

Pandit Deendayal Energy University
School of Technology
Department of ICT
Academic Year: 2022-23
Computer Communication and Networking Lab
20IC306P

Name: Janakar Patel

Roll No: 20BIT061

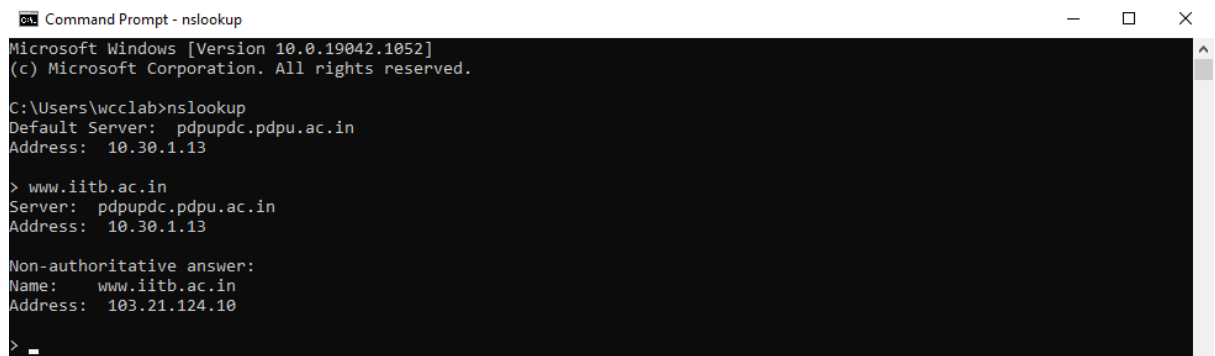
Experiment 4:

Aim: To understand the working of DNS by using wire shark and packet tracer.

Software Tools required: - Wire-shark and Cisco packet tracer

1. nslookup

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`
Ans:



```
Microsoft Windows [Version 10.0.19042.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\wcc\lab>nslookup
Default Server:  pdpupdc.pdpu.ac.in
Address:  10.30.1.13

> www.iitb.ac.in
Server:  pdpupdc.pdpu.ac.in
Address:  10.30.1.13

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

>
```

IP Address: 103.21.124.18

2. What is the IP address of the DNS server that provided the answer to your `nslookup` command in question 1 above?
Ans: IP Address: 103.21.124.18
3. Did the answer to your `nslookup` command in question 1 above come from an authoritative or non-authoritative server?
Ans: Non-authoritative server
4. Use the `nslookup` command to determine the name of the authoritative name server for the `iitb.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?
Ans:

```
Command Prompt
Microsoft Windows [Version 10.0.19042.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\wclab>nslookup -type=NS iitb.ac.in
Server: pdpupdc.pdpu.ac.in
Address: 10.30.1.13

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

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

C:\Users\wclab>
```

Three authoritative servers. The first server name is dns2.iitb.ac.in and internet address 103.21.126.129

2. The DNS cache on your computer

```
C:\Users\wclab>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\wclab>
```

3. Tracing DNS with Wireshark

```
C:\Users\wclab>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\wclab>
```

Wireshark packet capture showing DNS traffic. The packet list shows a GET request for /kurose_ross/ HTTP/1.1. The packet details show the Hypertext Transfer Protocol section. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
793	23.770632	10.30.7.191	128.119.245.12	HTTP	388	GET /kurose_ross/ HTTP/1.1
800	24.041713	128.119.245.12	10.30.7.191	HTTP	650	HTTP/1.1 301 Moved Permanently (text/html)
801	24.050270	10.30.7.191	128.119.245.12	HTTP	397	GET /kurose_ross/index.php HTTP/1.1
817	24.359374	128.119.245.12	10.30.7.191	HTTP	778	HTTP/1.1 200 OK (text/html)
822	24.381995	10.30.7.191	128.119.245.12	HTTP	380	GET /kurose_ross/custom.css HTTP/1.1
827	24.384103	10.30.7.191	128.119.245.12	HTTP	364	GET /kurose_ross/script.js HTTP/1.1
858	24.593377	10.30.7.191	117.18.237.29	OCSP	490	Request
871	24.686691	128.119.245.12	10.30.7.191	HTTP	389	HTTP/1.1 200 OK (text/css)
874	24.690844	128.119.245.12	10.30.7.191	HTTP	1349	HTTP/1.1 200 OK (application/javascript)
876	24.694297	117.18.237.29	10.30.7.191	OCSP	601	Response
968	24.871886	10.30.7.191	128.119.245.12	HTTP	383	GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1
1031	25.129177	10.30.7.191	142.250.192.67	OCSP	492	Request
1071	25.248448	142.250.192.67	10.30.7.191	OCSP	755	Response
1341	28.364946	128.119.245.12	10.30.7.191	HTTP	704	HTTP/1.1 200 OK (JPEG JFIF image)
1346	28.383667	10.30.7.191	128.119.245.12	HTTP	357	GET /favicon.ico HTTP/1.1
1364	28.674957	128.119.245.12	10.30.7.191	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1365	28.676800	10.30.7.191	128.119.245.12	HTTP	357	GET /favicon.ico HTTP/1.1
1378	28.978440	128.119.245.12	10.30.7.191	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 793: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits) on interface \Device\NPF_{289F6DB3-7883-408D-842C-44FF5C4F0AA}, id 0

Ethernet II, Src: HewlettP_87:79:93 (84:a9:3e:87:79:93), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)

Internet Protocol Version 4, Src: 10.30.7.191, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 56884, Dst Port: 80, Seq: 1, Ack: 1, Len: 334

Hypertext Transfer Protocol

0000 c8 f9 f9 58 32 00 84 a9 3e 87 79 93 00 00 45 00 ...X2...>y...E
0010 81 76 fd 01 40 00 00 00 00 00 0a 1e 07 bf 80 77 ...v...g... ..
0020 f5 0c de 34 00 50 39 cd 1e 90 cd 04 3f 06 50 18 ...4:P9:P-
0030 02 04 88 c9 00 00 47 45 54 20 2f 6b 75 72 6f 73GE T /kuros
0040 65 5f 72 6f 73 2f 20 48 54 54 50 2f 31 2e 31 e_ross/ HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e ...Host: gaia.co.

5. Locate the first DNS query message resolving the name `gaia.cs.umass.edu`. What is the packet number¹ in the trace for the DNS query message? Is this query message sent over UDP or TCP?

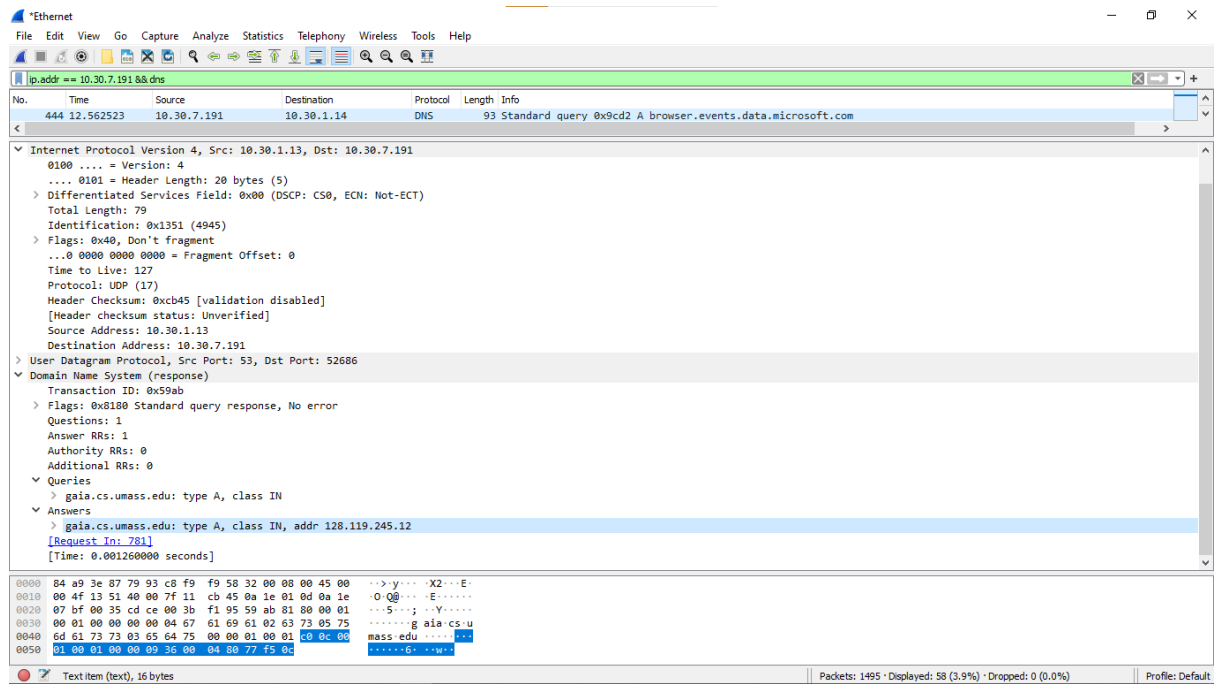
The screenshot shows a Wireshark packet capture of network traffic. The packet list pane at the top shows several DNS messages. Packet 781 is highlighted, showing a DNS query for `gaia.cs.umass.edu`. The packet details pane below shows the structure of the query, including the transaction ID (0x59ab) and the query type (A). The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Domain Name System (query) data.

The screenshot shows a Wireshark packet capture of network traffic. The packet list pane at the top shows several DNS messages. Packet 782 is highlighted, showing a DNS response for `gaia.cs.umass.edu`. The packet details pane below shows the structure of the response, including the transaction ID (0x59ab) and the response type (A). The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Domain Name System (response) data.

Ans: The query is sent over a UDP Protocol. The packet number is 781.

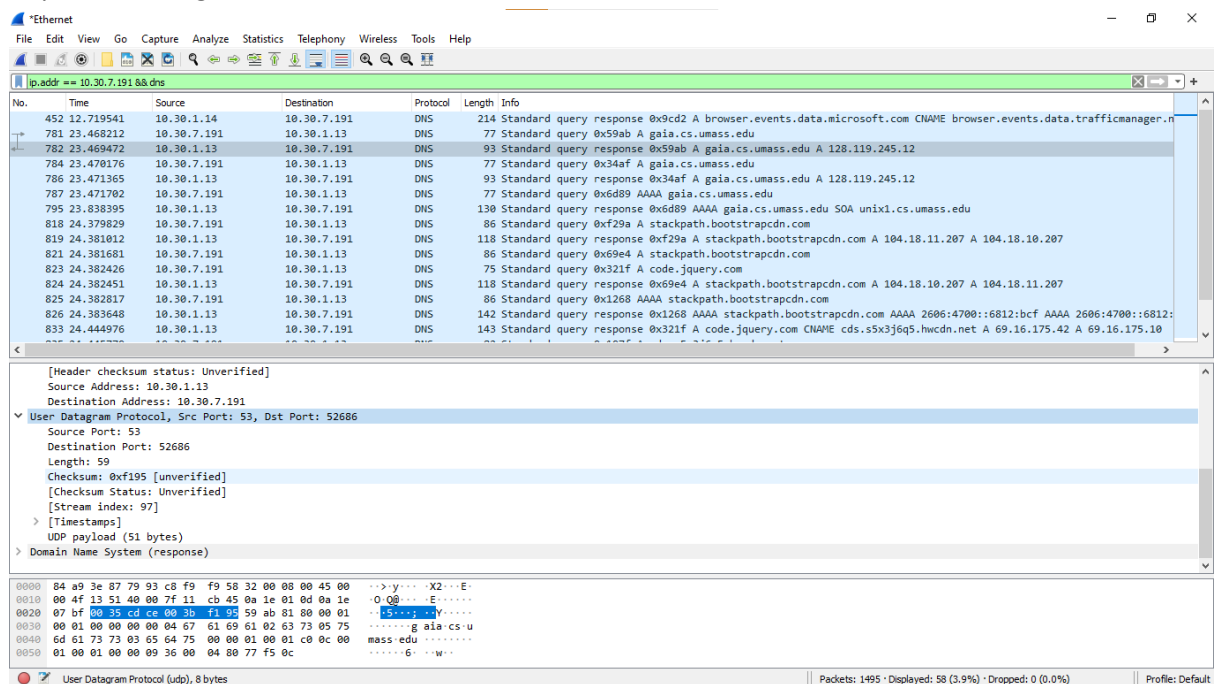
6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

¹ Remember that this “packet number” is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.



Ans: The message is received via UDP and packet number is 782.

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



Ans: The port number of destination port for query and source source port of response is 53.

- To what IP address is the DNS query message sent?

Ans: IP Address: 10.30.1.13

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

Ans:

Question is 1 and the answer is 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?

Ans:

Question is 1 and Answer is 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.

Ans:

Wireshark packet capture showing HTTP traffic. The initial GET request for /kurose_ross/ HTTP/1.1 is highlighted in green. The packet list shows it as packet 793. The packet details pane shows the full HTTP request structure.

No.	Time	Source	Destination	Protocol	Length	Info
793	23.778632	10.30.7.191	128.119.245.12	HTTP	388	GET /kurose_ross/ HTTP/1.1
800	24.041713	128.119.245.12	10.30.7.191	HTTP	650	HTTP/1.1 301 Moved Permanently (text/html)
801	24.050270	10.30.7.191	128.119.245.12	HTTP	397	GET /kurose_ross/index.php HTTP/1.1
817	24.359374	128.119.245.12	10.30.7.191	HTTP	778	HTTP/1.1 200 OK (text/html)
822	24.381995	10.30.7.191	128.119.245.12	HTTP	380	GET /kurose_ross/custom.css HTTP/1.1
827	24.384183	10.30.7.191	128.119.245.12	HTTP	364	GET /kurose_ross/script.js HTTP/1.1
858	24.593377	10.30.7.191	117.18.237.29	OCSP	490	Request
871	24.686591	128.119.245.12	10.30.7.191	HTTP	389	HTTP/1.1 200 OK (text/css)
874	24.690844	128.119.245.12	10.30.7.191	HTTP	1349	HTTP/1.1 200 OK (application/javascript)
876	24.694297	117.18.237.29	10.30.7.191	OCSP	601	Response
968	24.871886	10.30.7.191	128.119.245.12	HTTP	383	GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1
1031	25.129177	10.30.7.191	142.250.192.67	OCSP	492	Request
1071	25.248448	142.250.192.67	10.30.7.191	OCSP	755	Response
1341	28.364946	128.119.245.12	10.30.7.191	HTTP	704	HTTP/1.1 200 OK (JPEG JFIF image)
1346	28.383667	10.30.7.191	128.119.245.12	HTTP	357	GET /favicon.ico HTTP/1.1

Frame 793: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits) on interface \Device\NPF_{289F60B3-78B3-408D-842C-44FF5CACF0AA}, id 0
Ethernet II, Src: HewlettP_87:79:93 (84:a9:3e:87:79:93), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
Internet Protocol Version 4, Src: 10.30.7.191, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56884, Dst Port: 80, Seq: 1, Ack: 1, Len: 334
Source Port: 56884
Destination Port: 80
[Stream index: 27]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 334]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 969744016
[Next Sequence Number: 335 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3439607558

Packet Number for initial HTTP is 793.

Wireshark packet capture showing DNS traffic. The initial query for gaia.cs.umass.edu is highlighted in blue. The packet list shows it as packet 111. The packet details pane shows the full DNS query structure.

No.	Time	Source	Destination	Protocol	Length	Info
111	5.652905	10.30.7.191	10.30.1.13	DNS	77	Standard query 0xd126 A gaia.cs.umass.edu
122	5.996882	10.30.1.13	10.30.7.191	DNS	93	Standard query response 0xd126 A gaia.cs.umass.edu A 128.119.245.12
124	5.999763	10.30.7.191	10.30.1.13	DNS	77	Standard query 0xa80c A gaia.cs.umass.edu
125	6.000957	10.30.1.13	10.30.7.191	DNS	93	Standard query response 0xa80c A gaia.cs.umass.edu A 128.119.245.12
126	6.002807	10.30.7.191	10.30.1.13	DNS	77	Standard query 0x0e90 AAAA gaia.cs.umass.edu
127	6.003833	10.30.1.13	10.30.7.191	DNS	130	Standard query response 0x0e90 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
159	6.553802	10.30.7.191	10.30.1.13	DNS	86	Standard query 0x5e46 A stackpath.bootstrapcdn.com
161	6.554972	10.30.1.13	10.30.7.191	DNS	118	Standard query response 0x5e46 A stackpath.bootstrapcdn.com A 104.18.11.207 A 104.18.10.207
164	6.555747	10.30.7.191	10.30.1.13	DNS	86	Standard query 0xfeb8 A stackpath.bootstrapcdn.com
165	6.556663	10.30.1.13	10.30.7.191	DNS	118	Standard query response 0xfeb8 A stackpath.bootstrapcdn.com A 104.18.10.207 A 104.18.11.207
167	6.557012	10.30.7.191	10.30.1.13	DNS	86	Standard query 0xc89e AAAA stackpath.bootstrapcdn.com
168	6.557965	10.30.1.13	10.30.7.191	DNS	142	Standard query response 0xc89e AAAA stackpath.bootstrapcdn.com AAAA 2606:4700::6812:bcf AAAA 2606:4700::6812:
255	6.791687	10.30.7.191	10.30.1.13	DNS	80	Standard query 0xfbd1 A fonts.googleapis.com
256	6.792930	10.30.1.13	10.30.7.191	DNS	96	Standard query response 0xfbd1 A fonts.googleapis.com A 172.217.160.202
258	6.794156	10.30.7.191	10.30.1.13	DNS	80	Standard query 0x73a7 A fonts.googleapis.com

Frame 111: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{289F60B3-78B3-408D-842C-44FF5CACF0AA}, id 0
Ethernet II, Src: HewlettP_87:79:93 (84:a9:3e:87:79:93), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
Internet Protocol Version 4, Src: 10.30.7.191, Dst: 10.30.1.13
User Datagram Protocol, Src Port: 56209, Dst Port: 53
Domain Name System (query)

Packet number is 111, In response to query the packet number is 112

No.	Time	Source	Destination	Protocol	Length	Info
9	0.235489	10.30.7.191	34.117.35.28	HTTP	55	Continuation
139	6.279177	10.30.7.191	128.119.245.12	HTTP	397	GET /kurose_ross/index.php HTTP/1.1
156	6.538385	128.119.245.12	10.30.7.191	HTTP	779	HTTP/1.1 200 OK (text/html)
158	6.553647	10.30.7.191	128.119.245.12	HTTP	380	GET /kurose_ross/custom.css HTTP/1.1
162	6.555144	10.30.7.191	128.119.245.12	HTTP	364	GET /kurose_ross/script.js HTTP/1.1
267	6.829757	128.119.245.12	10.30.7.191	HTTP	389	HTTP/1.1 200 OK (text/css)
270	6.843239	128.119.245.12	10.30.7.191	HTTP	1349	HTTP/1.1 200 OK (application/javascript)
333	7.091458	10.30.7.191	128.119.245.12	HTTP	383	GET /kurose_ross/header_graphic_book_0E_3.jpg HTTP/1.1
618	9.998911	10.30.7.191	34.117.35.28	HTTP	473	GET /pub/firefox/releases/56.0b3/update/win32/en-US/firefox-56.0b3.complete.mar HTTP/1.1
960	10.169062	34.117.35.28	10.30.7.191	HTTP	952	HTTP/1.1 206 Partial Content
1009	10.515530	128.119.245.12	10.30.7.191	HTTP	704	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 9: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{289F60B3-78B3-408D-842C-44FF5CACF0AA}, id 0
 > Ethernet II, Src: HewlettP_87:79:93 (84:a9:3e:87:79:93), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
 > Internet Protocol Version 4, Src: 10.30.7.191, Dst: 34.117.35.28
 > Transmission Control Protocol, Src Port: 57013, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
 > Hypertext Transfer Protocol

0000 c8 f9 f9 58 32 00 84 a9 3e 87 79 93 08 00 45 00 ...X2...>y...E
 0010 00 29 a5 09 40 00 00 06 00 00 0a 1e 07 bf 22 75 ...@... ..u
 0020 23 1c de b5 00 00 0e df dd 8d f5 f9 12 db 50 10 ...P... ..p
 0030 18 4b 57 89 00 00 00 00 ...Kl....

Packet number is 333.

No DNS query is sent for the second HTTP GET request. Because the IP address is already store in local DNS cache memory.

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

Ans:

No.	Time	Source	Destination	Protocol	Length	Info
870	35.279635	10.30.1.13	10.30.7.191	DNS	113	Standard query response 0x63da A array616.prod.do.sdp.mp.microsoft.com A 20.54.25.4
940	38.529661	10.30.7.191	10.30.1.13	DNS	83	Standard query 0x0001 PTR 13.1.30.10.in-addr.arpa
941	38.530802	10.30.1.13	10.30.7.191	DNS	115	Standard query response 0x0001 PTR 13.1.30.10.in-addr.arpa PTR pdpudc.pdpu.ac.in
942	38.532302	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0002 A www.cs.umass.edu.pdpu.ac.in
943	38.533512	10.30.1.13	10.30.7.191	DNS	152	Standard query response 0x0002 No such name A www.cs.umass.edu.pdpu.ac.in SOA pdpudc.pdpu.ac.in
944	38.533799	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0003 AAAA www.cs.umass.edu.pdpu.ac.in
945	38.534951	10.30.1.13	10.30.7.191	DNS	152	Standard query response 0x0003 No such name AAAA www.cs.umass.edu.pdpu.ac.in SOA pdpudc.pdpu.ac.in
946	38.535211	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0004 A www.cs.umass.edu.pdeu.local
947	38.536327	10.30.1.13	10.30.7.191	DNS	142	Standard query response 0x0004 No such name A www.cs.umass.edu.pdeu.local SOA pdcpeu.pdeu.local
948	38.536503	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0005 AAAA www.cs.umass.edu.pdeu.local
949	38.537519	10.30.1.13	10.30.7.191	DNS	142	Standard query response 0x0005 No such name AAAA www.cs.umass.edu.pdeu.local SOA pdcpeu.pdeu.local

> Frame 942: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{289F60B3-78B3-408D-842C-44FF5CACF0AA}, id 0
 > Ethernet II, Src: HewlettP_87:79:93 (84:a9:3e:87:79:93), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
 > Internet Protocol Version 4, Src: 10.30.7.191, Dst: 10.30.1.13
 > User Datagram Protocol, Src Port: 59379, Dst Port: 53
 > Source Port: 59379
 > Destination Port: 53
 > Length: 53
 > Checksum: 0x1d4e [unverified]
 > [Checksum Status: Unverified]
 > [Stream Index: 111]
 > [Timestamps]
 > UDP payload (45 bytes)
 > Domain Name System (query)

0000 c8 f9 f9 58 32 00 84 a9 3e 87 79 93 08 00 45 00 ...X2...>y...E
 0010 00 45 f7 bc 00 00 00 11 00 00 0a 1e 07 bf 0a 1e5..N.....
 0020 01 0d e7 f3 00 35 00 35 1d 4e 00 02 01 00 00 01w ww cs um
 0030 00 00 00 00 00 03 77 77 77 02 63 73 05 75 6dss edu pdpu ac
 0040 61 73 73 03 65 64 75 04 70 64 70 75 02 61 63 02in.....
 0050 69 6e 00 00 01 00 01

The port number of destination for query and source for response is 53.

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

Ans:

The screenshot shows a Wireshark packet capture of a DNS query. The packet list at the top shows a query from 10.30.7.191 to 10.30.7.191. The packet details pane shows the destination address is 10.30.7.191. The packet bytes pane shows the destination address in hexadecimal: 0a 30 07 19.

It is a local dns server.

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

Ans:

The screenshot shows a Wireshark packet capture of a DNS query. The packet details pane shows the query type is A and the query is for www.cs.umass.edu.pdu.ac.in. The packet bytes pane shows the query type in hexadecimal: 00 01.

Type is A, It contains 0 answers.

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

Ans:

The image shows a Wireshark packet capture of a DNS transaction. The packet list shows a query (No. 944) and a response (No. 951). The packet details pane for packet 951 shows a Standard query response with no error, containing one question and one answer. The question is for 'www.cs.umass.edu' type A, class IN. The answer is 'www.cs.umass.edu' type A, class IN, with IP address 128.119.240.84. The packet bytes pane shows the raw data of the DNS response.

No.	Time	Source	Destination	Protocol	Length	Info
944	38.533799	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0003 AAAA www.cs.umass.edu.pdpu.ac.in
945	38.534951	10.30.1.13	10.30.7.191	DNS	152	Standard query response 0x0003 No such name AAAA www.cs.umass.edu.pdpu.ac.in SOA pdpudc.pdpu.ac.in
946	38.535211	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0004 A www.cs.umass.edu.pdeu.local
947	38.536327	10.30.1.13	10.30.7.191	DNS	142	Standard query response 0x0004 No such name A www.cs.umass.edu.pdeu.local SOA pdcpdeu.pdeu.local
948	38.536563	10.30.7.191	10.30.1.13	DNS	87	Standard query 0x0005 AAAA www.cs.umass.edu.pdeu.local
949	38.537519	10.30.1.13	10.30.7.191	DNS	142	Standard query response 0x0005 No such name AAAA www.cs.umass.edu.pdeu.local SOA pdcpdeu.pdeu.local
950	38.537747	10.30.7.191	10.30.1.13	DNS	76	Standard query 0x0006 A www.cs.umass.edu
951	38.538836	10.30.1.13	10.30.7.191	DNS	92	Standard query response 0x0006 A www.cs.umass.edu A 128.119.240.84
952	38.541501	10.30.7.191	10.30.1.13	DNS	76	Standard query 0x0007 AAAA www.cs.umass.edu
953	38.542814	10.30.1.13	10.30.7.191	DNS	129	Standard query response 0x0007 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu

Frame 951: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{289F60B3-7883-408D-842C-44FF5C8F0AA}, id 0
Ethernet II, Src: Cisco 58:32:00 (c8:f9:f9:58:32:00), Dst: HewlettP_87:79:93 (84:a9:3e:87:79:93)
Internet Protocol Version 4, Src: 10.30.1.13, Dst: 10.30.7.191
User Datagram Protocol, Src Port: 53, Dst Port: 5383
Domain Name System (response)
Transaction ID: 0x0006
Flags: 0x1800 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
Answers
Request In: 950
[Time: 0.001089000 seconds]

It is type A and it contains 1 question and 1 answer.

```
C:\Users\wcc\lab>nslookup -type=NS umass.edu
Server: pdpudc.pdpu.ac.in
Address: 10.30.1.13

Non-authoritative answer:
umass.edu       nameserver = ns3.umass.edu
umass.edu       nameserver = ns2.umass.edu
umass.edu       nameserver = ns1.umass.edu

ns3.umass.edu   internet address = 69.16.40.18
ns2.umass.edu   internet address = 128.119.10.28
ns1.umass.edu   internet address = 128.119.10.27

C:\Users\wcc\lab>
```

The image shows a Wireshark packet capture of a DNS transaction. The packet list shows a query (No. 180) and a response (No. 187). The packet details pane for packet 187 shows a Standard query response with no error, containing one question and one answer. The question is for 'PTR 13.1.30.10.in-addr.arpa' type PTR, class IN. The answer is 'PTR 13.1.30.10.in-addr.arpa' type PTR, class IN, with IP address 10.30.7.191. The packet bytes pane shows the raw data of the DNS response.

No.	Time	Source	Destination	Protocol	Length	Info
180	6.955093	10.30.7.191	10.30.1.13	DNS	83	Standard query 0x0001 PTR 13.1.30.10.in-addr.arpa
181	6.956418	10.30.1.13	10.30.7.191	DNS	115	Standard query response 0x0001 PTR 13.1.30.10.in-addr.arpa PTR pdpudc.pdpu.ac.in
182	6.960575	10.30.7.191	10.30.1.13	DNS	80	Standard query 0x0002 NS umass.edu.pdpu.ac.in
183	6.961831	10.30.1.13	10.30.7.191	DNS	145	Standard query response 0x0002 No such name NS umass.edu.pdpu.ac.in SOA pdpudc.pdpu.ac.in
184	6.962993	10.30.7.191	10.30.1.13	DNS	80	Standard query 0x0003 NS umass.edu.pdeu.local
185	6.963268	10.30.1.13	10.30.7.191	DNS	135	Standard query response 0x0003 No such name NS umass.edu.pdeu.local SOA pdcpdeu.pdeu.local
186	6.963652	10.30.7.191	10.30.1.13	DNS	69	Standard query 0x0004 NS umass.edu
187	6.964501	10.30.1.13	10.30.7.191	DNS	171	Standard query response 0x0004 NS umass.edu NS ns3.umass.edu NS ns2.umass.edu NS ns1.umass.edu A 69.16.40.18
295	9.458470	10.30.7.191	10.30.1.14	DNS	75	Standard query 0x5d3e A mail.google.com
296	9.451266	10.30.7.191	10.30.1.14	DNS	75	Standard query 0x0080 HTTPS mail.google.com
298	9.451485	10.30.1.14	10.30.7.191	DNS	91	Standard query response 0x5d3e A mail.google.com A 142.250.76.197

Frame 187: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface \Device\NPF_{289F60B3-7883-408D-842C-44FF5C8F0AA}, id 0
Ethernet II, Src: Cisco 58:32:00 (c8:f9:f9:58:32:00), Dst: HewlettP_87:79:93 (84:a9:3e:87:79:93)
Internet Protocol Version 4, Src: 10.30.1.13, Dst: 10.30.7.191
User Datagram Protocol, Src Port: 53, Dst Port: 51731
Domain Name System (response)
Transaction ID: 0x0004
Flags: 0x1800 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
PTR 13.1.30.10.in-addr.arpa: type PTR, class IN
Answers
Request In: 186
[Time: 0.001089000 seconds]

Wireshark capture of a DNS query. The packet list shows a query from 10.30.7.191 to 10.30.1.13. The packet details pane shows the query for 'umass.edu' type NS, class IN. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
180	6.955093	10.30.7.191	10.30.1.13	DNS	83	Standard query 0x0001 PTR 13.1.30.10.in-addr.arpa
181	6.956418	10.30.1.13	10.30.7.191	DNS	115	Standard query response 0x0001 PTR 13.1.30.10.in-addr.arpa PTR pdpupdc.pdpu.ac.in
182	6.960575	10.30.7.191	10.30.1.13	DNS	80	Standard query 0x0002 NS umass.edu.pdpu.ac.in
183	6.961831	10.30.1.13	10.30.7.191	DNS	145	Standard query response 0x0002 No such name NS umass.edu.pdpu.ac.in SOA pdpupdc.pdpu.ac.in
184	6.962093	10.30.7.191	10.30.1.13	DNS	80	Standard query 0x0003 NS umass.edu.pdeu.local
185	6.963260	10.30.1.13	10.30.7.191	DNS	135	Standard query response 0x0003 No such name NS umass.edu.pdeu.local SOA pdcpdeu.pdeu.local
186	6.963662	10.30.7.191	10.30.1.13	DNS	69	Standard query 0x0004 NS umass.edu
187	6.964501	10.30.1.13	10.30.7.191	DNS	171	Standard query response 0x0004 NS umass.edu NS ns3.umass.edu NS ns2.umass.edu NS ns1.umass.edu A 69.16.40.18
295	9.450470	10.30.7.191	10.30.1.14	DNS	75	Standard query 0x5d3e A mail.google.com
296	9.451266	10.30.7.191	10.30.1.14	DNS	75	Standard query 0xa080 HTTPS mail.google.com
298	9.451485	10.30.1.14	10.30.7.191	DNS	91	Standard query response 0x5d3e A mail.google.com A 142.250.76.197

Frame 186: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{289F60B3-7883-408D-842C-44FF5C8F0AA}, id 0
 Ethernet II, Src: HewlettP_87:79:93 (84:a9:3e:87:79:93), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
 Internet Protocol Version 4, Src: 10.30.7.191, Dst: 10.30.1.13
 User Datagram Protocol, Src Port: 51731, Dst Port: 53
 Domain Name System (query)
 Transaction ID: 0x0004
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 > umass.edu: type NS, class IN
 [Response In: 187]

Wireshark capture of a DNS response. The packet list shows a response from 10.30.1.13 to 10.30.7.191. The packet details pane shows the response for 'umass.edu' type NS, class IN. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
186	6.963662	10.30.7.191	10.30.1.13	DNS	69	Standard query 0x0004 NS umass.edu
187	6.964501	10.30.1.13	10.30.7.191	DNS	171	Standard query response 0x0004 NS umass.edu NS ns3.umass.edu NS ns2.umass.edu NS ns1.umass.edu A 69.16.40.18
295	9.450470	10.30.7.191	10.30.1.14	DNS	75	Standard query 0x5d3e A mail.google.com

Frame 187: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface \Device\NPF_{289F60B3-7883-408D-842C-44FF5C8F0AA}, id 0
 Ethernet II, Src: Cisco_58:32:00 (c8:f9:f9:58:32:00), Dst: HewlettP_87:79:93 (84:a9:3e:87:79:93)
 Internet Protocol Version 4, Src: 10.30.1.13, Dst: 10.30.7.191
 User Datagram Protocol, Src Port: 53, Dst Port: 51731
 Domain Name System (response)
 Transaction ID: 0x0004
 Flags: 0x0100 Standard query response, No error
 Questions: 1
 Answer RRs: 3
 Authority RRs: 0
 Additional RRs: 3
 Queries
 > umass.edu: type NS, class IN
 Answers
 > 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
 Additional records
 > ns3.umass.edu: type A, class IN, addr 69.16.40.18
 > ns2.umass.edu: type A, class IN, addr 128.119.10.28
 > ns1.umass.edu: type A, class IN, addr 128.119.10.27
 [Request In: 186]
 [Time: 0.000839000 seconds]

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

Ans: IP Address : 10.30.1.13 It is a local DNS Server.

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

It contains 1 question and 0 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? It contains 3 answers. It contained the name,type,class and browser name address. It also contains additional information about authoritative server information and their IP Address.

3. Implement a DNS server in packet tracer and understand how it works.

The screenshot displays two windows from the Packet Tracer application. The top window, titled 'PC0', shows the 'Desktop' tab with a 'Web Browser' application. The browser's address bar contains 'http://www.janakar.com', and the page content displays 'you are visiting www.janakar.com'. The bottom window, titled 'Server0', shows the 'Services' tab. On the left, a list of services includes HTTP, DHCP, DHCPv6, TFTP, DNS (highlighted), SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'DNS' and shows the 'DNS Service' is turned 'On'. Under 'Resource Records', a record is configured with 'Name' as 'www.janakar.com', 'Type' as 'A Record', and 'Address' as '192.168.1.1'. Below this, there are 'Add', 'Save', and 'Remove' buttons. A table at the bottom lists the configured record:

No.	Name	Type	Detail
0	www.janakar.com	A Record	192.168.1.1

Physical Config Services **Desktop** Programming AttributesIP Configuration ×

IP Configuration

☐ DHCP☒ Static

IPv4 Address

192.168.1.1

Subnet Mask

255.255.255.0

Default Gateway

0.0.0.0

DNS Server

192.168.1.1

IPv6 Configuration

☐ Automatic☒ Static

IPv6 Address

 /

Link Local Address

FE80::201:63FF:FEC1:C88A

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication

MD5

Username

Password

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 192.168.1.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::206:2AFF:FE75:B4A3

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

PC

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

File Name: index.html

```
<html>
you are visiting www.janakar.com
</html>
```