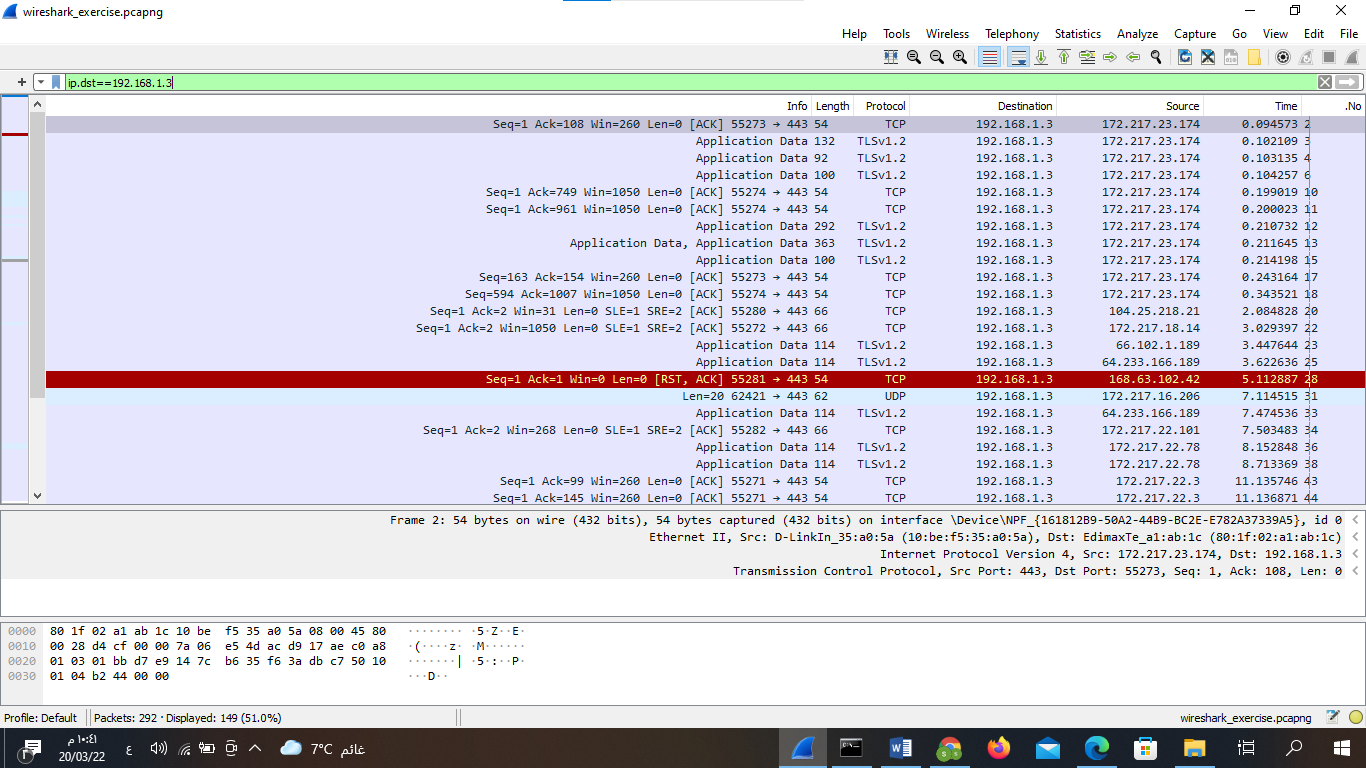
Wireshark Lab - Exercise 2 - PCAP

Download the PCAP file from Moodle and answer the following questions:

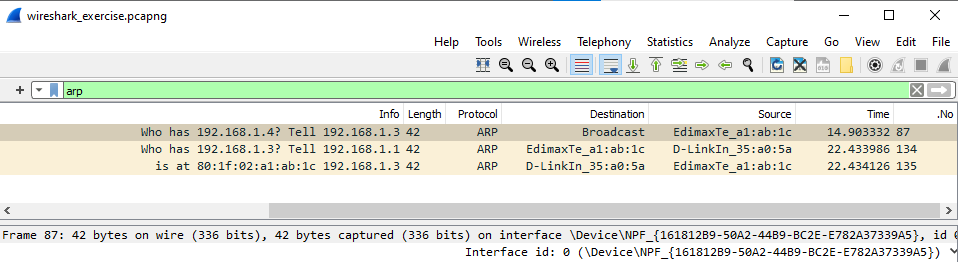
1. How many packets were sent to 192.168.1.3? 149 packet

ip.dst==192.168.1.3

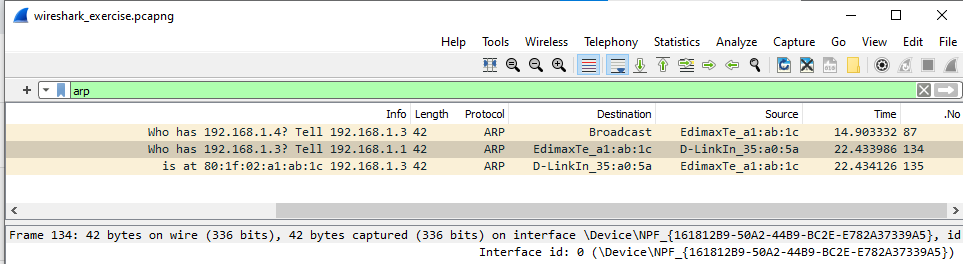
2) What frames are ARP frames? Provide the frame numbers.

arp

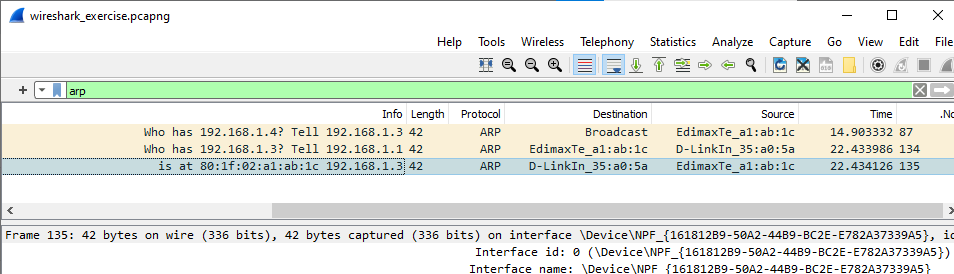
Frame1=87



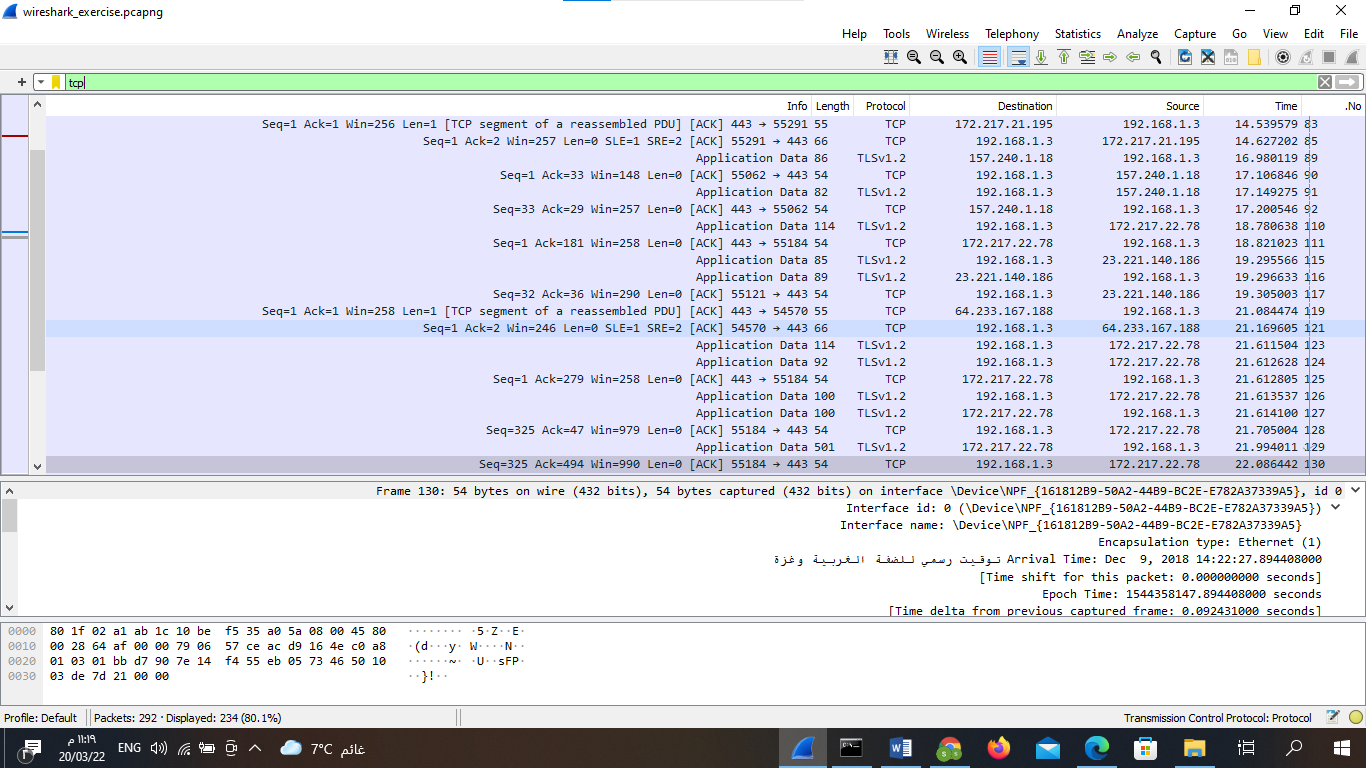
Frame2=134



Frame3=135

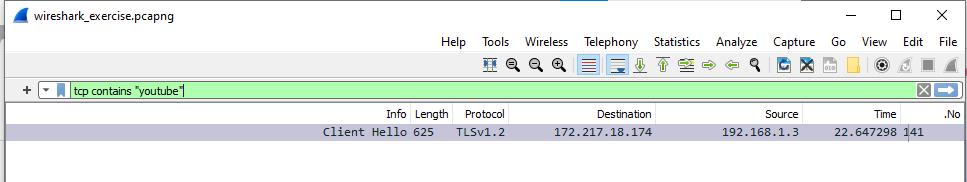
3) How many packets have we captured overall? 292

4) How many of these packets are TCP (Transmission Control Protocol) packets? 234



5) Write filter to find packets that request from YouTube 1 packet

tcp contains "youtube" or http.request



6) Analyze the packet number 84 into its equivalent in osi model

Network layer

Ip v4

header length =20bytes

time to live= 128

protocol UDP (17)

Source address: 192.168.1.3

Destination address: 82.102.187.85

Transport layer

Source port: 52684

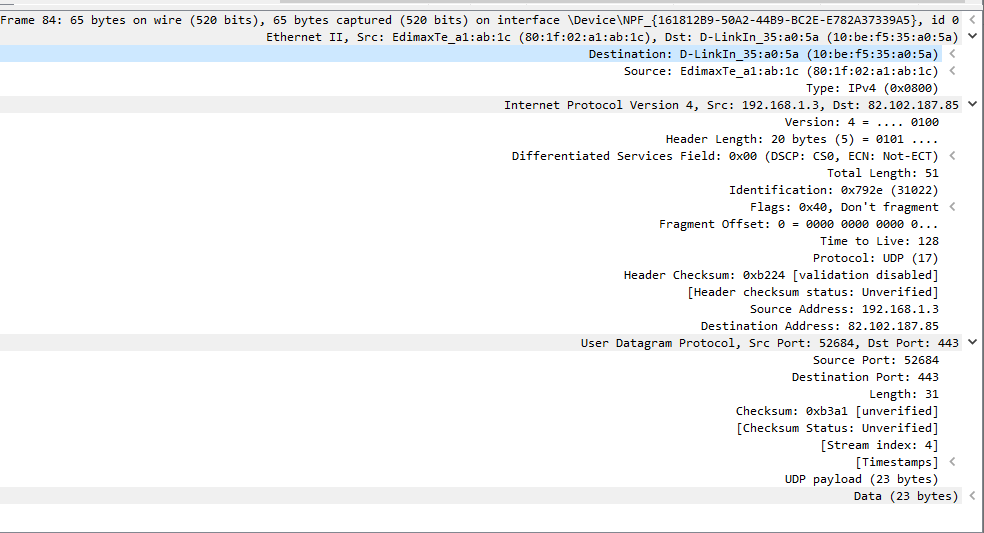
Destination port: 443

length =31

Ethernet layer

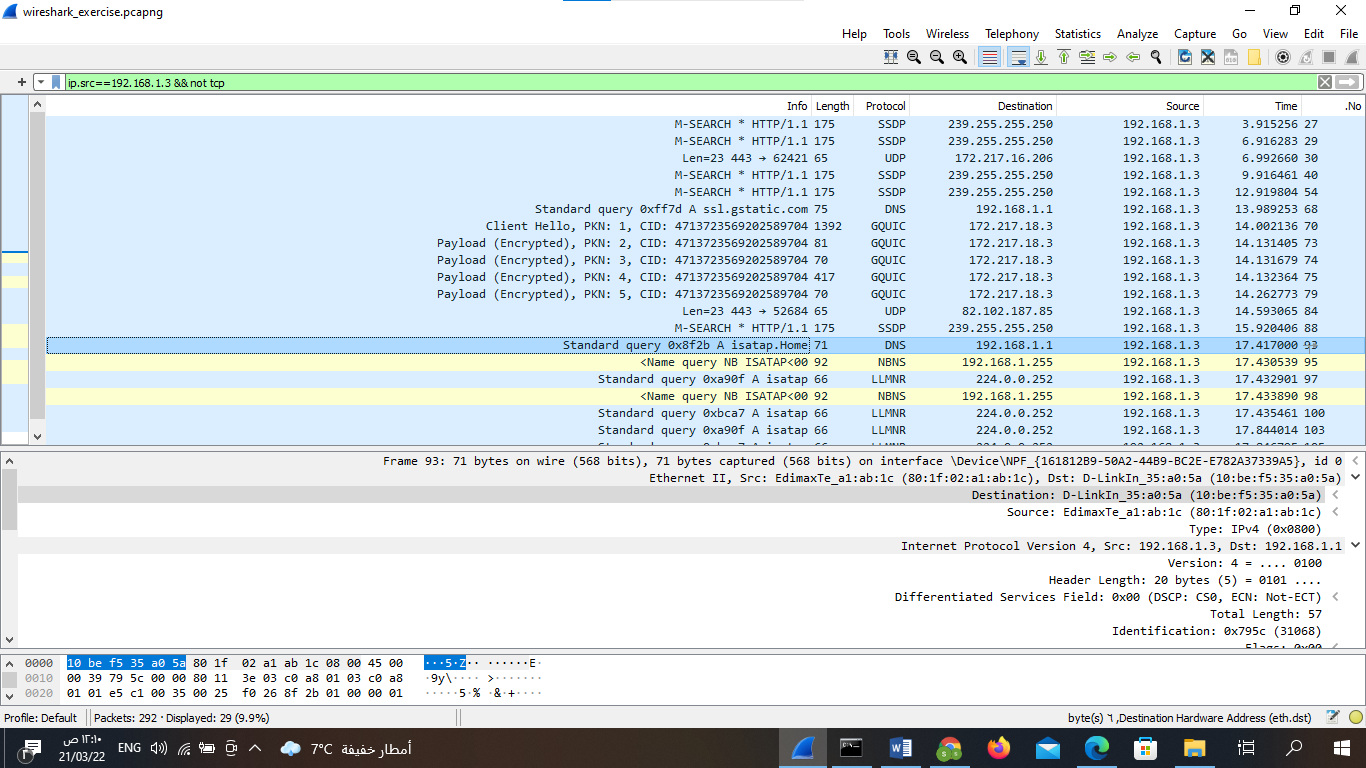
Destination:10:be:f5:35:a0:5a

Source: 80:1f:02:a1:ab:1c



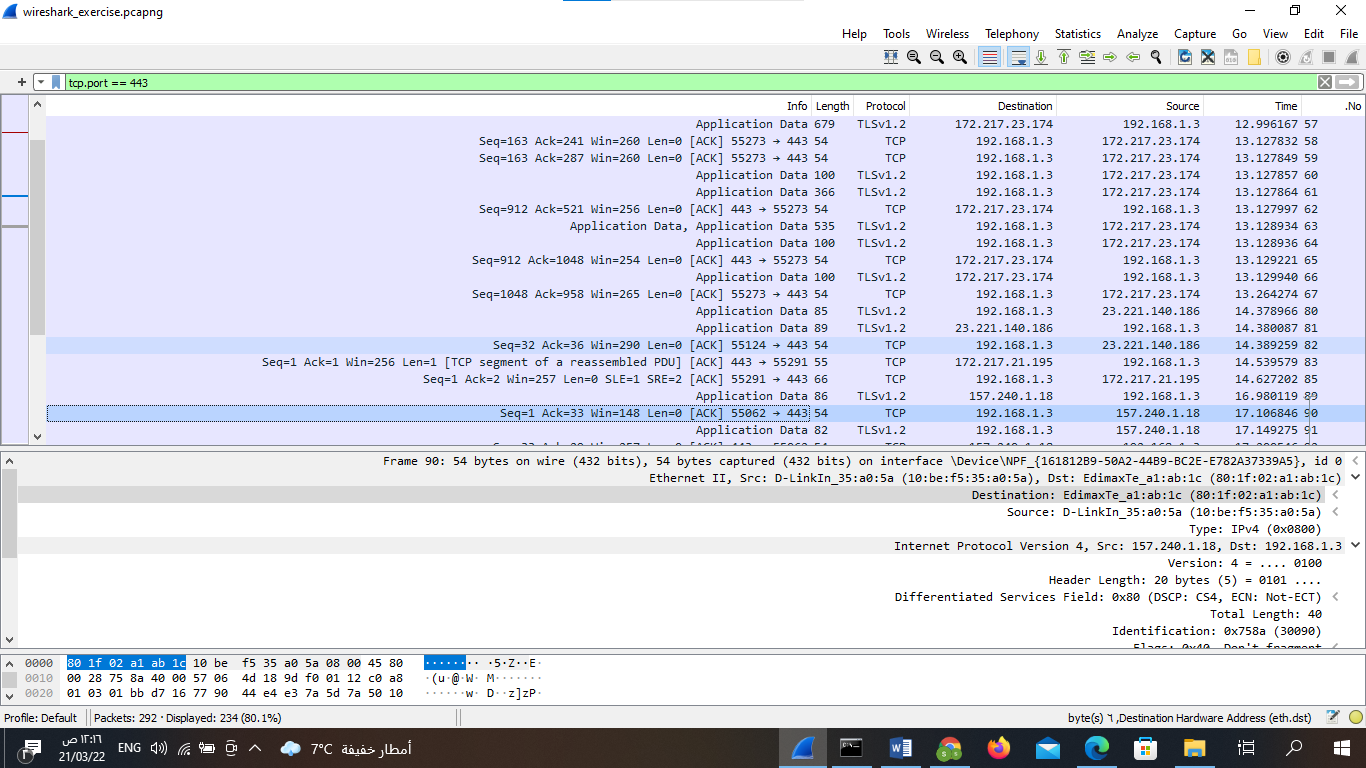
7) Filter all traffic coming out address 192.168.1.3 but not tcp packets

ip.src==192.168.1.3 && not tcp /29 packet



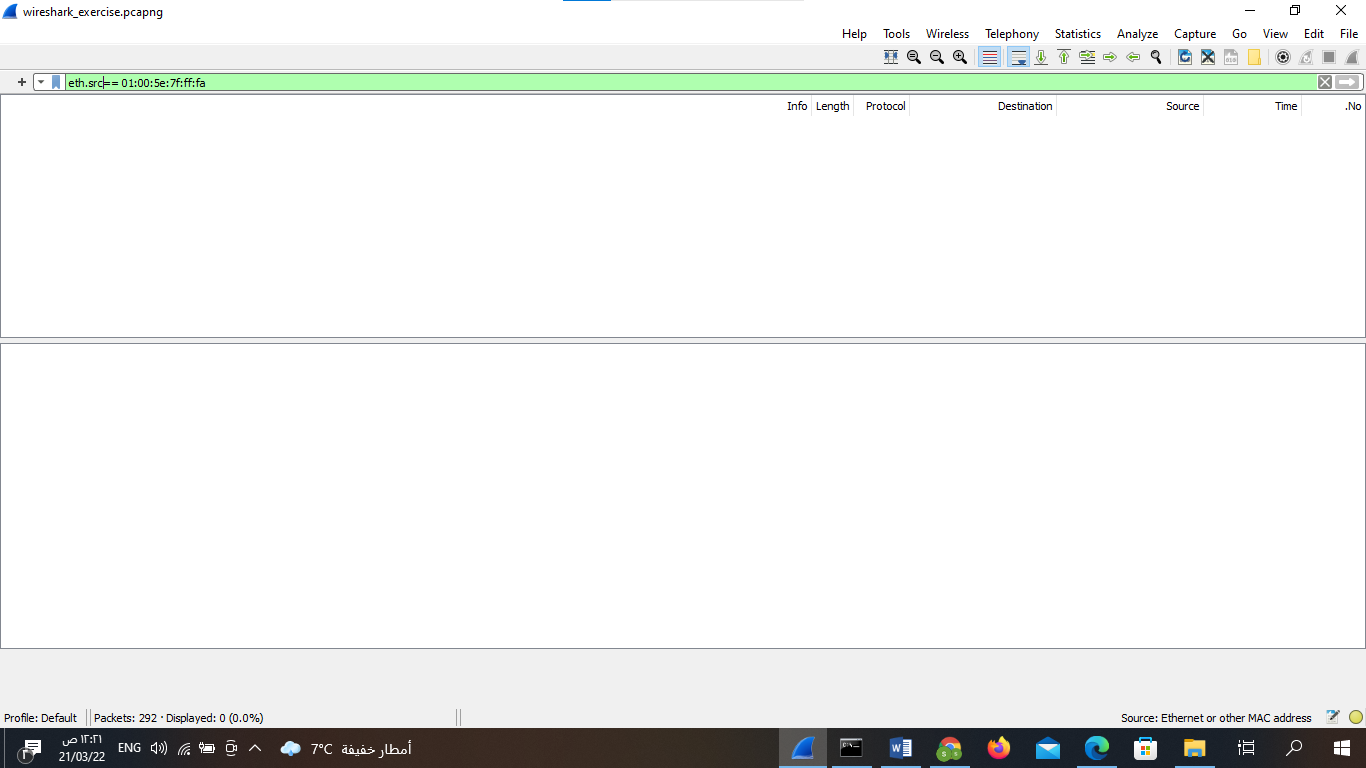
8) Filter all https traffic 234 packet

tcp.port == 443



9) Filter all traffic from mac 01:00:5e:7f:ff:fa 0 packet

eth.src== 01:00:5e:7f:ff:fa



10) Filter all dns traffic or traffic from host 192.168.1.3 130 packet

dns or ip.src==192.168.1.3

