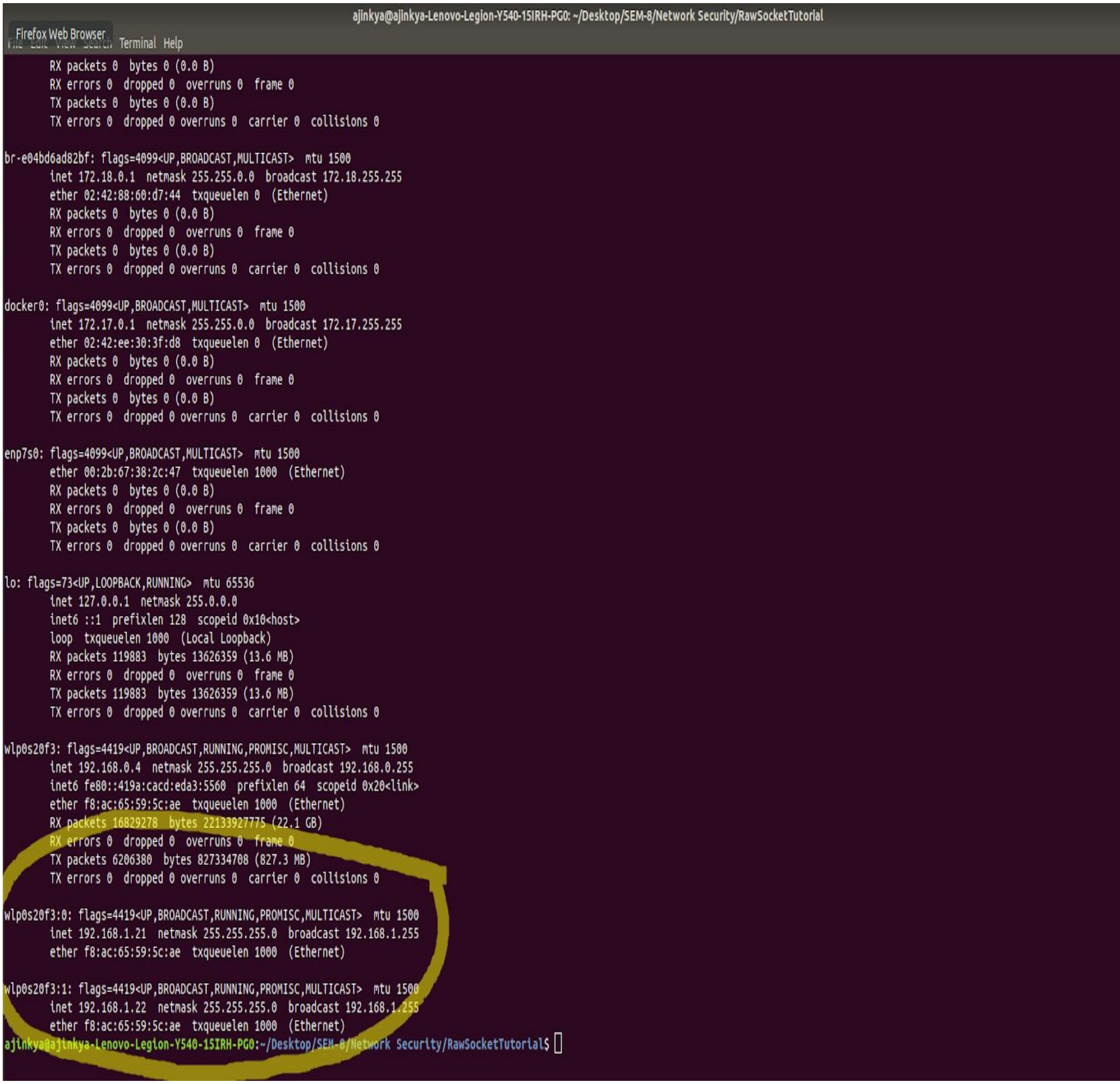
Ajinkya Bokade - CS17BTECH11001
Network Security Assignment
DNS with Raw Socket

Two virtual network interfaces are created using command
sudo ifconfig wlp0s20f3:0 192.168.1.21 up
sudo ifconfig wlp0s20f3:1 192.168.1.22 up

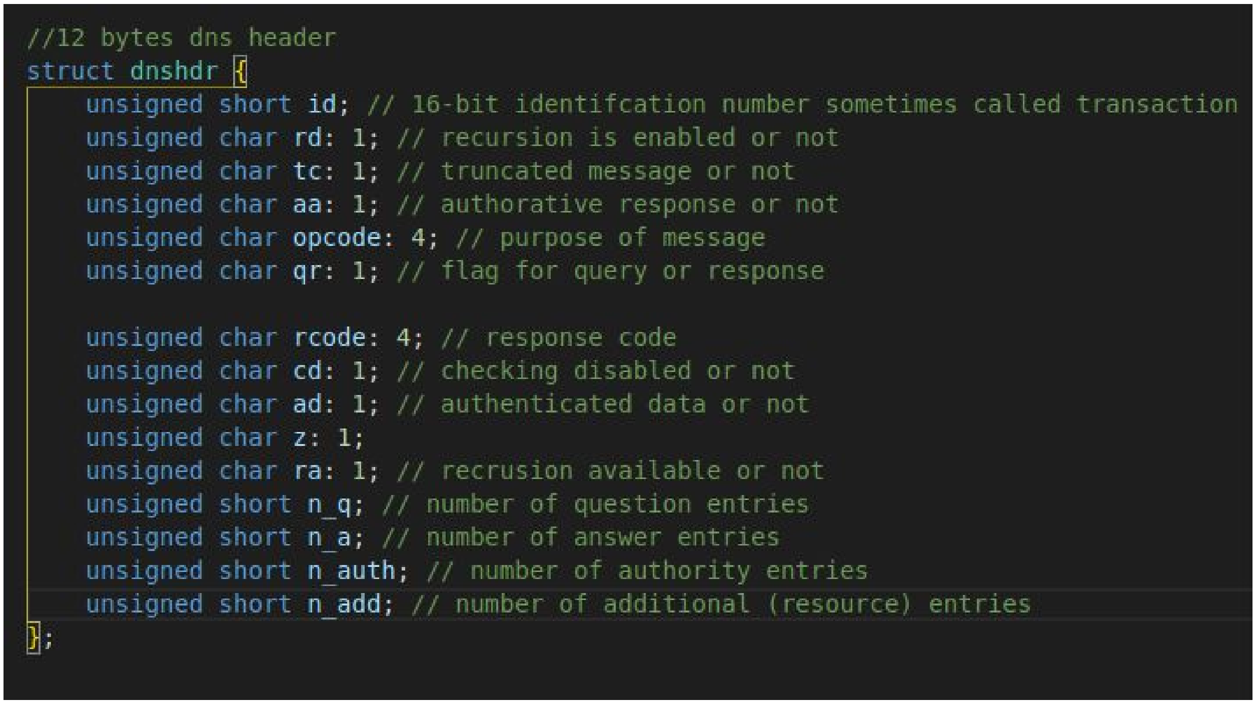


ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0: ~/Desktop/SEM-8/Network Security/RawSocketTutorial
Firefox Web Browser
File Edit View Search Terminal Help

```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-e04bd6ad82bf: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:88:60:d7:44  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ee:30:3f:d8  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp7s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:2b:67:38:2c:47  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 119883  bytes 13626359 (13.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 119883  bytes 13626359 (13.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.0.4  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::419a:cacd:eda3:5560  prefixlen 64  scopeid 0x20<link>
        ether f8:ac:65:59:5c:ae  txqueuelen 1000  (Ethernet)
        RX packets 16829278  bytes 22133927775 (22.1 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6206380  bytes 827334708 (827.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3:0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.1.21  netmask 255.255.255.0  broadcast 192.168.1.255
        ether f8:ac:65:59:5c:ae  txqueuelen 1000  (Ethernet)

wlp0s20f3:1: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.1.22  netmask 255.255.255.0  broadcast 192.168.1.255
        ether f8:ac:65:59:5c:ae  txqueuelen 1000  (Ethernet)
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$
```

Task 1 - DNS Packet Parser

DNS header comes after the UDP header in the packet.
DNS header struct is defined in “print.h”



```
//12 bytes dns header
struct dnshdr {
    unsigned short id; // 16-bit identifcation number sometimes called transaction
    unsigned char rd: 1; // recursion is enabled or not
    unsigned char tc: 1; // truncated message or not
    unsigned char aa: 1; // authorative response or not
    unsigned char opcode: 4; // purpose of message
    unsigned char qr: 1; // flag for query or response

    unsigned char rcode: 4; // response code
    unsigned char cd: 1; // checking disabled or not
    unsigned char ad: 1; // authenticated data or not
    unsigned char z: 1;
    unsigned char ra: 1; // recrusion available or not
    unsigned short n_q; // number of question entries
    unsigned short n_a; // number of answer entries
    unsigned short n_auth; // number of authority entries
    unsigned short n_add; // number of additional (resource) entries
};
```

,

Then in AnalyzeUdp function in ‘analyze.c’ , extra code is written to extract different fields in the DNS header and the dns record type is also extracted.
Since DNS header comes after the udp header, thus pointer is skipped till end of udp header to start extracting dns header fields. Then the pointer is typecasted to the DNS header and then all different fields of the DNS header defined above in the image are printed. Then for printing hostname of DNS query, it is first converted to normal string form from DNS format. Since in DNS query hostname “rawsocket.tut” is formatted as “9rawsocket3tut”. Thus code for the same is written and hostname is extracted and printed. Then the type of DNS query is printed.

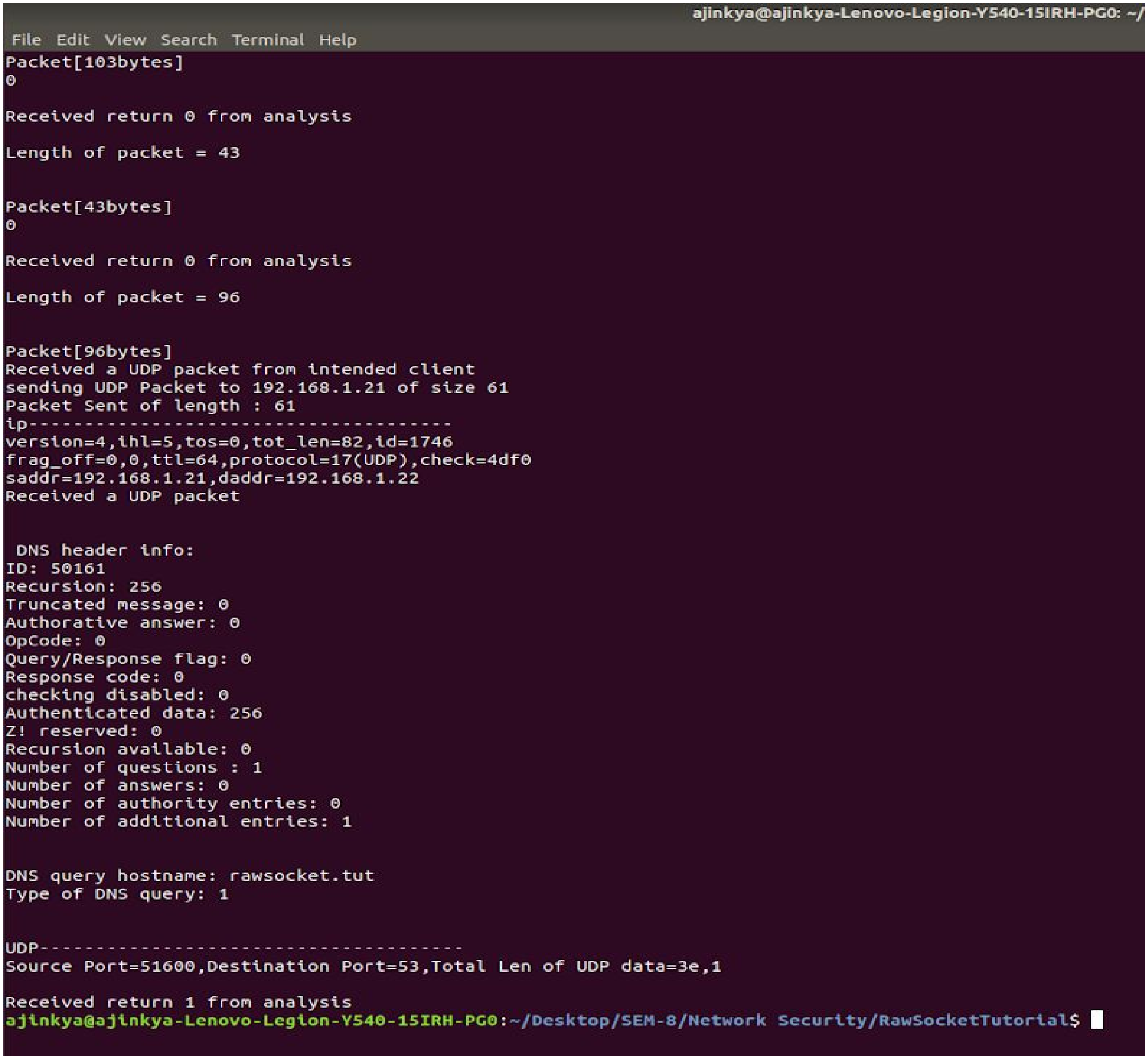
Two terminals were opened.
On first terminal, following commands were run:
sudo make
sudo ./rawSocket wlp0s20f3:0

On the second terminal, DNS query was sent using the dig command. Following command was run:

dig @192.168.1.22 rawsocket.tut

For convenience to view the dns output in the first terminal (since other packets details are also printed), whenever first udp packet is obtained, non zero value is returned in AnalyzeIp function in analyze.c and if non zero value is returned from the function AnalyzePacket in rawSocket.c, loop is broken and it stops.

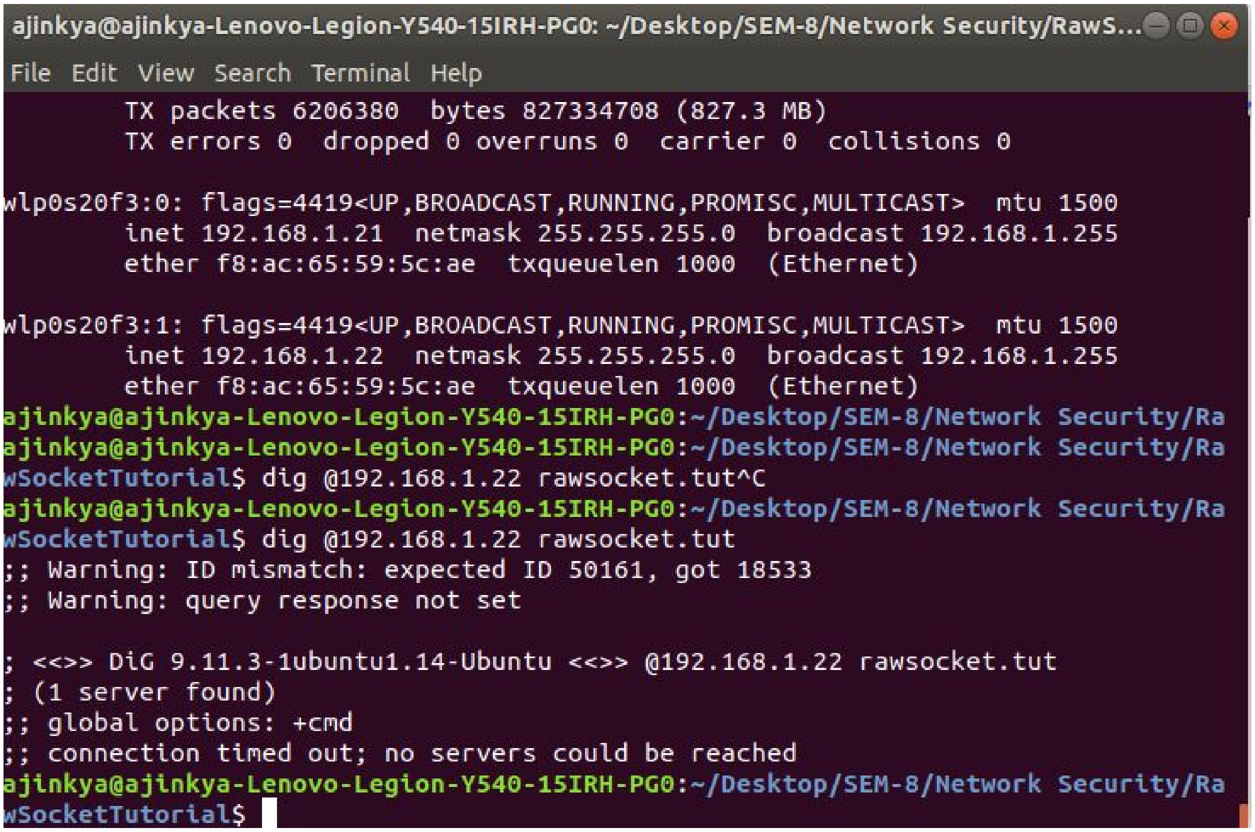
Results: -
First terminal screenshot


ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0: ~/
File Edit View Search Terminal Help

```
Packet[103bytes]
0

Received return 0 from analysis

Length of packet = 43


Packet[43bytes]
0

Received return 0 from analysis

Length of packet = 96


Packet[96bytes]
Received a UDP packet from intended client
sending UDP Packet to 192.168.1.21 of size 61
Packet Sent of length : 61
ip-------------------------------------
version=4,ihl=5,tos=0,tot_len=82,id=1746
frag_off=0,0,ttl=64,protocol=17(UDP),check=4df0
saddr=192.168.1.21,daddr=192.168.1.22
Received a UDP packet


 DNS header info:
ID: 50161
Recursion: 256
Truncated message: 0
Authorative answer: 0
OpCode: 0
Query/Response flag: 0
Response code: 0
checking disabled: 0
Authenticated data: 256
Z! reserved: 0
Recursion available: 0
Number of questions : 1
Number of answers: 0
Number of authority entries: 0
Number of additional entries: 1


DNS query hostname: rawsocket.tut
Type of DNS query: 1


UDP--------------------------------------
Source Port=51600,Destination Port=53,Total Len of UDP data=3e,1

Received return 1 from analysis
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$
```

ID is 50161
Number of questions are 1 since only one question was sent, DNS query hostname is “rawsocket.tut”, type of dns query is 1 (“A”)

Second terminal screenshot

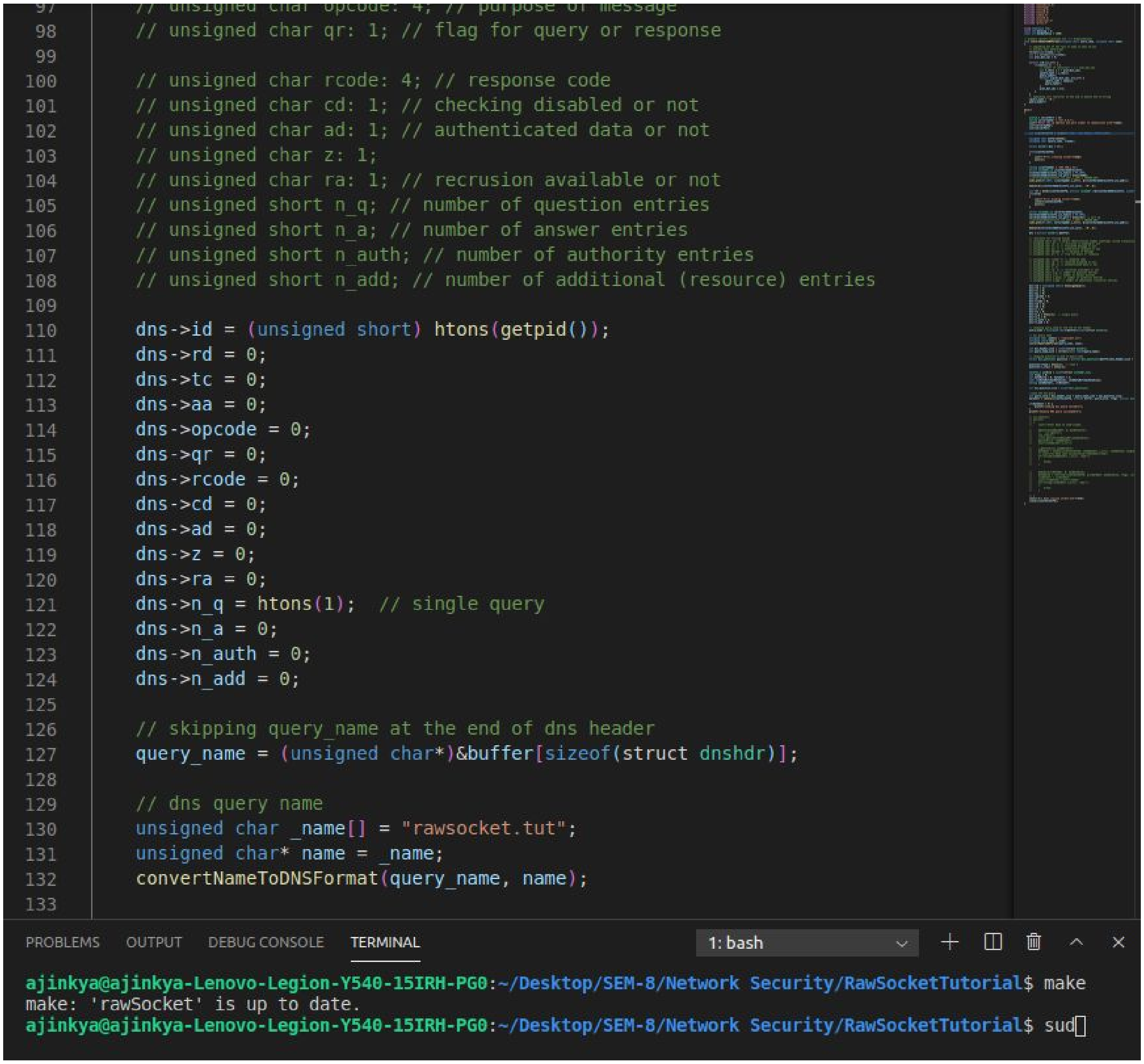


ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0: ~/Desktop/SEM-8/Network Security/RawS...
File Edit View Search Terminal Help

```
        TX packets 6206380  bytes 827334708 (827.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3:0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.1.21  netmask 255.255.255.0  broadcast 192.168.1.255
        ether f8:ac:65:59:5c:ae  txqueuelen 1000  (Ethernet)

wlp0s20f3:1: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.1.22  netmask 255.255.255.0  broadcast 192.168.1.255
        ether f8:ac:65:59:5c:ae  txqueuelen 1000  (Ethernet)
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/Ra
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/Ra
wSocketTutorial$ dig @192.168.1.22 rawsocket.tut^C
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/Ra
wSocketTutorial$ dig @192.168.1.22 rawsocket.tut
;; Warning: ID mismatch: expected ID 50161, got 18533
;; Warning: query response not set

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> @192.168.1.22 rawsocket.tut
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/Ra
wSocketTutorial$ 
```

Task 2 - DNS client with RAW socket

For DNS client, a new file is created dnsClient.cpp similar to udpClient.cpp. The only difference is that default server port is set as 53. DNS header is set with the fields set as below:-



```
    // unsigned char opcode: 4; // purpose of message
    // unsigned char qr: 1; // flag for query or response

    // unsigned char rcode: 4; // response code
    // unsigned char cd: 1; // checking disabled or not
    // unsigned char ad: 1; // authenticated data or not
    // unsigned char z: 1;
    // unsigned char ra: 1; // recrusion available or not
    // unsigned short n_q; // number of question entries
    // unsigned short n_a; // number of answer entries
    // unsigned short n_auth; // number of authority entries
    // unsigned short n_add; // number of additional (resource) entries

    dns->id = (unsigned short) htons(getpid());
    dns->rd = 0;
    dns->tc = 0;
    dns->aa = 0;
    dns->opcode = 0;
    dns->qr = 0;
    dns->rcode = 0;
    dns->cd = 0;
    dns->ad = 0;
    dns->z = 0;
    dns->ra = 0;
    dns->n_q = htons(1);  // single query
    dns->n_a = 0;
    dns->n_auth = 0;
    dns->n_add = 0;

    // skipping query_name at the end of dns header
    query_name = (unsigned char*)&buffer[sizeof(struct dnshdr)];

    // dns query name
    unsigned char _name[] = "rawsocket.tut";
    unsigned char* name = _name;
    convertNameToDNSFormat(query_name, name);
```

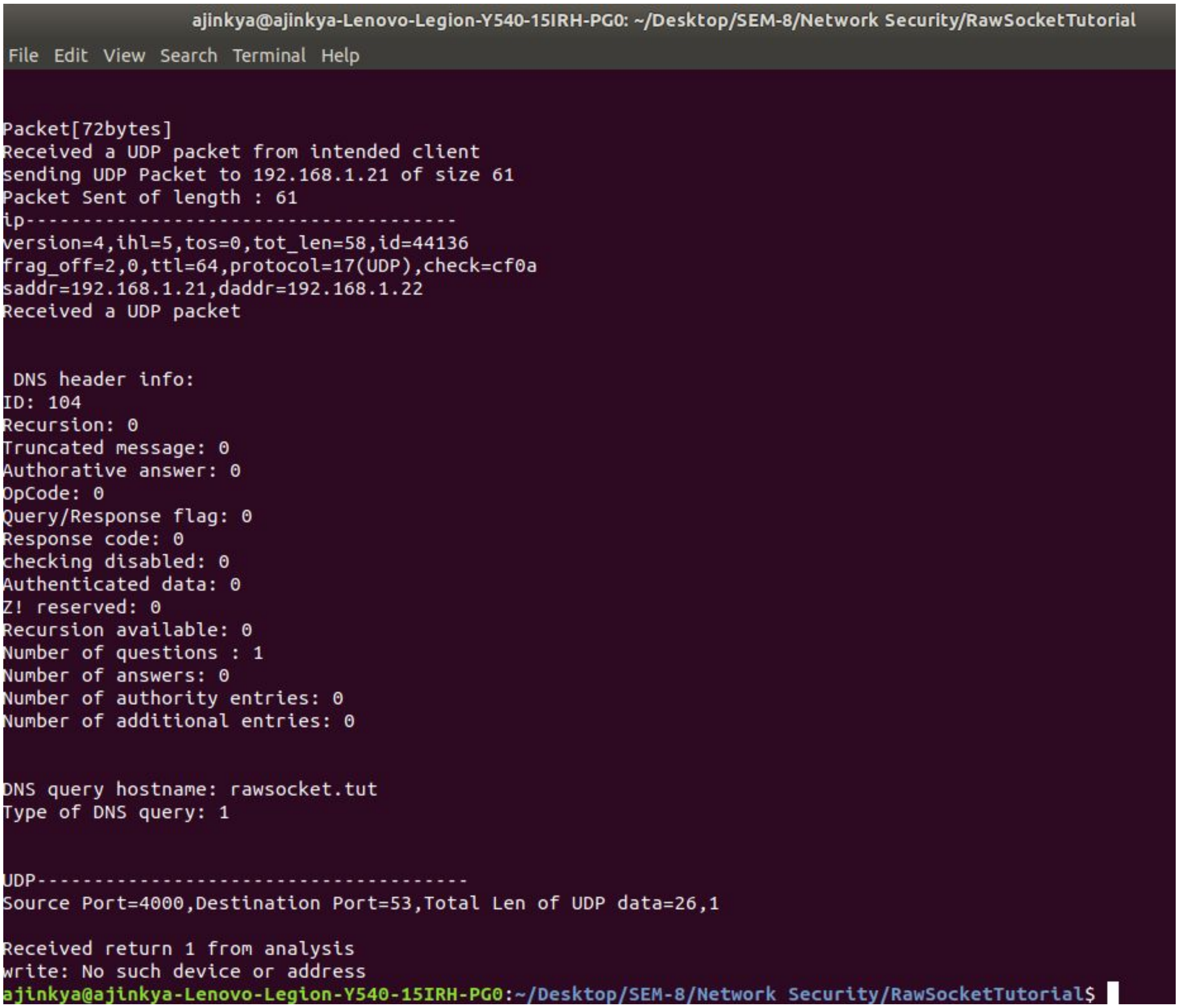
```
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$ make
make: 'rawSocket' is up to date.
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$ sud
```

qr is set to 0 since it is query. n_q is set as 1 since only one question is to be sent. DNS query hostname is set as “rawsocket.tut” (hardcoded but can be changed). Then this hostname is converted to DNS query hostname format “9rawsocket3tut” using function convertNameToDNSFormat.
dns_question struct is defined in “print.h” to store the type and class of DNS query. Type is set as 1 (“A”). The resulting query is sent to the desired IP address.

On first terminal, following commands are run:
sudo make
sudo ./rawSocket wlp0s20f3:0

On second terminal, following commands are run:
g++ dnsClient.cpp -o dnsClient
./dnsClient
Ip address and port is taken as input.

Results:-
First terminal screenshot :-

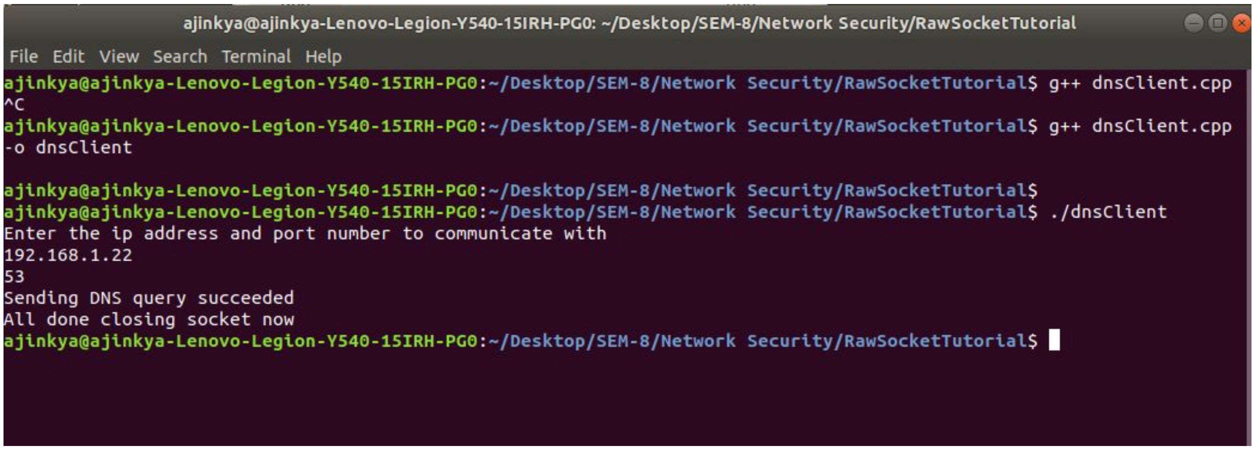


ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0: ~/Desktop/SEM-8/Network Security/RawSocketTutorial
File Edit View Search Terminal Help

```

Packet[72bytes]
Received a UDP packet from intended client
sending UDP Packet to 192.168.1.21 of size 61
Packet Sent of length : 61
ip-------------------------------------
version=4,ihl=5,tos=0,tot_len=58,id=44136
frag_off=2,0,ttl=64,protocol=17(UDP),check=cf0a
saddr=192.168.1.21,daddr=192.168.1.22
Received a UDP packet


 DNS header info:
ID: 104
Recursion: 0
Truncated message: 0
Authorative answer: 0
OpCode: 0
Query/Response flag: 0
Response code: 0
checking disabled: 0
Authenticated data: 0
Z! reserved: 0
Recursion available: 0
Number of questions : 1
Number of answers: 0
Number of authority entries: 0
Number of additional entries: 0


DNS query hostname: rawsocket.tut
Type of DNS query: 1


UDP-------------------------------------
Source Port=4000,Destination Port=53,Total Len of UDP data=26,1

Received return 1 from analysis
write: No such device or address
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$
```

ID is 104 and number of questions is 1, dns query hostname is ‘rawsocket.tut’ and dns query type is 1.

Second terminal screenshot:-



ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0: ~/Desktop/SEM-8/Network Security/RawSocketTutorial
File Edit View Search Terminal Help

```
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$ g++ dnsClient.cpp
^C
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$ g++ dnsClient.cpp
-o dnsClient

ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$ ./dnsClient
Enter the ip address and port number to communicate with
192.168.1.22
53
Sending DNS query succeeded
All done closing socket now
ajinkya@ajinkya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/SEM-8/Network Security/RawSocketTutorial$ █
```