LAB Assignment

Submitted by -
Name: Shah Alam Abir
Roll: BSSE-1439
E-mail: bsse1439@iit.du.ac.bd

Submitted to -
Name: Dr. Md. Shariful Islam
Professor, Institute of Information Technology, University of Dhaka
Email: shariful@iit.du.ac.bd

1. nslookup

Answers:

1. Run *nslookup httpd.apache.org.* IP Address of this server is **151.101.2.132**

2. Run *nslookup -type=NS cam.ac.uk* to get all the authoritative servers of University of Cambridge. List of authoritative DNS servers of University of Cambridge is -

1. cam.ac.uk nameserver = *ns3.mythic-beasts.com.*
2. cam.ac.uk nameserver = *ns2.ic.ac.uk.*
3. cam.ac.uk nameserver = *dns0.cl.cam.ac.uk.*
4. cam.ac.uk nameserver = *auth0.dns.cam.ac.uk.*
5. cam.ac.uk nameserver = *dns0.eng.cam.ac.uk.*
6. cam.ac.uk nameserver = *ns1.mythic-beasts.com.*

3. There is no DNS server obtained in Question 2 that could queried for the mail server for Yahoo! Mail. Yahoo! Mail can be queried from these servers

```
shahalamabir@iit-Vostro-460:~/Desktop$ nslookup -type=NS yahoo.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
yahoo.com       nameserver = ns1.yahoo.com.
yahoo.com       nameserver = ns4.yahoo.com.
yahoo.com       nameserver = ns5.yahoo.com.
yahoo.com       nameserver = ns2.yahoo.com.
yahoo.com       nameserver = ns3.yahoo.com.

Authoritative answers can be found from:
```

2. ifconfig

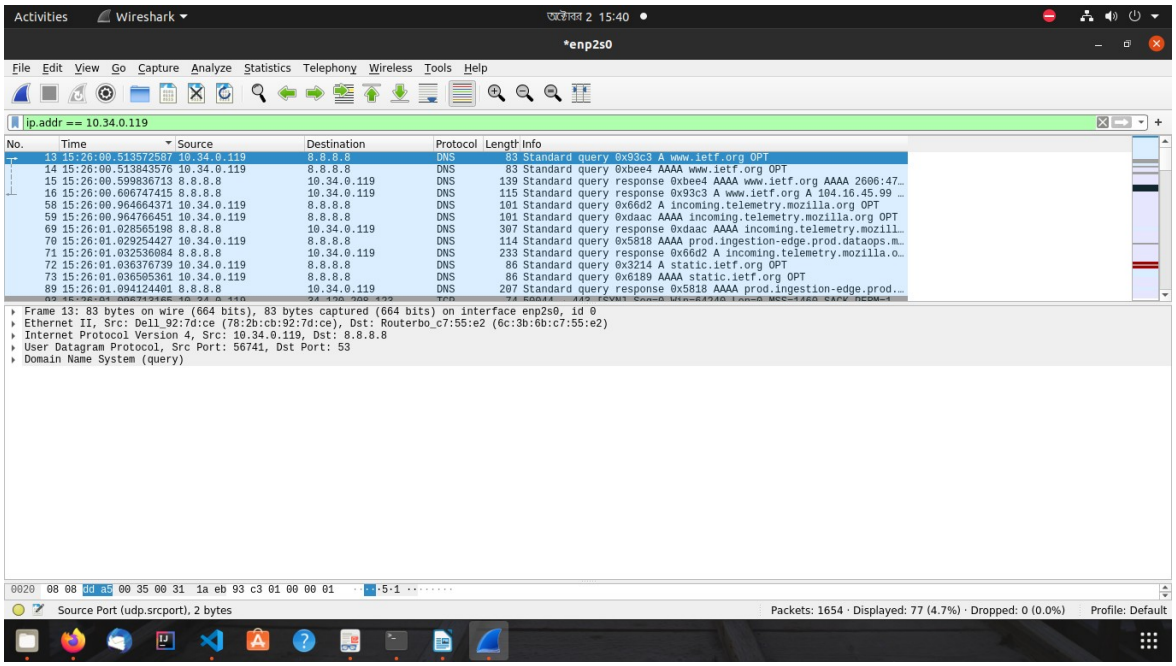
```
shahalamabir@iit-Vostro-460:~/Desktop$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.34.0.119  netmask 255.255.252.0  broadcast 10.34.3.255
        inet6 2405:ac80:c10:304:a560:cc14:492f:cd28  prefixlen 64  scopeid
 0x0<global>
        inet6 2405:ac80:c10:304:5721:96a:d7fd:e4cd  prefixlen 64  scopeid
0x0<global>
        inet6 fe80::8a9:d8c0:2faf:3bf0  prefixlen 64  scopeid 0x20<link>
        ether 78:2b:cb:92:7d:ce  txqueuelen 1000  (Ethernet)
        RX packets 246761  bytes 318589394 (318.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 98474  bytes 15692908 (15.6 MB)
        TX errors 2  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8092  bytes 1745032 (1.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8092  bytes 1745032 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Tracing DNS with Wireshark

Answers:

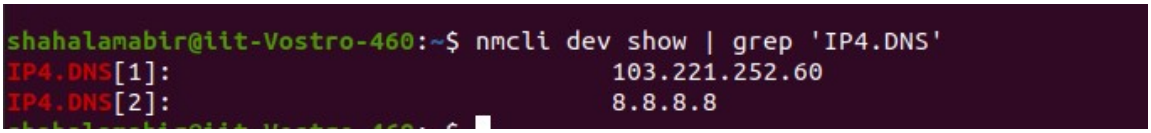
4.



These query and responses were sent over UDP.

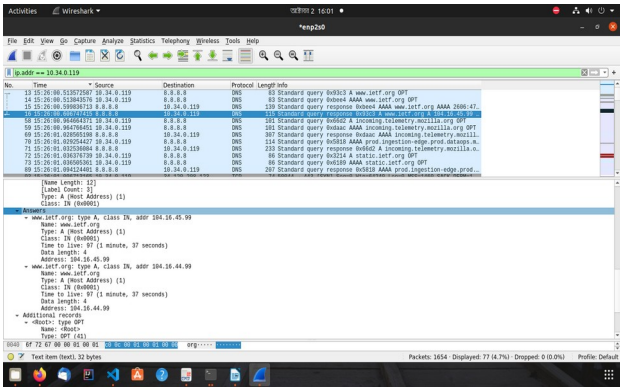
5. Destination port for DNS query message is 53. Source port for the DNS response message is 53.

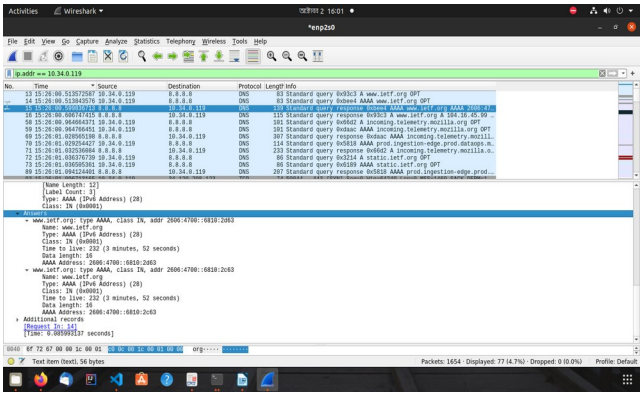
6. DNS query message has sent to IP Address 8.8.8.8. IP Address of my local DNS server is also 8.8.8.8. Both of them are same



7. First DNS query is of type A. Second DNS query is of type AAAA. No, none of this two DNS query messages contains any “answers”.

8. There are two “answers” provided in both of the DNS response messages.





9. No, the destination IP address of the SYN packet doesn't correspond to any of the IP addresses provided in the DNS response message.

10. No, there is only previous two DNS queries.

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

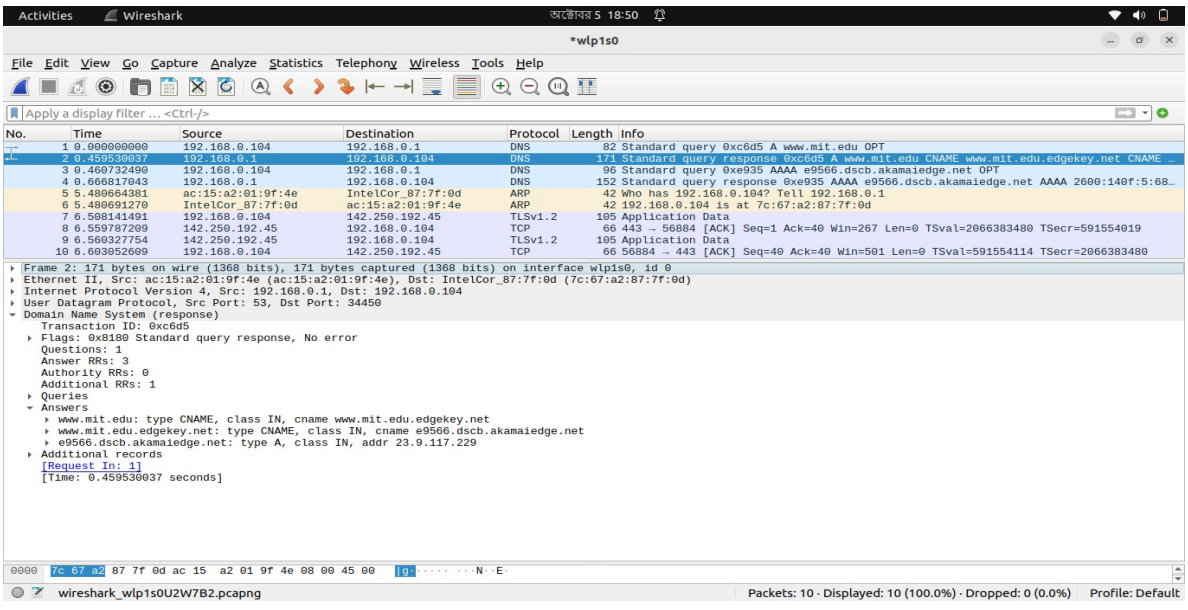
12. DNS query message sent at IP Address 192.168.0.1. Yes, this is the IP Address of my default DNS server.

13. This is 'A' type DNS query. No, the query message doesn't contains any "answers".

14. There are 3 answers provided into the DNS query response message. Answers contains

```
▾ 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: 1722 (28 minutes, 42 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 23.9.117.229
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 23.9.117.229
```

15.



16. DNS query message sent at IP Address 192.168.0.1. Yes, this is the IP Address of my default DNS server.

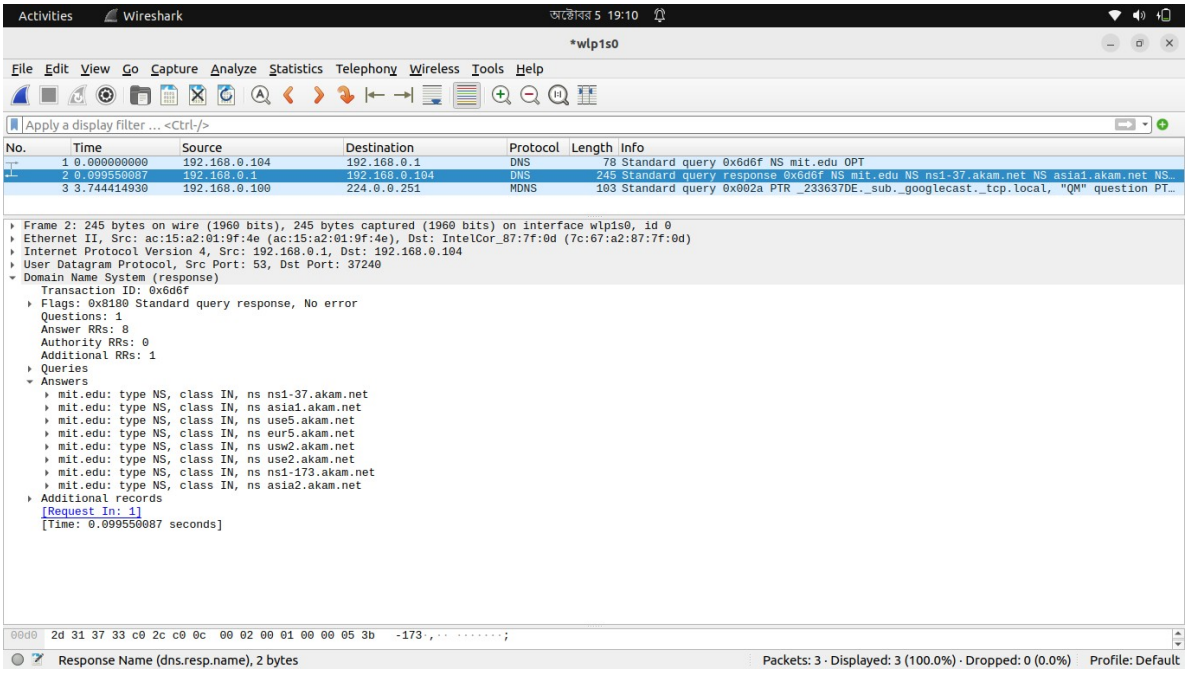
17. This is ‘NS’ type DNS query. No, the query message doesn’t contains any “answers”.

18. The response message provides 8 MIT nameservers name. These are -

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

No, this response message doesn’t provides the IP addresses of the MIT nameservers.

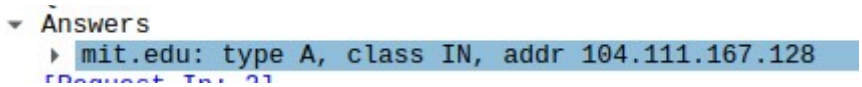
19.



20. DNS query message has been sent to 193.108.91.37. No, This is not the IP address of my default local DNS server. This ip address corresponds to the IP Address of the nameserver of mit.edu which is “ns1-37.akam.net”.

21. Type of the DNS query message is ‘A’. No, this query message doesn’t contains any answer.

22. There is only 1 answer is provided into the DNS response message. This contains -



23.