Cyber Security Lab

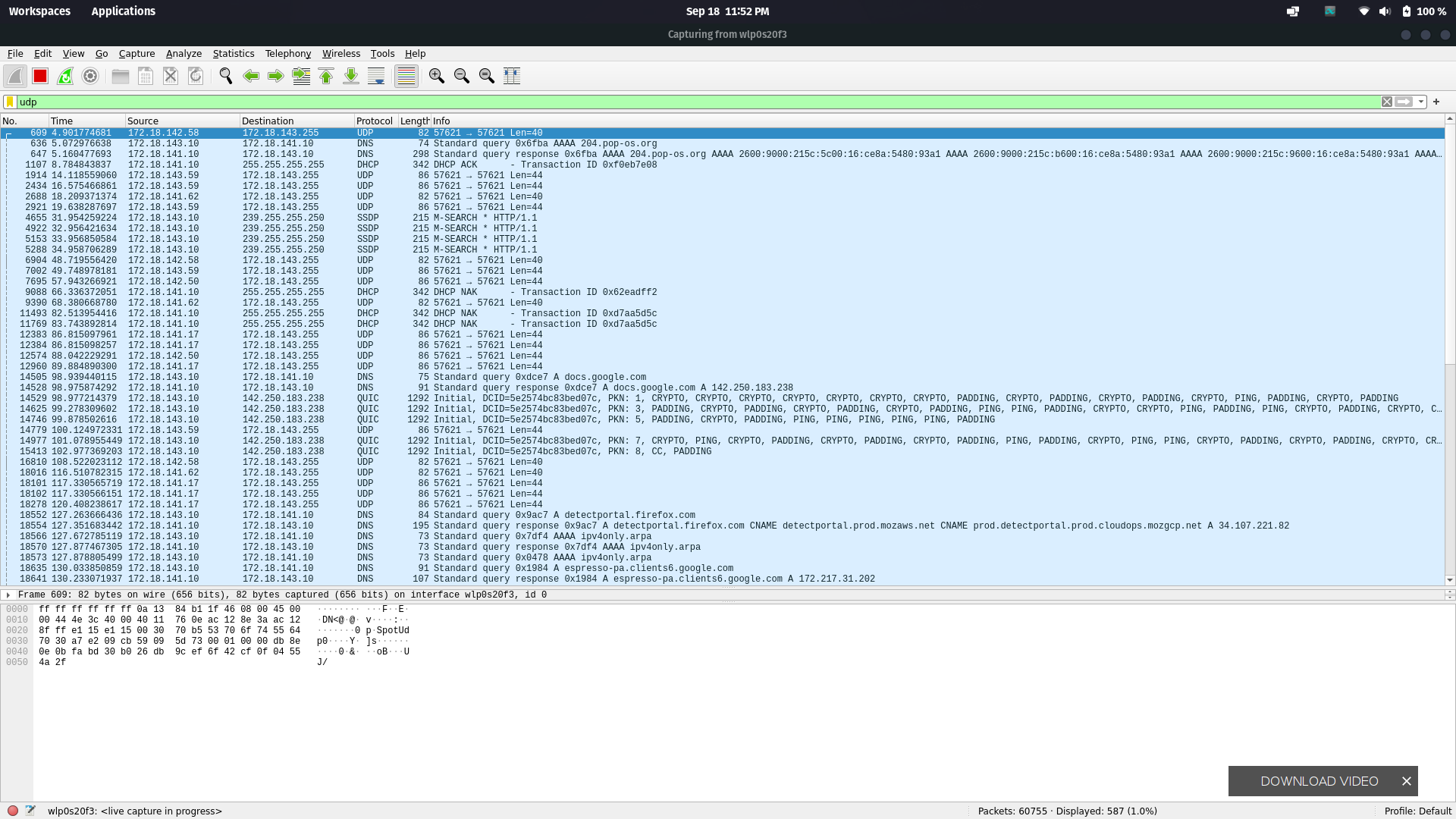
Lab Experiment 1 - Wireshark

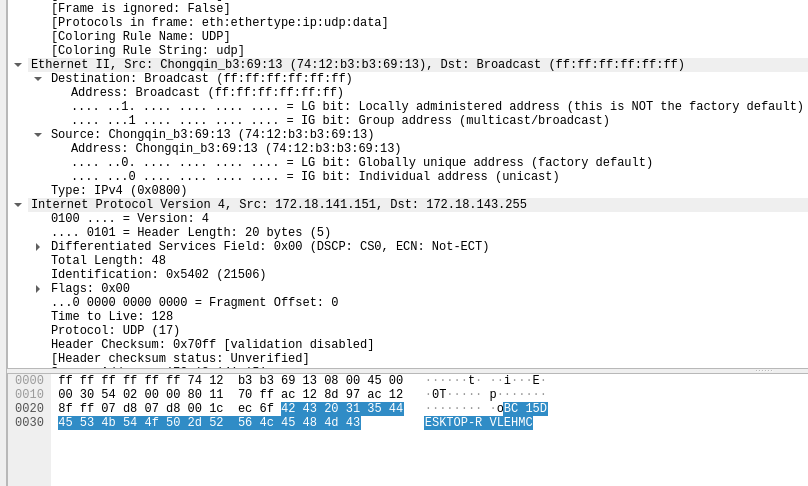
Name: Mohd Priyanshu Yakub

RegNo: 20BCE7305

1. Find the Broadcast Address.

**Method 1:**



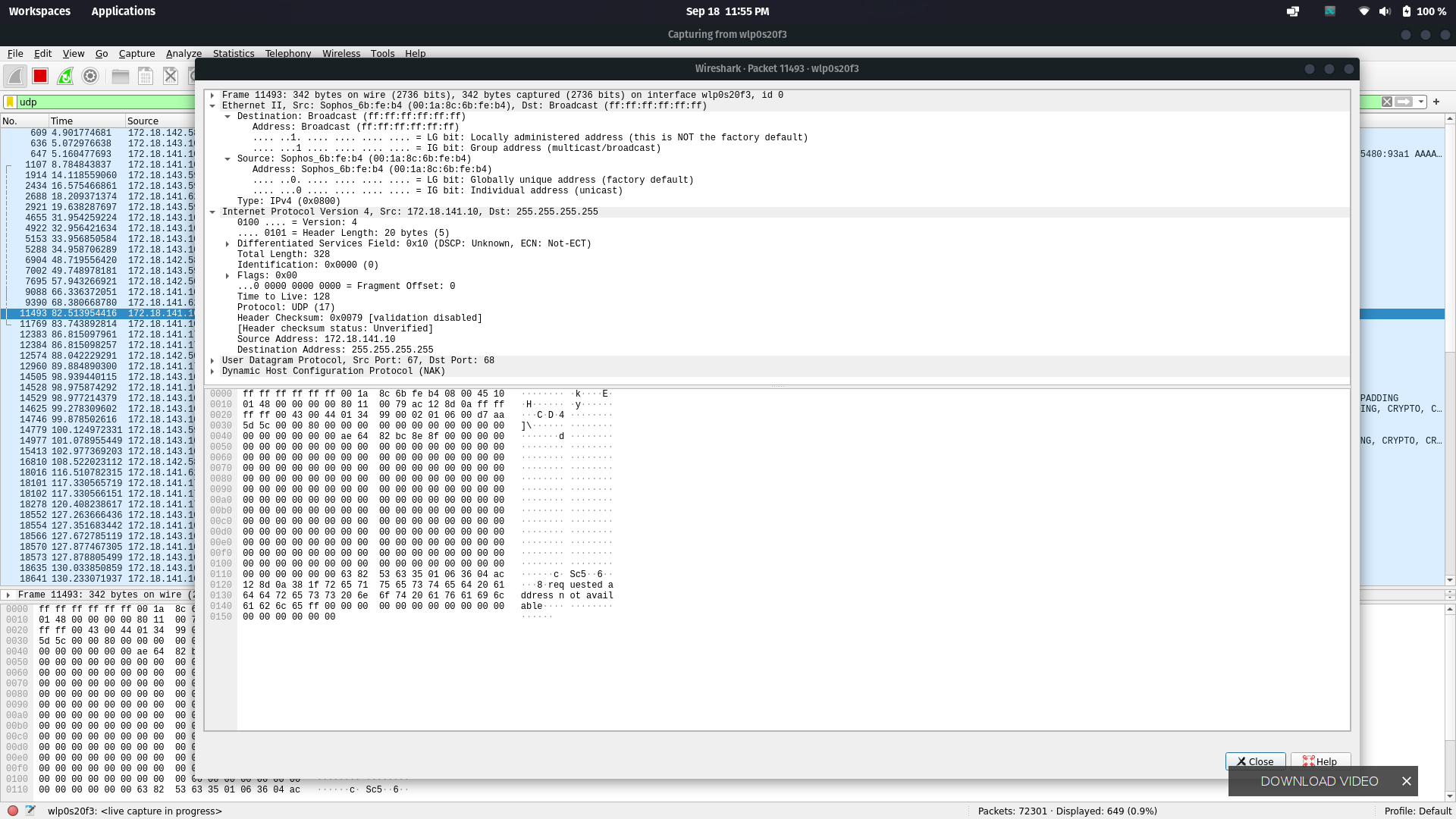


Filter UDP in wireshark as generally broadcasts are sent using UDP, search for a packet which has Destination as broadcast in Ethernet II field, then the packet is a broadcasted one and its ip address is the broadcast ip address.

The Brodcast:

MAC - ff:ff:ff:ff:ff:ff

IP address - 172.18.143.255



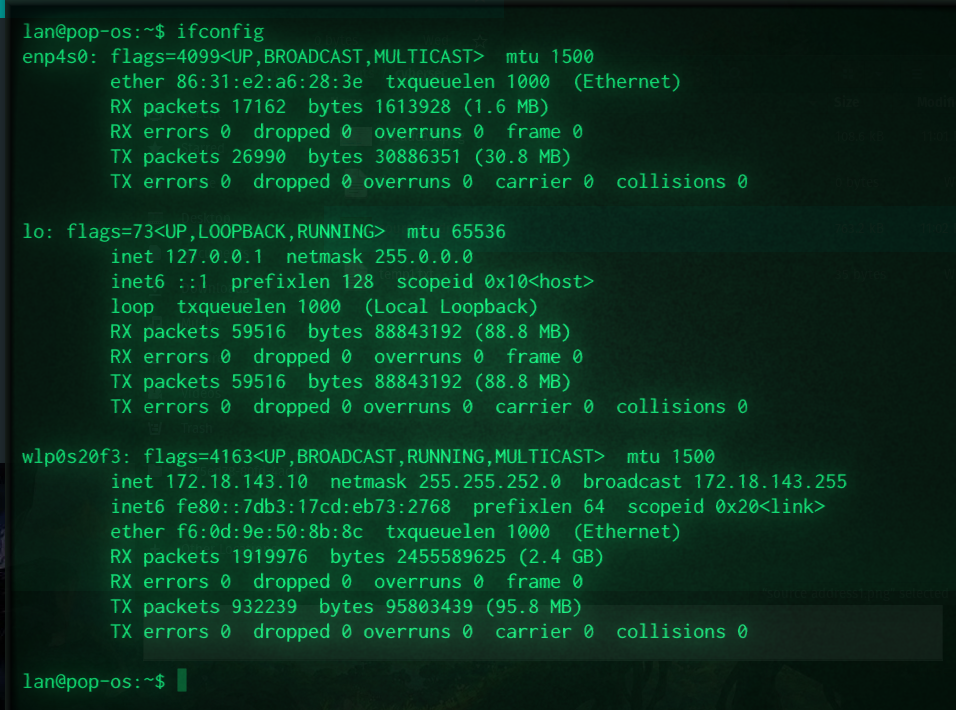
Another example where broadcast:

MAC:ff:ff:ff:ff:ff:ff

IP address:255.255.255.255 (reserved as broadcast address)

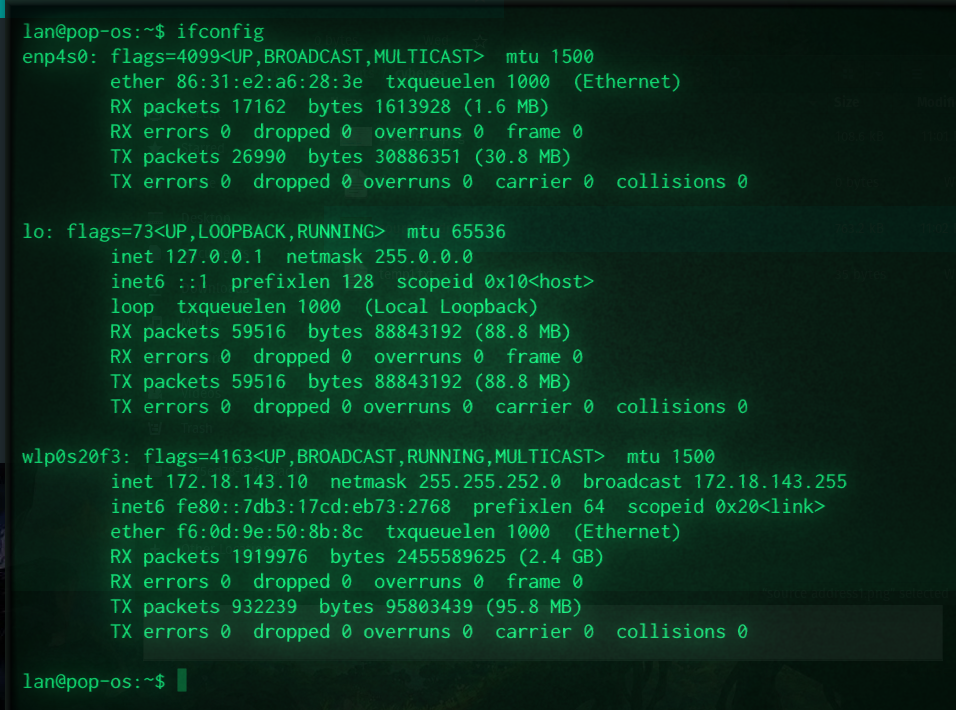
**Method 2:**

The broadcast ip address can be shown using ‘ifconfig command in terminal’



1. Find the src address

**Method 1 (using ifconfig):**

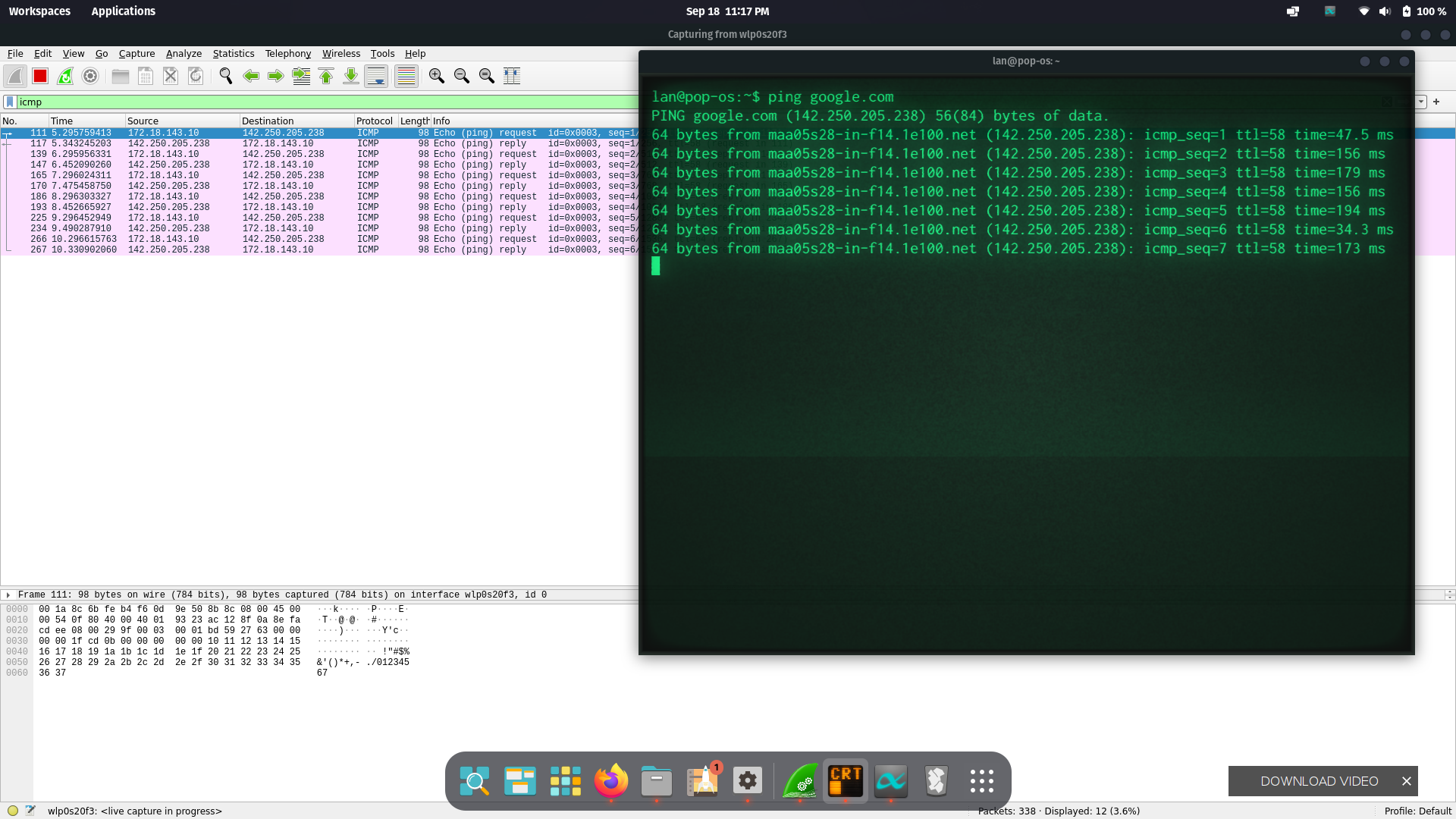


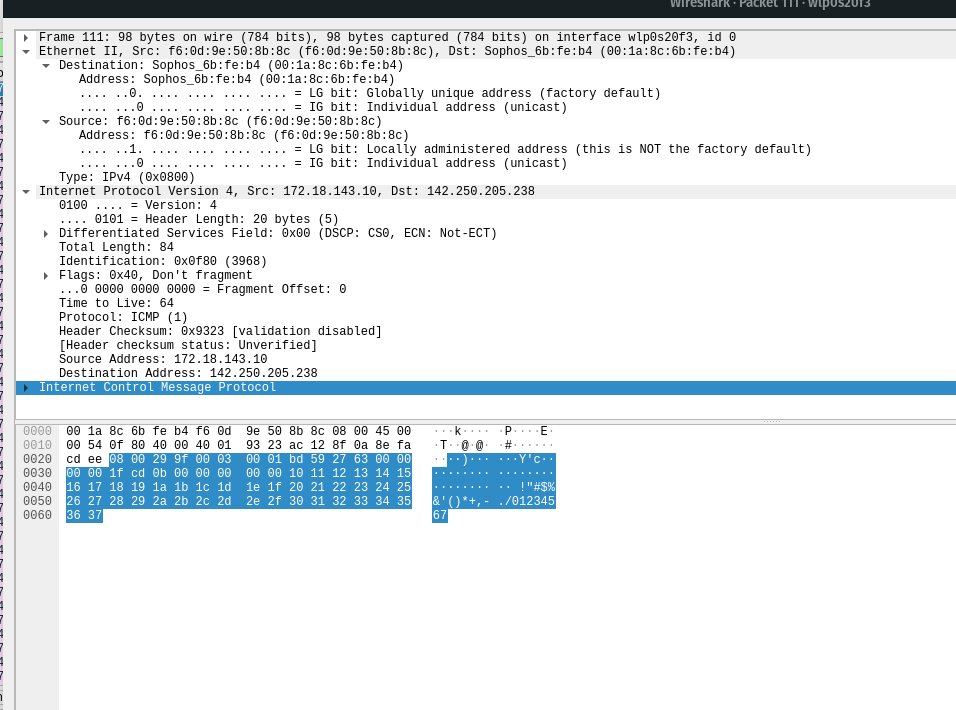
inet (ip address) - 172.18.143.10

ether (MAC) - f6:0d:9e:50:8b:8c

Method 2 (identifying your network in wireshark):

Send a ping to a random website and track icmp requests, as you are initiating the communication(ping) the first packet will be from your machine, i.e the source in the packet details is your machine.

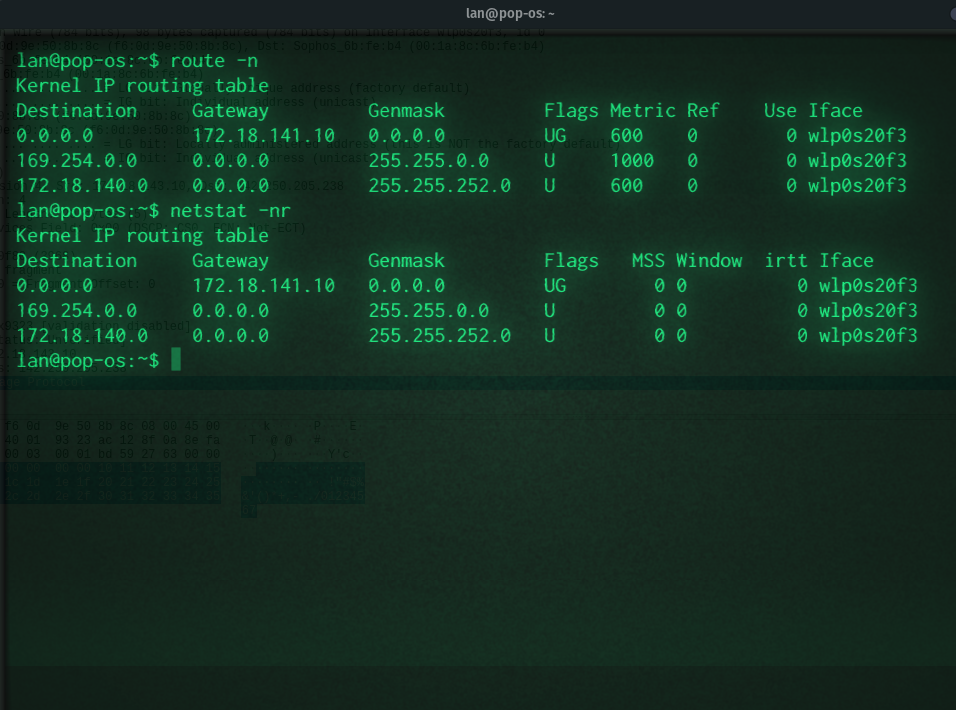




1. Find router address:

The router is the gateway of your network.

Method 1 (in terminal):

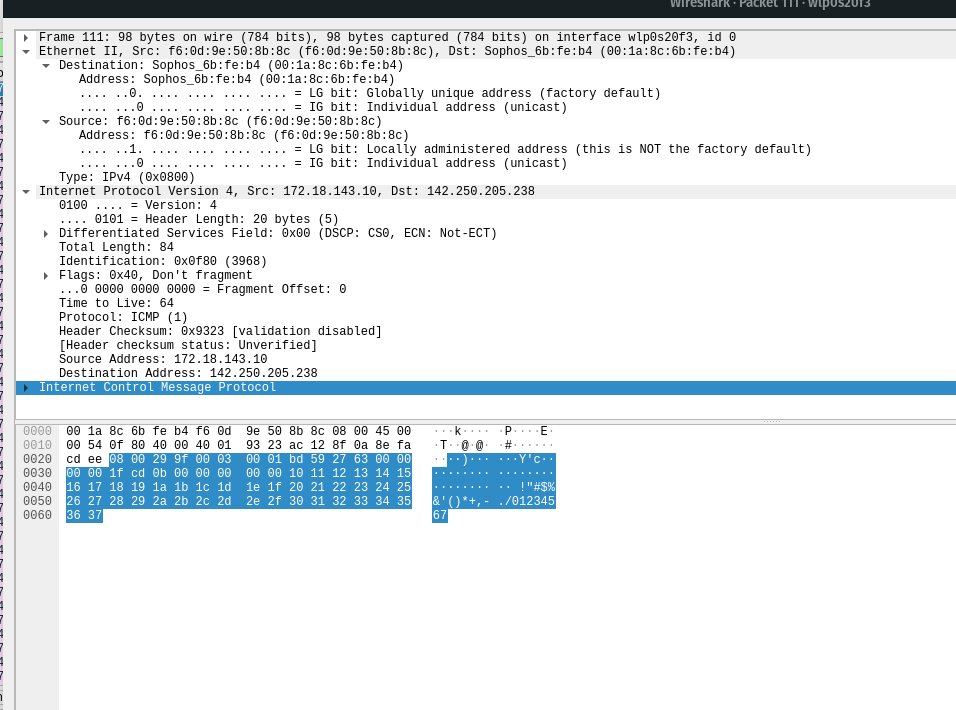


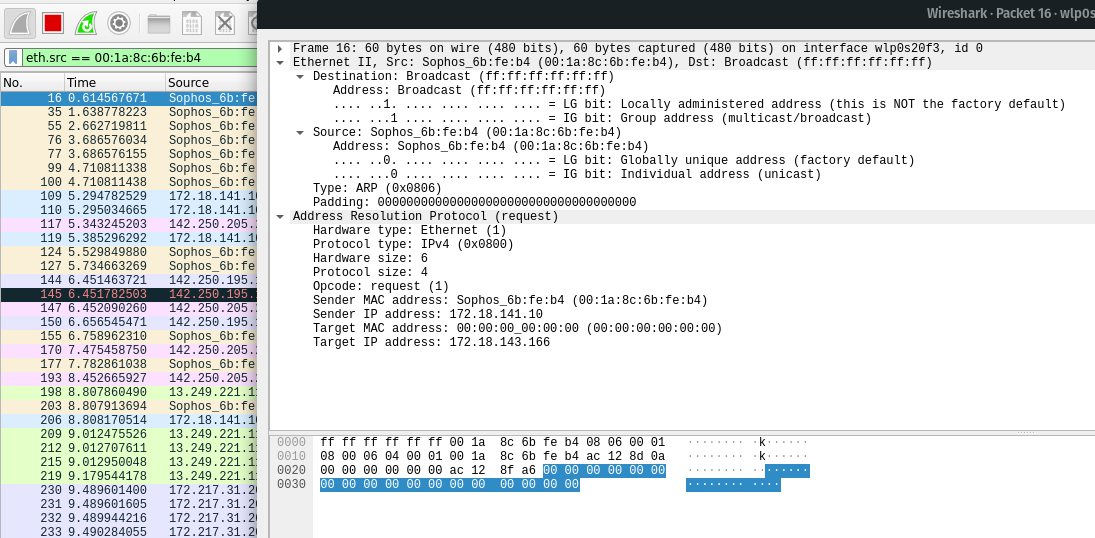
Using commands ‘netstat -nr’ or ‘route -n’ will show you the values present in your routing table, and the address present in the gateway column is the router(gateway to your network).

We can get its MAC by filtering packets in wireshark using the IP address we got (ip.addr == 172.18.141.10).

Method 2 (using wireshark):

When a packet is leaving the network, its destination MAC will be of the gateway router, so to get the router address we need to send a packet out of network (like using ping) and then get the dst MAC address, then we filter using “eth.src == <the mac address>” (we use source as many packets leaving will have different ip addresses for destination).



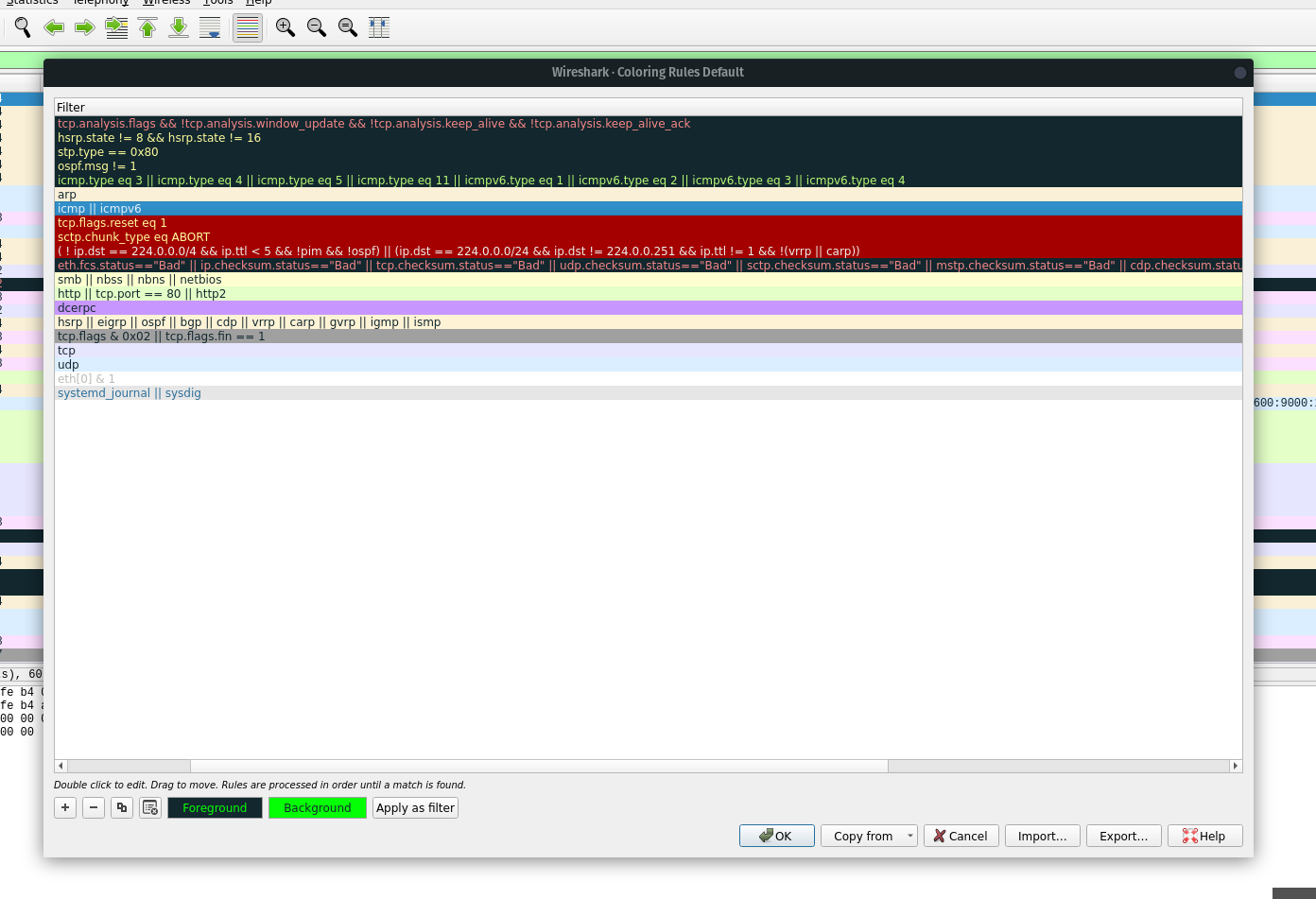


IP Address of router: 172.18.141.10

MAC of Router: 00:1a:8c:6b:fe:b4

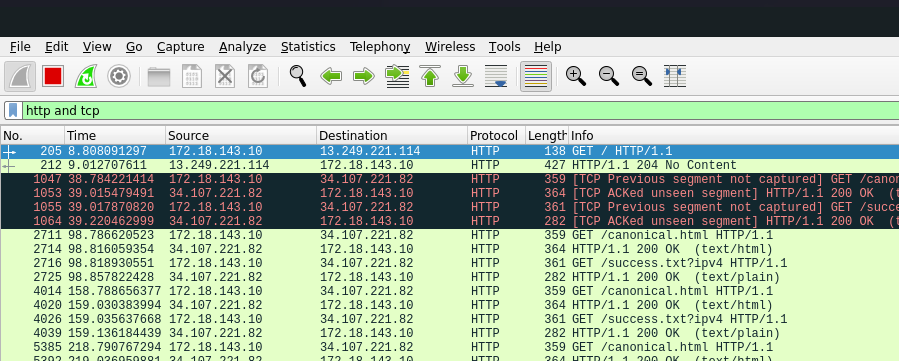
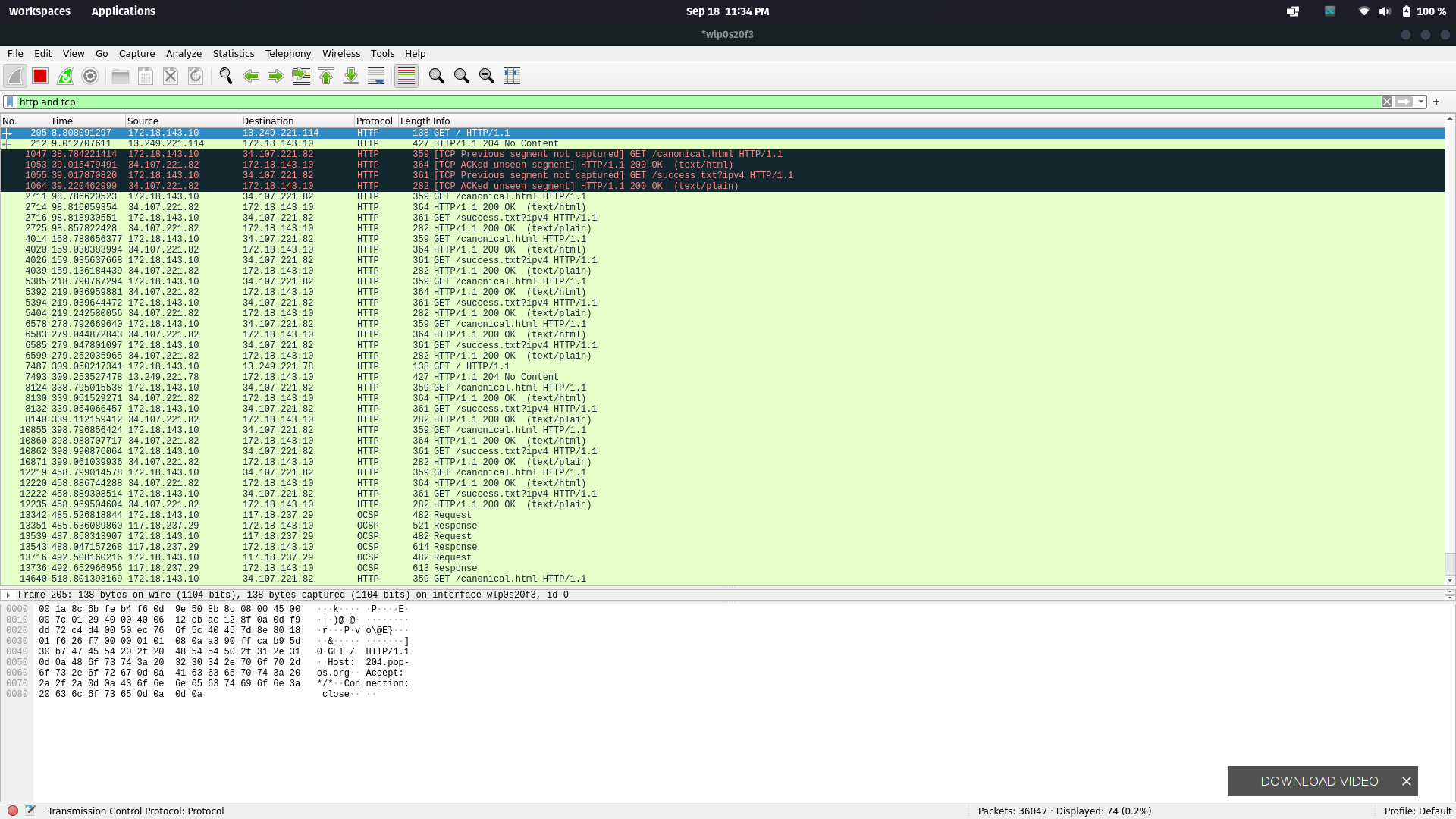
1. Change the color of packet and report the same.

Changing icmp packet color from yellow to green. (view>coloring rules)



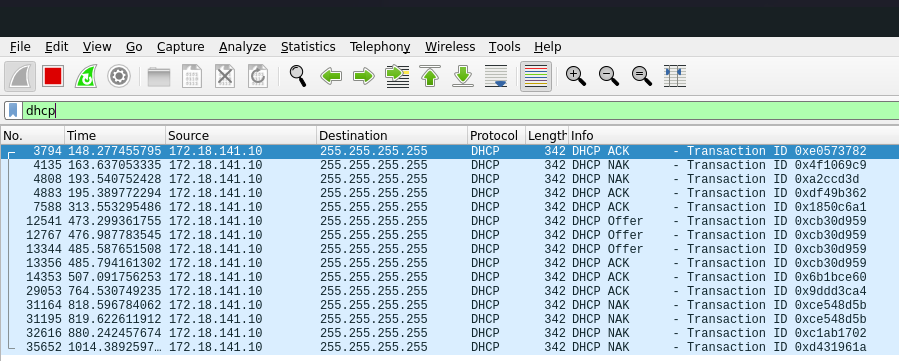
1. Filter Http and tcp packets.

Can be done using “http and tcp” in filter toolbar.



1. Filter DHCP packets

Same as before enter “dhcp” in filter toolbar



1. Ping any domain and filter the echo req and rep packets

