Use Wireshark to capture packets in your LAN.

1. Show a round of execution of the DHCP protocol. Write the filter and show the output in a screenshot.
    a. Show DHCP Request (2 marks), Reply (2 marks), and ACK messages (2 marks) in that round.
    b. Find out IP addresses of the DHCP server (2 marks) and client (2 marks).

2. Show a round of execution of the ARP protocol. Write the filter and show the output in a screenshot.
    a. Show ARP Request (2 marks) and Reply (2 marks) messages in that round.
    b. Find the MAC address of the the replier (2 marks).

3. Show a round of execution of the `traceroute' command for dns.google.
    a. What is the IP address of your host (1 mark) and the destination (1 mark)
    b. Examine the raw bytes of the ICMP echo packet. Capture a screenshot of the raw bytes and identify the bytes that represent the type and code. (3 marks)
    c. Examine the raw bytes of the ICMP error packet. Capture a screenshot of the raw bytes and identify the bytes that represent the type and code. (3 marks)
    d. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different? (4 marks)

Submit the pcap file and the PDF containing the answers. Please submit a single zip file named <Name>_<ID_number>. Make sure to turn in your submissions on time.