Name :

Abubaker Attique

Roll no :

P20-0560

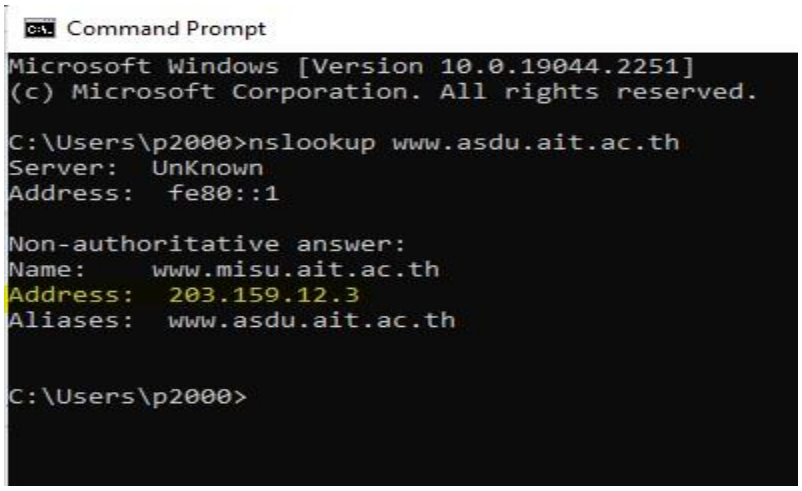
Lab no : 9 (Homework)

Task:

Do the following (and write down the results):

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

The IP address is 203.159.12.3.



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

I used the webpage for Cambridge University in England. This webpage is http://www.cam.ac.uk. The authoritative DNS server is **primary.dns.cam.ac.uk.**

```
Command Prompt

C:\Users\p2000>nslookup -type=NS www.cam.ac.uk
Server:  UnKnown
Address:  fe80::1

cam.ac.uk
        primary name server = primary.dns.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1669218230
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)

C:\Users\p2000>
```

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

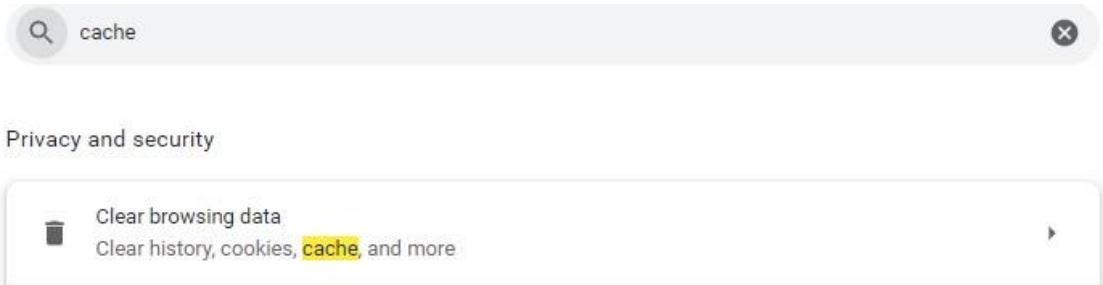
The IP address for the DNS server if queried for Yahoo! mail server is **87.248.119.252**.

```
Command Prompt

C:\Users\p2000>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.119.252

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\p2000>
```

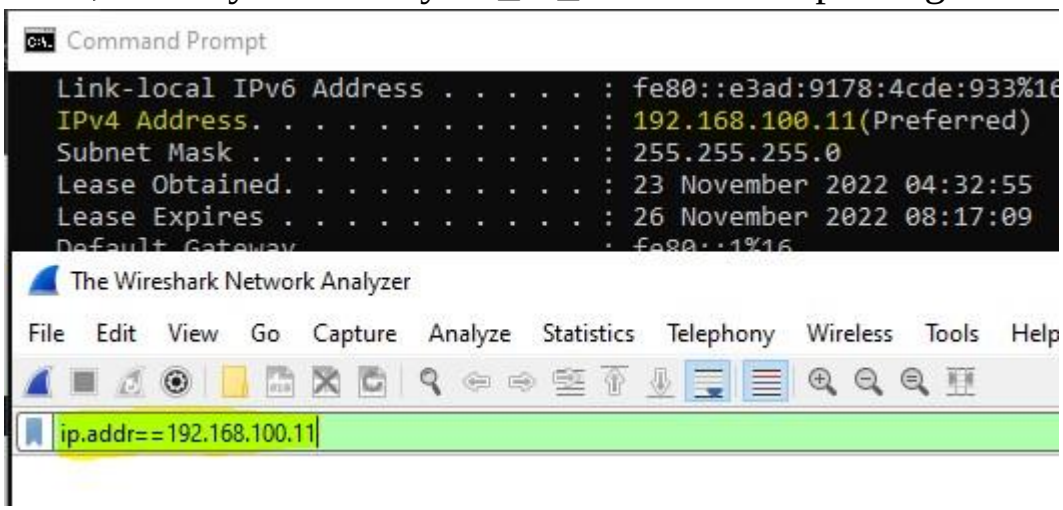
Tracing DNS with Wireshark :

- Use ipconfig to empty the DNS cache in your host.
-

- Open your browser and empty your browser cache.



- Open Wireshark and enter “ip.addr == your_IP_address” into the filter, where you obtain your_IP_address with ipconfig.



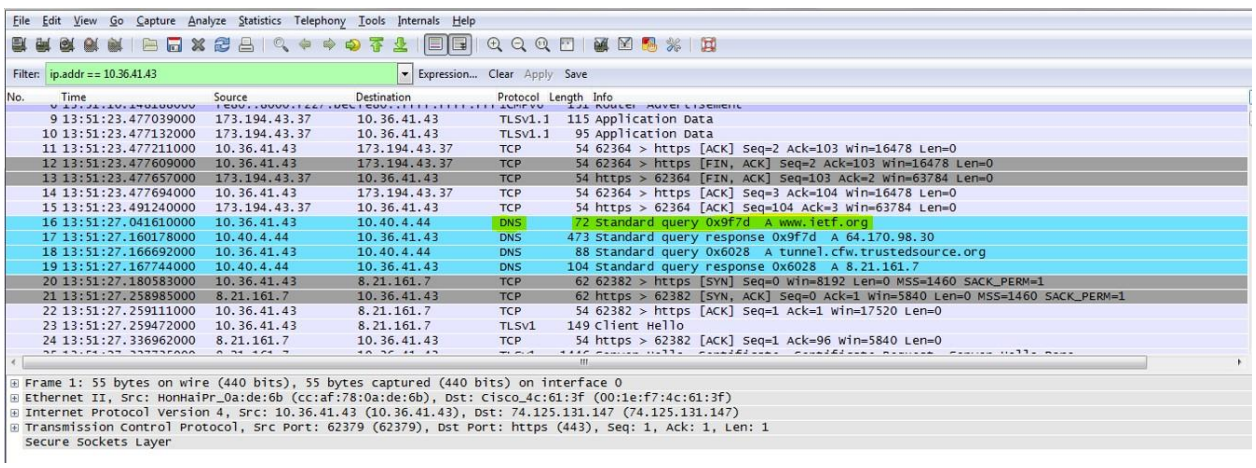
- Start packet capture in Wireshark.
- With your browser, visit the Web page: http://www.ietf.org ● Stop packet capture.

Task: Answer The following

1. Locate the DNS query and response messages. Are theysent over UDP or TCP?

Ans) The DNS query and response messages are sent over user Datagram protocol UDP.

```
User Datagram Protocol, Src Port: 50133 (50133), Dst Port: domain (53)
  Source port: 50133 (50133)
  Destination port: domain (53)
  Length: 38
⊞ Checksum: 0x3832 [validation disabled]
Domain Name System (query)
```



2. What is the destination port for the DNS query message?What is the source port of DNS response messages?

Ans)

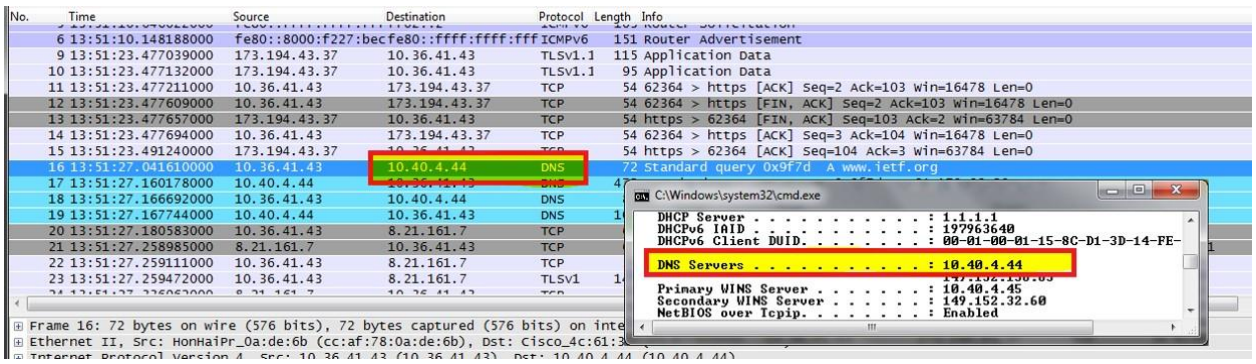
Source Port = 50133

Destination Port = 53

```
User Datagram Protocol, Src Port: 50133 (50133), Dst Port: domain (53)
  Source port: 50133 (50133)
  Destination port: domain (53)
  Length: 38
⊞ Checksum: 0x3832 [validation disabled]
Domain Name System (query)
```

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

Ans) Yes, It is the same IP address as that of my local DNS server 10.40.4.44.



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

Ans) NO, The message does not contain any "answers" and the Type of DNS query message is **Type A.**

```
⊟ Domain Name System (query)
    [Response In: 17]
    Transaction ID: 0x9f7d
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ www.ietf.org: type A, class IN
```

5. Examine the DNS response message. How many“answers” are provided? What do each of these answers contain?

Ans) The response message contained only one response to the query, which was the site's IP address **64.170.98.30**. Despite this, it provided **6** authoritative nameservers and **11** other responses with additional information.

```
⊟ Answers
  ⊞ www.ietf.org: type A, class IN, addr 64.170.98.30
⊟ Authoritative nameservers
  ⊞ ietf.org: type NS, class IN, ns ns1.yyz1.afilias-nst.info
  ⊞ ietf.org: type NS, class IN, ns ns0.ietf.org
  ⊞ ietf.org: type NS, class IN, ns ns1.sea1.afilias-nst.info
  ⊞ ietf.org: type NS, class IN, ns ns1.ams1.afilias-nst.info
  ⊞ ietf.org: type NS, class IN, ns ns1.mia1.afilias-nst.info
```

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

Ans) The SYN packet's destination is 64.170.98.30, which is the same address as the type "A" address of the webpage provided in the DNS response message.

7. This web page contains images. Before retrieving eachimage, does your host issue new DNS queries?

Ans) Yes, my host did perform new DNS queries before retrieving the images. One such query, for example, was for an image from open-stand.org. Until this query, the image corresponding to the page was not returned.

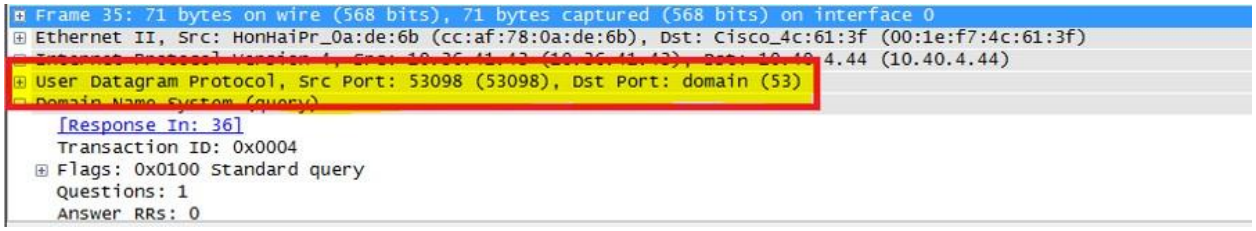
Now let's play with nslookup4.

- **Start packet capture.**
- **Do an nslookup on www.mit.edu ● Stop packet capture.**

8. What is the destination port for the DNS query message?What is the source port of DNS response messages?

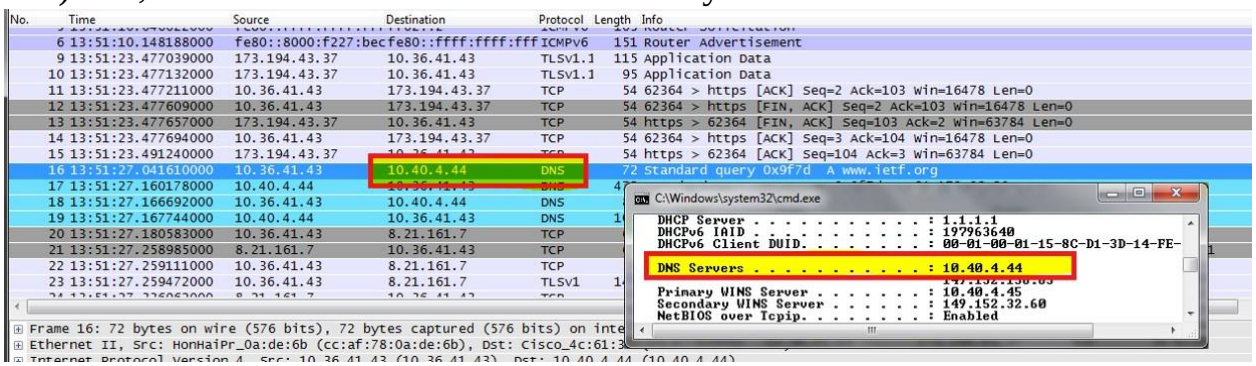
Ans) Source Port = 50133

Destination Port = 53



9. To what IP address is the DNS query message sent? Is thisthe IP address of your default local DNS server?

Ans) Yes, It is the same IP address as that of my local DNS server 10.40.4.44.



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

Ans) The DNS query message is a type "A" query that contains only one question and no “answers”.

11. Examine the DNS response message. How many“answers” are provided? What do each of these answers contain?

Ans) The response message contains only one response to the previously mentioned query, which is the type "A" address of http://www.mit.edu or 18.9.22.169. It also included data on three authoritative nameservers and three additional records.
