Lab #9 - SY310 Traffic Analysis (Layer 5 – Application Layer)

Using the provided `layer5part1.pcap` file in Wireshark, complete the following questions.

Question 1: List the MAC address and IP address for:

- The client device: ____ . ____ . ____ . ____ ___:___:___:___:___:___
- The DHCP Server: ____ . ____ . ____ . ____ ___:___:___:___:___:___
- Local DNS Server: ____ . ____ . ____ . ____ ___:___:___:___:___:___
- Gateway Router: ____ . ____ . ____ . ____ ___:___:___:___:___:___

Question 2: What is the network address (in CIDR notation)?

Question 3: What is the client’s hostname?

Question 4: List all of the URLs and associated webserver IP address that the client connected to.

Question 5: For each website list the frame numbers for the initial 3-way handshake.

Question 6: What was the URL for the first DNS lookup? What was the IP address of the URL? Why is there no associated HTTP traffic in the pcap?

Question 7: Which site required HTTPS?

Question 8: What specific article did the client read on the 3rd website?

Using the provided `layer5part2.pcap` file in Wireshark, complete the following questions.

Question 9: What is the physical medium for this capture?

Question 10: What channel was the SSID in frame 10875 transmitting on?

Question 11: List all the clients that received probe responses from SSID 'CMY'

Question 12: How many probe requests, response, and beacons were in this capture?

Question 13: What Access Points has the client 'd8:d1:cb:07:d1:c0' connected to in the past? List at least 5. What are the possible security aspects of this leaked information?

EXTRA CREDIT: Can you figure out what specific type of device sent the probe request in frame 9770?