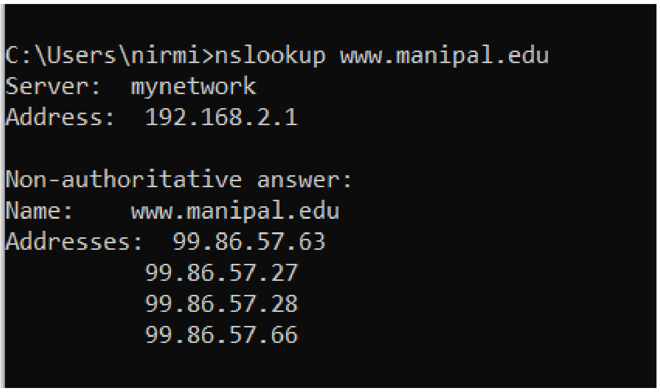
Wireshark lab 3

Name: Nirmith Victor D’Almeida
Student Number : 101160124

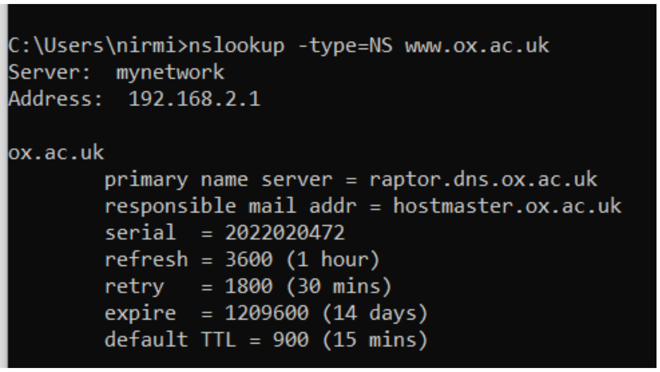
1. nslookup

1. Asian web server (link: www.manipal.edu)
   IP address is 99.86.57.63



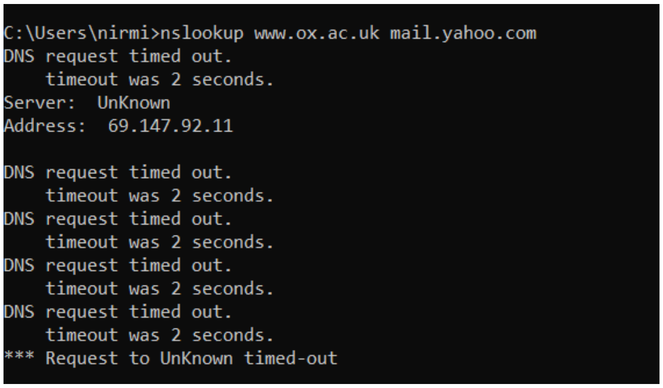
```
C:\Users\nirmi>nslookup www.manipal.edu
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
Name:    www.manipal.edu
Addresses:  99.86.57.63
          99.86.57.27
          99.86.57.28
          99.86.57.66
```

2. The authoritative DNS Server is raptor.dns.ox.ac.uk



```
C:\Users\nirmi>nslookup -type=NS www.ox.ac.uk
Server:  mynetwork
Address:  192.168.2.1

ox.ac.uk
        primary name server = raptor.dns.ox.ac.uk
        responsible mail addr = hostmaster.ox.ac.uk
        serial  = 2022020472
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 900 (15 mins)
```

3. The IP address for the DNS server if attached to the yahoo mail server is 69.147.92.11



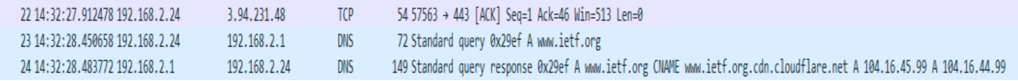
```
C:\Users\nirmi>nslookup www.ox.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  69.147.92.11

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
```

2. Ipconfig

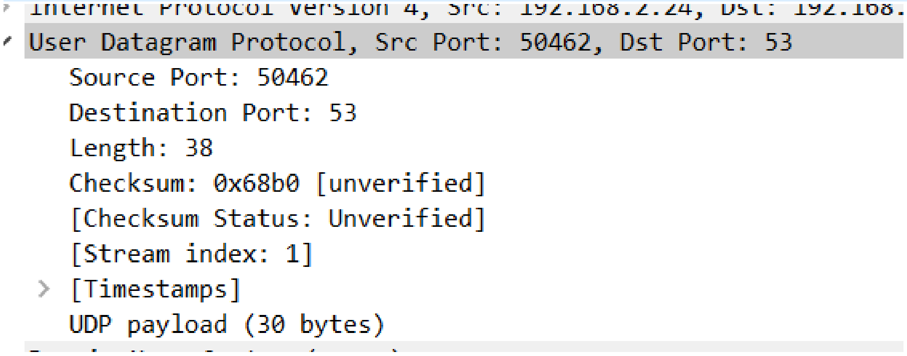
(Mostly images on how to do ipconfig)

3. Tracing DNS with Wireshark

4. The DNS query and response where sent over a UDP



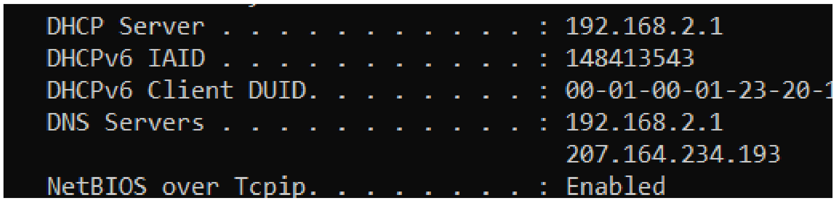
```
22 14:32:27.912478 192.168.2.24    3.94.231.48    TCP    54 57563 → 443 [ACK] Seq=1 Ack=46 Win=513 Len=0
23 14:32:28.450658 192.168.2.24    192.168.2.1    DNS    72 Standard query 0x29ef A www.ietf.org
24 14:32:28.483772 192.168.2.1     192.168.2.24   DNS    149 Standard query response 0x29ef A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
```



```
> Internet Protocol Version 4, Src: 192.168.2.24, Dst: 192.168.
v User Datagram Protocol, Src Port: 50462, Dst Port: 53
    Source Port: 50462
    Destination Port: 53
    Length: 38
    Checksum: 0x68b0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (30 bytes)
```

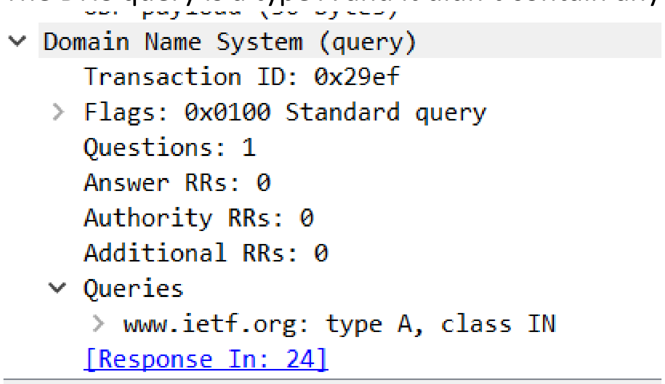
5. The Destination Port is 53 and the source port is 50462

6. The Ip Address is 192.168.2.1 and yes they are the same as my local DNS servers



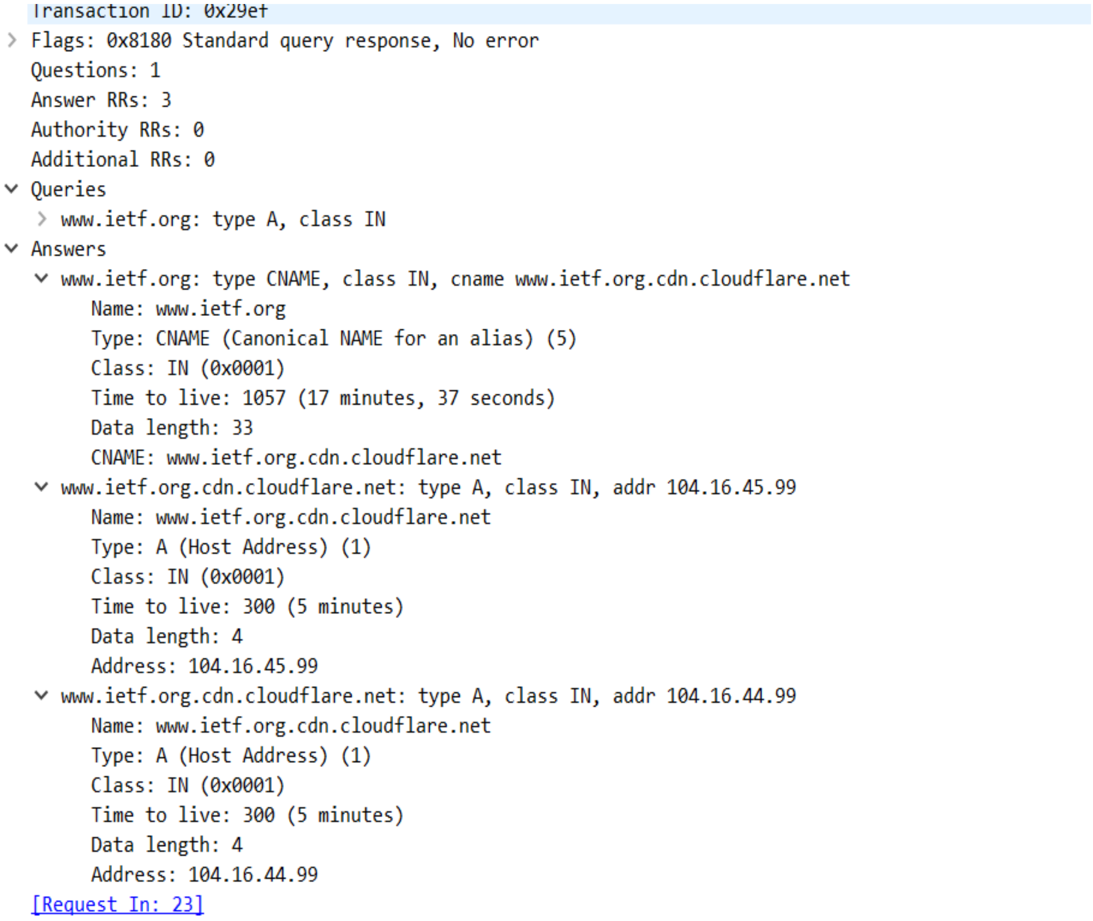
```
   DHCP Server . . . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . . . : 148413543
   DHCPv6 Client DUID. . . . . . . . . . : 00-01-00-01-23-20-1
   DNS Servers . . . . . . . . . . . . . : 192.168.2.1
                                           207.164.234.193
   NetBIOS over Tcpip. . . . . . . . . . : Enabled
```

7. The DNS query is a type A and it didn't contain any answers



```
v Domain Name System (query)
    Transaction ID: 0x29ef
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 24]
```

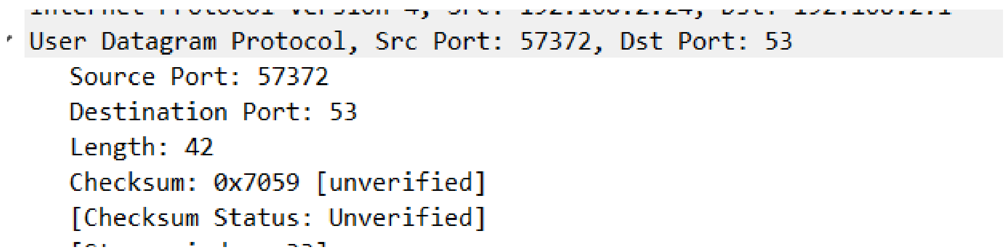
8. I was provided with 3 answers



```
Transaction ID: 0x29ef
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > www.ietf.org: type A, class IN
v Answers
  v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1057 (17 minutes, 37 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
  [Request In: 23]
```

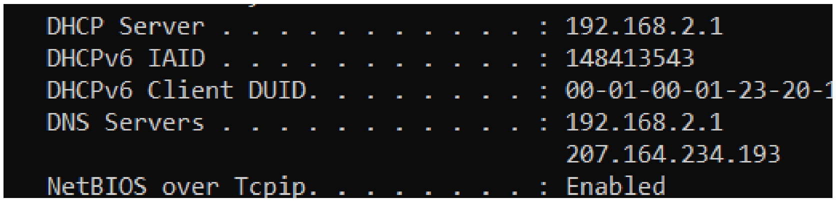
9. The Destination for the packet is similar to the host address therefore it is 192.168.2.1.
10. No my host doesn't issue any new DNS queries.

11. Destination: 53 and Port: 57372



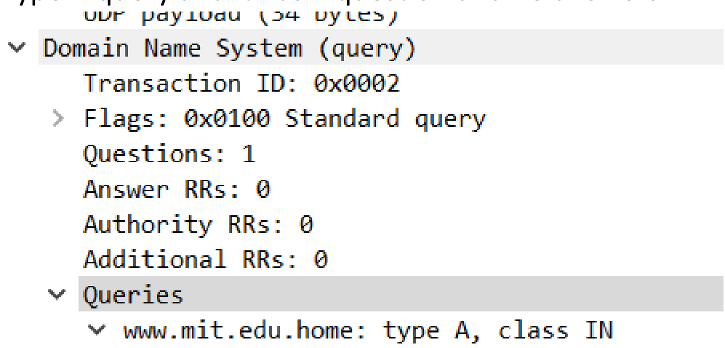
```
Internet Protocol Version 4, Src: 192.168.2.24, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 57372, Dst Port: 53
    Source Port: 57372
    Destination Port: 53
    Length: 42
    Checksum: 0x7059 [unverified]
    [Checksum Status: Unverified]
```

12. The Ip Address is 192.168.2.1 and yes they are the same as my local DNS servers



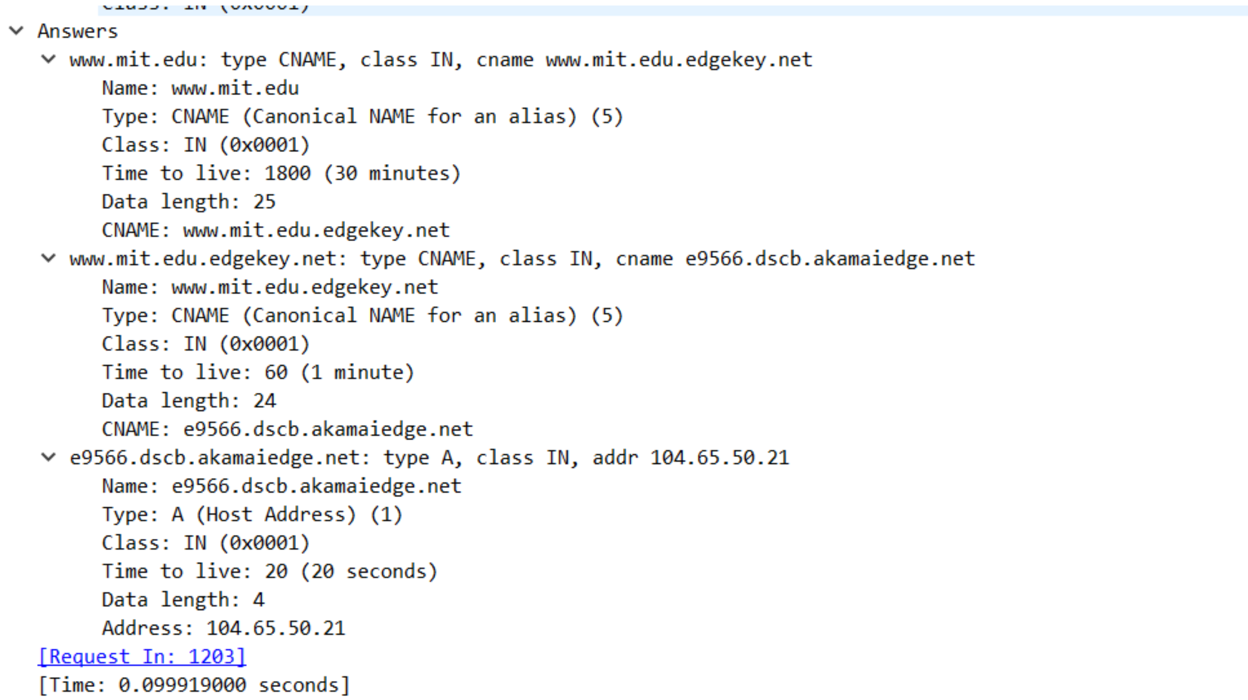
```
DHCP Server . . . . . . . . . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . . . . . . . . . : 148413543
DHCPv6 Client DUID. . . . . . . . . . : 00-01-00-01-23-20-1
DNS Servers . . . . . . . . . . . . . : 192.168.2.1
                                        207.164.234.193
NetBIOS over Tcpip. . . . . . . . . . : Enabled
```

13. Type A query and it has 1 question and no answers



```
    UDP payload (54 bytes)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu.home: type A, class IN
```

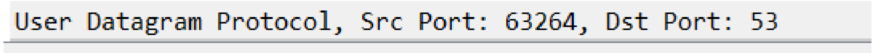
14. There are 3 answers provided and they are



```
      Class: IN (0x0001)
v Answers
  v 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: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  v 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
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.65.50.21
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 104.65.50.21
  [Request In: 1203]
  [Time: 0.099919000 seconds]
```

15. Provided under each answer as needed

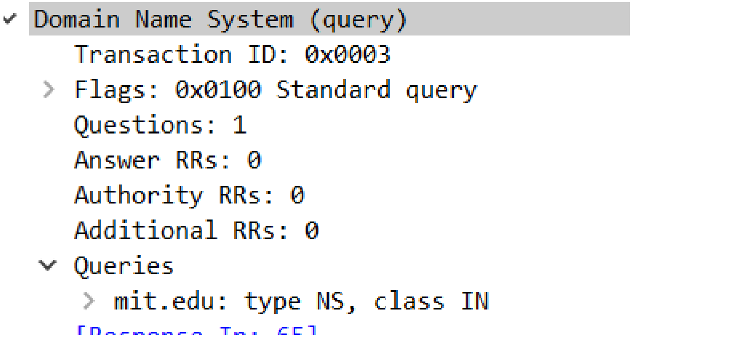
16. Destination port:53 and source port: 63264



```
User Datagram Protocol, Src Port: 63264, Dst Port: 53
```

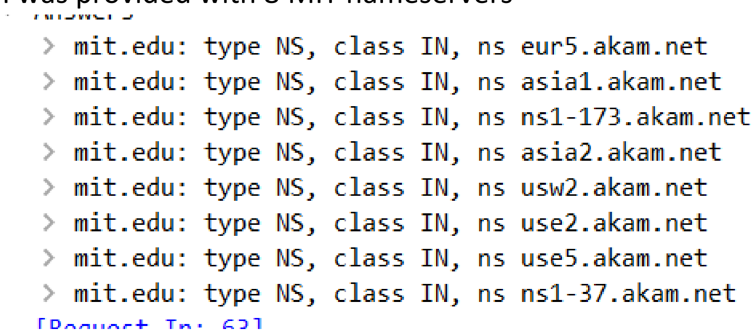
The IP address the query is sent to is similar to my default local DNS server 192.168.2.1

17. It is a type NS and there are no answers



```
✓ Domain Name System (query)
     Transaction ID: 0x0003
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ⌄ Queries
       > mit.edu: type NS, class IN
     [Response In: 65]
```

18. I was provided with 8 MIT nameservers

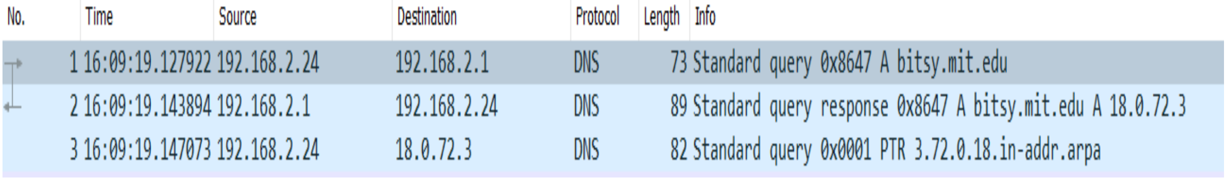


```
 ⌄ Answers
   > mit.edu: type NS, class IN, ns eur5.akam.net
   > mit.edu: type NS, class IN, ns asia1.akam.net
   > mit.edu: type NS, class IN, ns ns1-173.akam.net
   > mit.edu: type NS, class IN, ns asia2.akam.net
   > mit.edu: type NS, class IN, ns usw2.akam.net
   > mit.edu: type NS, class IN, ns use2.akam.net
   > mit.edu: type NS, class IN, ns use5.akam.net
   > mit.edu: type NS, class IN, ns ns1-37.akam.net
 [Request In: 63]
```

and no there is no IP addresses for the name servers

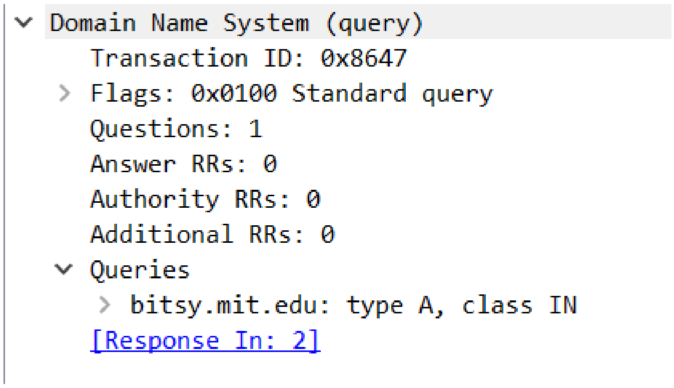
19. The screenshots are provided under each section

20. The ip address is 192.168.2.1 which is similar to my default IP address



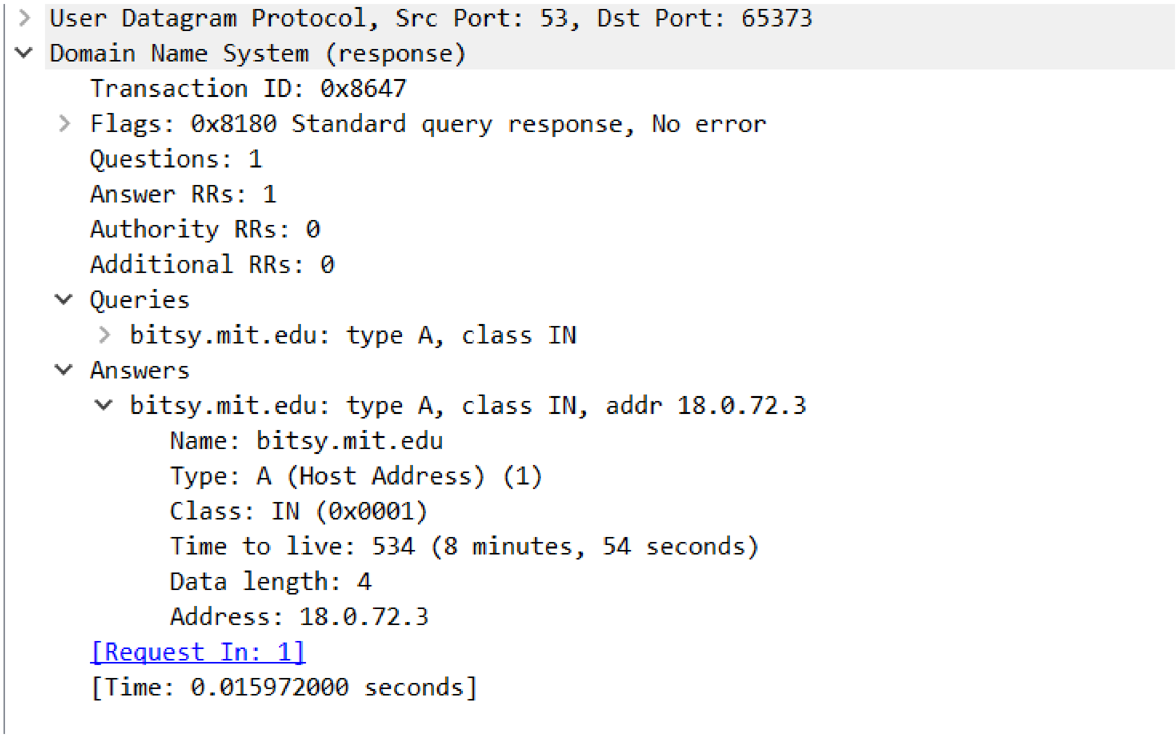
No.	Time	Source	Destination	Protocol	Length	Info
1	16:09:19.127922	192.168.2.24	192.168.2.1	DNS	73	Standard query 0x8647 A bitsy.mit.edu
2	16:09:19.143894	192.168.2.1	192.168.2.24	DNS	89	Standard query response 0x8647 A bitsy.mit.edu A 18.0.72.3
3	16:09:19.147073	192.168.2.24	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa

21. Type A and no answers



```
⌄ Domain Name System (query)
     Transaction ID: 0x8647
   > 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]
```

22. Contains 1 answers which contains the following address 18.0.72.3



```
› User Datagram Protocol, Src Port: 53, Dst Port: 65373
⌄ Domain Name System (response)
     Transaction ID: 0x8647
   › 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
           Name: bitsy.mit.edu
           Type: A (Host Address) (1)
           Class: IN (0x0001)
           Time to live: 534 (8 minutes, 54 seconds)
           Data length: 4
           Address: 18.0.72.3
     [Request In: 1]
     [Time: 0.015972000 seconds]
```

23. Screenshots provided under respective questions