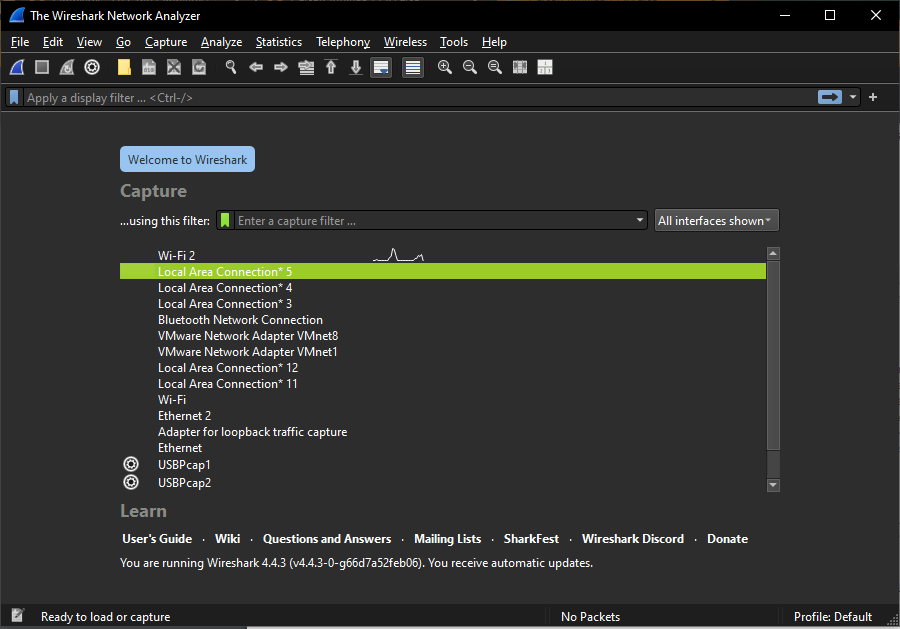
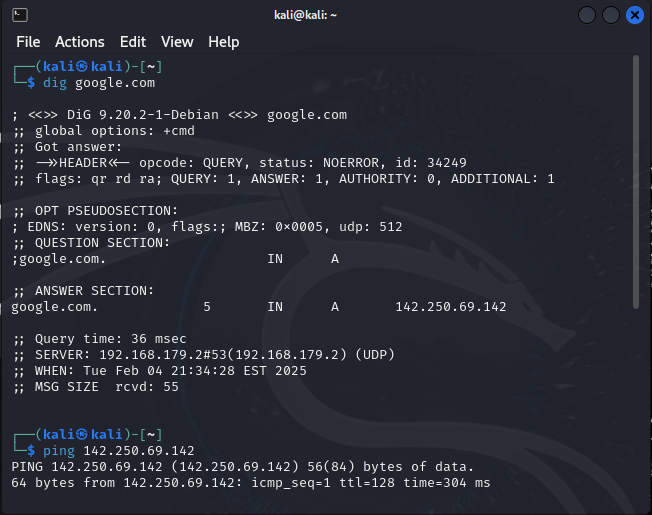
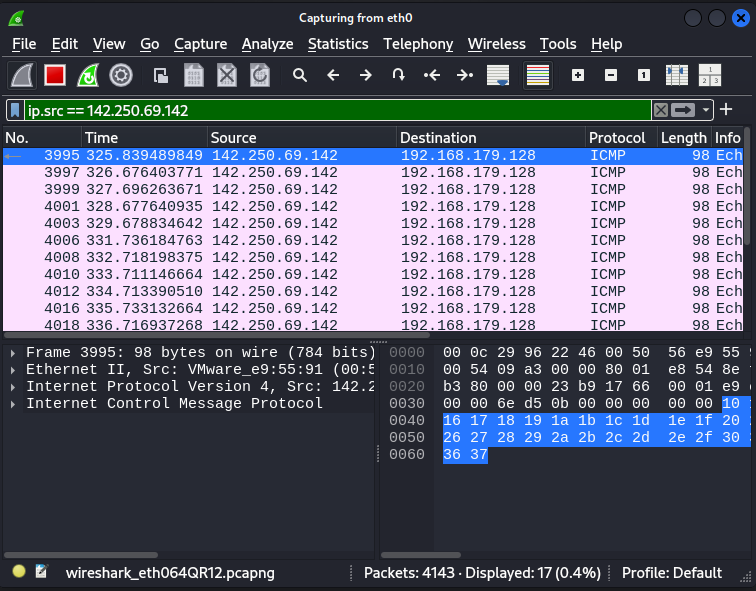
# 1 Install Wireshark

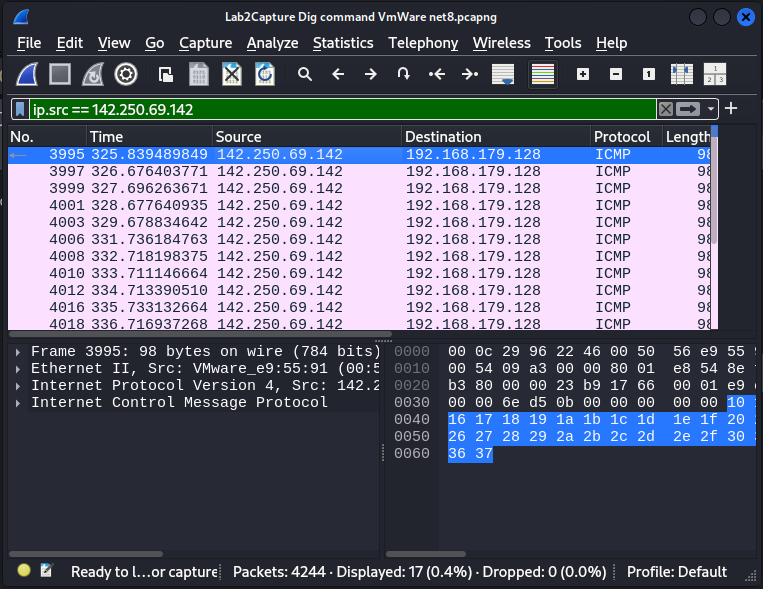


# 2 Ping, Dig, and Packet Capture



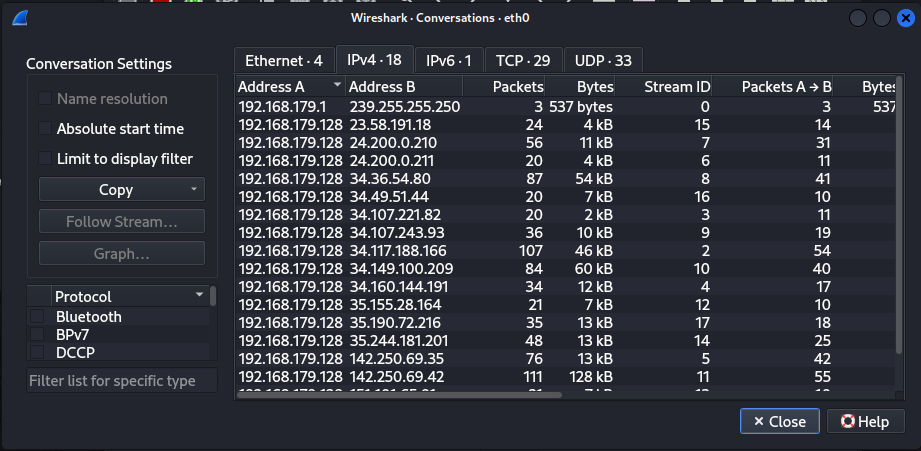


c) The ping command uses the **Internet Control Message Protocol (ICMP)** to test network connectivity by sending **ICMP Echo Request** packets to a target host and waiting for **ICMP Echo Reply** responses. It measures round-trip time (RTT) and detects packet loss, helping diagnose network issues. Each request includes a sequence number, identifier, and timestamp, while responses confirm the host's availability. The **Time To Live (TTL)** field prevents infinite loops by limiting hops. However, firewalls may block ICMP for security reasons, and it can be exploited in **DoS attacks** like ICMP flooding.

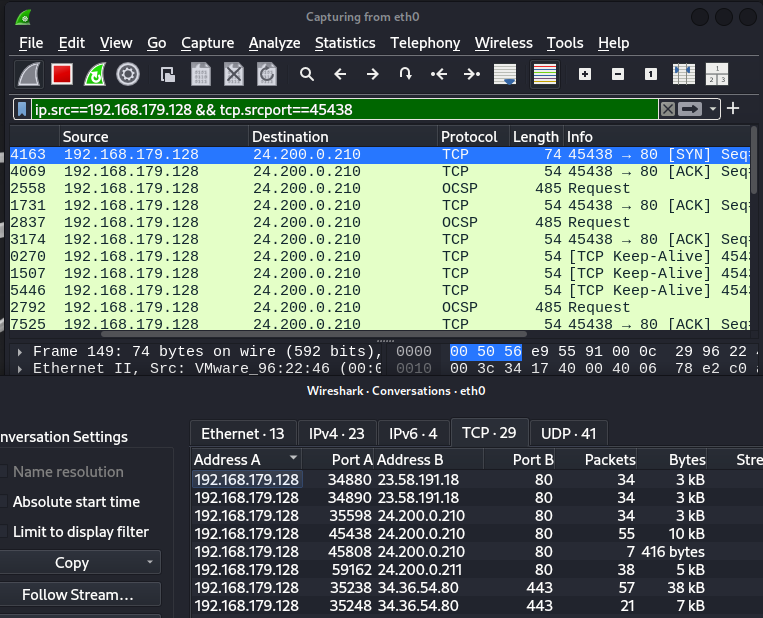


# 3 Conversations in WireShark Packet Analysis

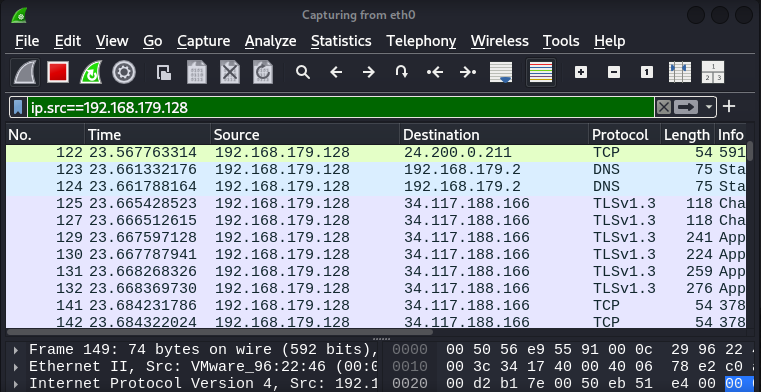
## A. Conversation statistics



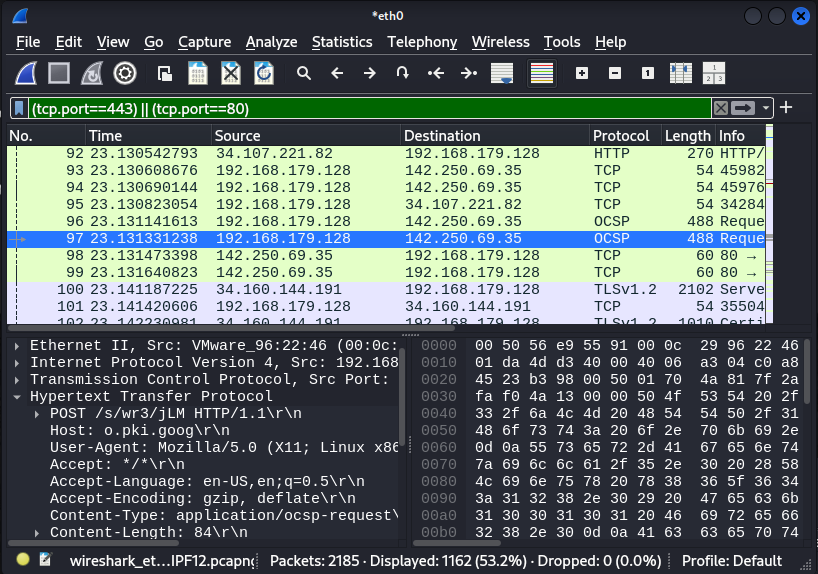
## B. apply filter with IP address and port number

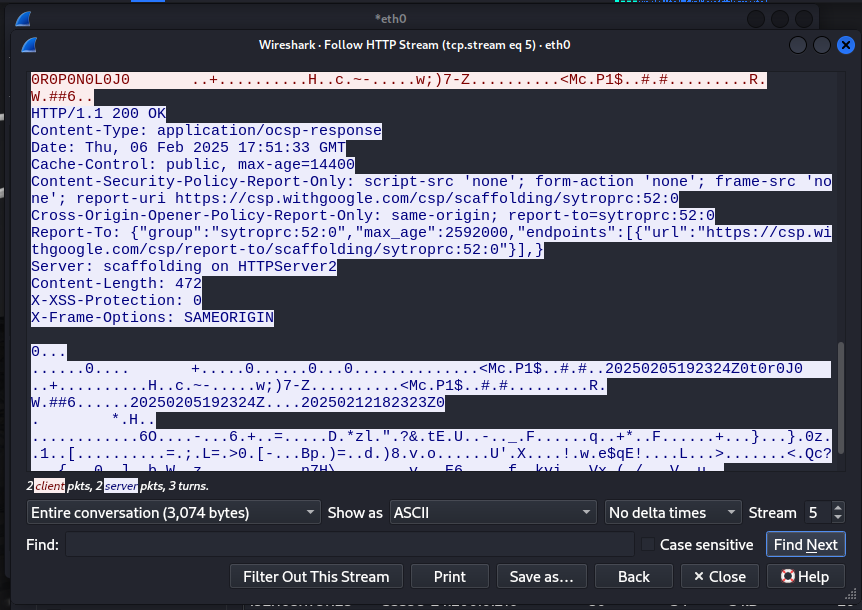


## C. Apply filter to find all traffic from my IP

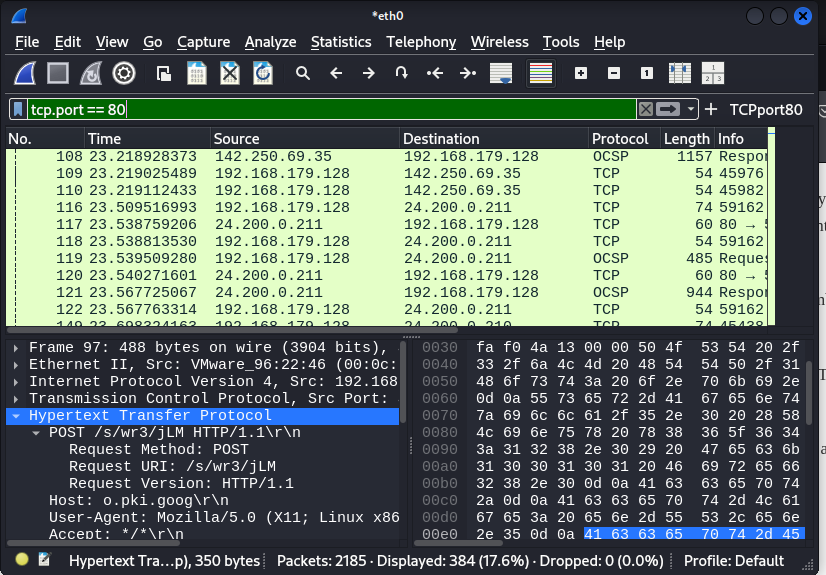


## D. Apply filter to display all http traffic and follow HTTP request

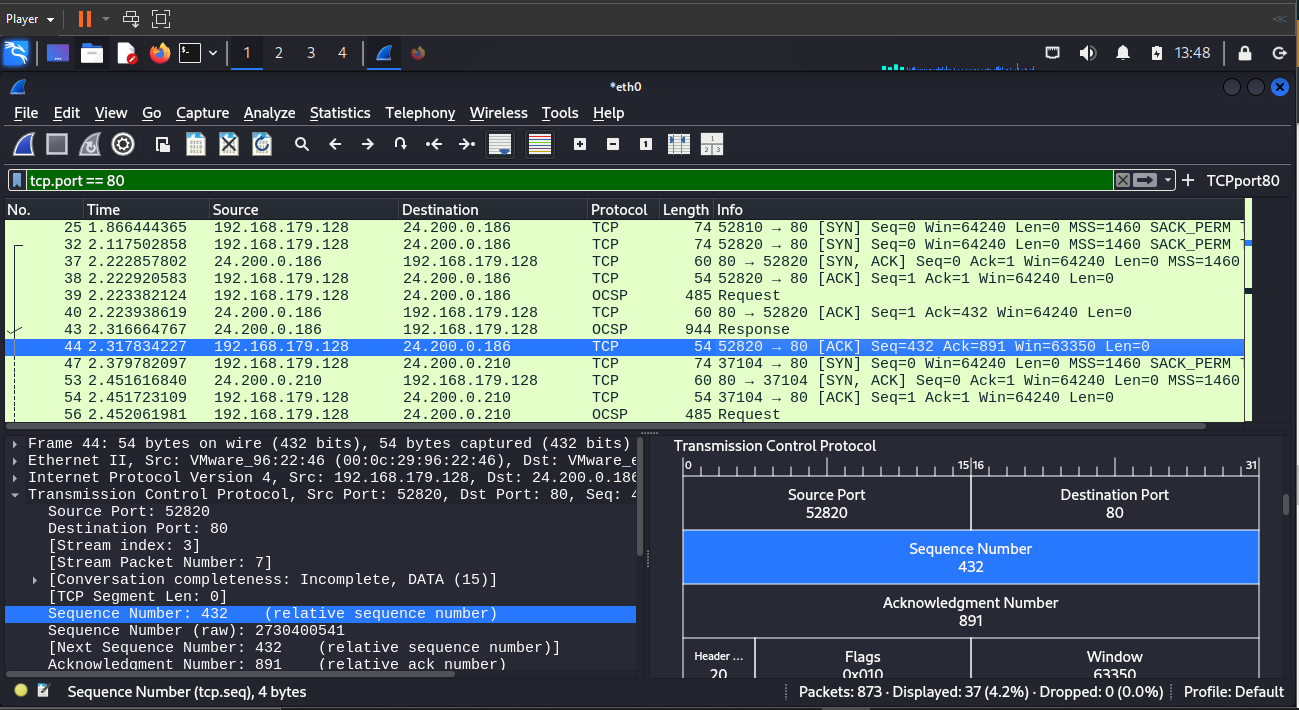




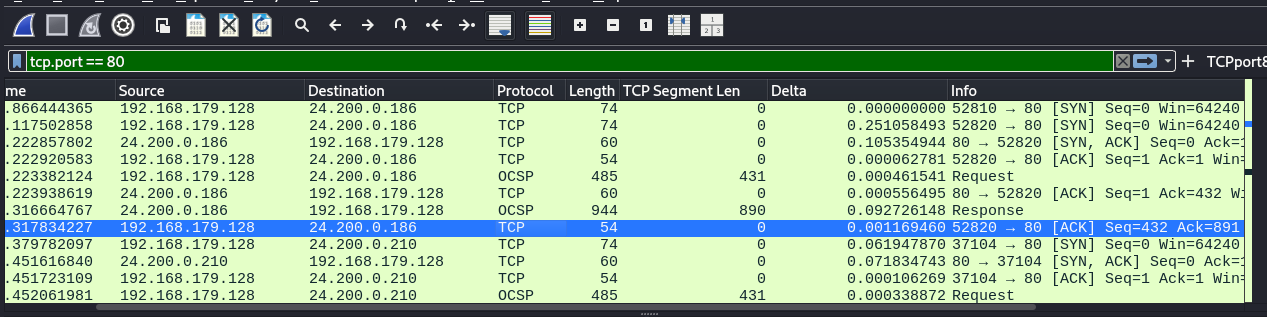
## E. Add button to filter TCP80



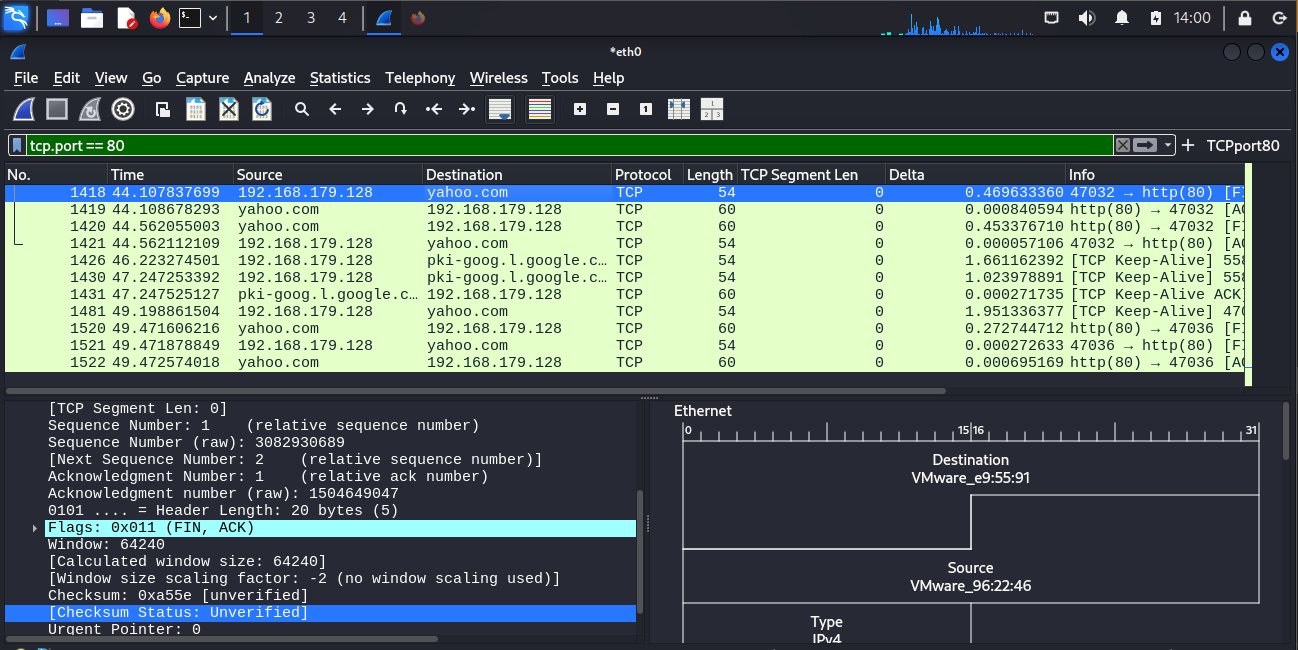
## F. Configure wireshark to display packet diagram



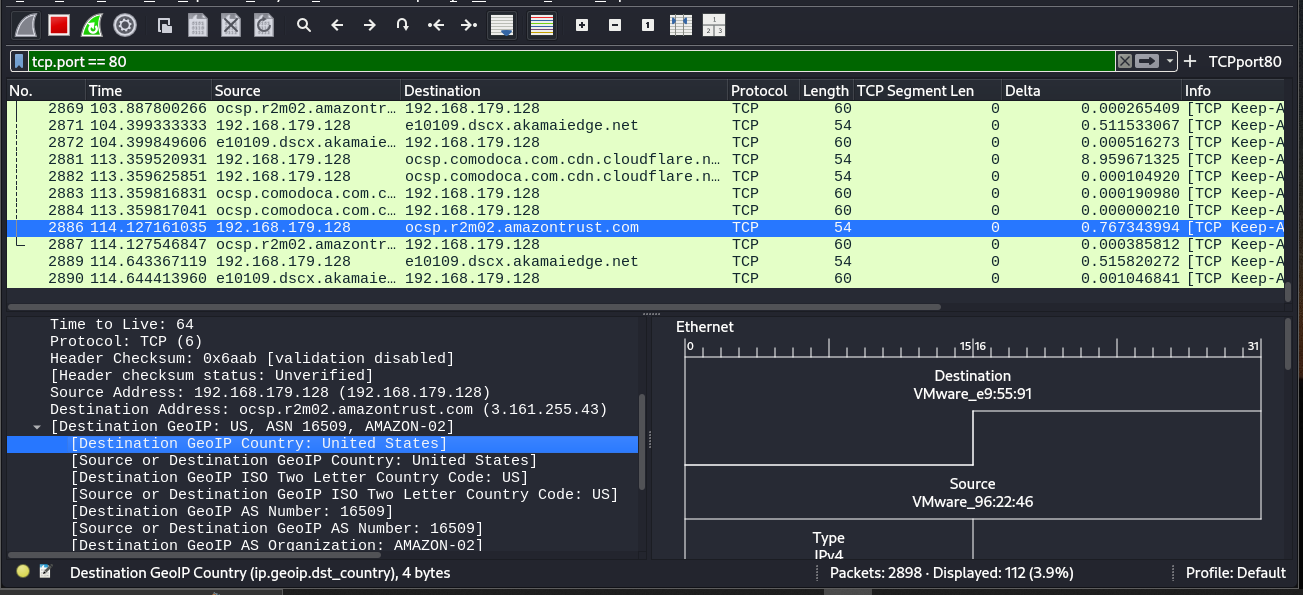
## G. Add Delta and TCP segment length in Packet List



## H. Resolve host names

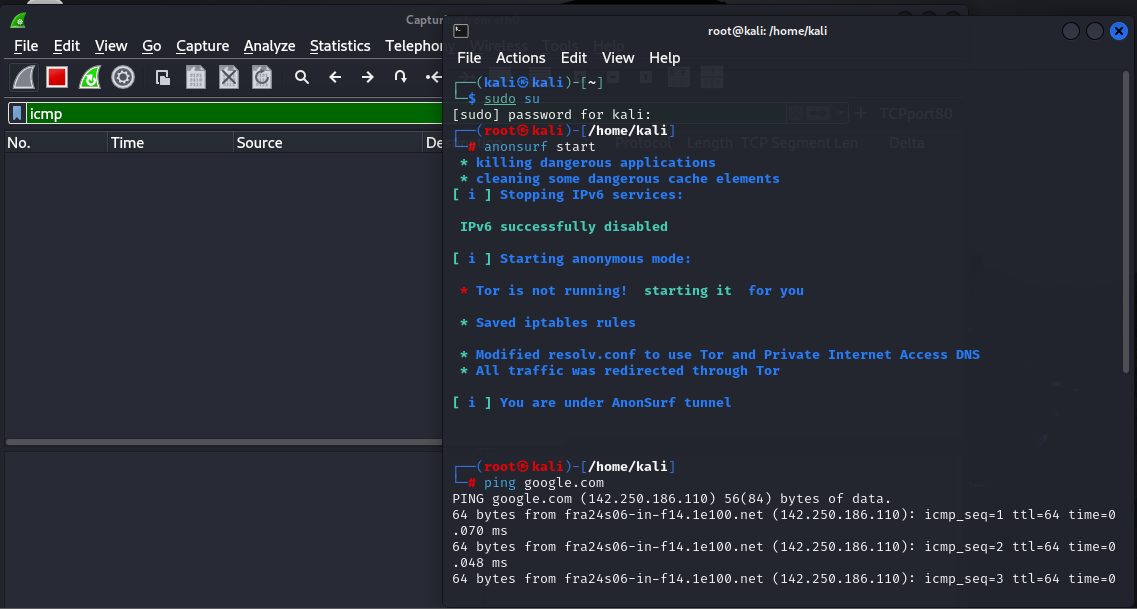


# 4. Geo IP using MaxMind database



# 5. Anonymous surfing

## A, B anonymous surfing and pinging



## C. Change MAC address

