Exercise 3 – Traffic analysis and identifying the OSI layers of the network packets

Difficulty: Hard

Prerequisite:

Search online and get familiar with the TCP's three-way handshake. Learn how to capture the three way handshake using Wireshark.

Install Wireshark on your computer and use it to capture traffic against a website or a server or your choice. It is recommended that you capture traffic against a simple website.

Name and the IP address of the website you plan to capture traffic:

Name:abv.bg

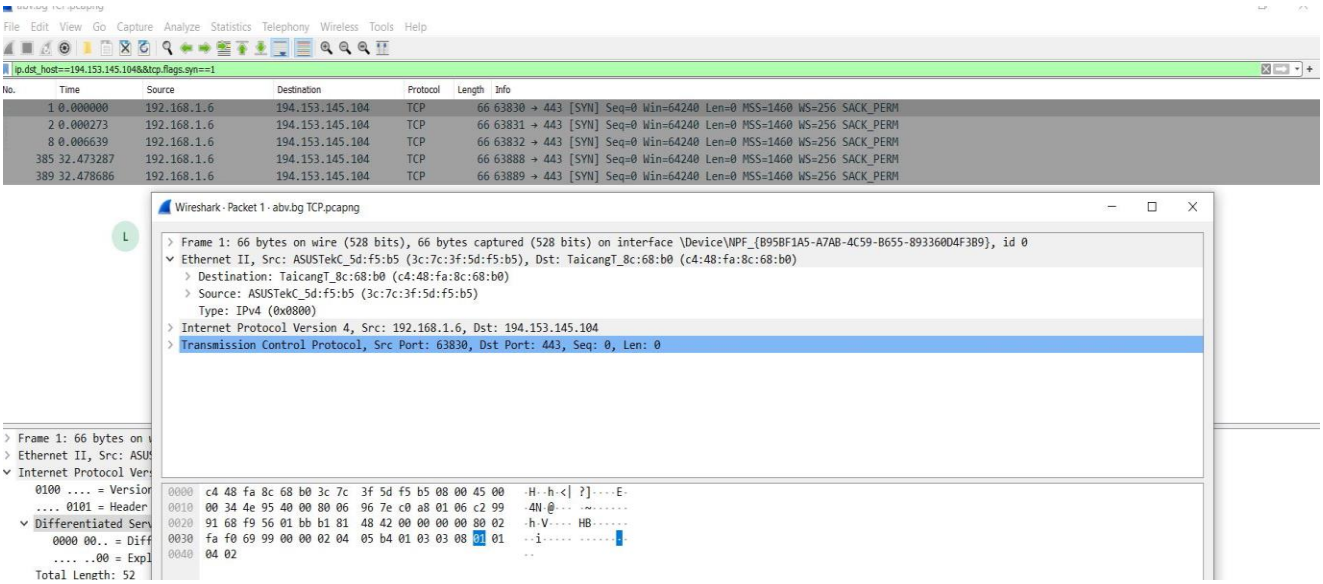
IP:194.153.145.104

Analyze the TCP's three-way handshake and using screenshots from the Wireshark window answer the questions bellow:

1. What is the source IP (of the initiating host): 192.168.1.6

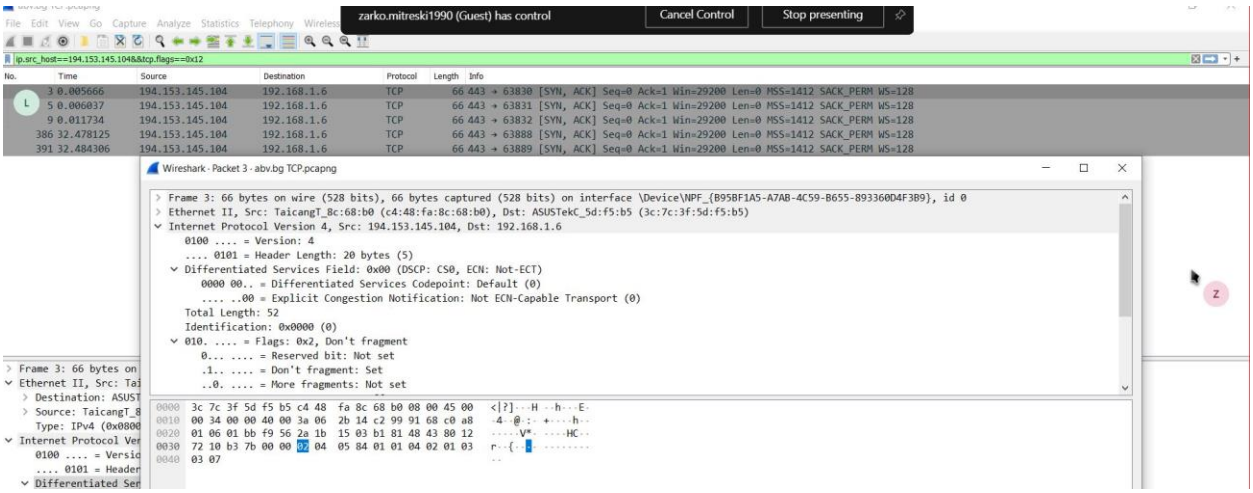
2. What is the destination IP? (target website): 194.153.145.104

Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:



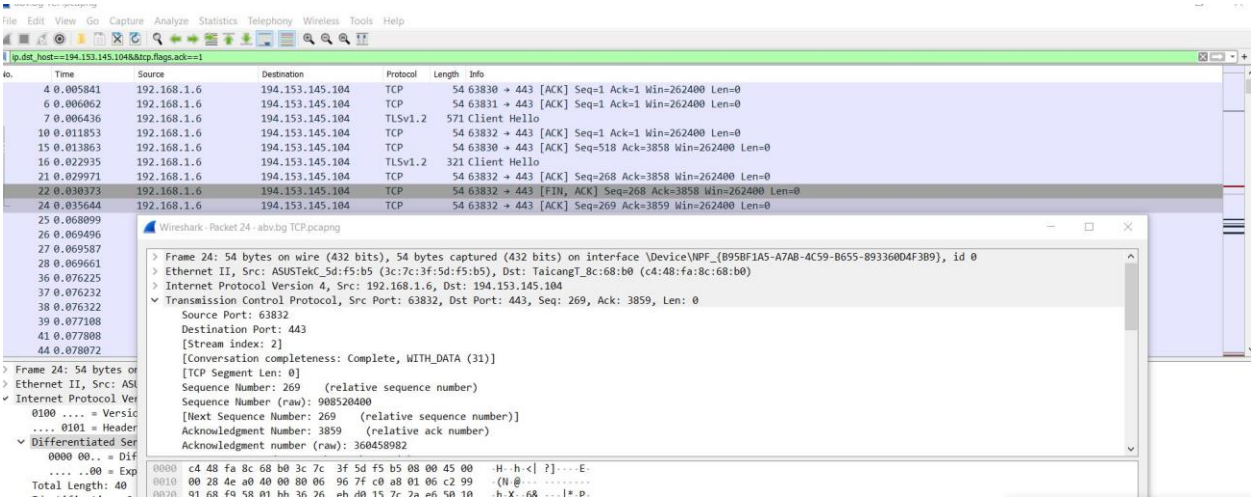
Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot

from it:



Identify the Transport Layer 4 section of the ACK packet and paste a screenshot

from it bellow:



Look closely at the L2 section of the three-way handshake packet details. Each of themshows the source and destination MAC address of the packets.

Who is the owner of the destination MAC address of the SYN packet?

Destination MAC: c4:48:fa:8c:68:b0