Question 1

Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address.

Discuss the importance of ARP in packet forwarding.

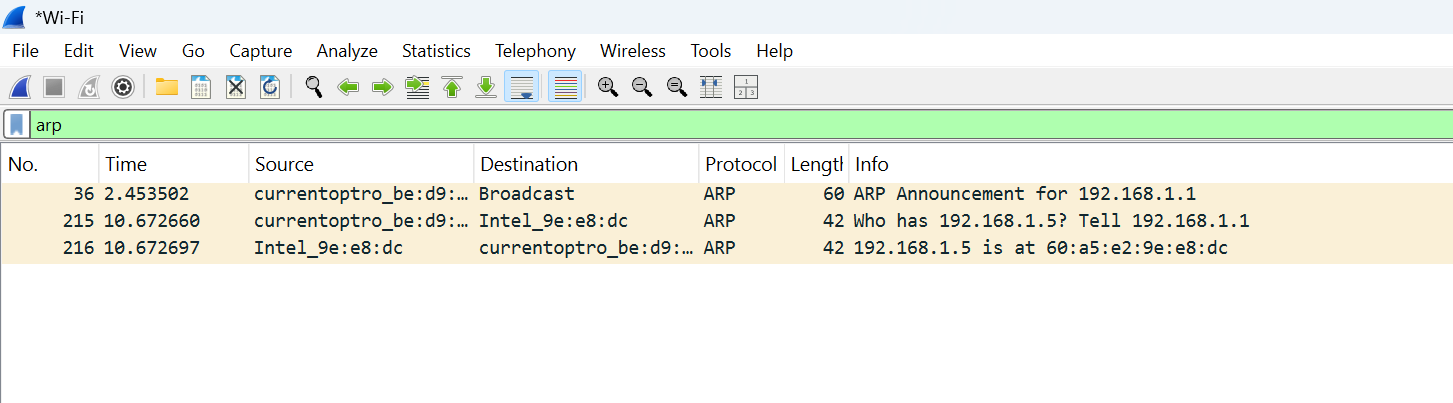
Approach

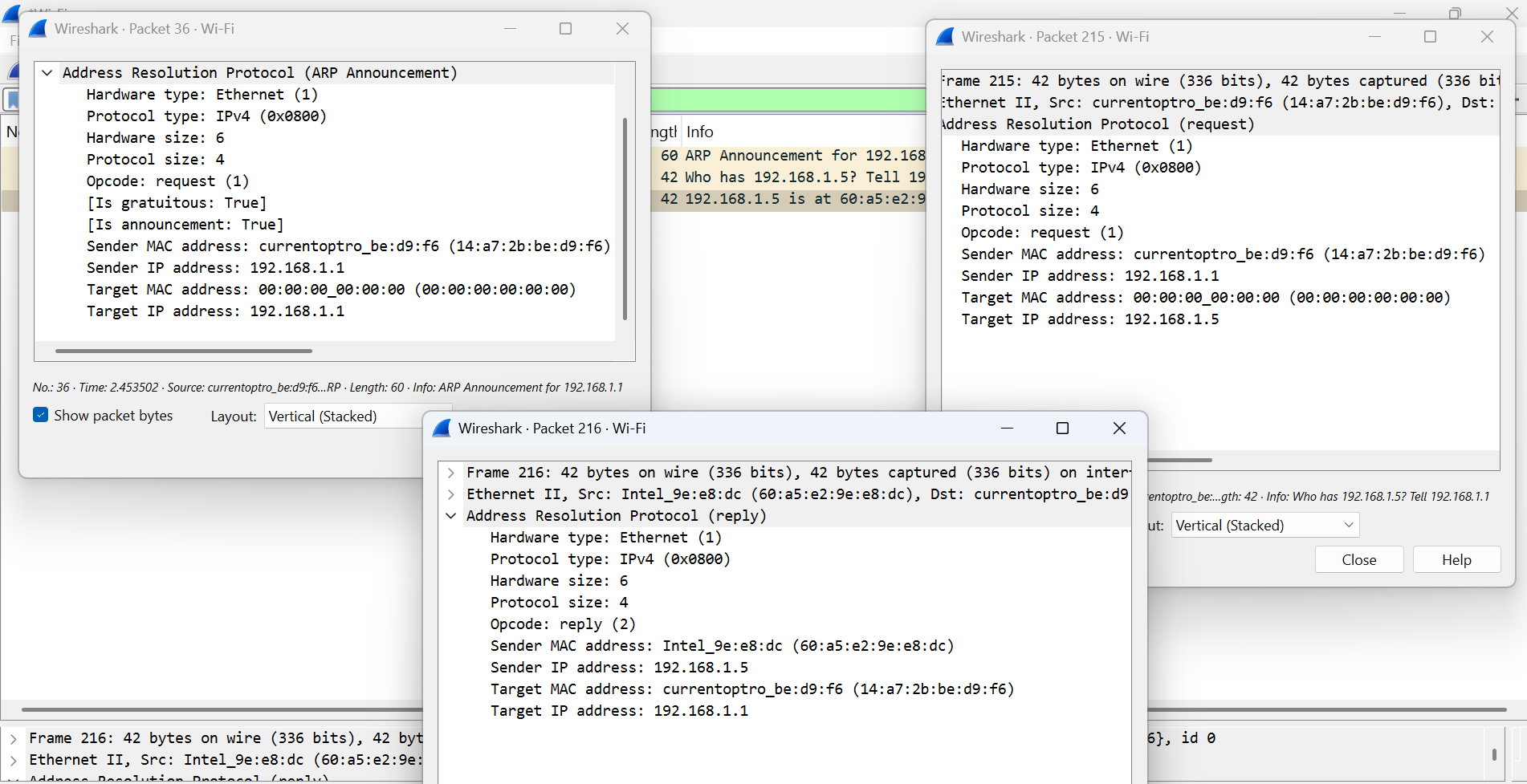
To start with, we are capturing the packet with wireshark. Ping the router ip address, and apply arp filter in wireshark.

You can see that a packet is broadcast with a announcement for router ip address

The next packet is the reply packet received from the router, It ask for the mac address who has the particular ip address (192.168.1.5)

The local machine reply with opcode 2 highlighting the mac address itself.





The Address Resolution Protocol (ARP) is essential for network communication, enabling devices to map IP addresses to MAC addresses. When a device wants to send a packet, it first checks its ARP cache; if the MAC address isn't found, it sends a broadcast ARP request. The destination device responds with an ARP reply, allowing direct communication within the subnet. In packet forwarding, ARP helps devices locate the MAC address of the default gateway, ensuring smooth data transmission across networks. Without ARP, devices wouldn’t know where to send packets, leading to network failures. Routers also rely on ARP to determine the next-hop MAC address for forwarding traffic between subnets. ARP caching optimizes network efficiency by storing recent mappings, reducing unnecessary broadcast traffic. However, ARP spoofing attacks can compromise security, making protective measures like dynamic ARP inspection necessary. Despite its vulnerabilities, ARP remains a crucial protocol in modern networking. Its role in resolving addresses ensures seamless data flow in both local and large-scale networks.