

**Name :**

**Abubaker Attique**

**Roll no :**

**P20-0560**

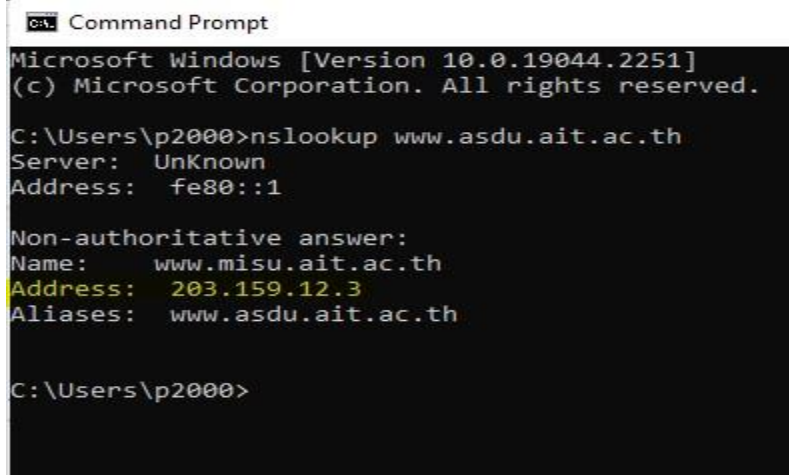
**Lab no : 9 (Homework)**

## 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.



```
Command Prompt
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\p2000>nslookup www.asdu.ait.ac.th
Server: UnKnown
Address: fe80::1

Non-authoritative answer:
Name: www.misu.ait.ac.th
Address: 203.159.12.3
Aliases: www.asdu.ait.ac.th

C:\Users\p2000>
```

- 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

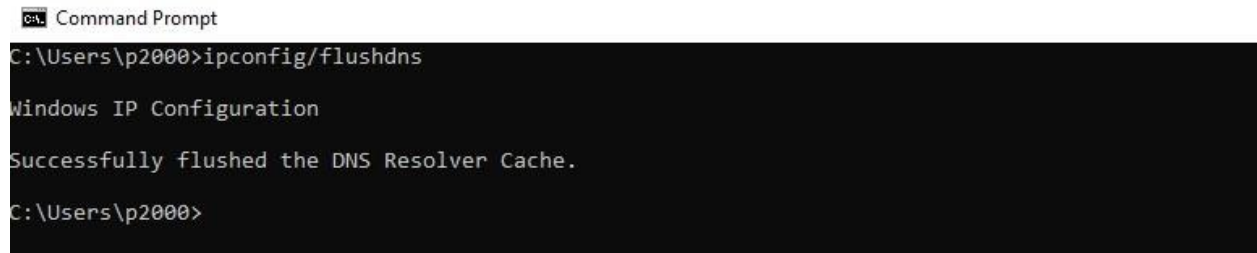
C:\Users\p2000>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 87.248.119.252

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.
- 



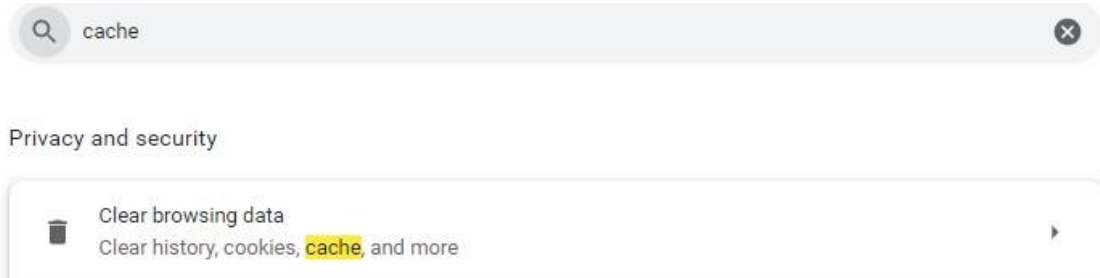
```
C:\Users\p2000>ipconfig /flushdns

Windows IP Configuration

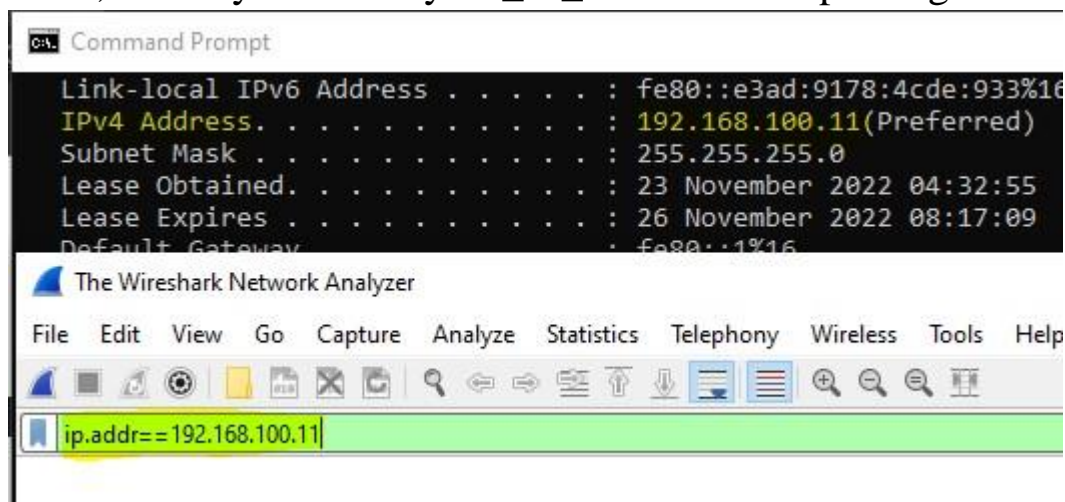
Successfully flushed the DNS Resolver Cache.

C:\Users\p2000>
```

- 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 they sent 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)
```

No.	Time	Source	Destination	Protocol	Length	Info
9	13:51:23.477039000	173.194.43.37	10.36.41.43	TLSv1.1	115	Application Data
10	13:51:23.477132000	173.194.43.37	10.36.41.43	TLSv1.1	95	Application Data
11	13:51:23.477211000	10.36.41.43	173.194.43.37	TCP	54	62364 > https [ACK] Seq=2 Ack=103 win=16478 Len=0
12	13:51:23.477609000	10.36.41.43	173.194.43.37	TCP	54	62364 > https [FIN, ACK] Seq=2 Ack=103 win=16478 Len=0
13	13:51:23.477657000	173.194.43.37	10.36.41.43	TCP	54	https > 62364 [FIN, ACK] Seq=103 Ack=2 win=63784 Len=0
14	13:51:23.477694000	10.36.41.43	173.194.43.37	TCP	54	62364 > https [ACK] Seq=3 Ack=104 win=16478 Len=0
15	13:51:23.491240000	173.194.43.37	10.36.41.43	TCP	54	https > 62364 [ACK] Seq=104 Ack=3 win=63784 Len=0
16	13:51:27.041610000	10.36.41.43	10.40.4.44	DNS	72	Standard query 0x9f7d A www.ietf.org
17	13:51:27.160178000	10.40.4.44	10.36.41.43	DNS	473	Standard query response 0x9f7d A 64.170.98.30
18	13:51:27.166692000	10.36.41.43	10.40.4.44	DNS	88	Standard query 0x6028 A tunnel.cfw.trustedsource.org
19	13:51:27.167744000	10.40.4.44	10.36.41.43	DNS	104	Standard query response 0x6028 A 8.21.161.7
20	13:51:27.180583000	10.36.41.43	8.21.161.7	TCP	62	62382 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
21	13:51:27.258985000	8.21.161.7	10.36.41.43	TCP	62	https > 62382 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1
22	13:51:27.259111000	10.36.41.43	8.21.161.7	TCP	54	62382 > https [ACK] Seq=1 Ack=1 win=17520 Len=0
23	13:51:27.259472000	10.36.41.43	8.21.161.7	TLSv1	149	Client Hello
24	13:51:27.336962000	8.21.161.7	10.36.41.43	TCP	54	https > 62382 [ACK] Seq=1 Ack=96 win=5840 Len=0

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0  
 Ethernet II, Src: HonHaiPr\_0a:de:6b (cc:af:78:0a:de:6b), Dst: cisco\_4c:61:3f (00:1e:f7:4c:61:3f)  
 Internet Protocol Version 4, Src: 10.36.41.43 (10.36.41.43), Dst: 74.125.131.147 (74.125.131.147)  
 Transmission Control Protocol, Src Port: 62379 (62379), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1  
 Secure Sockets Layer

### 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? Use ipconfig 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.

The image shows a Wireshark packet capture. The packet list on the left shows a DNS query (Frame 16) from 10.36.41.43 to 10.40.4.44. The packet details on the right show the DNS query structure. Overlaid on the Wireshark window is a Windows command prompt window showing the output of the 'ipconfig' command. The 'DNS Servers' line in the command prompt output is highlighted with a red box and shows the IP address 10.40.4.44.

4. Examine the DNS query message. What “Type” of DNS query 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**.

The image shows the packet details for a DNS query. The 'Domain Name System (query)' section is expanded, showing the 'Flags: 0x0100 Standard query' and 'Questions: 1'. The 'Answer RRs: 0' field is highlighted with a red box. The 'Queries' section is also expanded, showing the query for '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.afiliast.net
  ietf.org: type NS, class IN, ns ns0.ietf.org
  ietf.org: type NS, class IN, ns ns1.sea1.afiliast.net
  ietf.org: type NS, class IN, ns ns1.ams1.afiliast.net
  ietf.org: type NS, class IN, ns ns1.mia1.afiliast.net
```

**6. 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?**

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 each image, 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?

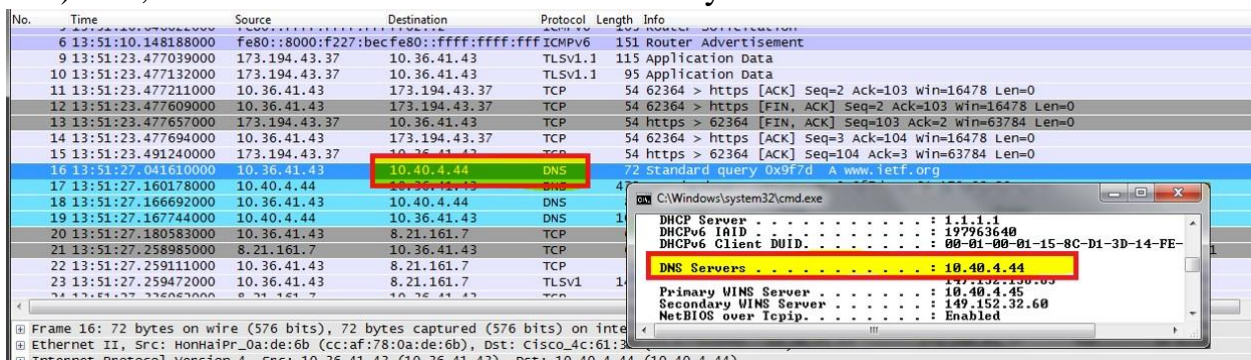
Ans) Source Port = 50133

Destination Port = 53



9. To what IP address is the DNS query message sent? Is this the 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 DNS query 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.

---

