# Lab Task: 12

***_____786**
**_____****

**Name: Muhammad Sherjeel Akhtar**

**Roll No: 20p-0101**

**Subject: Computer Networks Lab**

**Submitted To Respected**
**Ma’am: Hurmat Hidayat**

**Section: BCS-5B**

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

**Answer:**

**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.*

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

**Answer:**

**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.

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

**Answer:**

**frigate:**Desktop drb$ nslookup pku.edu.cn ns2.cuhk.edu.hk
**Server:** ns2.cuhk.edu.hk
**Address:** 137.189.6.21#53

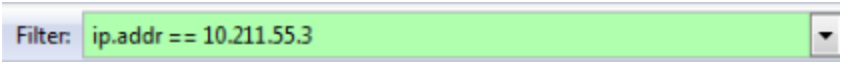
**Name:** pku.edu.cn
**Address:** 162.105.131.113

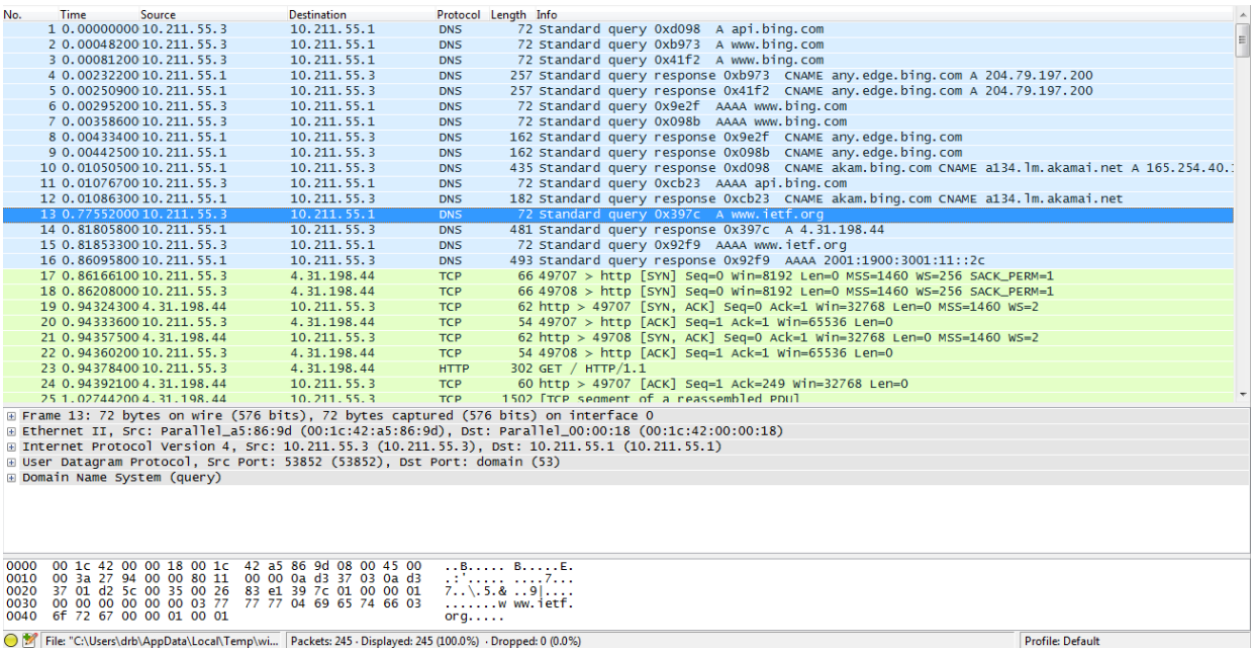
I was unable to get any of the DNS servers listed above to answer a query for a Yahoo mail server (even cn.mail.yahoo.com was refused) so I just queried another Chinese university
(Peking University).

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

**Answer:**

### Filtering: Step 1:






## Demonstration:


## Conclusion:

**UDP as shown in the screenshot.**

# Question 5: What is the destination port for the DNS query message? What is the source port of DNS response message?

**Answer:**

**Keypoint:**

Use the screenshot.

**Data Acquired:**

- Source port: 53853
- Dest port: 53.

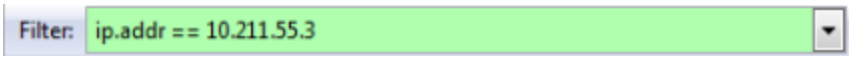
# Question 6: To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

**Answer:**

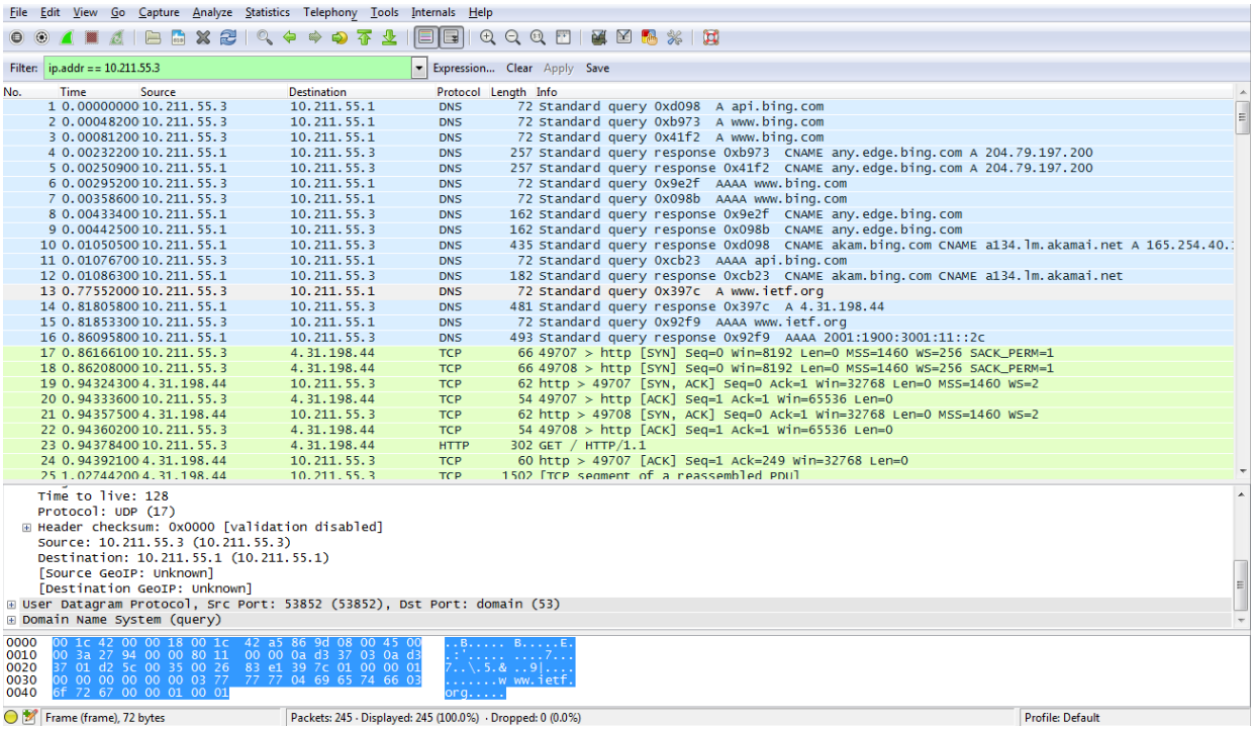
**Initial Step:**

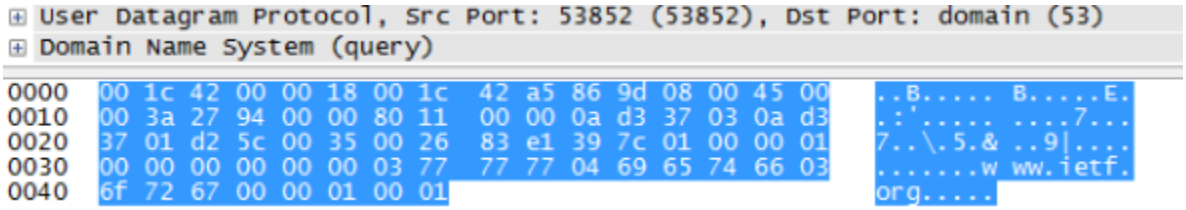
**Applying Filter**

**Demonstration:**




**Wireshark Acquired Data:**






**Conclusion:**

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.**

**Keypoint:** *The results are same as where acquired by running the command* ***"ipconfig /all".***

# Question 7: Examine the DNS query message. What "Type" of DNS query is it 1 ? Does the query message contain any "answers"?

**Answer:**

**Information Acquired:**

**Query Type:**

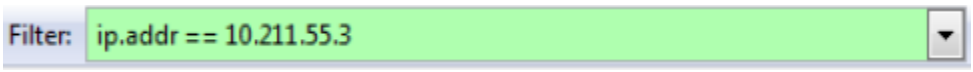
This is a query of "**type A**", which is for a standard host address resource record.

**Using Screenshot As A Resource:**

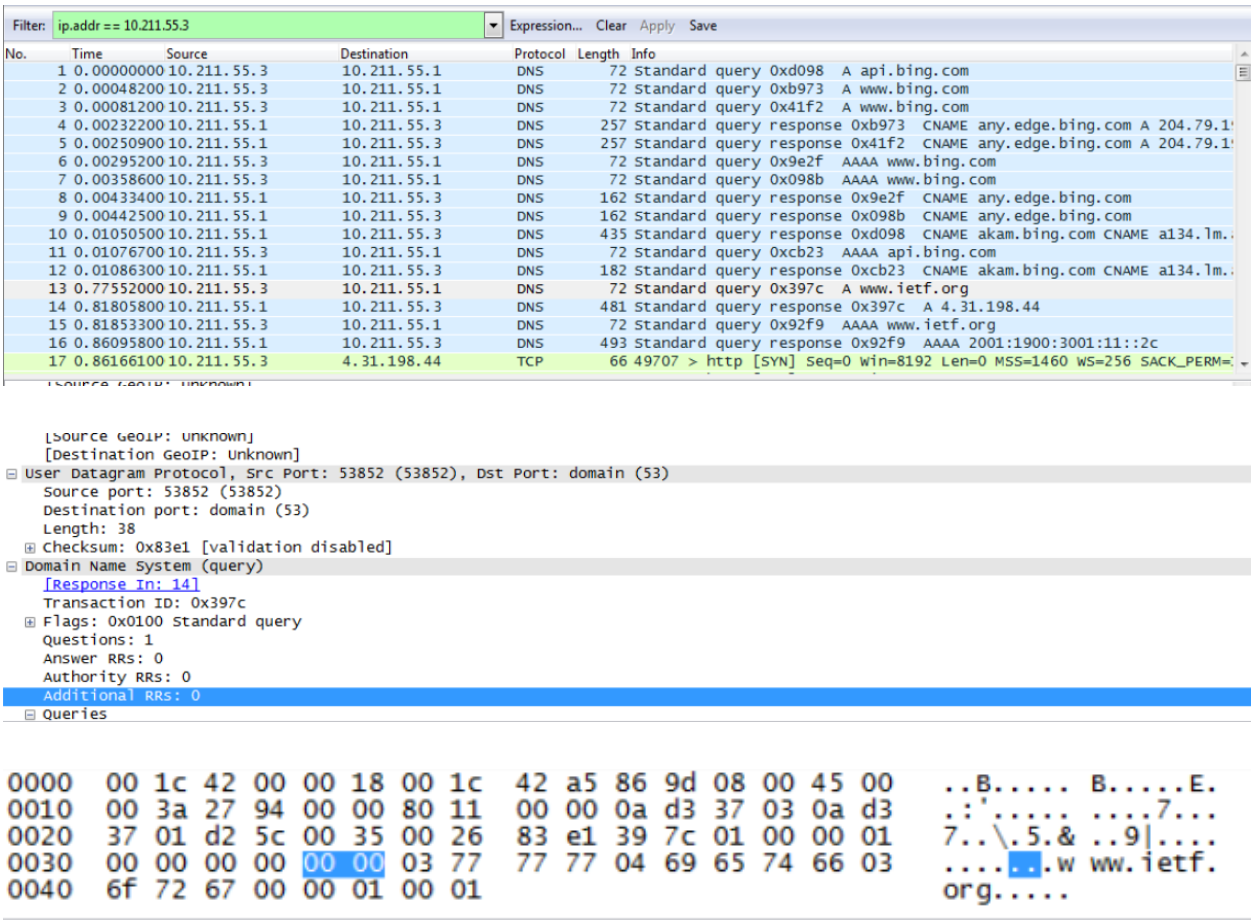
No answers as shown in screenshot of first question.

## Visual Demonstration:

**Step 1:** Applying Filter




**Step 2:** Observing the information attained




## Question 8: Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

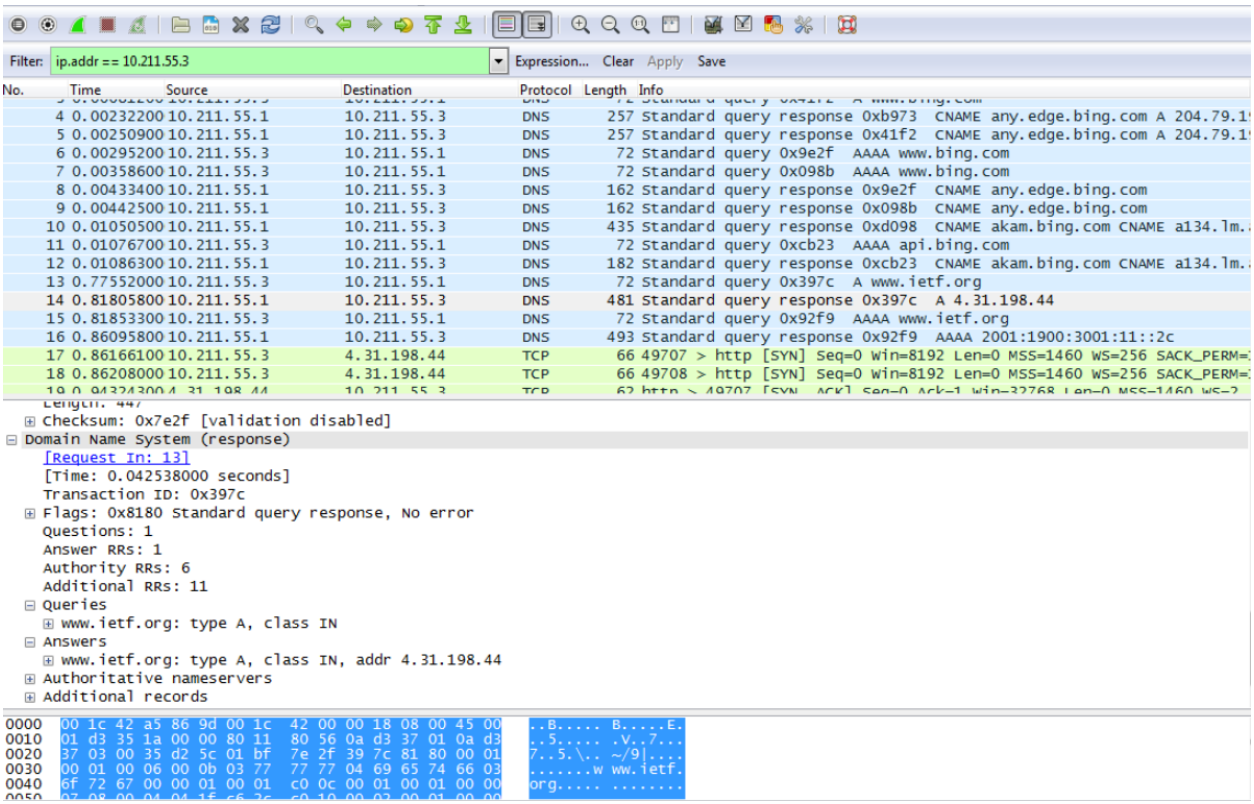
**Answer:**

**Keypoint:**

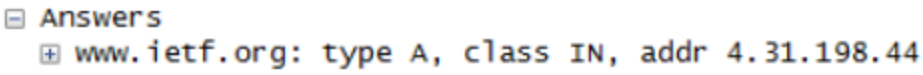
There will be only one answer containing the IP address of the given site which is www.ietf.org

**Visual Demonstration:**

Have a look at the screenshot attached below.




**Detailed View:**




*So there will be only one answer that will contain the IP Address of the given site.*

# Question 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?

**Answer:**

**Conclusion:**

Yes, as you can see in the previous screenshot,

**Destination address:** 4.31.198.44

This is the address provided by the Domain Name Server for the site www.ietf.org.

## Question 10: This web page contains images. Before retrieving each image, does your host issue new DNS queries?

**Answer:**

No, all the images are loaded from the site www.ietf.org

**Conclusion:**

***No additional DNS queries are necessary.***