

Cyber Security Lab

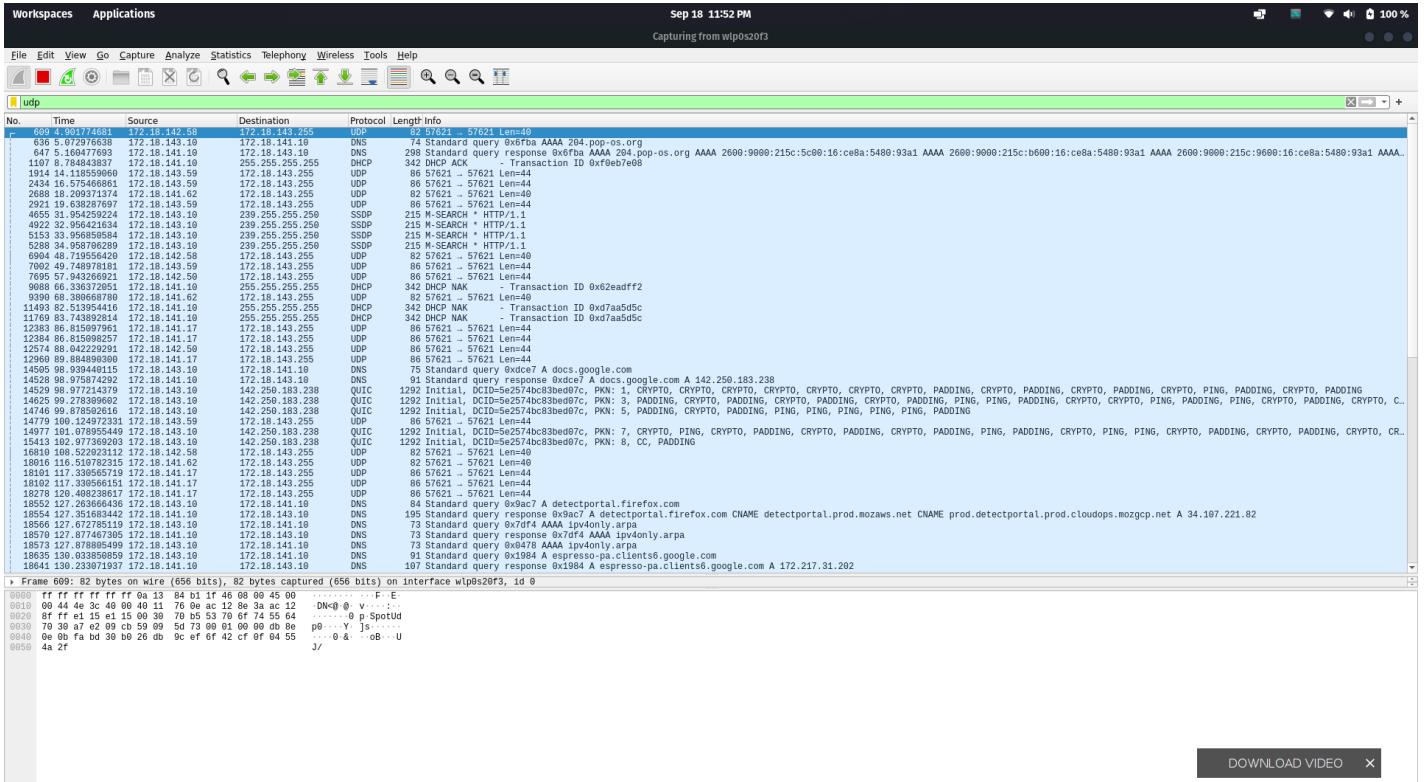
Lab Experiment 1 - Wireshark

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 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 .....dBC 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 Broadcast:

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

IP address - 172.18.143.255

Workspaces Applications

Sep 18 11:55 PM Capturing from wlp0s20f3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Frame 11493: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlp0s20f3, id 0

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Chongqin_b3:69:13 (74:12:b3:b3:69:13)

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 74 12 b3 b3 69 13 08 00 45 00t. .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 44dBC 15D

0030 45 53 4b 54 4f 50 2d 52 56 4c 45 48 4d 43 ESKTOP-R VLEHMC

Frame 11493: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlp0s20f3, id 0

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Chongqin_b3:69:13 (74:12:b3:b3:69:13)

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: Unknown, ECN: Not-ECT)

Identification: 0x0000 (0)

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]

Source Address: 172.18.141.151

Destination Address: 255.255.255.255

User Port: 67, System Port: 68

Dynamic Host Configuration Protocol (NACK)

11769 83 743892814 172.18.141.0

12383 86 815897961 172.18.141.1

12384 86 815897961 172.18.141.1

12574 88 042229294 172.18.142.5

12919 89 884890939 172.18.141.0

14528 98 075784292 172.18.141.0

14529 98 077214371 172.18.141.0

14530 98 077214371 172.18.141.0

14746 99 878502615 172.18.143.0

14779 100 124972331 172.18.143.5

14917 100 1351683449 172.18.143.0

15413 102 977285119 172.18.142.5

16810 108 522002312 172.18.142.5

18016 116 510782325 172.18.141.8

18101 117 330506151 172.18.141.1

18278 120 408238617 172.18.141.1

18382 120 408238617 172.18.141.1

18554 127 351683442 172.18.141.0

18566 127 672785119 172.18.142.0

18570 127 672785119 172.18.142.0

18673 127 878805499 172.18.143.0

18685 130 033859059 172.18.141.0

18684 130 033859059 172.18.141.0

Frame 11493: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlp0s20f3, id 0

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Chongqin_b3:69:13 (74:12:b3:b3:69:13)

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: Unknown, ECN: Not-ECT)

Identification: 0x0000 (0)

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]

Source Address: 172.18.141.151

Destination Address: 255.255.255.255

User Port: 67, System Port: 68

Dynamic Host Configuration Protocol (NAK)

0000 ff ff ff ff ff 74 12 b3 b3 69 13 08 00 45 10k. .y..E.

0010 01 40 00 00 00 00 80 00 11 00 99 79 ac 12 8d 0a ff H. C 04 ..

0020 ff ff 00 43 00 44 01 34 00 99 00 02 01 00 00 d7 aa J. D 4 ..

0030 5d 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

00A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

00B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

00C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

00D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

00E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

00F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0120 12 8d 0a 00 38 17 72 65 71 75 65 73 74 65 64 20 61 ..c. Sc5. 6 ..

0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0160 01 48 00 00 00 00 80 11 00 ..

0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

01A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

01B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

01C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

01D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

01E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

01F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

02A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

02B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

02C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

02D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

02E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

02F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

03A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

03B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

03C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

03D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

03E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

03F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0510 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0530 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0550 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0560 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0570 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0580 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0590 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0610 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0620 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0650 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0670 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0680 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0690 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0710 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0730 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0740 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0750 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0760 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0770 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0780 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0790 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0810 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0820 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0840 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0850 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0860 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0870 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0880 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0890 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0910 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0920 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0930 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0940 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0950 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0970 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0980 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

0990 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..d ..

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'

```
lan@pop-os:~$ ifconfig
enp4s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 86:31:e2:a6:28:3e txqueuelen 1000 (Ethernet)
      RX packets 17162 bytes 1613928 (1.6 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 26990 bytes 30886351 (30.8 MB)
      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 59516 bytes 88843192 (88.8 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 59516 bytes 88843192 (88.8 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.18.143.10 netmask 255.255.252.0 broadcast 172.18.143.255
    inet6 fe80::7db3:17cd:eb73:2768 prefixlen 64 scopeid 0x20<link>
        ether f6:0d:9e:50:8b:8c txqueuelen 1000 (Ethernet)
        RX packets 1919976 bytes 2455589625 (2.4 GB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 932239 bytes 95803439 (95.8 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lan@pop-os:~$
```

2. Find the src address

Method 1 (using ifconfig):

```
lan@pop-os:~$ ifconfig
enp4s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 86:31:e2:a6:28:3e txqueuelen 1000 (Ethernet)
      RX packets 17162 bytes 1613928 (1.6 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 26990 bytes 30886351 (30.8 MB)
      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 59516 bytes 88843192 (88.8 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 59516 bytes 88843192 (88.8 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.18.143.10 netmask 255.255.252.0 broadcast 172.18.143.255
    inet6 fe80::7db3:17cd:eb73:2768 prefixlen 64 scopeid 0x20<link>
        ether f6:0d:9e:50:8b:8c txqueuelen 1000 (Ethernet)
        RX packets 1919976 bytes 2455589625 (2.4 GB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 932239 bytes 95803439 (95.8 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lan@pop-os:~$
```

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 Capturing from wlp0s20f3

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length Info
115	14:55:29.000116	172.18.143.10	142.250.205.238	ICMP	98 Echo (ping) request id=0x0003 seq=1
117	14:55:29.000230	142.250.205.238	172.18.143.10	ICMP	98 Echo (ping) reply id=0x0003 seq=1
139	14:55:29.000531	172.18.143.10	142.250.205.238	ICMP	98 Echo (ping) request id=0x0003 seq=2
147	14:55:29.000926	142.250.205.238	172.18.143.10	ICMP	98 Echo (ping) reply id=0x0003 seq=2
165	14:55:31.111000	172.18.143.10	142.250.205.238	ICMP	98 Echo (ping) request id=0x0003 seq=3
178	14:55:31.111400	142.250.205.238	172.18.143.10	ICMP	98 Echo (ping) reply id=0x0003 seq=3
186	14:55:31.111800	172.18.143.10	142.250.205.238	ICMP	98 Echo (ping) request id=0x0003 seq=4
193	14:55:31.112200	142.250.205.238	172.18.143.10	ICMP	98 Echo (ping) reply id=0x0003 seq=4
223	14:55:31.112600	172.18.143.10	142.250.205.238	ICMP	98 Echo (ping) request id=0x0003 seq=5
234	14:55:31.113000	142.250.205.238	172.18.143.10	ICMP	98 Echo (ping) reply id=0x0003 seq=5
266	14:55:31.113400	172.18.143.10	142.250.205.238	ICMP	98 Echo (ping) request id=0x0003 seq=6
267	14:55:31.113800	142.250.205.238	172.18.143.10	ICMP	98 Echo (ping) reply id=0x0003 seq=6

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

wlp0s20f3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s20f3, id 0

0000 00 1a 8c 6b fe b4 f6 0d 9e 50 8b 8c 08 00 45 00 .k.....P...E.
0010 00 54 0f 80 40 00 40 01 93 23 ac 12 8f 0a 8e fa .T..@.##.....
0020 cd ee 08 00 29 9f 00 03 00 01 bd 59 27 63 00 00 .).)....Y'c...
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 &'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 67

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

Hex	Dec
0000	00 1a 8c 6b fe b4 f6 0d
0010	9e 50 8b 8c 08 00 45 00
0020k.....P...E.
0030	00 54 0f 80 40 00 40 01
0040	93 23 ac 12 8f 0a 8e fa
0050	.T..@.##....
0060	cd ee 08 00 29 9f 00 03
0070	00 01 bd 59 27 63 00 00
0080	.).)....Y'c...
0090	00 00 1f cd 0b 00 00 00
00a0	00 00 10 11 12 13 14 15
00b0!#\$%
00c0	16 17 18 19 1a 1b 1c 1d
00d0	1e 1f 20 21 22 23 24 25
00e0	26 27 28 29 2a 2b 2c 2d
00f0	2e 2f 30 31 32 33 34 35
0100	36 37 67

3. Find router address:

The router is the gateway of your network.

Method 1 (in terminal):

```
lan@pop-os:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         172.18.141.10   0.0.0.0        UG    600    0      0 wlp0s20f3
169.254.0.0     0.0.0.0        255.255.0.0    U      1000   0      0 wlp0s20f3
172.18.140.0    0.0.0.0        255.255.252.0  U      600    0      0 wlp0s20f3
lan@pop-os:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask        Flags  MSS Window irtt Iface
0.0.0.0         172.18.141.10   0.0.0.0        UG      0 0      0 wlp0s20f3
169.254.0.0     0.0.0.0        255.255.0.0    U      0 0      0 wlp0s20f3
172.18.140.0    0.0.0.0        255.255.252.0  U      0 0      0 wlp0s20f3
lan@pop-os:~$
```

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).

```
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
```

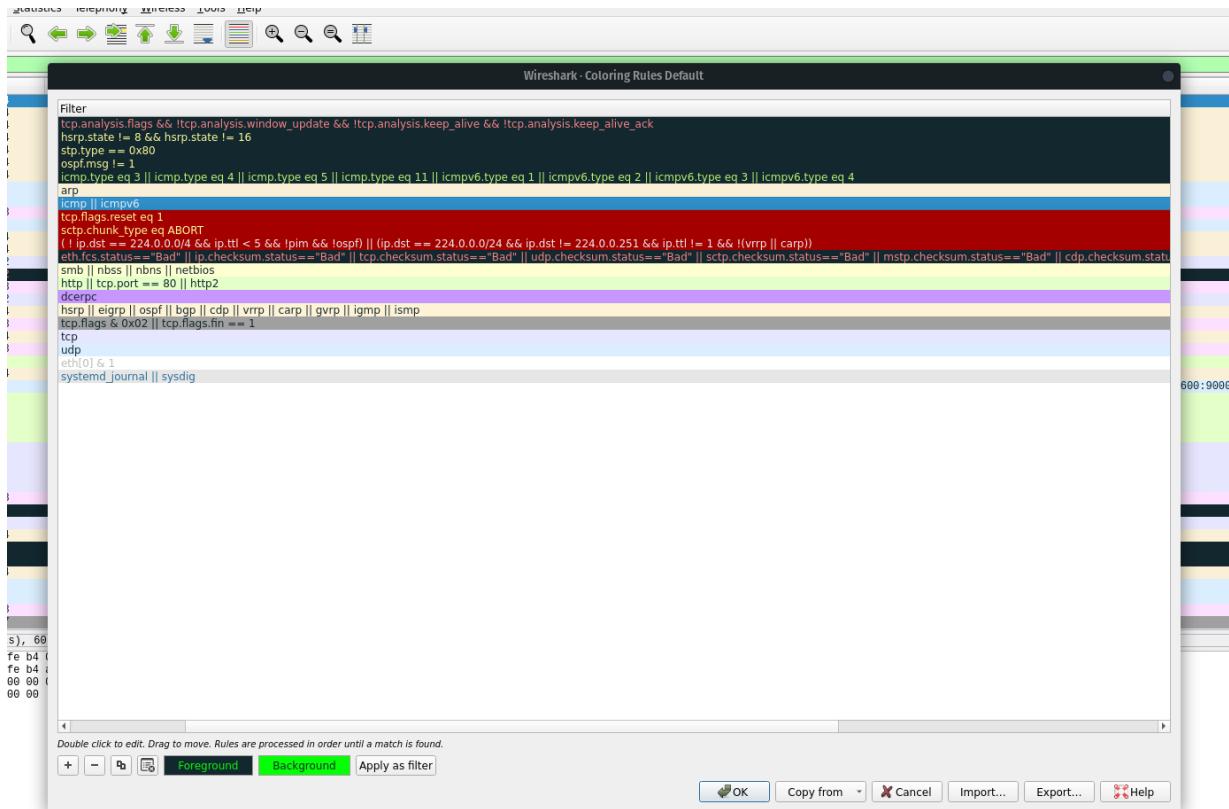
The Wireshark interface displays a list of captured network frames. The selected frame (Frame 16) is highlighted in green. The details pane shows the frame structure, including the source MAC address (Sophos_6b:fe:b4), destination (Broadcast), and type (ARP). The bytes pane shows the raw hex and ASCII data of the frame.

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)



The screenshot shows a Wireshark capture session with the following details:

- Workspaces**: Applications
- File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help**
- Interface**: wlp0s0f3
- Panels:**
 - Frame 111 - 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s0f3, id 0**
 - Details**: Shows fields like Time, Source, Destination, Protocol, Length, Info, and hex dump.
 - Bytes**: Hex and ASCII dump of the captured data.
- Status Bar**: 111 frames, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s0f3, id 0

0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 1^%\$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 39 31 32 33 34 35 &(')*+, ./012345
0060 36 37 67

[DOWNLOAD VIDEO](#)

[DOWNLOAD VIDEO](#)

Internet Control Message Protocol: Protocol Packets: 35637 · Displayed: 159 (0.4%) Profile: Default

5. Filter Http and tcp packets.

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

Wireshark interface showing captured traffic. The filter toolbar at the top has "http and tcp" selected. The main pane displays a list of network frames, mostly HTTP and TCP packets, with some OSCP and ICMP messages interspersed. The packet details, bytes, and error columns are visible below the list.

Wireshark interface showing captured traffic. The filter toolbar at the top has "http and tcp" selected. The main pane displays a list of network frames, mostly HTTP and TCP packets, with some OSCP and ICMP messages interspersed. The packet details, bytes, and error columns are visible below the list.

6. Filter DHCP packets

Same as before enter “dhcp” in filter toolbar

No.	Time	Source	Destination	Protocol	Length	Info
3794	148.277455795	172.18.141.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe0573782
4135	163.637053335	172.18.141.10	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x4f1069c9
4808	193.540752428	172.18.141.10	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xa2ccd3d
4883	195.389772294	172.18.141.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xdf49b362
7588	313.553295486	172.18.141.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1850c6a1
12541	473.299361755	172.18.141.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xcb30d959
12767	476.987783545	172.18.141.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xcb30d959
13344	485.587651508	172.18.141.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xcb30d959
13356	485.794161302	172.18.141.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xcb30d959
14353	507.091756253	172.18.141.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x6b1bce60
29053	764.530749235	172.18.141.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x9ddd3ca4
31164	818.596784062	172.18.141.10	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xce548d5b
31195	819.622611912	172.18.141.10	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xce548d5b
32616	880.242457674	172.18.141.10	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xc1ab1702
35652	1014.3892597...	172.18.141.10	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xd431961a

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

Sep 18 11:36 PM *wlp0s20f3

lan@pop-os:~\$ ping google.co.in

PING google.co.in (142.250.195.131) 56(84) bytes of data.

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=1 ttl=117 time=93.3 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=2 ttl=117 time=225 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=3 ttl=117 time=27.1 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=4 ttl=117 time=169 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=5 ttl=117 time=31.3 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=6 ttl=117 time=215 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=7 ttl=117 time=27.2 ms

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=8 ttl=117 time=157 ms

Frame 531: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s20f3, id 0

0000 00 1a 8c 6b fe b4 f6 0d 9e 50 b8 8c 08 45 08 .k...P...E

0001 00 54 d2 8f 40 08 40 01 da 7e ac 12 0f 0a 8e fa T-0-0-~-----

0002 c3 83 00 00 a8 07 00 04 00 01 5e 00 00 00 00 00 ..^c-----

0003 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..`-----

0004 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!%\$%

0005 00 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 8'(*+,-./012345

0006 36 37

Internet Control Message Protocol: Protocol

DOWNLOAD VIDEO

Packets: 691 - Displayed: 16 (2.3%)

Profile: Default

Sep 18 11:36 PM *wlp0s20f3

lan@pop-os:~\$ ping google.co.in

PING google.co.in (142.250.195.131) 56(84) bytes of data.

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=1 ttl=117 (request in 531)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=2 ttl=117 (request in 531)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=3 ttl=117 (request in 556)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=4 ttl=117 (request in 576)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=5 ttl=117 (request in 576)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=6 ttl=117 (request in 597)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=7 ttl=117 (request in 707)

64 bytes from maa03s40-in-f3.le100.net (142.250.195.131): icmp_seq=8 ttl=117 (request in 723)

Frame 598: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp0s20f3, id 0

0000 t6 0d 9e 50 b8 8c 00 1a 8c 6b fe b4 08 45 60 .P...K...E

0001 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..`-----

0002 08 00 00 75 95 00 04 00 04 10 00 27 63 00 00 00 ..U-----

0003 00 00 91 ce 02 00 00 00 00 00 00 11 12 13 14 15 ..`-----

0004 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!%\$%

0005 00 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 8'(*+,-./012345

0006 36 37

Internet Control Message Protocol: Protocol

DOWNLOAD VIDEO

Packets: 1338 - Displayed: 73 (5.5%)

Profile: Default