WioT - Postlab

Lab 1: Wireshark and your local network

What to submit?

Please use this document as a template, add your responses directly, and export it as a PDF to Gradescope. Each student should submit their own report.

Name:
Computing ID:

A: Finding and Inspecting Your Own Traffic

[2pts] Show a screenshot of your captured *ping* traffic:

[1pt] *Postlab:* What does "ICMP" stand for?

[3pts] *Postlab:* For one of your *ping* packets, start from the PHY and list each of the layers that were used to send the packet, and which technology was used:

B: Insecure Chat

[3pts] Show a screenshot of your captured *netcat* traffic from both you as a listener and as a sender. Clearly document which case is which.

[2pts] *Postlab:* Can you see other *netcat* traffic from other students in the class? Why or why not?

[2pts] *Postlab:* Imagine you were having a *netcat* conversation with a friend at George Mason. Besides you and your friend, who else could see the contents of your conversation?

C: Discover WiFi Networks Around You

[2pts] What is the name of the WiFi network we set up?

[2pts] *Postlab:* What are the types of probe packets that you see?

[2pts] *Postlab:* What filter did you use to see only packets from our test network?

[2pts] *Postlab:* What is the MAC address of the router for the test network?

D: Snooping Connection Formation

[4pts] Filter the traffic to isolate the connection process.
How did you identify the correct set of packets?

Show a screenshot of connection formation here:

[1pt] *Postlab:* What is the first type of packet that the computer sends to the router to initiate connection formation?

[2pt] *Postlab:* How do you figure out which packet is sent next? Is there some information in the packet that helps you identify this?

[1pt] *Postlab:* How do you know when the connection is established?

E: Inspecting Protocol Information

[2pts] What is the Tag Number for the SSID tag?

[1pt] Is the same tag number used for the SSID tag in all beacon packets?

[2pts] What is the Tag Number for the vendor specific tag?

[2pts] What is the access point name that ITS used?

Include a screenshot from wireshark showing the AP name here: