CN-Activity-01 (Aniruddha Mukherjee-2205533)

Caption: filter by DNS and DNS Query MessageFormat.png

💡 Name: Aniruddha Mukherjee

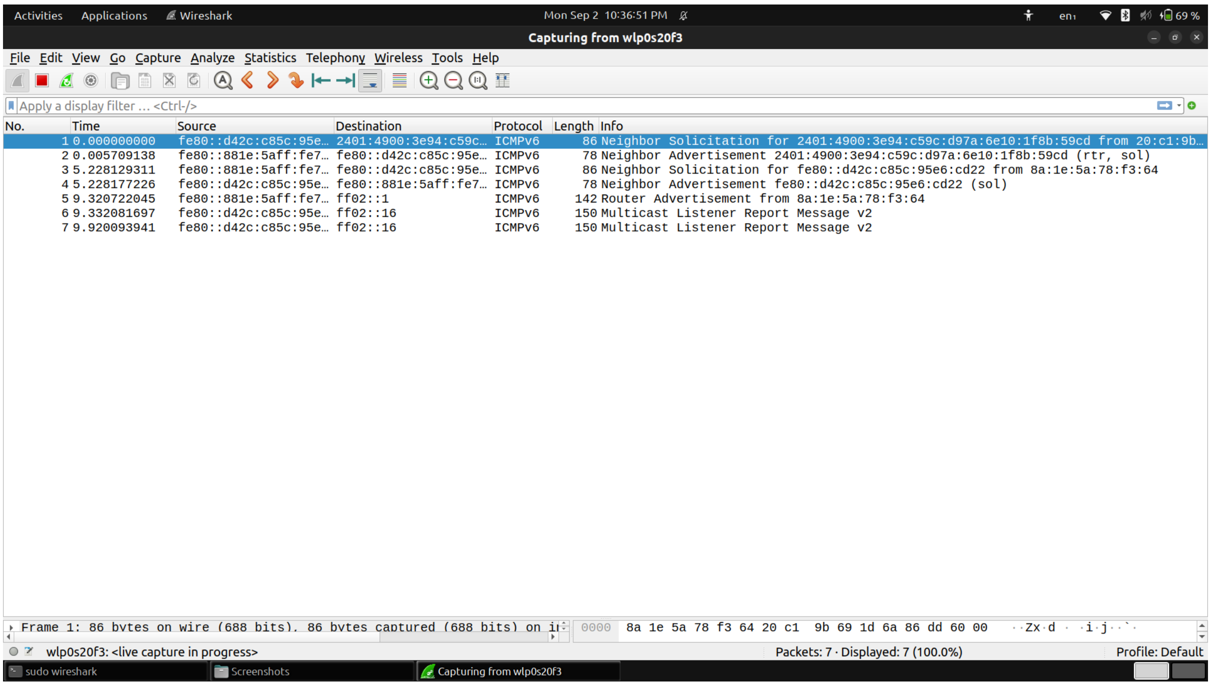
Roll: 2205533

Date: 02/09/2024

Activity-01: Capture and Analyze DNS Traffic

> 1. Install and start a Wireshark capture.

```
sudo add-apt-repository ppa:wireshark-dev/stable
sudo apt-get update
sudo apt-get install wireshark
sudo wireshark
```

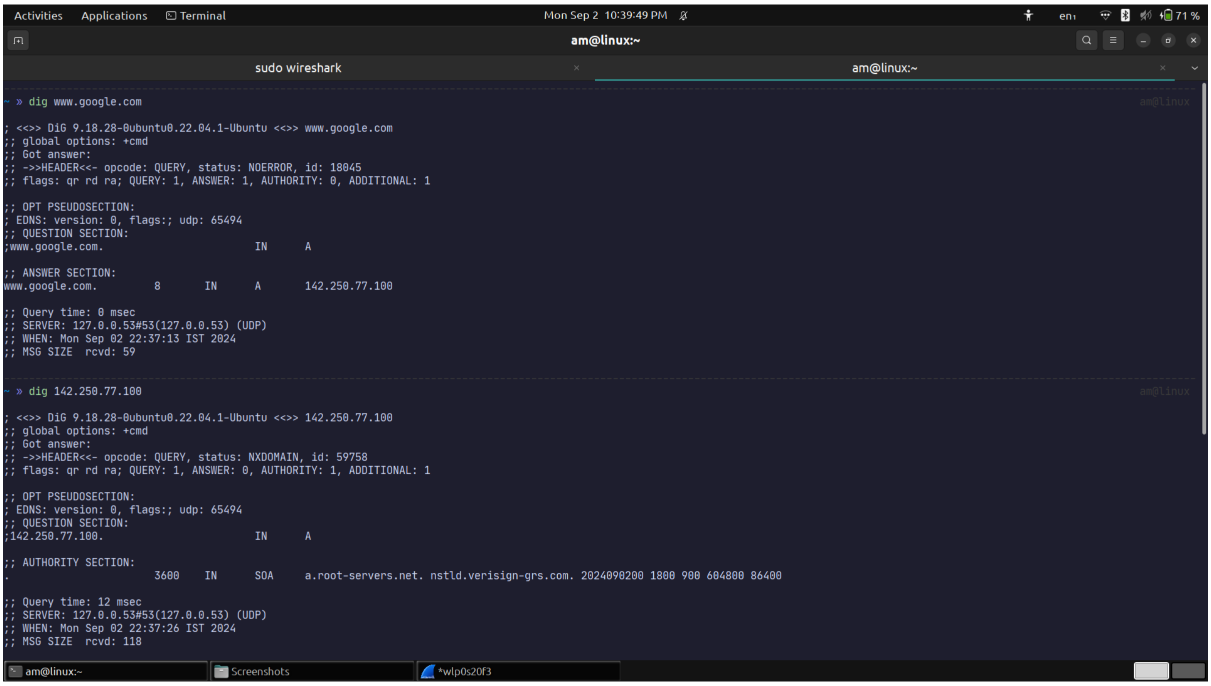


```
No.   Time          Source                Destination           Protocol  Length Info
    1 0.000000000   fe80::d42c:c85c:95e…  2401:4900:3e94:c59c…  ICMPv6        86 Neighbor Solicitation for 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd from 20:c1:9b…
    2 0.005709138   fe80::881e:5aff:fe7…  fe80::d42c:c85c:95e…  ICMPv6        78 Neighbor Advertisement 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd (rtr, sol)
    3 5.228129311   fe80::881e:5aff:fe7…  fe80::d42c:c85c:95e…  ICMPv6        86 Neighbor Solicitation for fe80::d42c:c85c:95e6:cd22 from 8a:1e:5a:78:f3:64
    4 5.228177226   fe80::d42c:c85c:95e…  fe80::881e:5aff:fe7…  ICMPv6        78 Neighbor Advertisement fe80::d42c:c85c:95e6:cd22 (sol)
    5 9.320722045   fe80::881e:5aff:fe7…  ff02::1               ICMPv6       142 Router Advertisement from 8a:1e:5a:78:f3:64
    6 9.332081697   fe80::d42c:c85c:95e…  ff02::16              ICMPv6       150 Multicast Listener Report Message v2
    7 9.920093941   fe80::d42c:c85c:95e…  ff02::16              ICMPv6       150 Multicast Listener Report Message v2

› Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on i   0000  8a 1e 5a 78 f3 64 20 c1  9b 69 1d 6a 86 dd 60 00   ··Zx·d · ·i·j··`·

wlp0s20f3: <live capture in progress>          Packets: 7 · Displayed: 7 (100.0%)          Profile: Default
```

Caption: started wireshark.png

Using `wlp0s20f3` for wireless connection.

> 2. Use one of the utility commands (nslookup/host/dig) to get the IP Address of the server say "www.google.com" and vice-versa (i.e. provide the IP address and get the hostname).\

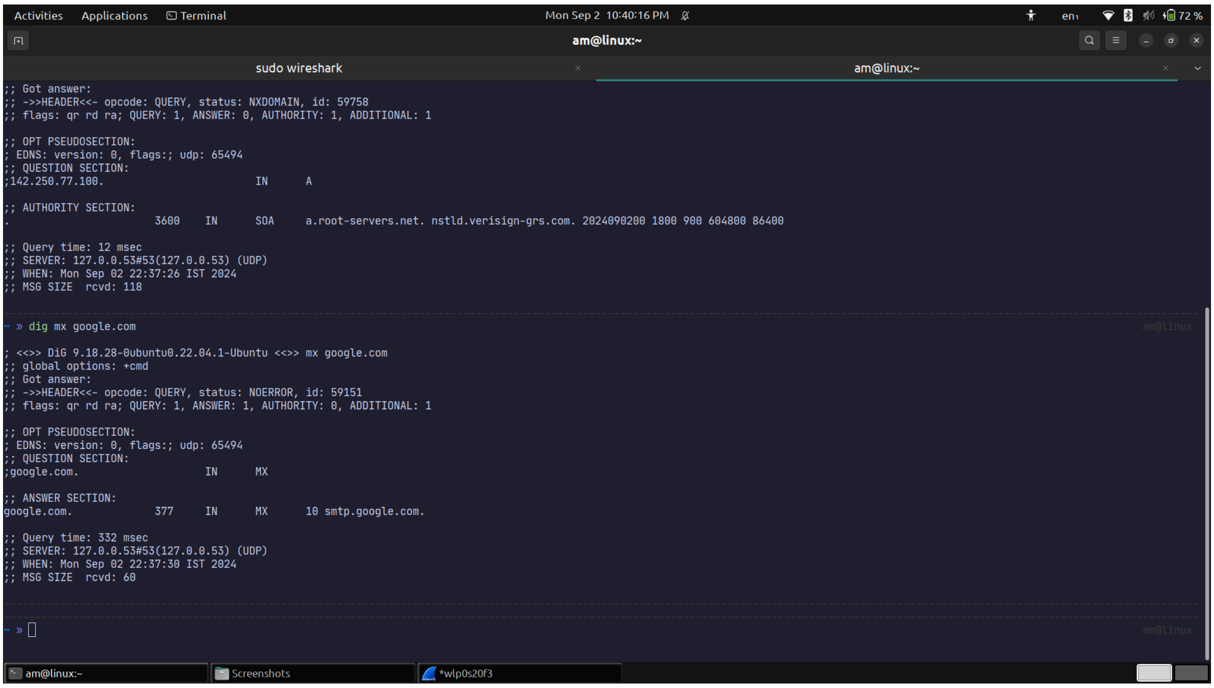


```
~ » dig www.google.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18045
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         8       IN      A       142.250.77.100

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Sep 02 22:37:13 IST 2024
;; MSG SIZE  rcvd: 59

~ » dig 142.250.77.100

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> 142.250.77.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59758
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;142.250.77.100.                        IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024090200 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Sep 02 22:37:26 IST 2024
;; MSG SIZE  rcvd: 118
```

Caption: screenshot of looking up googles ip.png

Google IP: `142.250.77.100`

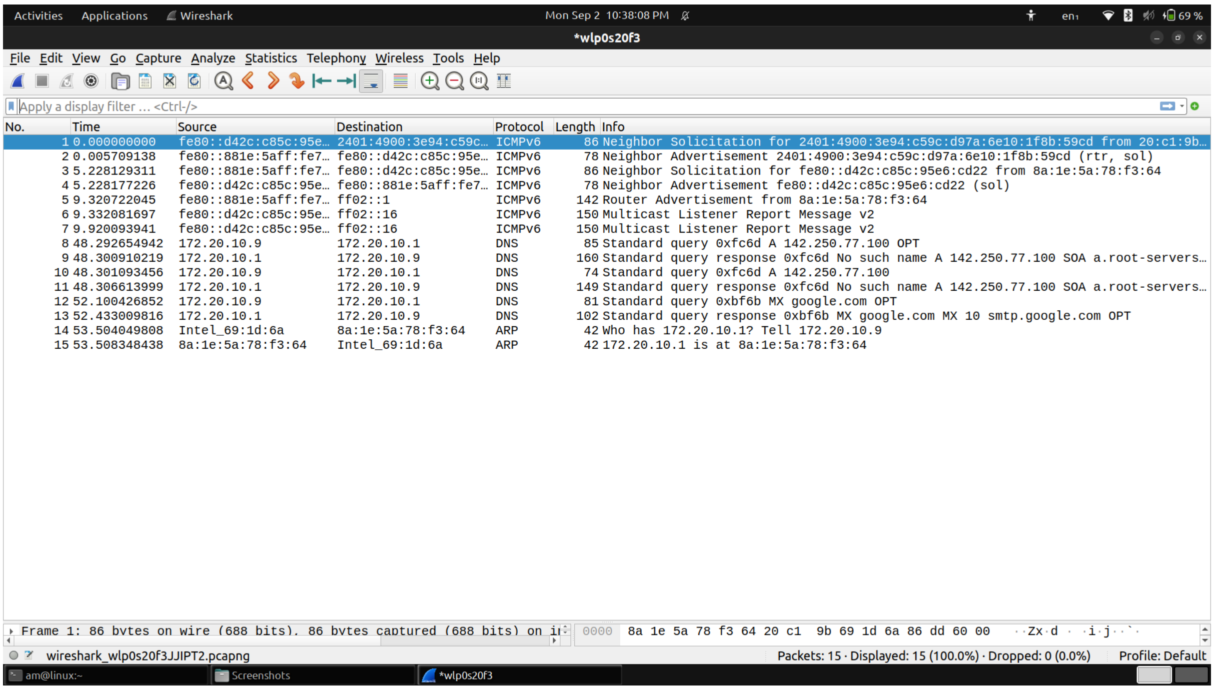
> 3. Using one of these utility tools find out the mail server attached to the webserver
> "
>
> google.com".



```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59758
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;142.250.77.100.                        IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024090200 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Sep 02 22:37:26 IST 2024
;; MSG SIZE  rcvd: 118

~ » dig mx google.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> mx google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59151
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             377     IN      MX      10 smtp.google.com.

;; Query time: 332 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Sep 02 22:37:30 IST 2024
;; MSG SIZE  rcvd: 60

~ »
```

MailServer: stmp.google.com

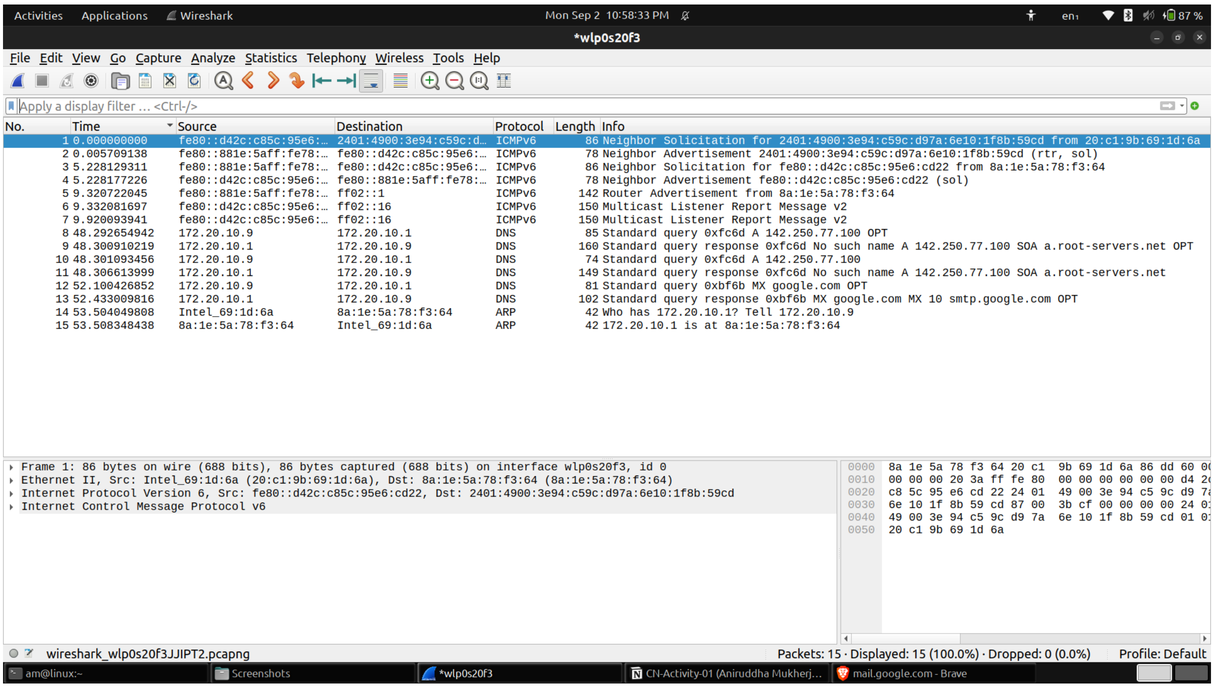
4. Stop the Wireshark capture.



```
No. Time         Source               Destination          Protocol Length Info
  1 0.000000000  fe80::d42c:c85c:95e… 2401:4900:3e94:c59c… ICMPv6     86 Neighbor Solicitation for 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd from 20:c1:9b…
  2 0.005709138  fe80::881e:5aff:fe7… fe80::d42c:c85c:95e… ICMPv6     78 Neighbor Advertisement 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd (rtr, sol)
  3 5.228129311  fe80::881e:5aff:fe7… fe80::d42c:c85c:95e… ICMPv6     86 Neighbor Solicitation for fe80::d42c:c85c:95e6:cd22 from 8a:1e:5a:78:f3:64
  4 5.228177226  fe80::d42c:c85c:95e… fe80::881e:5aff:fe7… ICMPv6     78 Neighbor Advertisement fe80::d42c:c85c:95e6:cd22 (sol)
  5 9.320722045  fe80::881e:5aff:fe7… ff02::1              ICMPv6    142 Router Advertisement from 8a:1e:5a:78:f3:64
  6 9.332081697  fe80::d42c:c85c:95e… ff02::16             ICMPv6    150 Multicast Listener Report Message v2
  7 9.920093941  fe80::d42c:c85c:95e… ff02::16             ICMPv6    150 Multicast Listener Report Message v2
  8 48.292654942 172.20.10.9          172.20.10.1          DNS        85 Standard query 0xfc6d A 142.250.77.100 OPT
  9 48.300910219 172.20.10.1          172.20.10.9          DNS       160 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers…
 10 48.301093456 172.20.10.9          172.20.10.1          DNS        74 Standard query 0xfc6d A 142.250.77.100
 11 48.306613999 172.20.10.1          172.20.10.9          DNS       149 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers…
 12 52.100426852 172.20.10.9          172.20.10.1          DNS        81 Standard query 0xbf6b MX google.com OPT
 13 52.433009816 172.20.10.1          172.20.10.9          DNS       102 Standard query response 0xbf6b MX google.com MX 10 smtp.google.com OPT
 14 53.504049808 Intel_69:1d:6a       8a:1e:5a:78:f3:64    ARP        42 Who has 172.20.10.1? Tell 172.20.10.9
 15 53.508348438 8a:1e:5a:78:f3:64    Intel_69:1d:6a       ARP        42 172.20.10.1 is at 8a:1e:5a:78:f3:64

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on i   0000  8a 1e 5a 78 f3 64 20 c1  9b 69 1d 6a 86 dd 60 00   ··Zx·d · ·i·j··`·
```

Filename: stopped capturing from wireshark.png

> 5. Filter the traffic captured in the Wireshark to view only DNS traffic and Findout the DNS
> message format from the same.


Activities
Applications
Wireshark
Mon Sep 2 10:58:33 PM
en₁
87 %
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time          Source                      Destination                 Protocol  Length Info
     1 0.000000000   fe80::d42c:c85c:95e6:…      2401:4900:3e94:c59c:d…      ICMPv6        86 Neighbor Solicitation for 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd from 20:c1:9b:69:1d:6a
     2 0.005709138   fe80::881e:5aff:fe78:…      fe80::d42c:c85c:95e6:…      ICMPv6        78 Neighbor Advertisement 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd (rtr, sol)
     3 5.228129311   fe80::881e:5aff:fe78:…      fe80::d42c:c85c:95e6:…      ICMPv6        86 Neighbor Solicitation for fe80::d42c:c85c:95e6:cd22 from 8a:1e:5a:78:f3:64
     4 5.228177226   fe80::d42c:c85c:95e6:…      fe80::881e:5aff:fe78:…      ICMPv6        78 Neighbor Advertisement fe80::d42c:c85c:95e6:cd22 (sol)
     5 9.320722045   fe80::881e:5aff:fe78:…      ff02::1                     ICMPv6       142 Router Advertisement from 8a:1e:5a:78:f3:64
     6 9.332081697   fe80::d42c:c85c:95e6:…      ff02::16                    ICMPv6       150 Multicast Listener Report Message v2
     7 9.920093941   fe80::d42c:c85c:95e6:…      ff02::16                    ICMPv6       150 Multicast Listener Report Message v2
     8 48.292654942  172.20.10.9                 172.20.10.1                 DNS           85 Standard query 0xfc6d A 142.250.77.100 OPT
     9 48.300910219  172.20.10.1                 172.20.10.9                 DNS          160 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers.net OPT
    10 48.301093456  172.20.10.9                 172.20.10.1                 DNS           74 Standard query 0xfc6d A 142.250.77.100
    11 48.306613999  172.20.10.1                 172.20.10.9                 DNS          149 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers.net
    12 52.100426852  172.20.10.9                 172.20.10.1                 DNS           81 Standard query 0xbf6b MX google.com OPT
    13 52.433009816  172.20.10.1                 172.20.10.9                 DNS          102 Standard query response 0xbf6b MX google.com MX 10 smtp.google.com OPT
    14 53.504049808  Intel_69:1d:6a              8a:1e:5a:78:f3:64           ARP           42 Who has 172.20.10.1? Tell 172.20.10.9
    15 53.508348438  8a:1e:5a:78:f3:64           Intel_69:1d:6a              ARP           42 172.20.10.1 is at 8a:1e:5a:78:f3:64
```

```
› Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlp0s20f3, id 0
› Ethernet II, Src: Intel_69:1d:6a (20:c1:9b:69:1d:6a), Dst: 8a:1e:5a:78:f3:64 (8a:1e:5a:78:f3:64)
› Internet Protocol Version 6, Src: fe80::d42c:c85c:95e6:cd22, Dst: 2401:4900:3e94:c59c:d97a:6e10:1f8b:59cd
› Internet Control Message Protocol v6
```

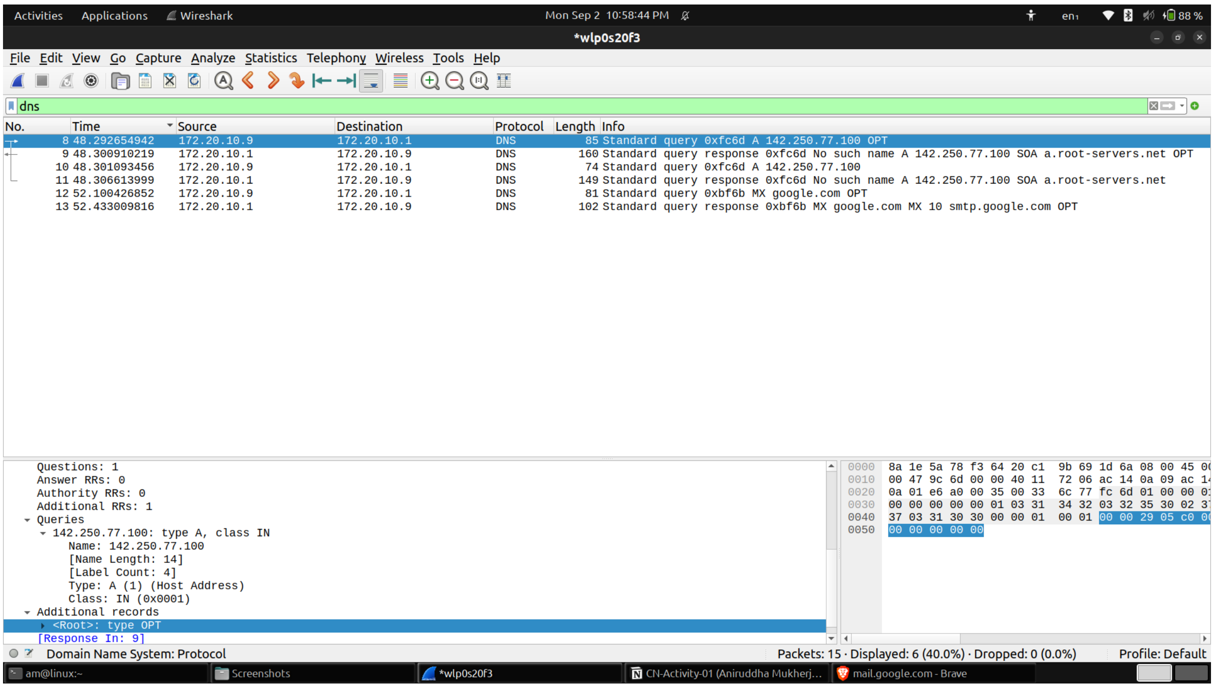
```
0000  8a 1e 5a 78 f3 64 20 c1  9b 69 1d 6a 86 dd 60 00
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 d4 2c
0020  c8 5c 95 e6 cd 22 24 01  49 00 3e 94 c5 9c d9 7a
0030  6e 10 1f 8b 59 cd 87 00  3b cf 00 00 00 00 24 01
0040  49 00 3e 94 c5 9c d9 7a  6e 10 1f 8b 59 cd 01 01
0050  20 c1 9b 69 1d 6a
```

wireshark_wlp0s20f3JJIPT2.pcapng

Packets: 15 · Displayed: 15 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Caption: pre-filtering-for-dns.png



Filter: dns

```
No.  Time          Source        Destination   Protocol Length Info
   8 48.292654942  172.20.10.9   172.20.10.1   DNS       85 Standard query 0xfc6d A 142.250.77.100 OPT
   9 48.300910219  172.20.10.1   172.20.10.9   DNS      160 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers.net OPT
  10 48.301093456  172.20.10.9   172.20.10.1   DNS       74 Standard query 0xfc6d A 142.250.77.100
  11 48.306613999  172.20.10.1   172.20.10.9   DNS      149 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers.net
  12 52.100426852  172.20.10.9   172.20.10.1   DNS       81 Standard query 0xbf6b MX google.com OPT
  13 52.433009816  172.20.10.1   172.20.10.9   DNS      102 Standard query response 0xbf6b MX google.com MX 10 smtp.google.com OPT
```

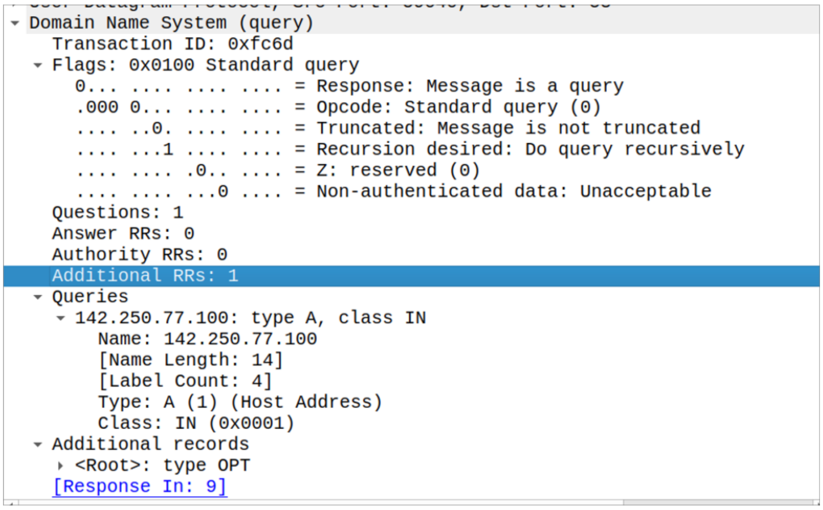
```
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ 142.250.77.100: type A, class IN
        Name: 142.250.77.100
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Additional records
    ▸ <Root>: type OPT
    [Response In: 9]
```

```
0000  8a 1e 5a 78 f3 64 20 c1  9b 69 1d 6a 08 00 45 0
0010  00 47 9c 6d 00 00 40 11  72 06 ac 14 0a 09 ac 1
0020  0a 01 e6 a0 00 35 00 33  6c 77 fc 6d 01 00 00 0
0030  00 00 00 00 00 01 03 31  34 32 03 32 35 30 02 3
0040  37 03 31 30 30 00 00 01  00 01 00 00 29 05 c0 0
0050  00 00 00 00 00
```

Domain Name System: Protocol   Packets: 15 · Displayed: 6 (40.0%) · Dropped: 0 (0.0%)   Profile: Default

Caption: post-filter-for-dns.png

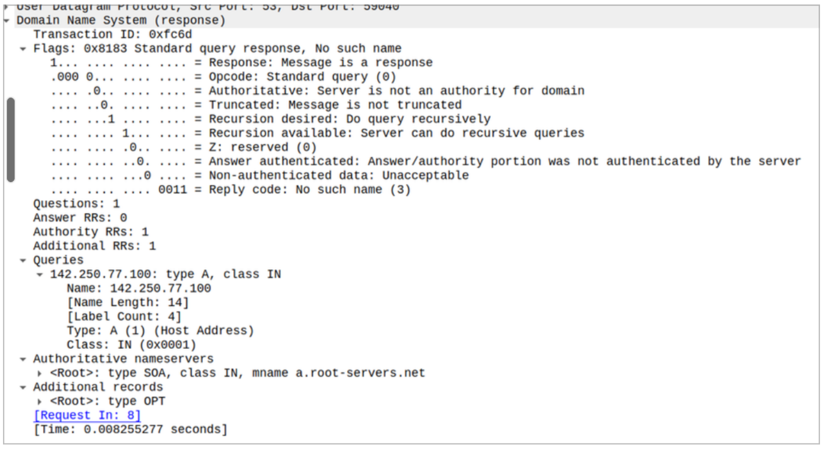
DNS Message format (Query):



```
▾ Domain Name System (query)
    Transaction ID: 0xfc6d
  ▾ Flags: 0x0100 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)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ 142.250.77.100: type A, class IN
        Name: 142.250.77.100
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Additional records
    ▸ <Root>: type OPT
    [Response In: 9]
```

`TransactionID,`
`Flags,`
`Questions,`
`AnswerRRs,`
`AdditionalRRs`
`Queries,`
`Additional recrods`

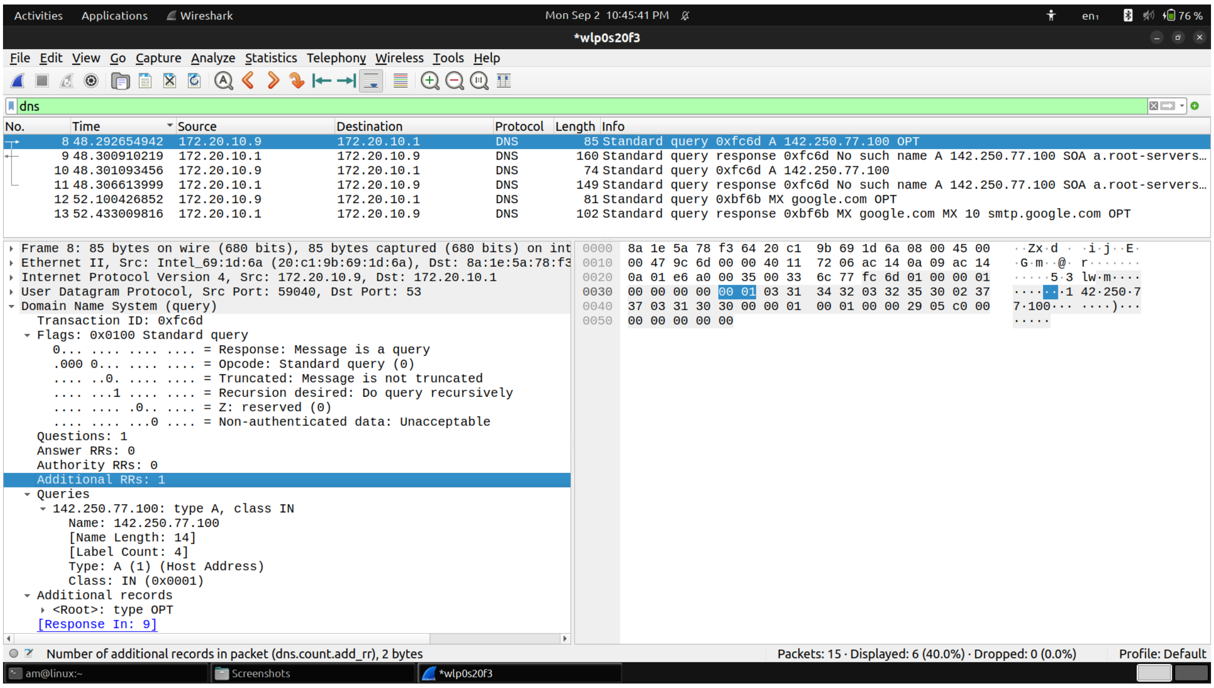
DNSQueryResponse Message Format



```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 59040
▾ Domain Name System (response)
    Transaction ID: 0xfc6d
  ▾ Flags: 0x8183 Standard query response, No such name
      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)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 1
  ▾ Queries
    ▾ 142.250.77.100: type A, class IN
        Name: 142.250.77.100
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Authoritative nameservers
    ▸ <Root>: type SOA, class IN, mname a.root-servers.net
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 8]
    [Time: 0.008255277 seconds]
```

```
TransactionID,
Flags,
Questions,
AnswerRRs,
AuthorityRRs,
AdditionalRRs,
Queries,
Authoritative nameservers,
Additional records
```

> 6. From the above filtered DNS traffic, select the first packet which should be a packet containing DNS Query and findout the following information and it's significance.
>
> - SrcIP and DestIP.
> - SrcPort and DestPort.
> - Transport Layer Protocol Used.
> - It's a query or response message?
> - Query type is iterative or recusive?
> - What is queried and through which type of resource record (RR)?


Activities
Applications
Wireshark
Mon Sep 2 10:45:41 PM
en₁
76 %
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time          Source        Destination   Protocol Length Info
    8 48.292654942  172.20.10.9   172.20.10.1   DNS      85 Standard query 0xfc6d A 142.250.77.100 OPT
    9 48.300910219  172.20.10.1   172.20.10.9   DNS     160 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers…
   10 48.301093456  172.20.10.9   172.20.10.1   DNS      74 Standard query 0xfc6d A 142.250.77.100
   11 48.306613999  172.20.10.1   172.20.10.9   DNS     149 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers…
   12 52.100426852  172.20.10.9   172.20.10.1   DNS      81 Standard query 0xbf6b MX google.com OPT
   13 52.433009816  172.20.10.1   172.20.10.9   DNS     102 Standard query response 0xbf6b MX google.com MX 10 smtp.google.com OPT
```

```
› Frame 8: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on int
› Ethernet II, Src: Intel_69:1d:6a (20:c1:9b:69:1d:6a), Dst: 8a:1e:5a:78:f3
› Internet Protocol Version 4, Src: 172.20.10.9, Dst: 172.20.10.1
› User Datagram Protocol, Src Port: 59040, Dst Port: 53
˅ Domain Name System (query)
    Transaction ID: 0xfc6d
  ˅ Flags: 0x0100 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)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ˅ Queries
    ˅ 142.250.77.100: type A, class IN
        Name: 142.250.77.100
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ˅ Additional records
    › <Root>: type OPT
    [Response In: 9]
```

```
0000  8a 1e 5a 78 f3 64 20 c1  9b 69 1d 6a 08 00 45 00   ··Zx·d · ·i·j··E·
0010  00 47 9c 6d 00 00 40 11  72 06 ac 14 0a 09 ac 14   ·G·m··@· r·······
0020  0a 01 e6 a0 00 35 00 33  6c 77 fc 6d 01 00 00 01   ·····5·3 lw·m····
0030  00 00 00 00 00 01 03 31  34 32 03 32 35 30 02 37   ·······1 42·250·7
0040  37 03 31 30 30 00 00 01  00 01 00 00 29 05 c0 00   7·100··· ····)···
0050  00 00 00 00 00                                     ·····
```

Number of additional records in packet (dns.count.add_rr), 2 bytes   Packets: 15 · Displayed: 6 (40.0%) · Dropped: 0 (0.0%)   Profile: Default

Caption: filter by DNS and DNS Query MessageFormat.png

SrcIP and DestIP: `172.20.10.9` | `172.20.10.1`

SrcPort and DestPort: `59040` | `53`

Transport Layer Protocol Used: `User Datagram Protocol`

Is it a query or response message: It is a Query message
(Look at the first Flag (0) , "Message is a query")

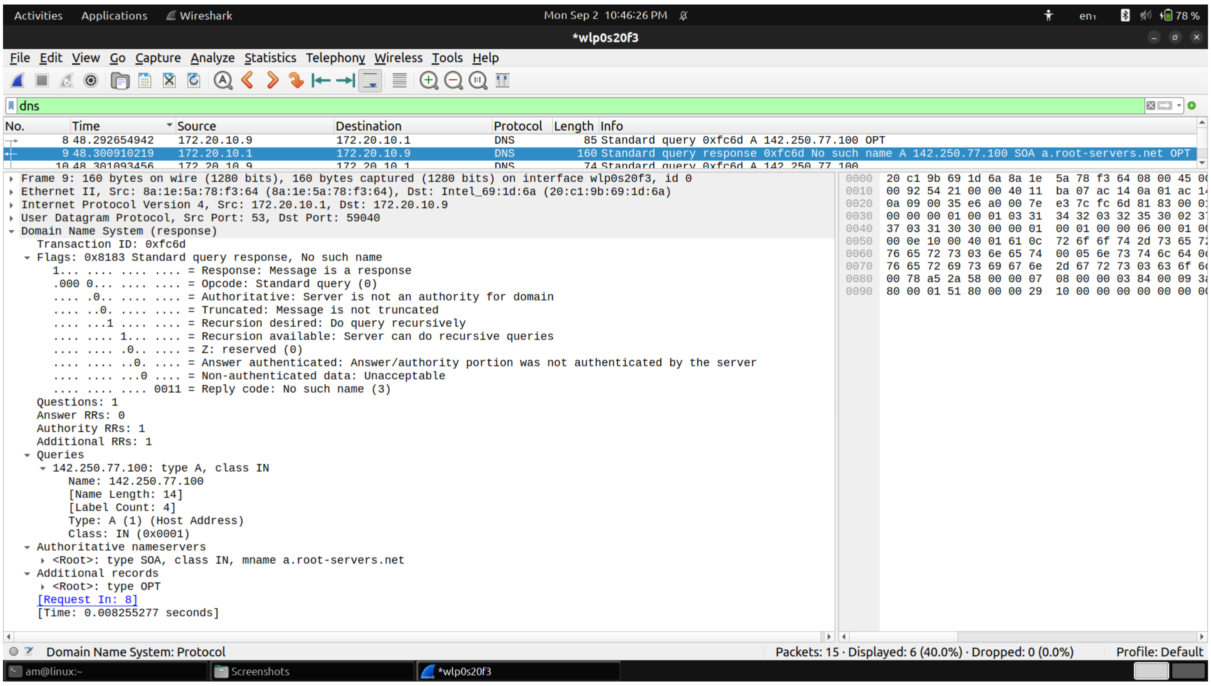
Query type is `recursive`
(Look at the Flag: Recursion desired, do query recursively)

The IP Address of www.google.com is queried.
(142.150.77.100: type A, class IN)

This is done using the `Additional RRs`

> 7. From the above filtered DNS traffic, select the a packet containing DNS Answer and
> findout the following information and it's significance.
> - SrcIP and DestIP.
> - SrcPort and DestPort.
> - Transport Layer Protocol Used.
> - It's a query or response message?

- Query type is iterative or recusive?
- What is the Answer for the requested Query?


Activities
Applications
Wireshark
Mon Sep 2 10:46:26 PM
en₁
78 %
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time            Source         Destination    Protocol  Length Info
   8 48.292654942    172.20.10.9    172.20.10.1    DNS           85 Standard query 0xfc6d A 142.250.77.100 OPT
   9 48.300910219    172.20.10.1    172.20.10.9    DNS          160 Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers.net OPT
  10 48.301093456    172.20.10.9    172.20.10.1    DNS           74 Standard query 0xfc6d A 142.250.77.100
```

```
› Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlp0s20f3, id 0
› Ethernet II, Src: 8a:1e:5a:78:f3:64 (8a:1e:5a:78:f3:64), Dst: Intel_69:1d:6a (20:c1:9b:69:1d:6a)
› Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.9
› User Datagram Protocol, Src Port: 53, Dst Port: 59040
⌄ Domain Name System (response)
    Transaction ID: 0xfc6d
  ⌄ Flags: 0x8183 Standard query response, No such name
      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)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 1
  ⌄ Queries
    ⌄ 142.250.77.100: type A, class IN
        Name: 142.250.77.100
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ⌄ Authoritative nameservers
    › <Root>: type SOA, class IN, mname a.root-servers.net
  ⌄ Additional records
    › <Root>: type OPT
    [Request In: 8]
    [Time: 0.008255277 seconds]
```

```
0000  20 c1 9b 69 1d 6a 8a 1e  5a 78 f3 64 08 00 45
0010  00 92 54 21 00 00 40 11  ba 07 ac 14 0a 01 ac
0020  0a 09 00 35 e6 a0 00 7e  e3 7c fc 6d 81 83 00
0030  00 00 00 01 00 01 03 31  34 32 03 32 35 30 02
0040  37 03 31 30 30 00 00 01  00 01 00 00 06 00 01
0050  00 0e 10 00 40 01 61 0c  72 6f 6f 74 2d 73 65
0060  76 65 72 73 03 6e 65 74  00 05 6e 73 74 6c 64
0070  76 65 72 69 73 69 67 6e  2d 67 72 73 03 63 6f
0080  00 78 a5 2a 58 00 00 07  08 00 00 03 84 00 09
0090  80 00 01 51 80 00 00 29  10 00 00 00 00 00 00
```

```
Domain Name System: Protocol    Packets: 15 · Displayed: 6 (40.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Caption: Filter by DNS and DNSQueryResponse Message Format.png

SrcIP and DestIP: `172.20.10.9` | `172.20.10.1`

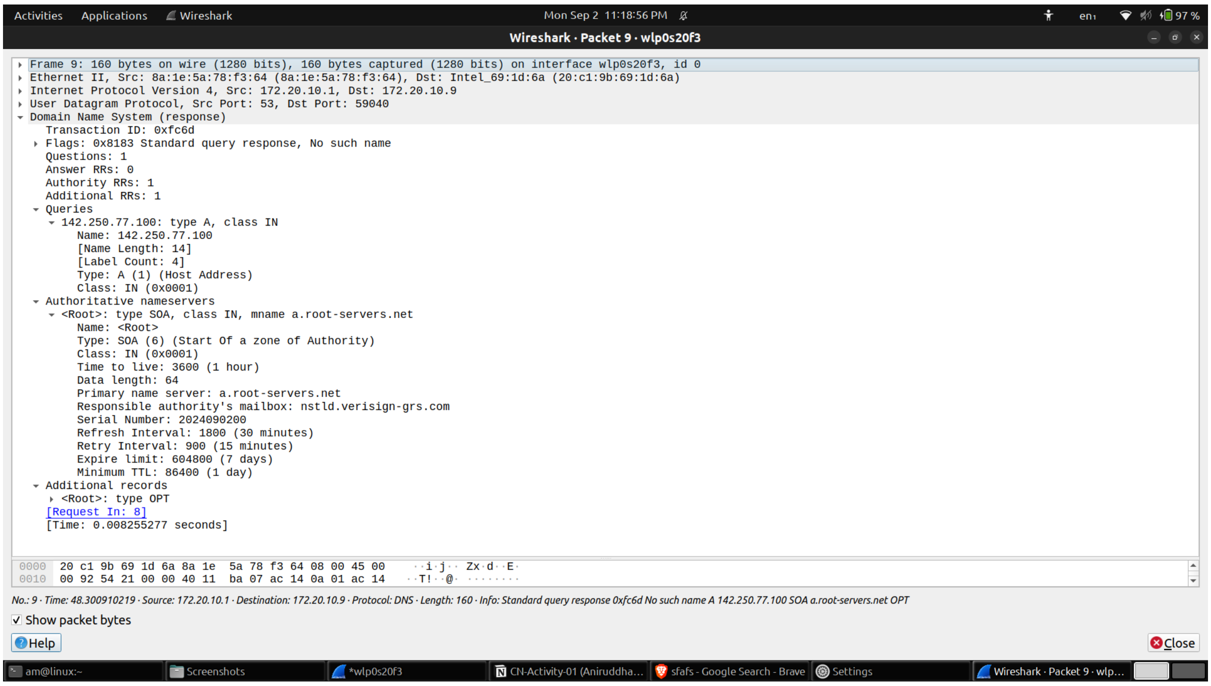
SrcPort and DestPort: `53` | `59040`

Transport Layer Protocol Used: `User Datagram Protocol`

Is it a query or response message: It is a Response message
(Look at the first Flag (1) , "Message is a response")

Query type is `recursive`
(Look at the Flag: Recursion desired, do query recursively)

The "Authority nameservers" is the Answer for the record.
Also the A record which is an Address record is the answer which maps www.google.com to a IPv4 address.



```
▸ Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlp0s20f3, id 0
▸ Ethernet II, Src: 8a:1e:5a:78:f3:64 (8a:1e:5a:78:f3:64), Dst: Intel_69:1d:6a (20:c1:9b:69:1d:6a)
▸ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.9
▸ User Datagram Protocol, Src Port: 53, Dst Port: 59040
▾ Domain Name System (response)
    Transaction ID: 0xfc6d
  ▸ Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 1
  ▾ Queries
    ▾ 142.250.77.100: type A, class IN
        Name: 142.250.77.100
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Authoritative nameservers
    ▾ <Root>: type SOA, class IN, mname a.root-servers.net
        Name: <Root>
        Type: SOA (6) (Start Of a zone of Authority)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 64
        Primary name server: a.root-servers.net
        Responsible authority's mailbox: nstld.verisign-grs.com
        Serial Number: 2024090200
        Refresh Interval: 1800 (30 minutes)
        Retry Interval: 900 (15 minutes)
        Expire limit: 604800 (7 days)
        Minimum TTL: 86400 (1 day)
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 8]
    [Time: 0.008255277 seconds]

0000  20 c1 9b 69 1d 6a 8a 1e  5a 78 f3 64 08 00 45 00    ··i·j·· Zx·d··E·
0010  00 92 54 21 00 00 40 11  ba 07 ac 14 0a 01 ac 14    ··T!··@· ········
```

No.: 9 · Time: 48.300910219 · Source: 172.20.10.1 · Destination: 172.20.10.9 · Protocol: DNS · Length: 160 · Info: Standard query response 0xfc6d No such name A 142.250.77.100 SOA a.root-servers.net OPT

☑ Show packet bytes

Help
Close
am@linux:~
Screenshots
*wlp0s20f3
CN-Activity-01 (Aniruddha...
sfafs - Google Search - Brave
Settings
Wireshark · Packet 9 · wlp...