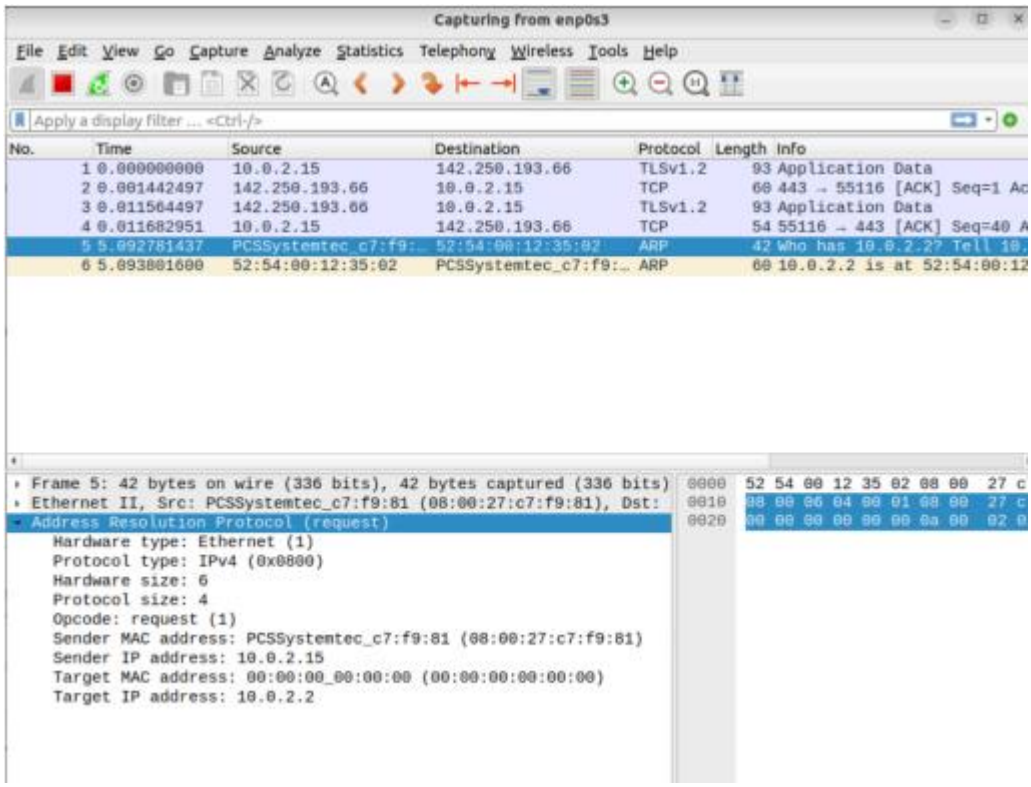
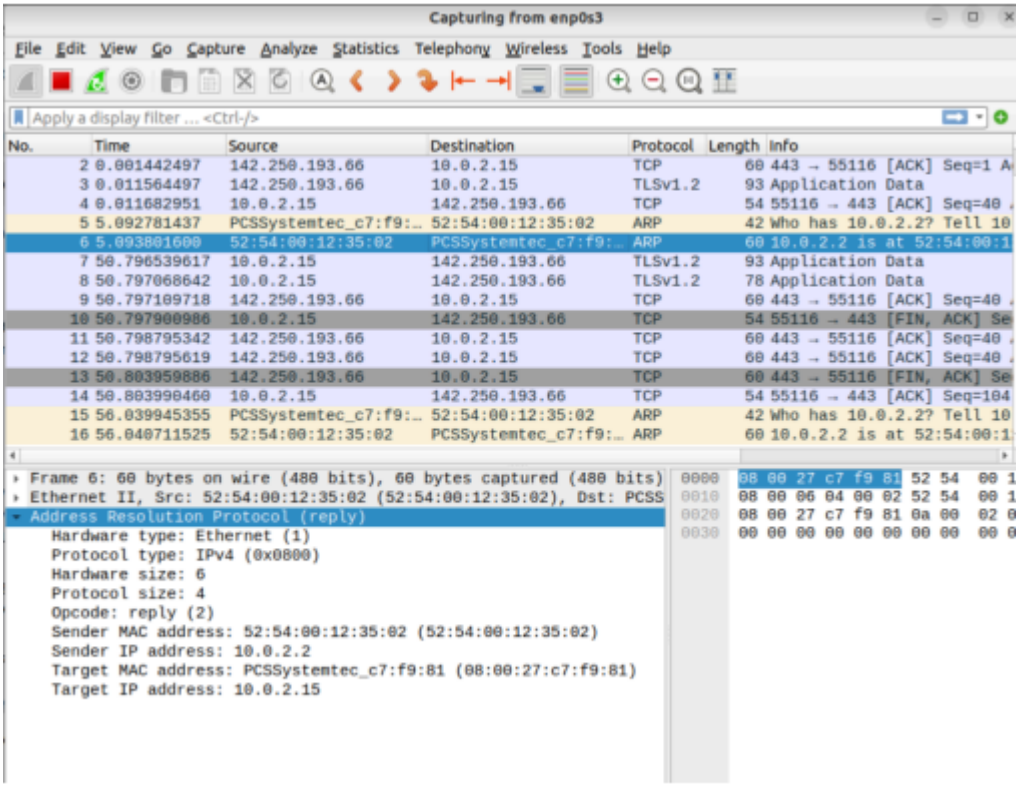
ARP Poisoning

i). Suppose you have two machines A and B on the same network (take Virtual Machines for the same). Machine A (Client) wants to communicate with Machine B (Server) but is unaware about the MAC address of B. Hence, it sends an ARP broadcast request. Use wireshark to study and analyse the ARP packet information. In detail, explain all the fields of an ARP packet.

In this scenario, Machine A (the client) wants to communicate with Machine B (the server) on the same network but doesn't know the MAC address of Machine B. To find out the MAC address, Machine A sends an ARP (Address Resolution Protocol) broadcast request.

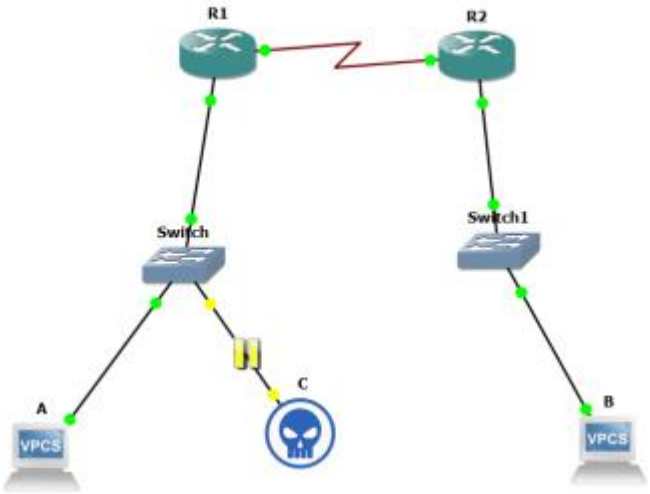
1. Machine A broadcasts an ARP request packet to all devices on the local network. This ARP request contains Machine A's IP address and MAC address
2. Machine B, upon receiving the ARP request and recognizing its own IP address, responds with its MAC address directly to Machine A. This response is unicast, meaning it's sent only to Machine A.
3. Upon receiving the response, Machine A updates its ARP cache with the MAC address of Machine B. This allows Machine A to communicate directly with Machine B in subsequent network communications without needing to perform another ARP broadcast





ii). Consider Machines A and B on different networks. Consider another machine C (you may take it as a default gateway). Create a scenario in which ARP MAC entry corresponding to Machine B is poisoned in the local ARP cache of Machine A and instead a MAC entry of Machine C is placed and returned. Similarly, to Machine B, the corresponding entry to Machine C is there instead of A. (Machine C acting as a mediator and performing the Man-in-the-Middle attack). Show the packet transmission being carried out after ARP Poisoning.

Initial Setup: Machines A and B are on different networks. Machine C is positioned between A and the gateway/router for A's network.



ARP Poisoning: Machine C sends ARP spoofed packets to Machine A and the router, claiming to be the router. Both Machine A and the router update their ARP cache with Machine C's MAC address associated with the router's IP address.

Man-in-the-Middle Setup: Machine C now intercepts traffic between Machine A and the router.

Packet Transmission from A to C to B: When A wants to communicate with B, it sends packets to the router, but they're intercepted by C. C inspects/modifies the packets and forwards them to B.

MitM Attack Execution: B responds to the intercepted packets, thinking they're from the router. C intercepts these responses, potentially modifying them, before forwarding them to A.

Inspection and Manipulation: Throughout, C can inspect, modify, or drop packets, potentially compromising the communication between A and B