WioT - Postlab

Lab 1: Wireshark and your local network

## What to submit?

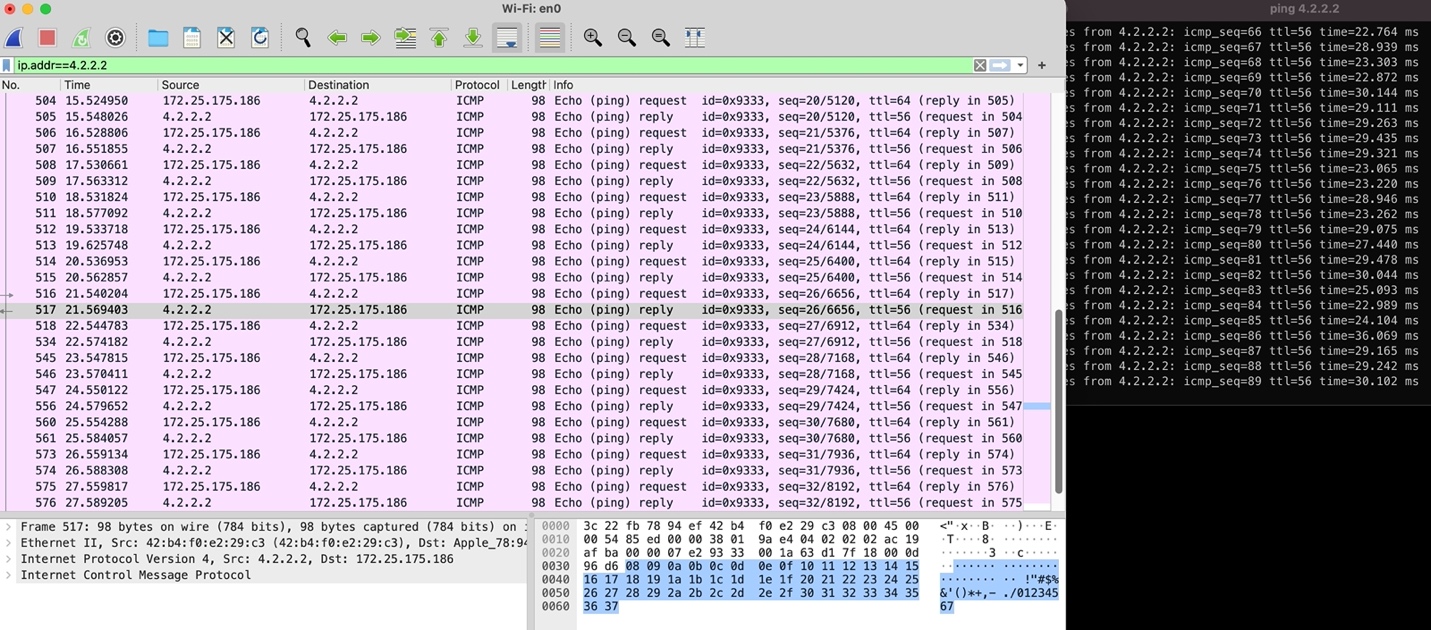
Please use this document as a template, add your responses directly, and export it as a PDF to Gradescope. Each student should submit their own report.

Name: Robert Owens

Computing ID: rao7utn

A: Finding and Inspecting Your Own Traffic

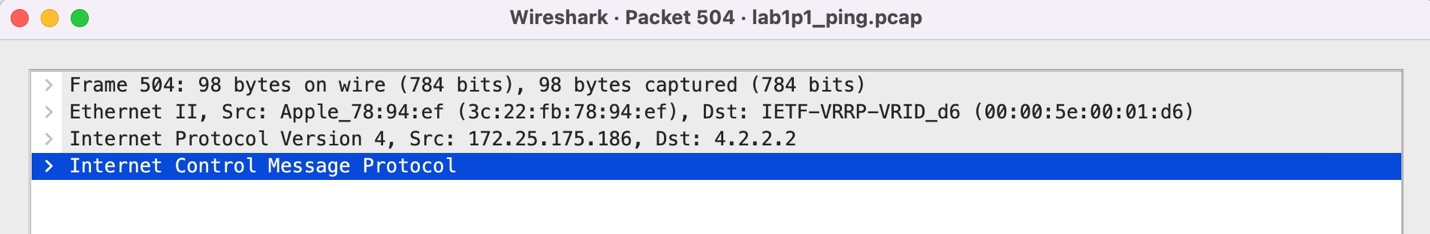
**[2pts] Show a screenshot of your captured *ping* traffic:**

****

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

Internet Control Message Protocol

**[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:**

****

Frame 504 – 98 bytes ICMP rule

Ethernet II - specifies an IPv4 source and destination address

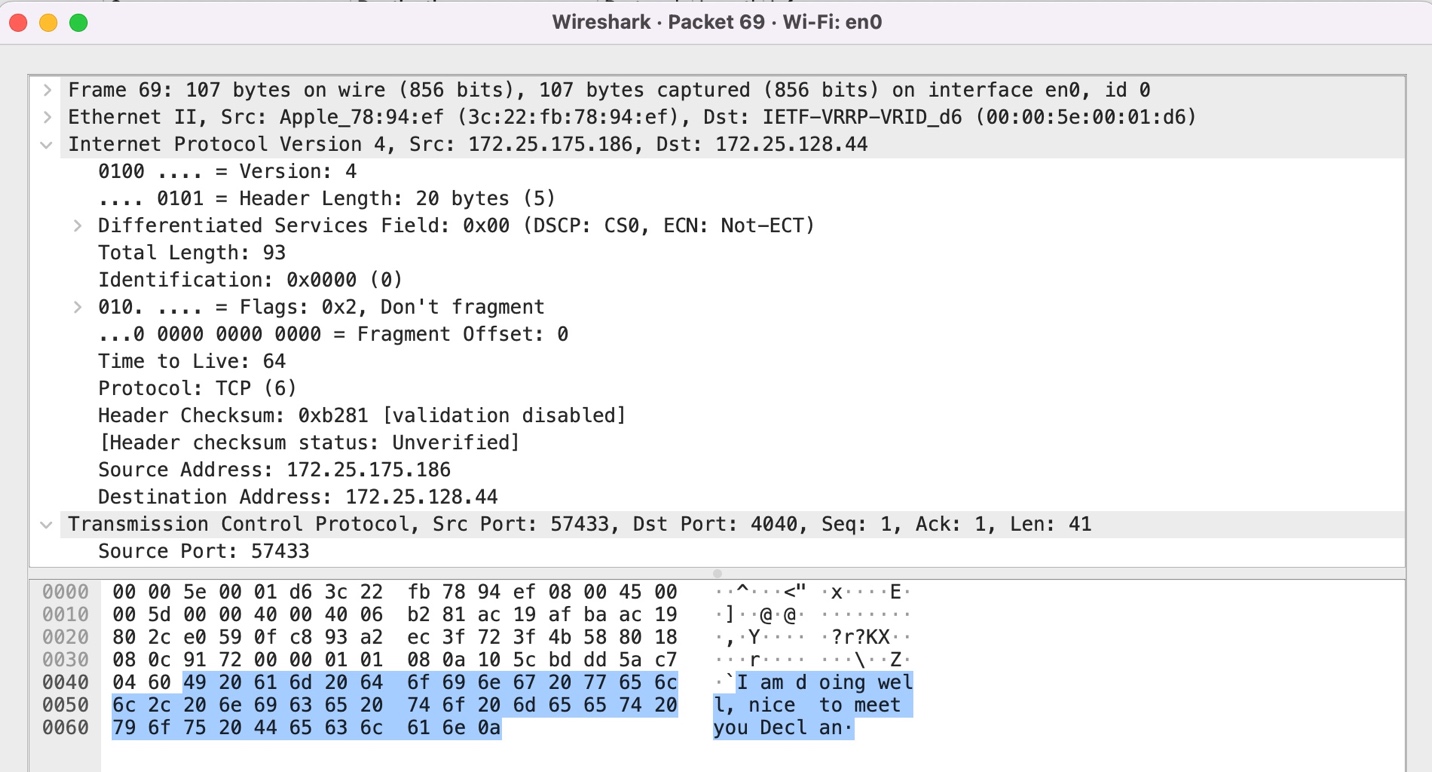
Internet Protocol Version 4 – this looks like the packet header – 20 bytes

Internet Control Message Protocol – I think this is just the returned ping 8 bytes an integer indicating the status is good.

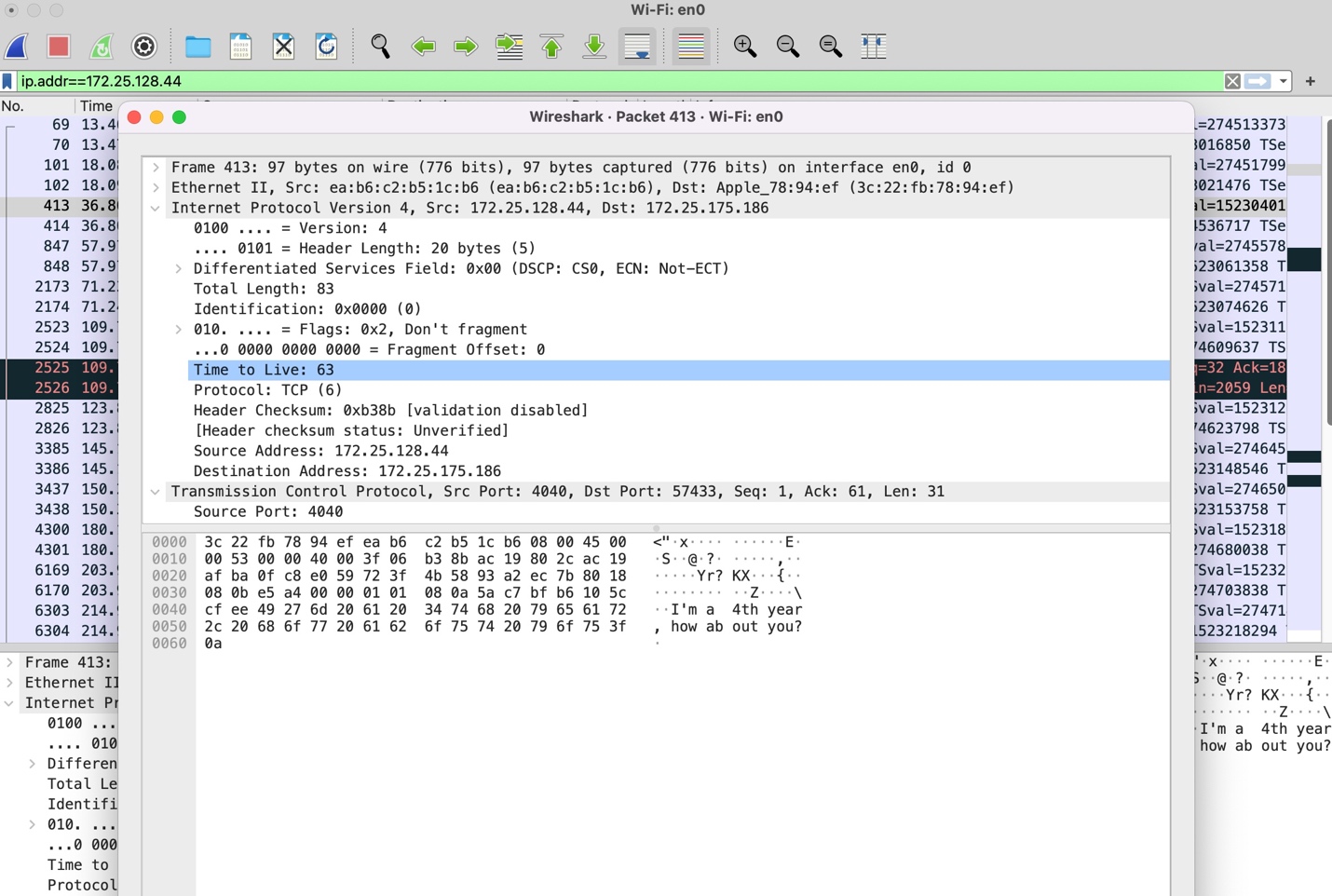
B: Insecure Chat

**[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.**

Myself as sender

****

Myself as listener



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

No. Because I did not run the command for my ncat to listen to other students. If I had then I would be about to see their ncat traffic, I think.

**[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?**

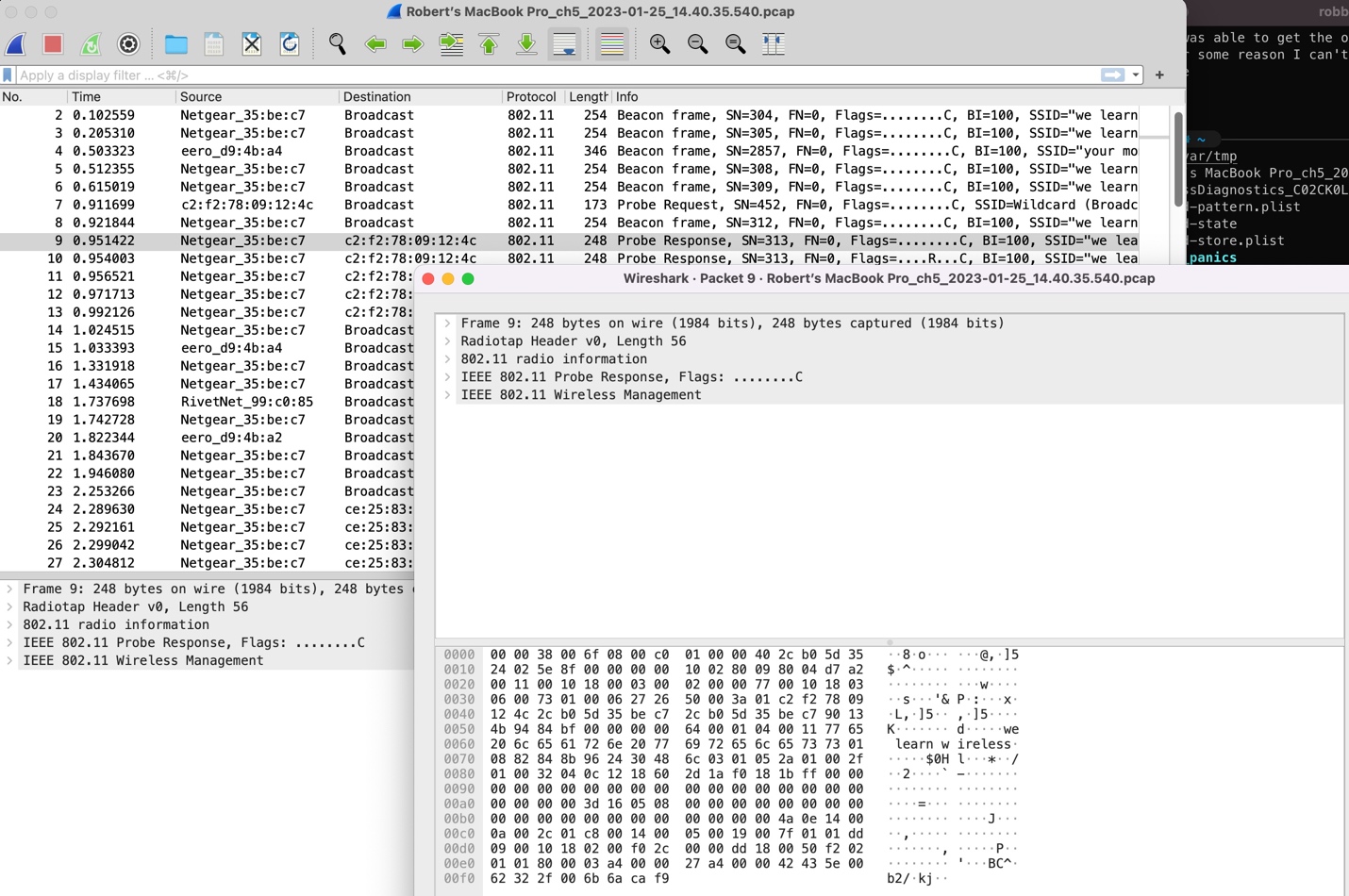
Anyone who could packet sniff the packets in transit. So, at UVA people connected to the eduroam wifi. The IPS provider routes the packet from Charlottesville to George Mason. And then anyone who is packet sniffing at the George Mason wifi networks.

# 

# C: Discover WiFi Networks Around You

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

we learn wireless. Netgear\_35:be:c7

****

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

Broadcast – Beacon frame

Broadcast – Probe Request & Response

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

wlan.bssid == 2c:b0:5d:35:be:c7

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

2c:b0:5d:35:be:c7

# 

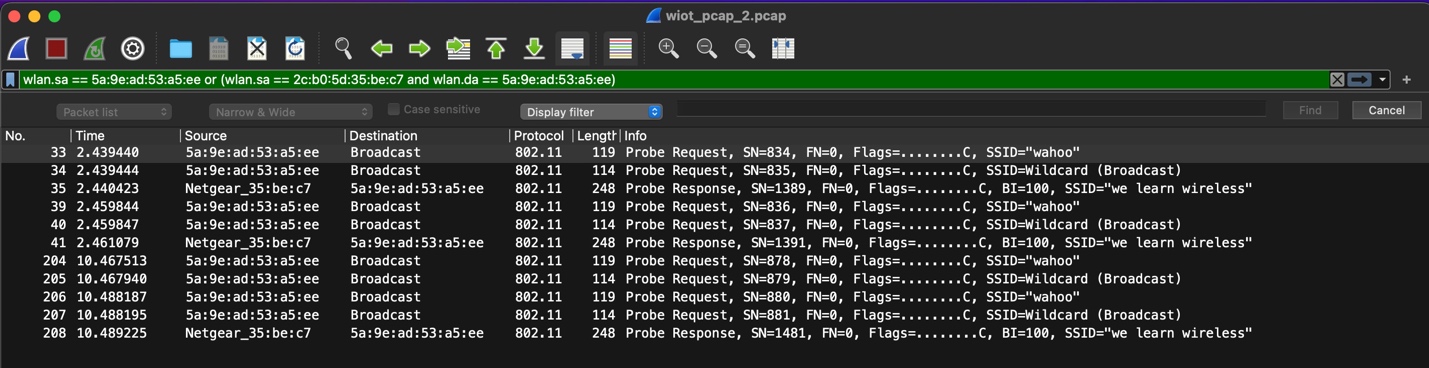
# D: Snooping Connection Formation

**[4pts] Filter the traffic to isolate the connection process.**

**How did you identify the correct set of packets?**

I first filtered packets that came from “we learn wireless” mac address and were being sent to the device trying to connect. Or packets being sent by the device trying to connect

**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?**

Packet number 34. It is a wildcard Probe Request Packet. the device is asking for wifi connection

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

Packet number 35 is the wireless router informing the device that it is available to connect. The identifying information is that it is the next sequential packet and it is the router sending a packet to that specific device and not a broadcast.

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

Packet 41 is a second probe response from the router to the device and then when un-applying the filter the router sends an acknowledgment for packet 42 as a broadcast which I believe is the router informing the network of the new devices' local IP address

# 

# E: Inspecting Protocol Information

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

Tag number 0.

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

Yes

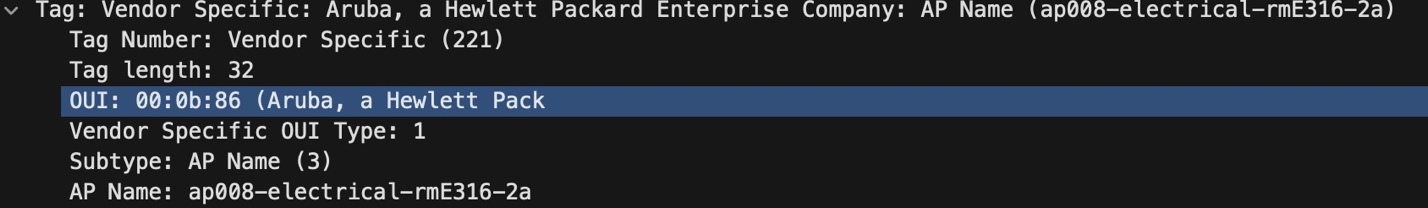
**[2pts] What is the Tag Number for the vendor specific tag?**

221

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

Ap008-electrical-rmE316-2a

**Include a screenshot from wireshark showing the AP name here:**

****