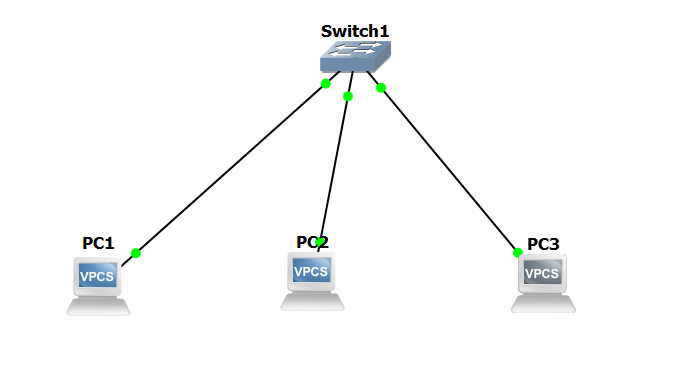
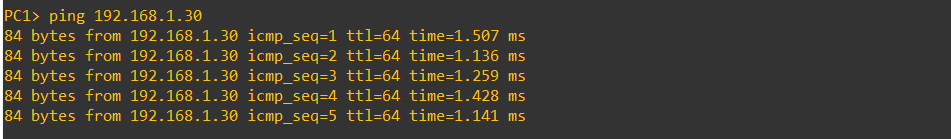
**Capture and analyze Ethernet frames using Wireshark. Inspect the structure of the frame, including destination and source MAC addresses, Ethertype, payload, and FCS Use GNS3 or Packet Tracer to simulate network traffic.**

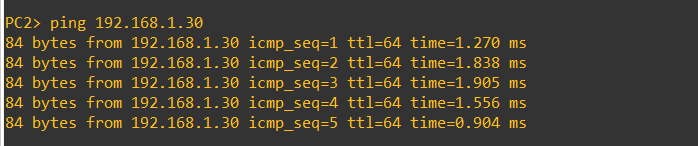
****

**Traffic Generation:**

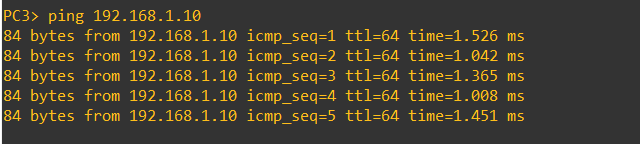
**Pinging PC1🡪 PC3**

****

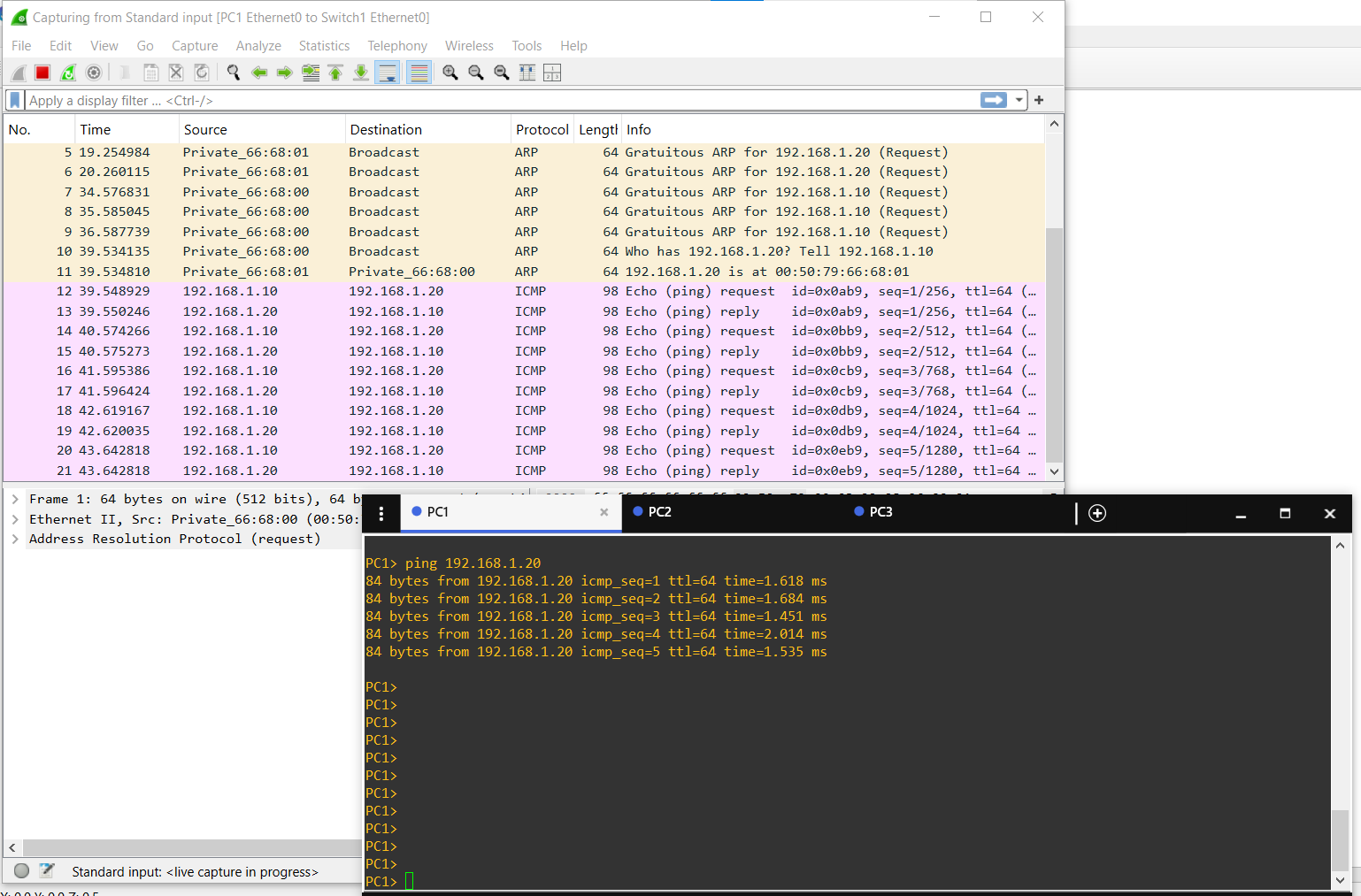
**Pinging PC2🡪PC3**

****

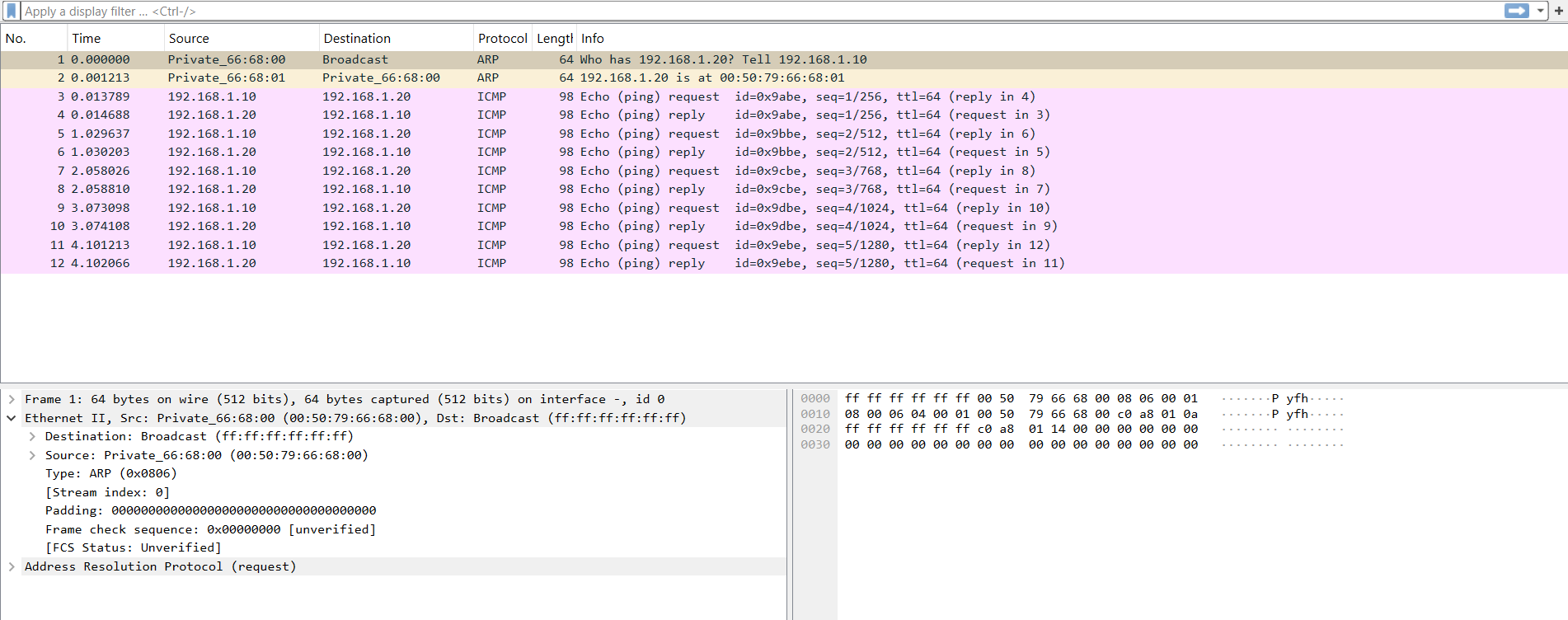
**Pinging PC3🡪PC1**

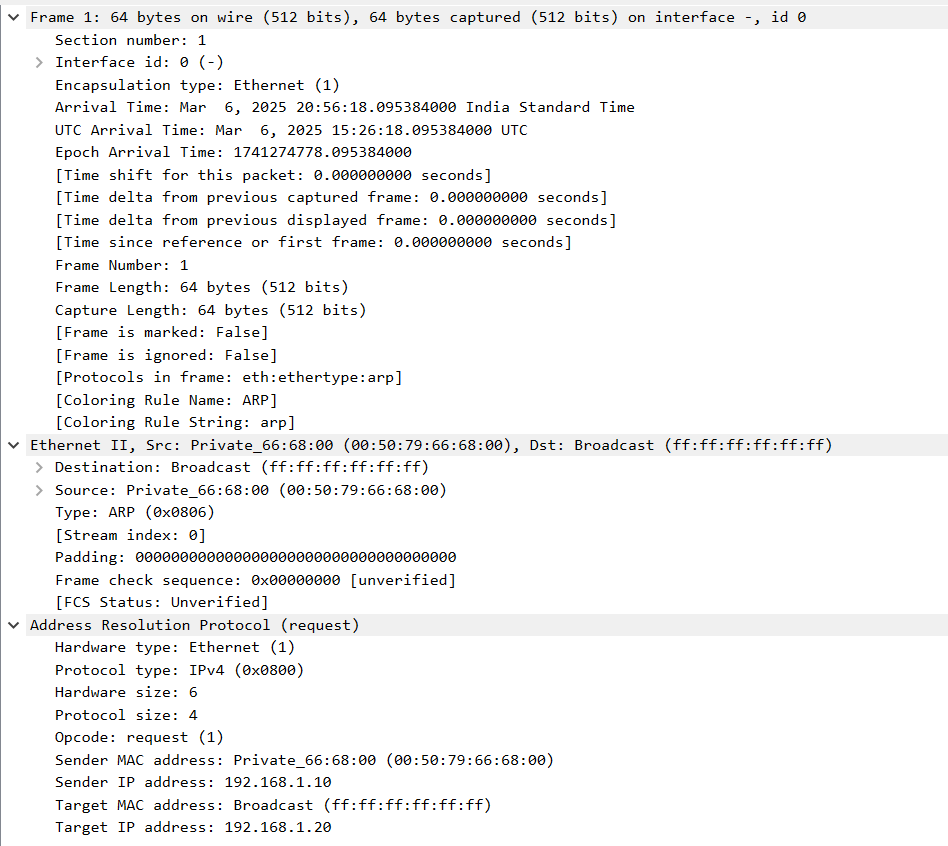
****

**Capturing Packets:**

****

**Frame Details:**

****

****

**Observation:**

* The captured frame is an ARP request sent by a device with the MAC address 00:50:79:66:68:00.
* The destination MAC address is ff:ff:ff:ff:ff:ff, meaning it is a broadcast message.
* The sender IP address is 192.168.1.10, and it is asking for the MAC address of 192.168.1.20.
* The Ethernet frame encapsulates an ARP packet, as indicated by the Ethertype value 0x0806.
* The FCS (Frame Check Sequence) is unverified.
* The system sending the ARP request does not yet know the MAC address of 192.168.1.20, which is why it is broadcasting the request.
* There is no ARP reply in this capture, meaning 192.168.1.20 either did not receive or did not respond to the request.