Kazi Shadman Sakib

FH-92

wireshark DNS:-

1) command:-

nslookup www.lenovo.com

Name: e7241.x.akamaiedge.net

Address: 104.69.151.8

2) command:-

nslookup -type=NS ox.ac.uk (for university of Oxford)

Authonative DNS servers:-

ns2.ja.net

dns0.ox.ac.uk

dns1.ox.ac.uk

dns2.ox.ac.uk

auth4.dns.ox.ac.uk

auth5.dns.ox.ac.uk

auth6.dns.ox.ac.uk

~~ns2.ja.net~~

~~auth4.dns.ox.ac.uk~~

3) Command:-

nslookup www.yahoo.com dns2.ox.ac.uk

Name: new-fp-shed.wg1.b.yahoo.com

Address: 202.165.102.49

202.165.107.150 — Got two IP adresses for same host name

4) UDP.

5) Destination Port : 59035

Source Port : 53

6) Query message sent to IP Address: 118.179.223.130

My Local DNS server is : 118.179.223.130

Yes, the two addresses are the same.

7) DNS query "Type": A (Host Address) (1)

Yes the query message contains 1 answer.

Answer RRs: 1

8) Only 1 answer is provided. The one

Answers contains :-

analytics.ietf.org: Type A, class IN, addr 4.31.198.45

Name: analytics.ietf.org

Type : A (Host Address)(1)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data Length : 4

Address: 4.31.198.45

9) Yes the destination IP address of the SYN packet connespond to one of the IP addresses provided in the DNS nesponse message. That is, In the 'Answens' header, there was an IP address: 4.31.198.45, which connesponds.

10) No, there were no new queries before netnieving each image.

11) Destination pont: 63219
Source pont: 53

12) To 118.179.223.130 IP Address, the DNS queny message was sent. Yes this is my IP address of default local DNS senven.

13) ~~Eth~~ - The queny "Type": A (Host address) (1)
Yes the queny message contains 3 answens.

14) There are 3 answers provided. Each answers contains: Informations such as, Name, Type, class, Time to live, Data length and CNAME / Address.

15) providing the screenshot in google classroom. (nslookup_01)

16) The IP Address 118.179.223.130 was used to send DNS query message. Yes it is my IP Address of default local DNS server.

17) Query "type": NS (authoritative Name server) (2)

Yes the query message contains eight (8) answers.

18) Name servers:-

use2.akam.net

use5.akam.net

usw2.akam.net

asia1.akam.net

asia2.akam.net

ns1-37.akam.net

ns1-173.akam.net

eur5.akam.net

Yes, in the additional records it also provides IP addresses of the ~~nam~~ MIT nameserver.

19) provided screenshot in google classroom.
(nslookup-02)

20) DNS query message sent to 18.0.72.3
No this is not my default local DNS server.
It corresponds to bitsy.mit.edu IP address

21) DNS query "Type": A (Host Address) (1)

No, the query message does not contain any message.

22) There are no answers provided.

23) screenshot given in google classroom.

(nslookup_03)