

Name: Stuti Parmar
Student ID: 218516625

Assignment 1 - EECS 3214

QUESTION 2:

Q.4) The following screenshot specifies the located DNS queries and response messages. Out of which there are 2 DNS queries and 2 response messages.

The screenshot shows a Wireshark packet capture of DNS traffic. The packet list at the top shows four packets:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 1 | 0.000000 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0x02a7 HTTPS mask-h2.icloud.com |
| 2 | 0.000079 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0xbd11 A mask-h2.icloud.com |
| 5 | 0.011366 | 130.63.10.18 | 10.24.199.55 | DNS | 195 | Standard query response 0x02a7 HTTPS mask-h2.icloud.com CNAME mask.apple-dns.net SOA ns-1096.awsdns-09... |
| 6 | 0.011367 | 130.63.10.18 | 10.24.199.55 | DNS | 545 | Standard query response 0xbd11 A mask-h2.icloud.com CNAME mask.apple-dns.net A 172.224.186.14 A 172.22... |

The packet details for packet 6 (a response) are expanded, showing the domain name system (response) and the authoritative nameservers:

- Frame 6: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface en0
- Ethernet II, Src: Cisco_3c:2b:7f (f8:39:18:3c:2b:7f), Dst: Apple_44:70:38 (3c:06:30:44:70:38)
- Internet Protocol Version 4, Src: 130.63.10.18, Dst: 10.24.199.55
- User Datagram Protocol, Src Port: 53, Dst Port: 64497
 - Source Port: 53
 - Destination Port: 64497
 - Length: 511
 - Checksum: 0x3c33 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 1]
- [Timestamps]
- UDP payload (503 bytes)
- Domain Name System (response)
 - Transaction ID: 0xbd11
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 9
 - Authority RRs: 13
 - Additional RRs: 5
 - Queries
 - Answers
 - Authoritative nameservers

The packet bytes pane shows the raw data of the packet, including the domain name system (response) and the authoritative nameservers.

I used 'udp.port == 53' to check for UDP to TCP protocol. As specified in screenshot below, the DNS queries and response messages are all sent over UDP.

After Using ipconfig to determine the IP address of your local DNS server, The IP address for DNS servers are: 130.63.10.18. Comparing the 2 IP addresses we get that both IP addresses are same. If the IP addresses are the same, it means that the DNS query is being sent to the local DNS server.

```
stuti — -zsh — 80x24

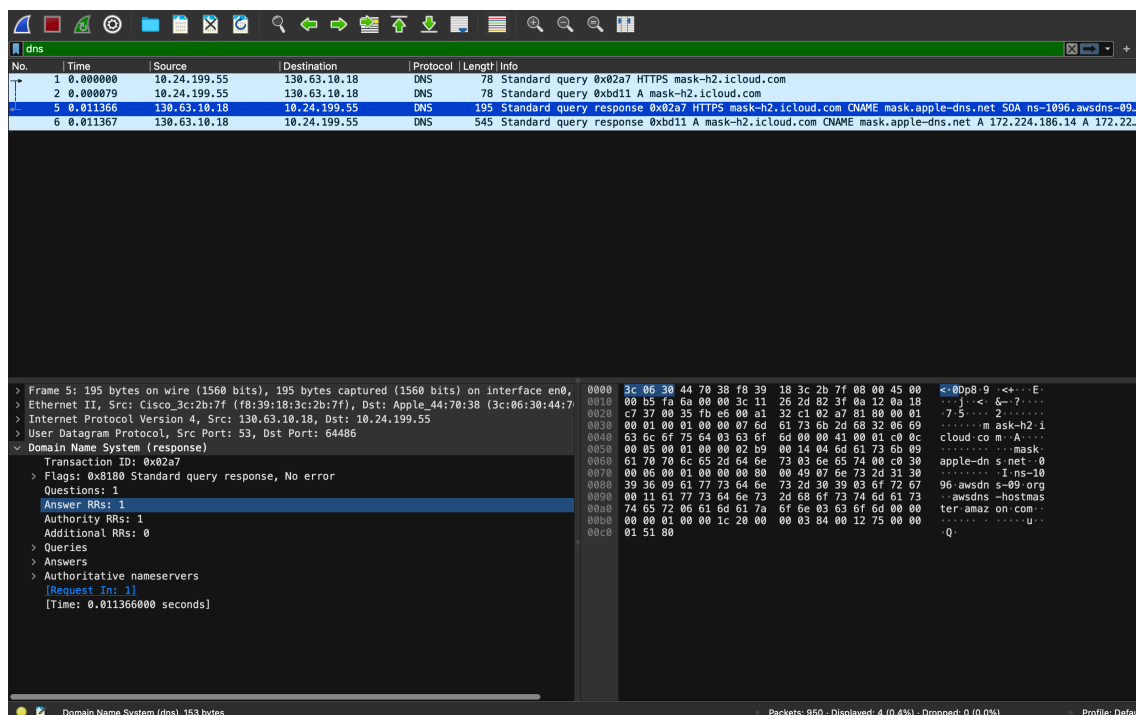
domain : a.e.f.ip6.arpa
options : mdns
timeout : 5
flags : Request A records
reach : 0x00000000 (Not Reachable)
order : 300800

resolver #7
domain : b.e.f.ip6.arpa
options : mdns
timeout : 5
flags : Request A records
reach : 0x00000000 (Not Reachable)
order : 301000

DNS configuration (for scoped queries)

resolver #1
nameserver[0] : 130.63.10.18
nameserver[1] : 130.63.9.18
if_index : 12 (en0)
flags : Scoped, Request A records
reach : 0x00000002 (Reachable)
stuti@stutis-MacBook-Pro ~ %
```

Q.8) Answers provided by DNS response message is 1 and 9
(Screenshots added below)



Upon examining the answers column, following results were obtained (screenshots attached below). Each answer typically includes the following fields: **Name**, **Type**, **Class**, **Time to live (TTL)**, **Data length**, **Address/Data**.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 1 | 0.000000 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0x02a7 HTTPS mask-h2.icloud.com |
| 2 | 0.000079 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0xbd11 A mask-h2.icloud.com |
| 5 | 0.011366 | 130.63.10.18 | 10.24.199.55 | DNS | 195 | Standard query response 0x02a7 HTTPS mask-h2.icloud.com CNAME mask.apple-dns.net SOA ns-1096.awsdns-09... |
| 6 | 0.011367 | 130.63.10.18 | 10.24.199.55 | DNS | 545 | Standard query response 0xbd11 A mask-h2.icloud.com CNAME mask.apple-dns.net A 172.224.186.14 A 172.22... |

> Frame 6: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface en0, ...
> Ethernet II, Src: Cisco_3c:2b:7f (f8:39:18:3c:2b:7f), Dst: Apple_44:70:38 (3c:06:30:44:7...
> Internet Protocol Version 4, Src: 130.63.10.18, Dst: 10.24.199.55
> User Datagram Protocol, Src Port: 53, Dst Port: 64497
Domain Name System (response)
Transaction ID: 0xbd11
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 9
Authority RRs: 13
Additional RRs: 5
Queries
Answers
Authoritative nameservers
Additional records
[Request In: 2]
[Time: 0.01128000 seconds]

0020 c7 37 00 35 fb f1 01 ff 3c 33 bd 11 81 80 00 01 75 5... <3...
0009 00 0d 00 05 07 6d 61 73 6b 2d 68 32 06 69m ask-h2 i
0040 63 6c 6f 75 64 03 63 6f 6d 00 00 01 00 01 c0 0c cloud:co m...ask
0050 00 05 00 01 00 00 02 b9 00 14 04 6d 61 73 6b 09mask
0060 61 70 70 6c 65 2d 64 6e 73 03 6e 65 74 00 c0 30 apple-dn s-net-0
0070 00 01 00 01 00 00 00 40 00 04 ac e0 ba 0e c0 30@0
0080 00 01 00 01 00 00 00 40 00 04 ac e0 ba 0d c0 30@0
0090 00 01 00 01 00 00 00 40 00 04 ac e0 ba 0e c0 30@0
00a0 00 01 00 01 00 00 00 40 00 04 ac e0 ba 08 c0 30@0
00b0 00 01 00 01 00 00 00 40 00 04 ac e0 a7 59 c0 30@0
00c0 00 01 00 01 00 00 00 40 00 04 ac e0 ba 0a c0 30@0
00d0 00 01 00 01 00 00 00 40 00 04 ac e0 a7 83 c0 30@0
00e0 00 01 00 01 00 00 00 40 00 04 ac e0 a7 88 03 6e@n
00f0 65 74 00 00 02 00 01 00 00 1b c9 00 14 01 6a 0c et.....j
0100 67 74 6c 64 2d 73 65 72 76 65 72 73 03 6e 65 74 gtld-ser vers.net
0110 00 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 61 c0a
0120 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 67 c0g
0130 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 66 c0f
0140 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 62 c0b
0150 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6b c0k
0160 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6c c0l
0170 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 63 c0c
0180 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 68 c0h
0190 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 65 c0e
01a0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6d c0m
01b0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 64 c0d

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 1 | 0.000000 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0x02a7 HTTPS mask-h2.icloud.com |
| 2 | 0.000079 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0xbd11 A mask-h2.icloud.com |
| 5 | 0.011366 | 130.63.10.18 | 10.24.199.55 | DNS | 195 | Standard query response 0x02a7 HTTPS mask-h2.icloud.com CNAME mask.apple-dns.net SOA ns-1096.awsdns-09... |
| 6 | 0.011367 | 130.63.10.18 | 10.24.199.55 | DNS | 545 | Standard query response 0xbd11 A mask-h2.icloud.com CNAME mask.apple-dns.net A 172.224.186.14 A 172.22... |

> Frame 5: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface en0, ...
> Ethernet II, Src: Cisco_3c:2b:7f (f8:39:18:3c:2b:7f), Dst: Apple_44:70:38 (3c:06:30:44:7...
> Internet Protocol Version 4, Src: 130.63.10.18, Dst: 10.24.199.55
> User Datagram Protocol, Src Port: 53, Dst Port: 64486
Domain Name System (response)
Transaction ID: 0x02a7
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
Queries
Answers
> mask-h2.icloud.com: type CNAME, class IN, cname mask.apple-dns.net
Authoritative nameservers
[Request In: 1]
[Time: 0.01136000 seconds]

0000 3c 06 30 44 70 38 f8 39 18 3c 2b 7f 08 00 45 00 <0dp8 9 <+...E
0010 00 b5 fa 6a 00 00 3c 11 26 2d 82 3f 0a 12 0a 15j...< 6-7...
0020 c7 37 00 35 fb e6 00 a1 32 c1 02 a7 81 80 00 01 75 5... 2
0030 00 01 00 01 00 00 07 6d 61 73 6b 2d 68 32 06 69m ask-h2 i
0040 63 6c 6f 75 64 03 63 6f 6d 00 00 01 00 01 c0 0c cloud:co m...A...
0050 00 05 00 01 00 00 02 b9 00 14 04 6d 61 73 6b 09mask
0060 61 70 70 6c 65 2d 64 6e 73 03 6e 65 74 00 c0 30 apple-dn s-net-0
0070 00 06 00 01 00 00 00 80 00 49 07 6e 73 2d 31 30t-rs-10
0080 39 36 09 61 77 73 64 6e 73 2d 30 39 03 6f 72 67 96-awsdn s-00-org
0090 00 11 61 77 73 64 6e 73 2d 68 6f 73 74 6d 61 73 ..awsdns-hostmas
00a0 74 65 72 06 61 6d 61 7a 6f 6e 03 63 6f 6d 00 00 ter-amaz on-com...
00b0 00 00 01 00 00 1c 20 00 00 03 84 00 12 75 00 00u...
00c0 01 51 80Q

Wireshark DNS capture showing a query for mask-h2.icloud.com and its response. The response includes authoritative nameservers and additional records.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 1 | 0.000000 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0x02a7 HTTPS mask-h2.icloud.com |
| 2 | 0.000079 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0xbd11 A mask-h2.icloud.com |
| 5 | 0.011366 | 130.63.10.18 | 10.24.199.55 | DNS | 195 | Standard query response 0x02a7 HTTPS mask-h2.icloud.com CNAME mask.apple-dns.net SOA ns-1096.awsdns-09... |
| 6 | 0.011367 | 130.63.10.18 | 10.24.199.55 | DNS | 545 | Standard query response 0xbd11 A mask-h2.icloud.com CNAME mask.apple-dns.net A 172.224.186.14 A 172.22... |

Answers

- mask-h2.icloud.com: type CNAME, class IN, cname mask.apple-dns.net
- mask.apple-dns.net: type A, class IN, addr 172.224.186.14
- mask.apple-dns.net: type A, class IN, addr 172.224.186.13
- mask.apple-dns.net: type A, class IN, addr 172.224.186.6
- mask.apple-dns.net: type A, class IN, addr 172.224.186.8
- mask.apple-dns.net: type A, class IN, addr 172.224.167.137
- mask.apple-dns.net: type A, class IN, addr 172.224.186.10
- mask.apple-dns.net: type A, class IN, addr 172.224.167.131
- mask.apple-dns.net: type A, class IN, addr 172.224.167.136

Authoritative nameservers

- net: type NS, class IN, ns j.gtld-servers.net
- net: type NS, class IN, ns a.gtld-servers.net
- net: type NS, class IN, ns g.gtld-servers.net
- net: type NS, class IN, ns f.gtld-servers.net
- net: type NS, class IN, ns b.gtld-servers.net
- net: type NS, class IN, ns k.gtld-servers.net
- net: type NS, class IN, ns l.gtld-servers.net
- net: type NS, class IN, ns c.gtld-servers.net
- net: type NS, class IN, ns h.gtld-servers.net
- net: type NS, class IN, ns e.gtld-servers.net
- net: type NS, class IN, ns m.gtld-servers.net

Additional records

- d.gtld-servers.net: type A, class IN, addr 192.31.80.30
- b.gtld-servers.net: type A, class IN, addr 192.33.14.30
- h.gtld-servers.net: type A, class IN, addr 192.54.112.30
- c.gtld-servers.net: type A, class IN, addr 192.26.92.30
- k.gtld-servers.net: type A, class IN, addr 192.52.178.30

[Request in: 2]
[Time: 0.011288000 seconds]

Packets: 950 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%) · Profile: Default

Wireshark DNS capture showing a query for mask-h2.icloud.com and its response. The response includes authoritative nameservers and additional records.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 1 | 0.000000 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0x02a7 HTTPS mask-h2.icloud.com |
| 2 | 0.000079 | 10.24.199.55 | 130.63.10.18 | DNS | 78 | Standard query 0xbd11 A mask-h2.icloud.com |
| 5 | 0.011366 | 130.63.10.18 | 10.24.199.55 | DNS | 195 | Standard query response 0x02a7 HTTPS mask-h2.icloud.com CNAME mask.apple-dns.net SOA ns-1096.awsdns-09... |
| 6 | 0.011367 | 130.63.10.18 | 10.24.199.55 | DNS | 545 | Standard query response 0xbd11 A mask-h2.icloud.com CNAME mask.apple-dns.net A 172.224.186.14 A 172.22... |

Authoritative nameservers

- net: type NS, class IN, ns j.gtld-servers.net
- net: type NS, class IN, ns a.gtld-servers.net
- net: type NS, class IN, ns g.gtld-servers.net
- net: type NS, class IN, ns f.gtld-servers.net
- net: type NS, class IN, ns b.gtld-servers.net
- net: type NS, class IN, ns k.gtld-servers.net
- net: type NS, class IN, ns l.gtld-servers.net
- net: type NS, class IN, ns c.gtld-servers.net
- net: type NS, class IN, ns h.gtld-servers.net
- net: type NS, class IN, ns e.gtld-servers.net
- net: type NS, class IN, ns m.gtld-servers.net
- net: type NS, class IN, ns i.gtld-servers.net

Additional records

- d.gtld-servers.net: type A, class IN, addr 192.31.80.30
- b.gtld-servers.net: type A, class IN, addr 192.33.14.30
- h.gtld-servers.net: type A, class IN, addr 192.54.112.30
- c.gtld-servers.net: type A, class IN, addr 192.26.92.30
- k.gtld-servers.net: type A, class IN, addr 192.52.178.30

[Request in: 2]
[Time: 0.011288000 seconds]

Packets: 950 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%) · Profile: Default