Questions on Wireshark

Before you begin this assignment, close all other applications that may introduce network traffic, eg. browsers, chat/email clients

1. List atleast 4 different protocols that appear in the protocol column on running wireshark.

2. Do the following:

    a)Start the packet capture

    b)open a web page: say www.google.com/

Report the timegap between the HTTP GET message and HTTP OK reply (Refer to the time column in Wireshark).

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Show the selected packet in wireshark to the TA

a) What is the 48-bit MAC of your machine?

b) What is the 48 bit destination address in the Ethernet frame? Whose Ethernet address is that (of the website)?

c) Look at the contents of the Ethernet frame containing the first byte of the HTTP response message and state:

i) what is the value of the Ethernet source address? Which device has this Ethernet address?

ii) What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?