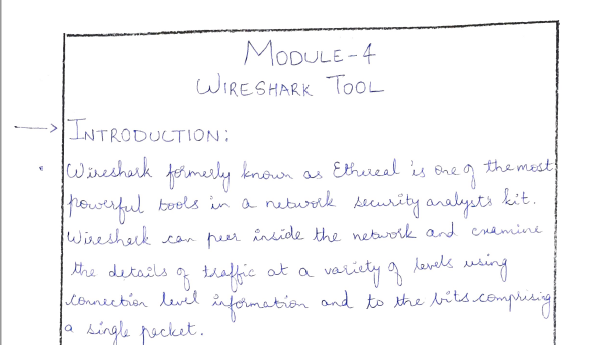
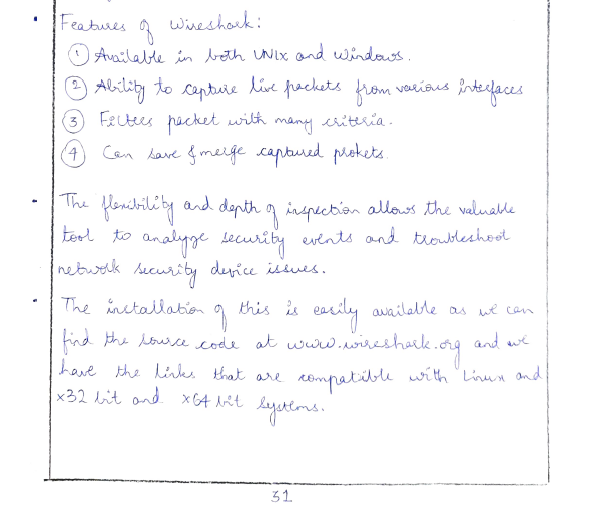
Module – 4

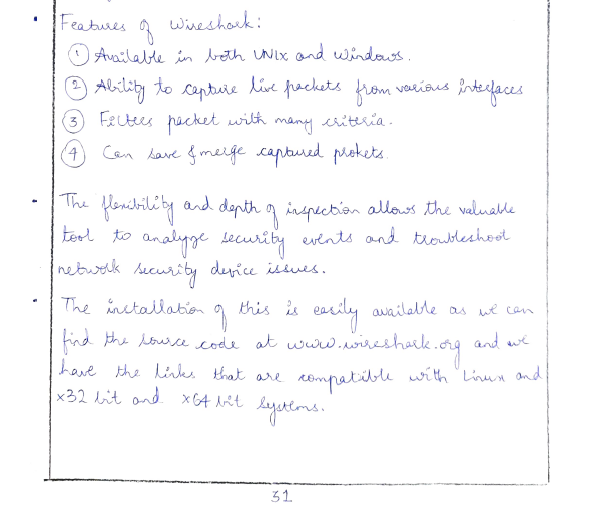
Wireshark Tool

Introduction

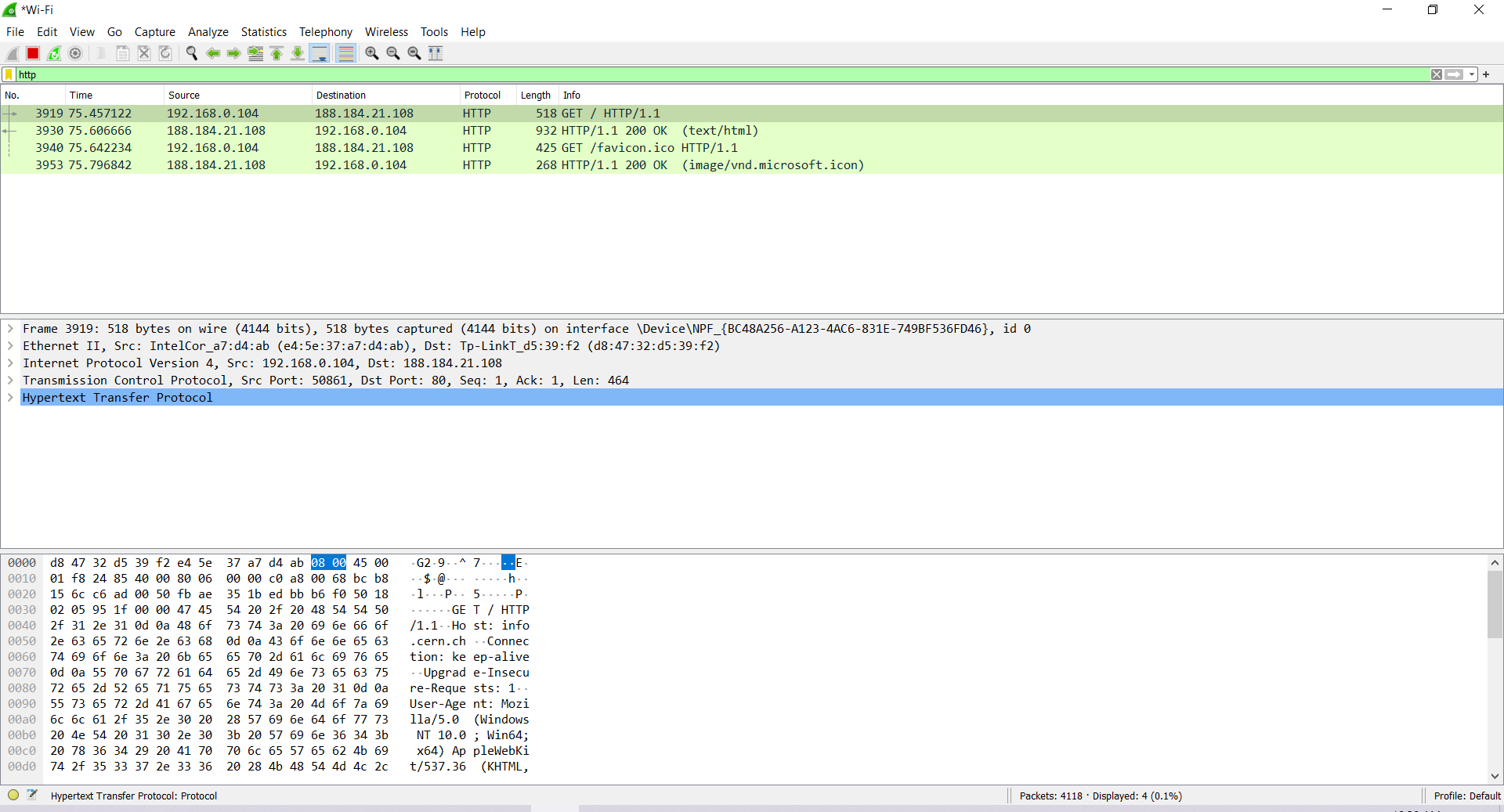


Features of Wireshark: -

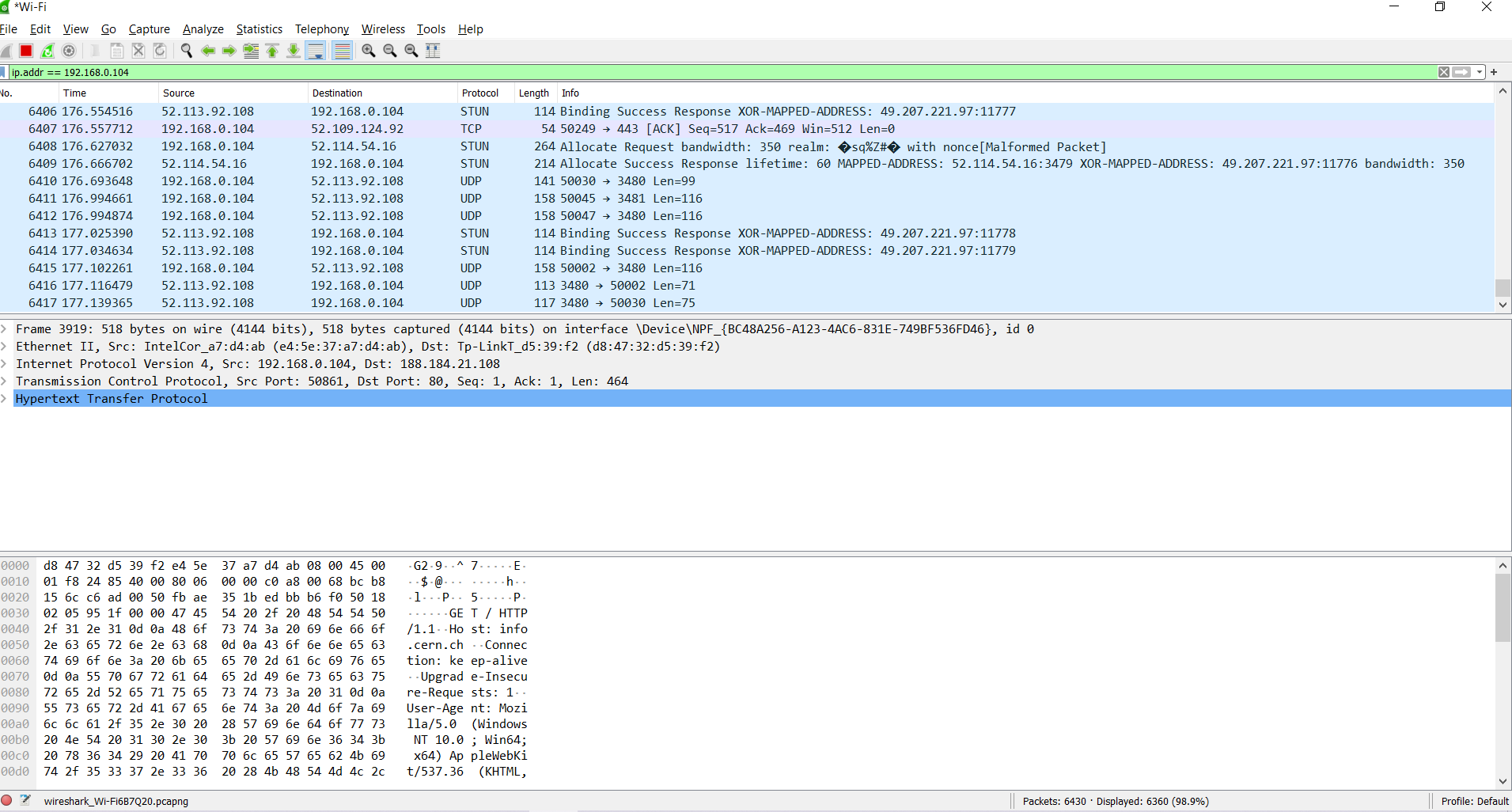




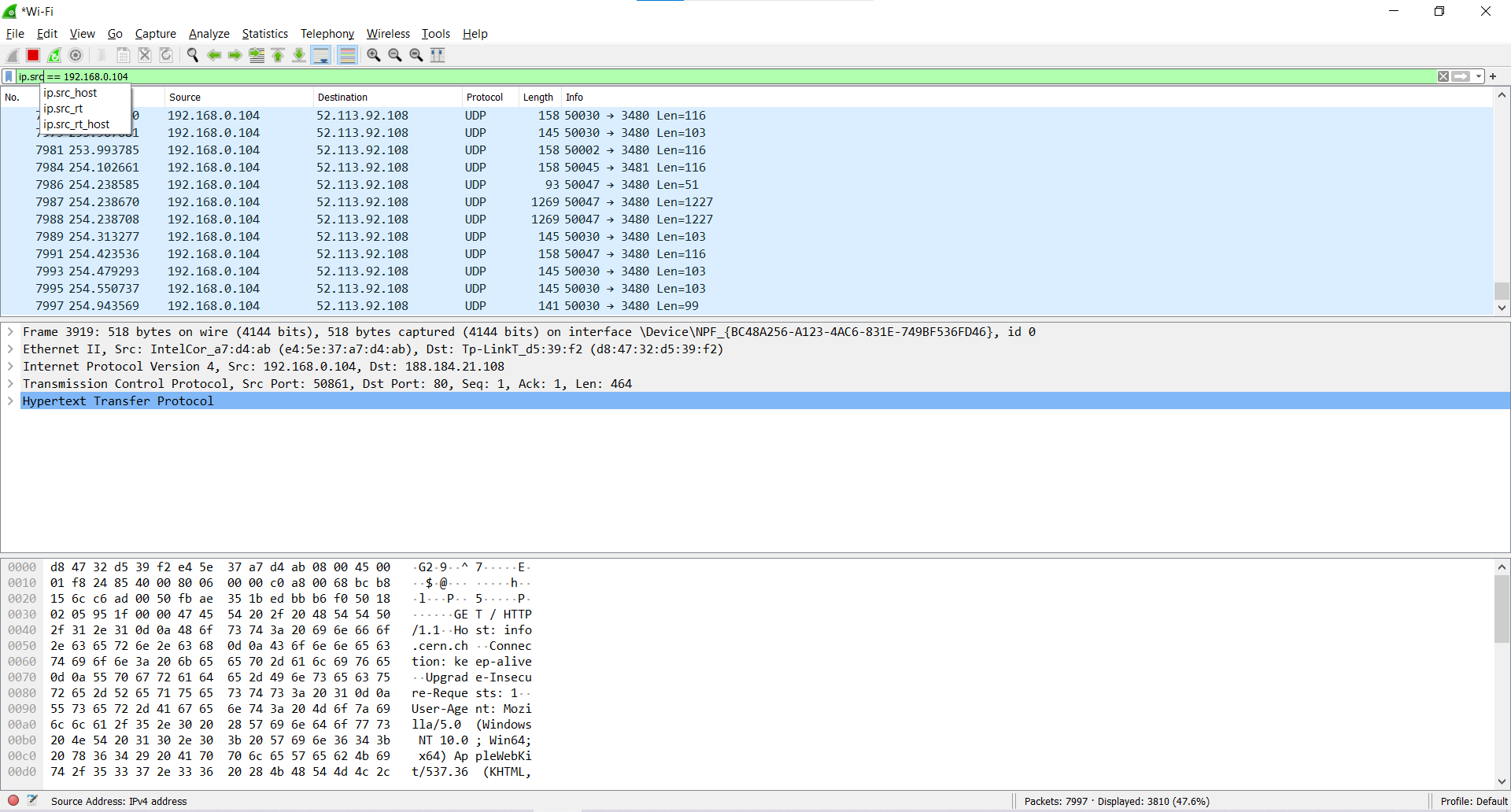
Commands in Wireshark

1. Http Filter

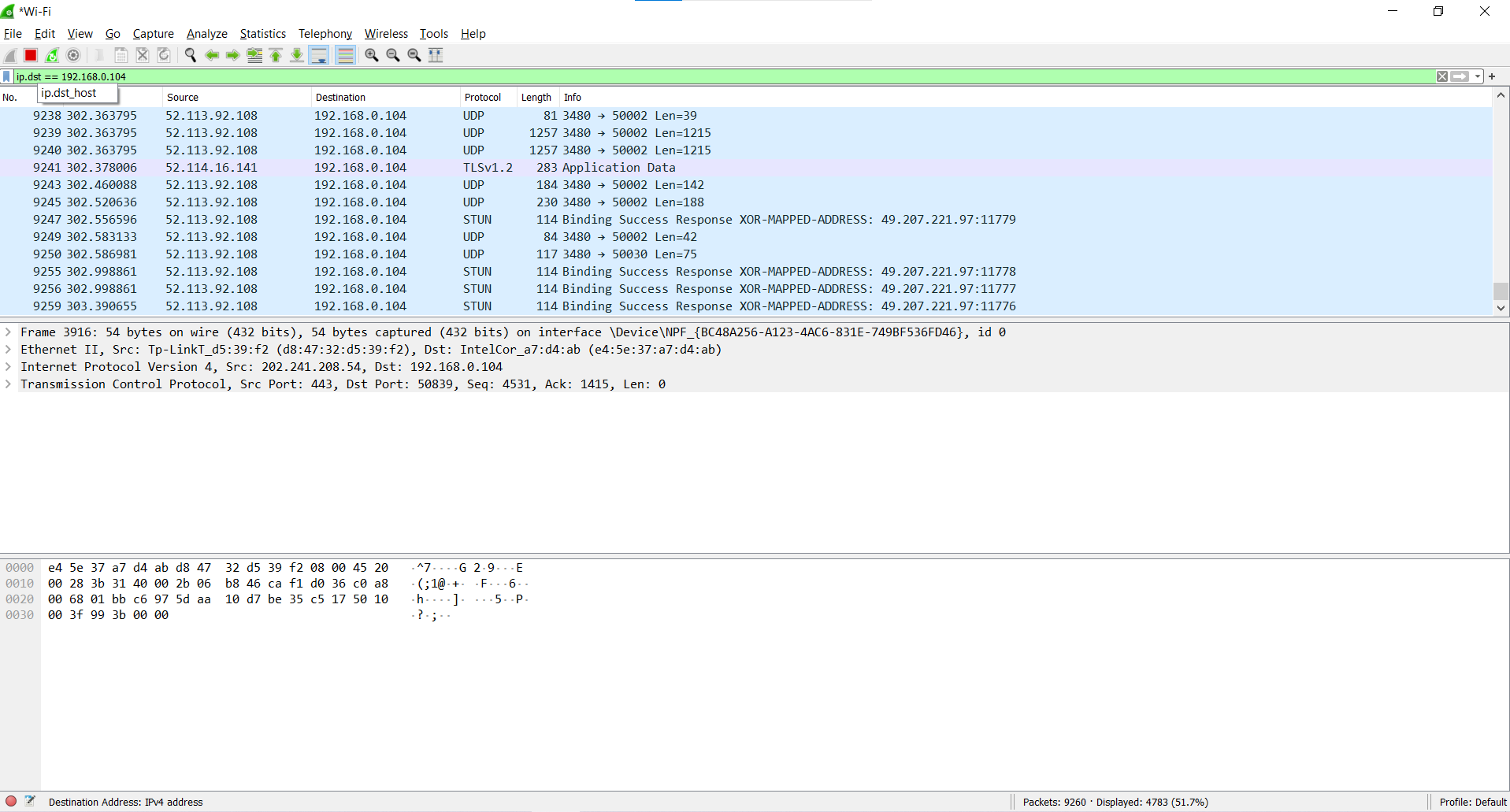
2. Ip.addr==192.168.0.\_\_



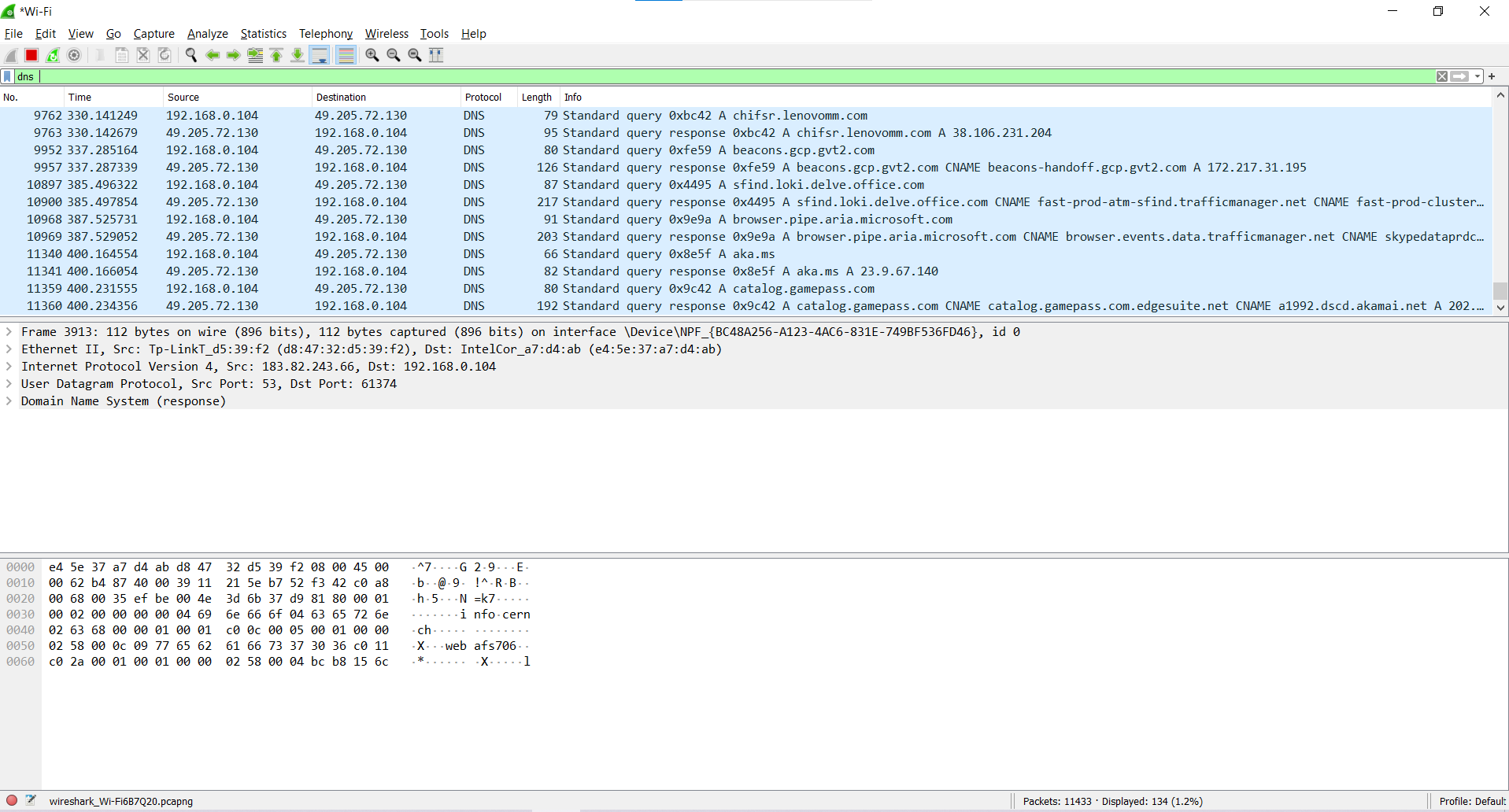
3. Ip.src == 192.168.0.104

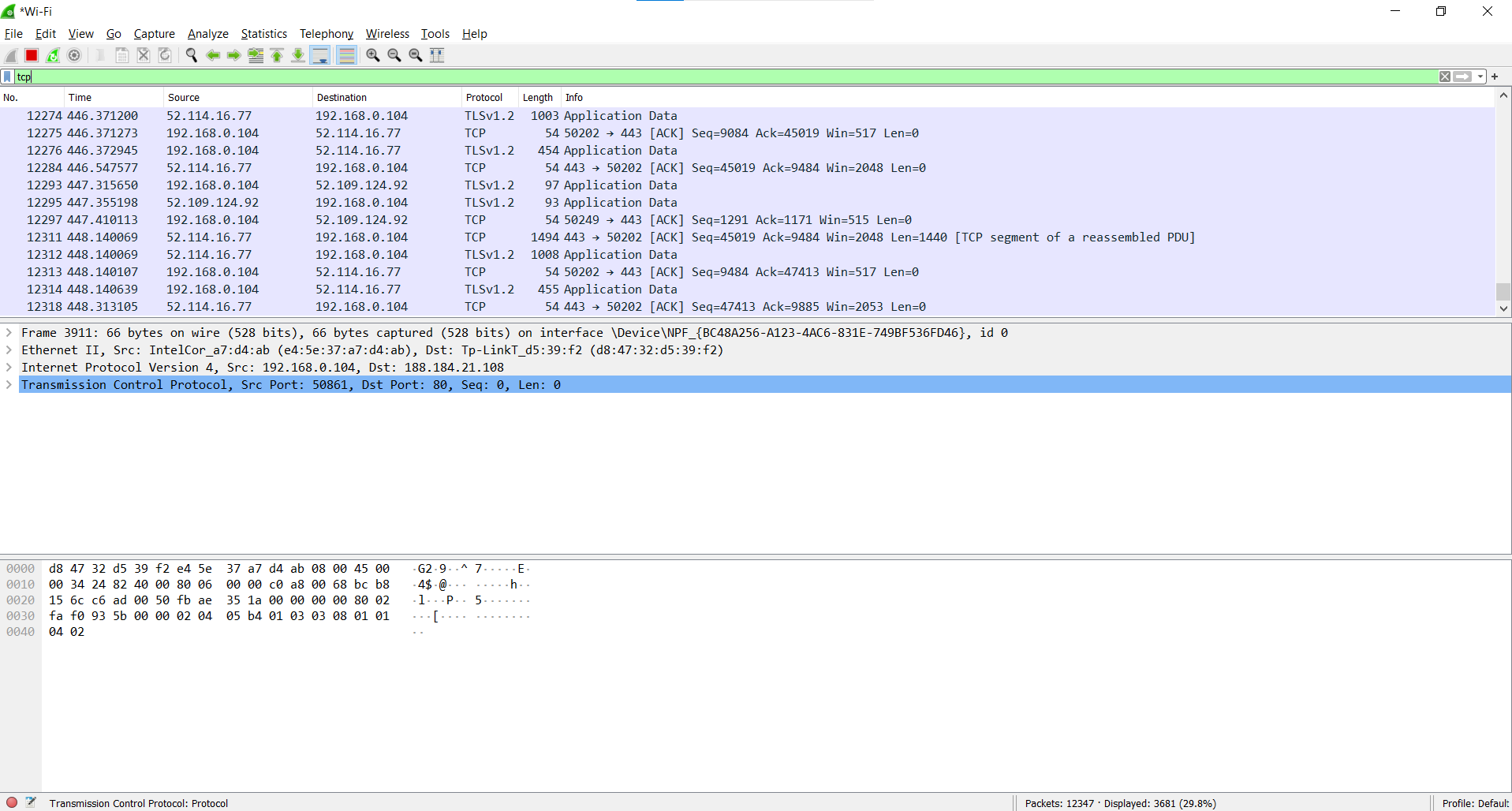


4. Ip.dst == 192.168.0.104

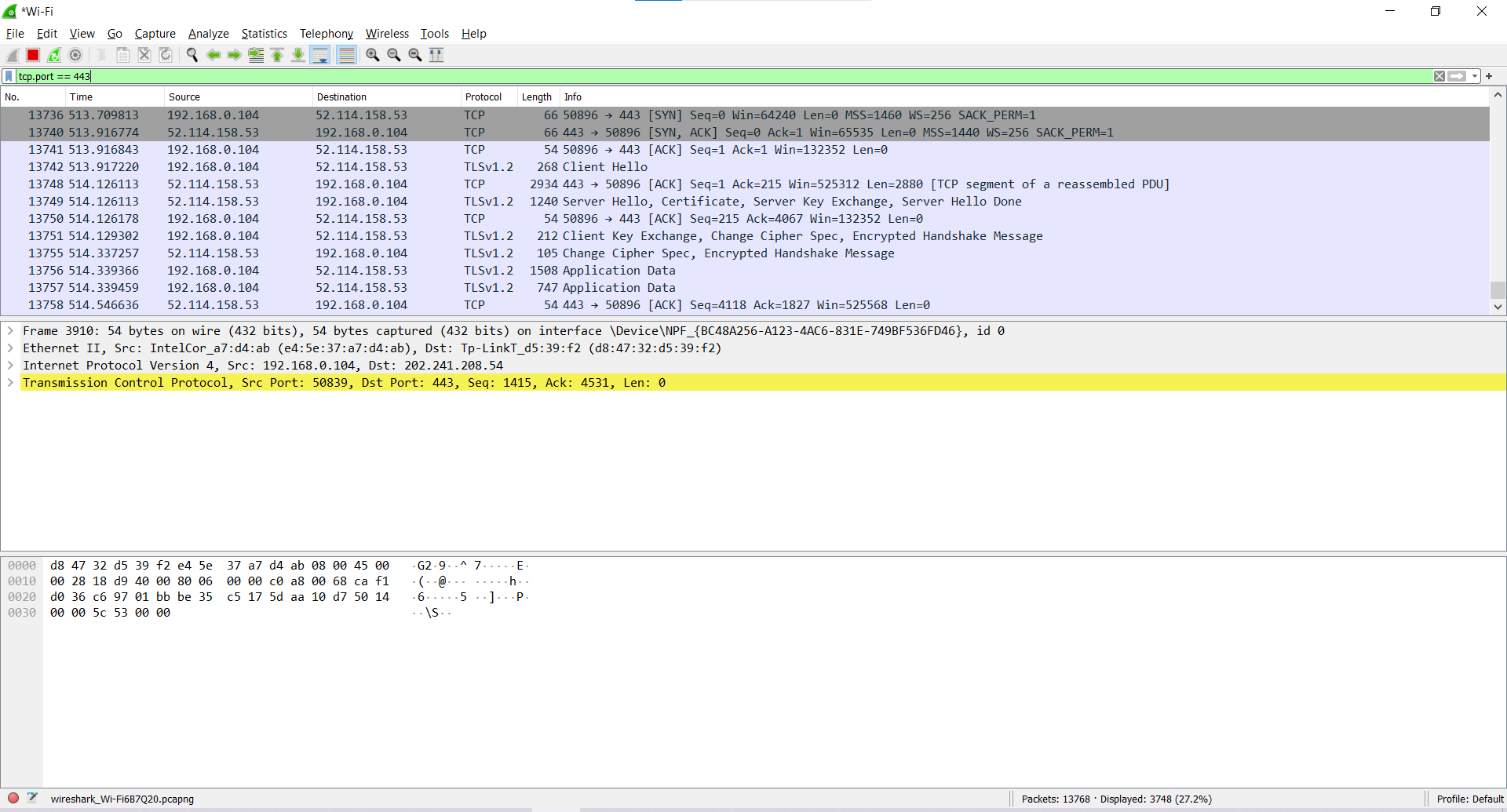


5. Dns or tcp

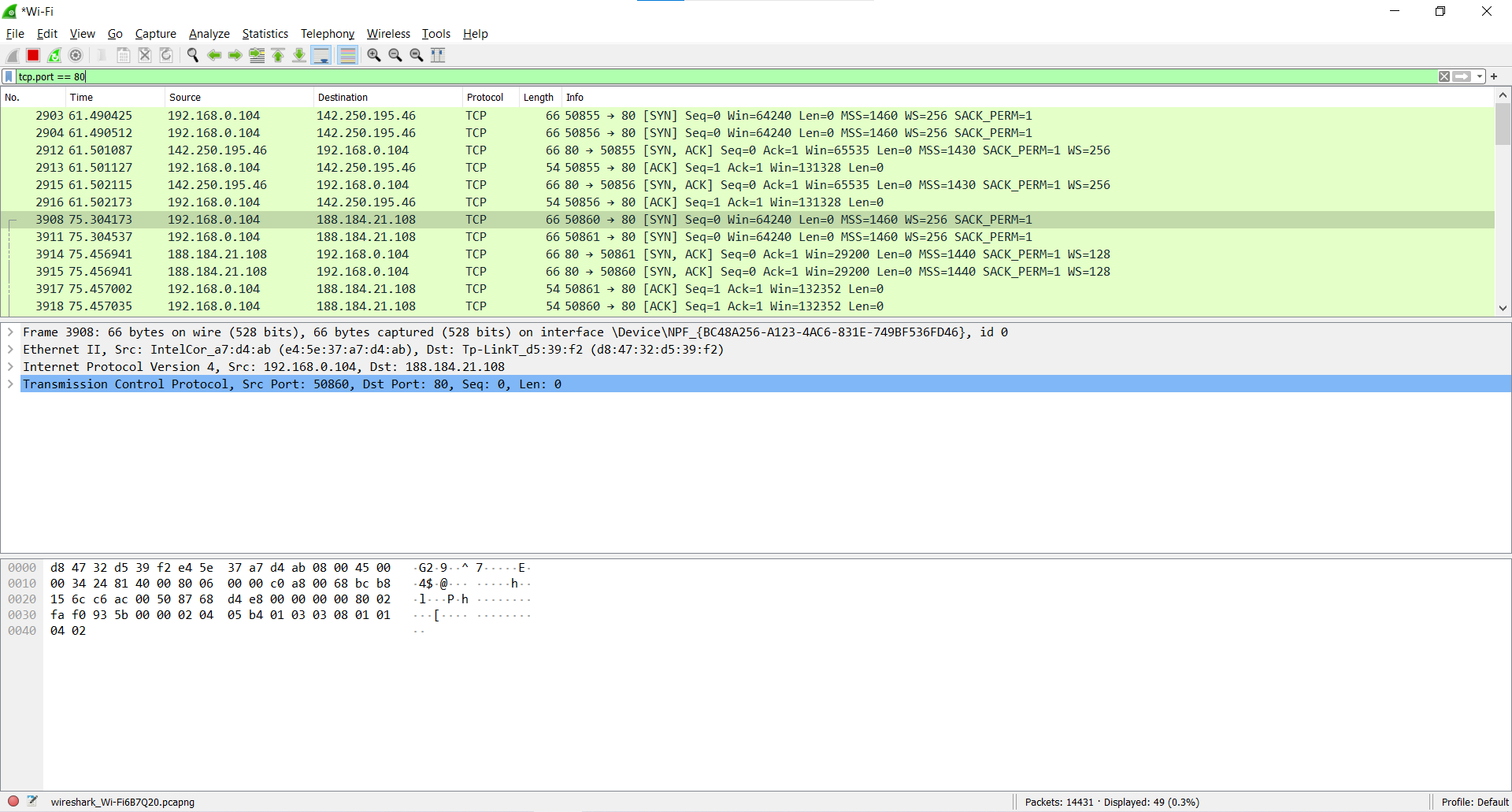




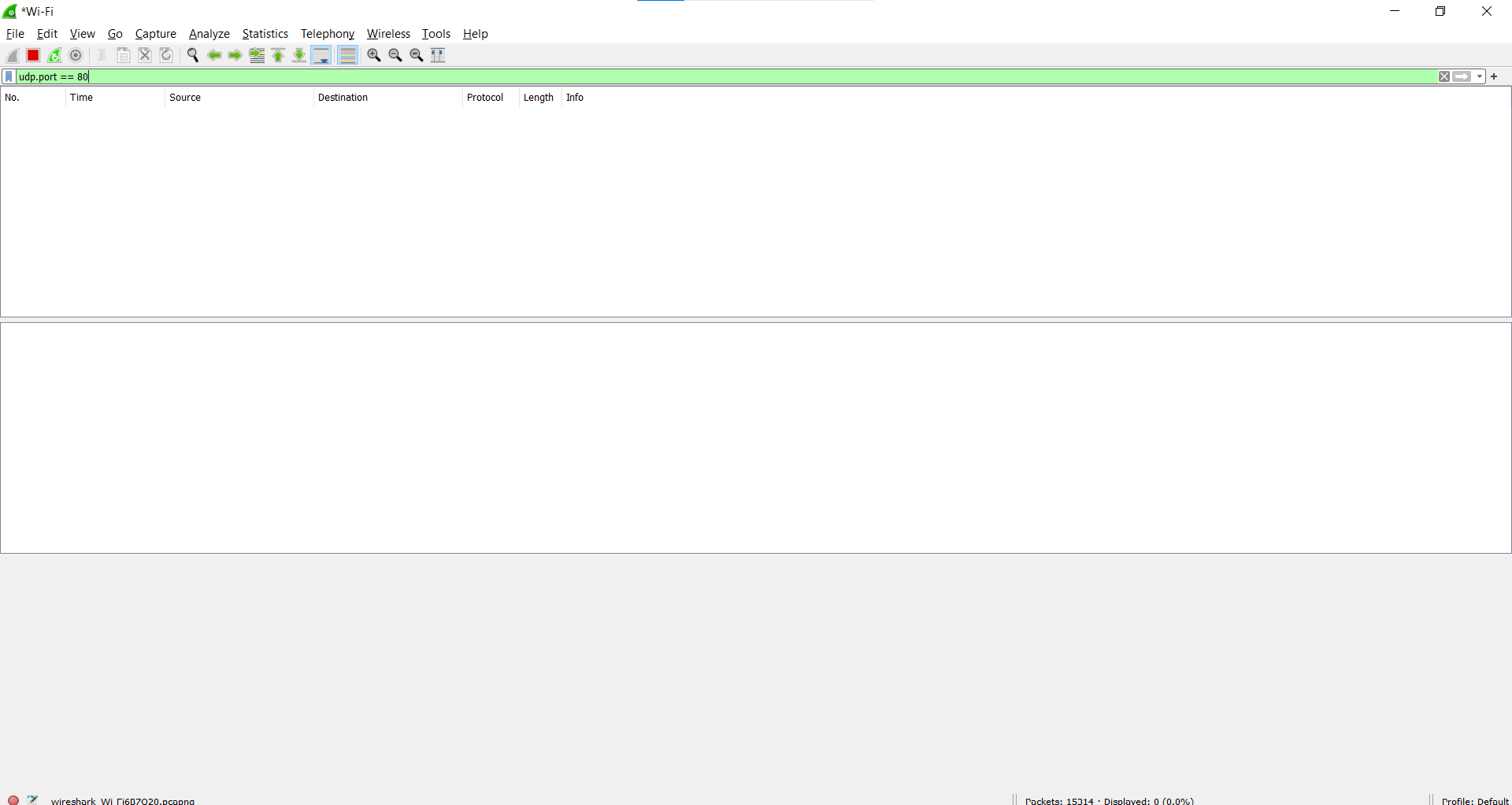
6. Tcp.port ==443



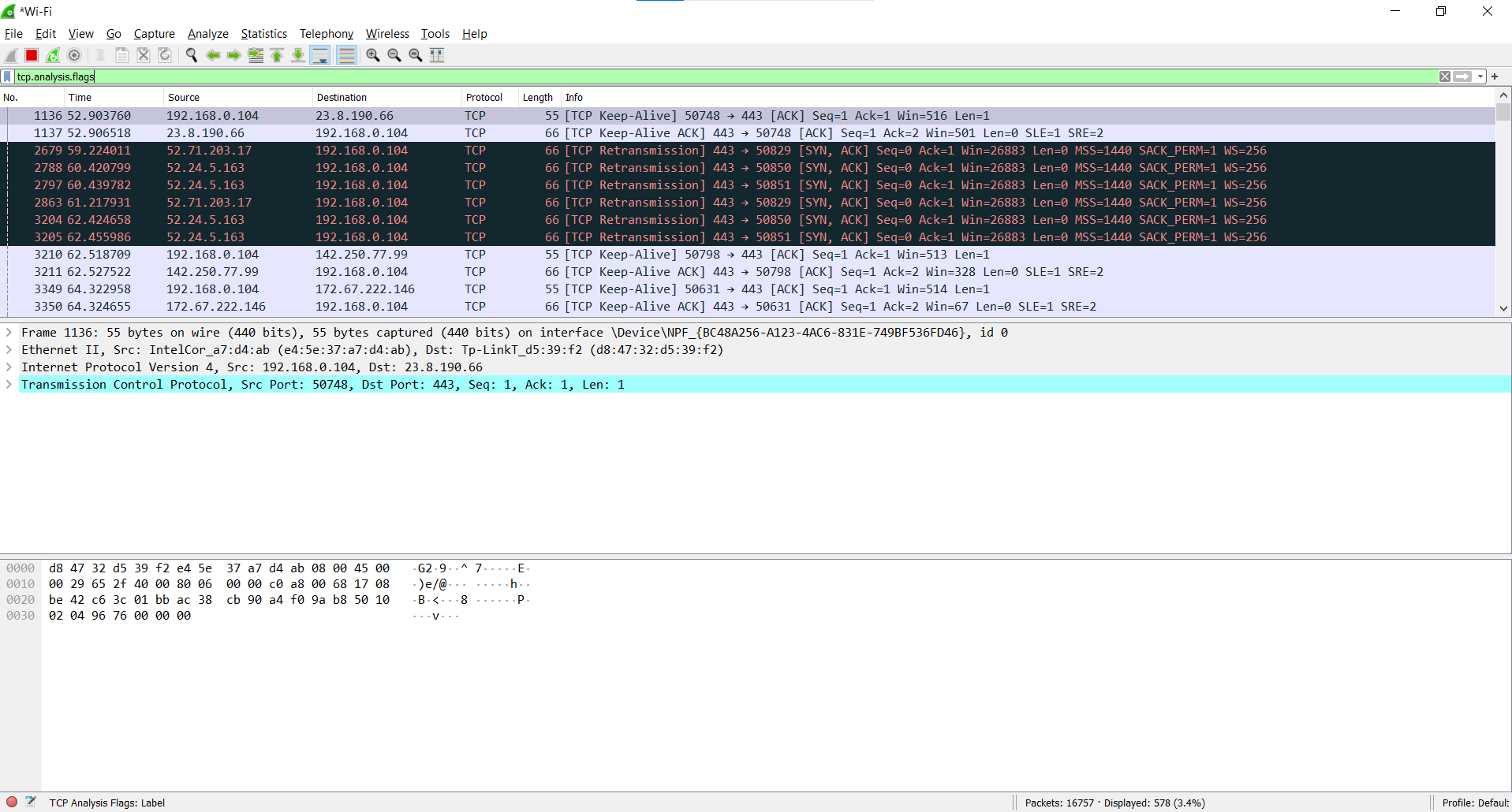
7. Tcp.port == 80



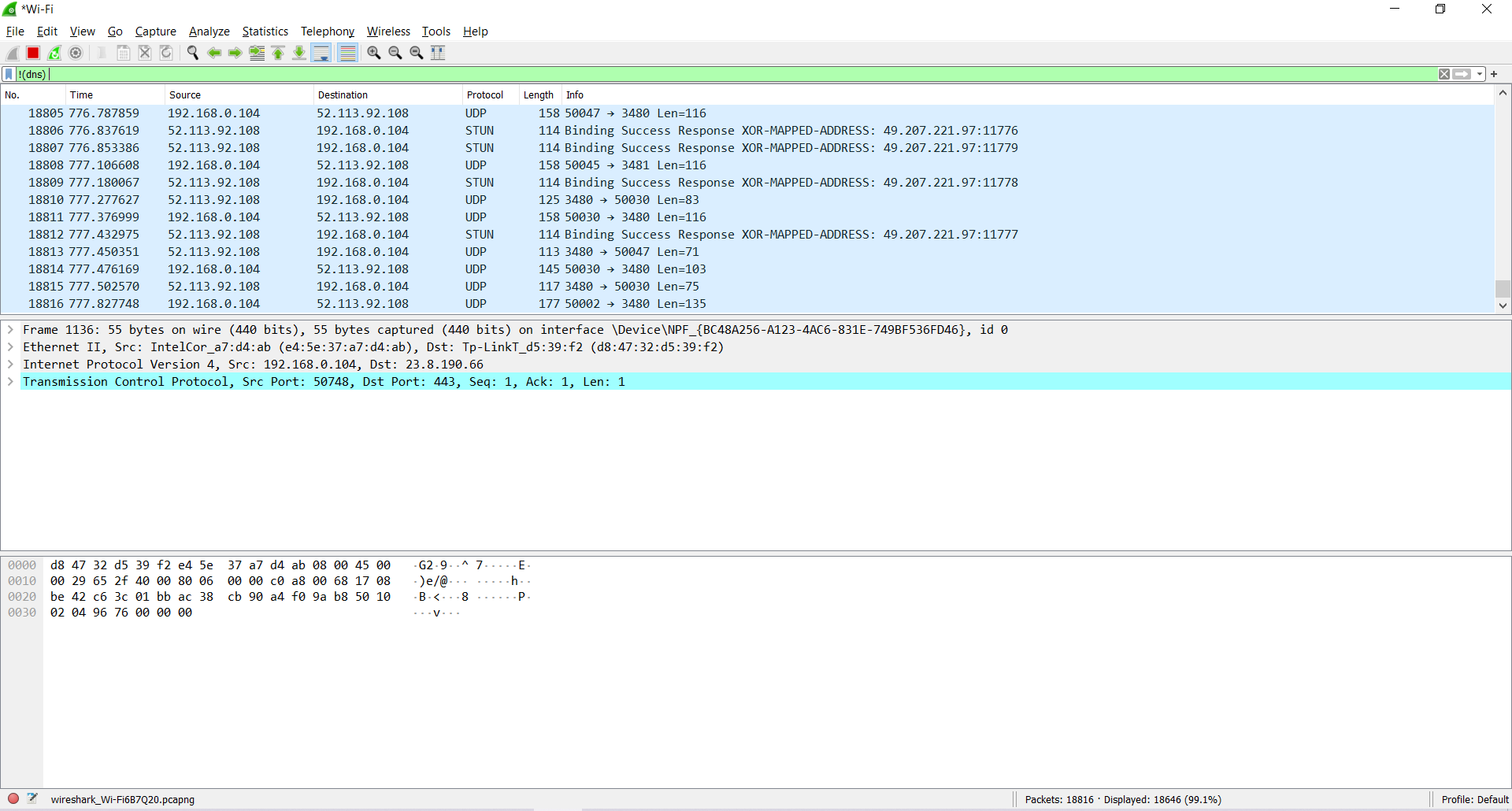
8. Udp.port == 80



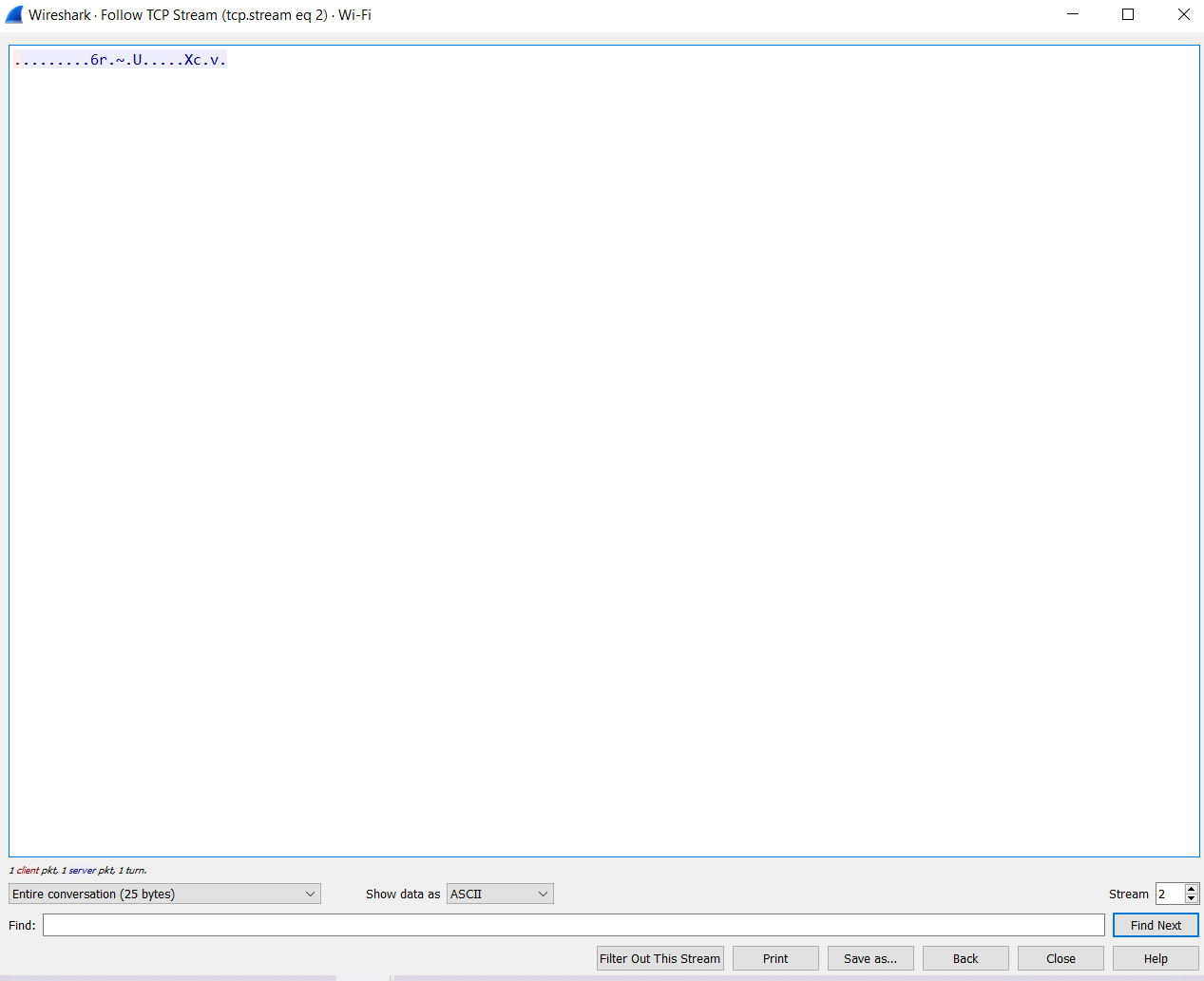
9. Tcp.analysis.flags



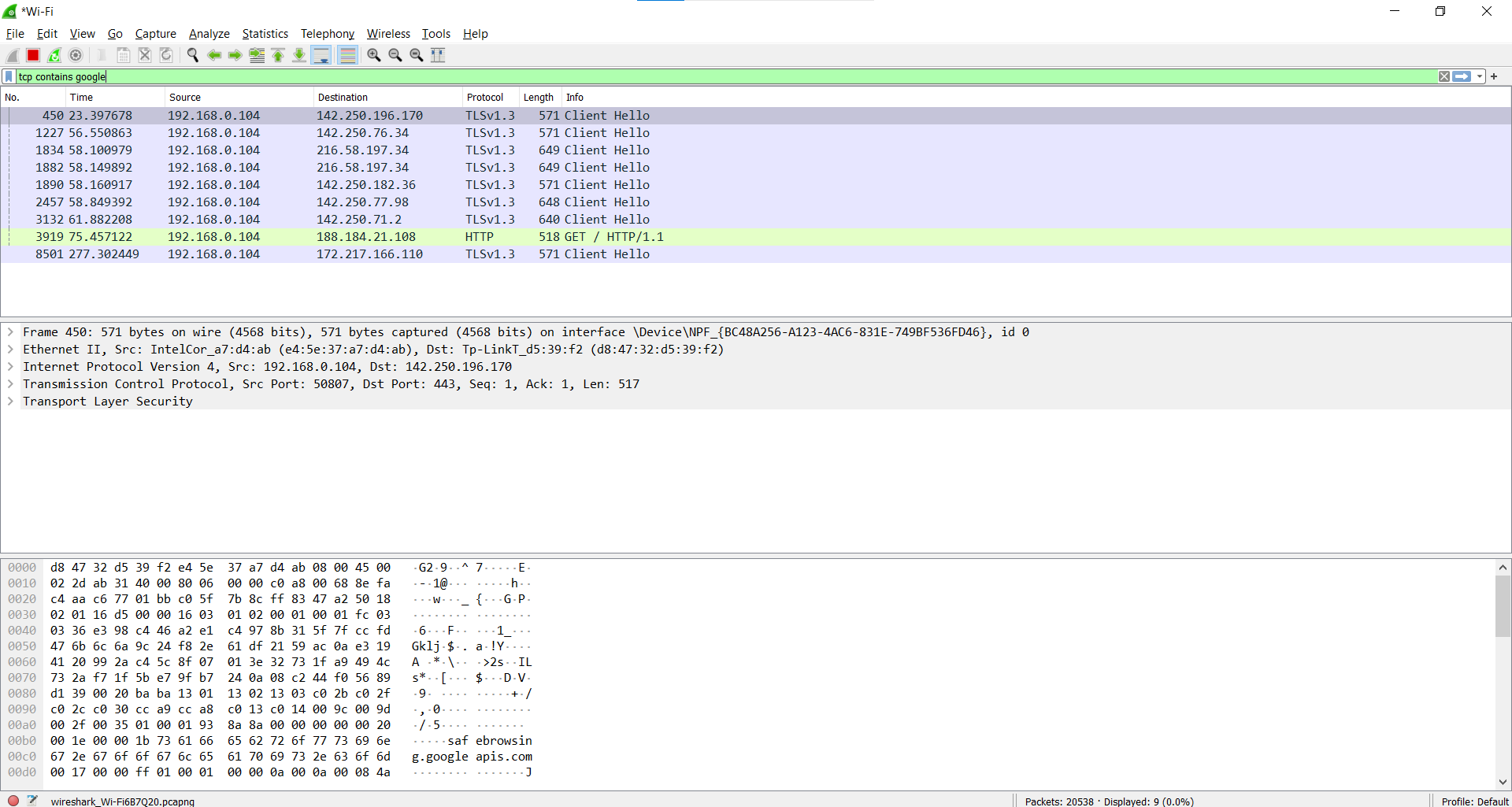
10. !(udp)



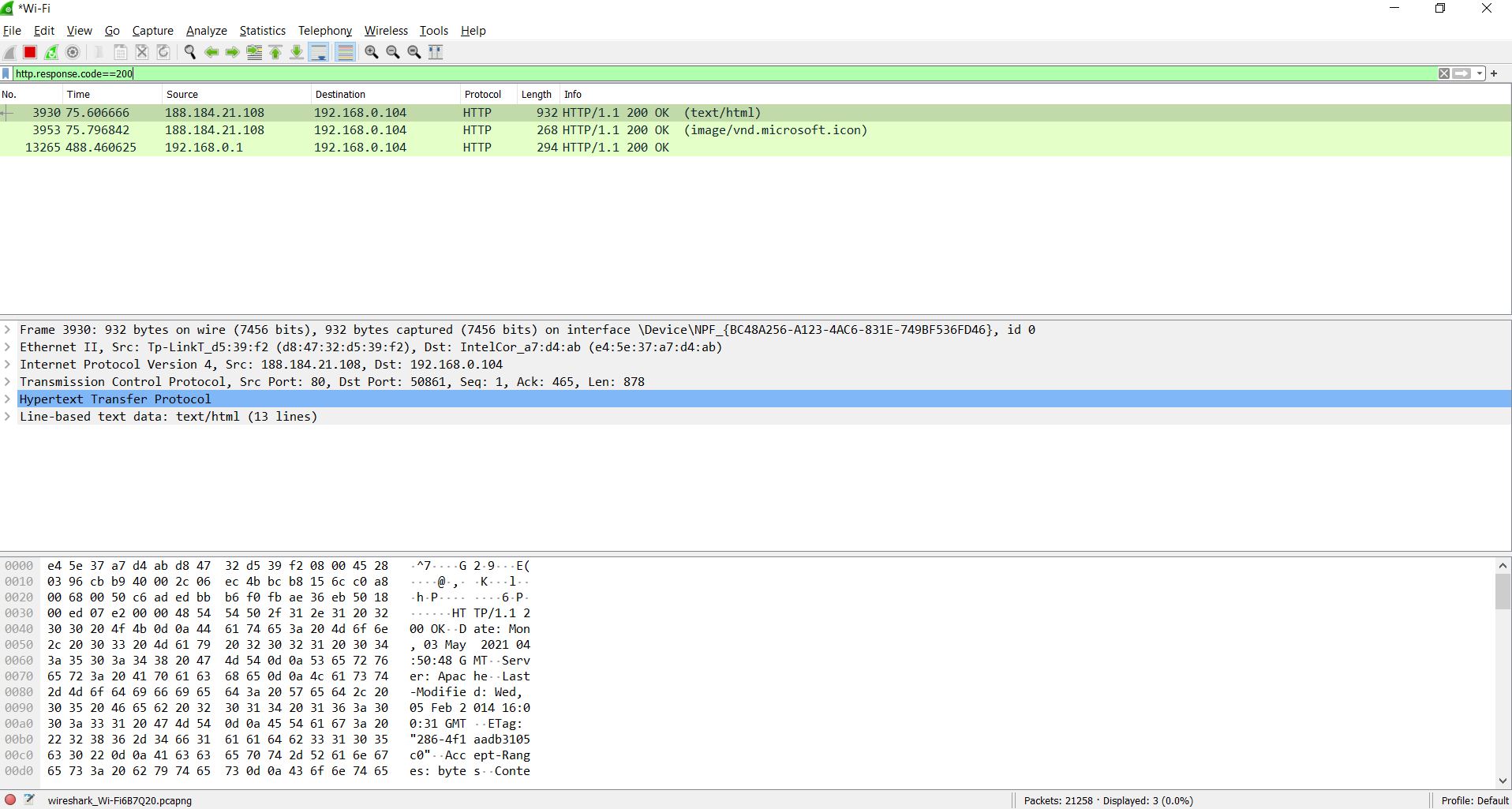
11. Follow tcp stream



12. Tcp contains google



13. Tcp.response.code==200



14. Tcp.flags.syn==1

