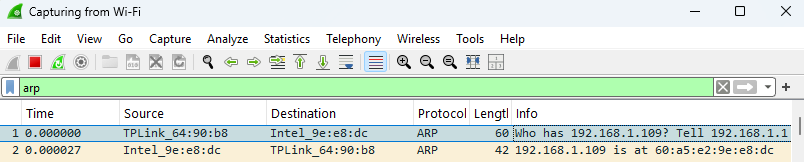
Question 1

Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.

Approach:

We are asked to capture the ARP packet using wireshark. Once you start the wireshark apply a arp filter to analyse the arp packets.

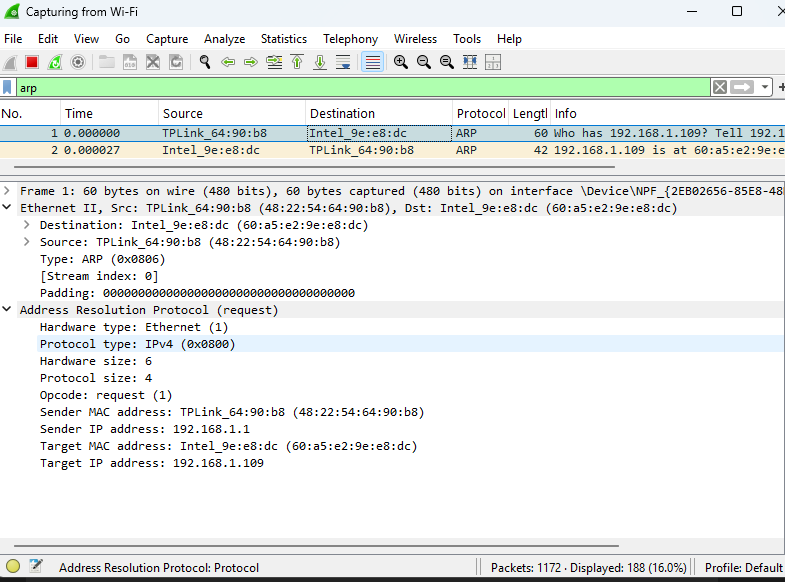


The flow goes like below

* The router will send an ARP request requesting the mac address of our machine.
* The ARP request consist of
  + Hardware type
  + Protocol type (Ip version)
  + Hardware size
  + Protocol size
  + Opcode
  + Sender’s MAC address
  + Sender’s IP address
  + Receiver MAC address
  + Receiver IP address
* The router will fill all details leaving Receiver MAC address. The packet will be broadcast to all host in the network. The host which has Receiver ip will respond back by giving reply to particular ip which is in sender ip address. The router will receive the packet and will the MAC address of the desired ip holder in the arp table
* We also have some other terms in arp packet
  + Hardware type:
    - This will tell the hardware type used for communication (Ethernet)
  + Protocol Type
    - This will tell the protocol which is used for communication (Internet Protocol)
  + Hardware Size
    - This will tell the size of MAC address (6 bytes)
  + Protocol Size
    - This will tell the size of protocol used (4 bytes for IP)
  + Opcode
    - This is the operation code used for understanding
      * 1 – Request
      * 2 – Reply
  + Sender MAC address
    - MAC address of the router
  + Sender IP address
    - IP address of the router
  + Receiver MAC address
    - The MAC address of the receiver. It is empty initially. But will be filled and send back to router with help of sender mac address and ip address in ARP reply
  + Receiver IP address
    - This is host ip address which is going to respond to request with sender mac address, IP, and receiver MAC address.
* Once the reply is received to router the router will fill the arp table for further communication
* Here ARP request plays important role in helping ARP table

Below I attached the ARP request and ARP reply that has been captured in wireshark

ARP Request (Who has 192.168.1.109? tell 192.168.1.1)



ARP reply (192.168.1.109 is at 60:a5:e2:9e:e8:dc)

