Part a.

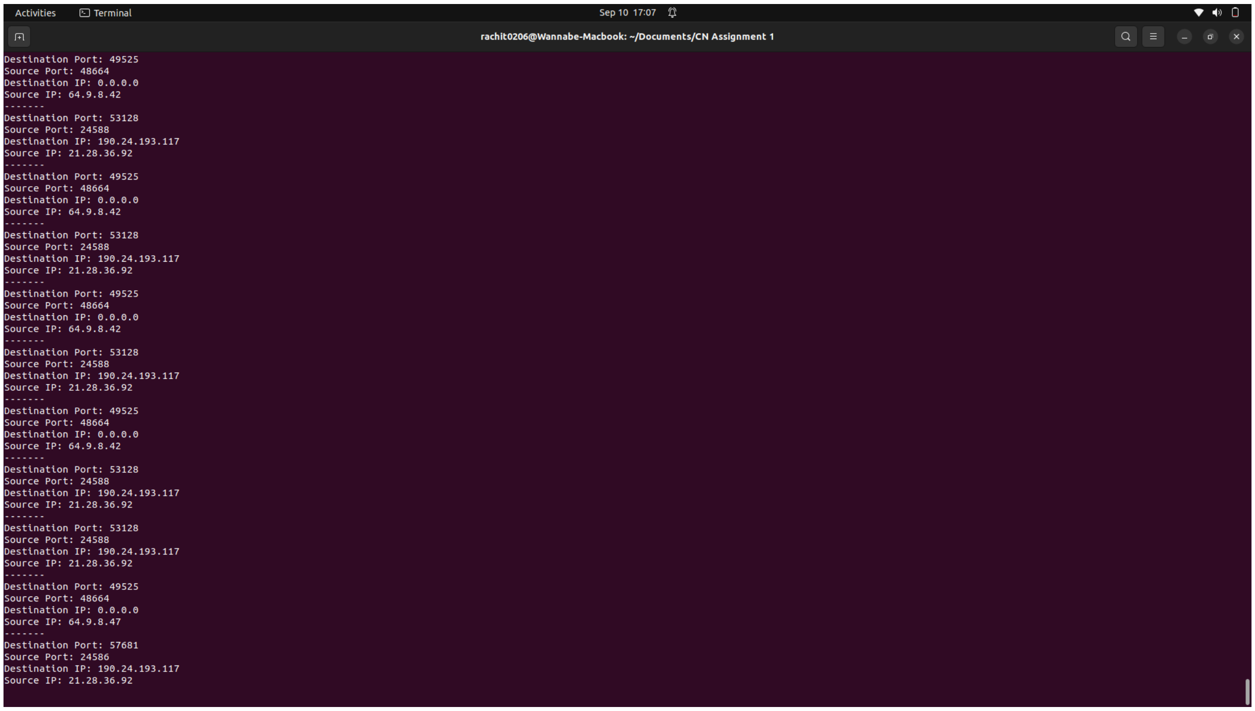
Steps to execute the program:

Step 1: Compile the packet_sniffer.c program.
Command: `gcc packet_sniffer.c -o <output file name>`
`[Generic] gcc <path to packet_sniffer.c> -o <output file name>`

Step 2: Run the compiled executable file. Make sure that you are in the directory where the executable file is present.
Command: `sudo ./<output file name>`

Note: Sudo is very important as we are opening a raw socket which requires super user permissions.

Step 3: To exit the program use (Ctrl + C).



```
Destination Port: 49525
Source Port: 48664
Destination IP: 0.0.0.0
Source IP: 64.9.8.42
-------
Destination Port: 53128
Source Port: 24588
Destination IP: 190.24.193.117
Source IP: 21.28.36.92
-------
Destination Port: 49525
Source Port: 48664
Destination IP: 0.0.0.0
Source IP: 64.9.8.42
-------
Destination Port: 53128
Source Port: 24588
Destination IP: 190.24.193.117
Source IP: 21.28.36.92
-------
Destination Port: 49525
Source Port: 48664
Destination IP: 0.0.0.0
Source IP: 64.9.8.42
-------
Destination Port: 53128
Source Port: 24588
Destination IP: 190.24.193.117
Source IP: 21.28.36.92
-------
Destination Port: 49525
Source Port: 48664
Destination IP: 0.0.0.0
Source IP: 64.9.8.42
-------
Destination Port: 53128
Source Port: 24588
Destination IP: 190.24.193.117
Source IP: 21.28.36.92
-------
Destination Port: 53128
Source Port: 24588
Destination IP: 190.24.193.117
Source IP: 21.28.36.92
-------
Destination Port: 49525
Source Port: 48664
Destination IP: 0.0.0.0
Source IP: 64.9.8.47
-------
Destination Port: 57681
Source Port: 24586
Destination IP: 190.24.193.117
Source IP: 21.28.36.92
```

Explanation:

We use the socket call to open a socket: 'socket(AF_PACKET, SOCK_RAW, htons(ETH_P_ALL))' and the arguments are used so as to sniff all the packets passing through. The htons() function converts the unsigned short integer hostshort from host byte order to network byte order. Once the socket is created we use the recvfrom function to receive the packet data passing through the socket and temporarily store it in an unsigned char buffer. Now, we use two different functions, one to process the IP addresses present in the IP Headers and another to retrieve the ports information from TCP Headers. We know that the packets contain a variety of headers as they pass through different layers in the network stack. Hence, the packet will initially contain the ethernet headers which are of 14 bytes and we type cast the buffer data(with an offset of 14 bytes: buffer + 14) to struct ip and using this we can extract all the information contained in the IP Headers. Similarly, we type cast the buffer data(with an offset of 14 bytes(ethernet header) + size of ip(IP header)) to struct tcphdr and using this we can extract the ports data.

Part b.

PCAP file used : 2.pcap

Steps of execution

Step 1: Compile the packet_sniffer.c program.
Command: `gcc countflow.cpp -o <output file name> -lstdc++`

Step 2: Run the compiled executable file. Make sure that you are in the directory where the executable file is present.
Command: `sudo ./<output file name>`

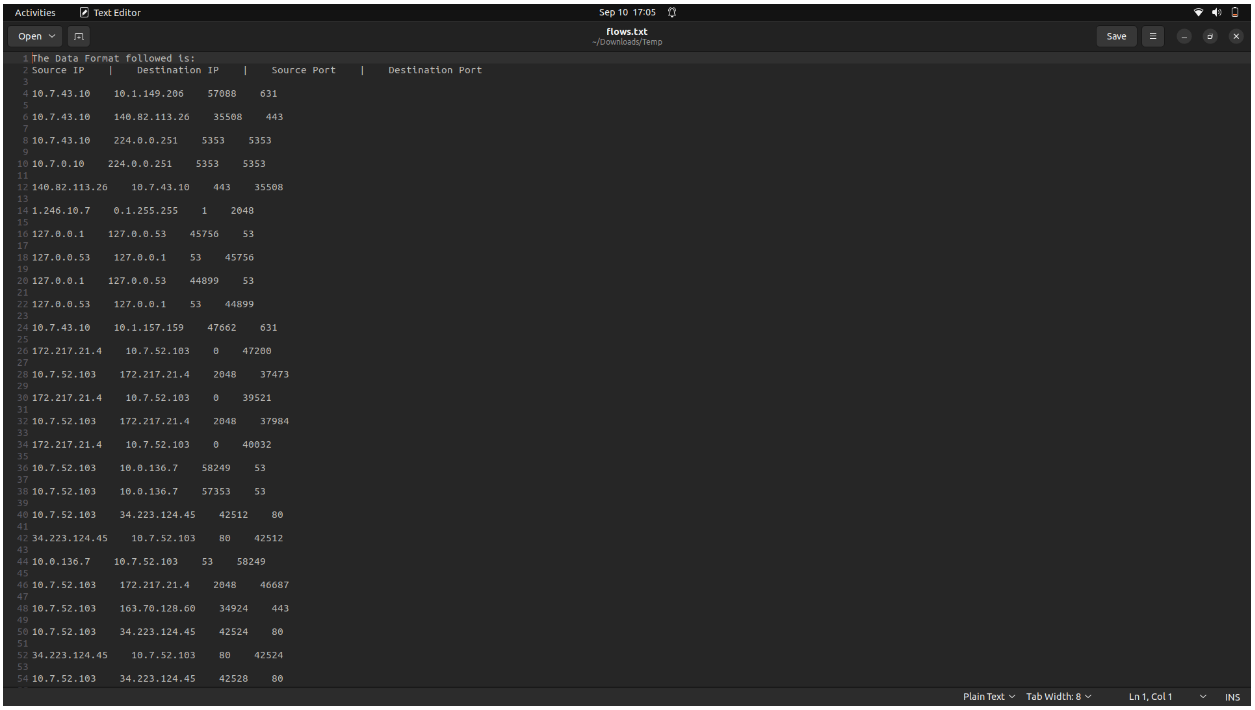
Step 3: Open another terminal instance, and use tcp replay to replay the provided pcap file and extract its information in the running packet sniffer program. Command: `sudo tcpreplay -i lo --mbps=2 <path to pcap file>`

Step 4: Once the tcpreplay program is done, exit the main program using Ctrl + C.

Step 5: Open the flows.txt file generated to view the data

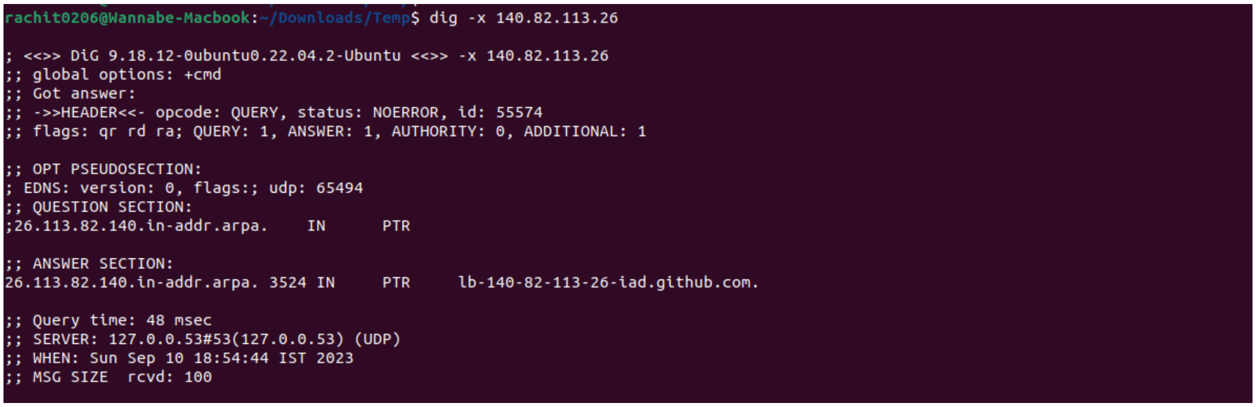
The b. part involves extracting certain information from the packets. More specifically, we record the total number flows and store all of them in a text file. To do this, we manipulate the extracted data to make a tuple as indicated in the program. We make a map of all the tuples and add each tuple to the tuple as and when we encounter it the first time. When the same happens, we also write the tuple into a separate text document for further analysis. We wrote the code for this portion in C++, to utilize the map data structure available in the STL library.

Note: Owing to the loopback lo interface, the program records some excess flows which are not part of the pcap file.

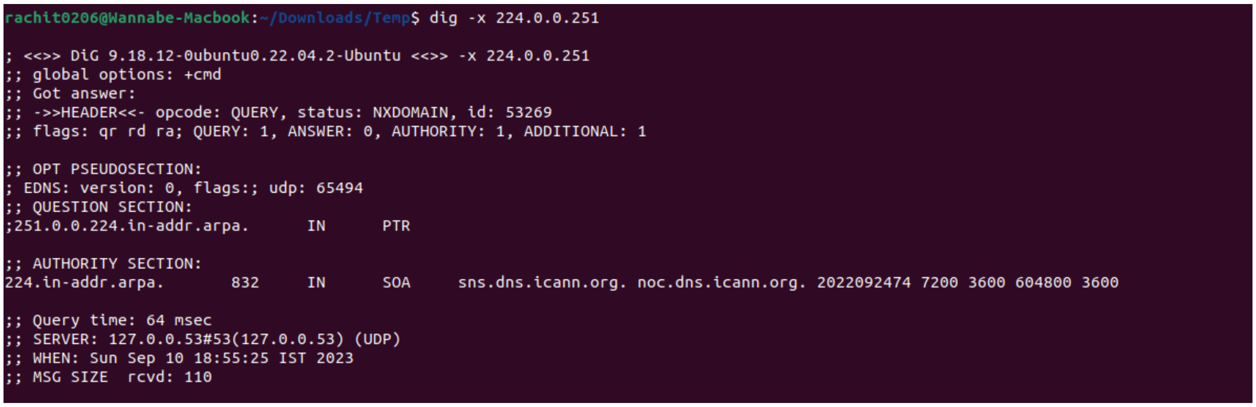


```
The Data Format followed is:
Source IP    |    Destination IP    |    Source Port    |    Destination Port

10.7.43.10    10.1.149.206    57088    631

10.7.43.10    140.82.113.26    35508    443

10.7.43.10    224.0.0.251    5353    5353

10.7.0.10    224.0.0.251    5353    5353

140.82.113.26    10.7.43.10    443    35508

1.246.10.7    0.1.255.255    1    2048

127.0.0.1    127.0.0.53    45756    53

127.0.0.53    127.0.0.1    53    45756

127.0.0.1    127.0.0.53    44899    53

127.0.0.53    127.0.0.1    53    44899

10.7.43.10    10.1.157.159    47662    631

172.217.21.4    10.7.52.103    0    47200

10.7.52.103    172.217.21.4    2048    37473

172.217.21.4    10.7.52.103    0    39521

10.7.52.103    172.217.21.4    2048    37984

172.217.21.4    10.7.52.103    0    40032

10.7.52.103    10.0.136.7    58249    53

10.7.52.103    10.0.136.7    57353    53

10.7.52.103    34.223.124.45    42512    80

34.223.124.45    10.7.52.103    80    42512

10.0.136.7    10.7.52.103    53    58249

10.7.52.103    172.217.21.4    2048    46687

10.7.52.103    163.70.128.60    34924    443

10.7.52.103    34.223.124.45    42524    80

34.223.124.45    10.7.52.103    80    42524

10.7.52.103    34.223.124.45    42528    80
```

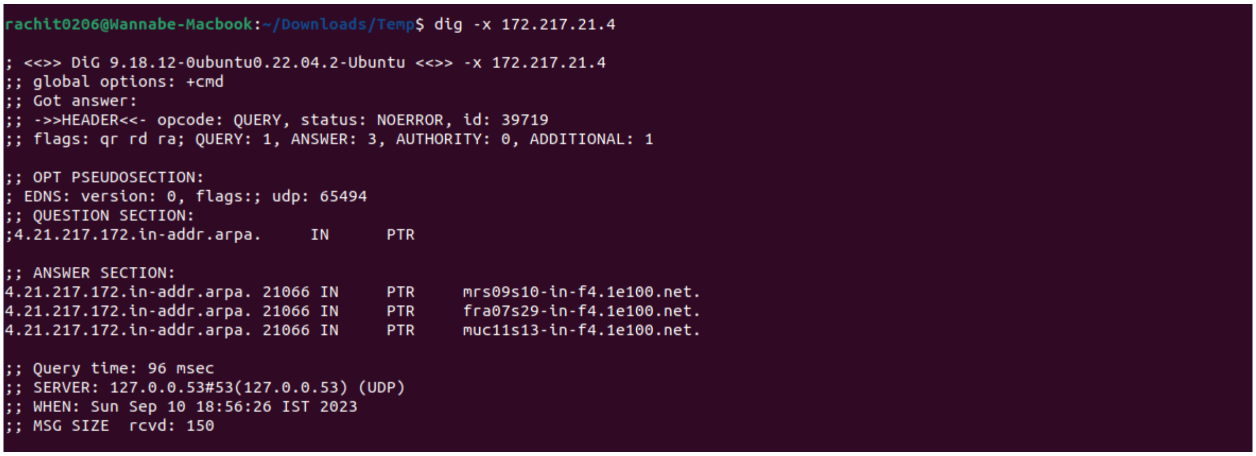
Reverse DNS lookups



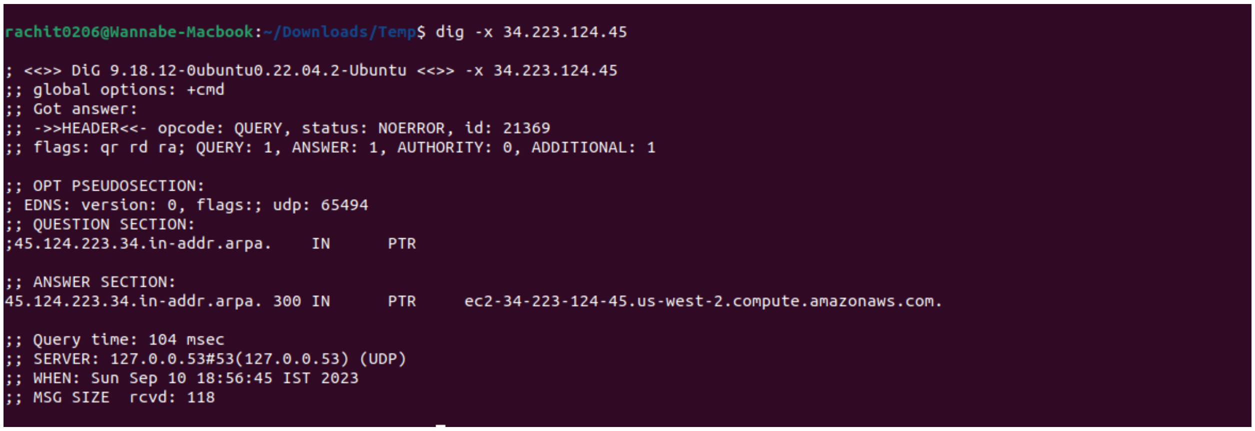
```
rachit0206@Wannabe-Macbook:~/Downloads/Temp$ dig -x 140.82.113.26

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> -x 140.82.113.26
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55574
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;26.113.82.140.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
26.113.82.140.in-addr.arpa. 3524 IN     PTR     lb-140-82-113-26-iad.github.com.

;; Query time: 48 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 18:54:44 IST 2023
;; MSG SIZE  rcvd: 100
```



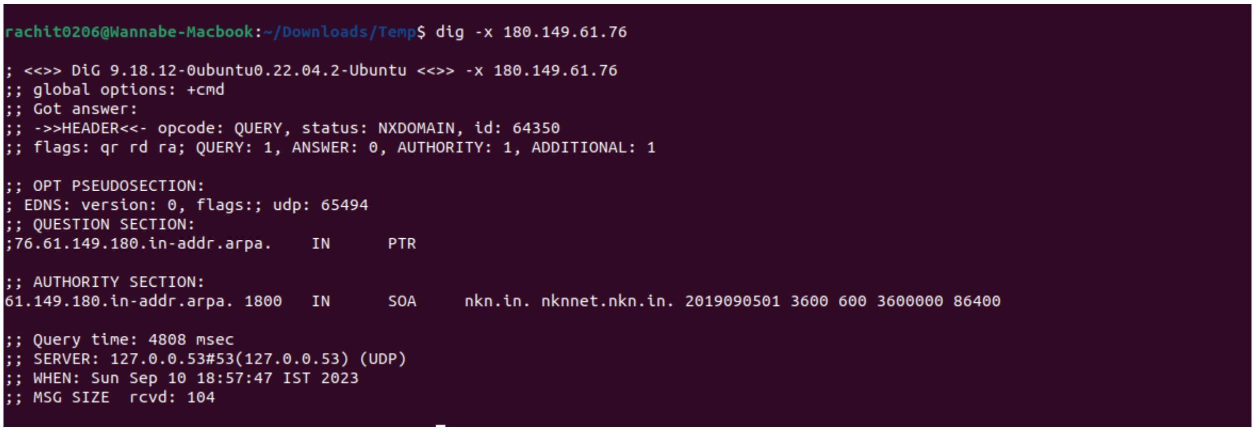
```
rachit0206@Wannabe-Macbook:~/Downloads/Temp$ dig -x 224.0.0.251

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> -x 224.0.0.251
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 53269
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;251.0.0.224.in-addr.arpa.      IN      PTR

;; AUTHORITY SECTION:
224.in-addr.arpa.       832     IN      SOA     sns.dns.icann.org. noc.dns.icann.org. 2022092474 7200 3600 604800 3600

;; Query time: 64 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 18:55:25 IST 2023
;; MSG SIZE  rcvd: 110
```



```
rachit0206@Wannabe-Macbook:~/Downloads/Temp$ dig -x 172.217.21.4

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> -x 172.217.21.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39719
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;4.21.217.172.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
4.21.217.172.in-addr.arpa. 21066 IN     PTR     mrs09s10-in-f4.1e100.net.
4.21.217.172.in-addr.arpa. 21066 IN     PTR     fra07s29-in-f4.1e100.net.
4.21.217.172.in-addr.arpa. 21066 IN     PTR     muc11s13-in-f4.1e100.net.

;; Query time: 96 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 18:56:26 IST 2023
;; MSG SIZE  rcvd: 150
```



```
rachit0206@Wannabe-Macbook:~/Downloads/Temp$ dig -x 34.223.124.45

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> -x 34.223.124.45
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21369
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;45.124.223.34.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
45.124.223.34.in-addr.arpa. 300 IN      PTR     ec2-34-223-124-45.us-west-2.compute.amazonaws.com.

;; Query time: 104 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 18:56:45 IST 2023
;; MSG SIZE  rcvd: 118
```



```
rachit0206@Wannabe-Macbook:~/Downloads/Temp$ dig -x 180.149.61.76

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> -x 180.149.61.76
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64350
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;76.61.149.180.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
61.149.180.in-addr.arpa. 1800   IN      SOA     nkn.in. nknnet.nkn.in. 2019090501 3600 600 3600000 86400

;; Query time: 4808 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 18:57:47 IST 2023
;; MSG SIZE  rcvd: 104
```