At the beginning of the page, specify the following:

1. Hammud Haq (996013884) (A03)
2. Hoai-An Ho (917000915) (A01)
3. Name of the code and Pcap files submitted:
    a. pcap_analyze.py

Answer the following questions:

1. How many devices are connected to this hotspot? (4 points)
    a. We counted 15 unique MAC addresses
2. Which device sends out the most number of packets? (3 points)
    a. A device by the MAC address of **2c:db:07:49:39:b9**
3. Which device receives the most number of packets? (3 points)
    a. A device by the MAC address of **2c:db:07:49:39:b9**
4. Is there any endpoint where more than one device sends out a network packet to it? List the IP addresses of these endpoint(s)? (4 points)

    Frame 156404:
    Src: 10.42.0.149 (10.42.0.149), Dst: youtube-ui.l.google.com (142.250.189.238)

    Frame 161374:
    Src: 10.42.0.52 (10.42.0.52), Dst: youtube-ui.l.google.com (142.250.189.238)

    Frame 65321:
    Src: 10.42.0.32 (10.42.0.32), Dst: youtube-ui.l.google.com (142.250.72.142)

    Frame 64186:
    Src: 10.42.0.149 (10.42.0.149), Dst: youtube-ui.l.google.com (142.250.217.142)

5. Which application layer protocol has been used the most by the devices? (4 points)
    a. DNS protocol, or Domain Name System.
6. Identify how much time did it take for us to capture this Pcap file (in minutes). (4 points)
    a. Looking at the first and last packets, the timestamp range is from 2022-10-07 01:01:47.781776, to 2022-10-07 01:12:44.637144. This spans a range of 656.855368 seconds
    b. **10.9475895 minutes**

7. Can you tell whether the devices send packets concurrently or sequentially 1? Explain your approach to figure the sets of devices with concurrent/sequential network traffic. List the sets of devices with concurrent traffic. (4 points)
    a. You can check what devices send packets concurrently vs sequentially by looking at the protocols used to transmit the data. TCP, XID, HTTP, DNS, MDNS, and TLSv1.3 (is encrypted but still sequenced) use sequential data transmission while UDP, QUIC IETF, IGMPv3, ICMP, ICMPv3.
    Concurrent Devices + Packets Transmitted or received Concurrently
    Address: ff:ff:ff:ff:ff:ff # of packets: 4
    Address: 01:00:5e:00:00:fb # of packets: 85
    Address: d4:c9:4b:a0:c8:a2 # of packets: 526 + 1331
    Address: 22:18:82:26:e2:56 # of packets: 2938 + 4361
    Address: f8:e6:1a:6d:5f:89 # of packets: 4490 + 7614
    Address: a8:7e:ea:67:30:d6 # of packets: 5990 + 28630
    Address: 2c:db:07:49:39:b9 # of packets: 41937 + 13856
8. Can you figure out at approximately what point of time the devices were disconnected from the hotspot? (hint: Look at the final packets using Wireshark) (4 points)
    a. Frame: 186683
    TimeStamp: 536.296887
    Source IP: 142.251.214.132 (Intel Device)
    Destination IP: 10.42.0.193 (Motorola Device)
    Protocol: TCP
    Packet Length (Bytes): 156