

NAME : SHOAIB AKHTAR

ROLL NUMBER : 20P-0147

SECTION: BCS-9A

SUBMITTED TO : SIR

Muhammad ALI

1-NS LOOKUP

A-nslookup www.mahidol.ac.th

```
C:\Users\zeesh>nslookup www.mahidol.ac.th
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: mahidol.ac.th
Addresses: 2001:3c8:2707:10a0::10
           202.28.152.207
Aliases: www.mahidol.ac.th

C:\Users\zeesh>
```

B-nslookup -type=NS www.uninettunouniversity.net

```
C:\Users\zeesh>nslookup -type=NS www.uninettunouniversity.net
Server: UnKnown
Address: 192.168.0.1

uninettunouniversity.net
    primary name server = ns-645.awsdns-16.net
    responsible mail addr = awsdns-hostmaster.amazon.com
    serial = 1
    refresh = 7200 (2 hours)
    retry = 900 (15 mins)
    expire = 1209600 (14 days)
    default TTL = 86400 (1 day)

C:\Users\zeesh>
```

C->nslookup www.uninettunouniversity.netrsity.net mail.yahoo.com

```
C:\Users\zeesh>nslookup www.uninettunouniversity.netrsity.net mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:    UnKnown
Address:   87.248.119.251

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\zeesh>
```

2-IP CONFIG

A-ipconfig/all

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

Windows IP Configuration

```
Host Name . . . . . : KING
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection I218-LM
Physical Address. . . . . : 14-58-D0-05-7C-C1
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Local Area Connection* 1:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : E8-2A-EA-C6-02-5B
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 #2
Physical Address. . . . . : EA-2A-EA-C6-02-5A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Ethernet adapter VMware Network Adapter VMnet1:

```
Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Physical Address. . . . . : 00-50-56-C0-00-01
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::67d3:e193:690e:194b%5(Preferred)
IPv4 Address. . . . . : 192.168.174.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, November 19, 2022 6:20:37 PM
Lease Expires . . . . . : Saturday, November 19, 2022 7:20:34 PM
```

B-ipconfig/displaydns

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

Windows IP Configuration

www.gstatic.com

```
-----
Record Name . . . . . : www.gstatic.com
Record Type . . . . . : 1
Time To Live . . . . . : 276
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 142.250.181.163
```

array607.prod.do.dsp.mp.microsoft.com

```
-----
Record Name . . . . . : array607.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 1485
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 51.104.167.186
```

scontent.fpew2-1.fna.fbcdn.net

```
-----
Record Name . . . . . : scontent.fpew2-1.fna.fbcdn.net
Record Type . . . . . : 1
Time To Live . . . . . : 2200
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 101.50.104.19
```

uop.edu.pk

```
-----
Record Name . . . . . : uop.edu.pk
Record Type . . . . . : 1
Time To Live . . . . . : 17706
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 121.52.147.18
```

C-ipconfig/flushdns

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\zeesh>
```

3. Tracing DNS with Wireshark

Step1

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\zeesh>ipconfig
```

Step2-

×

Clear browsing data

Time range

Last hour

1 item. Includes autocompletions in the address bar.

✓

Download history

None

✓

Cookies and other site data

From 3 sites. Signs you out of most sites.

✓

Cached images and files

Frees up less than 57.6 MB. Some sites may load more slowly on your next visit.

Sync is turned off. When you turn on sync, this data will be cleared across all synced devices signed in to zeeshankhan6669@gmail.com. To clear browsing data from this device only, [sign out first](#).

Clear now

Cancel

Step3-Run wireshark.

Step4- Start capturing

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

The DNS query and response messages are sent over UDP.

```

Frame 16: 72 bytes on wire (576 bits), 72 bytes captured (576 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)
Internet Protocol Version 4, Src: 10.26.41.42 (10.26.41.42), Dst: 10.40.4.44 (10.40.4.44)
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)

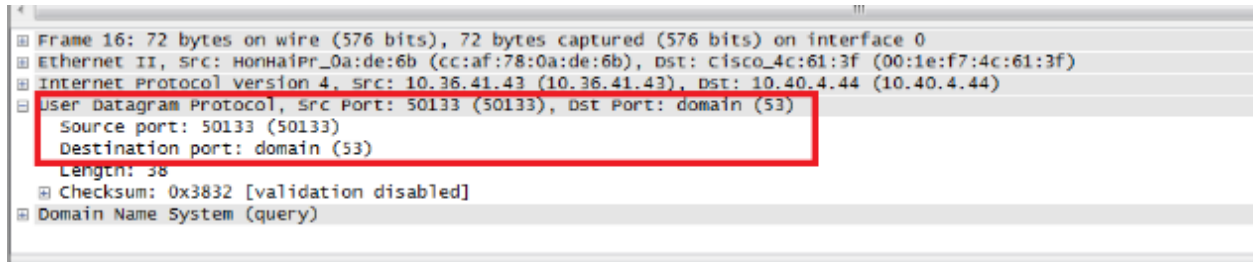
```

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

response message?

The destination port is 53

The source port is 50133



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?

Yes it is the same IP address as that of my local DNS server.

173.194.43.37	TCP
10.36.41.43	TCP
10.40.4.44	DNS
10.36.41.43	DNS
10.40.4.44	DNS

Examine the DNS query message. What “Type” of DNS query is it?

Does the query

message contain any “answers”?

The query message was a type “A” query, but the message did not have “answers.”


```

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
0000 00 1e 77 4c 01 5f cc af 78 0a 0e 00 08 00 45 00 ...La?...x..k..E.
0010 00 3a 47 7d 00 00 80 11 b1 93 0a 24 29 2b 0a 28 ...:G)... ..$)+.C
0020 04 2c c3 d5 00 35 00 26 38 32 9f 7d 01 00 00 01 .....5.& 82.}..

```

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

The response message contained one answer to the query which was the site's address [64.170.98.30]. Although it also provided 6 authoritative nameservers, and 11 other responses containing additional information.

```

Authority RRs: 6
Additional RRs: 11
Queries
www.ietf.org: type A, class IN
Name: www.ietf.org
Type: A (Host address)
Answers
www.ietf.org: type A, class IN, addr 64.170.98.30
Authoritative nameservers
ietf.org: type NS, class IN, ns ns1.yyz1.afillias-nst.info
ietf.org: type NS, class IN, ns ns0.ietf.org
ietf.org: type NS, class IN, ns ns1.seal.afillias-nst.info
ietf.org: type NS, class IN, ns ns1.ams1.afillias-nst.info
ietf.org: type NS, class IN, ns ns1.mial.afillias-nst.info
000 cc af 78 0a de 6b 00 1e f7 4c 61 3f 08 00 45 00 ...x..k..La?...E.
010 01 cb 63 b4 40 00 7e 11 55 cb 0a 28 04 2c 0a 24 ...c.@...U..(...$
020 29 2b 00 35 c3 d5 01 b7 1a 58 9f 7d 81 80 00 01 ...)+.5....x.}....
030 00 01 00 06 00 0b 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf.
040 6f 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00 org.....
050 07 08 00 04 40 aa 62 1e c0 10 00 02 00 01 00 00 ...@.b. ....
0070 69 6c 69 61 73 7d 6e 73 74 04 69 6e 66 6f 00 c0 fillias-nst.info

```

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?

The destination of the SYN packet is 64.170.98.30, the same address that was provided in the DNS response message as the type “A” address of the webpage

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

DNS queries?

Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made.

127.946857000	10.36.41.43	10.40.4.44	DNS	74 Standard query 0x485a A open-stand.org
127.985597000	10.40.4.44	10.36.41.43	DNS	474 Standard query response 0x663f A 64.170.98.31
127.987664000	10.36.41.43	10.40.4.44	DNS	74 Standard query 0xf4e6 A rfc-editor.org
127.987673000	10.36.41.43	10.40.4.44	DNS	74 Standard query 0xa59c A tools.ietf.org
128.002019000	10.36.41.43	64.170.98.30	HTTP	427 GET /css/ietf4.css HTTP/1.1
128.002419000	10.36.41.43	64.170.98.30	HTTP	427 GET /css/ietf3.css HTTP/1.1
128.005693000	10.36.41.43	64.170.98.30	TCP	62 62384 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
128.008610000	10.36.41.43	64.170.98.30	TCP	62 62385 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
128.011399000	10.36.41.43	64.170.98.30	TCP	62 62386 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
128.011717000	10.40.4.44	10.36.41.43	DNS	172 Standard query response 0x485a A 50.116.53.77
128.012972000	64.170.98.30	10.36.41.43	TCP	62 http > 62384 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
128.013081000	10.36.41.43	64.170.98.30	TCP	54 62384 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
128.014198000	10.36.41.43	64.170.98.30	HTTP	427 GET /css/ietf2.css HTTP/1.1
128.014918000	10.36.41.43	64.170.98.30	HTTP	423 GET /images/ietflogotrans.gif HTTP/1.1
128.016496000	64.170.98.30	10.36.41.43	TCP	62 http > 62385 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
128.016611000	10.36.41.43	64.170.98.30	TCP	54 62385 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
128.017149000	10.36.41.43	64.170.98.30	HTTP	420 GET /images/chat-trans.png HTTP/1.1
128.018448000	10.36.41.43	10.40.4.44	DNS	76 Standard query 0x4ce2 A trustee.ietf.org
128.019338000	64.170.98.30	10.36.41.43	TCP	62 http > 62386 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
128.019447000	10.36.41.43	64.170.98.30	TCP	54 62386 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
128.020179000	10.36.41.43	64.170.98.30	HTTP	422 GET /images/openstand-md.png HTTP/1.1
128.020377000	64.170.98.30	10.36.41.43	TCP	62 http > 62387 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
128.020377000	64.170.98.30	10.36.41.43	TCP	54 62387 > http [ACK] Seq=1 Ack=1 win=17520 Len=0

```

C:\Users\zeesh>nslookup www.mit.edu
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:128:1ab::255e
           2a02:26f0:128:1ad::255e
           23.66.153.41
Aliases: www.mit.edu
         www.mit.edu.edgekey.net

C:\Users\zeesh>

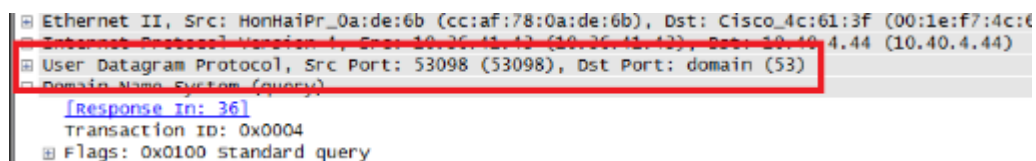
```

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

response message?

Destination Port: 53

Source Port: 53098



```

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: 10.36.41.13 (10.36.41.13), Dst: 10.40.4.44 (10.40.4.44)
User Datagram Protocol, Src Port: 53098 (53098), Dst Port: domain (53)
Domain Name System (query)
  Response in: 36
  Transaction ID: 0x0004
  Flags: 0x0100 standard query

```

To what IP address is the DNS query message sent? Is this the IP address of your default

local DNS server?

The DNS query message is sent to the same address as my default local DNS server.

Examine the DNS query message. What “Type” of DNS query is it? Does the query

message contain any “answers”?

The DNS query message is a type “A” query, containing only one question and not containing any answers.

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

The response message contains one answer to the query which is the type “A” address of <http://www.mit.edu> or 18.9.22.169. It also contained information on 3 authoritative nameservers and 3 additional records.

Provide a screenshot.

Offset	Hex	ASCII
0000	00 1e f7 4c 61 3f cc af 78 0a de 6b 08 00 45 00	...La?... x..k..E.
0010	00 35 15 ac 00 00 80 11 e3 69 0a 24 29 2b 0a 28	.5..... .i.\$)+.(
0020	04 2c c8 af 00 35 00 21 1c 65 00 03 01 00 00 015.! .e.....
0030	00 00 00 00 00 00 03 6d 69 74 03 65 64 75 00 00m it.edu..
0040	02 00 01	...