

Lab Report

CSE351, Computer Networks

Name: Malak Mohamed Helmy Elbakry ID: 20P2434

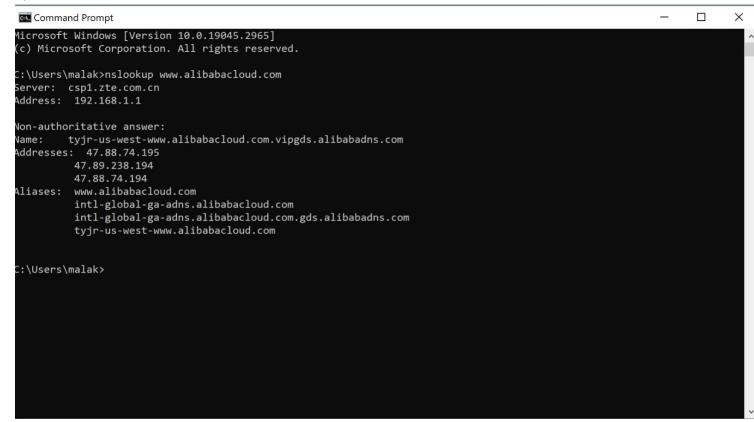
Lab No: (3) Experiment Title: Wireshark_DNS_v7.0

Date: 25 / 10 /2023

Note: I am a mac user so I had to run the commands on windows which is the cause of the different fonts and ip addresses.

nslookup

1. Question 1



The IP Address of middle-east.alibabacloud.com: 47.88.74.195

```
C:\Users\malak>nslookup -type=NS cam.ac.uk
Server: csp3.zte.com.cn
Address: 192.168.1.1
Non-authoritative answer:
cam.ac.uk
                nameserver = ns2.ic.ac.uk
cam.ac.uk
                nameserver = ns3.mythic-beasts.com
cam.ac.uk
                nameserver = ns1.mythic-beasts.com
cam.ac.uk
                nameserver = auth0.dns.cam.ac.uk
cam.ac.uk
                nameserver = dns0.cl.cam.ac.uk
cam.ac.uk
                nameserver = dns0.eng.cam.ac.uk
```

3. Question 3

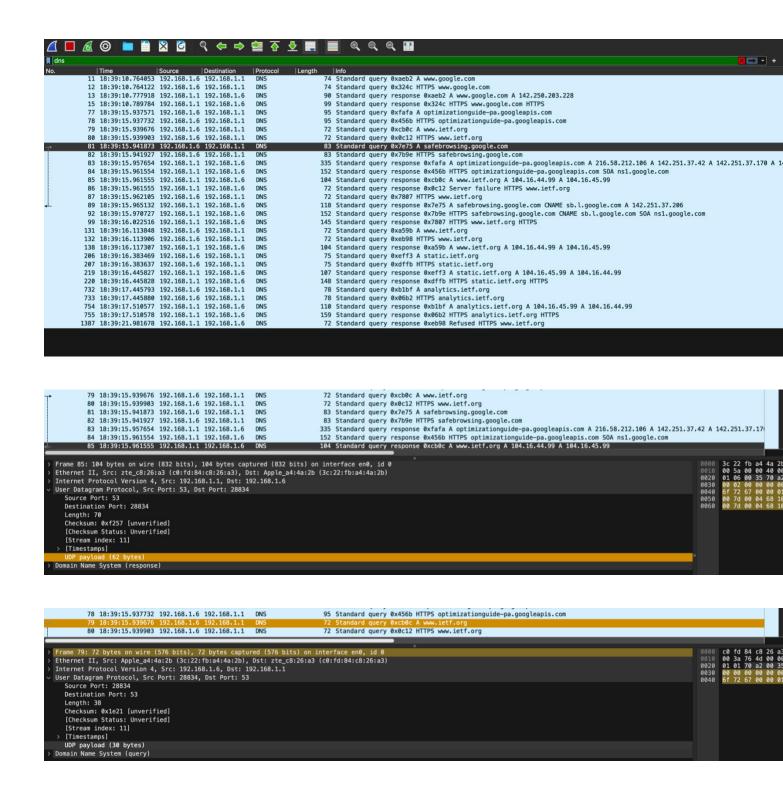
```
C:\Users\malak>nslookup ns3.mythic-beasts.com mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 87.248.119.251

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

```
C:\Users\malak>ipconfig /all
Windows IP Configuration
  Host Name . . . . . . . . . . . . . DESKTOP-6DGMV0G
  Primary Dns Suffix . . . . . . :
  IP Routing Enabled. . . . . . : No
  WINS Proxy Enabled. . . . . . : No
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . . Broadcom 802.11ac Network Adapter
  Physical Address. . . . . . . . : 3C-22-FB-A4-4A-2B
  DHCP Enabled. . . . . . . . . . Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . : fe80::1342:7169:6849:2702%9(Preferred)
  IPv4 Address. . . . . . . . . . . . . 192.168.1.6(Preferred)
  Lease Obtained. . . . . . . . : Thursday, October 26, 2023 6:14:16 PM
  Lease Expires . . . . . . . . : Friday, October 27, 2023 6:14:16 PM
  Default Gateway . . . . . . . . : 192.168.1.1
  DHCP Server . . . . . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . . . . . . . . . . 71049979
  DHCPv6 Client DUID. . . . . . . : 00-01-00-01-2C-B6-88-FB-3C-22-FB-A4-4A-2B
  DNS Servers . . . . . . . . . : 192.168.1.1
  NetBIOS over Tcpip. . . . . . : Enabled
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . . . . . . . . . Media disconnected
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . . . Bluetooth Device (Personal Area Network)
  Physical Address. . . . . . . . : 14-7D-DA-15-89-E1
  DHCP Enabled. . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
```

Tracing DNS with Wireshark

4. Question 4



The Photos show that there are UDP and they are the query and its response

(Using Question 4 Photo)

The Destination port of query: 28843

The Source Port of response: 28834

6. Question 6

```
79 18:39:15.939676 192.168.1.6 192.168.1.1 DNS
                                                                           72 Standard query 0xcb0c A www.ietf.org
 Frame 79: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b), Dst: zte_c8:26:a3 (c0:fd:84:c8:26:a3)
✓ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x764d (30285)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x810e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.6
```

```
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . Broadcom 802.11ac Network Adapter
  Physical Address. . . . . . . : 3C-22-FB-A4-4A-2B
  DHCP Enabled. . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::1342:7169:6849:2702%9(Preferred
  IPv4 Address. . . . . . . . . . . . . . . . 192.168.1.6(Preferred)
  Lease Obtained. . . . . . . . : Thursday, October 26, 2023 6:14:16 PM
  Lease Expires . . . . . . . : Friday, October 27, 2023 6:14:16 PM
  Default Gateway . . . . . . . : 192.168.1.1
  DHCP Server . . . . . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . . . . . . . . . . . 71049979
  DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-B6-88-FB-3C-22-FB-A4-4/
  NetBIOS over Tcpip. . . . . . : Enabled
```

Both the destination IP address of the query and the DNS Server IP address are the same

Type: A

Answer: 0

8. Question 8

2 answers were sent

The Answers contains:

Name, type, class, time-to-leave, data-length, address

```
85 18:39:15.961555 192.168.1.1 192.168.1.6 DNS
                                                                             104 Standard query response 0xcb0c A www.ietf.org A 104.16.44.99 A 104.16.45.99
    Name: www.ietf.org
    [Name Length: 12]
    [Label Count: 3]
   Class: IN (0x0001)
www.ietf.org: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org
   Type: A (Host Address) (1) Class: IN (0x0001)
    Time to live: 125 (2 minutes, 5 seconds)
    Data length: 4
   Address: 104.16.44.99
 www.ietf.org: type A, class IN, addr 104.16.45.99
   Name: www.ietf.org
Type: A (Host Address) (1)
Class: IN (0x0001)
    Time to live: 125 (2 minutes, 5 seconds)
   Data length: 4
Address: 104.16.45.99
Time: 0.021879000 seco
```

9. Question 9

DNS response:

```
79 18:39:15.939676 192.168.1.6 192.168.1.1 DNS 72 Standard query 0xcb0c A www.ietf.org
80 18:39:15.939939 192.168.1.6 192.168.1.1 DNS 72 Standard query 0xcb0c A www.ietf.org
81 18:39:15.941873 192.168.1.6 192.168.1.1 DNS 83 Standard query 0x7e75 A safebrowsing.google.com
82 18:39:15.941927 192.168.1.1 192.168.1.1 DNS 83 Standard query 0x7b9e HTTPS safebrowsing.google.com
83 18:39:15.957654 192.168.1.1 192.168.1.0 DNS 83 Standard query personse 0xfafa A optimizationguide-pa.googleapis.com A 216.58.212.106 A 142.251.37.17
84 18:39:15.961555 192.168.1.1 192.168.1.6 DNS 335 Standard query response 0xfafa A optimizationguide-pa.googleapis.com SOA nsl.google.com
85 18:39:15.961555 192.168.1.1 192.168.1.6 DNS 104 Standard query response 0xfafa A optimizationguide-pa.googleapis.com SOA nsl.google.com

85 18:39:15.961555 192.168.1.1 192.168.1.6 DNS 104 Standard query response 0xfafa A optimizationguide-pa.googleapis.com SOA nsl.google.com

95 18:39:15.961555 192.168.1.1 192.168.1.6 DNS 104 Standard query response 0xcb0c A www.ietf.org A 104.16.44.99 A 104.16.45.99

96 Frame 85: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface en0, id 0

97 Ethernet II, Src: zte_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b)

98 Jonatarion Port: 28834

105 Length: 70

106 Checksum: 0xf257 [unverified]

107 [Checksum: 0xf257 [unverified]

108 Standard query presponse 0xf257 [unverified]

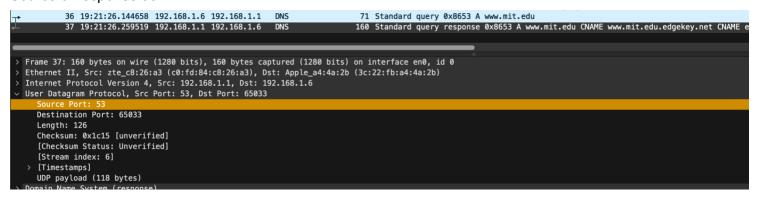
109 Domain Name System (response)
```

TCP:

No there was not issued any images

Destination of query:53

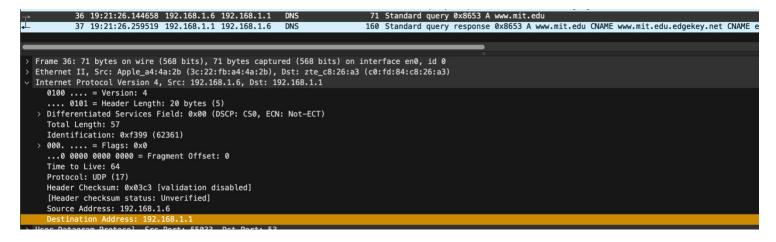
Source of response:53



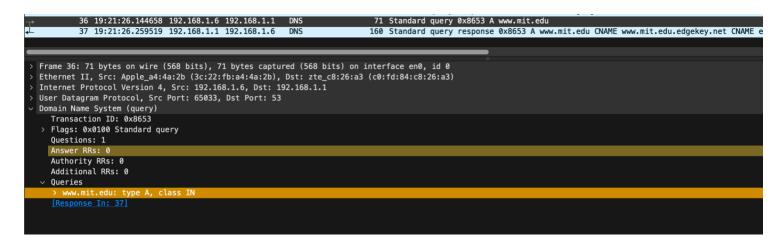
12. Question 12

local DNS server

```
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . Broadcom 802.11ac Network Adapter
  Physical Address. . . . . . . . . . . . 3C-22-FB-A4-4A-2B
  DHCP Enabled. . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::1342:7169:6849:2702%9(Preferred)
  IPv4 Address. . . . . . . . . . . . . . . 192.168.1.6(Preferred)
  Lease Obtained. . . . . . . . : Thursday, October 26, 2023 6:14:16 PM
  Lease Expires . . . . . . . . : Friday, October 27, 2023 6:14:16 PM
  Default Gateway . . . . . . . . : 192.168.1.1
  DHCP Server . . . . . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . . . . . : 71049979
  NetBIOS over Tcpip. . . . . . : Enabled
```



"Type" of DNS query :A



Answers: 0

```
36 19:21:26.144658 192.168.1.6 192.168.1.1 DNS
                                                                                     71 Standard query 0x8653 A www.mit.edu
          37 19:21:26.259519 192.168.1.1 192.168.1.6 DNS
                                                                                    160 Standard query response 0x8653 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akama:
Frame 37: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0
Ethernet II, Src: zte_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b) Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6 User Datagram Protocol, Src Port: 53, Dst Port: 65033
Domain Name System (response)
Transaction ID: 0x8653
> Flags: 0x8180 Standard query response, No error
  Questions: 1
   Authority RRs: 0
   Additional RRs: 0
∨ Queries
   > www.mit.edu: type A, class IN
      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: 1351 (22 minutes, 31 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: 30 (30 seconds)
         Data length: 24
         CNAME: e9566.dscb.akamaiedge.net
     e9566.dscb.akamaiedge.net: type A, class IN, addr 104.106.109.234
Name: e9566.dscb.akamaiedge.net
         Type: A (Host Address) (1) Class: IN (0x0001)
         Time to live: 20 (20 seconds)
         Data length: 4
         Address: 104.106.109.234
```

Answers: 3

Provide: Name, class, type, time to live, data length, CNAME

15. Question 15

Done under every question its screenshot.

```
(base) malakelbakry@malaks-mbp ~ % nslookup -type=NS mit.edu

Server: 192.168.1.1

Address: 192.168.1.1#53

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

local DNS server

```
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . Broadcom 802.11ac Network Adapter
  Physical Address. . . . . . . : 3C-22-FB-A4-4A-2B
  DHCP Enabled. . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . : fe80::1342:7169:6849:2702%9(Preferred)
  IPv4 Address. . . . . . . . . . . . . . . . 192.168.1.6(Preferred)
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Lease Obtained. . . . . . . : Thursday, October 26, 2023 6:14:16 PM
  Lease Expires . . . . . . . : Friday, October 27, 2023 6:14:16 PM
  Default Gateway . . . . . . . : 192.168.1.1
  DHCP Server . . . . . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . . . . . . . . . . . . 71049979
  DHCPv6 Client DUID. . . . . . . : 00-01-00-01-2C-B6-88-FB-3C-22-FB-A4-4/
  DNS Servers . . . . . . . . . . : 192.168.1.1
  NetBIOS over Tcpip. . . . . . : Enabled
```

IP address is the DNS query message sent

They are the same.

17. Question 17

"Type" of DNS query: NS

Answers: 0

Answers:8

Provided 8 nameservers for MIT

No, it did not provide the IP address

```
|Info
67 Standard query 0x28f2 NS mit.edu
                   5 19:37:50.127866 192.168.1.1 192.168.1.6
                                                                                                                                         234 Standard query response 0x28f2 NS mit.edu NS
Frame 5: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface en0, id 0 Ethernet II, Src: zte_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b) Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6 User Datagram Protocol, Src Port: 53, Dst Port: 56790 Domain Name System (response)
     Transaction ID: 0x28f2
     Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 8
     Authority RRs: 0
     Additional RRs: 0
    Queries
               [Name Length: 7] [Label Count: 2]
               Type: NS (authoritative Name Server) (2)
               Class: IN (0x0001)
     Answers
         mit.edu: type NS, class IN, ns asia2.akam.net
      > mit.edu: type NS, class IN, ns asia2.akam.net
> mit.edu: type NS, class IN, ns ns1e173.akam.net
> mit.edu: type NS, class IN, ns ns1e173.akam.net
> mit.edu: type NS, class IN, ns ns1e37.akam.net
> mit.edu: type NS, class IN, ns use3.akam.net
> mit.edu: type NS, class IN, ns asia1.akam.net
> mit.edu: type NS, class IN, ns eur5.akam.net
> mit.edu: type NS, class IN, ns usw2.akam.net
     [Time: 0.015037000 seconds]
```

19. Question 19

Done under every question its screenshot.

For Question 20, 21,22,23: I used my mobile data and I could not execute and capture at the same time as the mac os and windows are not parallel to each other, so I used the trace files provided by Wireshark.

local DNS server

```
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . . Broadcom 802.11ac Network Adapter
  Physical Address. . . . . . . : 3C-22-FB-A4-4A-2B
  DHCP Enabled. . . . . . . . . . . Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::1342:7169:6849:2702%9(Preferred
  IPv4 Address. . . . . . . . . : 192.168.1.6(Preferred)
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Lease Obtained. . . . . . . : Thursday, October 26, 2023 6:14:16 PM
  Lease Expires . . . . . . . . : Friday, October 27, 2023 6:14:16 PM
  Default Gateway . . . . . . . : 192.168.1.1
  DHCP Server . . . . . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . . . . . . . . . . . . 71049979
  DNS Servers . . . . . . . . . . : 192.168.1.1
  NetBIOS over Tcpip. . . . . . : Enabled
```

🕆 104 00:36:49.859652 128.238.38… 18.72.0.3 DNS 74 Standard query 0x0003 A www.aiit.or.kr
↓ 105 00:36:49.873994 18.72.0.3 128.238.38 DNS 156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.k
> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
√ Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
0100 = Version: 4
0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CSO, ECN: Not-ECT)
Total Length: 60
Identification: 0x2805 (10245)
> 000 = Flags: 0x0
0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x58d3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.238.38.160
Destination Address: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
> Domain Name System (query)

Type: A Answers:0

```
104 00:36:49.859652 128.238.38... 18.72.0.3
                                                                                                        74 Standard query 0x0003 A www.aiit.or.kr
             105 00:36:49.873994 18.72.0.3
                                                          128.238.38....
                                                                                                       156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.k
> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0003
   > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    Queries
          www.aiit.or.kr: type A, class IN
             Name: www.aiit.or.kr
             [Name Length: 14]
             [Label Count: 4]
             Type: A (Host Address) (1)
             Class: IN (0x0001)
```

22. Question 22

Answers: 1

```
Contain: Name, type, class, data length, address, time to live
                                                                                                                         74 Standard query 0x0003 A www.aiit.or.kr
156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.1
      Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
User Datagram Protocol, Src Port: 53, Dst Port: 3753
Domain Name System (response)
       Transaction ID: 0x0003
> Flags: 0x8180 Standard query response, No error
          Questions: 1
          Authority RRs: 2
Additional RRs: 2
          Queries
              www.aiit.or.kr: type A, class IN
                  Name: www.aiit.or.kr
[Name Length: 14]
                  [Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
              www.aiit.or.kr: type A, class IN, addr 218.36.94.200
                  Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
                  Time to live: 3338 (55 minutes, 38 seconds)
Data length: 4
Address: 218.36.94.200
          Authoritative nameservers
          Additional records
          [Time: 0.014342000 seconds]
```

23. Question 23

Done under every question its screenshot.