retry = 2048

expire = 1048576

a. minimum = 3960

b. I would find the IP address by the SOA record get the primary name server and then do another nslookup with the original ip address and specify this name server

The image shows a Wireshark packet capture of a network conversation. The top pane shows the packet list with 47 packets. The middle pane shows the packet details for the selected packet (No. 10, a DNS query). The bottom pane shows the packet bytes. The DNS query is for 'iitb.ac.in' and is sent over UDP. The response is also shown in the packet list (No. 11).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.102	192.168.0.1	TCP	90	Application Data
2	0.393137	192.168.0.102	18.172.124.101	TCP	90	[TCP Retransmission] 56063 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=30608 Len=24 TSval=954824618 TSecr=
3	0.414664	162.159.135.234	192.168.0.102	TLSv1	187	Application Data
4	0.415096	192.168.0.102	162.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=122 Win=3674 Len=0 TSval=3481956706 TSecr=3966846814
5	0.427127	192.168.0.102	162.159.61.4	TLSv1	185	Application Data
6	0.440998	162.159.61.4	192.168.0.102	TLSv1	185	Application Data
7	0.441272	192.168.0.102	162.159.61.4	TCP	66	55689 → 443 [ACK] Seq=40 Ack=40 Win=2047 Len=0 TSval=714404222 TSecr=1323283132
9	0.978153	192.168.0.102	18.172.124.101	TCP	90	[TCP Retransmission] 56063 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=30608 Len=24 TSval=954825203 TSecr=
10	1.388911	192.168.0.102	192.168.0.1	DNS	87	Standard query 0xedca HTTPS roaming.officeapps.live.com
11	1.389081	192.168.0.102	192.168.0.1	DNS	87	Standard query 0x2d9a A roaming.officeapps.live.com
12	1.394857	162.159.135.234	192.168.0.102	TLSv1	188	Application Data
13	1.395841	192.168.0.102	162.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=244 Win=3674 Len=0 TSval=3481957686 TSecr=3966847742
14	1.448944	192.168.0.1	192.168.0.102	DNS	315	Standard query response 0xedca HTTPS roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.
15	1.449777	192.168.0.102	192.168.0.1	DNS	114	Standard query 0x0212 HTTPS osiproduct-cus-buff-azsc-000.centralus.cloudapp.azure.com
16	1.463189	192.168.0.1	192.168.0.102	DNS	185	Standard query response 0x0212 HTTPS osiproduct-cus-buff-azsc-000.centralus.cloudapp.azure.com SOA ns1-2
18	1.562522	192.168.0.1	192.168.0.102	DNS	260	Standard query response 0x2d9a A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net
19	1.563351	192.168.0.102	192.168.0.1	DNS	114	Standard query 0x493d A osiproduct-cus-buff-azsc-000.centralus.cloudapp.azure.com
20	1.576334	192.168.0.1	192.168.0.102	DNS	130	Standard query response 0x493d A osiproduct-cus-buff-azsc-000.centralus.cloudapp.azure.com A 52.109.8.36
21	1.577634	192.168.0.102	52.109.8.36	TCP	78	55952 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3356891744 TSecr=0 SACK_PERM
22	1.610580	52.109.8.36	192.168.0.102	TCP	66	443 → 55952 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
23	1.611096	192.168.0.102	52.109.8.36	TCP	54	55952 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
24	1.611101	192.168.0.102	52.109.8.36	TLSv1	571	Client Hello (SNI=roaming.officeapps.live.com)
25	1.645460	52.109.8.36	192.168.0.102	TCP	1514	443 → 55952 [ACK] Seq=1 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
26	1.645462	52.109.8.36	192.168.0.102	TCP	1514	443 → 55952 [ACK] Seq=1461 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
27	1.645463	52.109.8.36	192.168.0.102	TCP	1514	443 → 55952 [ACK] Seq=2921 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
28	1.645465	52.109.8.36	192.168.0.102	TCP	1514	443 → 55952 [ACK] Seq=4381 Ack=518 Win=525056 Len=1460 [TCP segment of a reassembled PDU]
29	1.645517	52.109.8.36	192.168.0.102	TLSv1	369	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
30	1.646688	192.168.0.102	52.109.8.36	TCP	54	55952 → 443 [ACK] Seq=518 Ack=5841 Win=256256 Len=0
31	1.646696	192.168.0.102	52.109.8.36	TCP	54	55952 → 443 [ACK] Seq=518 Ack=6156 Win=255936 Len=0
32	1.646702	192.168.0.102	52.109.8.36	TCP	54	[TCP Window Update] 55952 → 443 [ACK] Seq=518 Ack=6156 Win=262144 Len=0
33	1.660321	192.168.0.102	52.109.8.36	TLSv1	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
34	1.694222	52.109.8.36	192.168.0.102	TLSv1	105	Change Cipher Spec, Encrypted Handshake Message
35	1.694223	52.109.8.36	192.168.0.102	TLSv1	123	Application Data
36	1.695795	192.168.0.102	52.109.8.36	TCP	54	55952 → 443 [ACK] Seq=676 Ack=6276 Win=262016 Len=0
37	1.697459	192.168.0.102	52.109.8.36	TLSv1	345	Application Data
38	1.698272	192.168.0.102	52.109.8.36	TLSv1	1494	Application Data
39	1.698323	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=2407 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
40	1.698339	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=3847 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
41	1.698346	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=5287 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
42	1.698385	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=6727 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
43	1.698391	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=8167 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
44	1.698396	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=9607 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
45	1.698401	192.168.0.102	52.109.8.36	TCP	1494	55952 → 443 [ACK] Seq=11847 Ack=6276 Win=262144 Len=1440 [TCP segment of a reassembled PDU]
46	1.698422	192.168.0.102	52.109.8.36	TLSv1	1444	Application Data
47	1.738322	52.109.8.36	192.168.0.102	TLSv1	92	Application Data

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 query4 message sent over UDP or TCP?
 - a. The message is sent over 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. 20, the response is received via UDP

```
> Frame 18: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface en0, id 0
> Ethernet II, Src: Apple_19:35:a0 (bc:d0:74:19:35:a0), Dst: TPLinkTechno_82:86:b7 (84:d0:1b:82:86:b7)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
  > User Datagram Protocol, Src Port: 57879, Dst Port: 53
    > Source Port: 57879
    > Destination Port: 53
    > Length: 53
    > Checksum: 0x9f60 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    > [Timestamps]
    > UDP payload (45 bytes)
  > Domain Name System (query)
    > Transaction ID: 0xedca
    > Flags: 0x0100 Standard query
    > Questions: 1
    > Answer RRs: 0
    > Authority RRs: 0
    > Additional RRs: 0
    > Questions: 1
```

7. What is the destination port for the DNS query message? What is the source port of the DNS response message?
 - a. Destination is 53, Source is 578979
8. To what IP address is the DNS query message sent?
 - a. 192.168.0.1
9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain? Why?
 - a. 1 Question, 0 answers. This is because it is trying to find an answer for it question.
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? Why?
 - a. There is 1 question and 4 answers. This is because there were 4 different answers to the original 1 question.
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_8E_3.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.
 - a. Packet number 217
 - b. Packet number 19
 - c. Packet number 20
 - d. Packet number 317
 - e. Packet number 214

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.159.135.234	192.168.0.102	TCP	168	Application Data
2	0.000346	192.168.0.102	192.159.135.234	TLSv1	66	55698 → 443 [ACK] Seq=1 Ack=103 Win=3674 Len=0 TSval=3482927758 TSecr=3967817792
3	0.718381	192.159.135.234	192.168.0.102	TLSv1	559	Application Data
4	0.718787	192.168.0.102	192.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=596 Win=3674 Len=0 TSval=3482928476 TSecr=3967818545
5	0.771796	192.159.135.234	192.168.0.102	TLSv1	114	Application Data
6	0.772112	192.168.0.102	192.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=644 Win=3674 Len=0 TSval=3482928530 TSecr=3967818639
7	0.787959	192.159.135.234	192.168.0.102	TLSv1	137	Application Data
8	0.788276	192.168.0.102	192.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=715 Win=3674 Len=0 TSval=3482928546 TSecr=3967818656
9	1.025975	192.168.0.102	192.159.61.4	TLSv1	105	Application Data
10	1.043772	192.159.61.4	192.168.0.102	TLSv1	105	Application Data
11	1.044058	192.168.0.102	192.159.61.4	TCP	66	55689 → 443 [ACK] Seq=40 Ack=40 Win=2047 Len=0 TSval=715376292 TSecr=1324255203
12	2.652099	192.168.0.102	35.186.224.39	TLSv1	109	Application Data
13	2.687204	35.186.224.39	192.168.0.102	TCP	66	443 → 55745 [ACK] Seq=1 Ack=44 Win=268 Len=0 TSval=3455518099 TSecr=630602060
14	2.693646	35.186.224.39	192.168.0.102	TLSv1	106	Application Data
15	2.693779	192.168.0.102	35.186.224.39	TCP	66	55745 → 443 [ACK] Seq=44 Ack=41 Win=2047 Len=0 TSval=630602102 TSecr=3455518106
16	5.259197	192.168.0.102	192.168.0.1	DNS	76	Standard query 0x803d A www.cs.umass.edu
17	5.308774	192.168.0.1	192.168.0.102	DNS	92	Standard query response 0x803d A www.cs.umass.edu A 128.119.240.84
18	6.656848	192.159.135.234	192.168.0.102	TLSv1	177	Application Data
19	6.656515	192.168.0.102	192.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=826 Win=3674 Len=0 TSval=3482934414 TSecr=3967824465
20	7.043005	192.168.0.102	192.159.61.4	TLSv1	105	Application Data
21	7.046332	192.159.135.234	192.168.0.102	TLSv1	156	Application Data
22	7.046507	192.168.0.102	192.159.135.234	TCP	66	55698 → 443 [ACK] Seq=1 Ack=916 Win=3674 Len=0 TSval=3482934804 TSecr=3967824846
23	7.063428	192.159.61.4	192.168.0.102	TLSv1	105	Application Data
24	7.063536	192.168.0.102	192.159.61.4	TCP	66	55689 → 443 [ACK] Seq=79 Ack=79 Win=2047 Len=0 TSval=715382311 TSecr=1324261223

12. What is the destination port for the DNS query message? What is the source port of the DNS response message?
 - a. Source Port: 50154
 - b. Destination Port: 53
13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
 - a. 192.168.0.1, yes this is my default local DNS server
14. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
 - a. The query is a standard query, it contains no answers.
15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?
 - a. There is one question and one answer.

No.	Time	Source	Destination	Protocol	Length	Info
428	35.463176	192.168.0.1	192.168.0.102	DNS	183	Standard query response 0xbacd HTTPS osiproduct-eus2-buff-azsc-000.eastus2.cloudapp.azure.com SOA ns1-06.azu...
427	35.449573	192.168.0.102	192.168.0.1	DNS	113	Standard query 0xbacd HTTPS osiproduct-eus2-buff-azsc-000.eastus2.cloudapp.azure.com
426	35.449063	192.168.0.1	192.168.0.102	DNS	315	Standard query response 0xbcf6 HTTPS roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net ...
425	35.422066	192.168.0.1	192.168.0.102	DNS	260	Standard query response 0x131f A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAM...
421	35.347929	192.168.0.102	192.168.0.1	DNS	87	Standard query 0x131f A roaming.officeapps.live.com
420	35.347732	192.168.0.102	192.168.0.1	DNS	87	Standard query 0xbcf6 HTTPS roaming.officeapps.live.com
138	32.148762	192.168.0.1	192.168.0.102	DNS	106	Standard query response 0xc0b4 A imap.gmail.com A 142.250.123.108 A 142.250.123.109
137	32.133302	192.168.0.102	192.168.0.1	DNS	74	Standard query 0xc0b4 A imap.gmail.com
135	31.048984	192.168.0.102	128.119.8.148	DNS	70	Standard query 0xd589 A -type=NS
121	26.048563	192.168.0.102	128.119.8.148	DNS	70	Standard query 0xd589 A -type=NS
87	21.043481	192.168.0.102	128.119.8.148	DNS	70	Standard query 0xd589 A -type=NS
38	11.668261	192.168.0.102	128.119.8.148	DNS	70	Standard query 0x0514 A -type=NS
27	6.663230	192.168.0.102	128.119.8.148	DNS	70	Standard query 0x0514 A -type=NS
13	1.658319	192.168.0.102	128.119.8.148	DNS	70	Standard query 0x0514 A -type=NS
12	1.653089	192.168.0.1	192.168.0.102	DNS	85	Standard query response 0xbcf73 A umass.edu A 128.119.8.148
11	1.602888	192.168.0.102	192.168.0.1	DNS	69	Standard query 0xbcf73 A 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. The IP address is 128.119.8.148, this is not 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”?
 - a. The query message contains one question and no answers.

- a. 1 question no answers.
18. Examine the DNS response message. How many answers does the response have? If any, 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. There is no response received from umass.