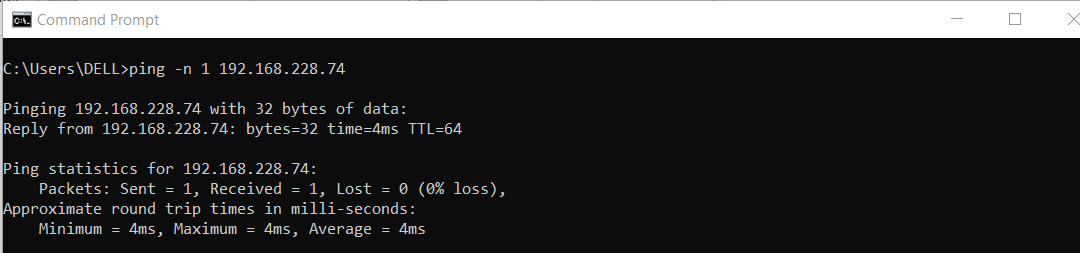
**Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.**

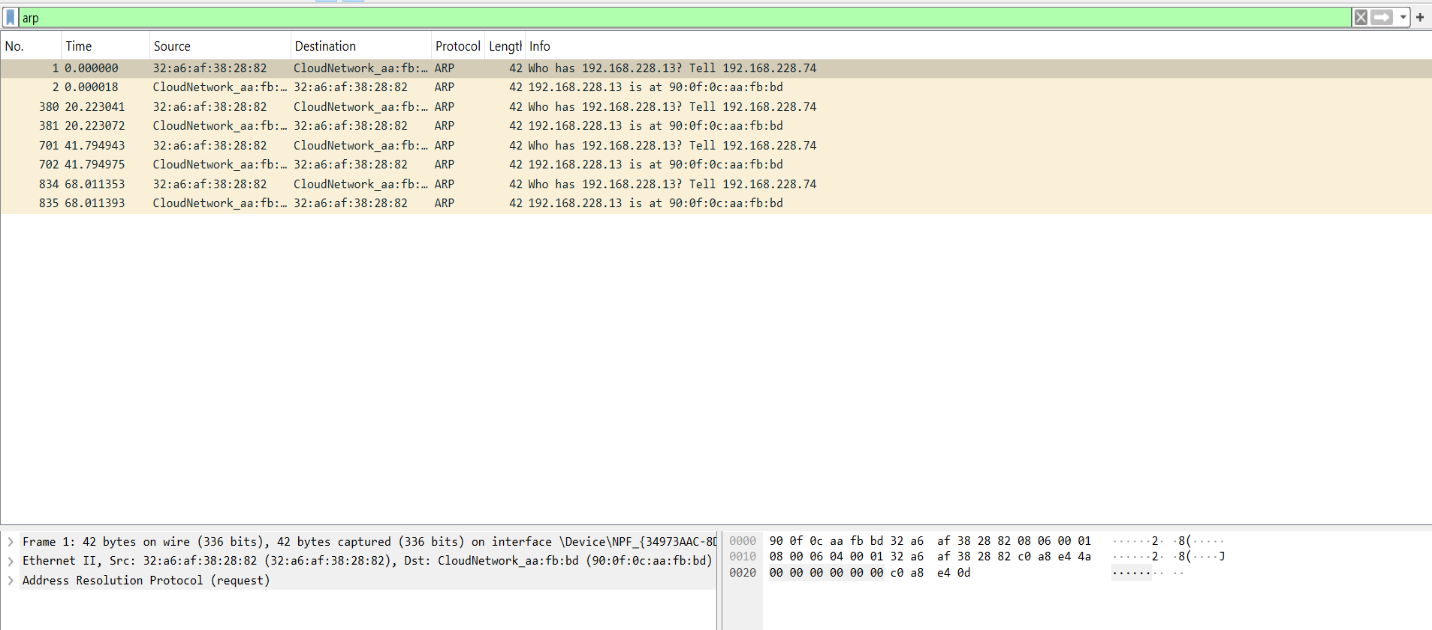
ARP (Address Resolution Protocol) is what helps a device figure out the MAC address of another device on the same network when all it has is the IP address.

I used ping to check if 192.168.228.74 was reachable. But before the actual ping packets (ICMP) could be sent, my system had to resolve the MAC address using ARP. This is why the ARP packets appeared in Wireshark.

**Pinging 192.168.228.74:**

****

**Capturing ARP Packets:**

****

**Observation:**

1. My system didn’t already know the MAC address of 192.168.228.74, it sent an ARP request.
2. The target device responded with its MAC address (90:0f:0c:aa:fb:bd), which my system then stored for future communication.
3. Now that my system knew the MAC address, it successfully sent ICMP packets, and I got a reply with 4ms response time.

**In Wireshark, I captured both the ARP request and reply:**

* ARP Request: My system (MAC: 32:a6:af:38:28:82) sent a broadcast message asking, "Who has 192.168.228.74? Tell me your MAC address."
* ARP Reply: The device using IP 192.168.228.74 responded with its MAC address: 90:0f:0c:aa:fb:bd.