**Assignment**

ARP

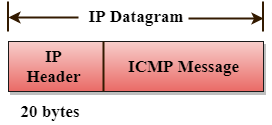
* ARP stands for Address Resolution Protocol.
* It is used to associate an IP address with the MAC address.
* Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC addresses can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but the IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

### How ARP works

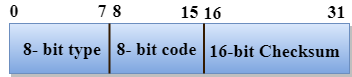
If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcasts it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends it back to the sender.

## ICMP

* ICMP stands for Internet Control Message Protocol.
* The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
* ICMP uses echo test/reply to check whether the destination is reachable and responding.
* ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
* An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
* ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
* ICMP messages are transmitted within an IP datagram.



### The Format of an ICMP message



* The first field specifies the type of the message.
* The second field specifies the reason for a particular message type.
* The checksum field covers the entire ICMP message.

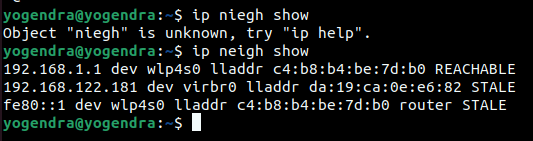
**ARP table list in our system:**

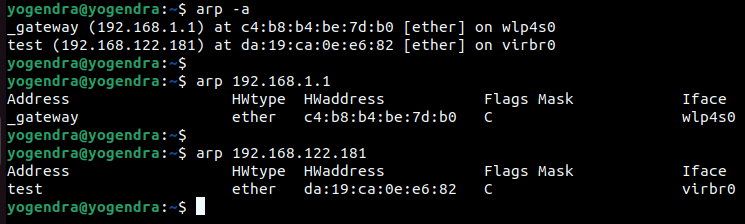
yogendra@yogendra:~$ **ip neigh show**

192.168.1.1 dev wlp4s0 lladdr c4:b8:b4:be:7d:b0 REACHABLE

192.168.122.181 dev virbr0 lladdr da:19:ca:0e:e6:82 STALE

fe80::1 dev wlp4s0 lladdr c4:b8:b4:be:7d:b0 router STALE

****

****

**ICMP Command:**

**Ping→**

**TCP Dump:**

yogendra@yogendra:~$ sudo tcpdump -i wlp4s0 -n -v -w test\_dump.pcap

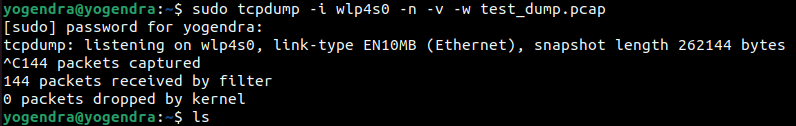
[sudo] password for yogendra:

tcpdump: listening on wlp4s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

^C144 packets captured

144 packets received by filter

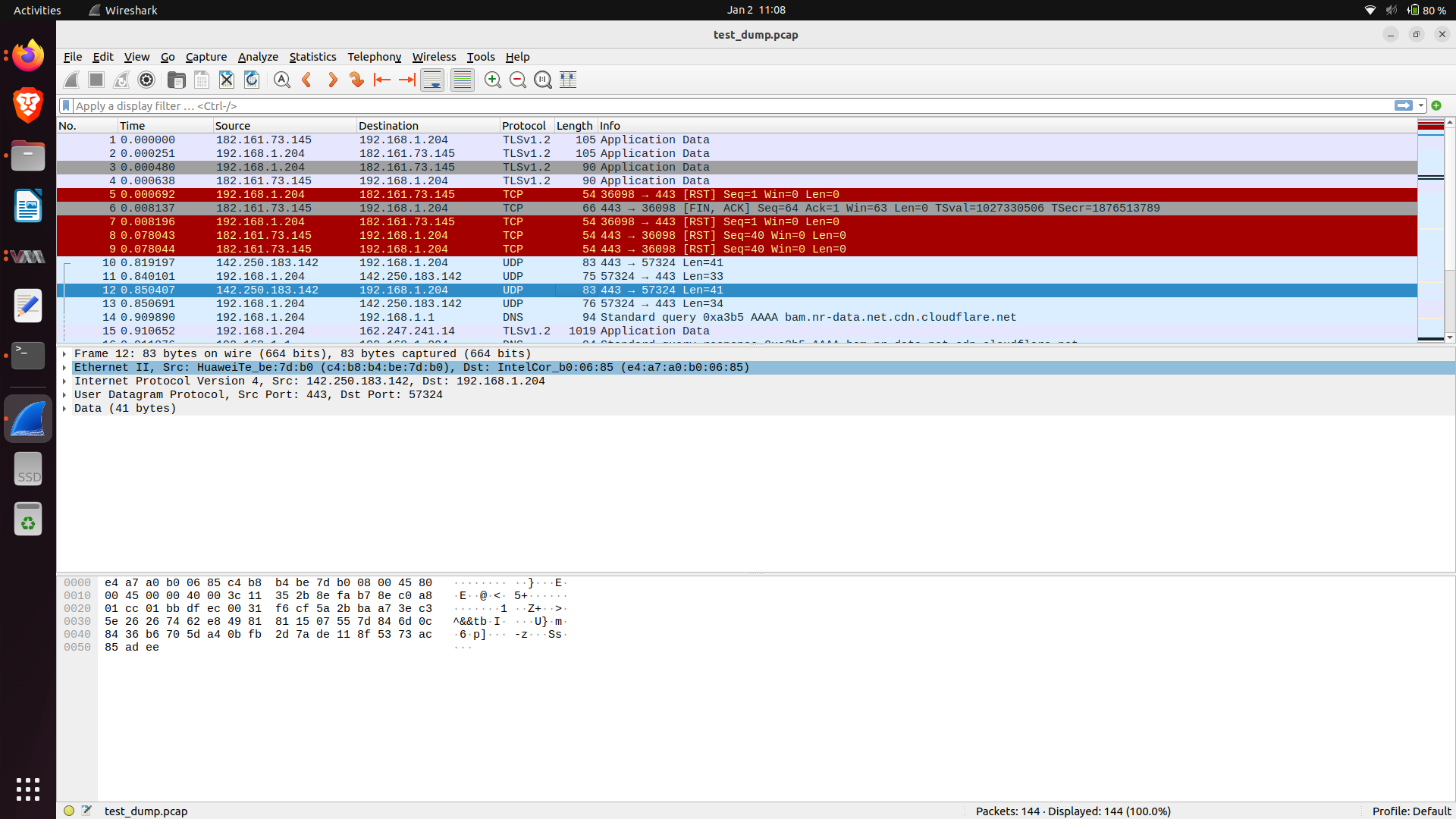
0 packets dropped by kernel

****

yogendra@yogendra:~$ **ls**

crontab Desktop Documents Downloads gitea guacamole known\_hosts.old Music mygov mysql Pictures Public session snap sumit Templates **test\_dump.pcap** Videos

yogendra@yogendra:~$ **wireshark test\_dump.pcap**

****

==========================================================================

### 