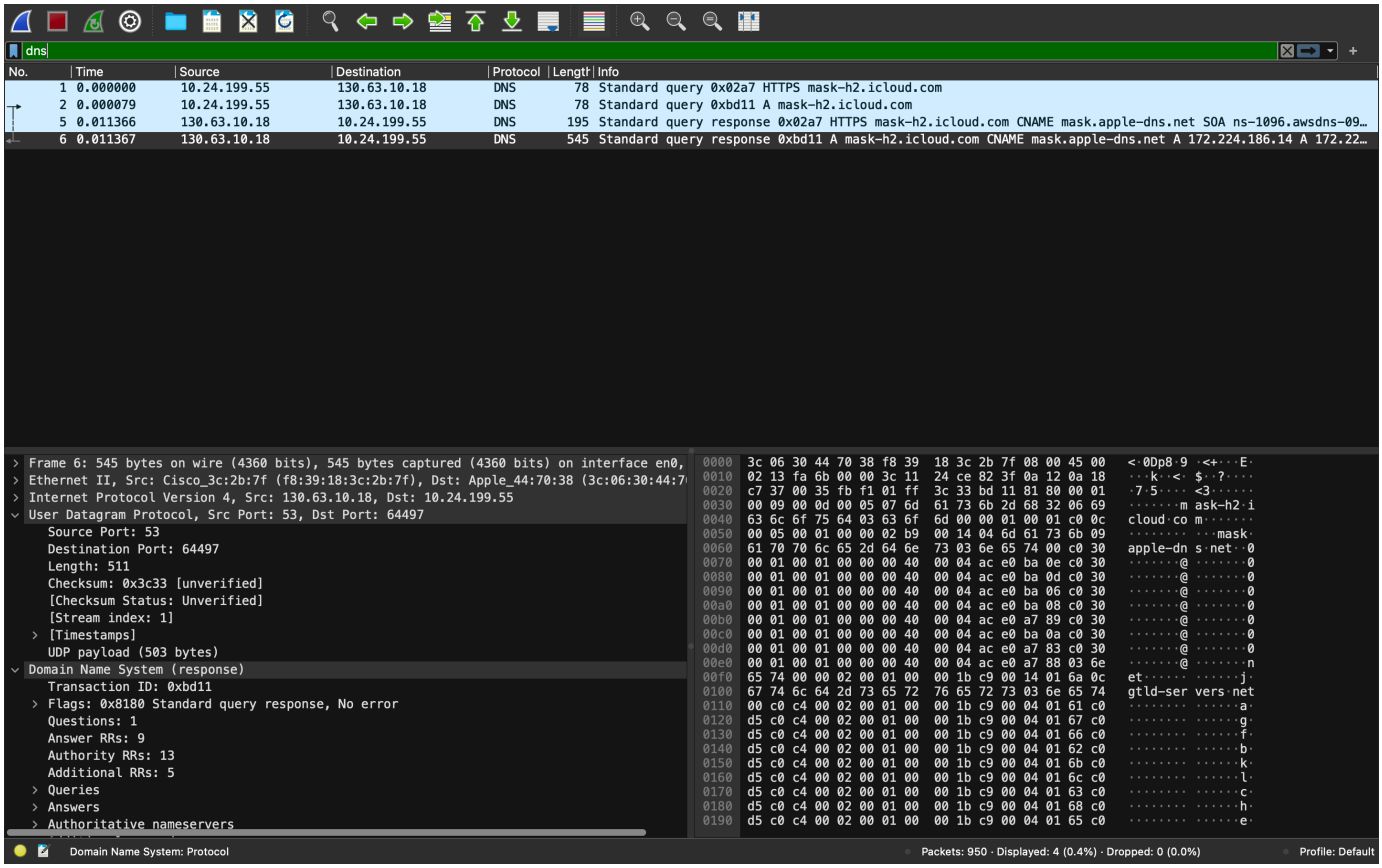
Name: Stuti Parmar
Student ID: 218516625

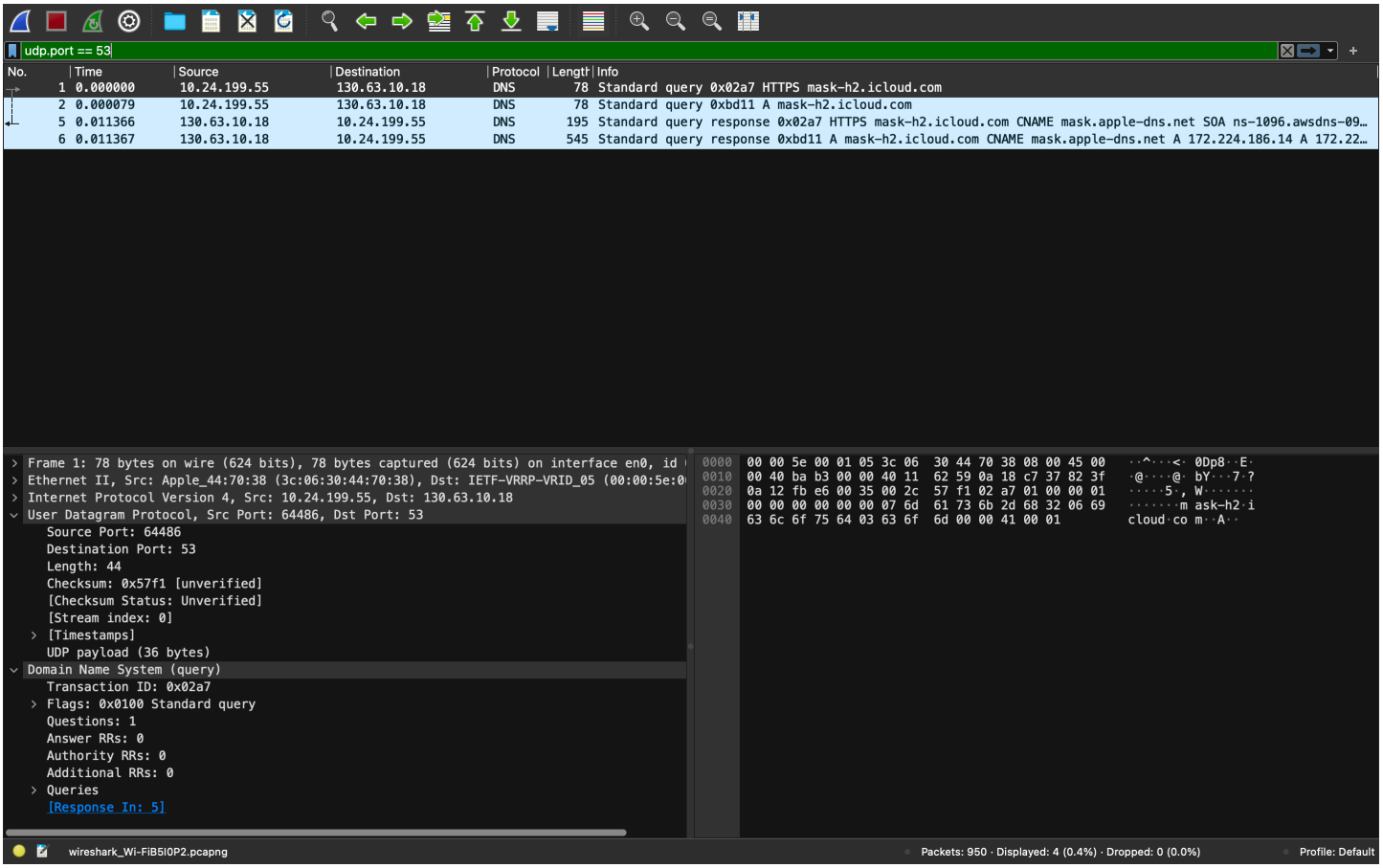
Assignment 1 - EECS 3214

QUESTION 2:

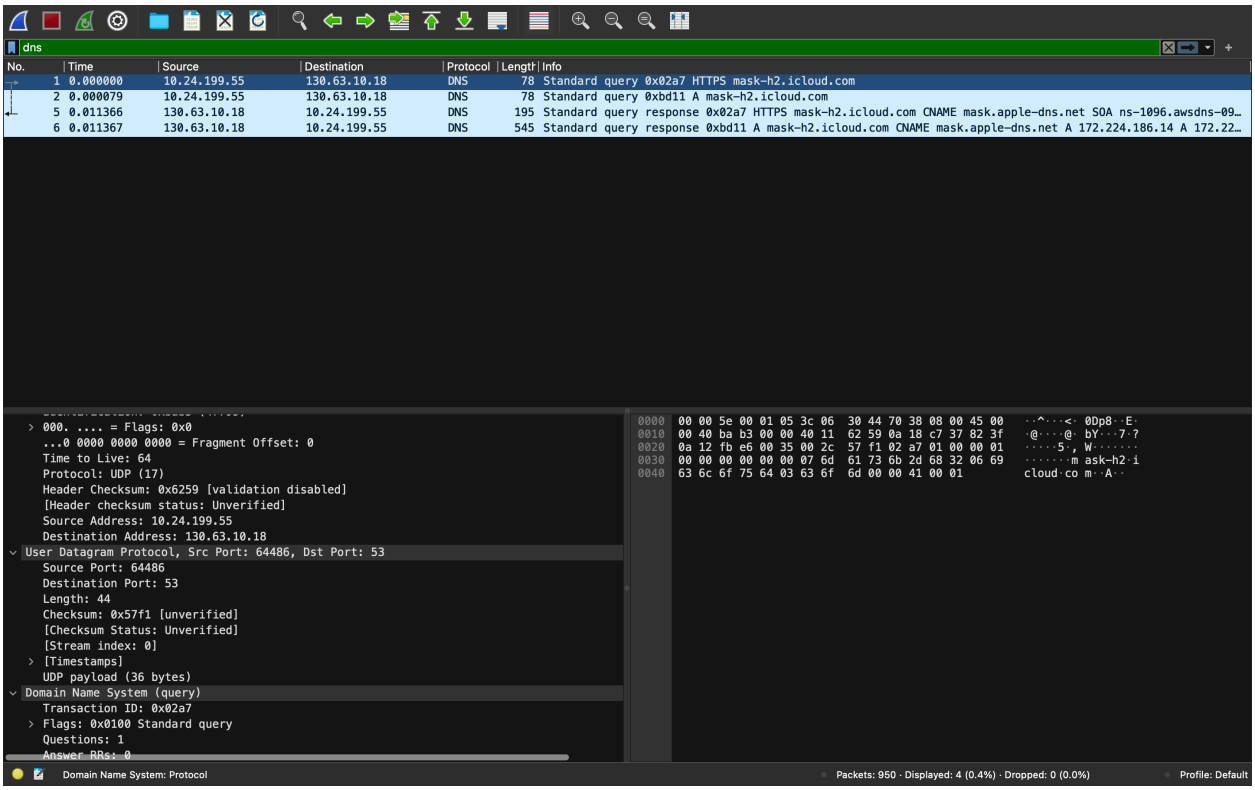
Q.4) The following screenshot specifies the located DNS queries and response messages. Out of which there are 2 DNS queries and 2 response messages.



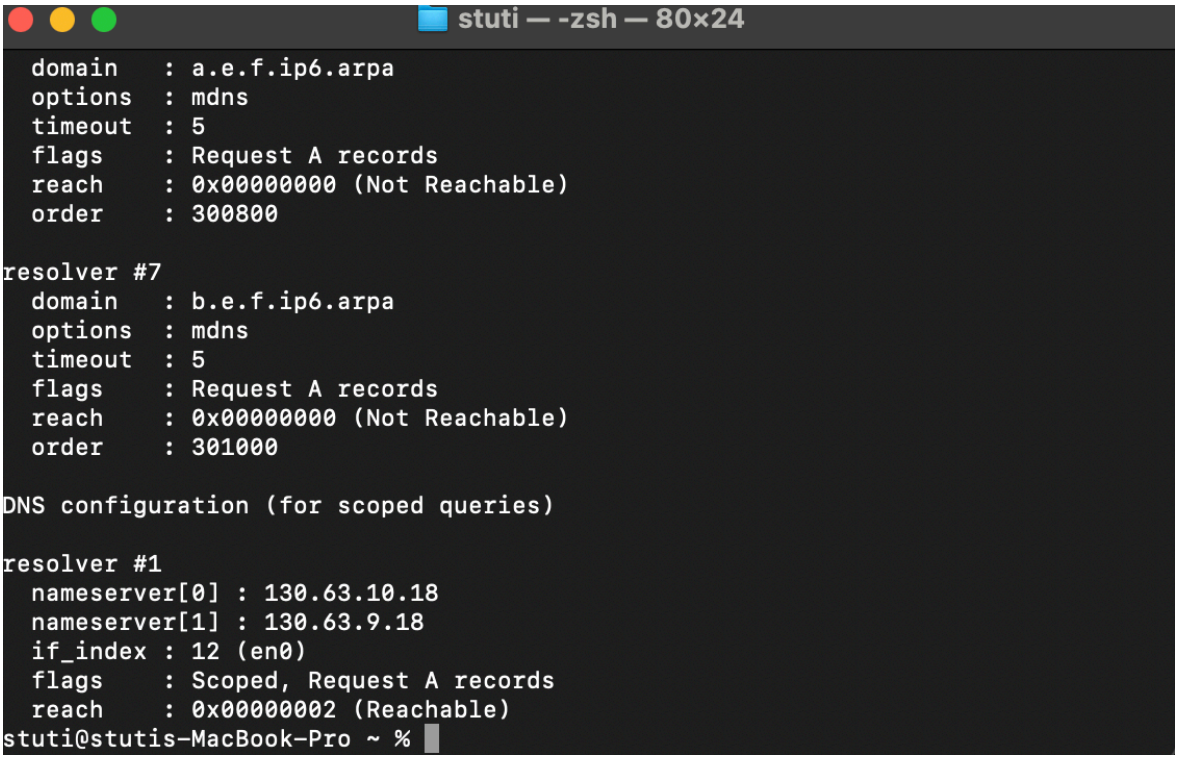
I used ‘udp.port == 53’ to check for UDP to TCP protocol. As specified in screenshot below, the DNS queries and response messages are all sent over UDP.



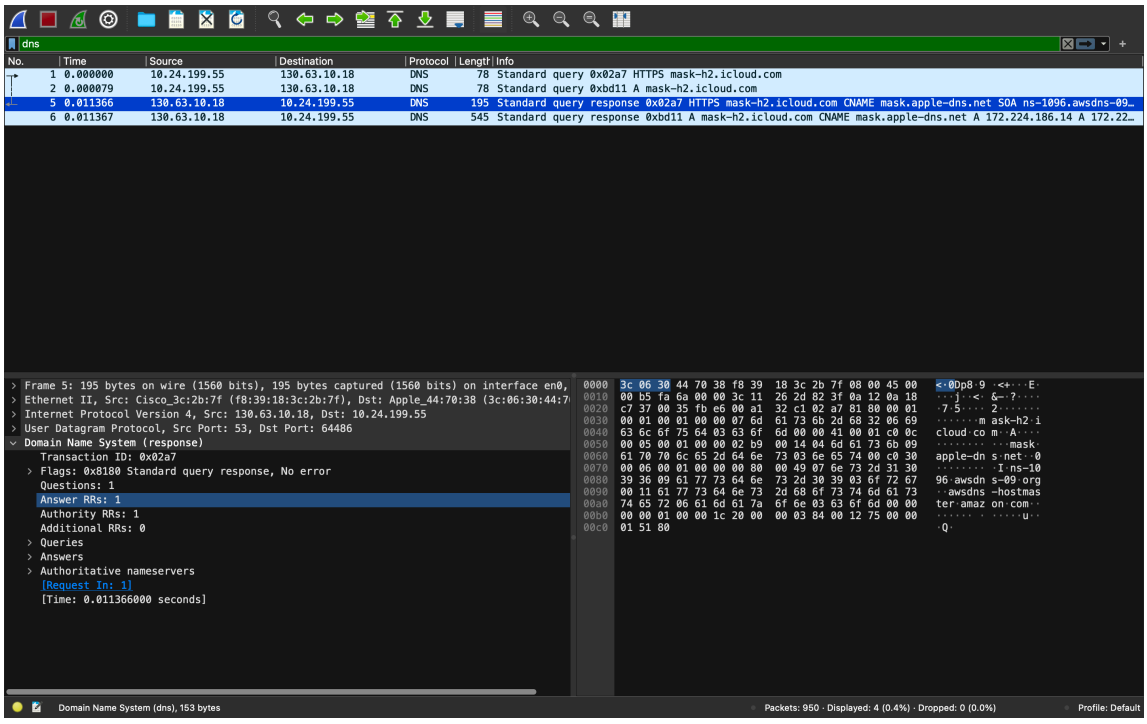
Q.6) The IP address to which the DNS query was sent is specified as Destination Address: 130.63.10.18



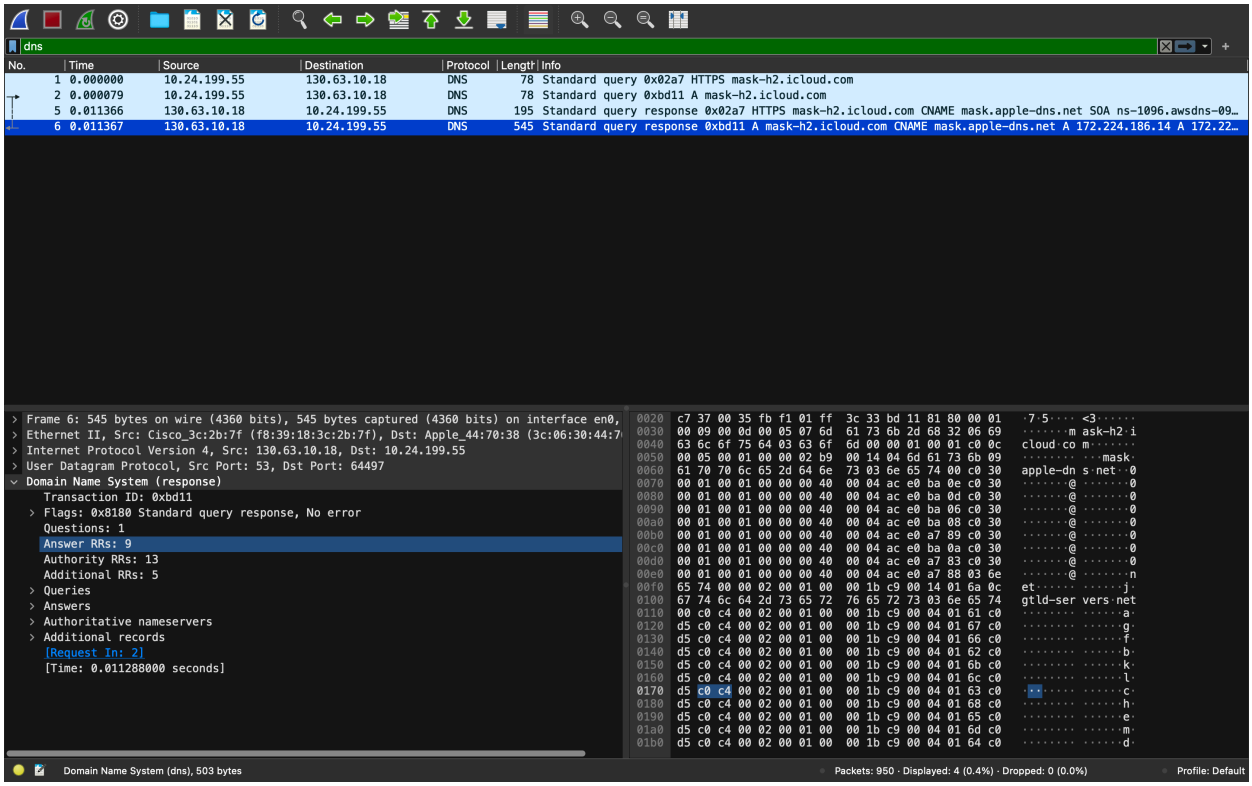
After Using ipconfig to determine the IP address of your local DNS server, The IP address for DNS servers are: 130.63.10.18. Comparing the 2 IP addresses we get that both IP addresses are same. If the IP addresses are the same, it means that the DNS query is being sent to the local DNS server.

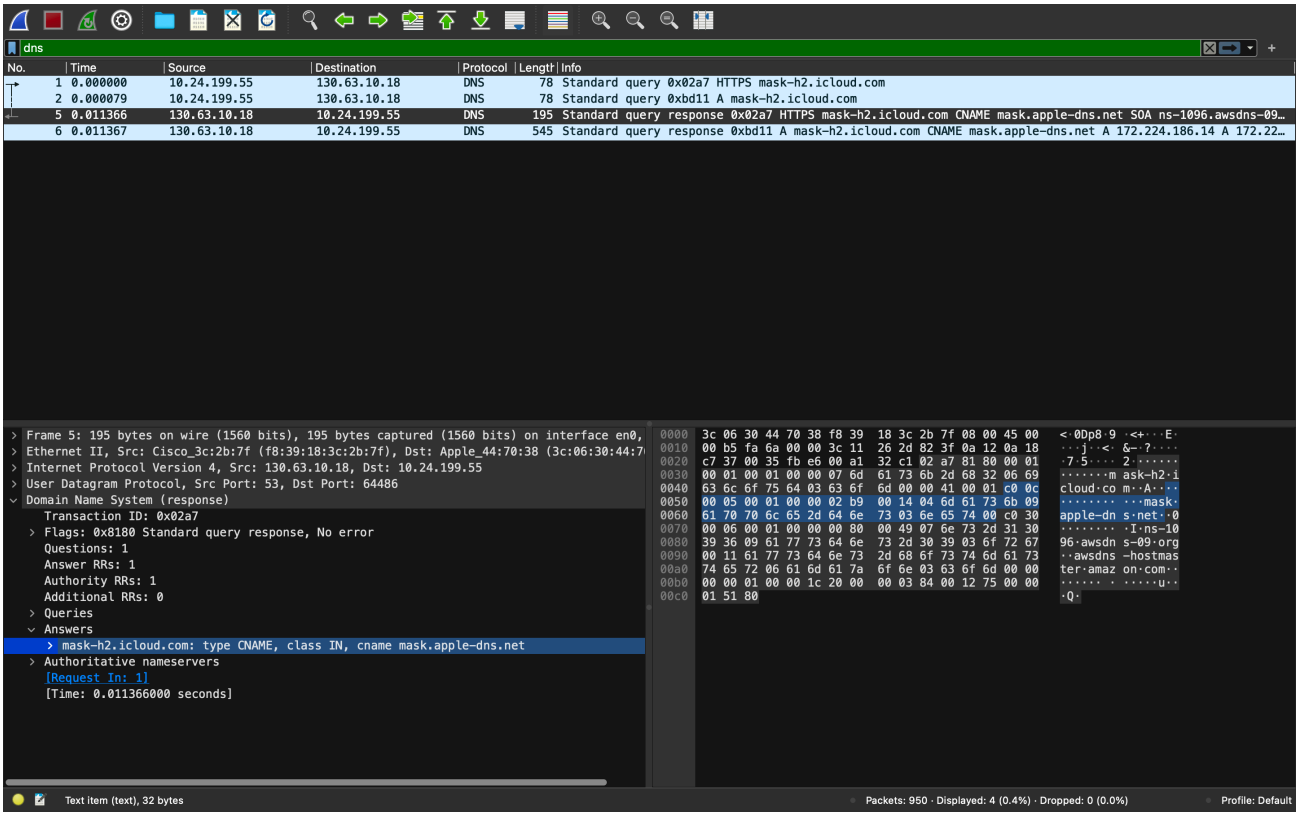


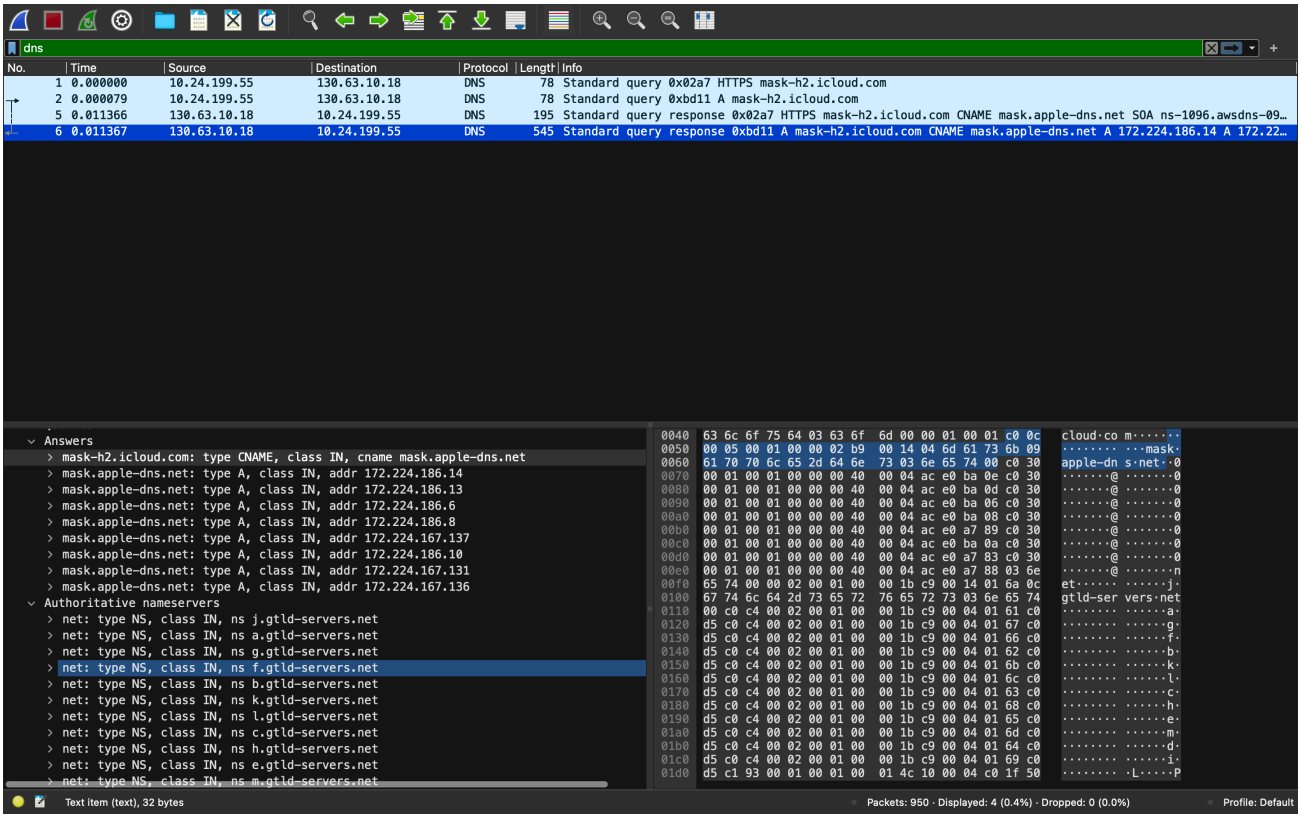
Q.8) Answers provided by DNS response message is 1 and 9
(Screenshots added below)

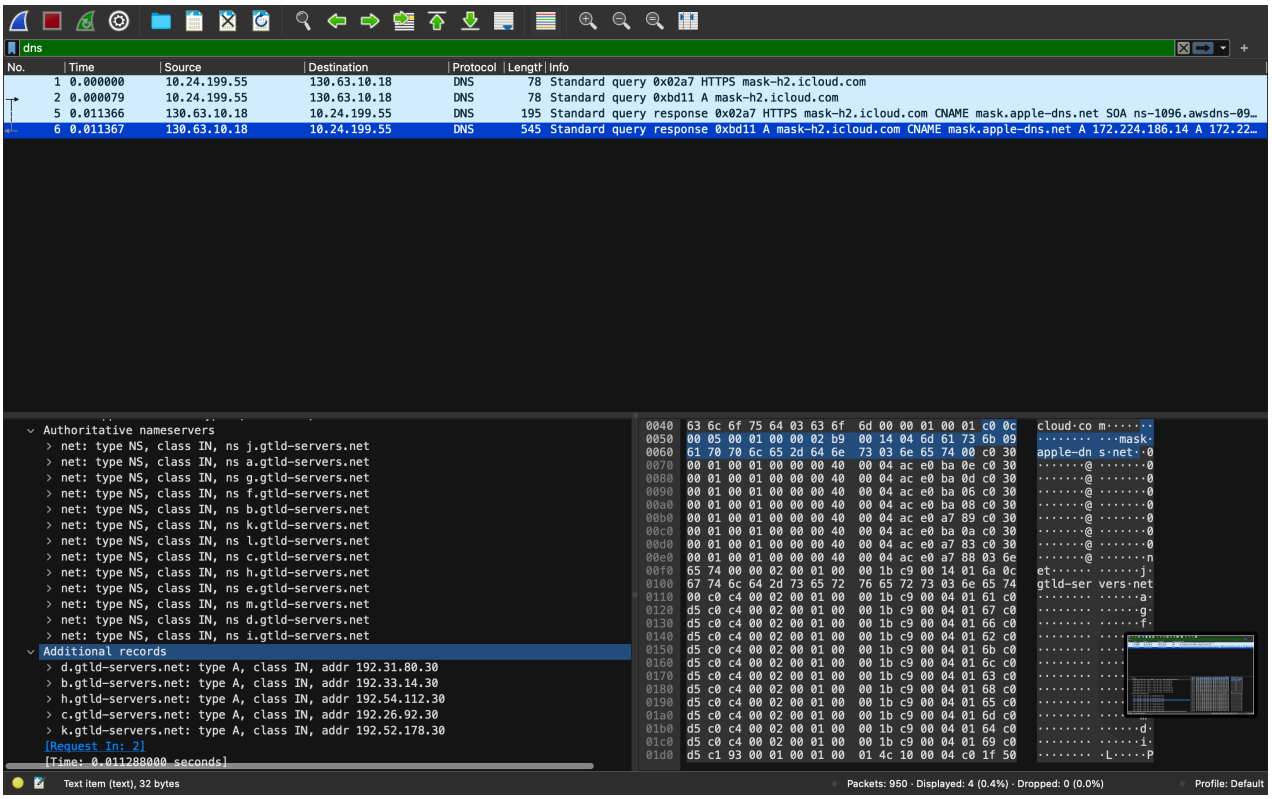


Upon examining the answers column, following results were obtained (screenshots attached below). Each answer typically includes the following fields: **Name, Type, Class, Time to live (TTL), Data length, Address/Data.**






dns
No. Time Source Destination Protocol Lengtl 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
0040 63 6c 6f 75 64 03 63 6f 6d 00 00 01 00 01 c0 0c cloud·co m·····
0050 00 05 00 01 00 00 02 b9 00 14 04 6d 61 73 6b 09 ····· ···mask·
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 06 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 89 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 c0 ····· ·····a·
0120 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 67 c0 ····· ·····g·
0130 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 66 c0 ····· ·····f·
0140 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 62 c0 ····· ·····b·
0150 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6b c0 ····· ·····k·
0160 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6c c0 ····· ·····l·
0170 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 63 c0 ····· ·····c·
0180 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 68 c0 ····· ·····h·
0190 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 65 c0 ····· ·····e·
01a0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6d c0 ····· ·····m·
01b0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 64 c0 ····· ·····d·
01c0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 69 c0 ····· ·····i·
01d0 d5 c1 93 00 01 00 01 00 01 4c 10 00 04 c0 1f 50 ····· ·L·····P
Text item (text), 32 bytes
Packets: 950 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)
Profile: Default


dns
No. Time Source Destination Protocol Lengtl 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 d.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]
0040 63 6c 6f 75 64 03 63 6f 6d 00 00 01 00 01 c0 0c cloud·co m·····
0050 00 05 00 01 00 00 02 b9 00 14 04 6d 61 73 6b 09 ····· ···mask·
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 06 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 89 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 c0 ····· ·····a·
0120 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 67 c0 ····· ·····g·
0130 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 66 c0 ····· ·····f·
0140 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 62 c0 ····· ·····b·
0150 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6b c0 ····· ·····k·
0160 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6c c0 ····· ·····l·
0170 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 63 c0 ····· ·····c·
0180 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 68 c0 ····· ·····h·
0190 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 65 c0 ····· ·····e·
01a0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 6d c0 ····· ·····m·
01b0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 64 c0 ····· ·····d·
01c0 d5 c0 c4 00 02 00 01 00 00 1b c9 00 04 01 69 c0 ····· ·····i·
01d0 d5 c1 93 00 01 00 01 00 01 4c 10 00 04 c0 1f 50 ····· ·L·····P
Text item (text), 32 bytes
Packets: 950 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)
Profile: Default