



Name : Ammaar Naeem Laghari

Roll No : 20P-0180

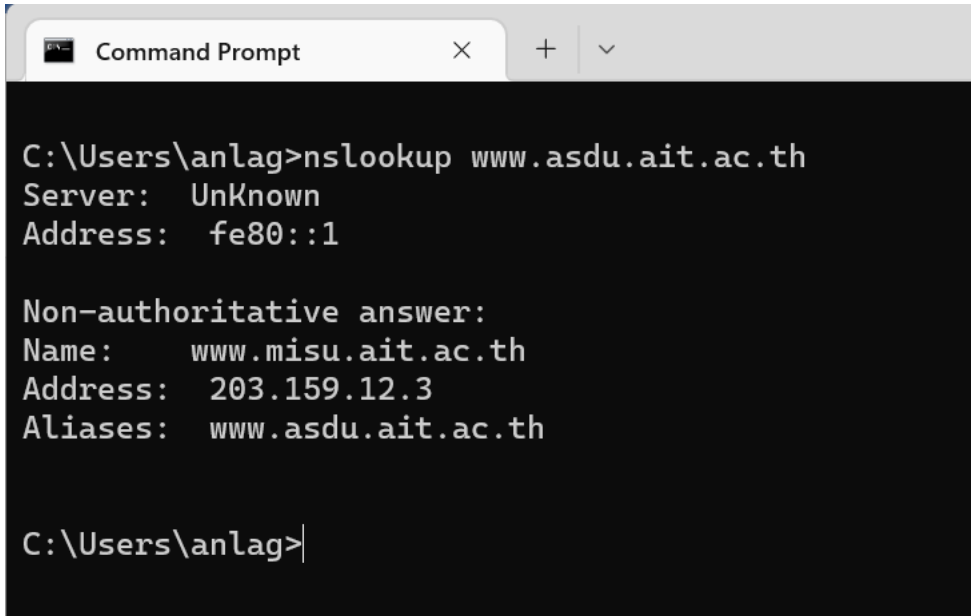
Section: BCS-5B

Course Name: Computer Networks LAB

Submitted to : Mam Hurmat Hidayat

nslookup Questions:

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



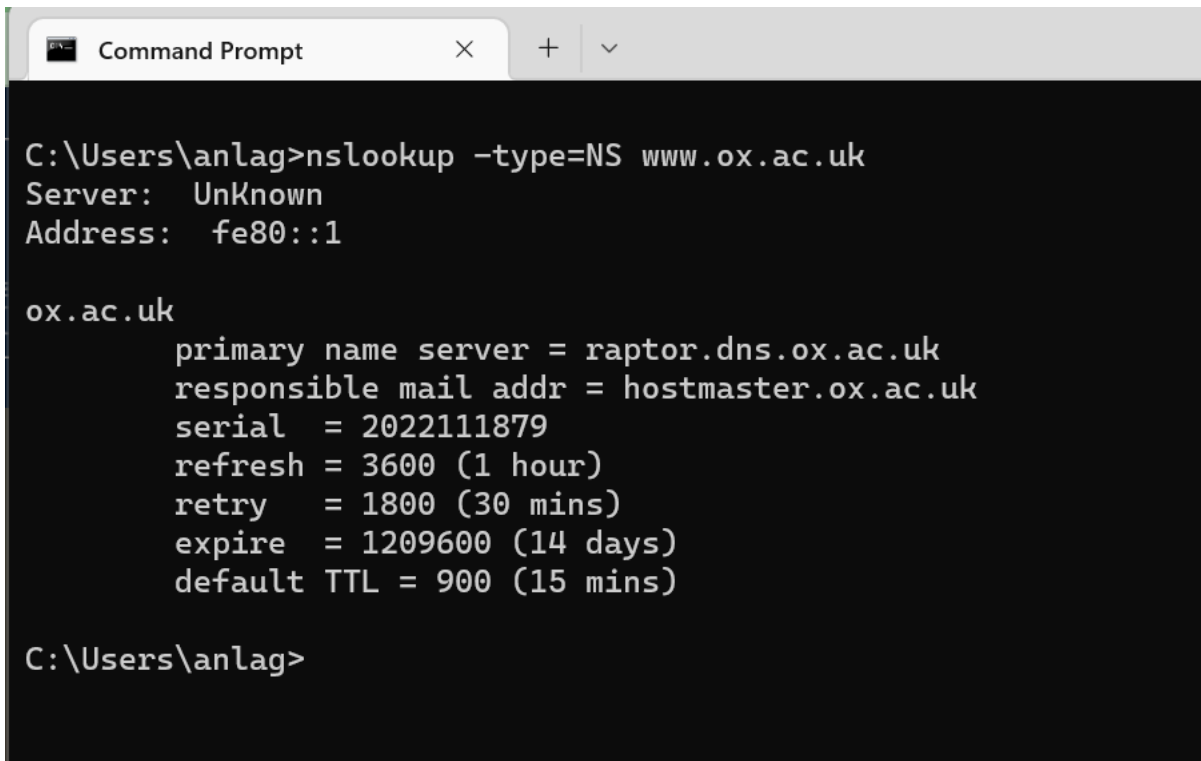
```
Command Prompt
C:\Users\anlag>nslookup www.asdu.ait.ac.th
Server: UnKnown
Address: fe80::1

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

C:\Users\anlag>
```

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

I used the webpage of oxford university in England. This webpage is www.ox.ac.uk.



```
Command Prompt
C:\Users\anlag>nslookup -type=NS www.ox.ac.uk
Server: UnKnown
Address: fe80::1

ox.ac.uk
    primary name server = raptor.dns.ox.ac.uk
    responsible mail addr = hostmaster.ox.ac.uk
    serial = 2022111879
    refresh = 3600 (1 hour)
    retry = 1800 (30 mins)
    expire = 1209600 (14 days)
    default TTL = 900 (15 mins)

C:\Users\anlag>
```

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 the Yahoo! mail server is 98.137.11.163

```
C:\Users\anlag>nslookup www.yahoo.com
Server:    UnKnown
Address:   fe80::1

Non-authoritative answer:
Name:      new-fp-shed.wg1.b.yahoo.com
Addresses: 2a00:1288:110:c305::1:8001
           2a00:1288:110:c305::1:8000
           98.137.11.163
           98.137.11.164
Aliases:   www.yahoo.com

C:\Users\anlag>
```

ipconfig Questions:

1)ipconfig/all

```
C:\Users\anlag>ipconfig/all

Windows IP Configuration

Host Name . . . . . : LAPTOP-1V1712A8
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address. . . . . : C8-09-A8-13-73-48
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : CA-09-A8-13-73-47
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : C8-09-A8-13-73-47
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2400:adcc:104:f600::c(Preferred)
Lease Obtained. . . . . : Saturday, November 19, 2022 9:13:04 PM
Lease Expires . . . . . : Sunday, November 20, 2022 9:13:04 PM
IPv6 Address. . . . . : 2400:adcc:104:f600:ac2f:bb98:c9d7:90f8(Preferred)
Temporary IPv6 Address. . . . . : 2400:adcc:104:f600:3918:66d6:4c7a:e4fc(Preferred)
Link-local IPv6 Address . . . . . : fe80::78c:6ddc:4f93:5d2f%10(Preferred)
IPv4 Address. . . . . : 192.168.18.29(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, November 19, 2022 9:13:06 PM
Lease Expires . . . . . : Saturday, November 19, 2022 10:13:06 PM
Default Gateway . . . . . : fe80::1%10
                             192.168.18.1
DHCP Server . . . . . : 192.168.18.1
DHCPv6 IAID . . . . . : 180881832
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-07-31-29-C8-09-A8-13-73-47
DNS Servers . . . . . : fe80::1%10
                             192.168.18.1
NetBIOS over Tcpip. . . . . : Enabled
```

Ethernet adapter Bluetooth Network Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : C8-09-A8-13-73-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

C:\Users\anlag>

2) ipconfig /displaydns

```
C:\Users\anlag>ipconfig /displaydns
```

```
Windows IP Configuration
```

```
www.digitallibrary.edu.pk
```

```
-----
```

```
Record Name . . . . . : www.digitallibrary.edu.pk
Record Type . . . . . : 5
Time To Live . . . . . : 6122
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : digitallibrary.edu.pk
```

```
Record Name . . . . . : digitallibrary.edu.pk
Record Type . . . . . : 1
Time To Live . . . . . : 6122
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 210.56.11.12
```

```
Record Name . . . . . : n1.comsats.net.pk
Record Type . . . . . : 1
Time To Live . . . . . : 6122
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 210.56.11.130
```

```
Record Name . . . . . : n2.comsats.net.pk
```

Record Name : n1.comsats.net.pk
Record Type : 1
Time To Live : 6122
Data Length : 4
Section : Additional
A (Host) Record . . . : 210.56.11.130

Record Name : n2.comsats.net.pk
Record Type : 1
Time To Live : 6122
Data Length : 4
Section : Additional
A (Host) Record . . . : 210.56.11.131

numen.nu.edu.pk

Record Name : numen.nu.edu.pk
Record Type : 1
Time To Live : 10751
Data Length : 4
Section : Answer
A (Host) Record . . . : 210.56.9.84

Record Name : root-e.pknic.pk
Record Type : 1
Time To Live : 10751
Data Length : 4

classroom.google.com

Record Name : classroom.google.com
Record Type : 28
Time To Live : 56
Data Length : 16
Section : Answer
AAAA Record : 2a00:1450:4019:80c::200e

Record Name : ns1.google.com
Record Type : 1
Time To Live : 56
Data Length : 4
Section : Additional
A (Host) Record : 216.239.32.10

Record Name : ns1.google.com
Record Type : 28
Time To Live : 56
Data Length : 16
Section : Additional
AAAA Record : 2001:4860:4802:32::a

Record Name : ns2.google.com
Record Type : 1
Time To Live : 56
Data Length : 4
Section : Additional

3)Ipconfig/flushdns

```
C:\Users\anlag>ipconfig /flushdns  
  
Windows IP Configuration  
  
Successfully flushed the DNS Resolver Cache.  
  
C:\Users\anlag>
```


TASKS

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

The image shows a Wireshark packet capture window. The top pane displays a list of packets. Packet 2801 is a DNS Standard query from 192.168.18.29 to 192.168.18.1. Packet 2801 is highlighted in green. The bottom pane shows the details of packet 2801, which is a User Datagram Protocol (UDP) packet. The source port is 62027 and the destination port is 53. The payload is a Domain Name System (DNS) query.

No.	Time	Source	Destination	Protocol	Length	Info
2749	23.706082	50.223.129.196	192.168.18.29	TCP	66	[TCP Retransmission] 443 → 21380 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=
2759	23.793368	3.0.66.145	192.168.18.29	TCP	66	[TCP Retransmission] 443 → 21381 [SYN, ACK] Seq=0 Ack=1 Win=32500 Len=
2760	23.793468	192.168.18.29	3.0.66.145	TCP	66	[TCP Dup ACK 2564#1] 21381 → 443 [ACK] Seq=551 Ack=1 Win=131072 Len=0
2800	24.050382	192.168.18.29	192.168.18.1	DNS	86	Standard query 0x8d27 A b16pap003.storage.live.com
2801	24.050382	192.168.18.29	192.168.18.1	DNS	86	Standard query 0x0afe AAAA b16pap003.storage.live.com
2853	24.225656	108.177.15.188	192.168.18.29	TCP	66	[TCP Retransmission] 5228 → 21366 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
2857	24.344452	216.58.209.131	192.168.18.29	TCP	66	[TCP Retransmission] 443 → 21368 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=

> Frame 2801: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{5...}

> Ethernet II, Src: IntelCor_13:73:47 (c8:09:a8:13:73:47), Dst: HuaweiTe_c9:75:a6 (58:d0:61:c9:75:a6)

> Internet Protocol Version 4, Src: 192.168.18.29, Dst: 192.168.18.1

> User Datagram Protocol, Src Port: 62027, Dst Port: 53

Source Port: 62027

Destination Port: 53

Length: 52

Checksum: 0xa5b4 [unverified]

[Checksum Status: Unverified]

[Stream index: 88]

> [Timestamps]

UDP payload (44 bytes)

> Domain Name System (query)

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

Source port = 62027

destination port = 53

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?

192.168.18.1

yes both are same

The image shows the output of the ipconfig command. The DNS Servers are listed as fe80::1%10 and 192.168.18.1. The IP address 192.168.18.1 is highlighted in green.

DHCP Server	: 192.168.18.1
DHCPv6 IAID	: 180881832
DHCPv6 Client DUID.	: 00-01-00-01-29-07-31-29-C8-09-A8-13-73-47
DNS Servers	: fe80::1%10
	: 192.168.18.1
NetBIOS over Tcpip.	: Enabled

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

No not any answer.

ip.addr == 192.168.18.29						
No.	Time	Source	Destination	Protocol	Length	Info
2749	23.706082	50.223.129.196	192.168.18.29	TCP	66	[TCP Retransmission] 443 → 21380 [
2759	23.793368	3.0.66.145	192.168.18.29	TCP	66	[TCP Retransmission] 443 → 21381 [
2760	23.793468	192.168.18.29	3.0.66.145	TCP	66	[TCP Dup ACK 2564#1] 21381 → 443 [
2800	24.050382	192.168.18.29	192.168.18.1	DNS	86	Standard query 0x8d27 A bl6pap003.
2801	24.050382	192.168.18.29	192.168.18.1	DNS	86	Standard query 0x0afe AAAA bl6pap0
2853	24.225656	108.177.15.188	192.168.18.29	TCP	66	[TCP Retransmission] 5228 → 21366 [
2857	24.344452	216.58.209.131	192.168.18.29	TCP	66	[TCP Retransmission] 443 → 21368 [

Source Port: 62027	0000	58 d0
Destination Port: 53	0010	00 48
Length: 52	0020	12 01
Checksum: 0xa5b4 [unverified]	0030	00 00
[Checksum Status: Unverified]	0040	07 73
[Stream index: 88]	0050	6d 00
> [Timestamps]		
UDP payload (44 bytes)		
▼ Domain Name System (query)		
Transaction ID: 0x0afe		
> Flags: 0x0100 Standard query		
Questions: 1		
Answer RRs: 0		
Authority RRs: 0		
Additional RRs: 0		
▼ Queries		
> bl6pap003.storage.live.com: type AAAA, class IN		

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

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?

7. This web page contains images. Before retrieving each image, does your host issue new

DNS queries?