CS3205 A4 Report

E Santhosh Kumar (CS16B107)

1) DNS

Section 1.1.1

a) IIT Madras (Asia)

Domain Name: iitm.ac.in

1. Web Server: 14.139.160.194
2. Authoritative DNS servers:
    - dns1.iitm.ac.in
    - dns2.iitm.ac.in
    - dns3.iitm.ac.in
3. Computer Science Department
    - Web Server:
        - www.cse.iitm.ac.in - 14.139.160.81
    - Mail Servers:
        - mailx1.iitm.ac.in - 203.199.213.9
        - mailx2.iitm.ac.in - 203.199.213.10
        - mailx3.iitm.ac.in - 203.199.213.11
        - mailx4.iitm.ac.in - 203.199.213.14

4.IP addresses of Authoritative DNS servers:

- dns1.iitm.ac.in - 203.199.213.2
- dns2.iitm.ac.in - 14.139.160.3
- dns3.iitm.ac.in - 14.139.160.2

b) Cornell University (America)

Domain Name: cornell.edu

1. Web Server: 128.84.202.53
2. Authoritative DNS servers:
    - dns.cit.cornell.edu
    - cudns.cit.cornell.edu
    - drdns.cit.cornell.edu
    - bigred.cit.cornell.edu
    - drdns2.cit.cornell.edu
3. Computer Science Department (cs.cornell.edu)

Web Server:

www.cs.cornell.edu - 132.236.207.20

Mail Server:

cornellprod-mail-onmicrosoft-com.mail.eo.outlook.com - 104.47.49.36

4.IP addresses of Authoritative DNS servers:

dns.cit.cornell.edu - 192.35.82.53
cudns.cit.cornell.edu - 132.236.56.252
drdns.cit.cornell.edu - 192.195.74.252
bigred.cit.cornell.edu - 128.253.180.35
drdns2.cit.cornell.edu - 52.45.47.12

c) ETH Zurich (Europe)

Domain Name: ethz.ch

1. Web Server: 129.132.19.216
2. Authoritative DNS servers:

ns1.ethz.ch
ns2.ethz.ch
ns2.switch.ch

3. Computer Science Department (inf.ethz.ch)

Web Server:

www.inf.ethz.ch - 129.132.19.216

Mail Servers:

mc1.ethz.ch - 129.132.80.150
mc2.ethz.ch - 129.132.80.151
mc3.ethz.ch - 82.130.86.11
mc4.ethz.ch - 82.130.86.12s

4. IP addresses of Authoritative DNS servers:

ns1.ethz.ch - 129.132.98.8
ns2.ethz.ch - 129.132.250.8
ns2.switch.ch - 130.59.31.29

Section 1.1.2

(refer wireshark file dns1.pcapng)

5. DNS query and response messages are sent over UDP

6. Destination port of DNS Query message - 53
Source port of DNS Response message - 53

7. DNS Query message was sent to 172.20.10.1. This is also the IP address of the local DNS server (refer image 1_1_2_1)

8. The DNS Query message is of type A. It does not contain any answers.

9. The DNS Query Response message has the following three answers. One of them is of type CNAME and two are of type A.
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 104.20.1.85
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

10. Yes, the subsequent TCP SYN packets have destination 104.20.1.85, which was one of the answers in the DNS response message.

11. No, the DNS query was made only once while getting the IP address of the domain name.

(refer wireshark file dns2.pcapng)

11. Destination port of DNS Query message - 53
Source port of DNS Response message - 53

12. DNS Query message was sent to 172.20.10.1. This is also the IP address of the local DNS server (refer image 1_1_2_2)

13. The DNS Query message is of type A. It does not contain any answers.

14. The DNS Query Response message has the following three 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 104.85.142.137

15. The screenshot is present in image 1_1_2_2

(refer wireshark file dns3.pcapng)

16. DNS Query message was sent to 172.20.10.1. This is also the IP address of the local DNS server (refer image 1_1_2_3)

17. The DNS Query message is of type NS. It does not contain any answers.

18. The DNS response provides the following MIT nameservers (as shown by the received answers)

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

The DNS response message does not provide the IP addresses of these nameservers.

19. The screenshot is present in image 1_1_2_3

(refer wireshark file dns4.pcapng)

20. Two DNS queries are sent. The first query is sent to the local DNS server (172.20.10.1) and it asks for the IP address of the authoritative DNS server (use2.akam.net). The received IP address of the authoritative DNS server is 96.7.49.64. The next query is made to the authoritative DNS server using its IP address, and it asks for the IP address of

21. Both queries are of type A. The second query contains the IP address of the authoritative DNS server, which was received as answer for the first query.

22. The first DNS response message contains the answer
use2.akam.net: type A, class IN, addr 96.7.49.64

This gives the IP address of the authoritative DNS server use2.akam.net

The second DNS response message contains the answer
eecs.mit.edu: type A, class IN, addr 18.62.1.6

This gives the IP address of eecs.iitm.edu

23. The screenshot is present in image 1_1_2_4
