Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Computer Science & Engineering

CSE3501 – Information Security Analysis and Audit

LAB ASSIGNMENT 5

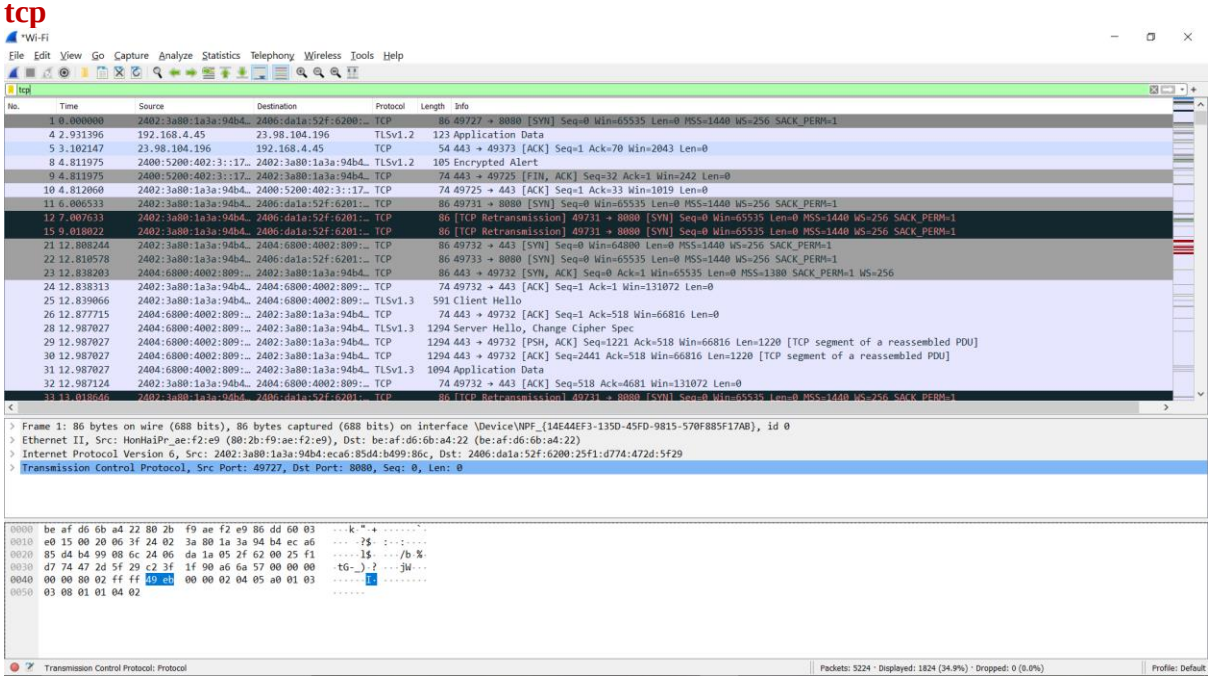
Submitted to **Prof. RAJA SP**

NAME: PUNIT MIDDHA
REG.NO: 19BCE2060
SLOT: L39+L40
DATE: 21/10/2021

Network Packets Sniffing using Wireshark

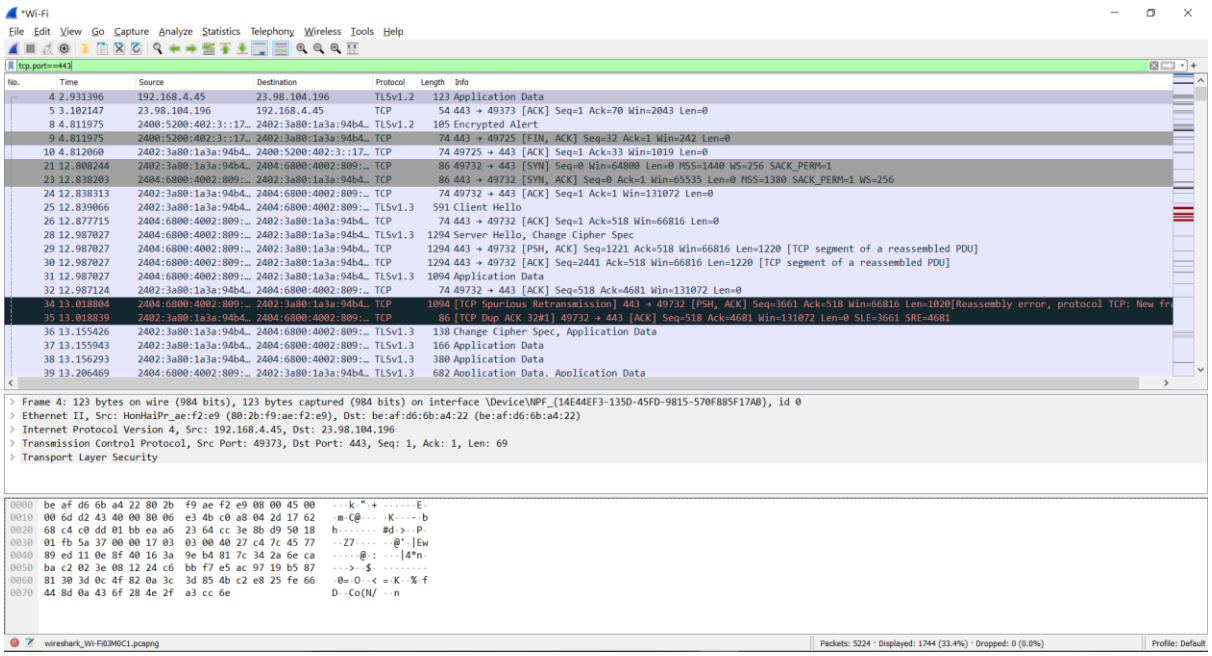
1. Filtering the packets by specifying a protocol

tcp

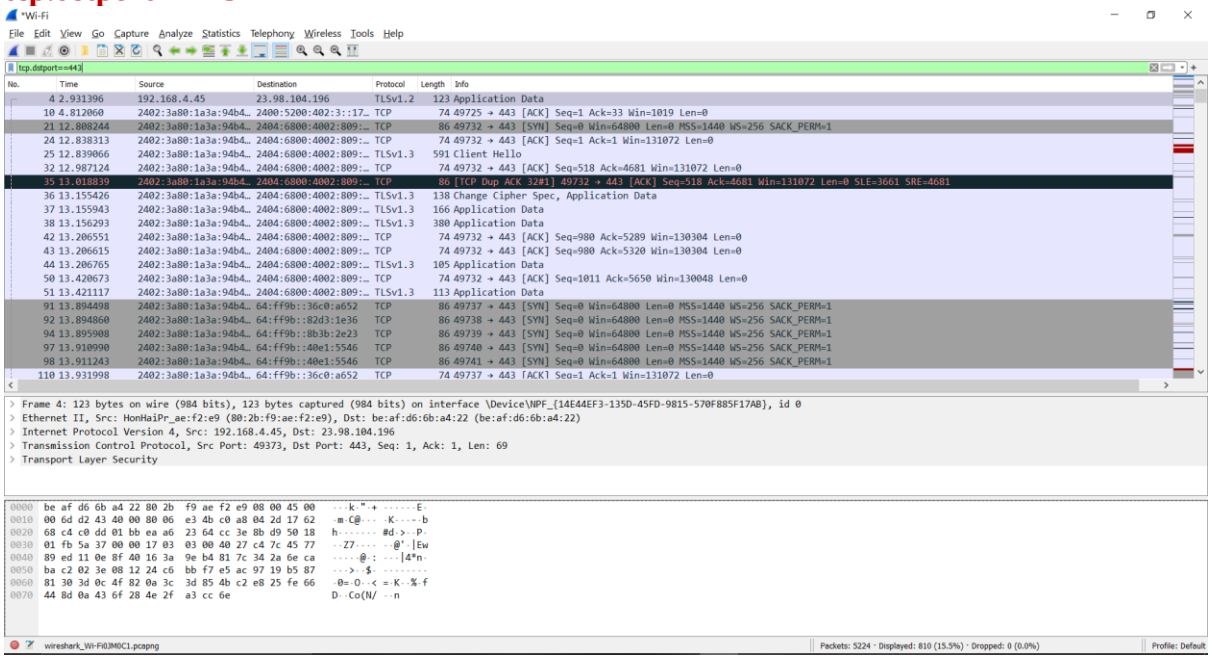


2. Filter the packets based on the port

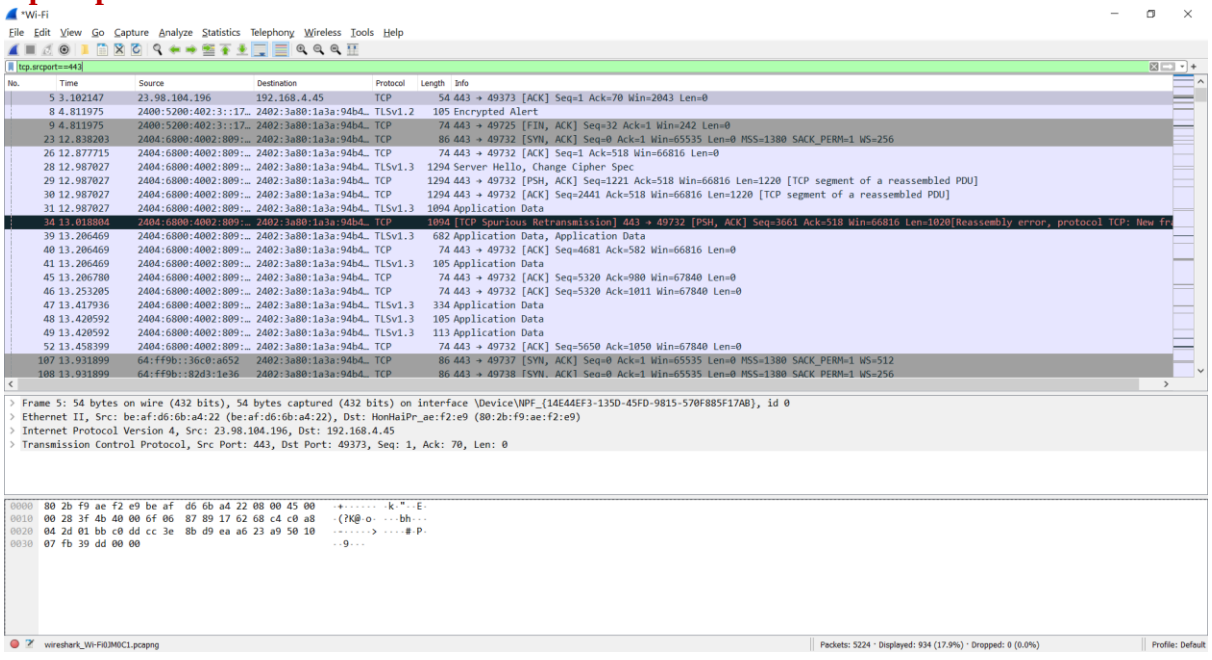
tcp.port==443



tcp.dstport==443

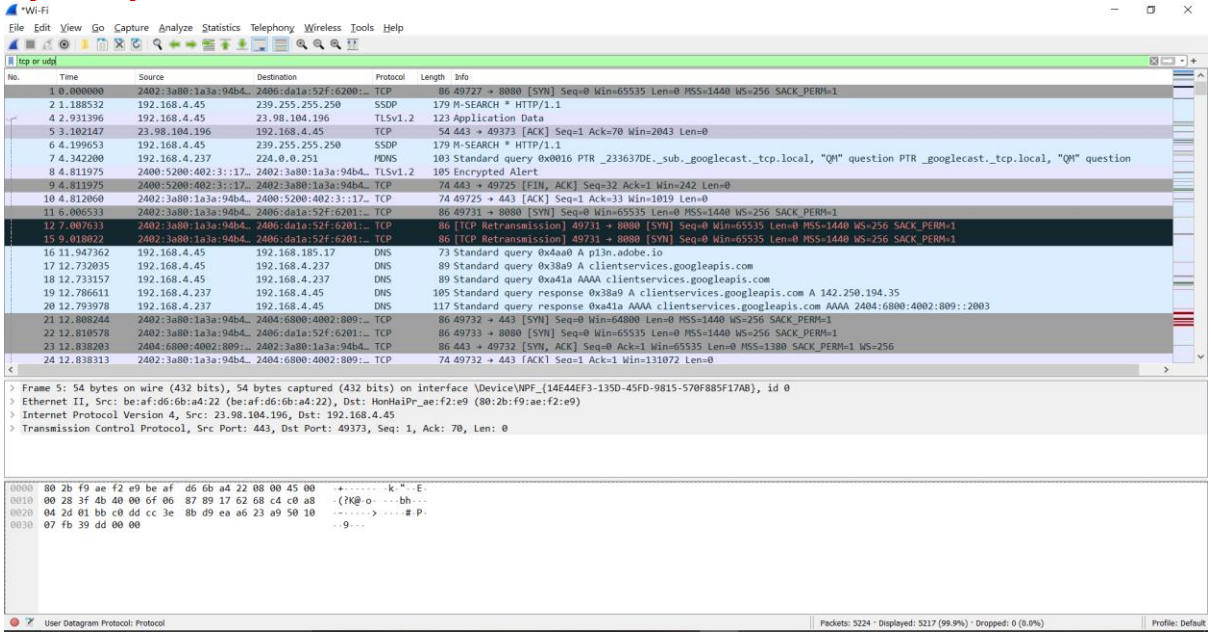


tcp.srcport==443

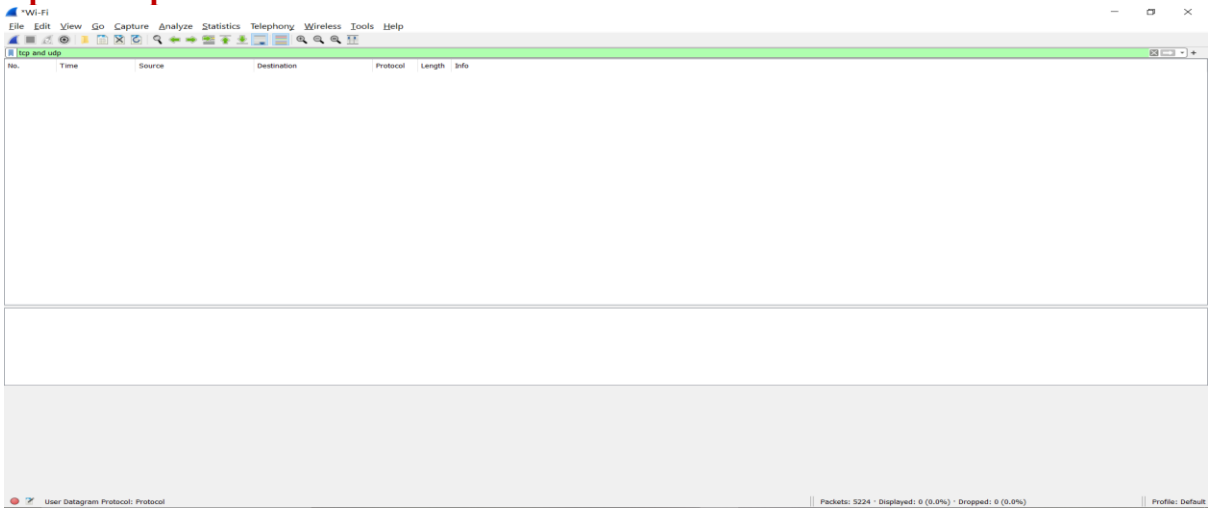


3. Filter results based on ‘or / and’

tcp or udp

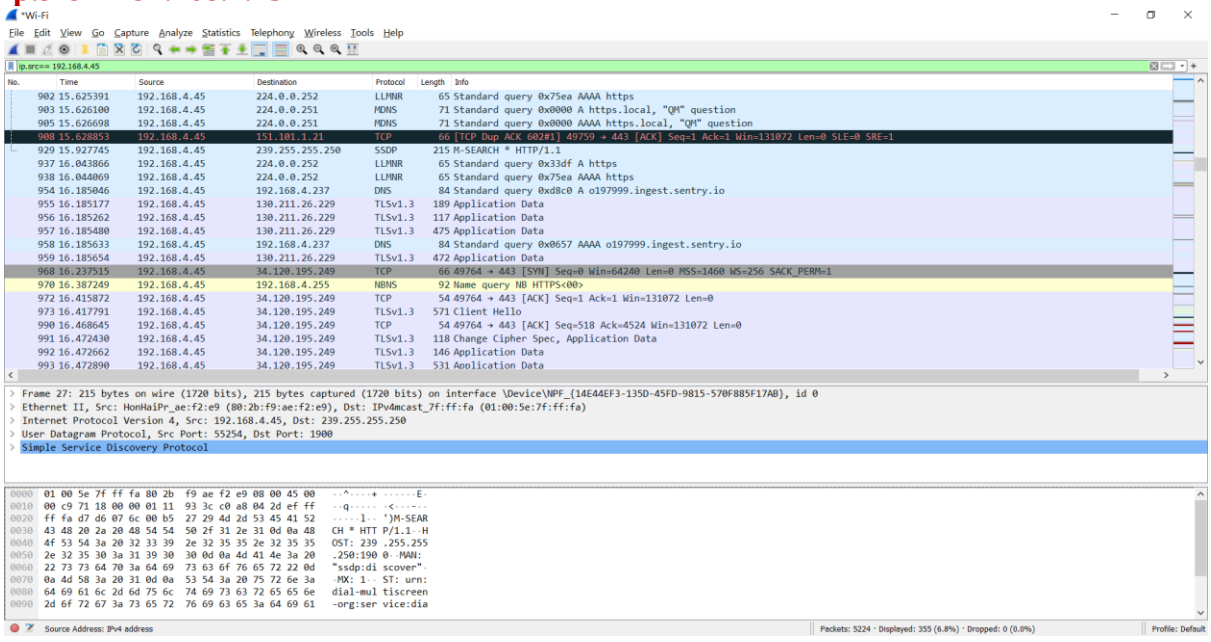


tcp and udp

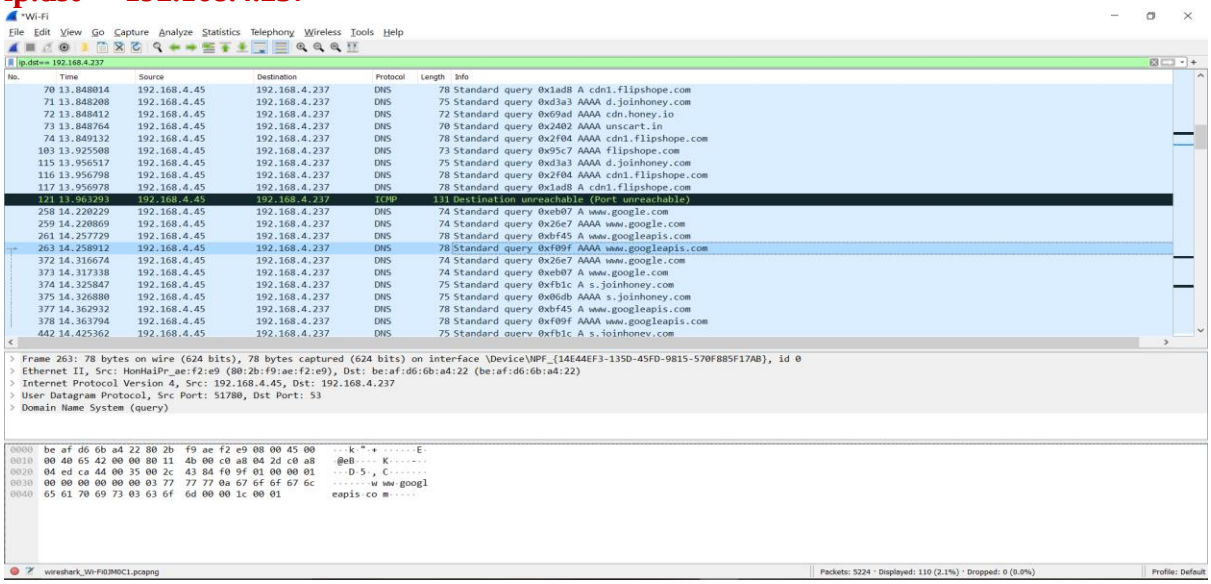


4. Filter results based on IP addresses

ip.src==192.168.4.45

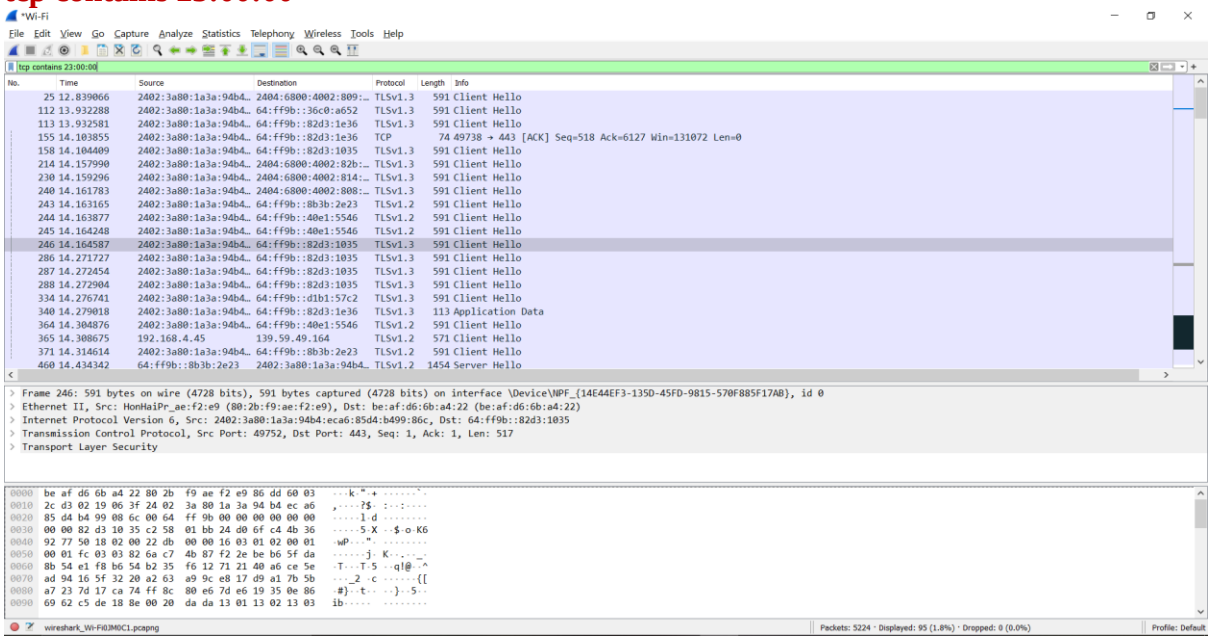


ip.dst== 192.168.4.237



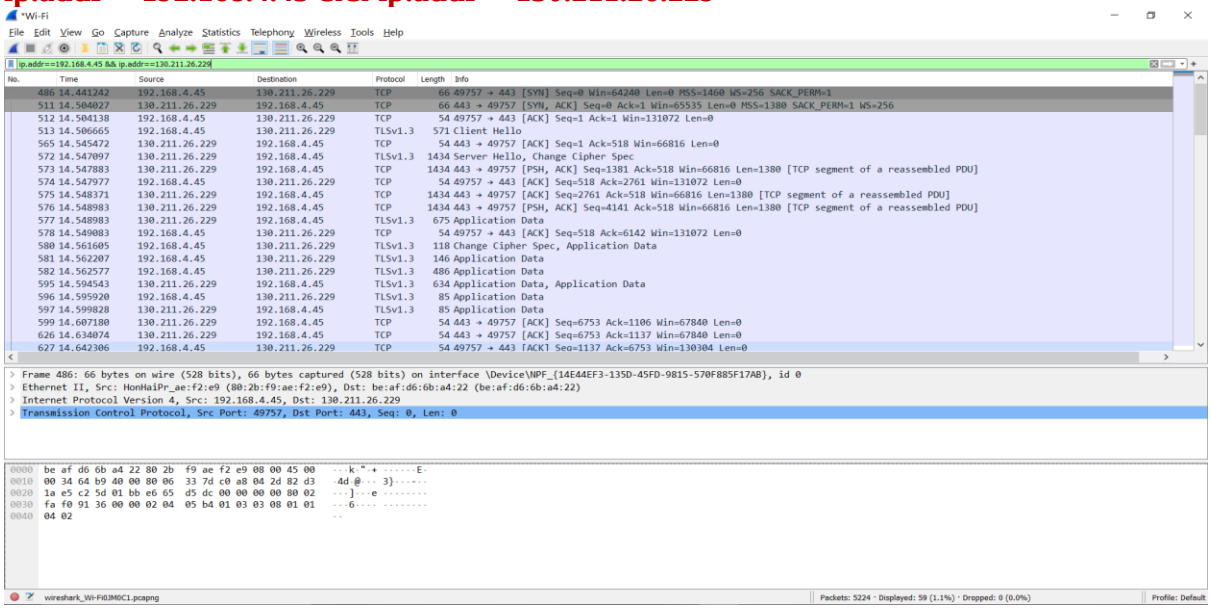
5. Filter results based on the byte sequence

tcp contains 23:00:00

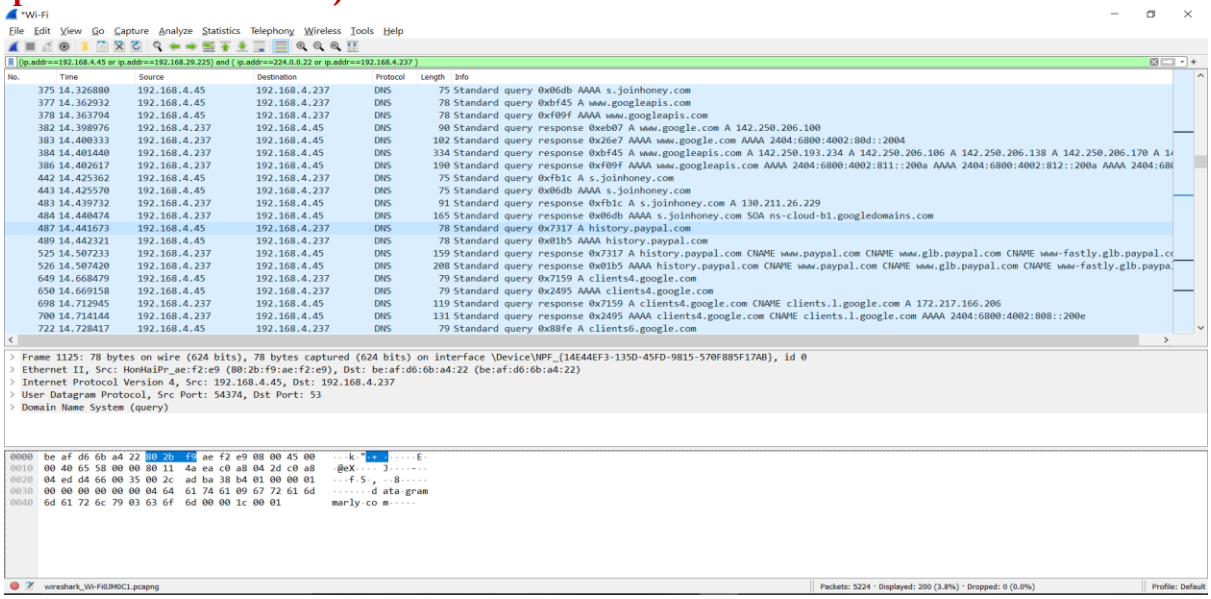


6. Filter results based on two IP addresses

ip.addr==192.168.4.45 && ip.addr==130.211.26.229

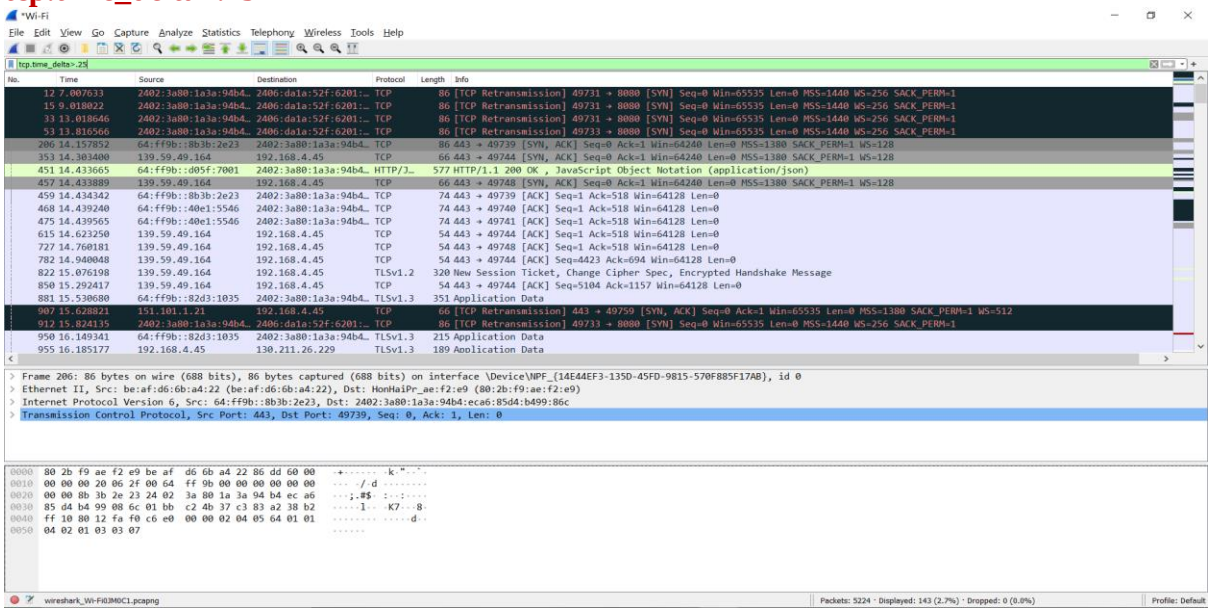


(ip.addr==192.168.4.45 or ip.addr==192.168.29.225) and (ip.addr==224.0.0.22 or ip.addr==192.168.4.237)

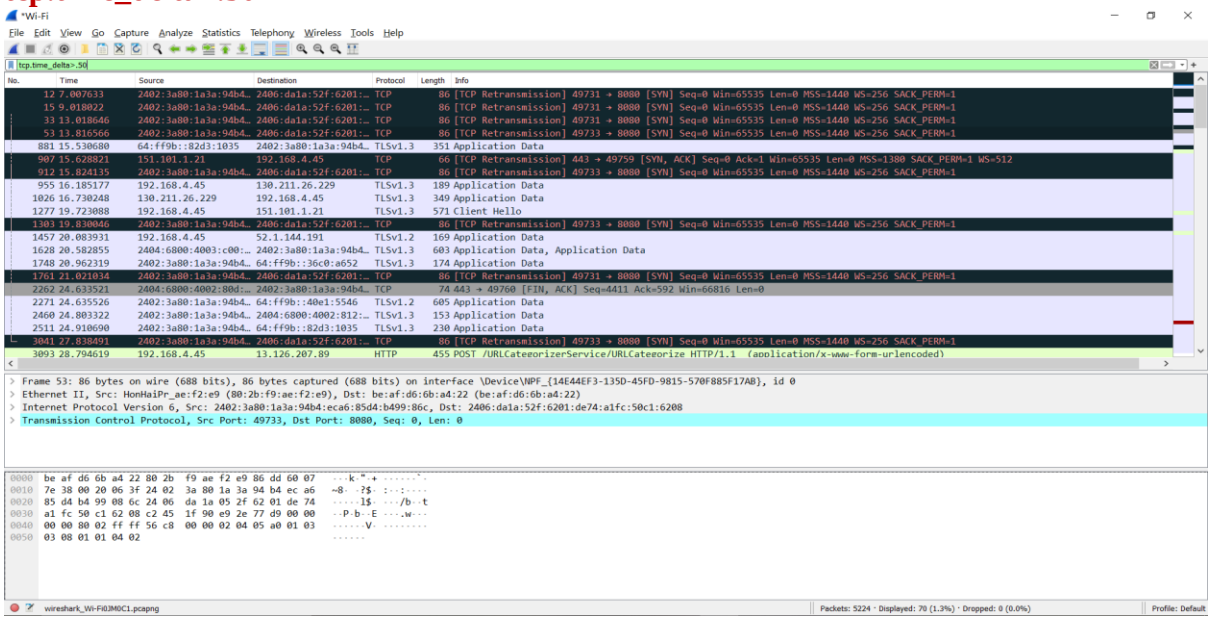


7. Filter the results based on the timestamp

tcp.time_delta>.25

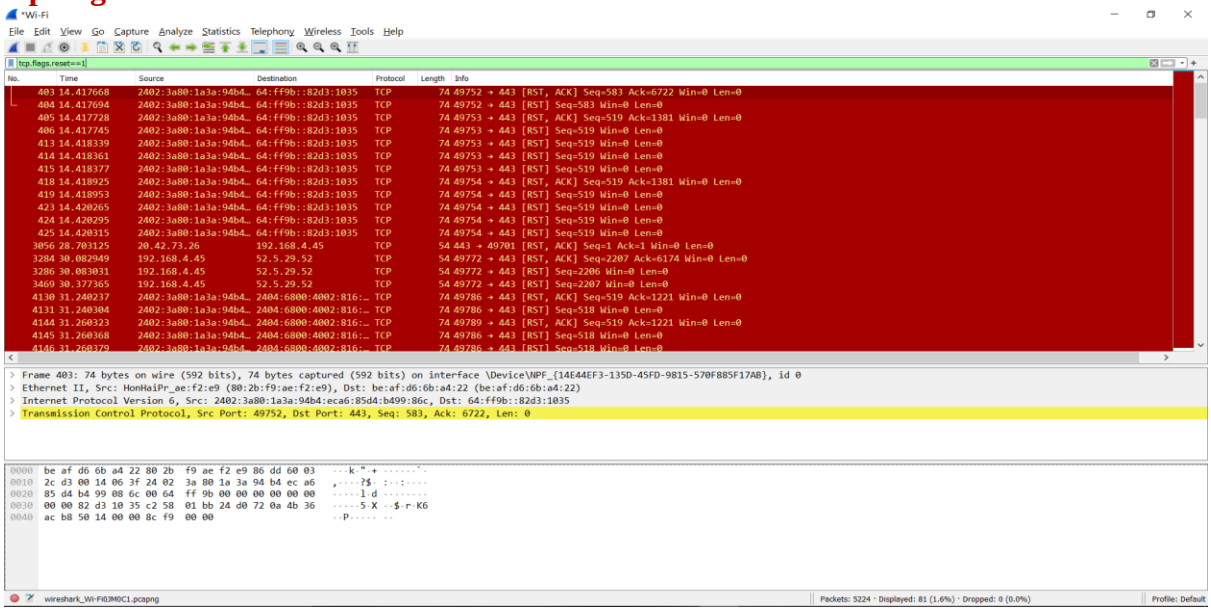


tcp.time_delta>.50

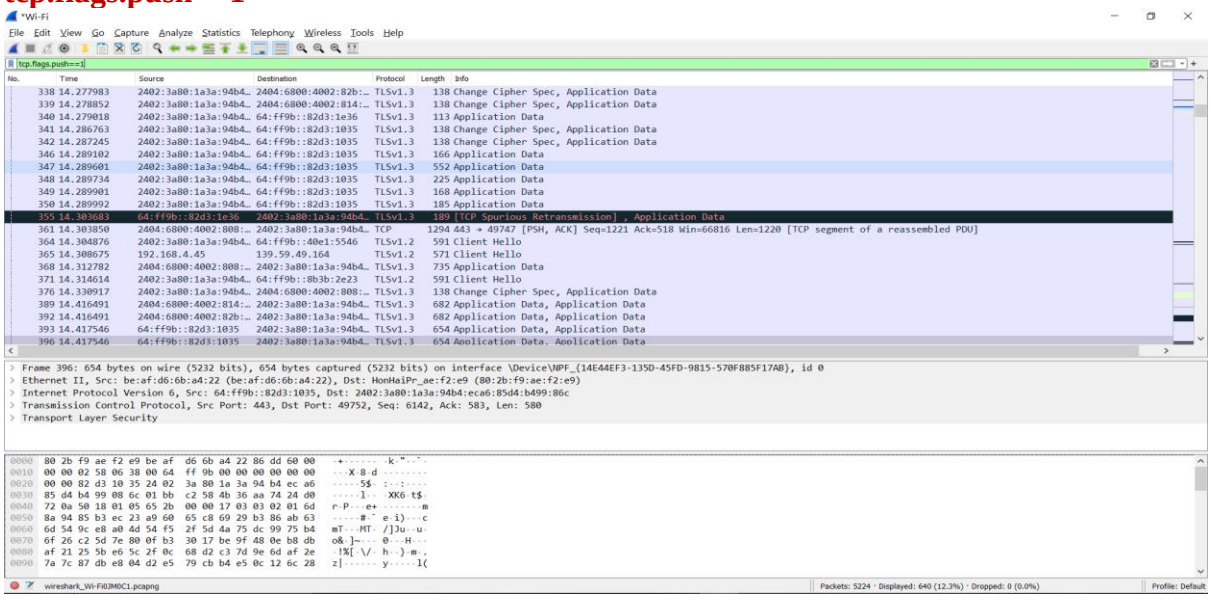


8. Filter the results based on the flags(ACK, SYN, PSH, RST)

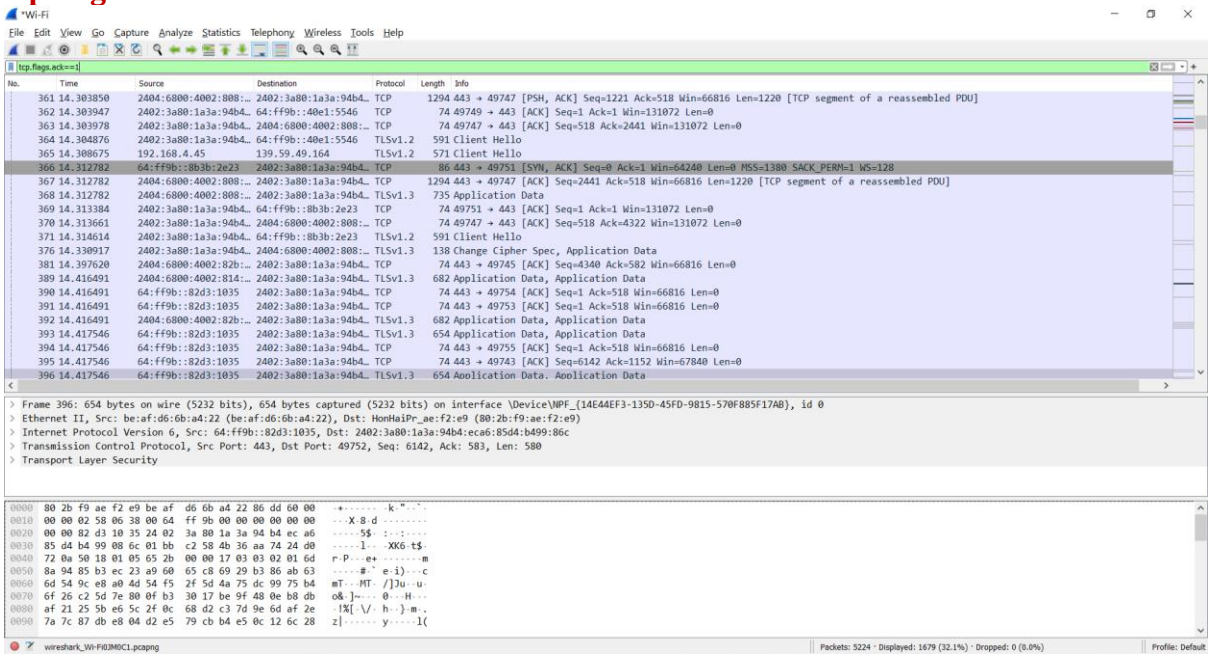
tcp.flags.reset==1



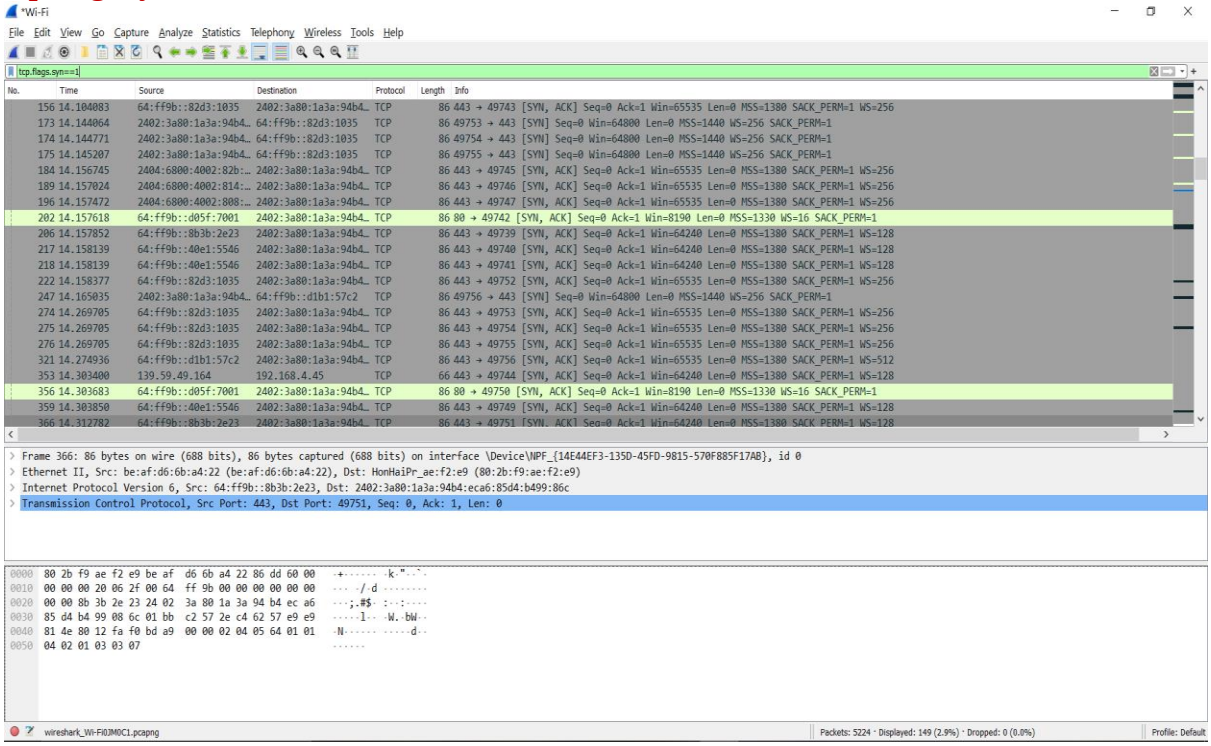
tcp.flags.push==1



tcp.flags.ack==1

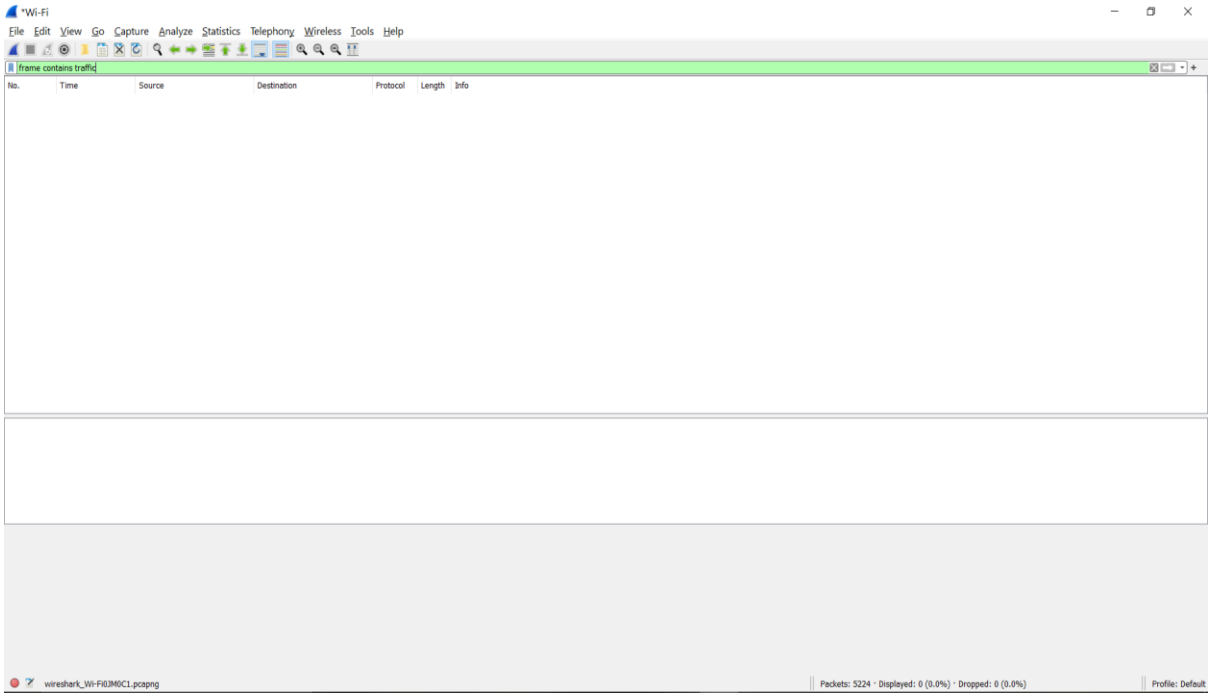


tcp.flags.syn==1



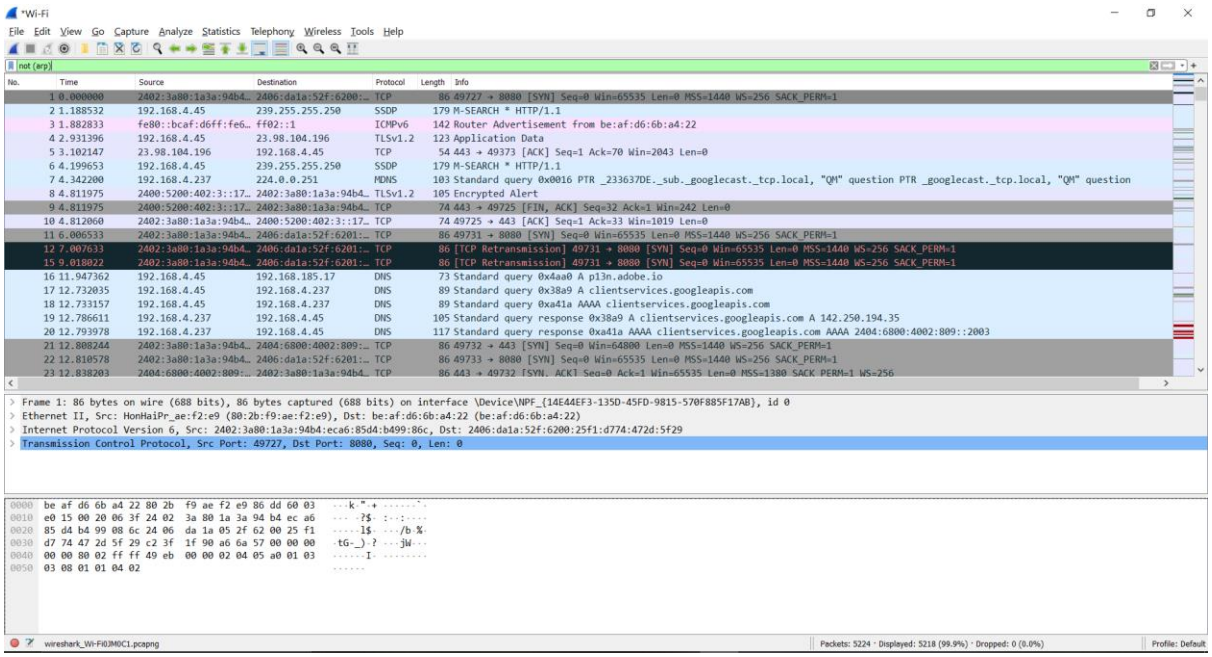
9. Traffic

frame contains traffic

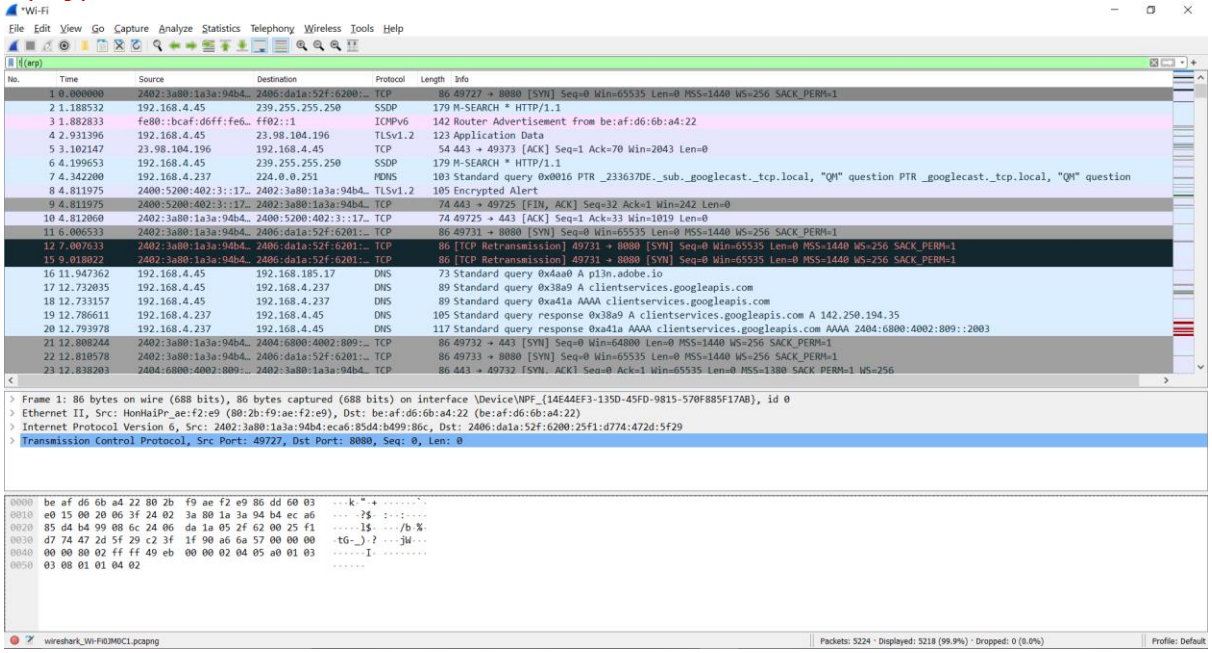


10. Filter the packets based on NOT (!)

not (arp)

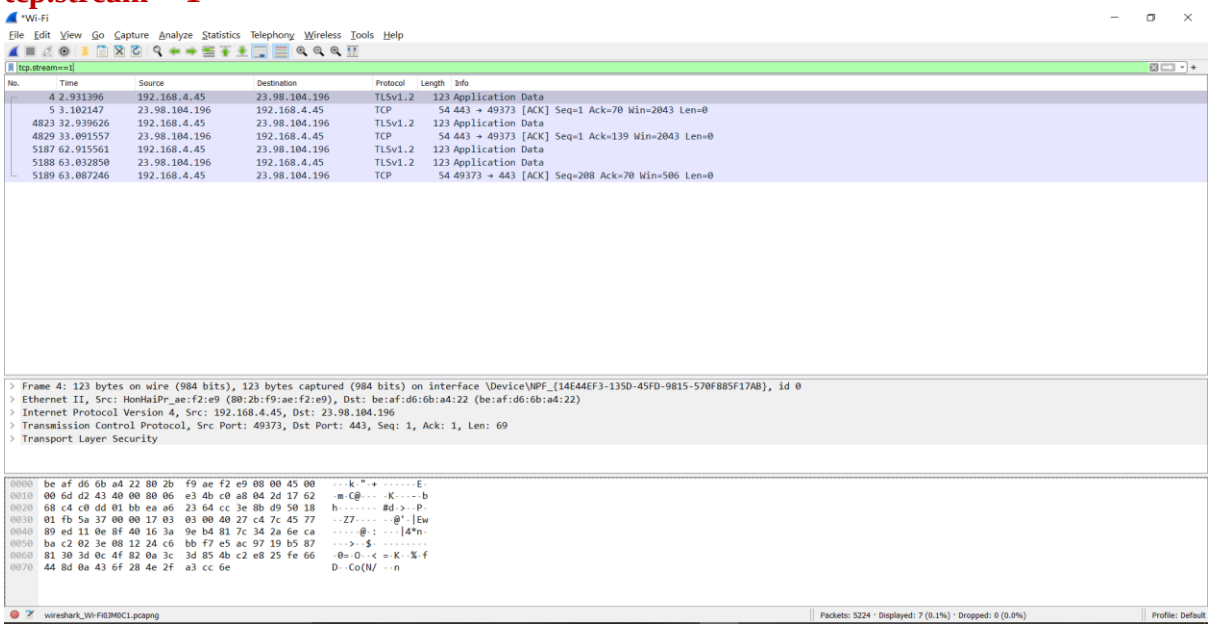


! (arp)



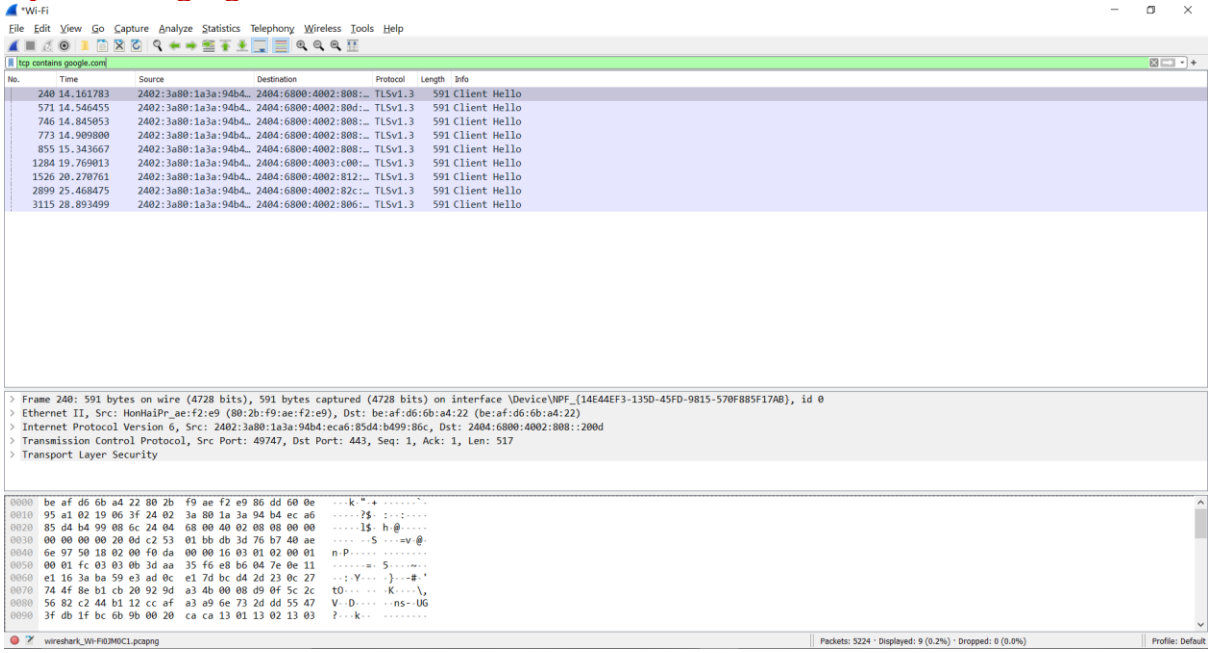
11. Filter the packets based on stream

tcp.stream==1



12. Filter based on the website

tcp contains google.com



13. Filter the packets based on retransmission and duplicate acks

tcp.analysis.flags