TASK-5

1. Capture Information
Capture File: wifi1.pcapng
Capture Interface: Wi-Fi (owned)]
Capture Duration: Approximately 3 minute
Total Protocols Identified: 4
2. Protocols Identified and Analysis
2.1 ARP (Address Resolution Protocol)
ARP is a network layer protocol used to resolve IP addresses to MAC (hardware) addresses. It is essential for communication within a local network. During the capture, several ARP requests and replies were observed, which is typical behavior as devices discover and communicate with each other.
Example: 'Who has 192.168.0.1? Tell 192.168.0.105'
2.2 QUIC (Quick UDP Internet Connections)
QUIC is a modern transport layer protocol developed by Google that operates over UDP. It offers reduced connection times and improved security. It is used by web applications that support HTTP/3. The capture shows that the system likely accessed web content served over QUIC, indicating browser-based activity (e.g., Google, YouTube).
2.3 ICMPv6 (Internet Control Message Protocol for IPv6)
ICMPv6 is used in IPv6 networks to report errors and perform diagnostic functions. It also plays a role in the Neighbor Discovery Protocol, which replaces ARP in IPv6. During the capture, ICMPv6 messages were seen, indicating the presence of IPv6-enabled devices and routing messages.
2.4 DNS (Domain Name System)
DNS is an application layer protocol responsible for translating human-friendly domain names (e.g., google.com) into IP addresses. Several DNS queries and responses were captured, which is expected when browsing the internet or launching network-aware applications.
3. General Observations
The captured traffic reflects typical residential or enterprise network activity. The presence of both ARP and ICMPv6 shows a dual-stack (IPv4 and IPv6) environment. QUIC traffic suggests modern web browsing behavior, while DNS traffic confirms name resolution for multiple hosts.
4. Recommendations
• Monitor QUIC traffic for potential encrypted tunnels or misuse.
• Consider implementing DNS over HTTPS (DoH) for improved privacy.
• Enable ARP spoofing detection for enhanced local network security.
• Log and analyze ICMPv6 traffic periodically to detect unusual IPv6 activity.