

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

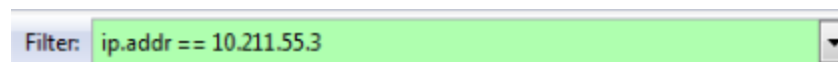
Address: 162.105.131.113

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:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xd098 A api.bing.com
2	0.00048200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xb973 A www.bing.com
3	0.00081200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x41f2 A www.bing.com
4	0.00232200	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0xb973 CNAME any.edge.bing.com A 204.79.197.200
5	0.00250900	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0x41f2 CNAME any.edge.bing.com A 204.79.197.200
6	0.00295200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x9e2f AAAA www.bing.com
7	0.00358600	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x098b AAAA www.bing.com
8	0.00433400	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x9e2f CNAME any.edge.bing.com
9	0.00442500	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x098b CNAME any.edge.bing.com
10	0.01050500	10.211.55.1	10.211.55.3	DNS	435	Standard query response 0xd098 CNAME akam.bing.com CNAME a134.lm.akamai.net A 165.254.40.1
11	0.01076700	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xcb23 AAAA api.bing.com
12	0.01086300	10.211.55.1	10.211.55.3	DNS	182	Standard query response 0xcb23 CNAME akam.bing.com CNAME a134.lm.akamai.net
13	0.77552000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x397c A www.ietf.org
14	0.81805800	10.211.55.1	10.211.55.3	DNS	481	Standard query response 0x397c A 4.31.198.44
15	0.81853300	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x92f9 AAAA www.ietf.org
16	0.86095800	10.211.55.1	10.211.55.3	DNS	493	Standard query response 0x92f9 AAAA 2001:1900:3001:11::2c
17	0.86166100	10.211.55.3	4.31.198.44	TCP	66	49707 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	0.86208000	10.211.55.3	4.31.198.44	TCP	66	49708 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	0.94324300	4.31.198.44	10.211.55.3	TCP	62	http > 49707 [SYN, ACK] Seq=0 Ack=1 win=32768 Len=0 MSS=1460 WS=2
20	0.94333600	10.211.55.3	4.31.198.44	TCP	54	49707 > http [ACK] Seq=1 Ack=1 win=65536 Len=0
21	0.94357500	4.31.198.44	10.211.55.3	TCP	62	http > 49708 [SYN, ACK] Seq=0 Ack=1 win=32768 Len=0 MSS=1460 WS=2
22	0.94360200	10.211.55.3	4.31.198.44	TCP	54	49708 > http [ACK] Seq=1 Ack=1 win=65536 Len=0
23	0.94378400	10.211.55.3	4.31.198.44	HTTP	302	GET / HTTP/1.1
24	0.94392100	4.31.198.44	10.211.55.3	TCP	60	http > 49707 [ACK] Seq=1 Ack=249 win=32768 Len=0
25	1.02744200	4.31.198.44	10.211.55.3	TCP	1502	TCP segment of a reassembled PDU

Frame 13: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 Ethernet II, Src: Parallel_a5:86:9d (00:1c:42:a5:86:9d), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
 Internet Protocol Version 4, Src: 10.211.55.3 (10.211.55.3), Dst: 10.211.55.1 (10.211.55.1)
 User Datagram Protocol, Src Port: 53852 (53852), Dst Port: domain (53)
 Domain Name System (query)

```

0000  00 1c 42 00 00 18 00 1c 42 a5 86 9d 08 00 45 00  ..B.... B....E.
0010  00 3a 27 94 00 00 80 11 00 00 0a d3 37 03 0a d3  .'. .... 7...
0020  37 01 d2 5c 00 35 00 26 83 e1 39 7c 01 00 00 01  7...\5.& ..9]...
0030  00 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66  ....w ww.ietf.
0040  6f 72 67 00 00 01 00 01                                org....
  
```

File: "C:\Users\drb\AppData\Local\Temp\wi... Packets: 245 · Displayed: 245 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Demonstration:

13	0.77552000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x397c A www.ietf.org
----	------------	-------------	-------------	-----	----	--------------------------------------

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.

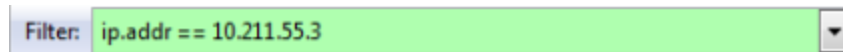
Question 6: To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Answer:

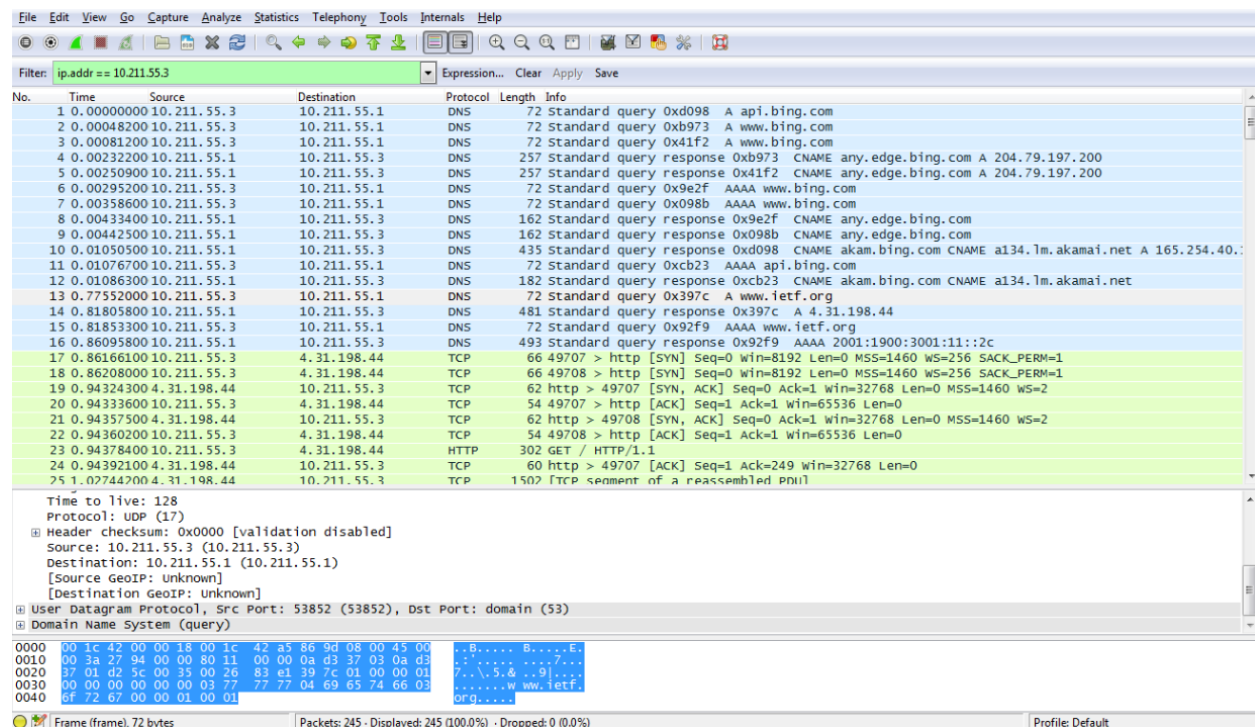
Initial Step:

Applying Filter

Demonstration:



Wireshark Acquired Data:



User Datagram Protocol, Src Port: 53852 (53852), Dst Port: domain (53)															
Domain Name System (query)															
0000	00	1c	42	00	00	18	00	1c	42	a5	86	9d	08	00	45 00
0010	00	3a	27	94	00	00	80	11	00	00	0a	d3	37	03	0a d3
0020	37	01	d2	5c	00	35	00	26	83	e1	39	7c	01	00	00 01
0030	00	00	00	00	00	00	03	77	77	77	04	69	65	74	66 03
0040	6f	72	67	00	00	01	00	01							

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:

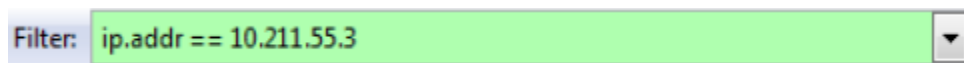
This is a query of “**type A**”, which is for a standard host address resource record.

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

Filter: `ip.addr == 10.211.55.3` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xd098 A api.bing.com
2	0.00048200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xb973 A www.bing.com
3	0.00081200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x41f2 A www.bing.com
4	0.00232200	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0xb973 CNAME any.edge.bing.com A 204.79.1
5	0.00250900	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0x41f2 CNAME any.edge.bing.com A 204.79.1
6	0.00295200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x9e2f AAAA www.bing.com
7	0.00358600	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x098b AAAA www.bing.com
8	0.00433400	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x9e2f CNAME any.edge.bing.com
9	0.00442500	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x098b CNAME any.edge.bing.com
10	0.01050500	10.211.55.1	10.211.55.3	DNS	435	Standard query response 0xd098 CNAME akam.bing.com CNAME a134.1m.
11	0.01076700	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xcb23 AAAA api.bing.com
12	0.01086300	10.211.55.1	10.211.55.3	DNS	182	Standard query response 0xcb23 CNAME akam.bing.com CNAME a134.1m.
13	0.77552000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x397c A www.ietf.org
14	0.81805800	10.211.55.1	10.211.55.3	DNS	481	Standard query response 0x397c A 4.31.198.44
15	0.81853300	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x92f9 AAAA www.ietf.org
16	0.86095800	10.211.55.1	10.211.55.3	DNS	493	Standard query response 0x92f9 AAAA 2001:1900:3001:11::2c
17	0.86166100	10.211.55.3	4.31.198.44	TCP	66	49707 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=

[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

User Datagram Protocol, Src Port: 53852 (53852), Dst Port: domain (53)
Source port: 53852 (53852)
Destination port: domain (53)
Length: 38
Checksum: 0x83e1 [validation disabled]

Domain Name System (query)
[Response in: 14]
Transaction ID: 0x397c
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries

```

0000  00 1c 42 00 00 18 00 1c 42 a5 86 9d 08 00 45 00  ..B.....B.....E.
0010  00 3a 27 94 00 00 80 11 00 00 0a d3 37 03 0a d3  :.'.....7...
0020  37 01 d2 5c 00 35 00 26 83 e1 39 7c 01 00 00 01  7..\5.&..9|...
0030  00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03  ....w ww.ietf.
0040  6f 72 67 00 00 01 00 01 77 77 04 69 65 74 66 03  org....

```

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.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.00232200	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0xb973 CNAME any.edge.bing.com A 204.79.1
5	0.00250900	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0x41f2 CNAME any.edge.bing.com A 204.79.1
6	0.00295200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x9e2f AAAA www.bing.com
7	0.00358600	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x098b AAAA www.bing.com
8	0.00433400	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x9e2f CNAME any.edge.bing.com
9	0.00442500	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x098b CNAME any.edge.bing.com
10	0.01050500	10.211.55.1	10.211.55.3	DNS	435	Standard query response 0xd098 CNAME akam.bing.com CNAME a134.1m.
11	0.01076700	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xcb23 AAAA api.bing.com
12	0.01086300	10.211.55.1	10.211.55.3	DNS	182	Standard query response 0xcb23 CNAME akam.bing.com CNAME a134.1m.
13	0.77552000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x397c A www.ietf.org
14	0.81805800	10.211.55.1	10.211.55.3	DNS	481	Standard query response 0x397c A 4.31.198.44
15	0.81853300	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x92f9 AAAA www.ietf.org
16	0.86095800	10.211.55.1	10.211.55.3	DNS	493	Standard query response 0x92f9 AAAA 2001:1900:3001:11::2c
17	0.86166100	10.211.55.3	4.31.198.44	TCP	66	49707 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
18	0.86208000	10.211.55.3	4.31.198.44	TCP	66	49708 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
19	0.86243000	10.211.55.3	10.211.55.3	TCP	62	http > 49707 [SYN, ACK] Seq=0 Ack=1 win=22768 Len=0 MSS=1460 WS=7
Checksum: 0x7e2f [validation disabled]						
Domain Name System (response)						
[Request In: 13]						
[Time: 0.042538000 seconds]						
Transaction ID: 0x397c						
Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 1						
Authority RRs: 6						
Additional RRs: 11						
Queries						
www.ietf.org: type A, class IN						
Answers						
www.ietf.org: type A, class IN, addr 4.31.198.44						
Authoritative nameservers						
Additional records						
0000	00 1c 42 a5 86 9d 00 1c	42 00 00 18 08 00 45 00	..B....B....E.			
0010	01 d3 35 1a 00 00 80 11	80 56 0a d3 37 01 0a d3	.5....v.7...			
0020	37 03 00 35 d2 5c 01 bf	7e 2f 39 7c 81 80 00 01	7..5...~/9]...			
0030	00 01 00 06 00 0b 03 77	77 77 04 69 65 74 66 03w ww.ietf.			
0040	6f 72 67 00 00 01 00 01	c0 0c 00 01 00 01 00 00	org.....			
0050	07 08 00 04 04 15 c6 3c	c0 10 00 03 00 01 00 00				

Detailed View:

Answers
 www.ietf.org: type A, class IN, addr 4.31.198.44

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.