

Lab 03

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?

```
C:\Users\DELL>nslookup tuoitre.vn
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     tuoitre.vn
Address:  14.225.199.147
```

The IP address of this server: 14.225.199.147

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

```
C:\Users\DELL>nslookup -type=NS www.rca.ac.uk
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
www.rca.ac.uk    canonical name = www.rca.ac.uk.cdn.cloudflare.net

cloudflare.net
    primary name server = ns1.cloudflare.net
    responsible mail addr = dns.cloudflare.com
    serial      = 2323811511
    refresh     = 10000 (2 hours 46 mins 40 secs)
    retry       = 2400 (40 mins)
    expire      = 604800 (7 days)
    default TTL = 1800 (30 mins)
```

the authoritative DNS servers: ns1.cloudflare.net

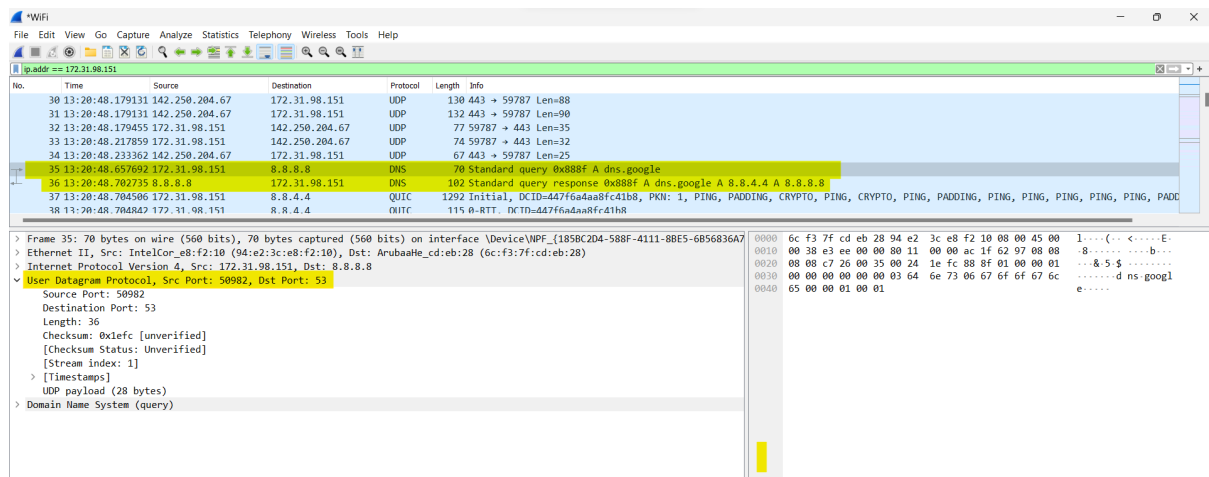
3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
C:\Users\DELL>nslookup rca.ac.uk mail.yahoo.com
Server: e2.ycpi.vip.hkb.yahoo.com
Address: 180.222.116.12

Non-authoritative answer:
Name: rca.ac.uk
Address: 89.106.200.1
```

It's IP address: 89.106.200.1

4. Locate the DNS query and response messages. Are then sent over UDP or TCP? UDP



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

✓ User Datagram Protocol, Src Port: 50982, Dst Port: 53

Source Port: 50982
Destination Port: 53

Length: 36
Checksum: 0x1efc [unverified]
[Checksum Status: Unverified]
[Stream index: 1]

> [Timestamps]
UDP payload (28 bytes)

Destination Port: 53

Source Port: 50982

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query was sent to IP address: 8.8.8.8

IP address of my local DNS server: 8.8.8.8

These two IP addresses are the same.

*WiFi							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
ip.addr == 172.31.98.151							
No.	Time	Source	Destination	Protocol	Length	Info	
33	13:20:48.217859	172.31.98.151	142.250.204.67	UDP	74	59787 → 443 Len=32	
34	13:20:48.233362	142.250.204.67	172.31.98.151	UDP	67	443 → 59787 Len=25	
35	13:20:48.657692	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x888f A dns.google	
36	13:20:48.702735	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0x888f A dns.google A 8.8.4.4 A 8.8.8.8	
37	13:20:48.704506	172.31.98.151	8.8.4.4	QUIC	1292	Initial, DCID=447f6a4aa8fc41b8, PKN: 1, PING, PADDING, CRYPTO, PING, C	
38	13:20:48.704842	172.31.98.151	8.8.4.4	QUIC	115	0-RTT, DCID=447f6a4aa8fc41b8	
39	13:20:48.705174	172.31.98.151	8.8.4.4	QUIC	288	0-RTT, DCID=447f6a4aa8fc41b8	
40	13:20:48.748891	8.8.4.4	172.31.98.151	QUIC	1292	Protected Payload (KP0)	
41	13:20:48.748986	8.8.4.4	172.31.98.151	QUIC	845	Protected Payload (KP0)	

Wireless LAN adapter WiFi:

```
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wireless-AC 9462
Physical Address. . . . . : 94-E2-3C-E8-F2-10
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6895:54fc:4298:ee12%5(Preferred)
IPv4 Address. . . . . : 172.31.98.151(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : 31 October 2023 09:09:24
Lease Expires . . . . . : 02 November 2023 01:04:48
Default Gateway . . . . . : 172.31.98.1
DHCP Server . . . . . : 172.31.98.1
DHCPv6 IAID . . . . . : 76866108
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-90-9C-92-60-18-95-4B-C7-D1
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled
```

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

Type” of DNS query was A.

The query message did not contain any “answers”.

```
✓ Domain Name System (query)
  Transaction ID: 0x888f
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ✓ Queries
    > dns.google: type A, class IN
    [Response In: 36]
```

8. Examine the DNS **response message**. How many “answers” are provided? What do each of these answers contain?

Two answers are provided. They contain the information for www.ietf.org:

The screenshot shows a Wireshark capture of a DNS response. The packet list pane shows two DNS packets: a query (No. 35) and a response (No. 36). The packet details pane for packet 36 shows the DNS response structure, including the transaction ID (0x888f), flags, and two answer records. The first answer record is for 'dns.google' with IP address 8.8.4.4, and the second is for 'dns.google' with IP address 8.8.8.8. The packet bytes pane shows the raw data of the response.

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The destination IP address of the SYN packet correspond is 172.31.98.151

Yes, it is the IP address for www.ietf.org

The screenshot shows a Wireshark capture of a TCP SYN packet. The packet list pane shows a list of packets, including a SYN packet (No. 55) with destination IP 172.31.98.151. The packet details pane for packet 55 shows the TCP header information, including the source port (443) and destination port (60958). The packet bytes pane shows the raw data of the SYN packet.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No. It uses the answer from the DNS response
ignore the first two sets of queries/responses.

The screenshot shows a Wireshark capture of DNS queries. The packet list pane shows a list of DNS packets, including queries for 'www.mit.edu' (No. 73) and 'www.mit.edu' (No. 74). The packet details pane for packet 73 shows the DNS query structure, including the transaction ID (0x0002) and the query name ('www.mit.edu'). The packet bytes pane shows the raw data of the query.

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

The destination port for the DNS query message is 53.

No.	Time	Source	Destination	Protocol	Length	Info
10	14:17:48.597610	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x84d1 A dns.google
11	14:17:48.639944	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0x84d1 A dns.google A 8.8.4.4 A 8.8.8.8
71	14:17:51.920651	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
72	14:17:51.962408	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
73	14:17:51.963771	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
74	14:17:52.199573	8.8.8.8	172.31.98.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net
75	14:17:52.202609	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
76	14:17:52.262465	8.8.8.8	172.31.98.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net

> Frame 73: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A7}	0000	6c f3 7f cd eb 28
> Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaHe_cd:eb:28 (6c:f3:7f:cd:eb:28)	0010	00 39 f4 4d 00 00
> Internet Protocol Version 4, Src: 172.31.98.151, Dst: 8.8.8.8	0020	08 08 fe 79 00 35
> User Datagram Protocol, Src Port: 52857, Dst Port: 53	0030	00 00 00 00 00 00
> Domain Name System (query)	0040	64 75 00 00 01 00

The source port of DNS response messages is 53.

No.	Time	Source	Destination	Protocol	Length	Info
10	14:17:48.597610	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x84d1 A dns.google
11	14:17:48.639944	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0x84d1 A dns.google A 8.8.4.4 A 8.8.8.8
71	14:17:51.920651	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
72	14:17:51.962408	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
73	14:17:51.963771	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
74	14:17:52.199573	8.8.8.8	172.31.98.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net
75	14:17:52.202609	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
76	14:17:52.262465	8.8.8.8	172.31.98.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net

> Frame 74: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A7}	0000	94 e2 3c e8 f2 10
> Ethernet II, Src: ArubaHe_cd:eb:28 (6c:f3:7f:cd:eb:28), Dst: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10)	0010	00 92 ef a9 00 00
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.31.98.151	0020	62 97 00 35 ce 79
> User Datagram Protocol, Src Port: 53, Dst Port: 52857	0030	00 03 00 00 00 00
> Domain Name System (response)	0040	64 75 00 00 01 00
	0050	ef 00 19 03 77 77

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

The DNS query message sent to IP address: 8.8.8.8

Yes. The IP address of my default local DNS server also is 8.8.8.8

No.	Time	Source	Destination	Protocol	Length	Info
10	14:17:48.597610	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x84d1 A dns.google
11	14:17:48.639944	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0x84d1 A dns.google A 8.8.4.4 A 8.8.8.8
71	14:17:51.920651	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
72	14:17:51.962408	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
73	14:17:51.963771	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
74	14:17:52.199573	8.8.8.8	172.31.98.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net
75	14:17:52.202609	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
76	14:17:52.262465	8.8.8.8	172.31.98.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net

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

Type” of DNS query was A.

The query message did not contain any “answers”.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
10	14:17:48.597610	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x84d1 A dns.google
11	14:17:48.639944	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0x84d1 A dns.google A 8.8.4.4
71	14:17:51.920651	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
72	14:17:51.962408	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa
73	14:17:51.963771	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
74	14:17:52.199573	8.8.8.8	172.31.98.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.50.16.12
75	14:17:52.202609	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
76	14:17:52.262465	8.8.8.8	172.31.98.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2001:ee0:3240:8...

> Internet Protocol Version 4, Src: 172.31.98.151, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 52857, 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

▼ www.mit.edu: type A, class IN

Name: www.mit.edu

[Name Length: 11]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 74]

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Three answers are provided. They contain the information for www.mit.edu:

10	14:17:48.597610	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x84d1 A dns.google
11	14:17:48.639944	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0x84d1 A dns.google A 8.8.4.4 A 8.8.8.8
71	14:17:51.920651	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
72	14:17:51.962408	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
73	14:17:51.963771	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
74	14:17:52.199573	8.8.8.8	172.31.98.151	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.50.16.12
75	14:17:52.202609	172.31.98.151	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
76	14:17:52.262465	8.8.8.8	172.31.98.151	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2001:ee0:3240:8...

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.mit.edu: type A, class IN

▼ Answers

▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

Name: www.mit.edu

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 1519 (25 minutes, 19 seconds)

Data length: 25

CNAME: www.mit.edu.edgekey.net

▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

Name: www.mit.edu.edgekey.net

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 60 (1 minute)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

▼ e9566.dscb.akamaiedge.net: type A, class IN, addr.23.50.16.12

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 23.50.16.12

[Request In: 73]

[Time: 0.235802000 seconds]

0000 94 e2 3c e8 f2 10 6c f3 7f cd eb 28 08 00 45 20 ...<...l. ...E
0010 00 92 ef a9 00 00 09 11 42 cb 08 08 08 ac 1f ...<...l. B.....
0020 62 97 00 35 ce 79 00 7e 3d 00 00 02 81 00 00 01 b-5-y-w-.....
0030 00 03 00 00 00 00 03 77 77 03 6d 69 74 03 65w ww-mit-e
0040 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 05
0050 ef 03 19 03 77 77 03 6d 69 74 03 65 64 75 07 ..www- mit-edu-
0060 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05 edgekey- net-)-<..
0070 00 01 00 00 00 3c 00 18 05 65 39 35 36 36 04 64<...e9566-d
0080 73 63 62 0a 61 6b 61 6d 61 69 65 64 67 65 c0 3d scb-akam aiedge=-
0090 c0 4e 00 01 00 01 00 00 00 14 00 04 17 32 10 0c -N-.....2..

15. Screenshot

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 IP address: 8.8.8.8

IP address of my local DNS server: 8.8.8.8

*WiFi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
dns						
No.	Time	Source	Destination	Protocol	Length	Info
48	15:30:45.340179	172.31.98.151	8.8.8.8	DNS	70	Standard query 0xbdd3 A dns.google
49	15:30:45.340349	172.31.98.151	8.8.8.8	DNS	70	Standard query 0x8f8d HTTPS dns.google
50	15:30:45.391716	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0xbdd3 A dns.google A 8.8.8.8 A 8.8.4.4
51	15:30:45.391865	8.8.8.8	172.31.98.151	DNS	146	Standard query response 0x8f8d HTTPS dns.google SOA ns1.zdns.google
751	15:30:50.486529	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
753	15:30:50.528885	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
754	15:30:50.531787	172.31.98.151	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
755	15:30:50.575542	8.8.8.8	172.31.98.151	DNS	234	Standard query response 0x0002 NS mit.edu NS use2.akam.net NS use5.akam.net

```

Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>nslookup -type=NS mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-173.akam.net

C:\Users\DELL>

```

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

Type” of DNS query was NS.

The query message did not contain any “answers”.

- ✓ Domain Name System (query)
 - Transaction ID: 0x0002
 - > Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - ✓ Queries
 - ✓ mit.edu: type NS, class IN
 - Name: mit.edu
 - [Name Length: 7]
 - [Label Count: 2]
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)
 - [\[Response In: 755\]](#)

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

The response message provides 8 MIT nameservers.

The response message does not also provide the IP address of the nameservers.

The image shows a Wireshark capture of a DNS transaction. The top pane displays a list of packets, with packet 755 selected, which is a DNS response from 172.31.98.151 to 8.8.8.8. The middle pane shows the details of this packet, highlighting the 'Domain Name System (response)' section. The 'Queries' section shows a query for 'mit.edu' of type NS and class IN. The 'Answers' section lists eight nameservers for 'mit.edu': use2.akam.net, use5.akam.net, ns1-173.akam.net, asia2.akam.net, usw2.akam.net, ns1-37.akam.net, asia1.akam.net, and eur5.akam.net. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
48	15:30:45.340179	172.31.98.151	8.8.8.8	DNS	70	Standard query 0xbdd3 A dns.google
49	15:30:45.340349	172.31.98.151	8.8.8.8	DNS	70	Standard query 0xbdd3 A dns.google
50	15:30:45.391716	8.8.8.8	172.31.98.151	DNS	102	Standard query response 0xbdd3 A dns.google A 8.8.8.8 A 8.8.4.4
51	15:30:45.391865	8.8.8.8	172.31.98.151	DNS	146	Standard query response 0xbdd3 A dns.google SOA ns1.zdns.google
751	15:30:50.486529	172.31.98.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
753	15:30:50.528885	8.8.8.8	172.31.98.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
754	15:30:50.531787	172.31.98.151	8.8.8.8	DNS	67	Standard query 0x0002 NS mit.edu
755	15:30:50.575542	8.8.8.8	172.31.98.151	DNS	234	Standard query response 0x0002 NS mit.edu NS use2.akam.net NS use5.akam.net M

Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x8100 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 0

Queries

- mit.edu: type NS, class IN
 - Name: mit.edu
 - [Name Length: 7]
 - [Label Count: 2]
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)

Answers

- mit.edu: type NS, class IN, ns use2.akam.net
- mit.edu: type NS, class IN, ns use5.akam.net
- mit.edu: type NS, class IN, ns ns1-173.akam.net
- mit.edu: type NS, class IN, ns asia2.akam.net
- mit.edu: type NS, class IN, ns usw2.akam.net
- mit.edu: type NS, class IN, ns ns1-37.akam.net
- mit.edu: type NS, class IN, ns asia1.akam.net
- mit.edu: type NS, class IN, ns eur5.akam.net

[Request In: 754]

[Time: 0.043755000 seconds]

19. Screenshot

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The DNS query was sent to IP address: 8.8.8.8

IP address of my local DNS server: 8.8.8.8

Wireshark interface showing a DNS query packet (No. 1) sent to 8.8.8.8. The packet details show a Standard query for bitsy.mit.edu. The packet bytes are displayed on the right.

No.	Time	Source	Destination	Protocol	Length	Info
1	16:42:30.873709	172.31.98.151	8.8.8.8	DNS	73	Standard query 0xb291 A bitsy.mit.edu
2	16:42:30.973807	8.8.8.8	172.31.98.151	DNS	89	Standard query response 0xb291 A bitsy.mit.edu A 18.0.72.3
3	16:42:30.977898	172.31.98.151	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
4	16:42:32.989780	172.31.98.151	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
5	16:42:34.987831	172.31.98.151	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A739C}, Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28)
Internet Protocol Version 4, Src: 172.31.98.151, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 55347, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xb291
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
bitsy.mit.edu: type A, class IN
[Response In: 2]

0000 6c f3 7f cd eb
0010 00 3b 09 06 00
0020 08 08 d8 33 00
0030 00 00 00 00 00
0040 03 65 64 75 00

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

Type” of DNS query was A.

The query message did not contain any “answers”.

Wireshark interface showing a DNS query packet (No. 1) sent to 8.8.8.8. The packet details show a Standard query for bitsy.mit.edu. The packet bytes are displayed on the right.

No.	Time	Source	Destination	Protocol	Length	Info
1	16:42:30.873709	172.31.98.151	8.8.8.8	DNS	73	Standard query 0xb291 A bitsy.mit.edu
2	16:42:30.973807	8.8.8.8	172.31.98.151	DNS	89	Standard query response 0xb291 A bitsy.mit.edu A 18.0.72.3
3	16:42:30.977898	172.31.98.151	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
4	16:42:32.989780	172.31.98.151	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
5	16:42:34.987831	172.31.98.151	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A739C}, Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28)
Internet Protocol Version 4, Src: 172.31.98.151, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 55347, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xb291
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
bitsy.mit.edu: type A, class IN
[Response In: 2]

0000 6c f3 7f cd eb
0010 00 3b 09 06 00
0020 08 08 d8 33 00
0030 00 00 00 00 00
0040 03 65 64 75 00

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

One answer is provided. They contain the information for bitsy.mit.edu:

The screenshot shows a Wireshark packet capture of DNS traffic. The packet list at the top shows five packets. Packet 2 is a DNS response from 8.8.8.8 to 172.31.98.151. The packet details pane on the right shows the structure of the response, including the answer for bitsy.mit.edu with IP 18.0.72.3.

No.	Time	Source	Destination	Protocol	Length	Info
1	16:42:30.873709	172.31.98.151	8.8.8.8	DNS	73	Standard query 0xb291 A bitsy.mit.edu
2	16:42:30.973807	8.8.8.8	172.31.98.151	DNS	89	Standard query response 0xb291 A bitsy.mit.edu A 18.0.72.3
3	16:42:30.977898	172.31.98.151	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
4	16:42:32.989780	172.31.98.151	18.0.72.3	DNS	74	Standard query 0x0002 A www.aait.or.kr
5	16:42:34.987831	172.31.98.151	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aait.or.kr

Frame 2: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A739C}, Ethernet II, Src: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28), Dst: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.31.98.151
User Datagram Protocol, Src Port: 53, Dst Port: 55347
Domain Name System (response)
Transaction ID: 0xb291
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
bitsy.mit.edu: type A, class IN
Answers
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
[Request In: 1]
[Time: 0.100098000 seconds]

23.Screenshot.

Additional:

24. What is Dynamic DNS? Give a brief introduction about Dynamic DNS? Why do we need Dynamic DNS?

- Dynamic DNS, also known as Dynamic Domain Name System (DDNS), is a system that enables devices with dynamic IP addresses to be accessed easily using a domain name.
- A brief introduction about Dynamic DNS:**
In a typical scenario, internet service providers (ISPs) assign dynamic IP addresses to their customers, which means that the IP address can change over time. However, most internet resources, such as websites or servers, are usually accessed using domain names.
- We need Dynamic DNS because:**
Dynamic DNS solves the problem of accessing devices with changing IP addresses by dynamically updating the IP address associated with a domain name. It works by running a piece of software or using a router that periodically communicates with a DDNS provider, notifying it of any IP address changes. The DDNS provider then updates the DNS records for the associated domain name, ensuring it points to the correct IP address.

25. List out some (at least 5) popular Dynamic DNS providers. Briefly compare them

Here are five popular Dynamic DNS providers:

1. **DynDNS:** DynDNS, now called Dyn, is one of the oldest and well-known dynamic DNS providers. It offers a range of services and features, including various DNS update methods, multiple domain support, and advanced security options. However, some of its services may require a paid subscription.
2. **No-IP:** No-IP provides a simple and user-friendly dynamic DNS service. It offers a free plan that allows users to manage up to three domain names and offers various update clients and integrations. No-IP also offers affordable paid plans with additional features and support.
3. **DuckDNS:** DuckDNS is a free dynamic DNS service that focuses on simplicity and ease of use. It doesn't require any account registration and provides a straightforward API for updating DNS records. While it may lack some advanced features, it is a popular choice for basic DDNS needs.
4. **ChangeIP:** ChangeIP offers both free and paid dynamic DNS services. Its free plan includes five hostnames and supports various update protocols. The paid plans provide additional features such as email forwarding, SSL certificates, and extended customer support.
5. **afraid.org:** afraid.org, also known as FreeDNS, is a unique dynamic DNS provider that offers free DDNS services. It allows users to create unlimited subdomains under a wide selection of domain names provided by the service. Although it doesn't offer advanced features like some other providers, it remains popular due to its free and flexible nature.

26. Demonstrate how to use Dynamic DNS:

- **Setup a SIMPLE web server, ftp server or something similar on your machine (host A)**
- **Register and config Dynamic DNS for host A**
- **Use your partner's machine (host B) to access the service running on host A**

