Computer Networks Lab Task

Name:
Abubakkar Abdullah

Roll No: 20P-0045

Section: BSCS(5B)

1. Run nslookup to obtain the IP address of a Web server in Asia.

frigate:Desktop drb$ nslookup home.web.cern.ch

Server: 130.215.32.18

Address: 130.215.32.18#53

Non-authoritative answer:

home.web.cern.ch canonical name = drupalprod.cern.ch.

Name: drupalprod.cern.ch

Address: 137.138.76.28

Note that the #53 denotes the DNS service is running on port 53.

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

frigate:Desktop drb$ nslookup -type=NS tsinghua.edu.cn

Server: 130.215.32.18

Address: 130.215.32.18#53

Non-authoritative answer:

tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn.

tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn.

tsinghua.edu.cn nameserver = dns2.edu.cn.

tsinghua.edu.cn nameserver = ns2.cuhk.edu.hk.

Authoritative answers can be found from:

dns2.tsinghua.edu.cn internet address = 166.111.8.31

ns2.cuhk.edu.hk internet address = 137.189.6.21

ns2.cuhk.edu.hk has AAAA address 2405:3000:3:6::15

dns2.edu.cn internet address = 202.112.0.13

dns.tsinghua.edu.cn internet address = 166.111.8.30

Note that there can be multiple authoritative servers. The response we got back was from a cached record. To confirm the authoritative DNS servers, we perform the same DNS query of one of the servers that can provide authoritative answers.

frigate:Desktop drb$ nslookup -type=NS tsinghua.edu.cn dns.tsinghua.edu.cn

Server: dns.tsinghua.edu.cn

Address: 166.111.8.30#53

tsinghua.edu.cn nameserver = dns2.edu.cn.

tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn.

tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn.

tsinghua.edu.cn nameserver = ns2.cuhk.edu.hk.

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

frigate:Desktop drb$ nslookup pku.edu.cn ns2.cuhk.edu.hk

Server: ns2.cuhk.edu.hk

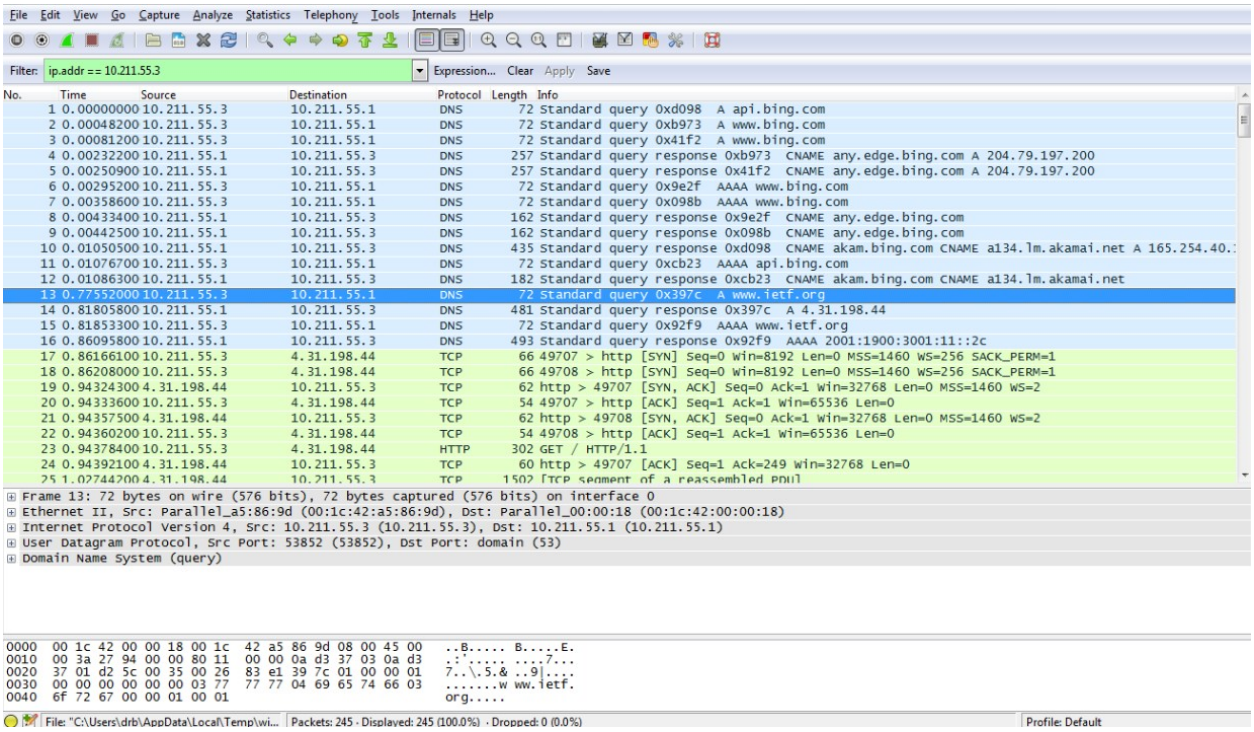
Address: 137.189.6.21#53

Name: pku.edu.cn

Address: 162.105.131.113

I was unable to get any of the DNS servers listed above to answer a query for a Yahoo mail server (even cn.mail.yahoo.com was refused) so I just queried another Chinese university (Peking University).

4. Locate the DNS query and response messages. Are they sent using the UDP or TCP protocol?



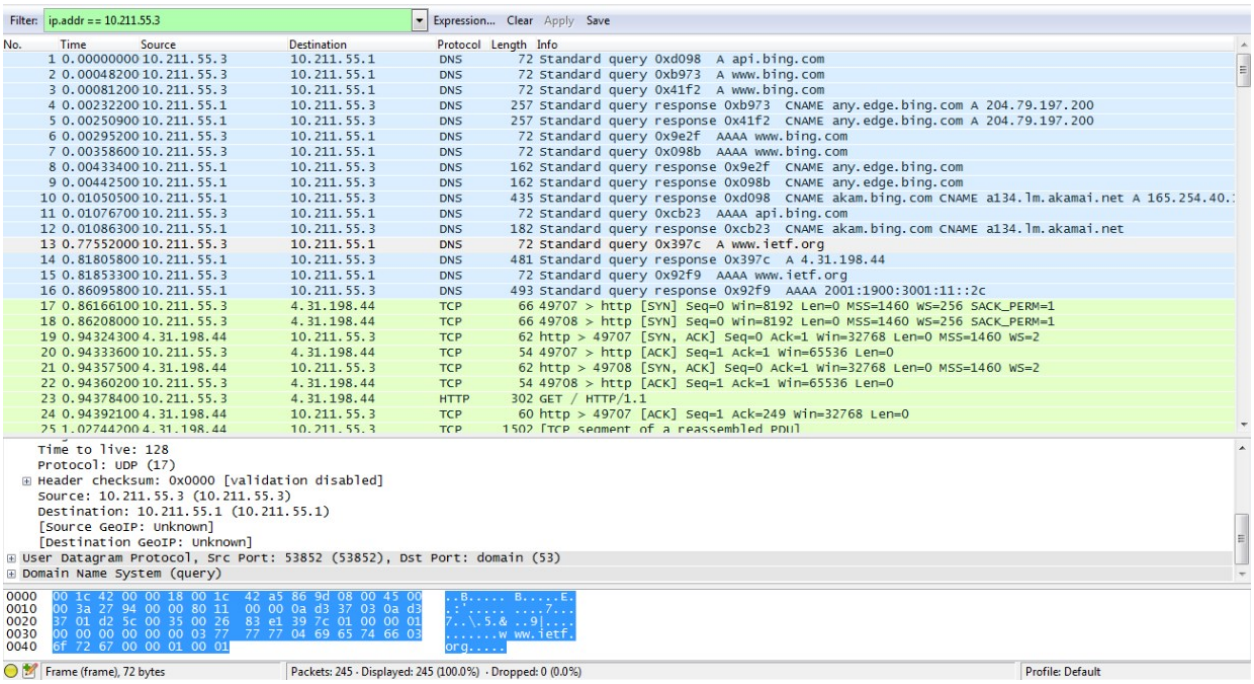
UDP as shown in the screenshot.

5. What is the destination port for the DNS query message? What is the source port of DNS response message? See screenshot.

Source port: 53853.

Dest port: 53.

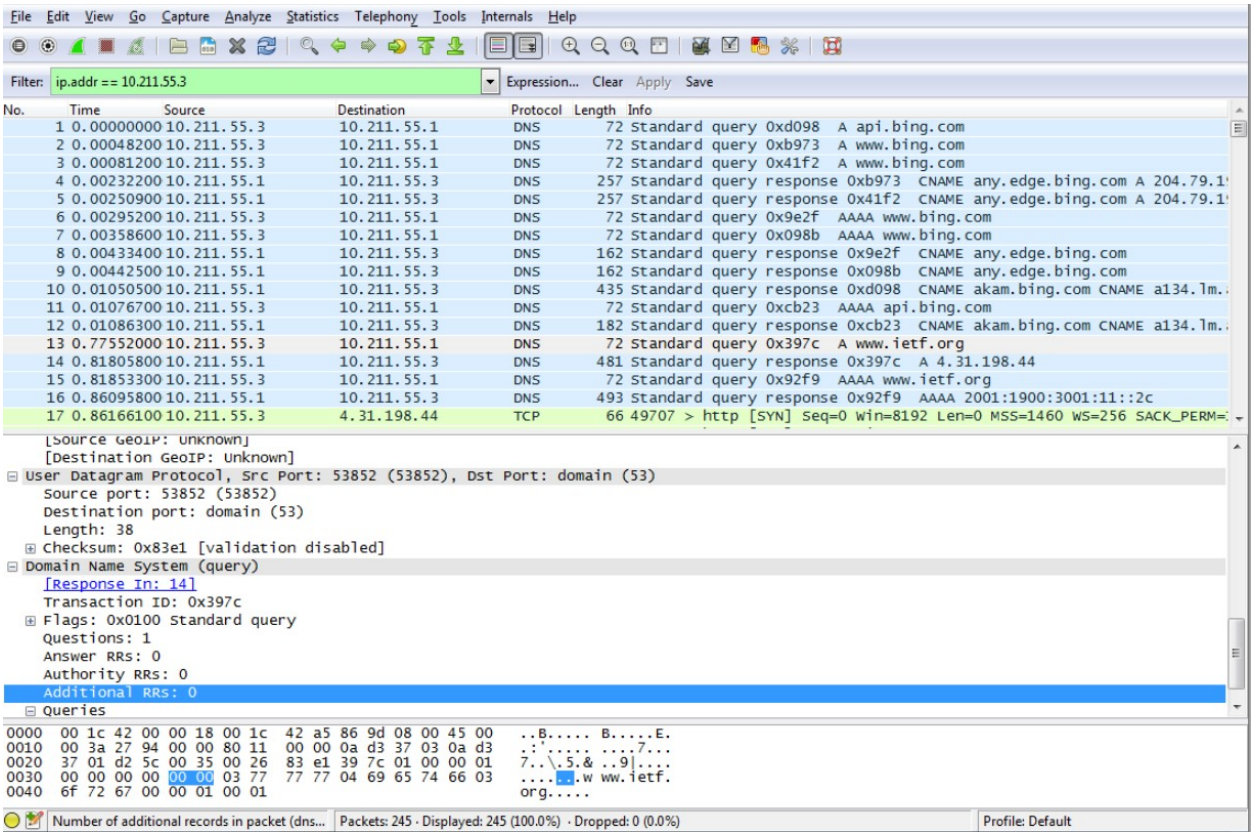
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



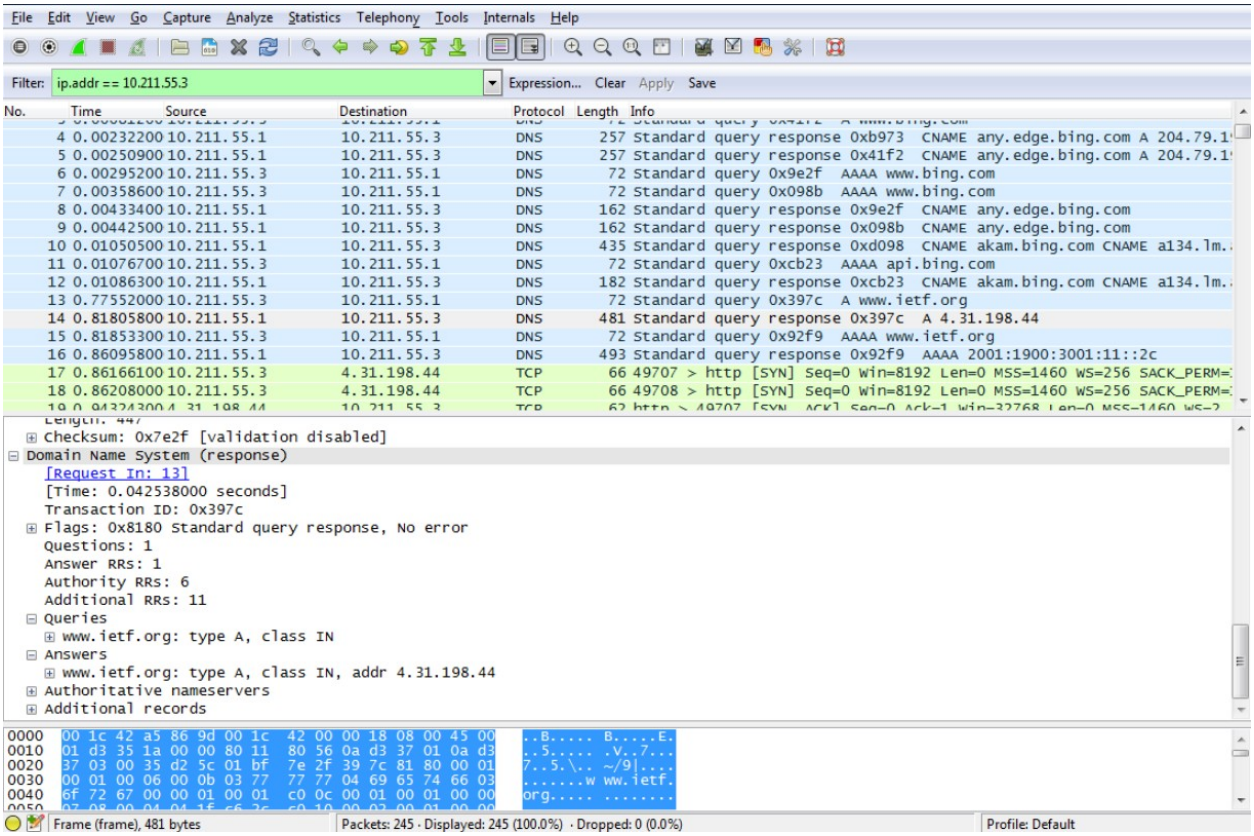
The screenshot shows that the DNS message was sent to 10.211.55.1. This matches the DNS server listed by the command ipconfig /all.

7. Examine the DNS query message. What “Type” of DNS query is it 1 ? Does the query message contain any “answers”? It is a “type A” query, which is for a standard host address resource record. No answers as shown in screenshot (one question).

A table of all the different “types” is available in your textbook (see “resource record types”).



8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain? One answer containing the IP address of www.ietf.org (see screenshot)



9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Yes, as seen in the prior screenshot, the destination address is 4.31.198.44 which is the address provided by the DNS server for www.ietf.org.

10. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

11. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers? Provide a screenshot.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

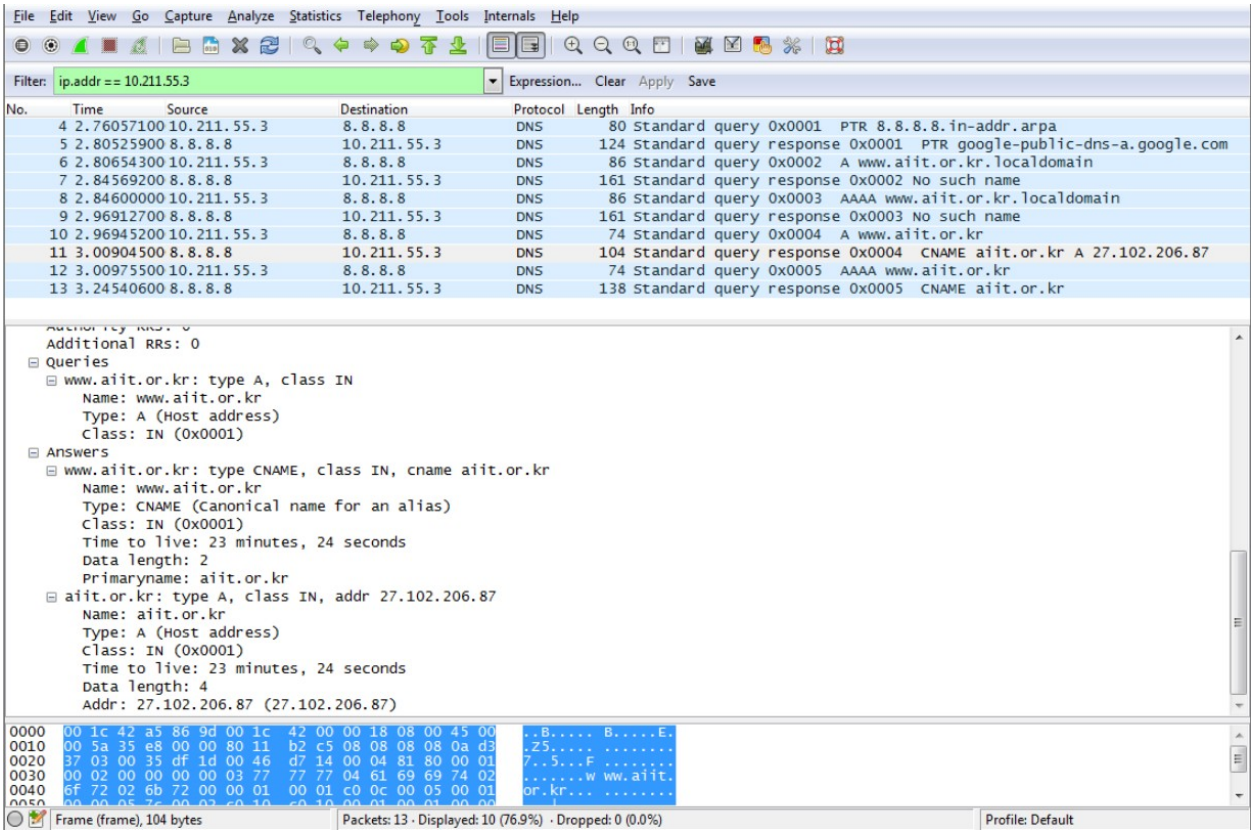
I was unable to get this to work with bitsy.mit.edu so I used the Google public DNS 8.8.8.8. The query is sent to 8.8.8.8 (not the default local DNS server).

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Same as before (Type A, 1 question, 0 answers).

14. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain? Provide a screenshot.

<u>Two answers, one a CNAME RR and the other a type A RR. See the screenshot.</u>



.