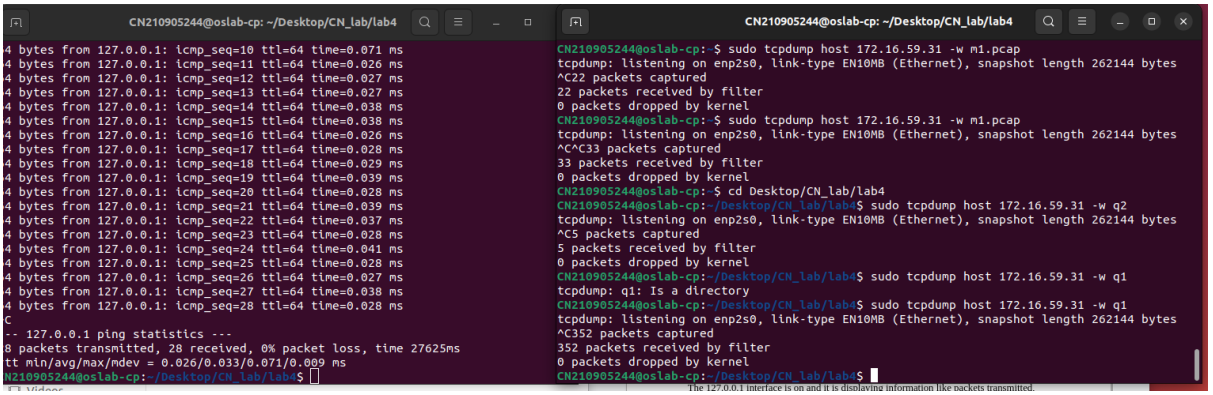
**LAB NO: 4** **Aditi Shrivastava-210905244**

**Network Data Analysis using tcpdump**

Network Analysis tools are used to identify problems in the network, as well as to help understand the behaviour of network protocols.
Tcpdump is a network traffic sniffer built on the packet capture library libpcap.

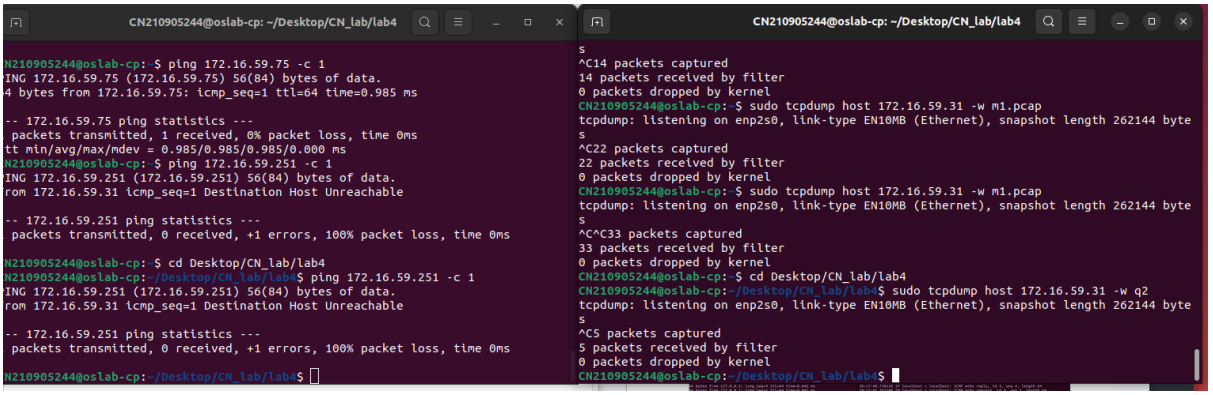
1. While tcpdump host your_host is running in one command window, run ping 127.0.0.1 from another command window. From the ping output, is the 127.0.0.1 interface on? Can you see any ICMP message sent from your host in the tcpdump output? Why?

**Answer**:

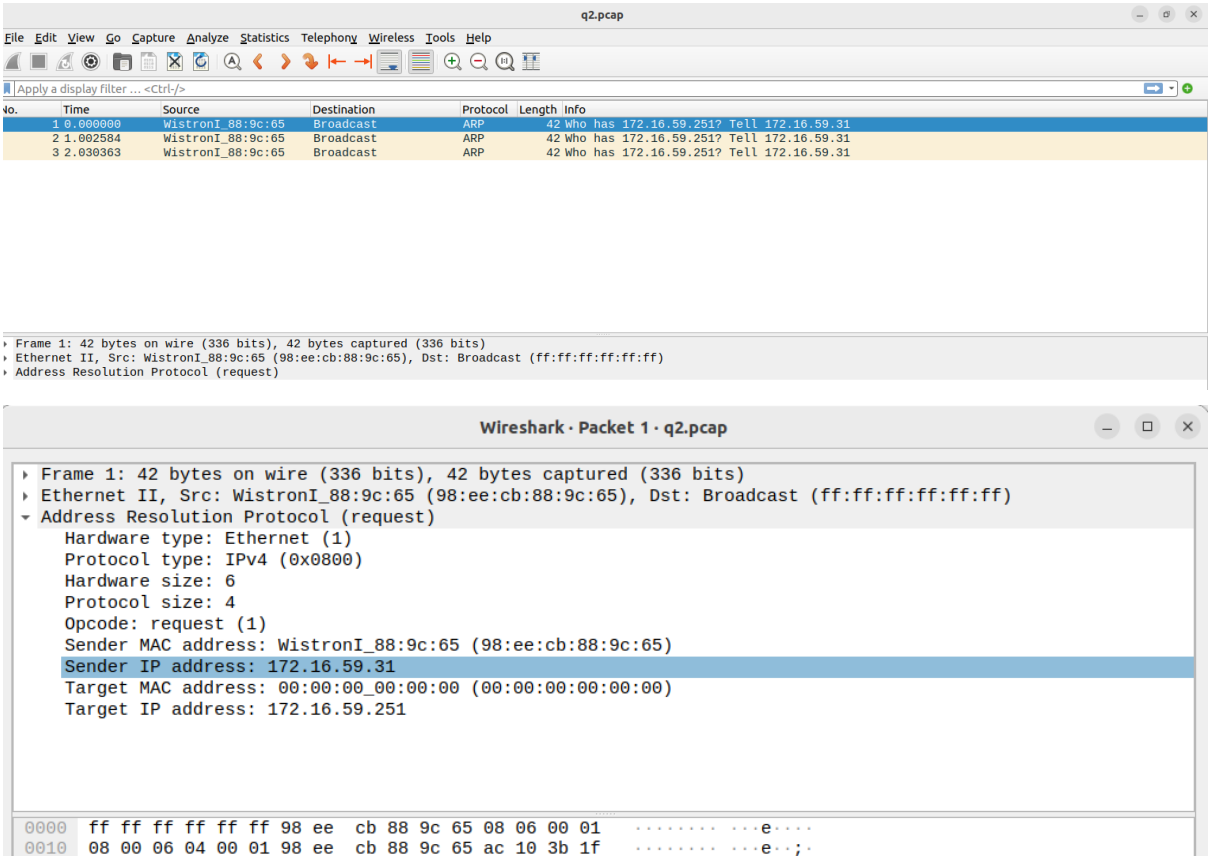



The 127.0.0.1 interface is on and it is displaying information like packets transmitted, received, loss and time. The ICMP message will not be displayed on the tcpdump host terminal because the connection is local.

2. While tcpdump host your_host is running to capture traffic from your machine, execute telnet 128.238.66.200. Note there is no host with this IP address in the current configuration of the lab network. Save the tcpdump output of the first few packets for the lab report. After getting the necessary output, terminate the telnet session. From the saved tcpdump output, describe how the ARP timeout and retransmission were performed. How many attempts were made to resolve a non-existing IP address?




Host terminal command: sudo tcpdump host 172.16.59.31 -w q2
Ping terminal command: ping 172.16.59.251 -c 1




Three Attempts were made by the host to find the MAC information of the non existent IP address.

3. Briefly explain the purposes of the following tcpdump expressions.

a. tcpdump udp port 520

- Used to display only the UDP packets received at port number 520

**-X** : Show the packet's *contents* in both **hex** and **ASCII**.

**-s** : Define the *snaplength* (size) of the capture in bytes. Use -s0 to get everything, unless you are intentionally capturing less.

Specific protocols can be filtered using the proto directive or by using the protocol name directly.

b. tcpdump -x -s 120 ip proto 89

- Capturing 120 snaplength of protocol 89 will be displayed in both hex and ASCII.

c. tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)

- Capturing 70 snaplength of host's IP address and the IP address1 or IP address2 in hex and ASCII

d. tcpdump -x -s 70 host ip addr1 and not ip addr2

- Capturing 70 snaplength of host's IP address and not IP address2 in hex and ASCII

4. Basic packet decoding

1) Write a tcpdump command to dump network traffic from an Ethernet connection to the screen in human readable output format. Perform the following operation and write down the observations.

a) Capture all the traffic of maximum snap length of 65,535 bytes and provide the hexadecimal and ASCII decodes of all the traffic in each packet.

b) Find the IP addresses, IP packet length, TCP port numbers, TCP flags, etc. by using the reference chart to locate those fields on the hexadecimal dump.