

Computer Networks Lab Task

Name:

Abubakkar Abdullah

Roll No: 20P-0045

Section: BSCS(5B)

1. Run nslookup to obtain the IP address of a Web server in Asia.

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.

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

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.

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

```
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).

4. Locate the DNS query and response messages. Are they sent using the UDP or TCP protocol?

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 204.79.197.200
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 a134.1m.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 a134.1m.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	10.211.55.1	10.211.55.3	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	1.02744700	4.31.198.44	10.211.55.3	TCP	1502	[TCP segment of a reassembled pdu]

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x0000 [validation disabled]

Source: 10.211.55.3 (10.211.55.3)

Destination: 10.211.55.1 (10.211.55.1)

[Source GeoIP: unknown]

[Destination GeoIP: unknown]

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 d37.....

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 03W ww.ietf.

0040 8f 72 67 00 00 01 00 01 org.....

Frame (frame), 72 bytes

Packets: 245 - Displayed: 245 (100.0%) - Dropped: 0 (0.0%)

Profile: Default

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`.

7. Examine the DNS query message. What “Type” of DNS query is it 1 ? Does the query message contain any “answers”? It is a “type A” query, which is for a standard host address resource record. No answers as shown in screenshot (one question).

A table of all the different “types” is available in your textbook (see “resource record types”).

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

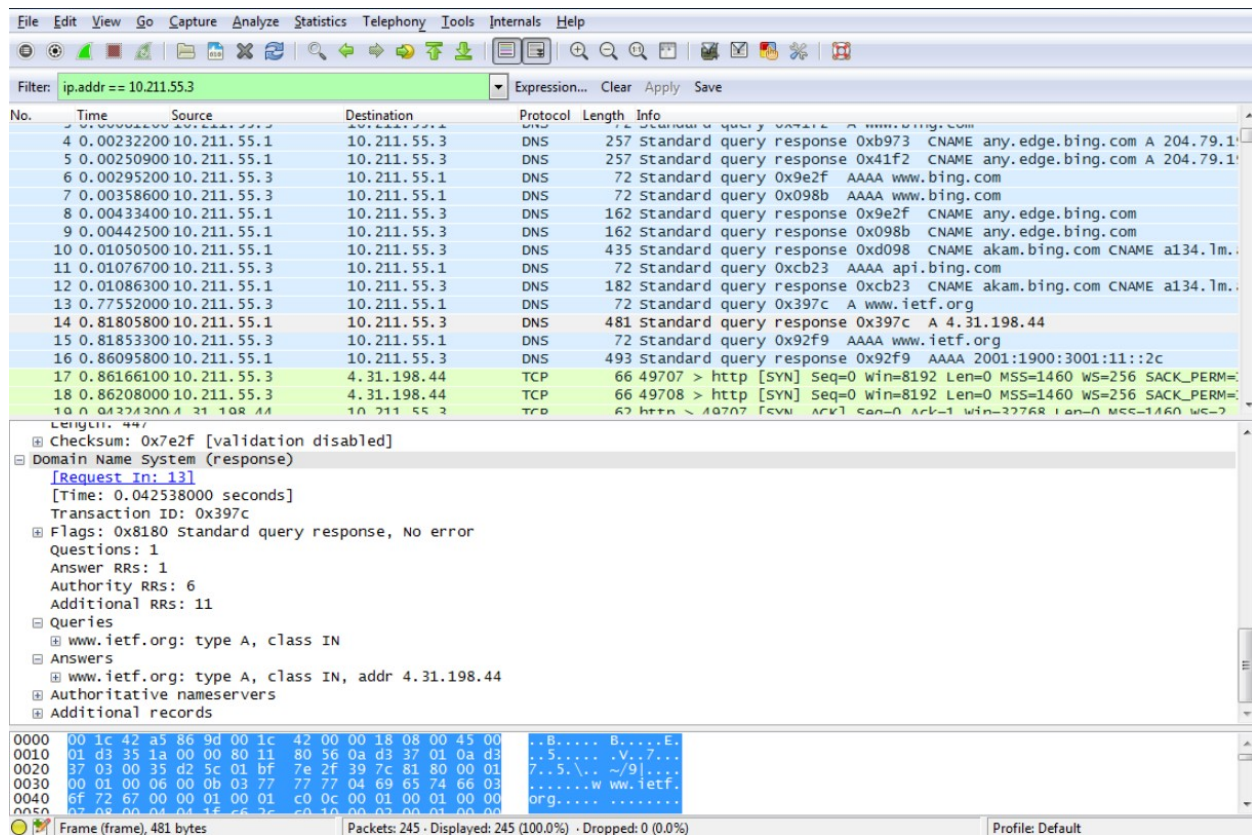
```

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.....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 03 77 77 77 04 69 65 74 66 03 ....w ww.ietf.
0040 6f 72 67 00 00 01 00 01 org.....

```

Number of additional records in packet (dns...) Packets: 245 · Displayed: 245 (100.0%) · Dropped: 0 (0.0%) Profile: Default

8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain? One answer containing the IP address of www.ietf.org (see screenshot)



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?

Yes, as seen in the prior screenshot, the destination address is 4.31.198.44 which is the address provided by the DNS server for www.ietf.org.

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

11. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers? Provide a screenshot.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

I was unable to get this to work with bitsy.mit.edu so I used the Google public DNS 8.8.8.8. The query is sent to 8.8.8.8 (not the default local DNS server).

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

Same as before (Type A, 1 question, 0 answers).

14. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain? Provide a screenshot.

Two answers, one a CNAME RR and the other a type A RR. See the screenshot.

Wireshark packet capture showing DNS traffic. The packet list shows a query and a response. The packet details pane shows the structure of the response, including a CNAME record and an A record. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
4	2.76057100	10.211.55.3	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
5	2.80525900	8.8.8.8	10.211.55.3	DNS	124	Standard query response 0x0001 PTR google-public-dns-a.google.com
6	2.80654300	10.211.55.3	8.8.8.8	DNS	86	Standard query 0x0002 A www.aiit.or.kr.localdomain
7	2.84569200	8.8.8.8	10.211.55.3	DNS	161	Standard query response 0x0002 No such name
8	2.84600000	10.211.55.3	8.8.8.8	DNS	86	Standard query 0x0003 AAAA www.aiit.or.kr.localdomain
9	2.96912700	8.8.8.8	10.211.55.3	DNS	161	Standard query response 0x0003 No such name
10	2.96945200	10.211.55.3	8.8.8.8	DNS	74	Standard query 0x0004 A www.aiit.or.kr
11	3.00904500	8.8.8.8	10.211.55.3	DNS	104	Standard query response 0x0004 CNAME aiit.or.kr A 27.102.206.87
12	3.00975500	10.211.55.3	8.8.8.8	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
13	3.24540600	8.8.8.8	10.211.55.3	DNS	138	Standard query response 0x0005 CNAME aiit.or.kr

Additional RRs: 0

Queries

- www.aiit.or.kr: type A, class IN
Name: www.aiit.or.kr
Type: A (Host address)
Class: IN (0x0001)

Answers

- www.aiit.or.kr: type CNAME, class IN, cname aiit.or.kr
Name: www.aiit.or.kr
Type: CNAME (Canonical name for an alias)
Class: IN (0x0001)
Time to live: 23 minutes, 24 seconds
Data length: 2
Primaryname: aiit.or.kr
- aiit.or.kr: type A, class IN, addr 27.102.206.87
Name: aiit.or.kr
Type: A (Host address)
Class: IN (0x0001)
Time to live: 23 minutes, 24 seconds
Data length: 4
Addr: 27.102.206.87 (27.102.206.87)

0000 00 1c 42 a5 86 9d 00 1c 42 00 00 18 08 00 45 00 ..B....B....E.
0010 00 5a 35 e8 00 00 80 11 b2 c5 08 08 08 08 0a d3 .ZS.....
0020 37 03 00 35 df 1d 00 46 d7 14 00 04 81 80 00 01 7..5...F.....
0030 00 02 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit.
0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 05 00 01 or.kr.....
0050 00 00 05 77 00 03 c0 10 c0 10 00 01 00 00 00 00

Frame (frame), 104 bytes Packets: 13 · Displayed: 10 (76.9%) · Dropped: 0 (0.0%) Profile: Default