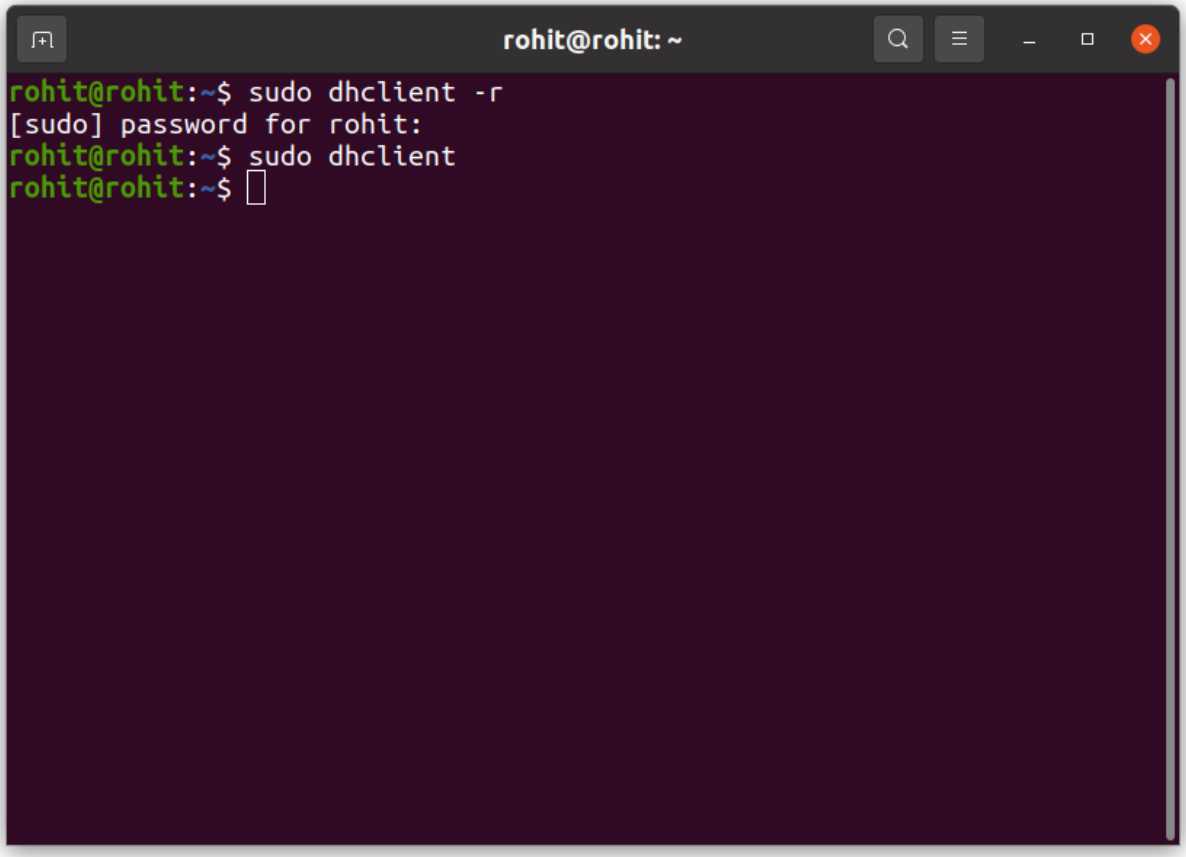
Rohit Garg
2018A7PS0193G

COMPUTER NETWORKS
CS F303

1. Show a round of execution of the DHCP protocol. Show DHCP Request (2 marks), Reply (2 marks), and ACK messages (2 marks) in that round. Find out IP addresses of the DHCP server (2 marks) and client (2 marks). Write the filter and show the output in a screenshot.

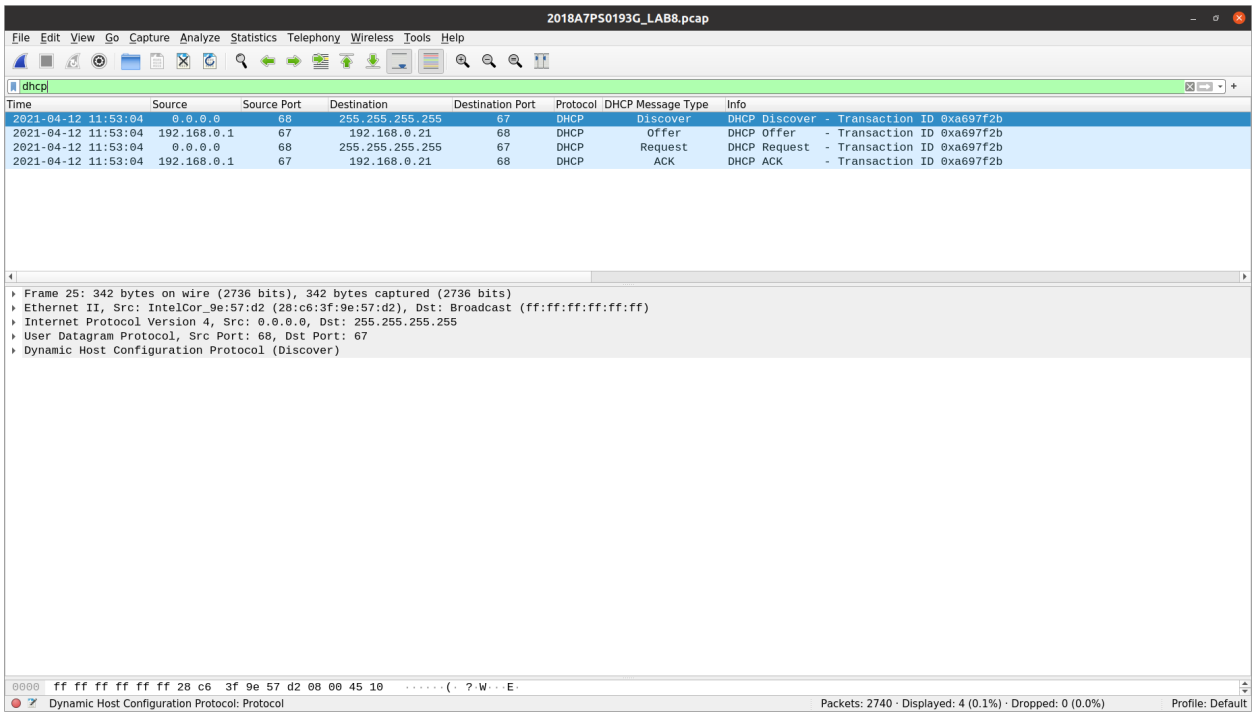
1.

In order to demonstrate the working of DHCP protocol, we instruct the host to obtain a network configuration, including a new IP address using dhclient command. Hence, to get issued a new address, we release the old IP address by typing 'sudo dhclient -r' at the terminal. Now open wireshark to start packet capture at LAN(wlo1 in my case). Now reissue IP address by typing 'sudo dhclient' on terminal to get a new IP address. the IP address gets released and reissued after these commands.

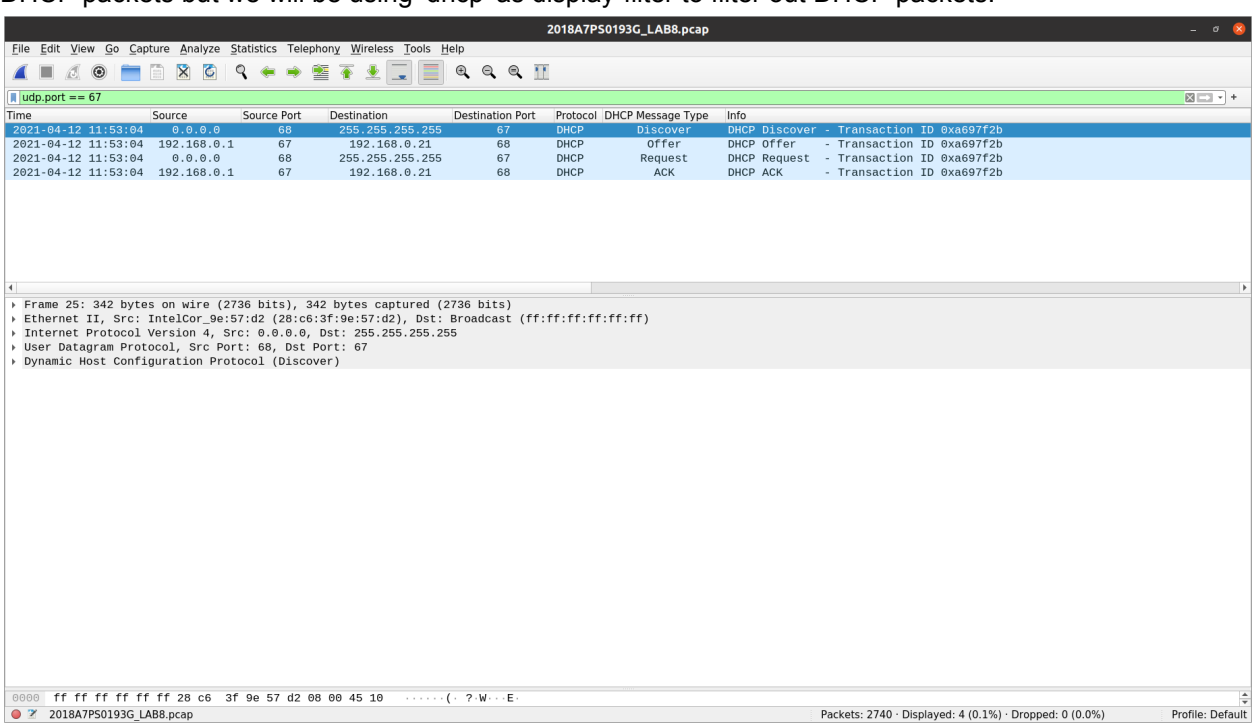


DHCP uses UDP transport layer protocol and uses port numbers 67 and 68.

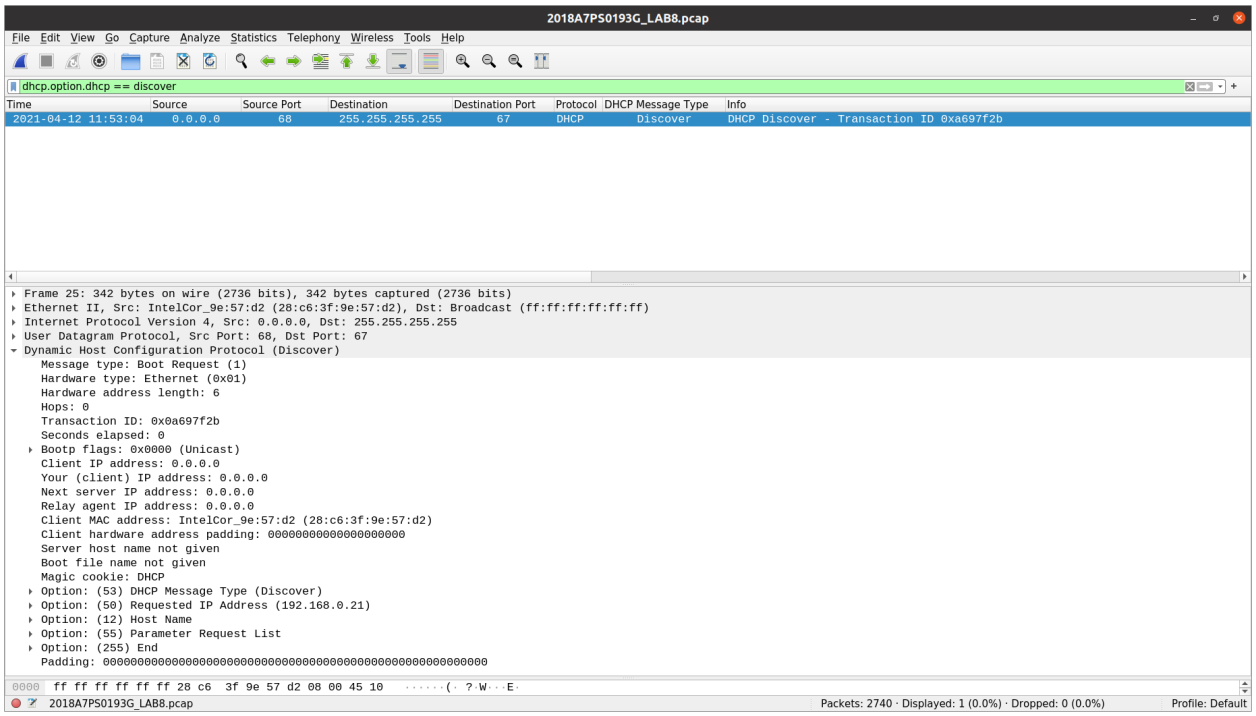
DHCP packets can be filtered out using **dhcp** filter.



Note :Since DHCP server is listening on port 67, we can also use ‘udp.port == 67’ as a filter to filter out DHCP packets but we will be using ‘dhcp’ as display filter to filter out DHCP packets.

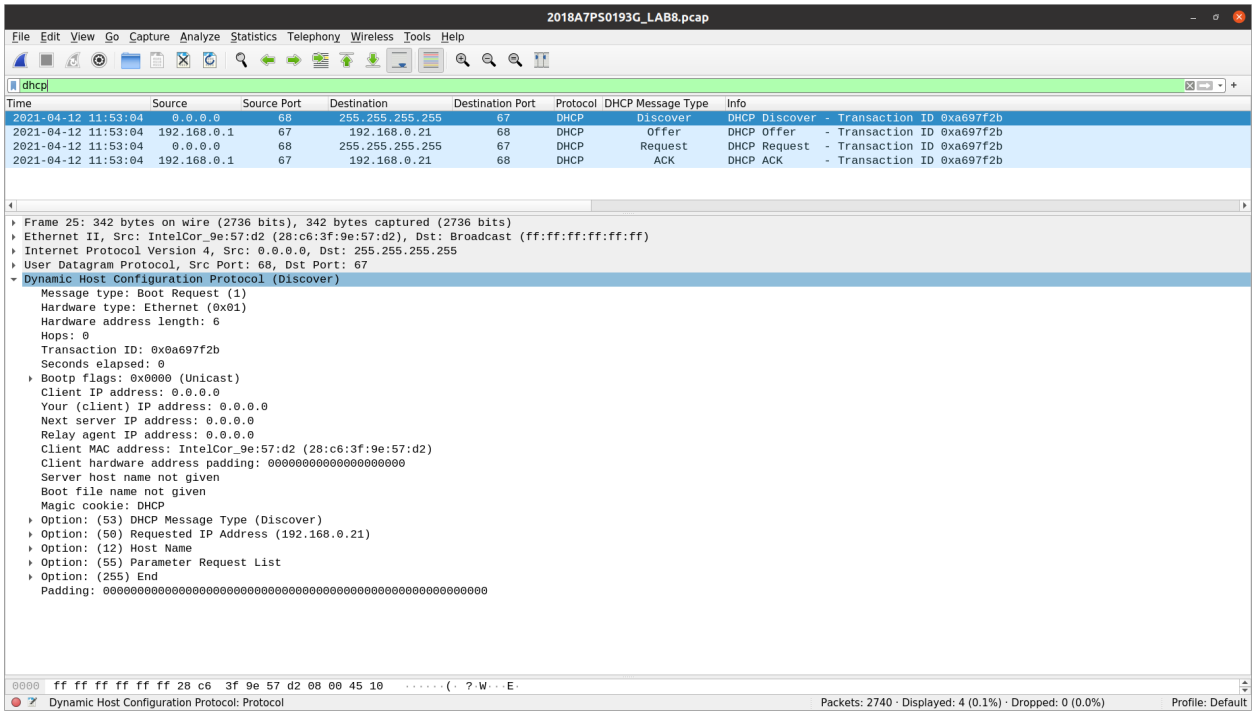


Discover messages can be filtered out using ‘dhcp.option.dhcp == dhcp_message_type’ display filter where message type can be ‘discover’, ‘offer’, ‘request’, ‘ack’. For Example:-



DHCP Discover Packet

DHCP discover is the first request message packet sent by a client to the DHCP server. Client broadcasts a DISCOVER message in order to locate the DHCP server to request for a new IP address.



<u>Ethernet II - Broadcast MAC address = ff:ff::ff:ff</u> -> Since client doesn't have the IP address or the information about the server, hence, it has to broadcast to discover a DHCP server.

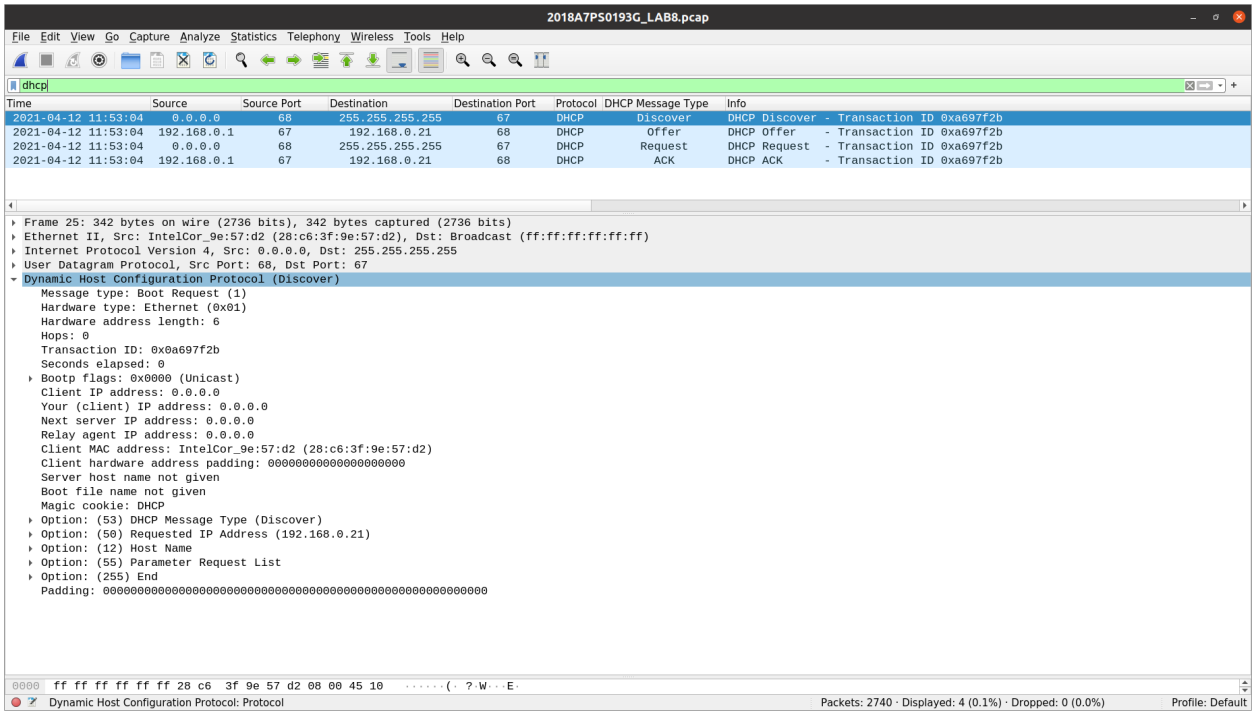
<u>Source IP Address = 0.0.0.0 -></u> Client after sudo dhclient -r command releases its IP address and its IP address is set to 0.0.0.0.

<u>Destination IP Address</u> = 255.255.255.255 -> Broadcast IP Address

<u>DHCP Message Type</u> = Discover (1) since it is a discover message

DHCP Offer

DHCP Offer message is the reply message packet sent by the server to the client.

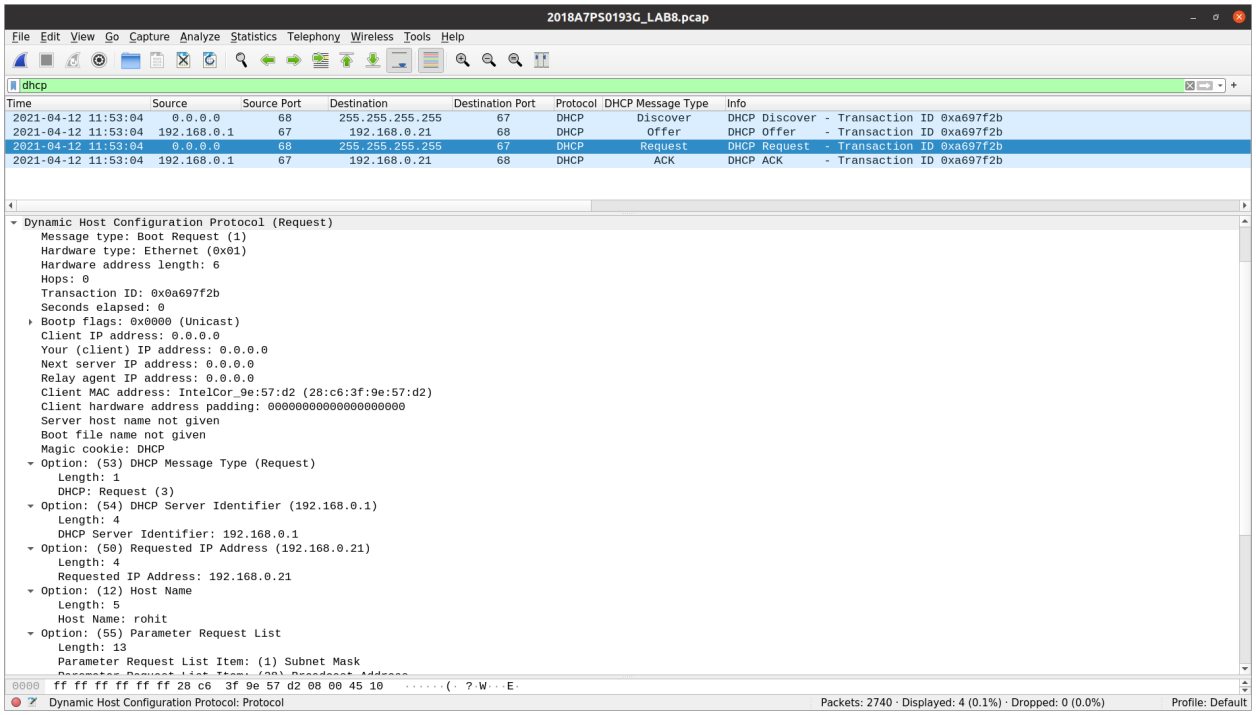


DHCP offer packet contains various details like :

<u>Client IP address:</u> Current IP address of the client

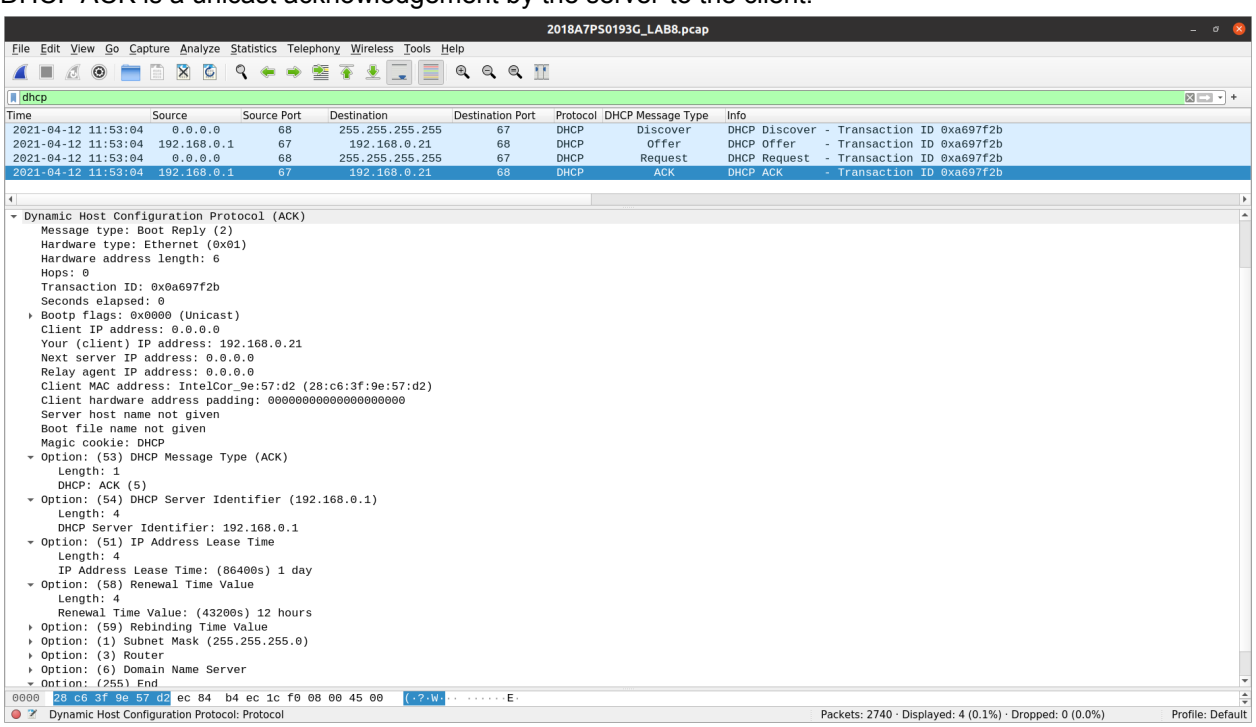
<u>Your IP Address:</u> The ‘offered’ IP address i.e. to be allocated to the client by DHCP server

DHCP Request



DHCP ACK

DHCP ACK is a unicast acknowledgement by the server to the client.

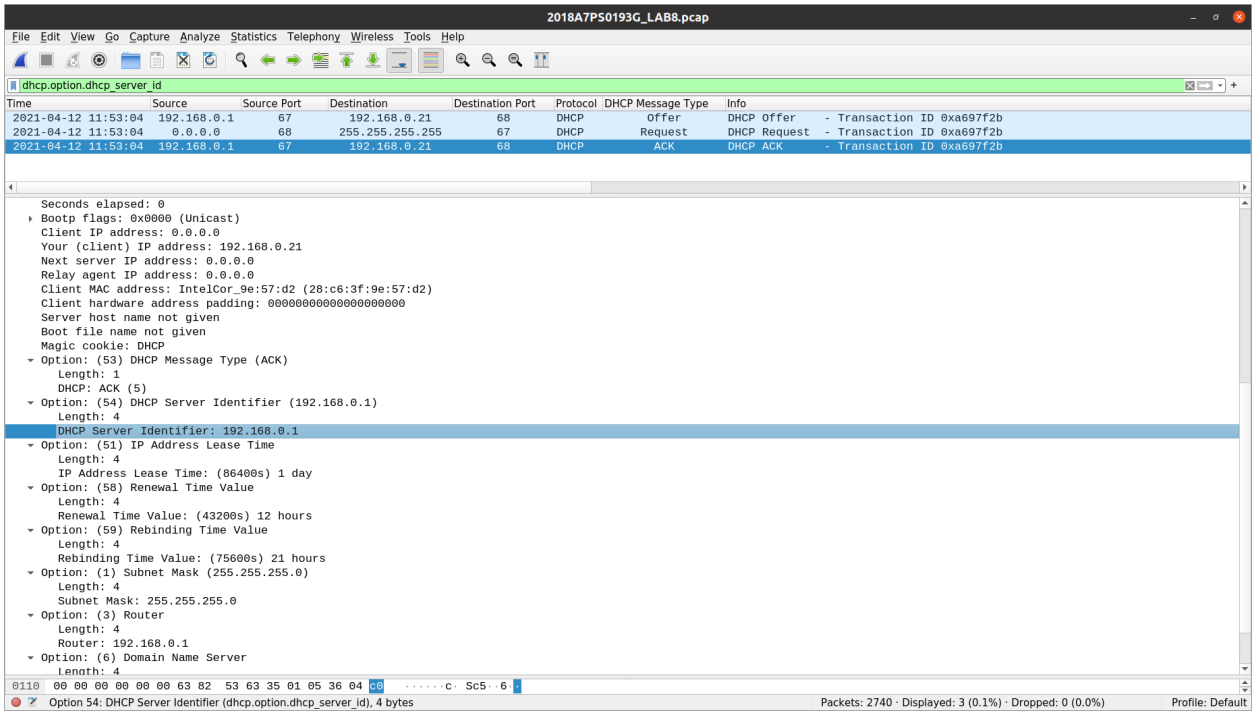


In Packet Details Section, we can see details like, source and destination address. ACK message body also contains other information like IP Address Lease Time, Subnet Mask, Router (Default Gateway), Domain Name Server, and Domain Name,

Finding out Server IP Address

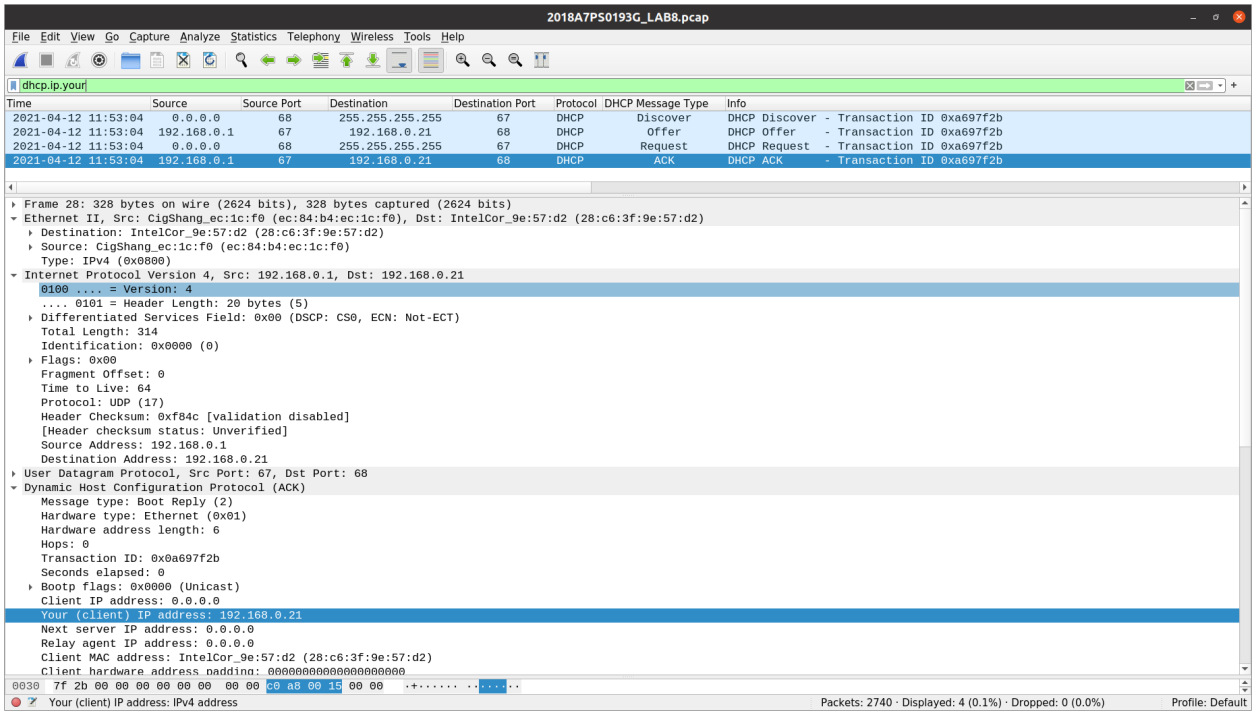
The server IP address of DHCP server can be identified using the server identifier located in the options section of DHCP ACK message. In this case, server IP address is 192.168.0.1

We can also apply it as filter ‘dhcp.option.dhcp_server_id’ to server IP address.



Finding out Client IP Address

The client's IP address can be identified using the Your Client IP under the DHCP ACK section. In this case, client's allocated IP address is 192.168.0.21. We can also apply it as filter 'dhcp.ip.your' to filter out client's IP address.



Note :dhcp.ip.client can also be used to filter out client's allocated IP address .

2. Show a round of execution of the ARP protocol. Show ARP Request (2 marks) and Reply (2 marks) messages in that round. Find the MAC address of the replier (2 marks). Write the filter and show the output in a screenshot.

```
rohit@rohit:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 wlo1
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 wlo1
rohit@rohit:~$ netstat -r -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG        0 0          0 wlo1
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 wlo1
rohit@rohit:~$
```

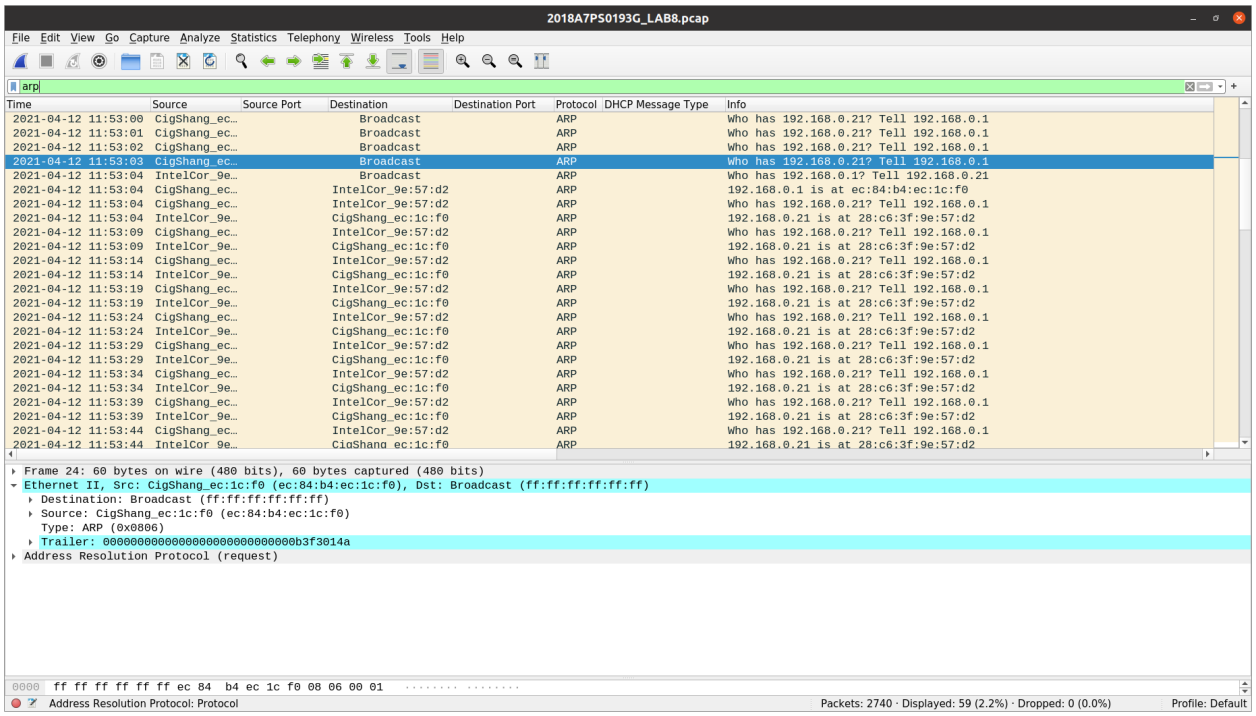
```
rohit@rohit:~$ sudo arp -a
[sudo] password for rohit:
dsldevice.lan (192.168.0.1) at ec:84:b4:ec:1c:f0 [ether] on wlo1
rohit@rohit:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
dsldevice.lan            ether   ec:84:b4:ec:1c:f0   C                     wlo1
Entries: 1      Skipped: 0      Found: 1
rohit@rohit:~$ sudo arp -d dsldevice.lan
rohit@rohit:~$
```

```
rohit@rohit:~$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=7.58 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=8.00 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=4.40 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=2.86 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=4.77 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=4.78 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=3.14 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=3.88 ms
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=4.27 ms
64 bytes from 192.168.0.1: icmp_seq=10 ttl=64 time=4.74 ms
64 bytes from 192.168.0.1: icmp_seq=11 ttl=64 time=4.70 ms
64 bytes from 192.168.0.1: icmp_seq=12 ttl=64 time=6.01 ms
64 bytes from 192.168.0.1: icmp_seq=13 ttl=64 time=5.18 ms
64 bytes from 192.168.0.1: icmp_seq=14 ttl=64 time=16.4 ms
64 bytes from 192.168.0.1: icmp_seq=15 ttl=64 time=5.61 ms
64 bytes from 192.168.0.1: icmp_seq=16 ttl=64 time=3.55 ms
64 bytes from 192.168.0.1: icmp_seq=17 ttl=64 time=3.16 ms
64 bytes from 192.168.0.1: icmp_seq=18 ttl=64 time=3.76 ms
64 bytes from 192.168.0.1: icmp_seq=19 ttl=64 time=4.48 ms
64 bytes from 192.168.0.1: icmp_seq=20 ttl=64 time=35.8 ms
```

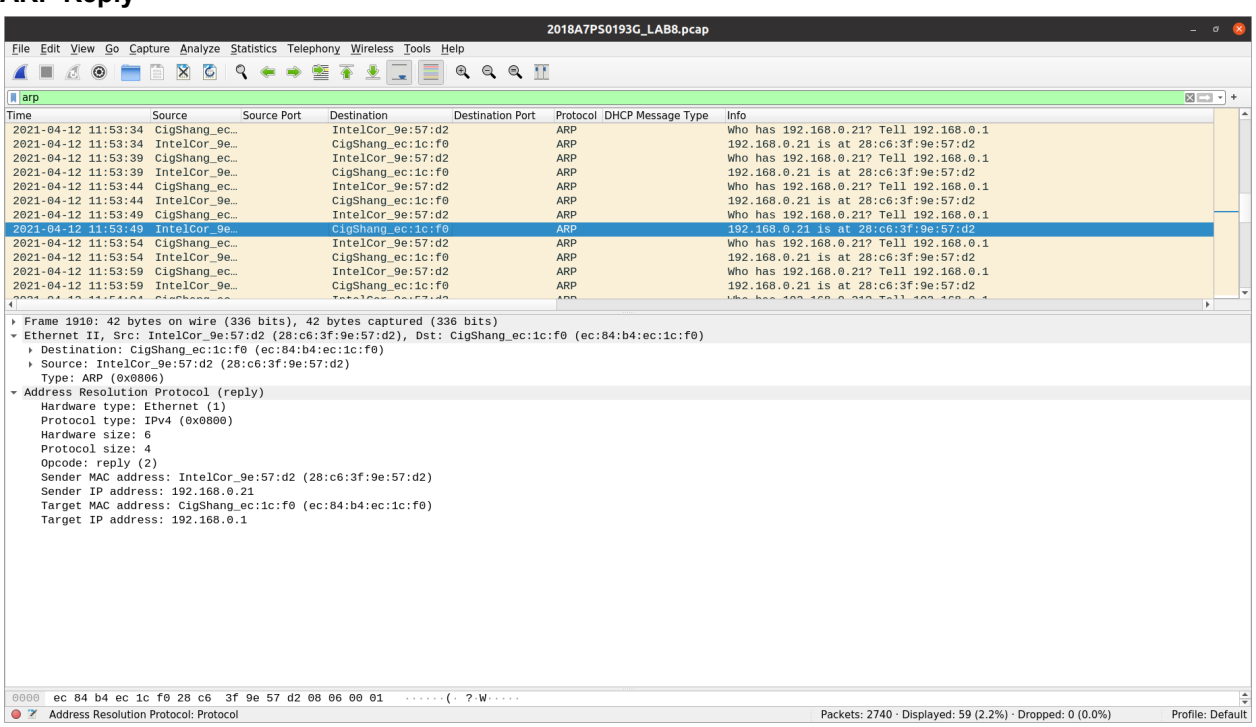
```
^C
--- 192.168.0.1 ping statistics ---
140 packets transmitted, 140 received, 0% packet loss, time 139198ms
rtt min/avg/max/mdev = 1.347/13.337/82.413/15.361 ms
rohit@rohit:~$
```

ARP Request

The need for an ARP request arises when a device wants to know the MAC address of the device to which the source wants to communicate with.

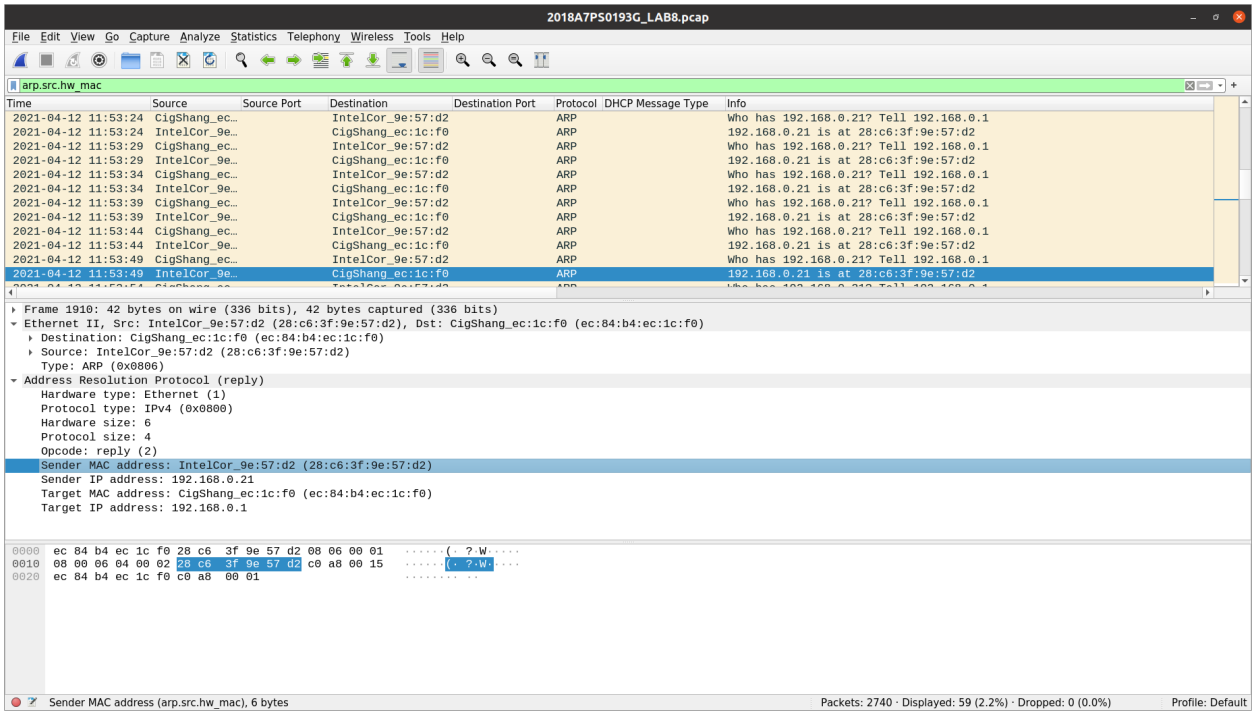


ARP Reply



MAC Address of the replier is the sender's MAC address in ARP Reply section which is **28:c6:3f:9e:57:d2**

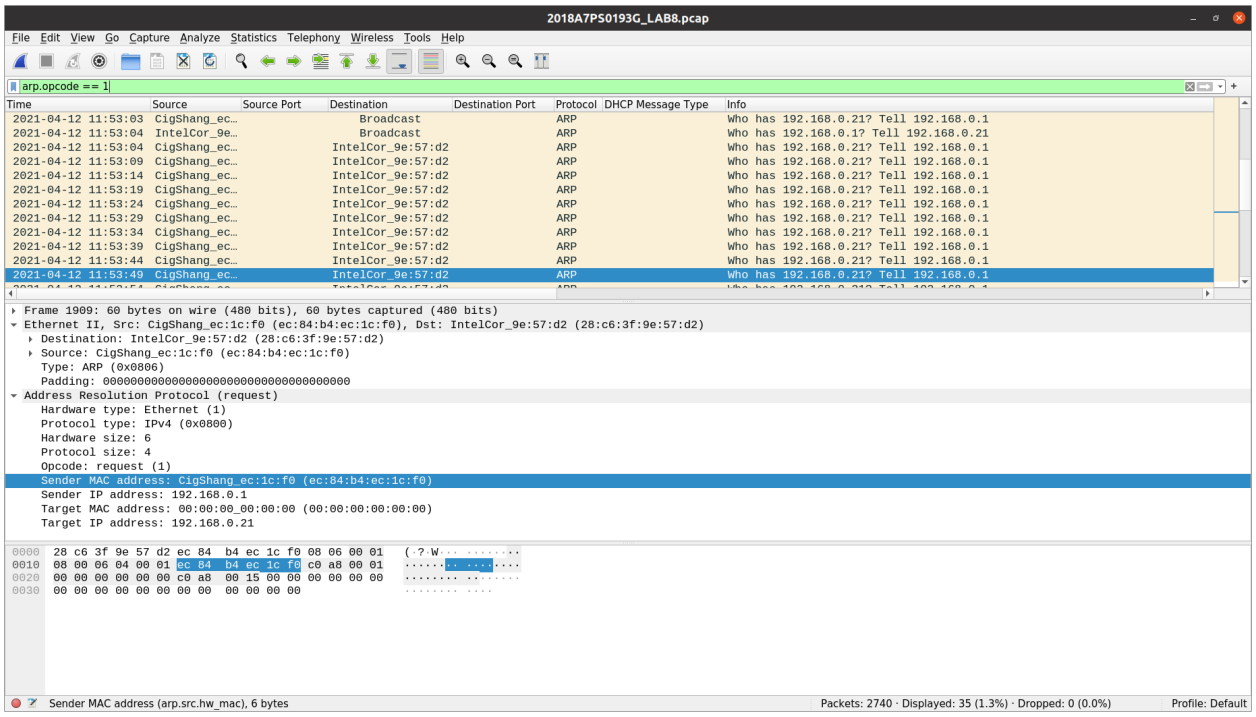
arp.src.hw_mac can be used as a filter to find out replier's mac address.



3. Find the MAC address and the IP address of the Gateway router (2 marks). Write the filter and show the output in a screenshot.

We can find the IP address and MAC address of Gateway router using ARP request packets.
Type arp.opcode == 1 and find out the sender's MAC address and IP address.
In my case,

MAC Address of Gateway Router is = ec:84:b4:ec:1c:f0
Filter for MAC Address of Gateway Router = **arp.src.hw_mac**
IP Address of Gateway Router is = 198.168.0.1
Filter for IP Address of Gateway Router = **arp.src.proto_ipv4**



These values can be verified using finding the router's IP and MAC using the terminal: