

Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 2b

1. nslookup

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

ANSWER:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>nslookup www.hcmut.edu.vn
Server: cachingdns1.vnpt.vn
Address: 123.23.23.23

Non-authoritative answer:
Name: server04.hcmut.edu.vn
Address: 221.133.13.114
Aliases: www.hcmut.edu.vn
```

IP address of server: 221.133.13.114

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

ANSWER:

```
Administrator: Command Prompt

C:\WINDOWS\system32>nslookup -type=NS www.cam.ac.uk
Server: cachingdns1.vnpt.vn
Address: 123.23.23.23

cam.ac.uk
primary name server = primary.dns.cam.ac.uk
responsible mail addr = hostmaster.cam.ac.uk
serial = 1633957332
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

Authoritative DNS server: primary.dns.cam.ac.uk

Question 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?

ANSWER:

```
C:\WINDOWS\system32>nslookup primary.dns.cam.ac.uk mail.yahoo.com
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: 106.10.236.40

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Request to UnKnown timed-out
```

IP address for Yahoo! mail server: 106.10.236.40

2. ipconfig

3. Tracing DNS with Wireshark

My IP address: 192.168.1.12

```
Administrator: Command Prompt

Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : 5A-5F-99-99-B2-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter
Physical Address. . . . . : 48-5F-99-99-B2-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:ee0:4c1b:ef10:fd25:b749:5292:a2fe(Preferred)
Temporary IPv6 Address. . . . . : 2001:ee0:4c1b:ef10:4828:e04e:8d7c:47da(Preferred)
Link-local IPv6 Address . . . . . : fe80::fd25:b749:5292:a2fe%12(Preferred)
IPv4 Address. . . . . : 192.168.1.12(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 11 Tha'ng Mưo'i 2021 7:41:33 CH
Lease Expires . . . . . : 12 Tha'ng Mưo'i 2021 7:41:32 CH
Default Gateway . . . . . : fe80::1%12
                             192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 55074713
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-C2-9A-CA-6C-2B-59-57-47-C0
DNS Servers . . . . . : 123.23.23.23
                             123.26.26.26
Primary WINS Server . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
```

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

ANSWER:

The DNS query and response message are sent over UDP

The image shows a Wireshark packet capture of a DNS query and response. The top pane shows a list of packets, with packet 178 selected. The middle pane shows the details of the selected packet, which is a DNS Standard query response from 192.168.1.12 to 123.23.23.23. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
152	20:22:51.697123	123.23.23.23	192.168.1.12	DNS	102	Standard query response 0x8e62 AAAA www.google.com AAAA 2404:6800:4005:81c::2004
178	20:22:52.434590	192.168.1.12	123.23.23.23	DNS	72	Standard query 0xf75d A www.ietf.org
179	20:22:52.435220	192.168.1.12	123.23.23.23	DNS	72	Standard query 0xabd7 AAAA www.ietf.org
180	20:22:52.447985	123.23.23.23	192.168.1.12	DNS	149	Standard query response 0xf75d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104...
181	20:22:52.447985	123.23.23.23	192.168.1.12	DNS	173	Standard query response 0xabd7 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::68...
391	20:22:52.971978	192.168.1.12	123.23.23.23	DNS	78	Standard query 0x5818 A analytics.ietf.org
392	20:22:52.972420	192.168.1.12	123.23.23.23	DNS	78	Standard query 0x121e AAAA analytics.ietf.org
396	20:22:52.979941	123.23.23.23	192.168.1.12	DNS	94	Standard query response 0x5818 A analytics.ietf.org A 4.31.198.45
412	20:22:53.036733	123.23.23.23	192.168.1.12	DNS	106	Standard query response 0x121e AAAA analytics.ietf.org AAAA 2001:1900:3001:11::2d
850	20:22:54.036712	192.168.1.12	123.23.23.23	DNS	91	Standard query 0x508a A content-autofill.googleapis.com
851	20:23:54.023336	192.168.1.12	123.23.23.23	DNS	91	Standard query 0x6076 AAAA content-autofill.googleapis.com

> Frame 178: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:b2:1d), Dst: Vnptech_6d:4b:f8 (d4:9a:1a:0d:4b:f8)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 123.23.23.23
v User Datagram Protocol, Src Port: 59015, Dst Port: 53
Source Port: 59015
Destination Port: 53
Length: 38
Checksum: 0xab5f [unverified]
[Checksum Status: Unverified]
[Stream index: 19]
> [Timestamps]
UDP payload (30 bytes)
Domain Name System (query)

```
0000 d4 9a a0 6d 4b f8 48 5f 99 99 b2 1d 00 00 45 00 ...mK_H_.....E
0010 00 3a 7f 1f 00 00 00 11 67 b1 c0 a8 01 0c 7b 17 .....g.....{
0020 17 1e e6 87 00 35 00 26 ab 5f 77 5d 01 00 00 01 .....5&.....]....
0030 30 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf
0040 6f 72 72 00 00 01 00 01 .....org.....
```

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

ANSWER:

The destination port: 53

The source port: 59015

Question 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?

ANSWER:

It's sent to 192.168.1.1, which is the IP address of one of my local DNS servers

```
Administrator: Command Prompt

Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : 5A-5F-99-99-B2-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter
Physical Address. . . . . : 48-5F-99-99-B2-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:ee0:4c1b:ef10:fd25:b749:5292:a2fe(Preferred)
Temporary IPv6 Address. . . . . : 2001:ee0:4c1b:ef10:4828:e04e:8d7c:47da(Preferred)
Link-local IPv6 Address . . . . . : fe80::fd25:b749:5292:a2fe%12(Preferred)
IPv4 Address. . . . . : 192.168.1.12(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 11 Tha'ng Mươ'i 2021 7:41:33 CH
Lease Expires . . . . . : 12 Tha'ng Mươ'i 2021 7:41:32 CH
Default Gateway . . . . . : fe80::1%12
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 55074713
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-C2-9A-CA-6C-2B-59-57-47-C0
DNS Servers . . . . . : 123.23.23.23
                          123.26.26.26
Primary WINS Server . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
```

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

ANSWER:

It's a type A Standard Query and it doesn't contain any answers.

No.	Time	Source	Destination	Protocol	Length	Info
152	20:22:51.697123	123.23.23.23	192.168.1.12	DNS	102	Standard query response 0x8e62 AAAA www.google.com AAAA 2404:6800:4005:81c::2004
178	20:22:52.434590	192.168.1.12	123.23.23.23	DNS	72	Standard query 0xf75d A www.ietf.org
179	20:22:52.435220	192.168.1.12	123.23.23.23	DNS	72	Standard query 0xabd7 AAAA www.ietf.org
180	20:22:52.447985	123.23.23.23	192.168.1.12	DNS	149	Standard query response 0xf75d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104...
181	20:22:52.447985	123.23.23.23	192.168.1.12	DNS	173	Standard query response 0xabd7 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::68...
391	20:22:52.971978	192.168.1.12	123.23.23.23	DNS	78	Standard query 0x5818 A analytics.ietf.org
392	20:22:52.972420	192.168.1.12	123.23.23.23	DNS	78	Standard query 0x121e AAAA analytics.ietf.org
396	20:22:52.979941	123.23.23.23	192.168.1.12	DNS	94	Standard query response 0x5818 A analytics.ietf.org A 4.31.198.45
412	20:22:53.036733	123.23.23.23	192.168.1.12	DNS	106	Standard query response 0x121e AAAA analytics.ietf.org AAAA 2001:1900:3001:11::2d
850	20:22:54.036712	192.168.1.12	123.23.23.23	DNS	91	Standard query 0x508a A content-autofill.googleapis.com
851	20:22:54.037335	192.168.1.12	123.23.23.23	DNS	91	Standard query 0x6076 AAAA content-autofill.googleapis.com

> Frame 178: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
 > Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:b2:1d), Dst: Vnptech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
 > Internet Protocol Version 4, Src: 192.168.1.12, Dst: 123.23.23.23
 > User Datagram Protocol, Src Port: 59015, Dst Port: 53
 > Domain Name System (query)
 Transaction ID: 0xf75d
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 [Response In: 180]

```

0000  d4 9a a0 6d 4b f8 48 5f 99 99 b2 1d 00 00 45 00  ...mK H .....E
0010  00 3a 7f 1f 00 00 80 11 67 b1 c0 a8 01 0c 7b 17  .....g .....{
0020  17 1e e6 87 00 35 00 26 ab 5f f7 54 01 00 00 01  .....5 & .]....
0030  00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03  .....w www.ietf.
0040  6f 72 67 00 00 01 00 01 00 00 00 00 00 00 00 00  ORG.....

```

Domain Name System (dns), 30 byte(s) | Packets: 960 · Displayed: 901 (93.9%) · Dropped: 0 (0.0%) | Profile: Default

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

ANSWER:

There were 3 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address

No.	Time	Source	Destination	Protocol	Length	Info
180	20:22:52.447985	123.23.23.23	192.168.1.12	DNS	149	Standard query response 0xf75d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99

Frame 180: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
 Ethernet II, Src: Vnptech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:b2:1d)
 Internet Protocol Version 4, Src: 123.23.23.23, Dst: 192.168.1.12
 User Datagram Protocol, Src Port: 53, Dst Port: 59015
 Domain Name System (response)
 Transaction ID: 0xf75d
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 3
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.ietf.org: type A, class IN
 Answers
 www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
 www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
 www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
 [Request In: 178]
 [Time: 0.013395000 seconds]

Question 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?

ANSWER:

The first SYN packet was sent to 104.16.44.99 which corresponds to the first IP address provided in the DNS response message.

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

ANSWER:

No

```
Administrator: Command Prompt

C:\WINDOWS\system32>nslookup www.mit.edu
Server: cachingdns1.vnpt.vn
Address: 123.23.23.23

Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2600:1417:a000:795::255e
           2600:1417:a000:7a3::255e
           104.84.170.92
Aliases: www.mit.edu
         www.mit.edu.edgekey.net

C:\WINDOWS\system32>
```

Question 11: What is the destination port for the DNS query message? What is the source port of DNS response message?

ANSWER:

The image shows a Wireshark packet capture of a DNS query and response. The packet list shows a DNS query (Standard query) from 192.168.1.12 to 123.23.23.23. The packet details pane shows the query for www.mit.edu. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
325	20:40:17.036289	123.23.23.23	192.168.1.12	DNS	118	Standard query response 0x0001 PTR 23.23.23.123.in-addr.arpa PTR cachingdns1.vnpt.vn
326	20:40:17.037903	192.168.1.12	123.23.23.23	DNS	71	Standard query 0x0002 A www.mit.edu
327	20:40:17.043506	123.23.23.23	192.168.1.12	DNS	168	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net
328	20:40:17.048176	192.168.1.12	123.23.23.23	DNS	71	Standard query 0x0003 AAAA www.mit.edu
329	20:40:17.053869	123.23.23.23	192.168.1.12	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net
85	20:40:00.120902	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)
88	20:40:03.122810	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)
170	20:40:03.938217	192.168.1.12	123.26.26.26	ICMP	119	Destination unreachable (Port unreachable)
197	20:40:06.122812	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)
337	20:40:18.124776	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)
356	20:40:21.120901	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)

Frame 326: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0

Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)

Internet Protocol Version 4, Src: 192.168.1.12, Dst: 123.23.23.23

User Datagram Protocol, Src Port: 61790, 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

0000 64 9a a0 6d 4b f8 48 5f 99 99 b2 1d 00 00 45 00 ...mK-H.....E

0010 00 39 7f 6f 00 00 00 11 67 62 c0 a0 01 0c 7b 17 ..9o.....pb....{

0020 17 17 f1 52 00 35 00 25 67 80 00 02 01 00 00 01 ...5:5%P.....

0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww/mit e

0040 64 75 00 00 01 00 01 ..du.....

Destination Port: 53
Source Port: 61790

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

ANSWER:

It's sent to 123.23.23.23, which is the IP address of one of my local DNS servers

Question 13: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANSWER:

The query is of type A and it doesn't contain any answers.

Question 14: Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

ANSWER:

The response DNS message contains 3 answer containing the name of the host, the type of address, the class, and the IP address.

```
No.      Time           Source           Destination      Protocol Length Info
 327 20:40:17.043586 123.23.23.23     192.168.1.12     DNS             160      Standard query response 0x0002 A www.mit.edu
CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.84.170.92
Frame 327: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 123.23.23.23, Dst: 192.168.1.12
User Datagram Protocol, Src Port: 53, Dst Port: 61790
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  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
    www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    e9566.dscb.akamaiedge.net: type A, class IN, addr 104.84.170.92
[Request In: 326]
[Time: 0.005683000 seconds]
```

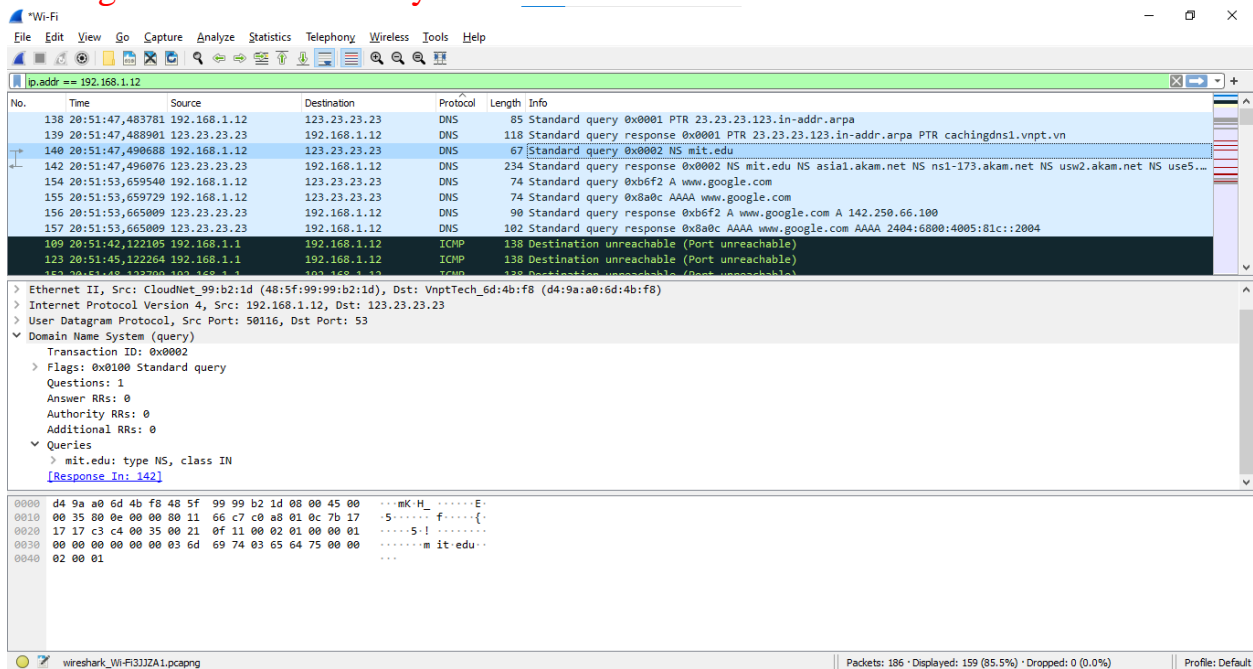
Question 15: Provide a screenshot.

ANSWER:

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

ANSWER:

The DNS query is a type “NS” message including one question. The query message did not contain any answers.



Question 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?

ANSWER:

The nameservers are asia1, ns1-173, usw2, use5, eur5, ns1-37, asia2m use2. We can find their IP addresses as seen below.

```
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 123.23.23.23, Dst: 192.168.1.12
User Datagram Protocol, Src Port: 53, Dst Port: 50116
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  Queries
    mit.edu: type NS, class IN
  Answers
    mit.edu: type NS, class IN, ns asia1.akam.net
    mit.edu: type NS, class IN, ns ns1-173.akam.net
    mit.edu: type NS, class IN, ns usw2.akam.net
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns eur5.akam.net
    mit.edu: type NS, class IN, ns ns1-37.akam.net
    mit.edu: type NS, class IN, ns asia2.akam.net
    mit.edu: type NS, class IN, ns use2.akam.net
  [Request In: 140]
  [Time: 0.005388000 seconds]
```

Question 19: Provide a screenshot.

ANSWER:

The image shows a Wireshark packet capture of network traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of the selected packet (No. 140), including the query and answers sections. The query is for 'mit.edu' and the answers list several IP addresses for 'mit.edu'.

No.	Time	Source	Destination	Protocol	Length	Info
138	20:51:47.483781	192.168.1.12	123.23.23.23	DNS	85	Standard query 0x0001 PTR 23.23.23.123.in-addr.arpa
139	20:51:47.488901	123.23.23.23	192.168.1.12	DNS	118	Standard query response 0x0001 PTR 23.23.23.123.in-addr.arpa PTR cachingdns1.vnpt.vn
140	20:51:47.490688	192.168.1.12	123.23.23.23	DNS	67	Standard query 0x0002 NS mit.edu
142	20:51:47.496076	123.23.23.23	192.168.1.12	DNS	234	Standard query response 0x0002 NS mit.edu NS asia1.akam.net NS ns1-173.akam.net NS usw2.akam.net NS use5...
154	20:51:53.659540	192.168.1.12	123.23.23.23	DNS	74	Standard query 0xb6f2 A www.google.com
155	20:51:53.659729	192.168.1.12	123.23.23.23	DNS	74	Standard query 0x8a0c AAAA www.google.com
156	20:51:53.665009	123.23.23.23	192.168.1.12	DNS	90	Standard query response 0xb6f2 A www.google.com A 142.250.66.100
157	20:51:53.665009	123.23.23.23	192.168.1.12	DNS	102	Standard query response 0x8a0c AAAA www.google.com AAAA 2404:6800:4005:81c::2004
109	20:51:42.122105	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)
123	20:51:45.122264	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)
163	20:51:45.133200	192.168.1.1	192.168.1.12	ICMP	138	Destination unreachable (Port unreachable)

Queries:
mit.edu: type NS, class IN

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

[Request In: 140]
[Time: 0.005388000 seconds]

The image shows a Windows Command Prompt window with the following output:

```
C:\WINDOWS\system32>nslookup www.ait.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out
```

Question 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?

ANSWER:

The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

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

ANSWER:

The screenshot shows a Wireshark packet capture of a DNS standard query response. The packet list pane shows a list of packets, with packet 66 selected. The packet details pane shows the structure of the DNS message, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (query) header. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
32	21:01:17.914378	123.23.23.23	192.168.1.12	DNS	158	Standard query response 0xb147 A dcg.microsoft.com CNAME dcg.microsoft.com.b-0005.b-msedge.net CNAME b-00...
33	21:01:17.914913	192.168.1.12	123.23.23.23	DNS	77	Standard query 0x66c7 AAAA dcg.microsoft.com
34	21:01:17.920406	123.23.23.23	192.168.1.12	DNS	189	Standard query response 0x66c7 AAAA dcg.microsoft.com CNAME dcg.microsoft.com.b-0005.b-msedge.net CNAME b...
66	21:01:19.747462	192.168.1.12	123.23.23.23	DNS	73	Standard query 0xb167 A bitsy.mit.edu
67	21:01:19.747910	192.168.1.12	123.23.23.23	DNS	73	Standard query 0xb5b0 AAAA bitsy.mit.edu
68	21:01:19.753652	123.23.23.23	192.168.1.12	DNS	138	Standard query response 0xb5b0 AAAA bitsy.mit.edu SOA use2.akam.net
69	21:01:19.753652	123.23.23.23	192.168.1.12	DNS	89	Standard query response 0xb167 A bitsy.mit.edu A 18.0.72.3
70	21:01:19.756742	192.168.1.12	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
78	21:01:21.759085	192.168.1.12	18.0.72.3	DNS	74	Standard query 0x0002 A www.ait.or.kr
97	21:01:23.760789	192.168.1.12	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.ait.or.kr

Packet 66 details:

- Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
- Internet Protocol Version 4, Src: 192.168.1.12, Dst: 123.23.23.23
- User Datagram Protocol, Src Port: 62828, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0xb167
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - bitsy.mit.edu: type A, class IN

Packet bytes:

```

0000 d4 9a a0 6d 4b f8 48 5f 99 99 b2 1d 00 00 45 00  ...mK_H.....E
0010 00 3b 00 61 00 00 00 11 66 6e c0 a0 01 0c 7b 17  ;a...fn...{
0020 17 17 f5 6c 00 35 00 27 e0 a7 1b 67 01 00 00 01  ...1.5'...g...
0030 00 00 00 00 00 00 05 62 69 74 73 79 03 6d 69 74  ....bitsy.mit
0040 03 65 64 75 00 00 01 00 01                      ....edu....

```

It's a standard type A query that doesn't contain any answers

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

ANSWER:

One answer is provided in the DNS response message

Answers

```

bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1621 (27 minutes, 1 second)
Data length: 4
Address: 18.0.72.3
[Request In: 66]
[Time: 0.006190000 seconds]

```

Question 23: Provide a screenshot

ANSWER:

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.12

No.	Time	Source	Destination	Protocol	Length	Info
32	21:01:17,914378	123.23.23.23	192.168.1.12	DNS	158	Standard query response 0xb147 A dcg.microsoft.com CNAME dcg.microsoft.com.b-0005.b-msedge.net CNAME b-00...
33	21:01:17,914913	192.168.1.12	123.23.23.23	DNS	77	Standard query 0x66c7 AAAA dcg.microsoft.com
34	21:01:17,920406	123.23.23.23	192.168.1.12	DNS	189	Standard query response 0x66c7 AAAA dcg.microsoft.com CNAME dcg.microsoft.com.b-0005.b-msedge.net CNAME b...
66	21:01:19,747462	192.168.1.12	123.23.23.23	DNS	73	Standard query 0xb67 A bitsy.mit.edu
67	21:01:19,747910	192.168.1.12	123.23.23.23	DNS	73	Standard query 0xb5b0 AAAA bitsy.mit.edu
68	21:01:19,753652	123.23.23.23	192.168.1.12	DNS	138	Standard query response 0xb5b0 AAAA bitsy.mit.edu SOA use2.akam.net
69	21:01:19,753652	123.23.23.23	192.168.1.12	DNS	89	Standard query response 0xb67 A bitsy.mit.edu A 18.0.72.3
70	21:01:19,756742	192.168.1.12	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
78	21:01:21,759885	192.168.1.12	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
97	21:01:23,760789	192.168.1.12	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
102	21:01:25,763016	192.168.1.12	18.0.72.3	DNS	74	Standard query 0x0004 AAAA www.aiit.or.kr

Authority RRs: 0
Additional RRs: 0

Queries

Answers

- bitsy.mit.edu: type A, class IN, addr 18.0.72.3
 - Name: bitsy.mit.edu
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 1621 (27 minutes, 1 second)
 - Data length: 4
 - Address: 18.0.72.3

[Request In: 66]
[Time: 0.006190000 seconds]

0000 48 5f 99 99 b2 1d d4 9a a0 6d 4b f8 00 00 45 00 H.....mK...E
0010 00 4b e8 31 00 00 3b 11 43 8e 7b 17 17 c0 a8 K1...C (.....
0020 01 0c 00 35 f5 6c 00 37 f4 e5 1b 67 81 00 00 01 ...517...g...
0030 00 01 00 00 00 00 05 62 69 74 73 79 03 6d 69 74bitsy.mit
0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu.....
0050 00 06 55 00 04 12 00 48 03 ..U...H..

Identification of transaction (dns.id, 2 byte(s))

Packets: 139 · Displayed: 104 (74.8%) · Dropped: 0 (0.0%)

Profile: Default

9:07 CH
11/10/2021