Cyber Security Lab

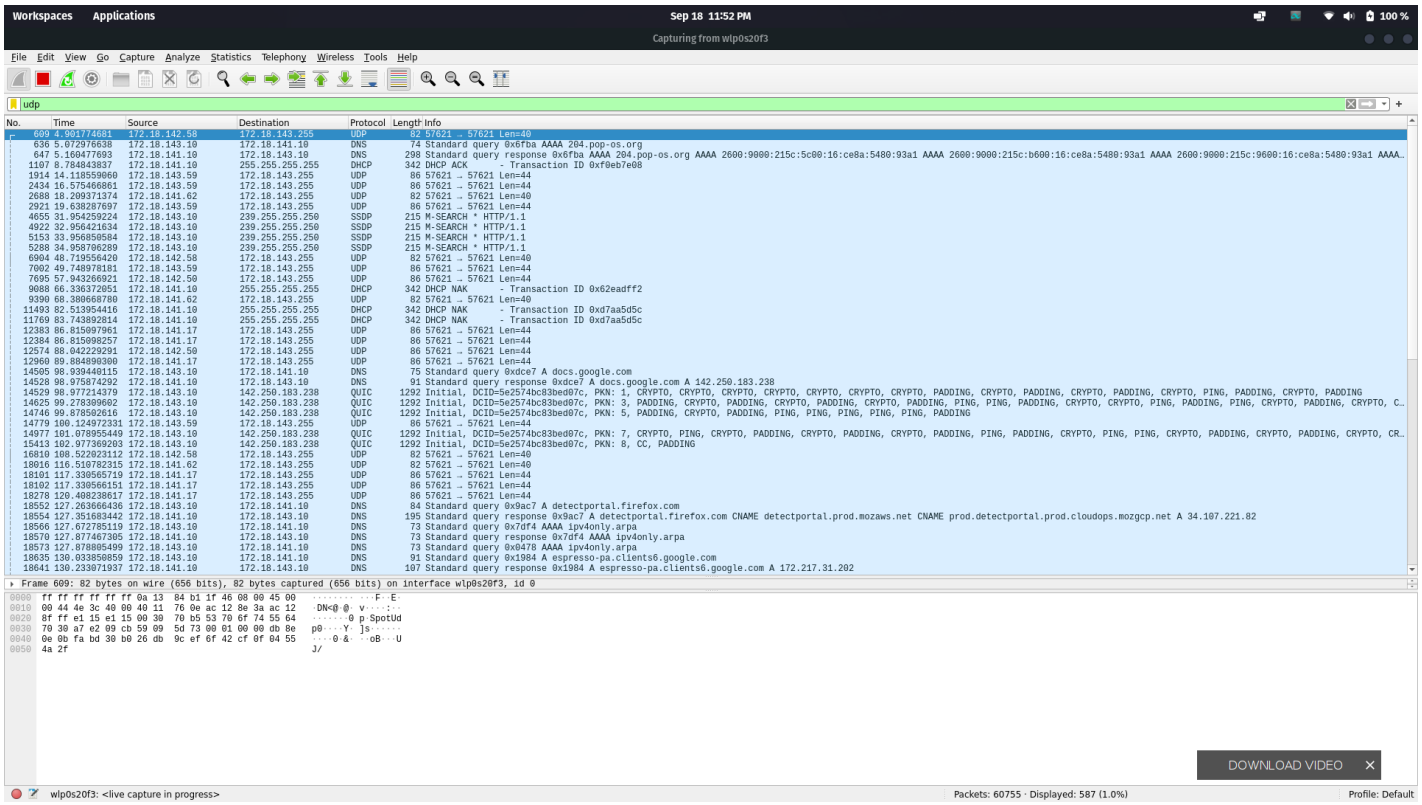
Lab Experiment 1 - Wireshark

Name: Mohd Priyanshu Yakub

RegNo: 20BCE7305

1. Find the Broadcast Address.

Method 1:



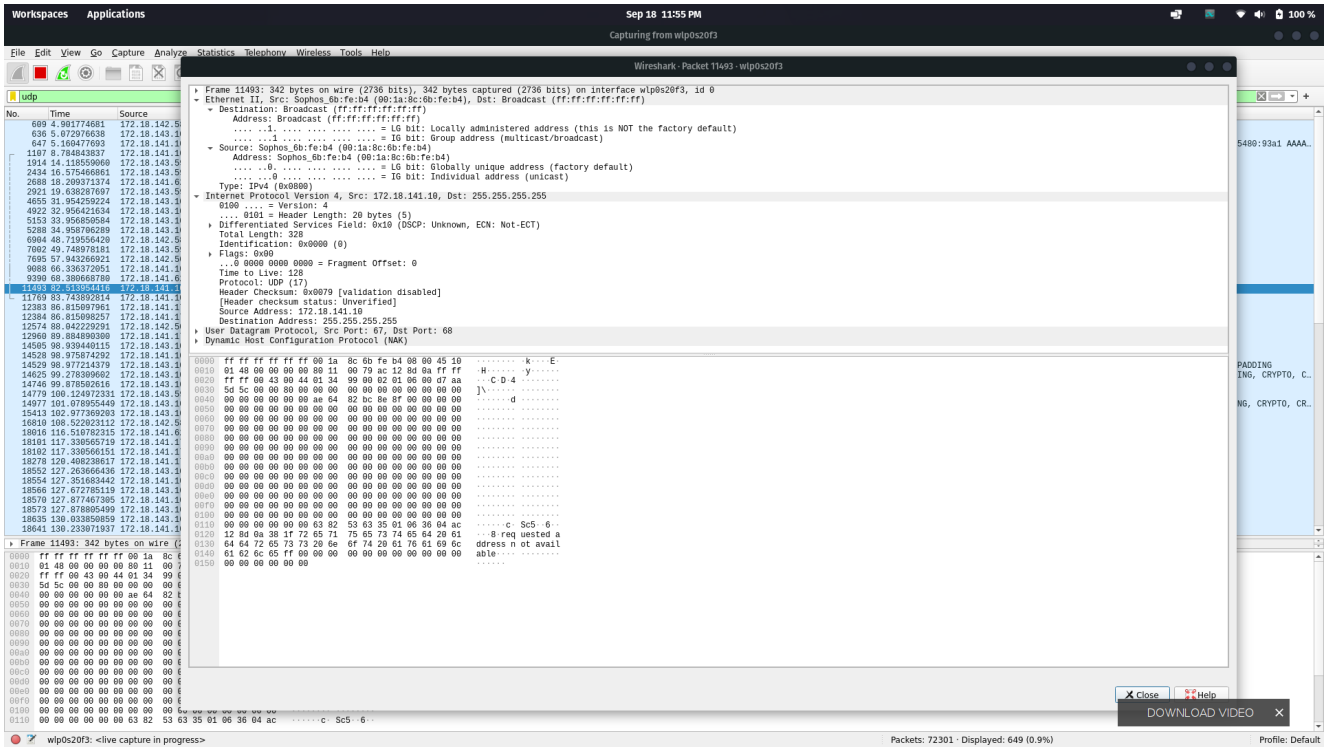
```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▾ Ethernet II, Src: Chongqin_b3:69:13 (74:12:b3:b3:69:13), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: Chongqin_b3:69:13 (74:12:b3:b3:69:13)
      Address: Chongqin_b3:69:13 (74:12:b3:b3:69:13)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 172.18.141.151, Dst: 172.18.143.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x5402 (21506)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x70ff [validation disabled]
    [Header checksum status: Unverified]

0000  ff ff ff ff ff ff 74 12  b3 b3 69 13 08 00 45 00   ......t·  ··i···E·
0010  00 30 54 02 00 00 80 11  70 ff ac 12 8d 97 ac 12   ·0T····· p·······
0020  8f ff 07 d8 07 d8 00 1c  ec 6f 42 43 20 31 35 44   ········ ·oBC 15D
0030  45 53 4b 54 4f 50 2d 52  56 4c 45 48 4d 43         ESKTOP-R VLEHMC
```

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



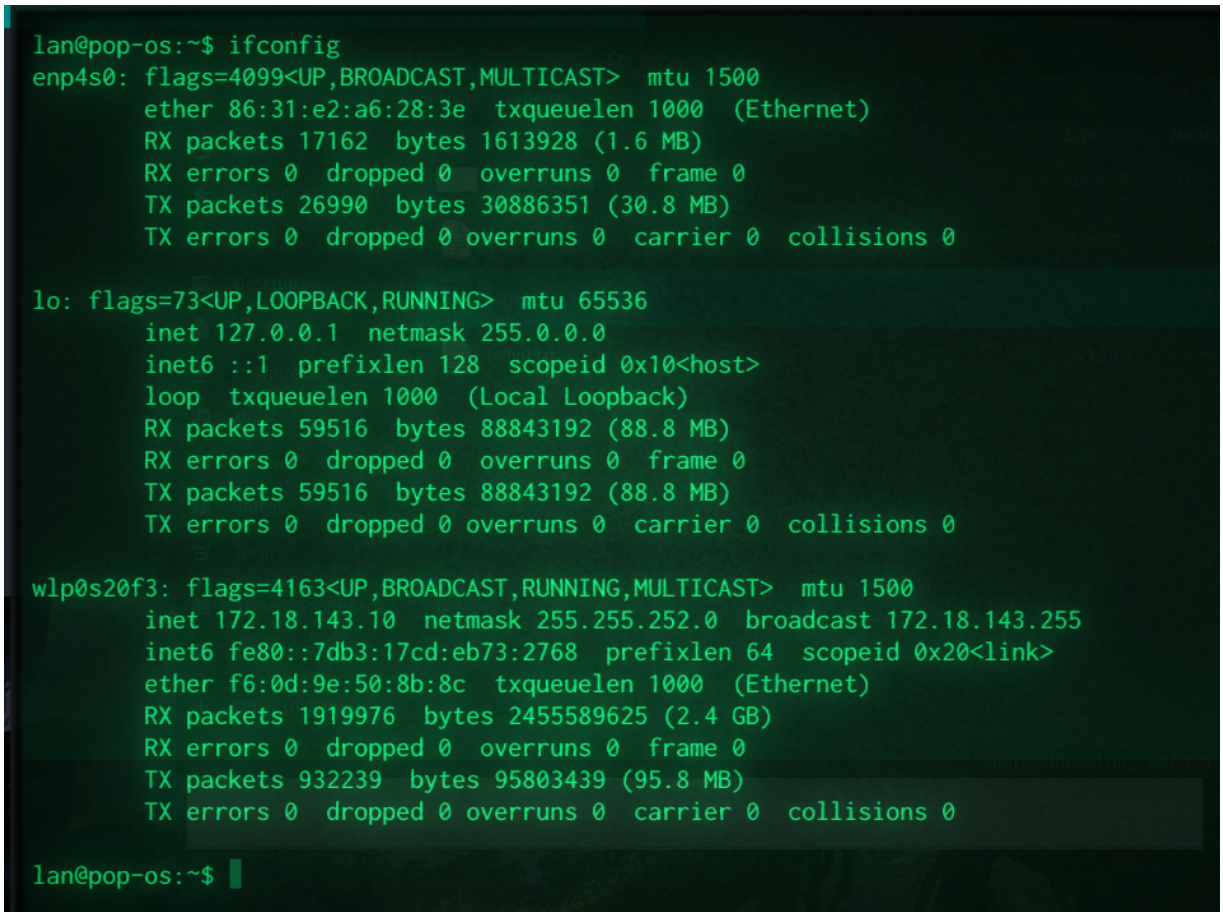
Another example where broadcast:

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

IP address:255.255.255.255 (reserved as broadcast address)

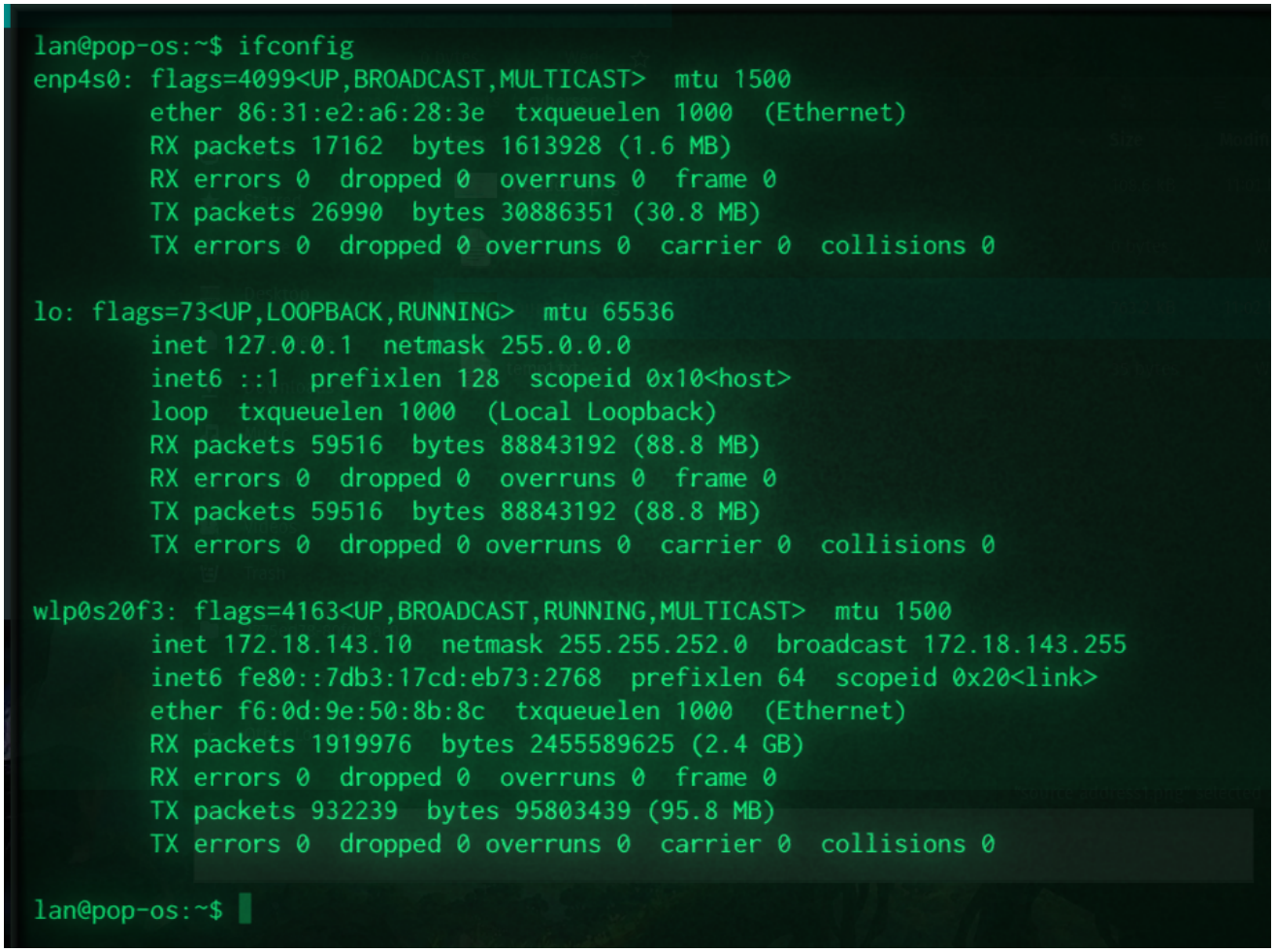
Method 2:

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



2. Find the src address

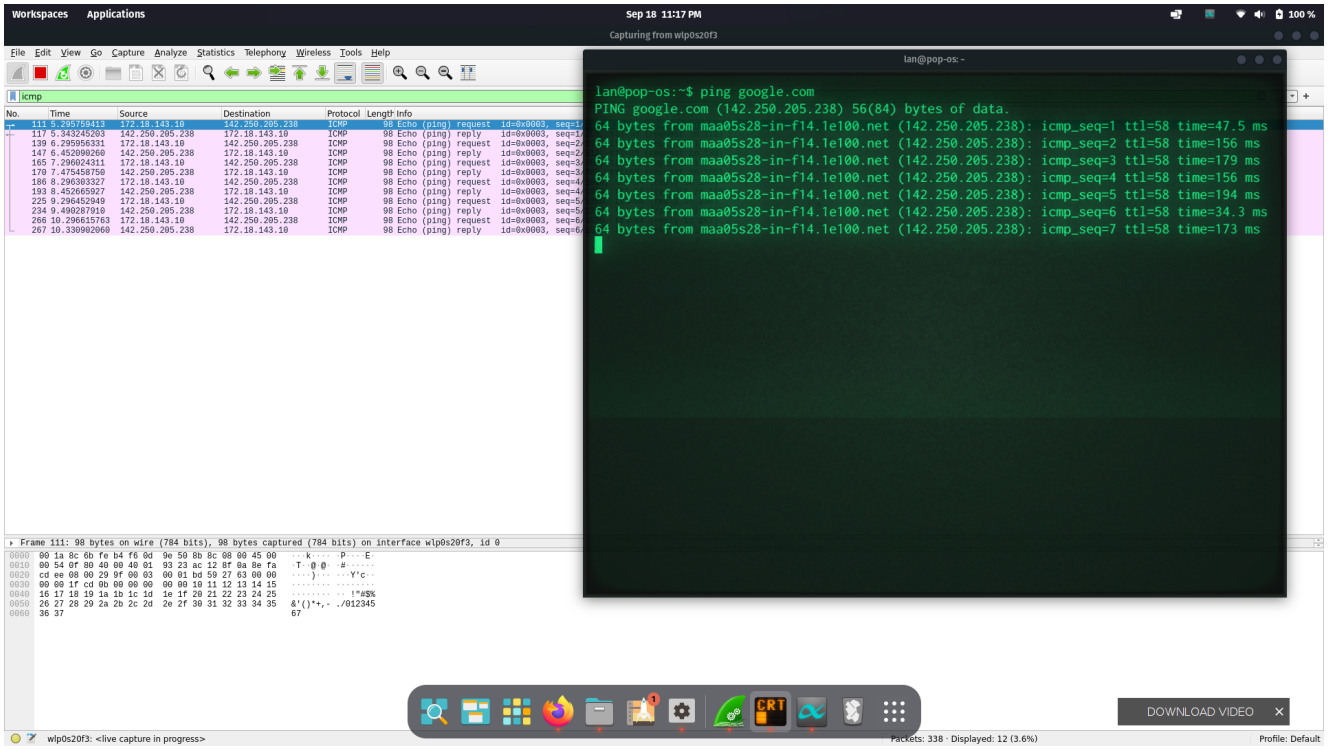
Method 1 (using ifconfig):

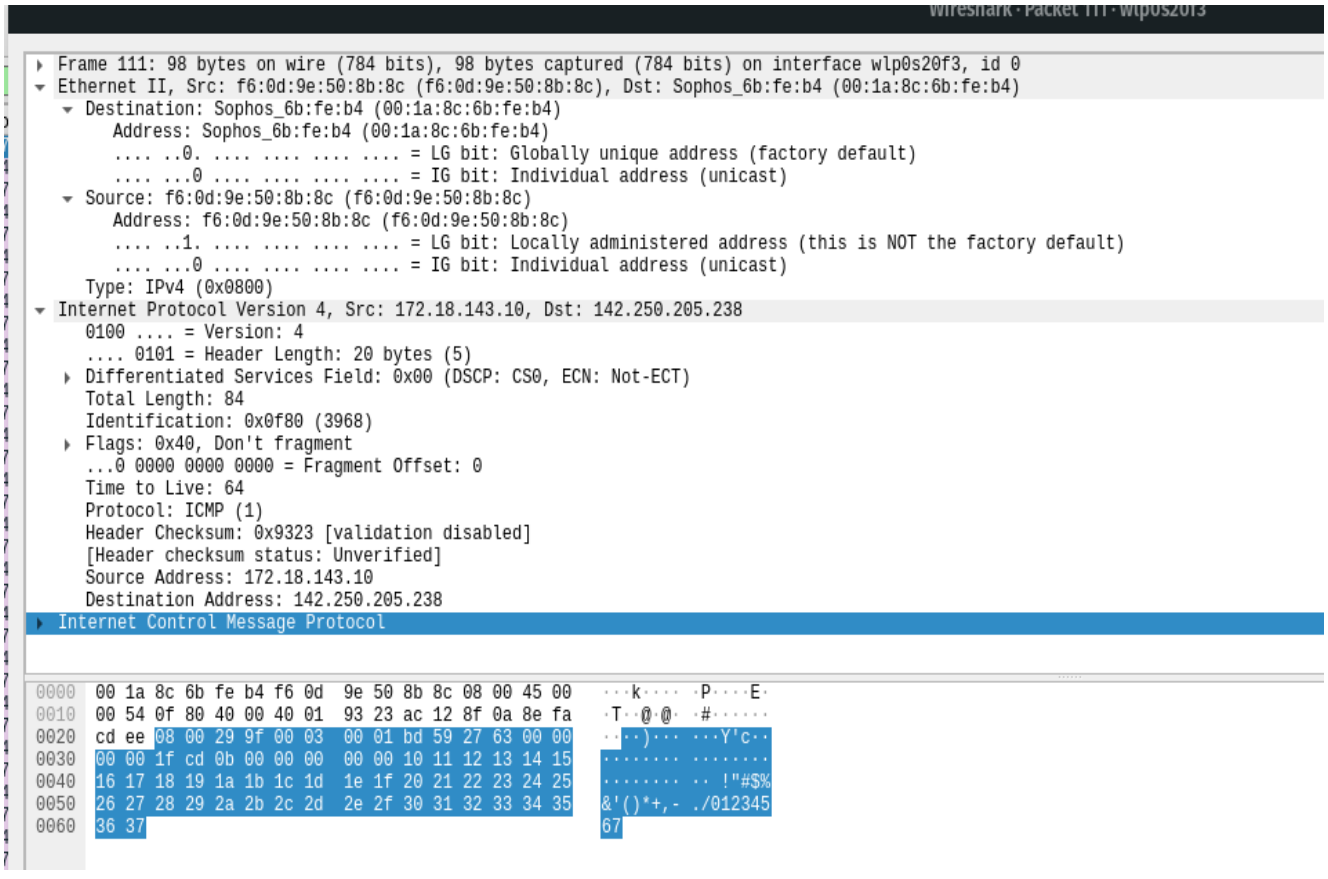


inet (ip address) - 172.18.143.10
ether (MAC) - f6:0d:9e:50:8b:8c

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.

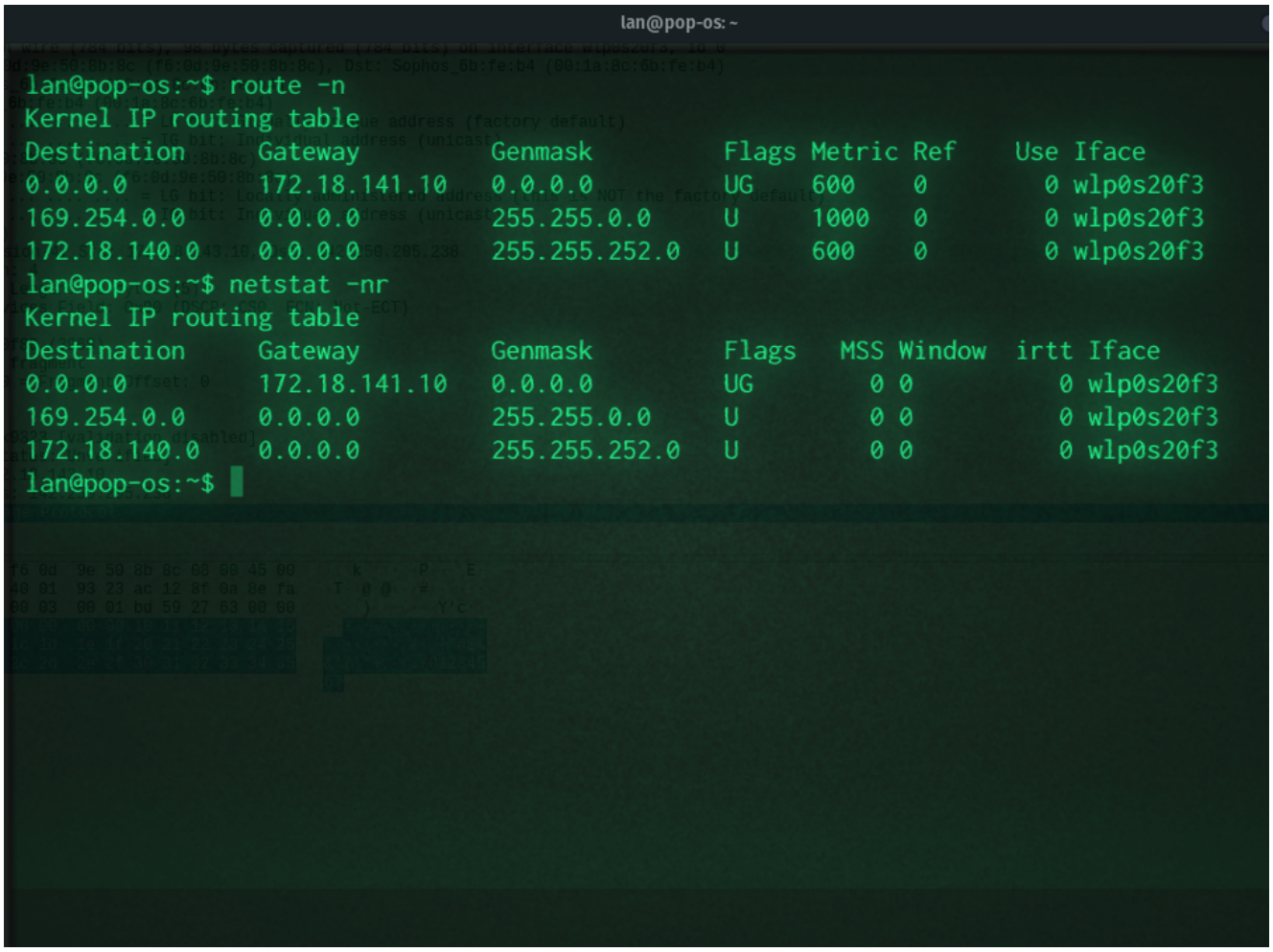

Workspaces
Applications
Sep 18 11:17 PM
100 %
Capturing from wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
111 5.295759413 172.18.143.10 142.250.205.238 ICMP 98 Echo (ping) request id=0x0003, seq=1
117 5.343245203 142.250.205.238 172.18.143.10 ICMP 98 Echo (ping) reply id=0x0003, seq=1
139 6.295956331 172.18.143.10 142.250.205.238 ICMP 98 Echo (ping) request id=0x0003, seq=2
147 6.452090260 142.250.205.238 172.18.143.10 ICMP 98 Echo (ping) reply id=0x0003, seq=2
165 7.296024311 172.18.143.10 142.250.205.238 ICMP 98 Echo (ping) request id=0x0003, seq=3
170 7.475458750 142.250.205.238 172.18.143.10 ICMP 98 Echo (ping) reply id=0x0003, seq=3
186 8.296303327 172.18.143.10 142.250.205.238 ICMP 98 Echo (ping) request id=0x0003, seq=4
193 8.452665927 142.250.205.238 172.18.143.10 ICMP 98 Echo (ping) reply id=0x0003, seq=4
225 9.296452949 172.18.143.10 142.250.205.238 ICMP 98 Echo (ping) request id=0x0003, seq=5
234 9.490287910 142.250.205.238 172.18.143.10 ICMP 98 Echo (ping) reply id=0x0003, seq=5
266 10.296615763 172.18.143.10 142.250.205.238 ICMP 98 Echo (ping) request id=0x0003, seq=6
267 10.330902060 142.250.205.238 172.18.143.10 ICMP 98 Echo (ping) reply id=0x0003, seq=6
lan@pop-os: ~
lan@pop-os:~$ ping google.com
PING google.com (142.250.205.238) 56(84) bytes of data.
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=1 ttl=58 time=47.5 ms
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=2 ttl=58 time=156 ms
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=3 ttl=58 time=179 ms
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=4 ttl=58 time=156 ms
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=5 ttl=58 time=194 ms
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=6 ttl=58 time=34.3 ms
64 bytes from maa05s28-in-f14.1e100.net (142.250.205.238): icmp_seq=7 ttl=58 time=173 ms
Frame 111: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s20f3, id 0
DOWNLOAD VIDEO
wlp0s20f3: <live capture in progress>
Packets: 338 · Displayed: 12 (3.6%)
Profile: Default


Wireshark · Packet 111 · wlp0s20f3
Frame 111: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: f6:0d:9e:50:8b:8c (f6:0d:9e:50:8b:8c), Dst: Sophos_6b:fe:b4 (00:1a:8c:6b:fe:b4)
Destination: Sophos_6b:fe:b4 (00:1a:8c:6b:fe:b4)
Address: Sophos_6b:fe:b4 (00:1a:8c:6b:fe:b4)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: f6:0d:9e:50:8b:8c (f6:0d:9e:50:8b:8c)
Address: f6:0d:9e:50:8b:8c (f6:0d:9e:50:8b:8c)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.18.143.10, Dst: 142.250.205.238
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x0f80 (3968)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x9323 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.18.143.10
Destination Address: 142.250.205.238
Internet Control Message Protocol
0000 00 1a 8c 6b fe b4 f6 0d 9e 50 8b 8c 08 00 45 00
0010 00 54 0f 80 40 00 40 01 93 23 ac 12 8f 0a 8e fa
0020 cd ee 08 00 29 9f 00 03 00 01 bd 59 27 63 00 00
0030 00 00 1f cd 0b 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37

3. Find router address:

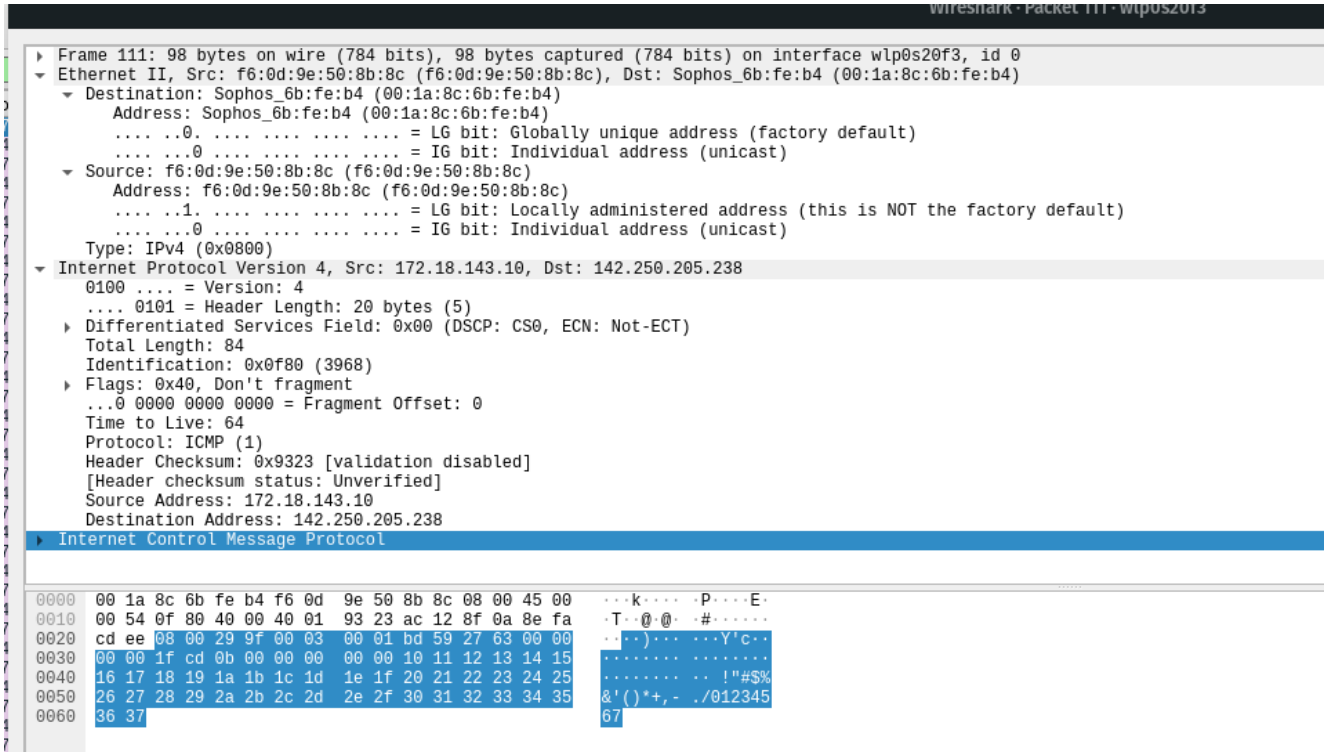
The router is the gateway of your network.

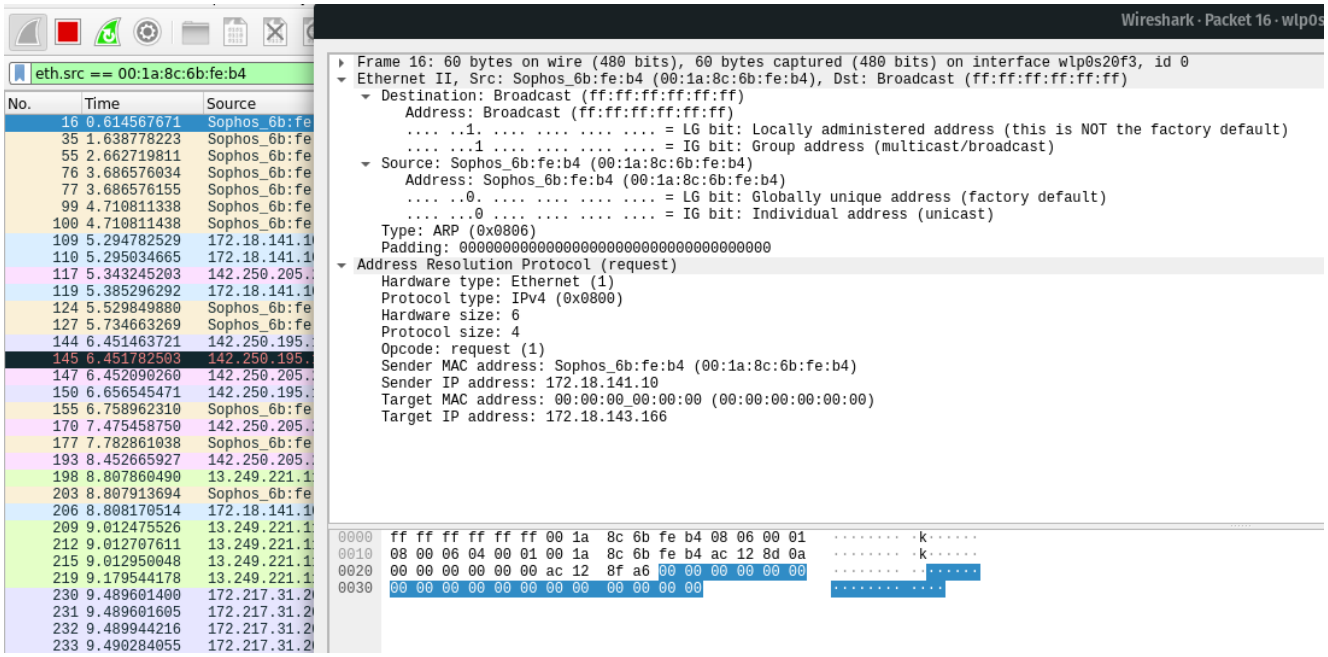
Method 1 (in terminal):



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).

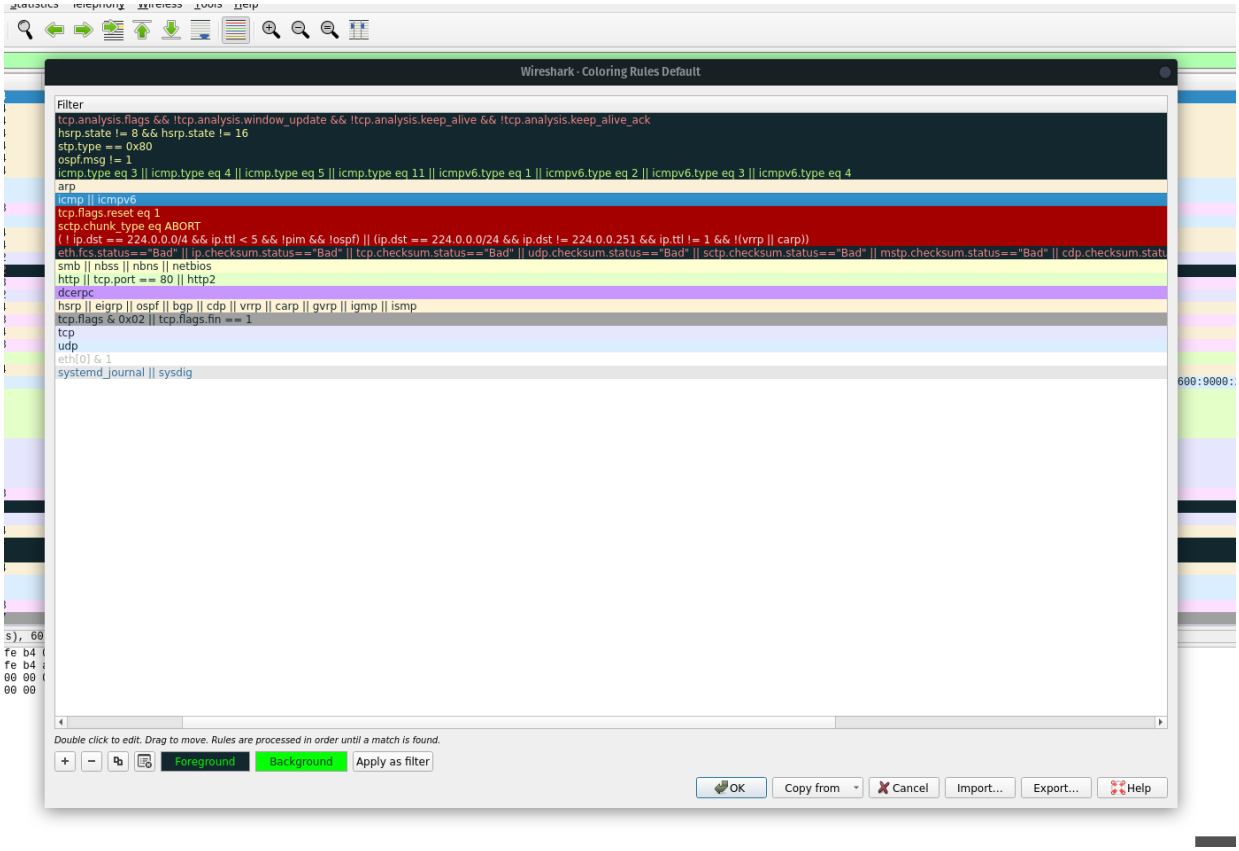


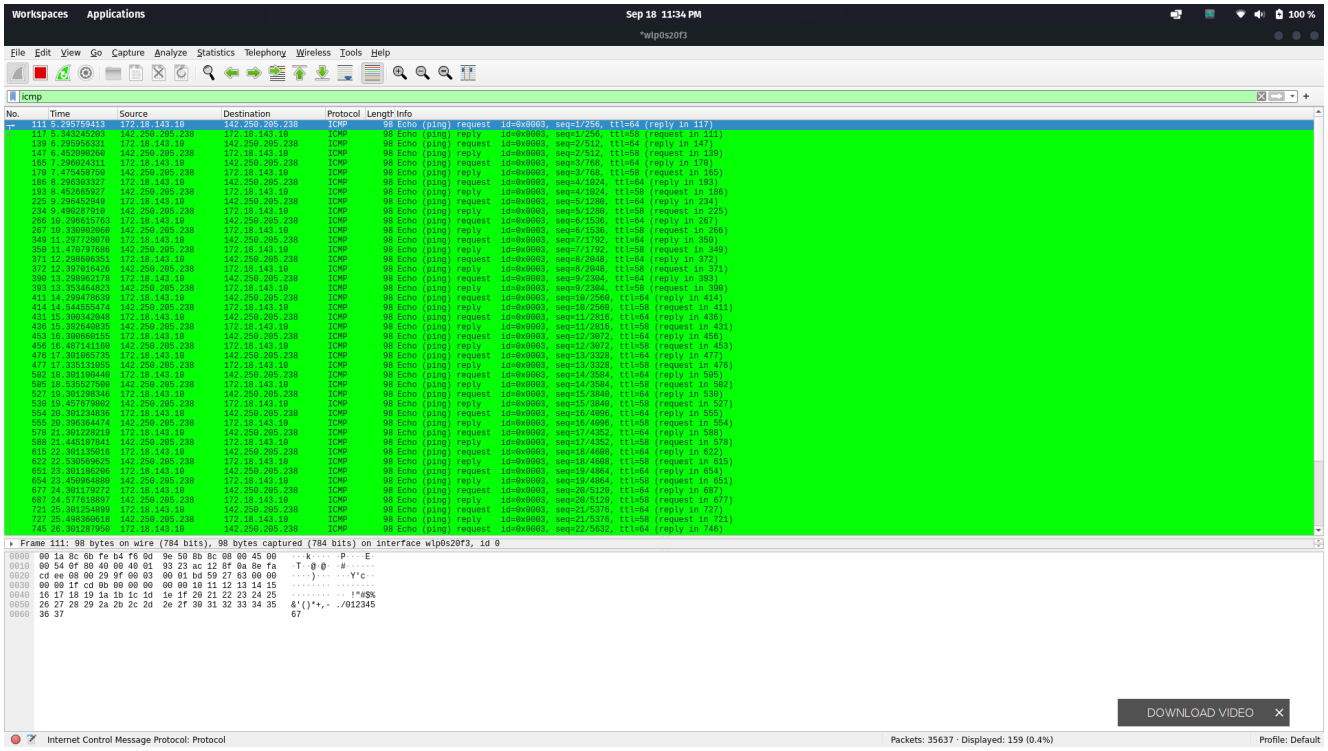


IP Address of router: 172.18.141.10
MAC of Router: 00:1a:8c:6b:fe:b4

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

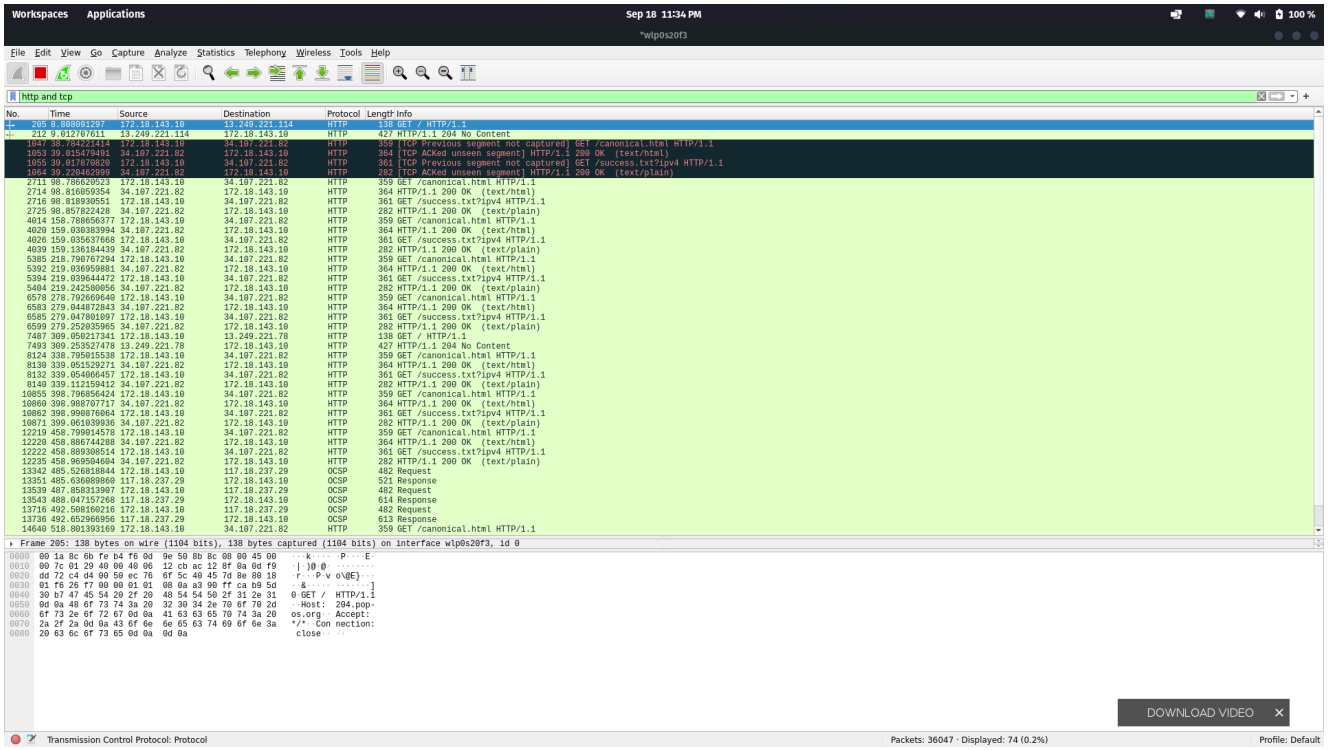
Changing icmp packet color from yellow to green. (view>coloring rules)

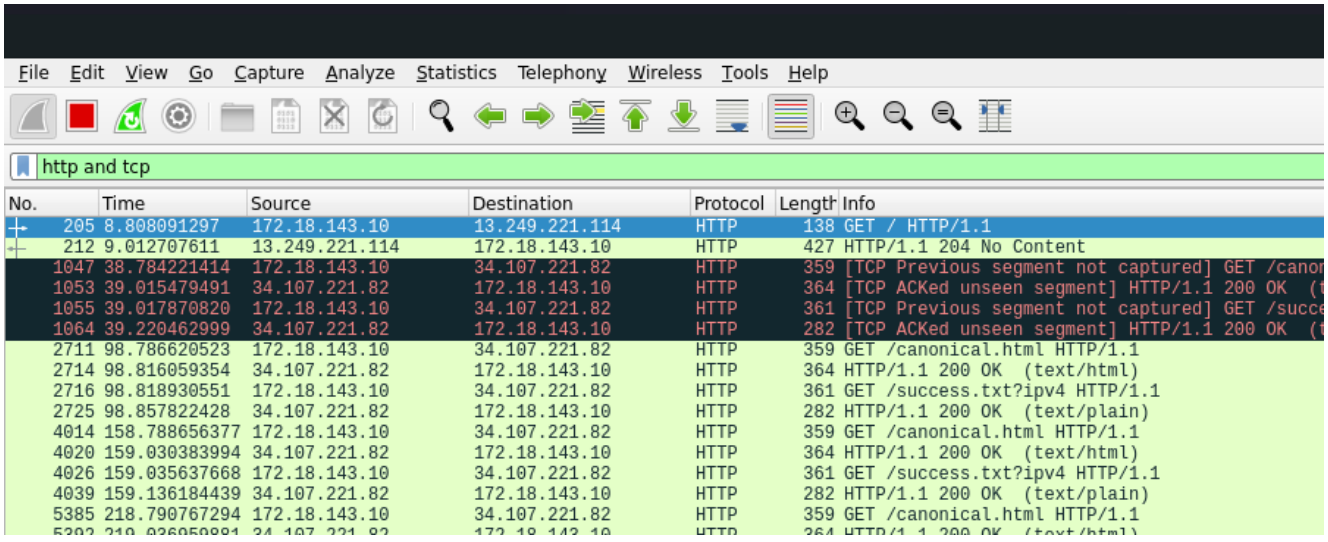




5. Filter Http and tcp packets.

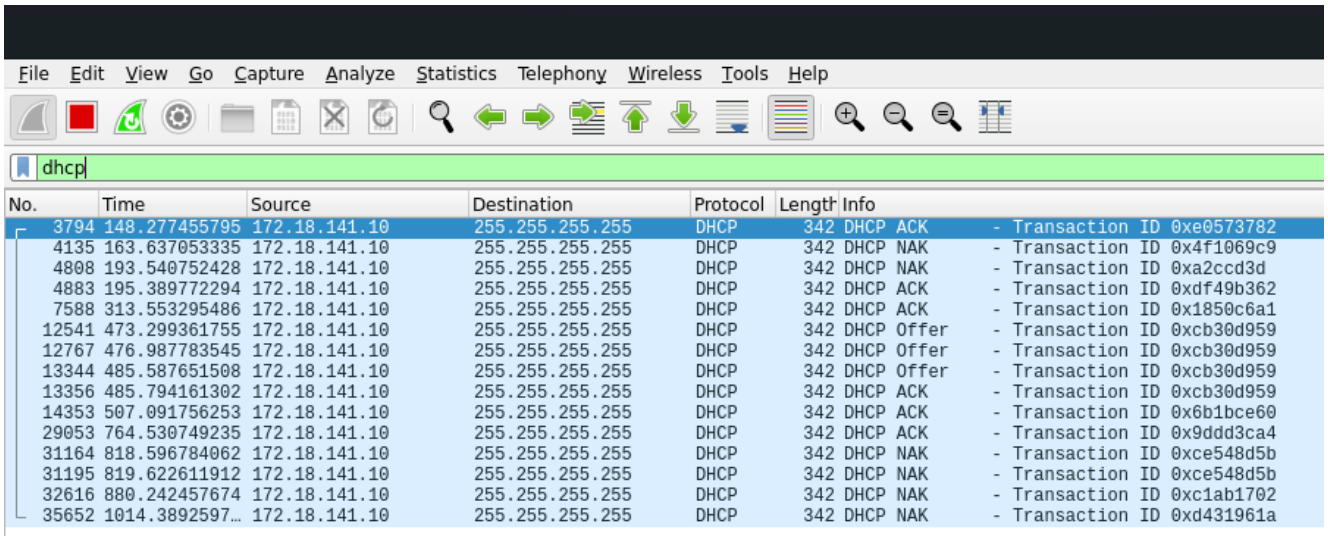
Can be done using “http and tcp” in filter toolbar.





6. Filter DHCP packets

Same as before enter “dhcp” in filter toolbar



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