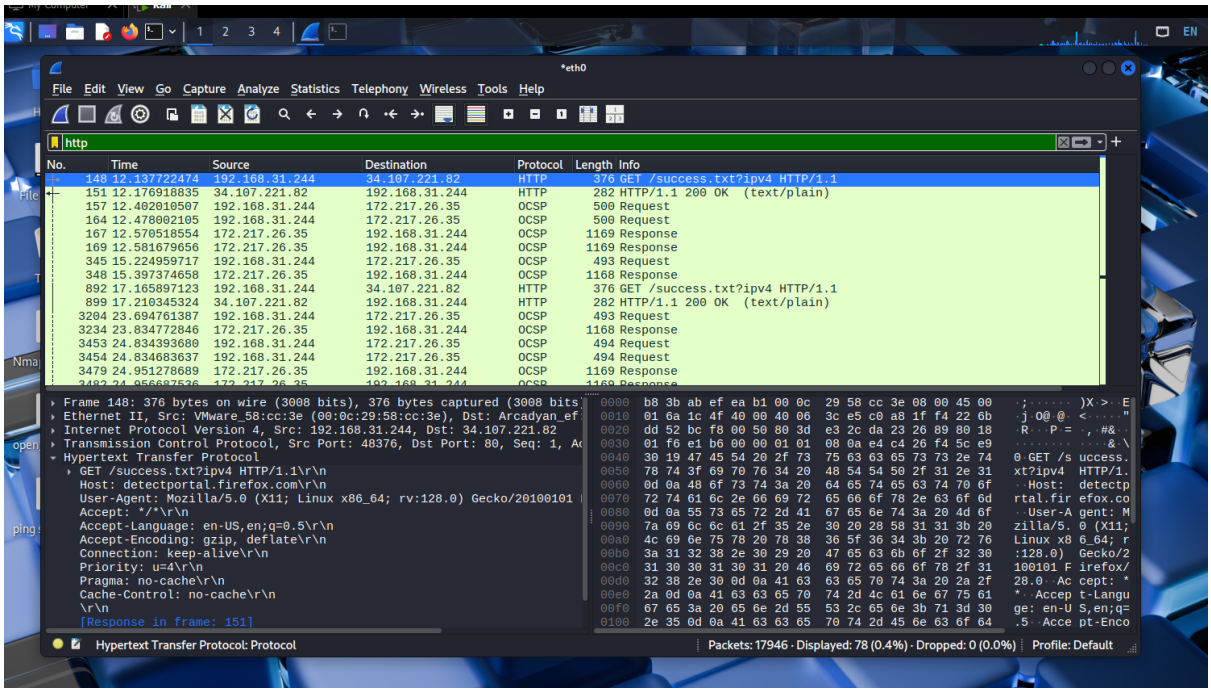
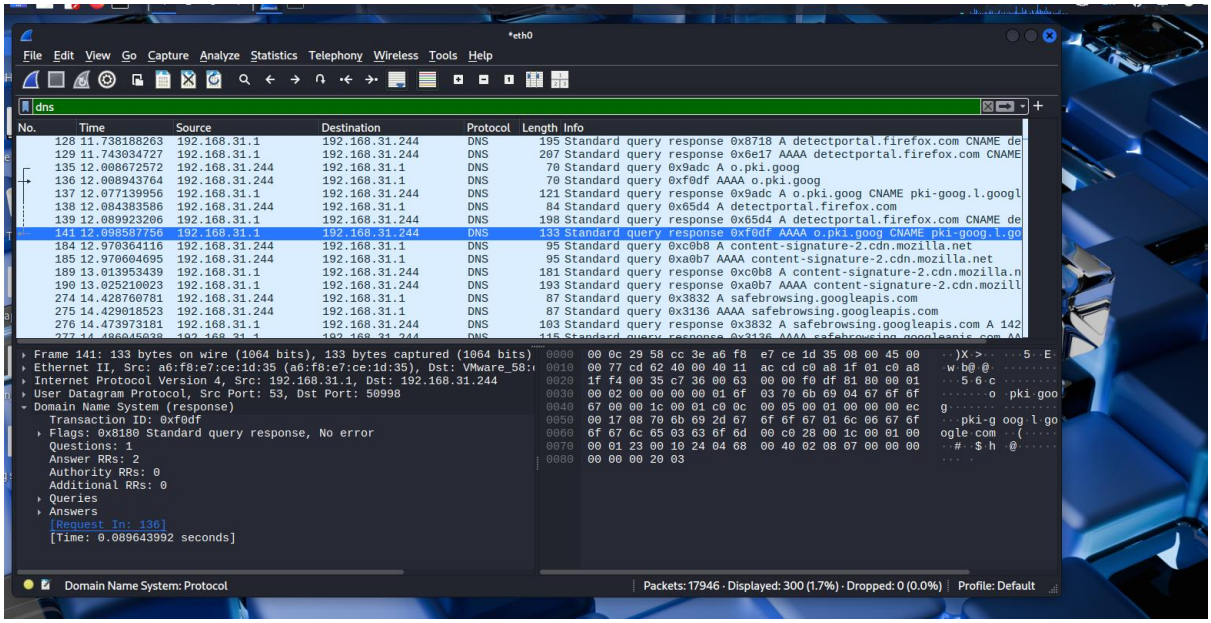
TASK 5

Wireshark

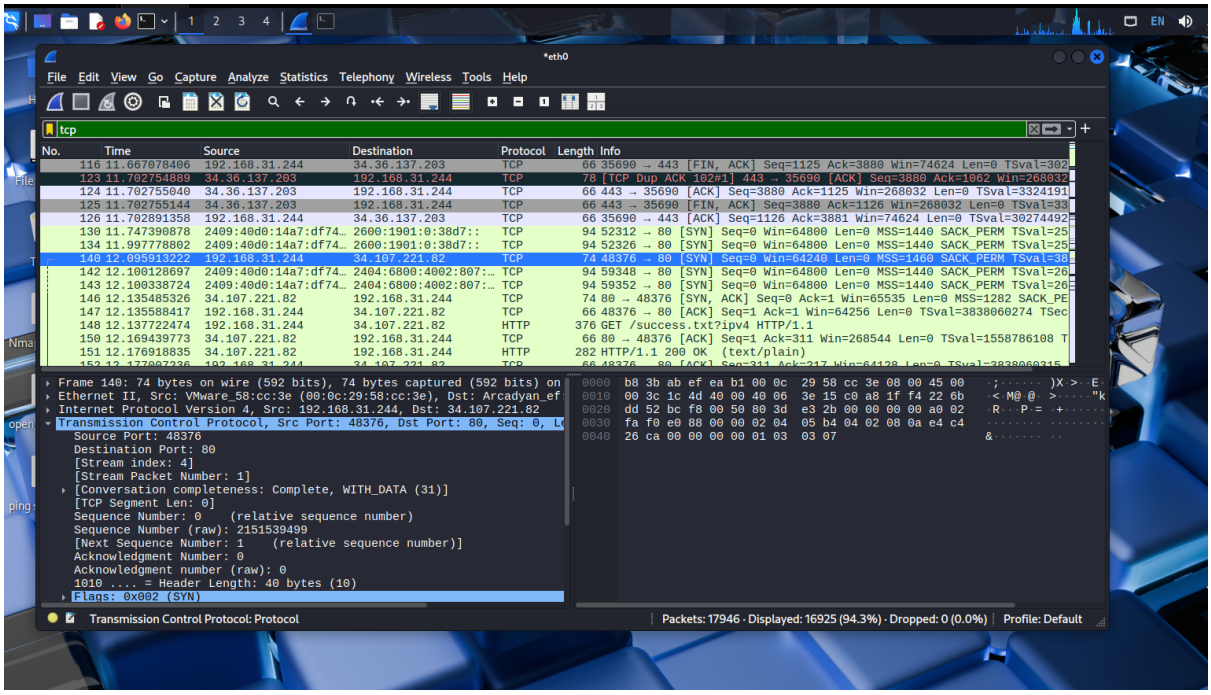
1. HTTP (http) – This filter shows only HTTP traffic, typically on port 80, which is used for unencrypted web communication. It allows you to view website requests such as GET and POST, along with server responses, making it easy to study how a webpage loads.



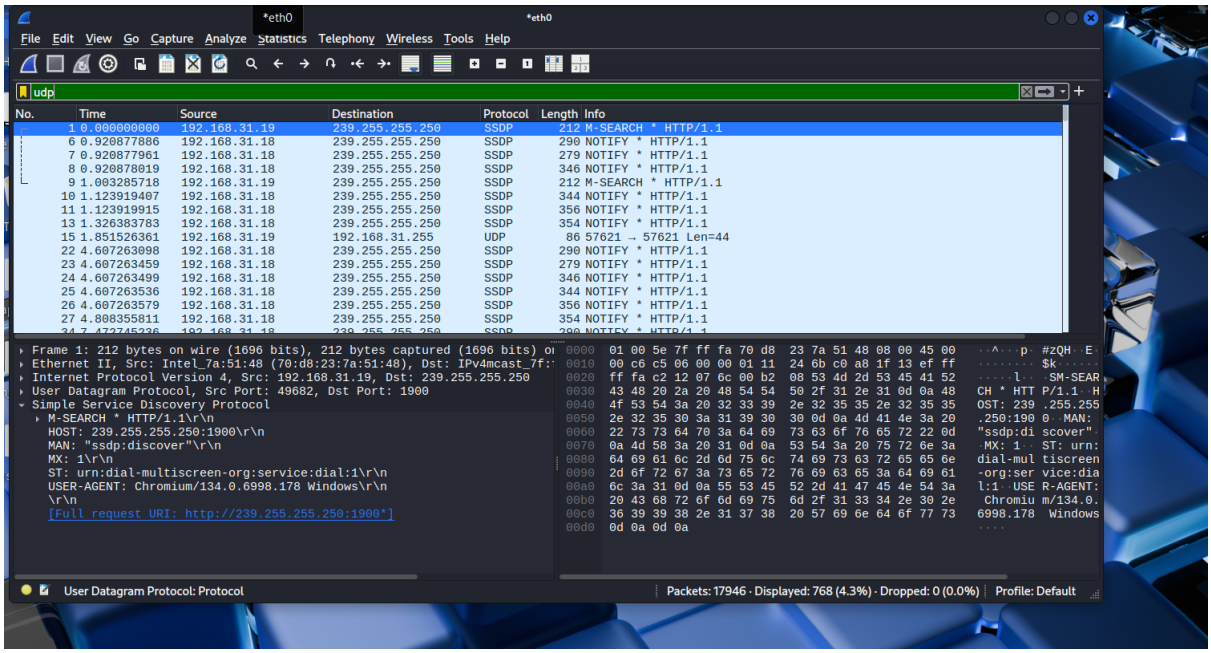
2. **DNS (dns)** – Displays only Domain Name System packets, which translate human-readable domain names (like google.com) into machine-readable IP addresses. This is usually the first communication step before web browsing begins.



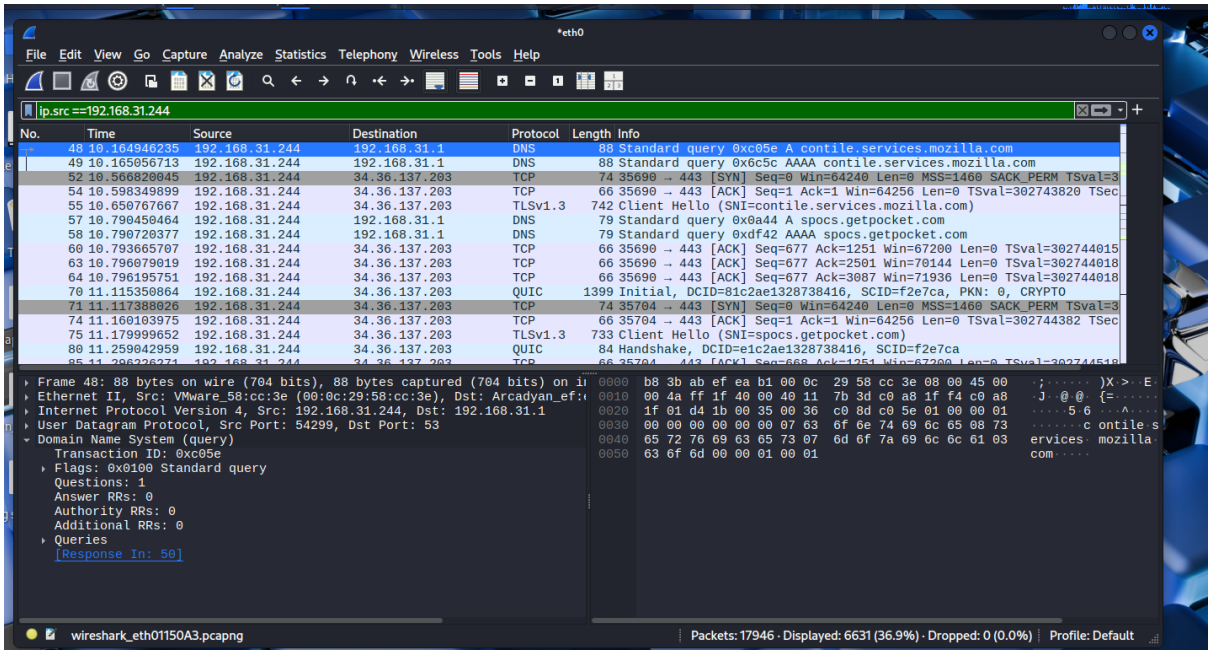
3. **TCP (tcp)** – Filters only Transmission Control Protocol packets, which provide reliable, ordered delivery of data. It also shows the TCP three-way handshake (SYN, SYN-ACK, ACK) that establishes a secure connection before data transfer.



4. **UDP (udp)** – Captures only User Datagram Protocol packets, which are faster but connectionless. This protocol is used in DNS queries, video/audio streaming, VoIP calls, and online gaming for quick data transmission without handshakes.



5. **Source IP (ip.src)** – Shows only packets originating from a specific source IP address. This is useful for tracking outgoing traffic from one device to see what it is sending across the network.



6. **Any IP (ip.addr)** – Displays packets either sent to or received from a specific IP address. This broader filter is used to monitor all communications related to a single host.