Computer Networks lab - 5

DNS

Yasaswini Tiramdas, 18mcme22

1. The web page used is the University of Hyderabad website which is in Hyderabad
   IP address: 172.104.34.236

```
C:\Users\yasas>nslookup www.uohyd.ac.in
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    www.uohyd.ac.in
Address:  172.104.34.236
```

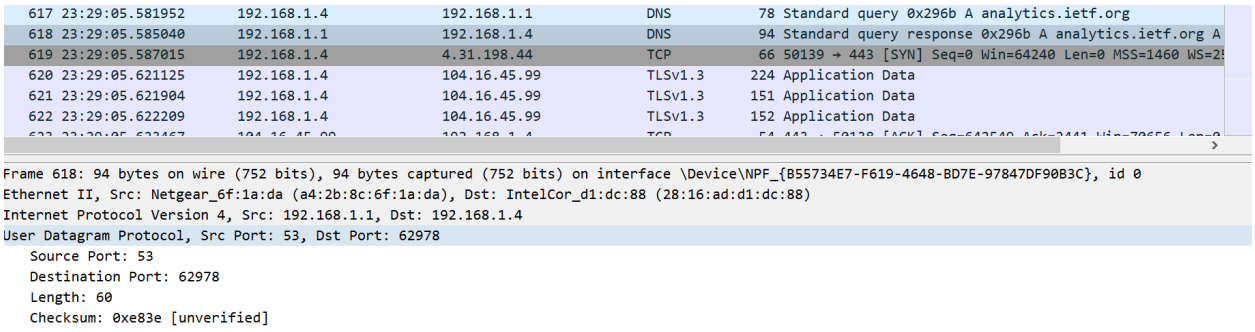
2. The Europen university used is Central European University
   Authoritative DNS server names are as in given below image

```
C:\Users\yasas>nslookup -type=NS www.ceu.edu
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
www.ceu.edu     canonical name = ceu.edu
ceu.edu nameserver = ns.ceu.edu
ceu.edu nameserver = zaurak.ceu.edu
ceu.edu nameserver = vega.ceu.edu
```

3. Got mail.yahoo.com IP address using zaurak.ceu.edu nameserver
   For others, I was getting timed out so I used this name server.

```
C:\Users\yasas>nslookup mail.yahoo.com zaurak.ceu.edu
Server:  UnKnown
Address:  40.85.83.241

Non-authoritative answer:
Name:    edge.gycpi.b.yahoodns.net
Addresses:  2a00:1288:7c:800::4000
          2a00:1288:7c:800::4001
          87.248.114.11
          87.248.114.12
Aliases:  mail.yahoo.com
```

4. They are sent over UDP as shown in the given figure.



5. The destination port for the DNS query message is 53.
   The source port of the DNS response message is 53.

6. The DNS query message sent to 192.168.1.1
   Using ipconfig, the IP address of the local DNS server is 192.168.1.1
   Yes, these two IP addresses the same

```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address. . . . . . . . . : 28-16-AD-D1-DC-88
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::682e:a9b:c32a:5434%15(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.1.4(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : 27 March 2021 23:04:11
Lease Expires . . . . . . . . . . : 28 March 2021 23:04:11
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . . . . . . . : 153622189
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-C8-A9-40-D4-81-D7-C5-5C-CB
DNS Servers . . . . . . . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

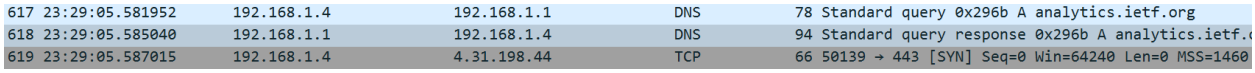
7. The query message was type ”A” and it did not contain any “answers”.

```
▾ Queries
  ▾ analytics.ietf.org: type A, class IN
      Name: analytics.ietf.org
      [Name Length: 18]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

8. The DNS response message provided only one answer. The answer contains the address of the website that it was queried for which is 4.31.198.44

```
▾ Queries
  ▾ analytics.ietf.org: type A, class IN
      Name: analytics.ietf.org
      [Name Length: 18]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▾ Answers
  ▾ analytics.ietf.org: type A, class IN, addr 4.31.198.44
      Name: analytics.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1519 (25 minutes, 19 seconds)
      Data length: 4
      Address: 4.31.198.44
  [Request In: 617]
  [Time: 0.003088000 seconds]
```

9. Yes, the destination IP address of the SYN packet corresponds to any of the IP addresses provided in the DNS response message.



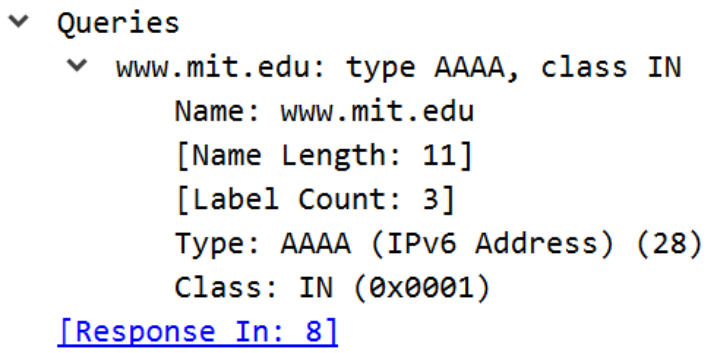
617	23:29:05.581952	192.168.1.4	192.168.1.1	DNS	78 Standard query 0x296b A analytics.ietf.org
618	23:29:05.585040	192.168.1.1	192.168.1.4	DNS	94 Standard query response 0x296b A analytics.ietf.c
619	23:29:05.587015	192.168.1.4	4.31.198.44	TCP	66 50139 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

10. No, the host doesn't issue new DNS queries.

11. The destination port for the DNS query message is 53.
    The source port of the DNS response message is 53.

12. The IP address is the DNS query message sent is 192.168.1.1. Yes, this is the IP address of my default local DNS server.

13. The DNS query is of type "AAAA". The query message does not contain any "answers".

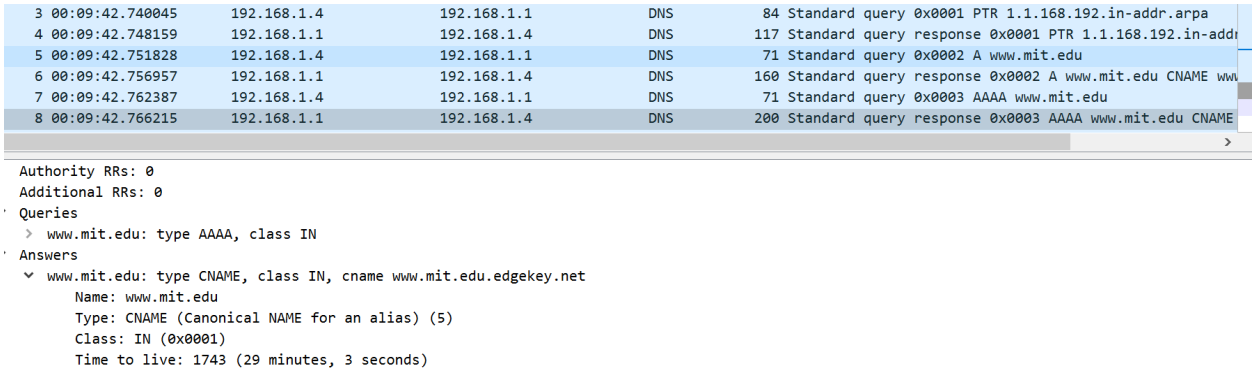


```
▾ Queries
  ▾ www.mit.edu: type AAAA, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
  [Response In: 8]
```

14. "4 answers" are provided. Each of the answers contains name, type, class, time to live, data length and CNAME.

```
Queries
    > www.mit.edu: type AAAA, 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 AAAA, class IN, addr 2600:140f:e:282::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:140f:e:29b::255e
    [Request In: 7]
    [Time: 0.003828000 seconds]
```

15.



16. The IP address is the DNS query message sent is 192.168.1.1. Yes, this is the IP address of my default local DNS server.

17. The DNS query is of type “NS”. The query message does not contain any “answers”.

```
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: 6]
```

18. The nameservers are asia1, use5, use2, ns1-173, asia2, usw2, ns1-37 and eur5. It doesn't provide the IP of the MIT nameservers.

```
Answers
    mit.edu: type NS, class IN, ns asia1.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1757 (29 minutes, 17 seconds)
        Data length: 16
        Name Server: asia1.akam.net
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns use2.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
```

19.

```
    3 00:27:28.312794   192.168.1.4   192.168.1.1   DNS   84 Standard query 0x0001 PTR 1.1.168.192.in-addr.ar
    4 00:27:28.336353   192.168.1.1   192.168.1.4   DNS  117 Standard query response 0x0001 PTR 1.1.168.192.i
    5 00:27:28.339111   192.168.1.4   192.168.1.1   DNS   67 Standard query 0x0002 NS mit.edu
    6 00:27:28.342919   192.168.1.1   192.168.1.4   DNS  234 Standard query response 0x0002 NS mit.edu NS asi
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 62737
v 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
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
```

20. The DNS query message sent to IP address 18.0.72.3. No, it is not the IP address of the default local DNS server. This IP address corresponds to the IP address of bitsy.mit.edu

21. The DNS query is of type "A" and "AAAA". The query message does not contain any "answers".

22. There is no response.

23.

16	00:48:26.912877	192.168.1.4	18.0.72.3	DNS	74 Standard query 0x0002 A www.aiit.or.kr
23	00:48:28.921641	192.168.1.4	18.0.72.3	DNS	74 Standard query 0x0003 AAAA www.aiit.or.kr
34	00:48:30.932275	192.168.1.4	18.0.72.3	DNS	74 Standard query 0x0004 A www.aiit.or.kr
35	00:48:32.946686	192.168.1.4	18.0.72.3	DNS	74 Standard query 0x0005 AAAA www.aiit.or.kr

```
Transaction ID: 0x0004
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
  v 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)
```