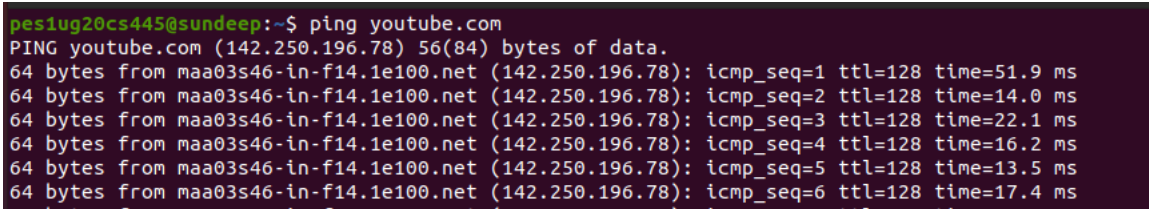
Name: SUNDEEP A **SRN: PES1UG20CS445**

ROLL NO : 48 **SEC:H**

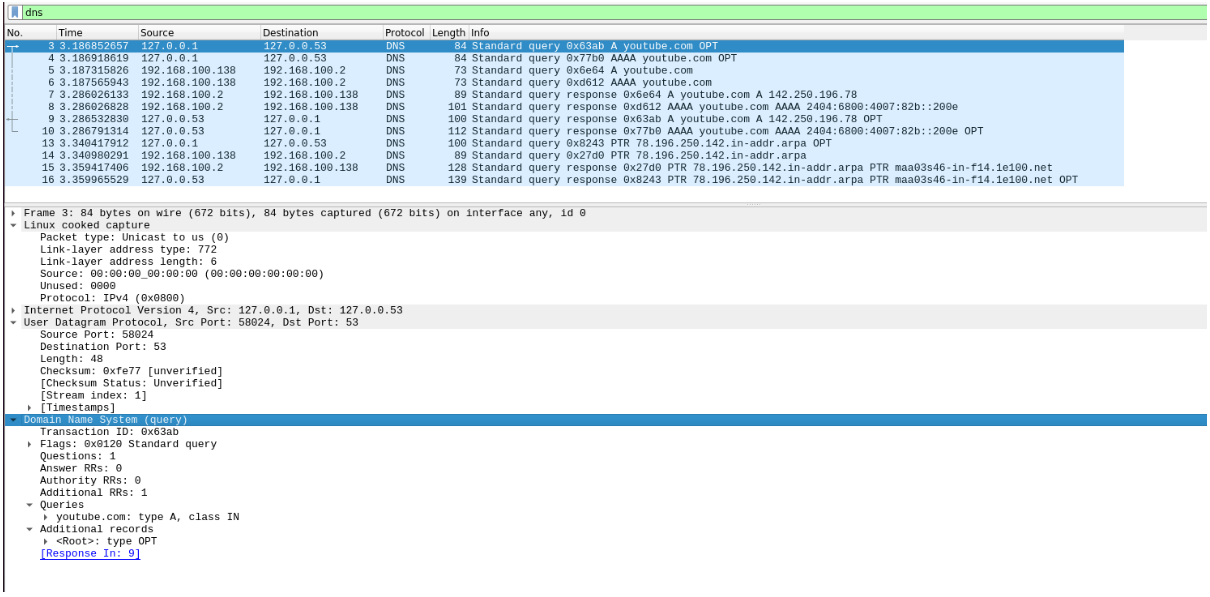
Observation 1:

Ping:



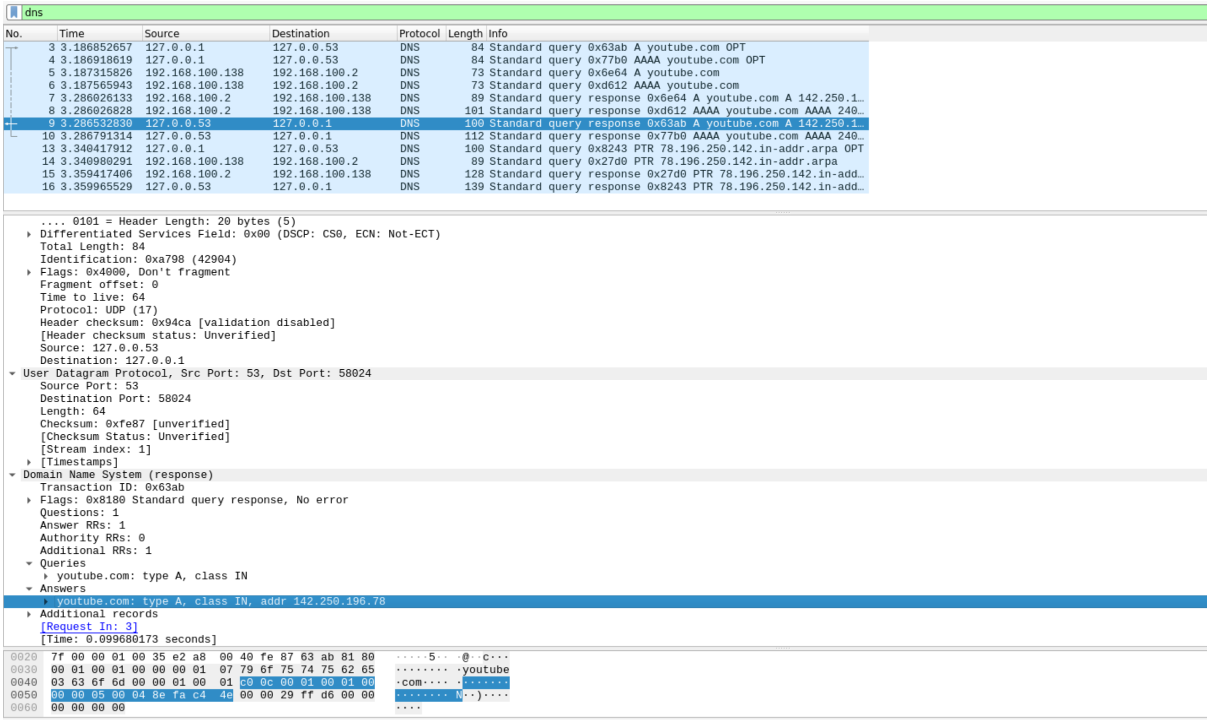
```
pes1ug20cs445@sundeep:~$ ping youtube.com
PING youtube.com (142.250.196.78) 56(84) bytes of data.
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=1 ttl=128 time=51.9 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=2 ttl=128 time=14.0 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=3 ttl=128 time=22.1 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=4 ttl=128 time=16.2 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=5 ttl=128 time=13.5 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=6 ttl=128 time=17.4 ms
```

Request:



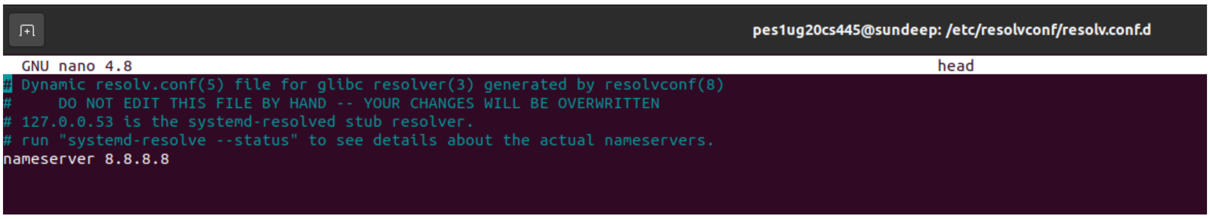
```
dns
No.   Time         Source           Destination      Protocol Length Info
   3 3.186852657  127.0.0.1        127.0.0.53       DNS       84 Standard query 0x63ab A youtube.com OPT
   4 3.186918619  127.0.0.1        127.0.0.53       DNS       84 Standard query 0x77b0 AAAA youtube.com OPT
   5 3.187315826  192.168.100.138  192.168.100.2    DNS       73 Standard query 0x6e64 A youtube.com
   6 3.187565943  192.168.100.138  192.168.100.2    DNS       73 Standard query 0xd612 AAAA youtube.com
   7 3.286026133  192.168.100.2    192.168.100.138  DNS       89 Standard query response 0x6e64 A youtube.com A 142.250.196.78
   8 3.286026828  192.168.100.2    192.168.100.138  DNS      101 Standard query response 0xd612 AAAA youtube.com AAAA 2404:6800:4007:82b::200e
   9 3.286532830  127.0.0.53       127.0.0.1        DNS      100 Standard query response 0x63ab A youtube.com A 142.250.196.78 OPT
  10 3.286791314  127.0.0.53       127.0.0.1        DNS      112 Standard query response 0x77b0 AAAA youtube.com AAAA 2404:6800:4007:82b::200e OPT
  13 3.340417912  127.0.0.1        127.0.0.53       DNS      100 Standard query 0x8243 PTR 78.196.250.142.in-addr.arpa OPT
  14 3.340980291  192.168.100.138  192.168.100.2    DNS       89 Standard query 0x27d0 PTR 78.196.250.142.in-addr.arpa
  15 3.359417406  192.168.100.2    192.168.100.138  DNS      128 Standard query response 0x27d0 PTR 78.196.250.142.in-addr.arpa PTR maa03s46-in-f14.1e100.net
  16 3.359965529  127.0.0.53       127.0.0.1        DNS      139 Standard query response 0x8243 PTR 78.196.250.142.in-addr.arpa PTR maa03s46-in-f14.1e100.net OPT

▸ Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▾ User Datagram Protocol, Src Port: 58024, Dst Port: 53
    Source Port: 58024
    Destination Port: 53
    Length: 48
    Checksum: 0xfe77 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0x63ab
  ▸ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ youtube.com: type A, class IN
  ▾ Additional records
    ▸ <Root>: type OPT
    [Response In: 9]
```

Response



```
dns
No.   Time         Source           Destination      Protocol Length Info
   3 3.186852657  127.0.0.1        127.0.0.53       DNS       84 Standard query 0x63ab A youtube.com OPT
   4 3.186918619  127.0.0.1        127.0.0.53       DNS       84 Standard query 0x77b0 AAAA youtube.com OPT
   5 3.187315826  192.168.100.138  192.168.100.2    DNS       73 Standard query 0x6e64 A youtube.com
   6 3.187565943  192.168.100.138  192.168.100.2    DNS       73 Standard query 0xd612 AAAA youtube.com
   7 3.286026133  192.168.100.2    192.168.100.138  DNS       89 Standard query response 0x6e64 A youtube.com A 142.250.1…
   8 3.286026828  192.168.100.2    192.168.100.138  DNS      101 Standard query response 0xd612 AAAA youtube.com AAAA 240…
   9 3.286532830  127.0.0.53       127.0.0.1        DNS      100 Standard query response 0x63ab A youtube.com A 142.250.1…
  10 3.286791314  127.0.0.53       127.0.0.1        DNS      112 Standard query response 0x77b0 AAAA youtube.com AAAA 240…
  13 3.340417912  127.0.0.1        127.0.0.53       DNS      100 Standard query 0x8243 PTR 78.196.250.142.in-addr.arpa OPT
  14 3.340980291  192.168.100.138  192.168.100.2    DNS       89 Standard query 0x27d0 PTR 78.196.250.142.in-addr.arpa
  15 3.359417406  192.168.100.2    192.168.100.138  DNS      128 Standard query response 0x27d0 PTR 78.196.250.142.in-add…
  16 3.359965529  127.0.0.53       127.0.0.1        DNS      139 Standard query response 0x8243 PTR 78.196.250.142.in-add…

    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xa798 (42904)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x94ca [validation disabled]
    [Header checksum status: Unverified]
    Source: 127.0.0.53
    Destination: 127.0.0.1
▾ User Datagram Protocol, Src Port: 53, Dst Port: 58024
    Source Port: 53
    Destination Port: 58024
    Length: 64
    Checksum: 0xfe87 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
▾ Domain Name System (response)
    Transaction ID: 0x63ab
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ youtube.com: type A, class IN
  ▾ Answers
    ▸ youtube.com: type A, class IN, addr 142.250.196.78
  ▸ Additional records
    [Request In: 3]
    [Time: 0.099680173 seconds]

0020  7f 00 00 01 00 35 e2 a8  00 40 fe 87 63 ab 81 80   ·····5·· ·@··c···
0030  00 01 00 01 00 00 00 01  07 79 6f 75 74 75 62 65   ········ ·youtube
0040  03 63 6f 6d 00 00 01 00  01 c0 0c 00 01 00 01 00   ·com···· ········
0050  00 00 05 00 04 8e fa c4  4e 00 00 29 ff d6 00 00   ········ N··)····
0060  00 00 00 00                                        ····
```

Task 1:

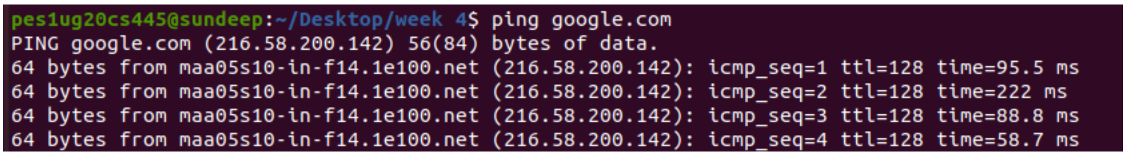


pes1ug20cs445@sundeep: /etc/resolvconf/resolv.conf.d

```
  GNU nano 4.8                                                                      head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 8.8.8.8
```

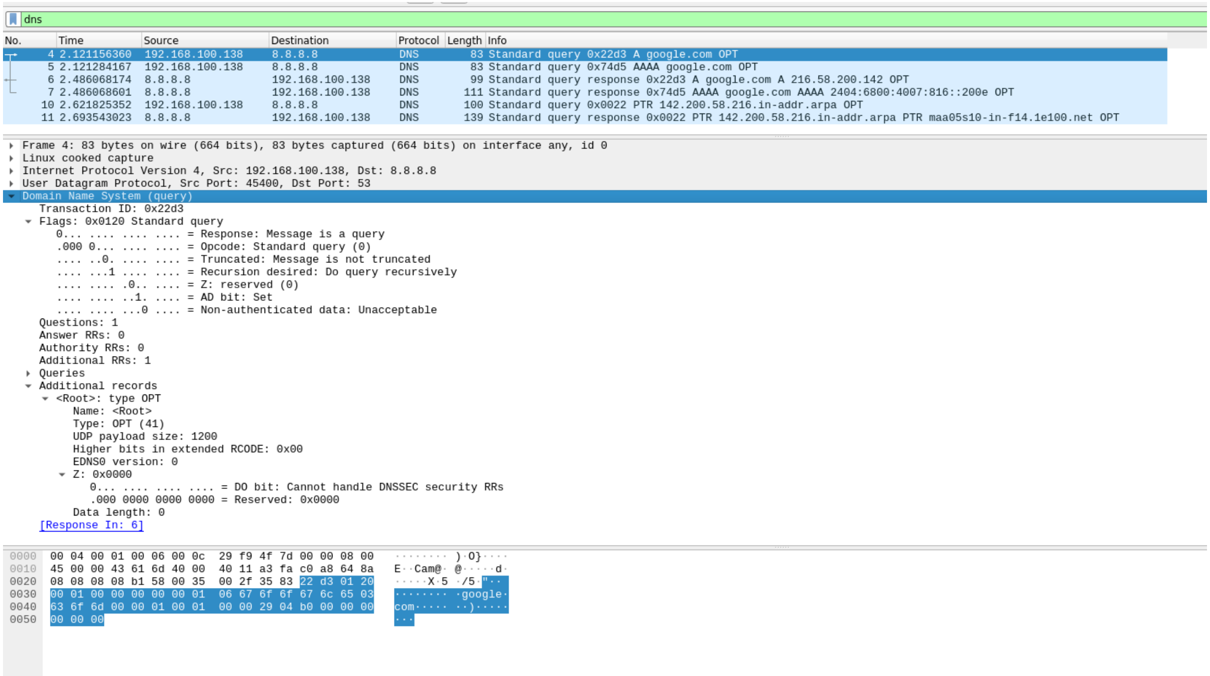
Observation 2:

Ping:



```
pes1ug20cs445@sundeep:~/Desktop/week 4$ ping google.com
PING google.com (216.58.200.142) 56(84) bytes of data.
64 bytes from maa05s10-in-f14.1e100.net (216.58.200.142): icmp_seq=1 ttl=128 time=95.5 ms
64 bytes from maa05s10-in-f14.1e100.net (216.58.200.142): icmp_seq=2 ttl=128 time=222 ms
64 bytes from maa05s10-in-f14.1e100.net (216.58.200.142): icmp_seq=3 ttl=128 time=88.8 ms
64 bytes from maa05s10-in-f14.1e100.net (216.58.200.142): icmp_seq=4 ttl=128 time=58.7 ms
```

Request:



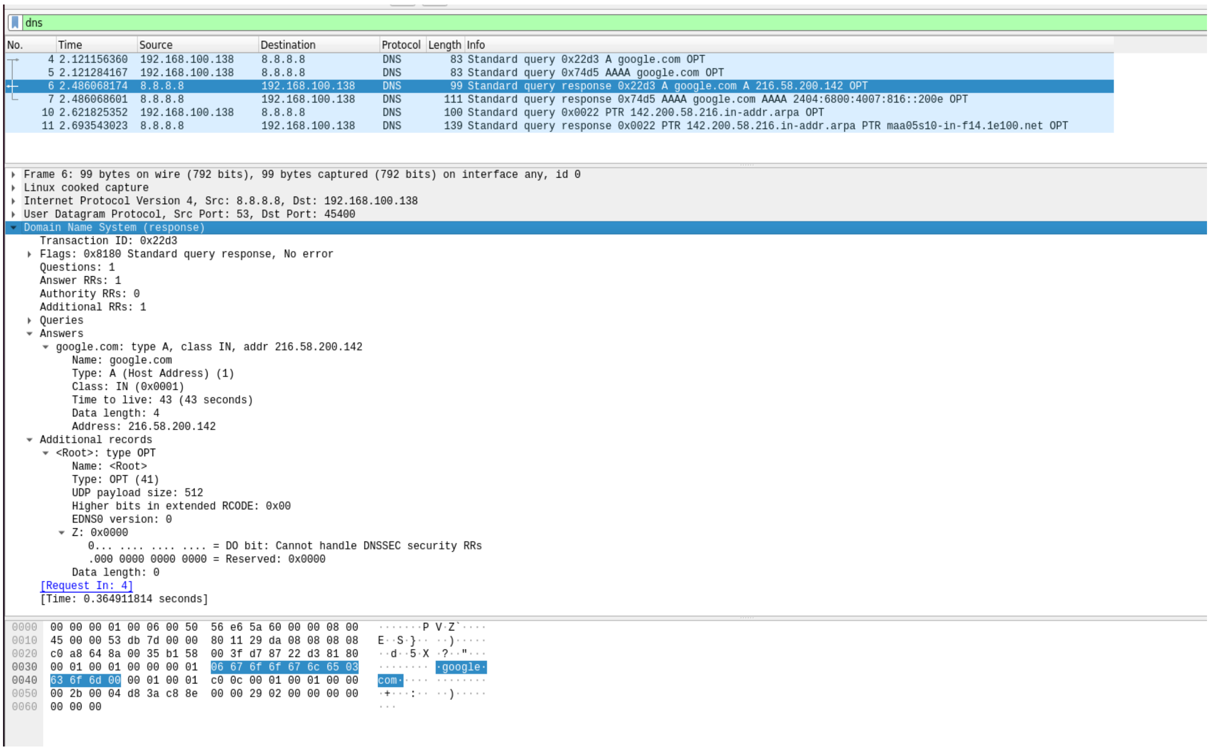
dns

No.	Time	Source	Destination	Protocol	Length	Info
4	2.121156360	192.168.100.138	8.8.8.8	DNS	83	Standard query 0x22d3 A google.com OPT
5	2.121284167	192.168.100.138	8.8.8.8	DNS	83	Standard query 0x74d5 AAAA google.com OPT
6	2.486068174	8.8.8.8	192.168.100.138	DNS	99	Standard query response 0x22d3 A google.com A 216.58.200.142 OPT
7	2.486068601	8.8.8.8	192.168.100.138	DNS	111	Standard query response 0x74d5 AAAA google.com AAAA 2404:6800:4007:816::200e OPT
10	2.621825352	192.168.100.138	8.8.8.8	DNS	100	Standard query 0x0022 PTR 142.200.58.216.in-addr.arpa OPT
11	2.693543023	8.8.8.8	192.168.100.138	DNS	139	Standard query response 0x0022 PTR 142.200.58.216.in-addr.arpa PTR maa05s10-in-f14.1e100.net OPT

```
▸ Frame 4: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 45400, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x22d3
  ▾ Flags: 0x0120 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..1. .... = AD bit: Set
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 1200
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▾ Z: 0x0000
          0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
    [Response In: 6]
```

```
0000  00 04 00 01 00 06 00 0c  29 f9 4f 7d 00 00 08 00   ········ )·O}····
0010  45 00 00 43 61 6d 40 00  40 11 a3 fa c0 a8 64 8a   E··Cam@· @·····d·
0020  08 08 08 08 b1 58 00 35  00 2f 35 83 22 d3 01 20   ·····X·5 ·/5·"·· 
0030  00 01 00 00 00 00 00 01  06 67 6f 6f 67 6c 65 03   ········ ·google·
0040  63 6f 6d 00 00 01 00 01  00 00 29 04 b0 00 00 00   com····· ··)·····
0050  00 00 00                                           ···
```

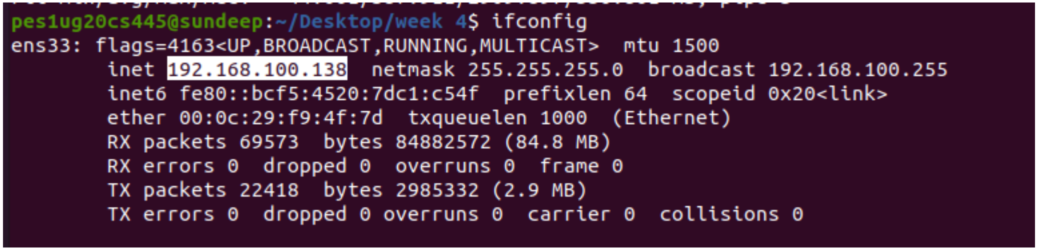
Response:



```
dns

No.   Time         Source           Destination      Protocol Length Info
    4 2.121156360  192.168.100.138  8.8.8.8          DNS       83 Standard query 0x22d3 A google.com OPT
    5 2.121284167  192.168.100.138  8.8.8.8          DNS       83 Standard query 0x74d5 AAAA google.com OPT
    6 2.486068174  8.8.8.8          192.168.100.138  DNS       99 Standard query response 0x22d3 A google.com A 216.58.200.142 OPT
    7 2.486068601  8.8.8.8          192.168.100.138  DNS      111 Standard query response 0x74d5 AAAA google.com AAAA 2404:6800:4007:816::200e OPT
   10 2.621825352  192.168.100.138  8.8.8.8          DNS      100 Standard query 0x0022 PTR 142.200.58.216.in-addr.arpa OPT
   11 2.693543023  8.8.8.8          192.168.100.138  DNS      139 Standard query response 0x0022 PTR 142.200.58.216.in-addr.arpa PTR maa05s10-in-f14.1e100.net OPT

Frame 6: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.100.138
User Datagram Protocol, Src Port: 53, Dst Port: 45400
Domain Name System (response)
    Transaction ID: 0x22d3
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
    Queries
    Answers
        google.com: type A, class IN, addr 216.58.200.142
            Name: google.com
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 43 (43 seconds)
            Data length: 4
            Address: 216.58.200.142
    Additional records
        <Root>: type OPT
            Name: <Root>
            Type: OPT (41)
            UDP payload size: 512
            Higher bits in extended RCODE: 0x00
            EDNS0 version: 0
            Z: 0x0000
                0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
                .000 0000 0000 0000 = Reserved: 0x0000
            Data length: 0
    [Request In: 4]
    [Time: 0.364911814 seconds]

0000  00 00 00 01 00 06 00 50  56 e6 5a 60 00 00 08 00   ·······P V·Z`····
0010  45 00 00 53 db 7d 00 00  80 11 29 da 08 08 08 08   E··S·}·· ··)·····
0020  c0 a8 64 8a 00 35 b1 58  00 3f d7 87 22 d3 81 80   ··d··5·X ·?··"···
0030  00 01 00 01 00 00 00 01  06 67 6f 6f 67 6c 65 03   ········ ·google·
0040  63 6f 6d 00 00 01 00 01  c0 0c 00 01 00 01 00 00   com····· ········
0050  00 2b 00 04 d8 3a c8 8e  00 00 29 02 00 00 00 00   ·+···:·· ··)·····
0060  00 00 00                                           ···
```

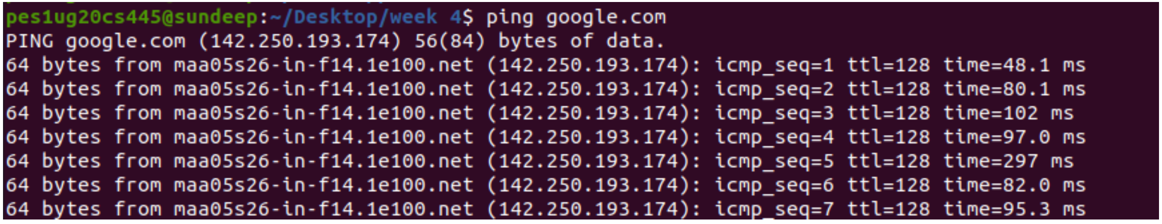
Observation 3:

Here we can see that My system IP address is 192.168.100.138



```
pes1ug20cs445@sundeep:~/Desktop/week 4$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.138  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::bcf5:4520:7dc1:c54f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f9:4f:7d  txqueuelen 1000  (Ethernet)
        RX packets 69573  bytes 84882572 (84.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22418  bytes 2985332 (2.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

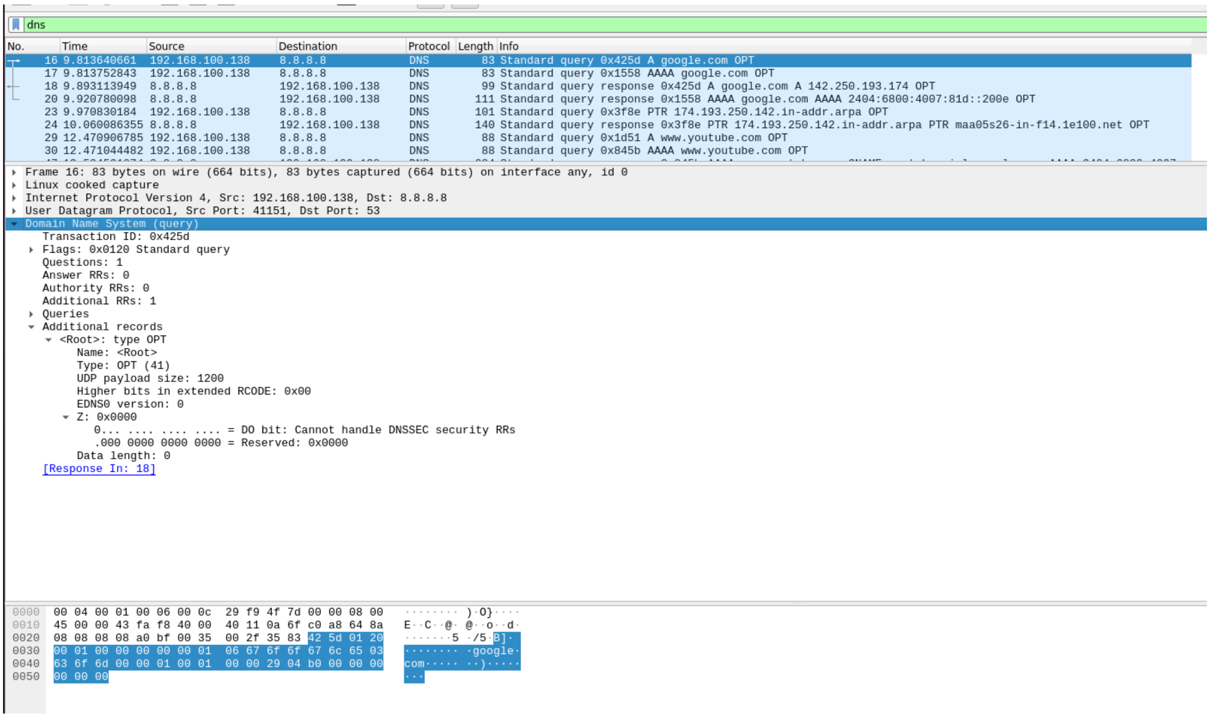
Ping google.com:



```
pes1ug20cs445@sundeep:~/Desktop/week 4$ ping google.com
PING google.com (142.250.193.174) 56(84) bytes of data.
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=1 ttl=128 time=48.1 ms
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=2 ttl=128 time=80.1 ms
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=3 ttl=128 time=102 ms
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=4 ttl=128 time=97.0 ms
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=5 ttl=128 time=297 ms
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=6 ttl=128 time=82.0 ms
64 bytes from maa05s26-in-f14.1e100.net (142.250.193.174): icmp_seq=7 ttl=128 time=95.3 ms
```

Wireshark capture :

Request:

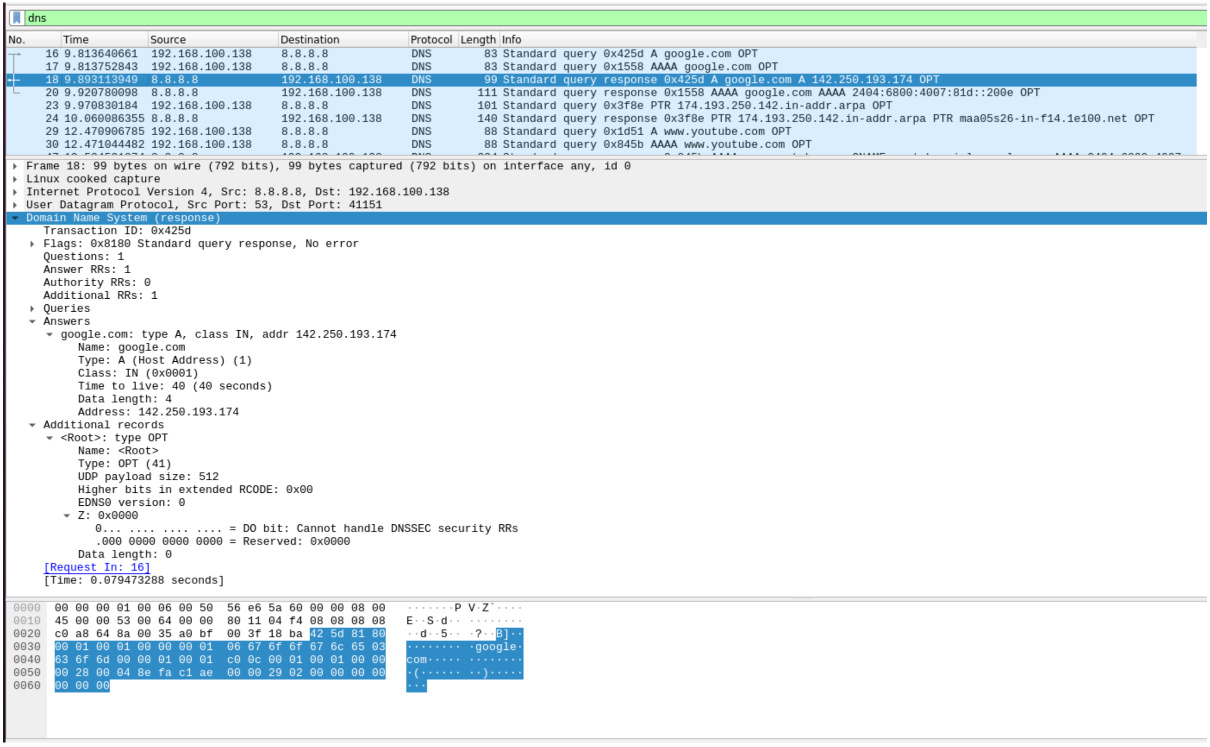


```
dns
No.  Time          Source           Destination      Protocol Length Info
  16 9.813640661   192.168.100.138  8.8.8.8          DNS       83 Standard query 0x425d A google.com OPT
  17 9.813752843   192.168.100.138  8.8.8.8          DNS       83 Standard query 0x1558 AAAA google.com OPT
  18 9.893113949   8.8.8.8          192.168.100.138  DNS       99 Standard query response 0x425d A google.com A 142.250.193.174 OPT
  20 9.920780098   8.8.8.8          192.168.100.138  DNS      111 Standard query response 0x1558 AAAA google.com AAAA 2404:6800:4007:81d::200e OPT
  23 9.970830184   192.168.100.138  8.8.8.8          DNS      101 Standard query 0x3f8e PTR 174.193.250.142.in-addr.arpa OPT
  24 10.060086355 8.8.8.8           192.168.100.138  DNS      140 Standard query response 0x3f8e PTR 174.193.250.142.in-addr.arpa PTR maa05s26-in-f14.1e100.net OPT
  29 12.470906785 192.168.100.138   8.8.8.8          DNS       88 Standard query 0x1d51 A www.youtube.com OPT
  30 12.471044482 192.168.100.138   8.8.8.8          DNS       88 Standard query 0x845b AAAA www.youtube.com OPT
```

```
▸ Frame 16: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 41151, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x425d
  ▸ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 1200
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▾ Z: 0x0000
          0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
    [Response In: 18]
```

```
0000  00 04 00 01 00 06 00 0c  29 f9 4f 7d 00 00 08 00   ········ )·O}····
0010  45 00 00 43 fa f8 40 00  40 11 0a 6f c0 a8 64 8a   E··C··@· @··o··d·
0020  08 08 08 08 a0 bf 00 35  00 2f 35 83 42 5d 01 20   ·······5 ·/5·B]· 
0030  00 01 00 00 00 00 00 01  06 67 6f 6f 67 6c 65 03   ········ ·google·
0040  63 6f 6d 00 00 01 00 01  00 00 29 04 b0 00 00 00   com····· ··)·····
0050  00 00 00                                           ···
```

Response:



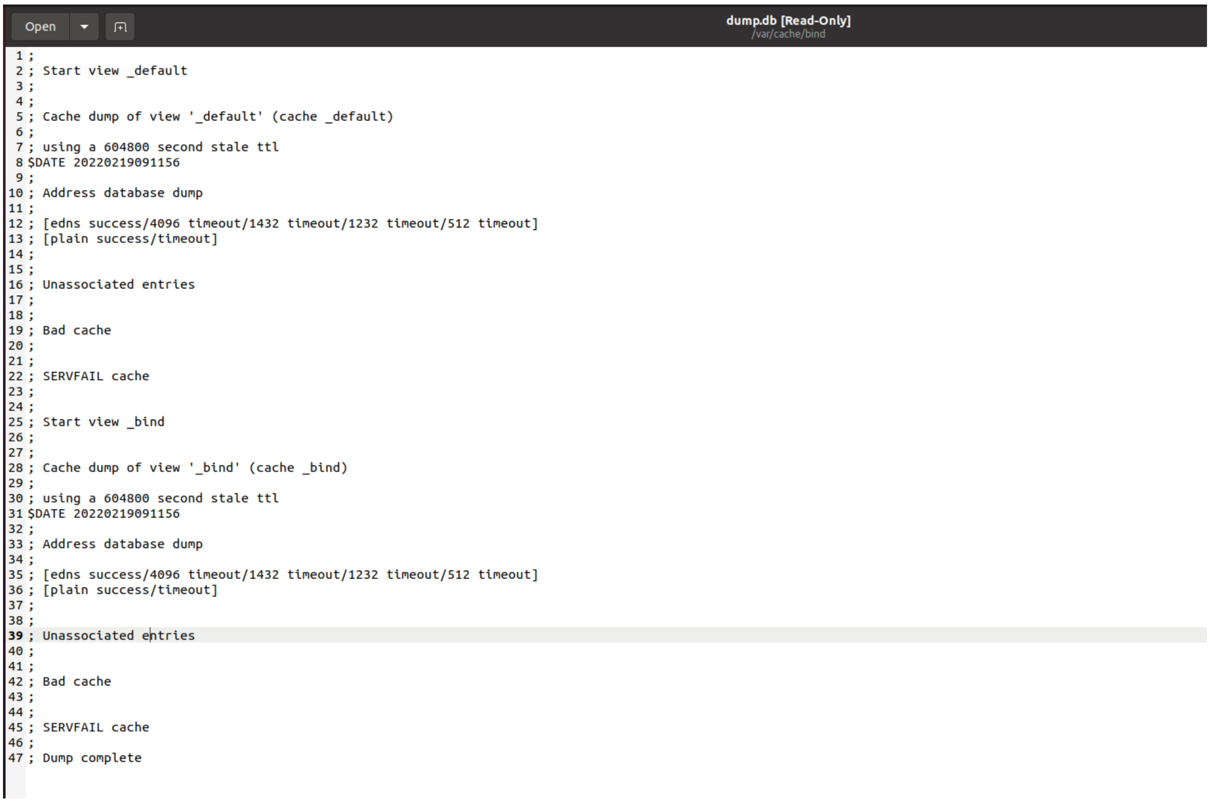
```
dns
No.  Time          Source           Destination      Protocol Length Info
  16 9.813640661   192.168.100.138  8.8.8.8          DNS       83 Standard query 0x425d A google.com OPT
  17 9.813752843   192.168.100.138  8.8.8.8          DNS       83 Standard query 0x1558 AAAA google.com OPT
  18 9.893113949   8.8.8.8          192.168.100.138  DNS       99 Standard query response 0x425d A google.com A 142.250.193.174 OPT
  20 9.920780098   8.8.8.8          192.168.100.138  DNS      111 Standard query response 0x1558 AAAA google.com AAAA 2404:6800:4007:81d::200e OPT
  23 9.970830184   192.168.100.138  8.8.8.8          DNS      101 Standard query 0x3f8e PTR 174.193.250.142.in-addr.arpa OPT
  24 10.060086355 8.8.8.8           192.168.100.138  DNS      140 Standard query response 0x3f8e PTR 174.193.250.142.in-addr.arpa PTR maa05s26-in-f14.1e100.net OPT
  29 12.470906785 192.168.100.138   8.8.8.8          DNS       88 Standard query 0x1d51 A www.youtube.com OPT
  30 12.471044482 192.168.100.138   8.8.8.8          DNS       88 Standard query 0x845b AAAA www.youtube.com OPT
```

```
▸ Frame 18: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.100.138
▸ User Datagram Protocol, Src Port: 53, Dst Port: 41151
▾ Domain Name System (response)
    Transaction ID: 0x425d
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ google.com: type A, class IN, addr 142.250.193.174
        Name: google.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 40 (40 seconds)
        Data length: 4
        Address: 142.250.193.174
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 512
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▾ Z: 0x0000
          0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
    [Request In: 16]
    [Time: 0.079473288 seconds]
```

```
0000  00 00 00 01 00 06 00 50  56 e6 5a 60 00 00 08 00   ·······P V·Z`····
0010  45 00 00 53 00 64 00 00  80 11 04 f4 08 08 08 08   E··S·d·· ········
0020  c0 a8 64 8a 00 35 a0 bf  00 3f 18 ba 42 5d 81 80   ··d··5·· ·?··B]··
0030  00 01 00 01 00 00 00 01  06 67 6f 6f 67 6c 65 03   ········ ·google·
0040  63 6f 6d 00 00 01 00 01  c0 0c 00 01 00 01 00 00   com····· ········
0050  00 28 00 04 8e fa c1 ae  00 00 29 02 00 00 00 00   ·(······ ··)·····
0060  00 00 00                                           ···
```

Dump.db file: contains cache details of google.com

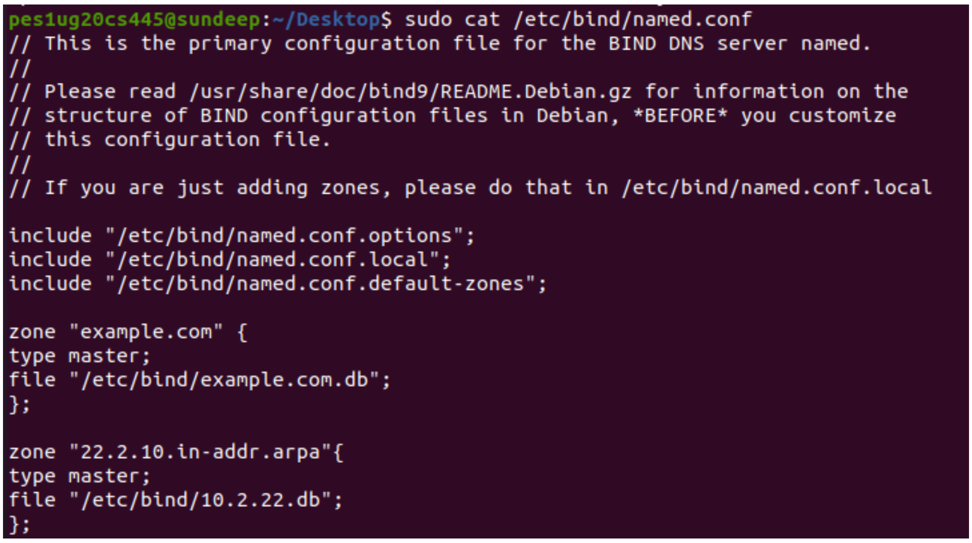
Observation 4:



```
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20220219091156
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; SERVFAIL cache
;
;
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
; using a 604800 second stale ttl
$DATE 20220219091156
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; SERVFAIL cache
;
; Dump complete
```

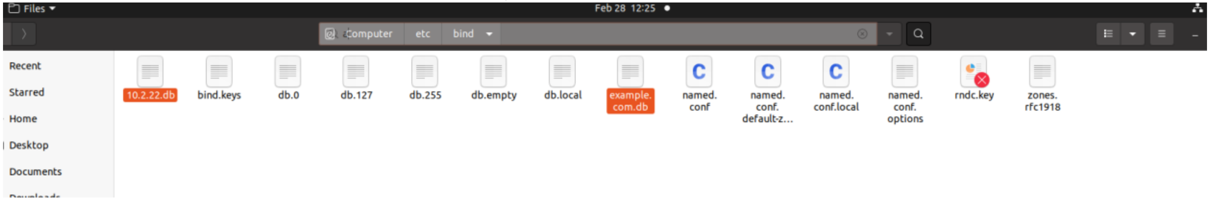
Part 2:

Task 3: Host a zone in the local DNS servere



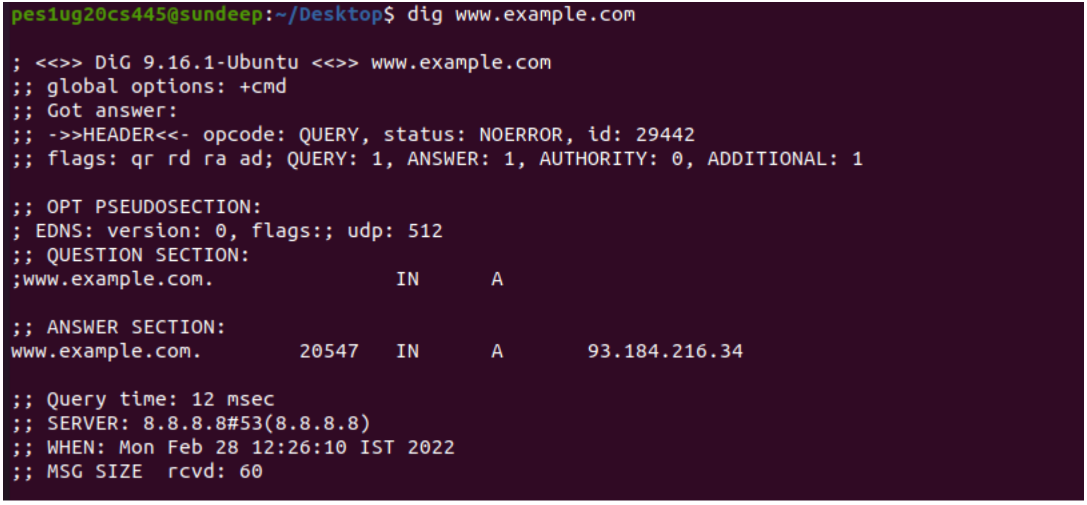
```
pes1ug20cs445@sundeep:~/Desktop$ sudo cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
type master;
file "/etc/bind/example.com.db";
};

zone "22.2.10.in-addr.arpa"{
type master;
file "/etc/bind/10.2.22.db";
};
```

Added both the files 10.2.22.db and example.com.db   to the location /etc/bind



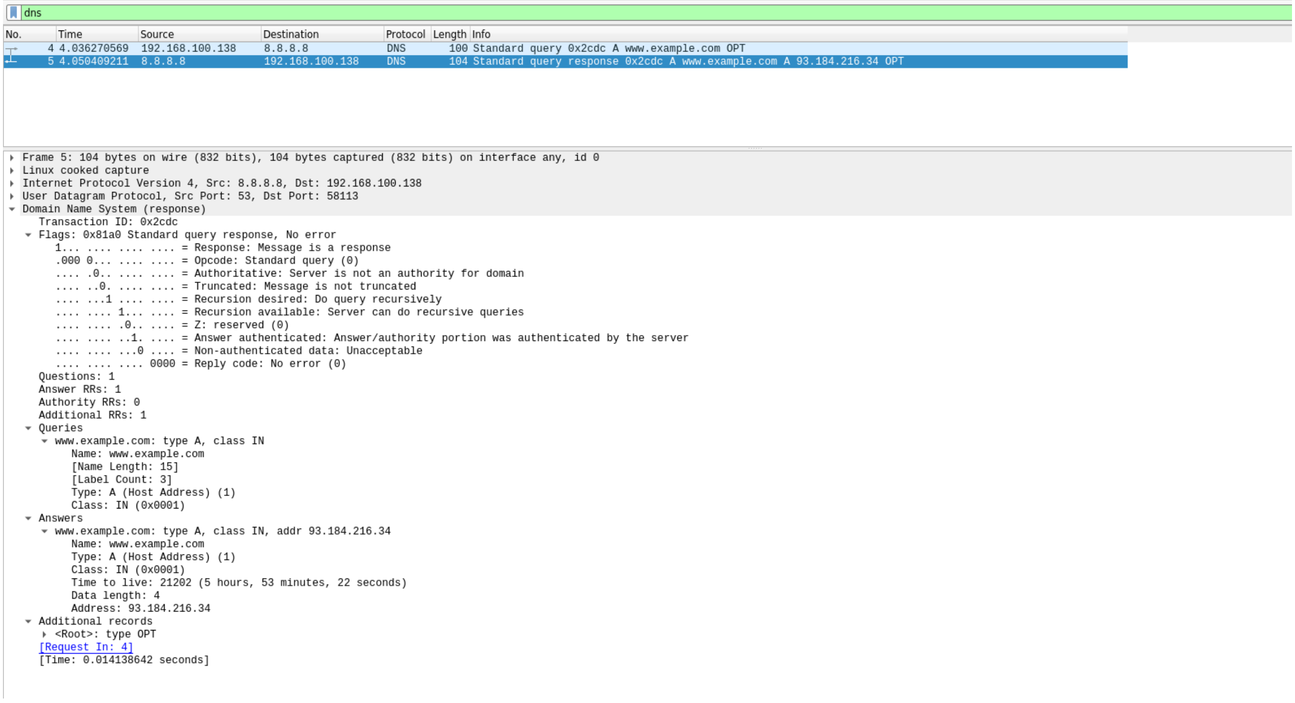
Task 4:

Using Dig command:



```
pes1ug20cs445@sundeep:~/Desktop$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29442
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        20547   IN      A       93.184.216.34

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Feb 28 12:26:10 IST 2022
;; MSG SIZE  rcvd: 60
```

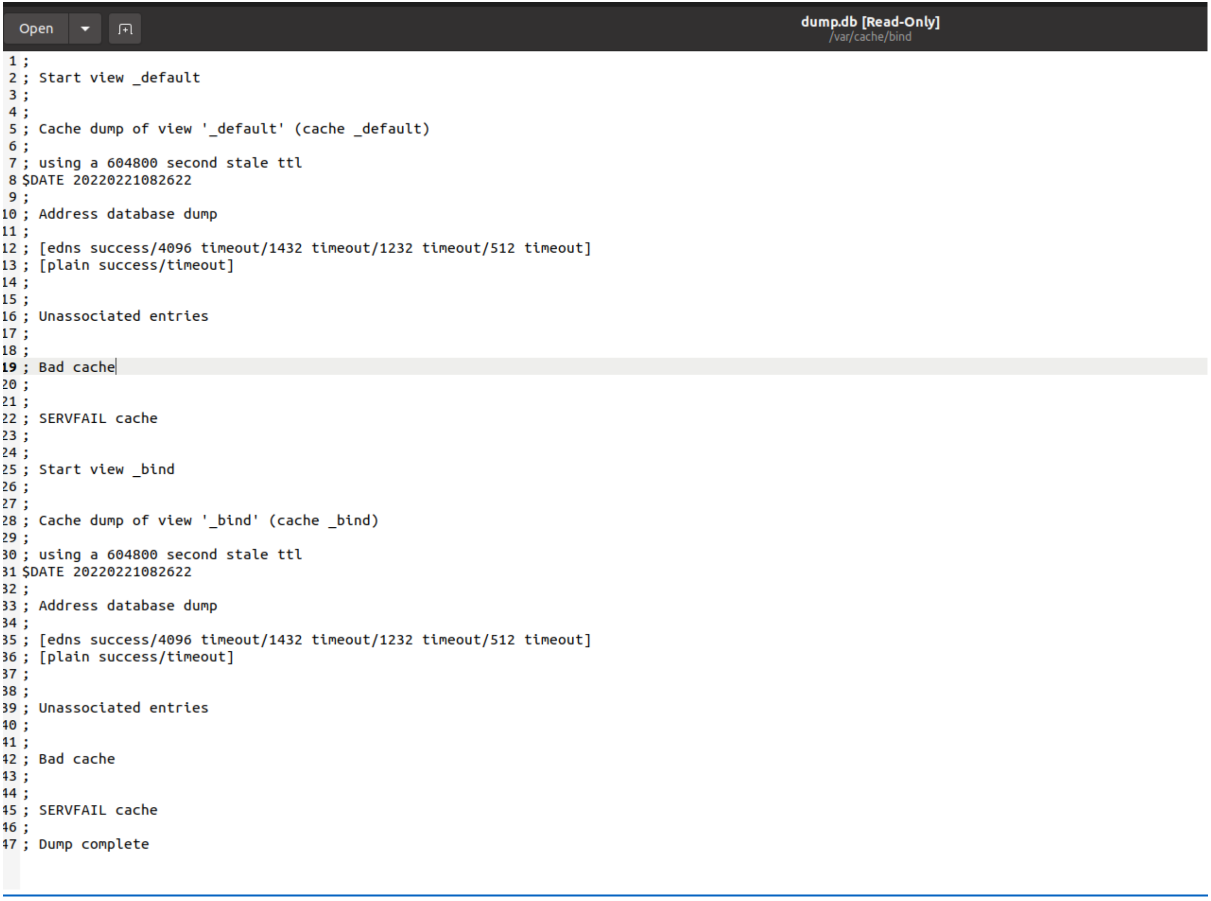
Observing in wireshark:



```
dns

No.     Time         Source           Destination      Protocol Length Info
      4 4.036270569  192.168.100.138  8.8.8.8          DNS      100 Standard query 0x2cdc A www.example.com OPT
      5 4.050409211  8.8.8.8          192.168.100.138  DNS      104 Standard query response 0x2cdc A www.example.com A 93.184.216.34 OPT

▸ Frame 5: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.100.138
▸ User Datagram Protocol, Src Port: 53, Dst Port: 58113
▾ Domain Name System (response)
    Transaction ID: 0x2cdc
  ▾ Flags: 0x81a0 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..1. .... = Answer authenticated: Answer/authority portion was authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ www.example.com: type A, class IN
        Name: www.example.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ www.example.com: type A, class IN, addr 93.184.216.34
        Name: www.example.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 21202 (5 hours, 53 minutes, 22 seconds)
        Data length: 4
        Address: 93.184.216.34
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 4]
    [Time: 0.014138642 seconds]
```

Here 192.168.100.138 is the IP address of my machine and
The IP address of the google dns server is 8.8.8.8

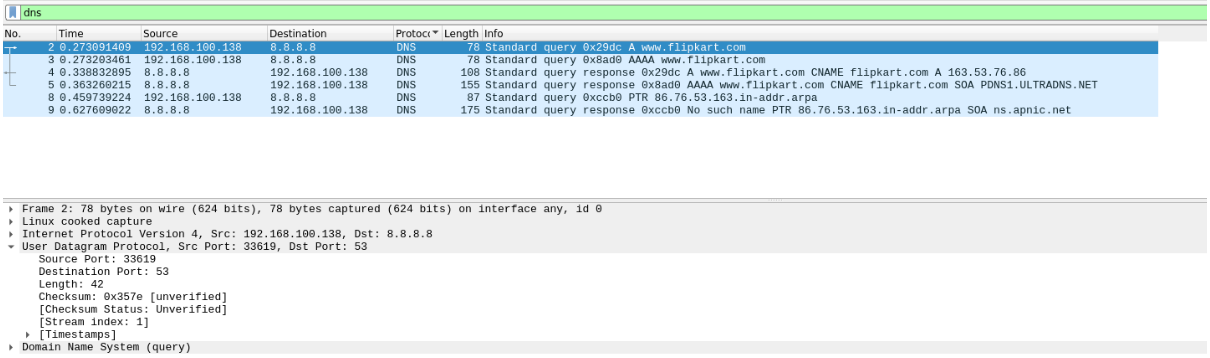
DNS cache after executing “dig www.example.com”



```
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20220221082622
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; SERVFAIL cache
;
;
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
; using a 604800 second stale ttl
$DATE 20220221082622
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; SERVFAIL cache
;
; Dump complete
```

Observation:

For ‘ping www.flipkart.com’, answer the following questions



```
No.  Time         Source           Destination      Protoco Length Info
   2 0.273091409  192.168.100.138  8.8.8.8          DNS        78 Standard query 0x29dc A www.flipkart.com
   3 0.273203461  192.168.100.138  8.8.8.8          DNS        78 Standard query 0x8ad0 AAAA www.flipkart.com
   4 0.338832895  8.8.8.8          192.168.100.138  DNS       108 Standard query response 0x29dc A www.flipkart.com CNAME flipkart.com A 163.53.76.86
   5 0.363260215  8.8.8.8          192.168.100.138  DNS       155 Standard query response 0x8ad0 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET
   8 0.459739224  192.168.100.138  8.8.8.8          DNS        87 Standard query 0xccb0 PTR 86.76.53.163.in-addr.arpa
   9 0.627609022  8.8.8.8          192.168.100.138  DNS       175 Standard query response 0xccb0 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net
```

```
▸ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 8.8.8.8
▾ User Datagram Protocol, Src Port: 33619, Dst Port: 53
    Source Port: 33619
    Destination Port: 53
    Length: 42
    Checksum: 0x357e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
▸ Domain Name System (query)
```

Q1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Answer - The DNS Query and Response messages are visible in the screenshots. They are sent over UDP.

Q2. What is the destination port for the DNS query message? What is the source port of DNS response message?

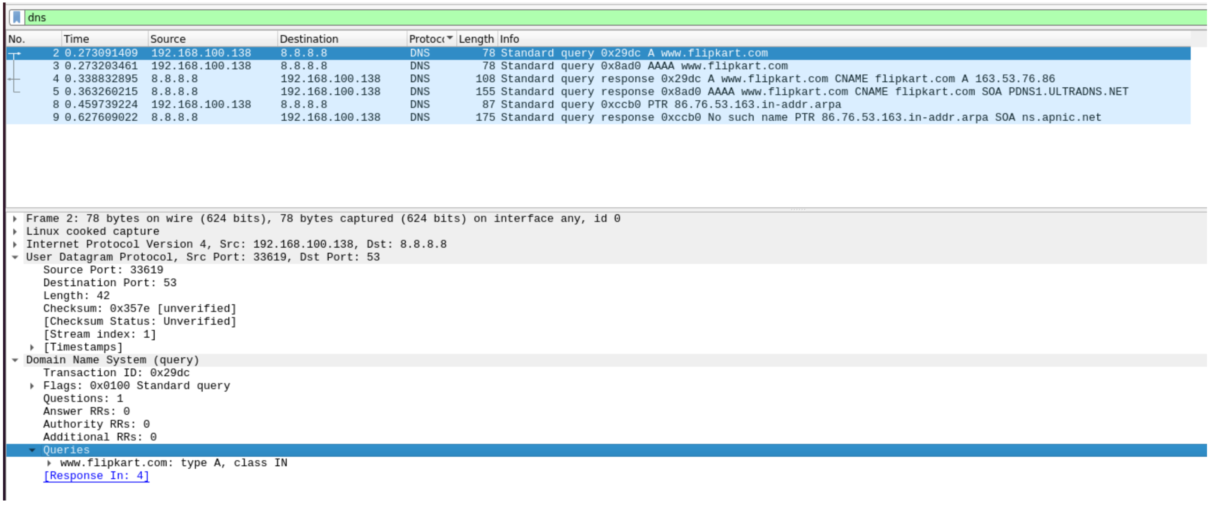
Answer – The destination Port is 53 and the source Port is 33619

Q3. 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 – The DNS query is made to server at the IP Address 8.8.8.8 This is the same as the local DNS server configured.

Q4. Examine the DNS query message. What “Type" of DNS query is it? Does the query message contain any “answers"?

Answer – The DNS Query is of type “A” since it requests for an authoritative record. The answer section is empty since it does not have any answer.

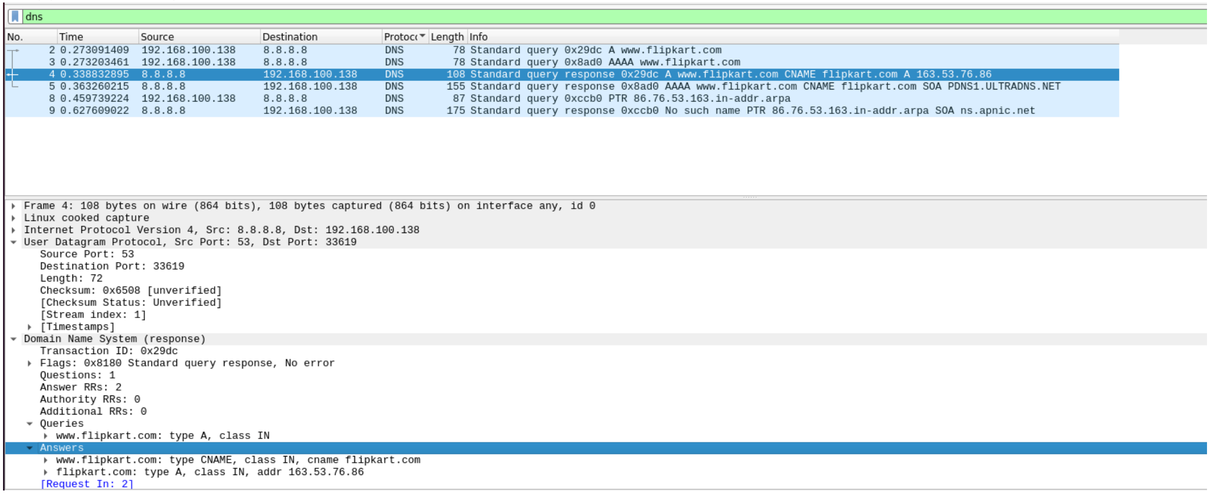


```
dns
No.   Time          Source             Destination       Protoc  Length Info
    2 0.273091409  192.168.100.138    8.8.8.8           DNS        78 Standard query 0x29dc A www.flipkart.com
    3 0.273203461  192.168.100.138    8.8.8.8           DNS        78 Standard query 0x8ad0 AAAA www.flipkart.com
    4 0.338832895  8.8.8.8            192.168.100.138   DNS       108 Standard query response 0x29dc A www.flipkart.com CNAME flipkart.com A 163.53.76.86
    5 0.363260215  8.8.8.8            192.168.100.138   DNS       155 Standard query response 0x8ad0 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET
    8 0.459739224  192.168.100.138    8.8.8.8           DNS        87 Standard query 0xccb0 PTR 86.76.53.163.in-addr.arpa
    9 0.627609022  8.8.8.8            192.168.100.138   DNS       175 Standard query response 0xccb0 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net

▸ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 8.8.8.8
▾ User Datagram Protocol, Src Port: 33619, Dst Port: 53
    Source Port: 33619
    Destination Port: 53
    Length: 42
    Checksum: 0x357e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0x29dc
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.flipkart.com: type A, class IN
    [Response In: 4]
```

Q5. Examine the DNS response message. How many “answers" are provided? What do each of these answers contain?

Answer – The answer section of the DNS response message contains two Resource Records.

- CNAME RR: This determines that the hostname flipkart.com refers to the canonical hostname www.flipkart.com.
- type A: This provides the IP Address of the canonical hostname.



```
dns
No.   Time          Source             Destination       Protoc  Length Info
    2 0.273091409  192.168.100.138    8.8.8.8           DNS        78 Standard query 0x29dc A www.flipkart.com
    3 0.273203461  192.168.100.138    8.8.8.8           DNS        78 Standard query 0x8ad0 AAAA www.flipkart.com
    4 0.338832895  8.8.8.8            192.168.100.138   DNS       108 Standard query response 0x29dc A www.flipkart.com CNAME flipkart.com A 163.53.76.86
    5 0.363260215  8.8.8.8            192.168.100.138   DNS       155 Standard query response 0x8ad0 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET
    8 0.459739224  192.168.100.138    8.8.8.8           DNS        87 Standard query 0xccb0 PTR 86.76.53.163.in-addr.arpa
    9 0.627609022  8.8.8.8            192.168.100.138   DNS       175 Standard query response 0xccb0 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net

▸ Frame 4: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.100.138
▾ User Datagram Protocol, Src Port: 53, Dst Port: 33619
    Source Port: 53
    Destination Port: 33619
    Length: 72
    Checksum: 0x6508 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
▾ Domain Name System (response)
    Transaction ID: 0x29dc
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.flipkart.com: type A, class IN
  ▾ Answers
    ▸ www.flipkart.com: type CNAME, class IN, cname flipkart.com
    ▸ flipkart.com: type A, class IN, addr 163.53.76.86
    [Request In: 2]
```

Q6. 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 – The destination IP Address of the SYN packet corresponds to the IP Address of hostname (www.flipkart.com) retrieved from the response message.