

Lab5: Dns Wireshark

MD. Abu Bakar Siddique

Roll: 47

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

```
Microsoft Windows [Version 10.0.19045.6332]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ASUS>nslookup www.iitb.ac.in
Server:    connectivity-check.warp-svc
Address:   127.0.2.2

Non-authoritative answer:
Name:      www.iitb.ac.in
Address:   103.21.124.133
```

of www.iitb.ac.in

Ans: The IP address for **www.iitb.ac.in** is **103.21.124.133**.

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

Ans: **127.0.2.2**

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

Ans: The answer came from a **non-authoritative server**

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?

```
C:\Users\User>nslookup -type=NS iitb.ac.in
Server:  dns.google
Address:  8.8.8.8

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
```

```
C:\Users\User>nslookup dns3.iitb.ac.in
Server:  dns.google
Address:  8.8.8.8

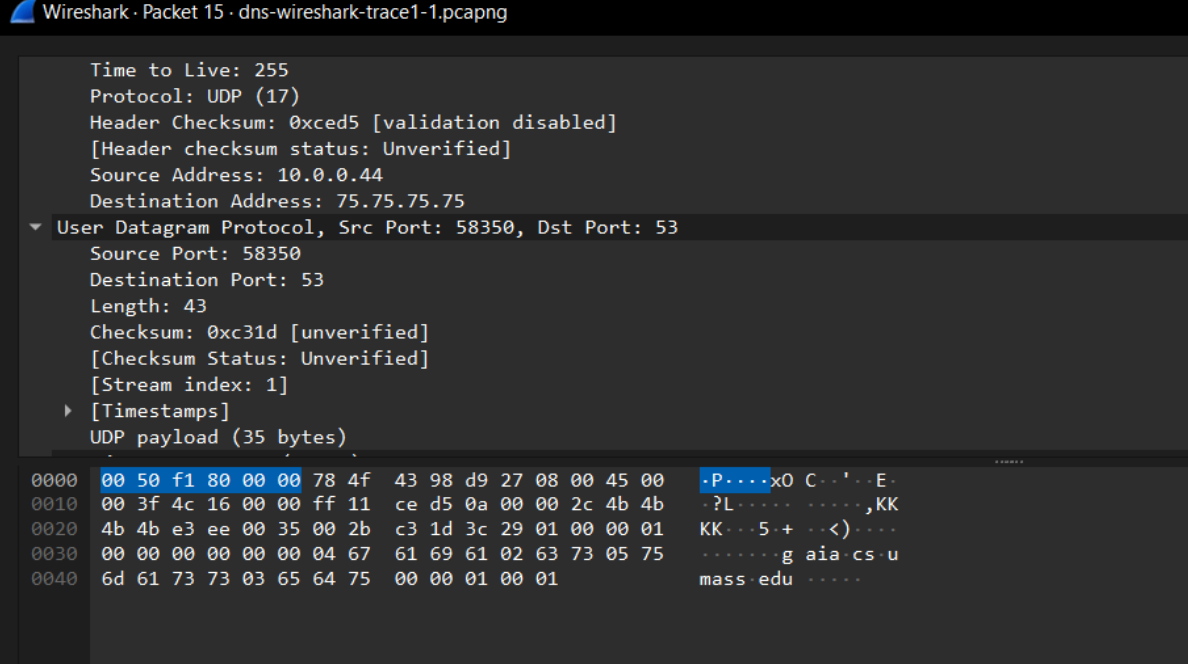
Non-authoritative answer:
Name:     dns3.iitb.ac.in
Address:  103.21.127.129
```

Ans: dns3.iitb.ac.in

Name: dns3.iitb.ac.in

Address: 103.21.127.129

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?



The image shows a Wireshark packet capture window titled "Wireshark · Packet 15 · dns-wireshark-trace1-1.pcapng". The packet list on the left shows packet 15 selected. The packet details pane on the right shows the structure of the packet:

- Time to Live: 255
- Protocol: UDP (17)
- Header Checksum: 0xcd5 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.0.0.44
- Destination Address: 75.75.75.75
- User Datagram Protocol, Src Port: 58350, Dst Port: 53
 - Source Port: 58350
 - Destination Port: 53
 - Length: 43
 - Checksum: 0xc31d [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 1]
 - [Timestamps]
 - UDP payload (35 bytes)

The packet bytes pane at the bottom shows the raw data of the packet, with the first 12 bytes highlighted in blue. The ASCII representation on the right shows the query for "gaia.cs.umass.edu".

Ans: packet number 15. And it's UDP.

6. Now locate the corresponding DNS response to the initial DNS query. What is the

dns					
No	Time	Source	Destination	Protocol	Length Info
15	0.001598	10.0.0.44	75.75.75.75	DNS	77 Standard query 0x3c29 A gaia.cs.umass.edu
17	0.002369	75.75.75.75	10.0.0.44	DNS	93 Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
30	0.003230	10.0.0.44	75.75.75.75	DNS	83 Standard query 0xed4a A maxcdn.bootstrapcdn.com
31	0.001122	10.0.0.44	75.75.75.75	DNS	79 Standard query 0xb079 A ajax.googleapis.com
35	0.011365	75.75.75.75	10.0.0.44	DNS	135 Standard query response 0xed4a A maxcdn.bootstrapcdn.com CNAME cds.j392r3p6.hwcdn.net A 209.197.3.15
36	0.003857	75.75.75.75	10.0.0.44	DNS	95 Standard query response 0xb079 A ajax.googleapis.com A 172.217.12.202
521	0.004452	10.0.0.44	75.75.75.75	DNS	75 Standard query 0xdcf4 A www.pearson.com
522	0.000165	10.0.0.44	75.75.75.75	DNS	79 Standard query 0xb436 A www.vitalsource.com
523	0.000205	10.0.0.44	75.75.75.75	DNS	72 Standard query 0xd3a3 A redshelf.com
526	0.003560	75.75.75.75	10.0.0.44	DNS	169 Standard query response 0xdcf4 A www.pearson.com CNAME wildcard.pearson.com.edgekey.net CNAME e290.x.akamaiedge.net A 2
527	0.002719	10.0.0.44	75.75.75.75	DNS	74 Standard query 0xe1a9 A www.amazon.com
528	0.005069	75.75.75.75	10.0.0.44	DNS	159 Standard query response 0xb436 A www.vitalsource.com A 104.17.67.241 A 104.17.65.241 A 104.17.68.241 A 104.17.69.241 A
529	0.001252	75.75.75.75	10.0.0.44	DNS	88 Standard query response 0xd3a3 A redshelf.com A 34.196.10.62
530	0.013188	75.75.75.75	10.0.0.44	DNS	169 Standard query response 0xe1a9 A www.amazon.com CNAME tp.47cf2c89-frontier.amazon.com CNAME d3ag4hukh62yn.cloudfront.
541	0.001493	10.0.0.44	75.75.75.75	DNS	96 Standard query 0x6cf4 A ss-prod-u01-notif-63.aws.adobess.com
542	0.016709	75.75.75.75	10.0.0.44	DNS	144 Standard query response 0x6cf4 A ss-prod-u01-notif-63.aws.adobess.com A 52.205.134.231 A 52.20.111.22 A 3.213.114.154

▶ Frame 17: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0
 ▶ Ethernet II, Src: Maxlinxar_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
 ▶ Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 58350
 Source Port: 53
 Destination Port: 58350
 Length: 59
 Checksum: 0x4af2 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 1]
 [Timezone]
 UDP payload (51 bytes)

0000	78 4f 43 98 d9 27 50 00	f1 80 00 00 00 00 45 00	x0c 00 00 00 00 00 00 00	E
0010	00 4f 00 00 40 00 3a 11	9f dc 4b 4b 4b 4b 0a 00	0 0 0 0 0 0 0 0	0
0020	00 2c 00 75 e3 ee 36 3a	f2 c3 29 81 80 00 00 01	0 0 0 0 0 0 0 0	0
0030	00 01 00 00 00 00 04 67	61 69 61 62 63 72 05 75	0 0 0 0 0 0 0 0	0
0040	6d 61 73 73 03 65 64 75	00 00 00 01 01 c0 0c 00	0 0 0 0 0 0 0 0	0
0050	01 00 01 00 00 54 60 80	04 80 77 f5 0c	0 0 0 0 0 0 0 0	0

Q7.What is the destination port for the DNS query message? What is the source port of the DNS response message?

Source Port: 53

```

▶ Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinear_80:00:00 (00:50:f1:80:00:00)
  ▶ Destination: Maxlinear_80:00:00 (00:50:f1:80:00:00)
  ▶ Source: Apple_98:d9:27 (78:4f:43:98:d9:27)
  Type: IPv4 (0x0800)
  [Stream index: 3]
▶ Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)

```

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

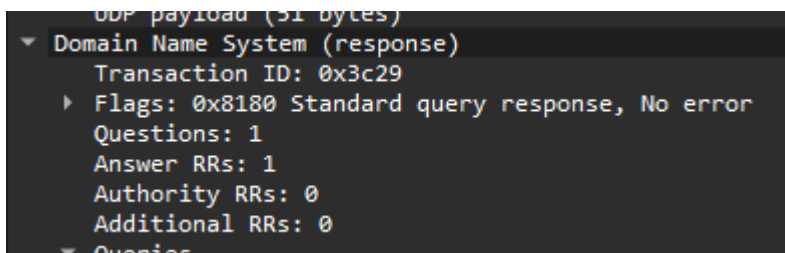
```

    ... payload (25 bytes)
  ▾ Domain Name System (query)
    Transaction ID: 0x3c29
    ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 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: Questions 1, Answers 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.

A) 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/?

Time	Source	Destination	Protocol	Length	Info
22	3.367054	10.0.0.44	128.119.245.12	HTTP	831 GET /kurose_ross/ HTTP/1.1
28	3.395005	128.119.245.12	10.0.0.44	HTTP	857 HTTP/1.1 200 OK (text/html)
205	3.570142	10.0.0.44	128.119.245.12	HTTP	817 GET /kurose_ross/header_graphic_book_8E_2.jpg
516	3.670350	128.119.245.12	10.0.0.44	HTTP	454 HTTP/1.1 200 OK (JPEG JFIF image)
520	3.673776	10.0.0.44	128.119.245.12	HTTP	788 GET /favicon.ico HTTP/1.1
524	3.692288	128.119.245.12	10.0.0.44	HTTP	550 HTTP/1.1 404 Not Found (text/html)

Ans: **22**

B) 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?

Ans: **15**

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

Ans: **17**

D) 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?

Ans: **205**

E) 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?

Ans: New Dns query not made

F) Discuss how DNS caching affects the answer to this last question

Ans: **Without caching:** Every HTTP request to a hostname may require a DNS query + response.

With caching (normal case): Only the first request requires DNS resolution; subsequent requests reuse the cached IP.

This is why, in most student traces, you will see **only one DNS query/response pair** for gaia.cs.umass.edu, even though two different HTTP objects are retrieved.

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

Ans: **53, 53**

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

Ans: **75.75.75.755, which is the IP address of the system's default local DNS server.**

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

```
[Time since previous frame: 0.00000000 seconds]
UDP payload (34 bytes)
✓ Domain Name System (query)
  Transaction ID: 0x609b
  ✓ 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
    ✓ www.cs.umass.edu: type A, class IN
      Name: www.cs.umass.edu
      [Name Length: 16]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  [Response In: 20]
```

Ans: **The type of DNS query is A (Address record) (IPv4) and query message does not contain any answers**

15. Examine the DNS response message to the query message. How many

“questions” does this DNS response message contain? How many “answers”?

```
Domain Name System (response)
  Transaction ID: 0x609b
  ▸ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▸ Queries
```

Ans: 1, 1

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

dns						
No.	Time	Source	Destination	Protocol	Length	Info
13	3.425869	10.0.0.44	75.75.75.75	DNS	69	Standard query 0x6683
14	3.450501	75.75.75.75	10.0.0.44	DNS	171	Standard query response

Ans: 75.75.75.75, which is the IP address of 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”?

```
Domain Name System (query)
  Transaction ID: 0x6683
  ▸ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▸ Queries
```

Ans: 1, 0

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?

```
Domain Name System (response)
  Transaction ID: 0x6683
  ▸ Flags: 0x8180 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 ns1.umass.edu
    ▸ umass.edu: type NS, class IN, ns ns3.umass.edu
    ▸ umass.edu: type NS, class IN, ns ns2.umass.edu
  ▸ Additional records
    ▸ ns2.umass.edu: type A, class IN, addr 128.119.10.28
    ▸ ns1.umass.edu: type A, class IN, addr 128.119.10.27
    ▸ ns3.umass.edu: type A, class IN, addr 128.103.38.68
  [Request In: 13]
  [Time: 0.024632000 seconds]
```

Ans:

3,

The answers contain the names of the authoritative name servers for the umass.edu domain:

ns1.umass.edu

ns2.umass.edu

[ns3.umass.edu](#)

The response returns 3 additional resource records. These records provide the IP addresses for the name servers listed in the answers, specifically

ns2.umass.edu

ns1.umass.edu

ns3.umass.edu