Wireshark Network Traffic Analysis Report

Objective: Capture live network packets using Wireshark and identify at least 3 different protocols for basic network traffic analysis.

Tool Used: Wireshark

File Analyzed: networkcapture.pcapng

Protocols Identified:

1. **TCP (Transmission Control Protocol):**
   - TCP is a connection-oriented protocol that ensures reliable communication between devices.
   - Commonly used for applications that require guaranteed delivery like web browsing, email, etc.

2. **ARP (Address Resolution Protocol):**
   - ARP is used to map IP addresses to MAC addresses within a local network.
   - Observed when the system looked up MAC addresses for nearby devices.

3. **IGMP (Internet Group Management Protocol):**
   - IGMP is used by IP hosts and adjacent routers to establish multicast group memberships.
   - Seen when the system communicated with multicast groups.

Sample Packet Details:

No.	Protocol	Source IP	Destination IP	Info
10	TCP	192.168.0.10	93.184.216.34	TCP handshake initiation

| 23 | ARP | 192.168.0.10 | Broadcast | Who has 192.168.0.1? Tell 192.168.0.10 |

| 35 | IGMP | 192.168.0.10 | 224.0.0.1 | Membership Report / Join Multicast |

Conclusion:

The network capture demonstrates successful identification of diverse protocol types: TCP (transport layer), ARP (link layer), and IGMP (network layer). These protocols serve different purposes and understanding them helps in analyzing network behavior, device communication, and multicast traffic.