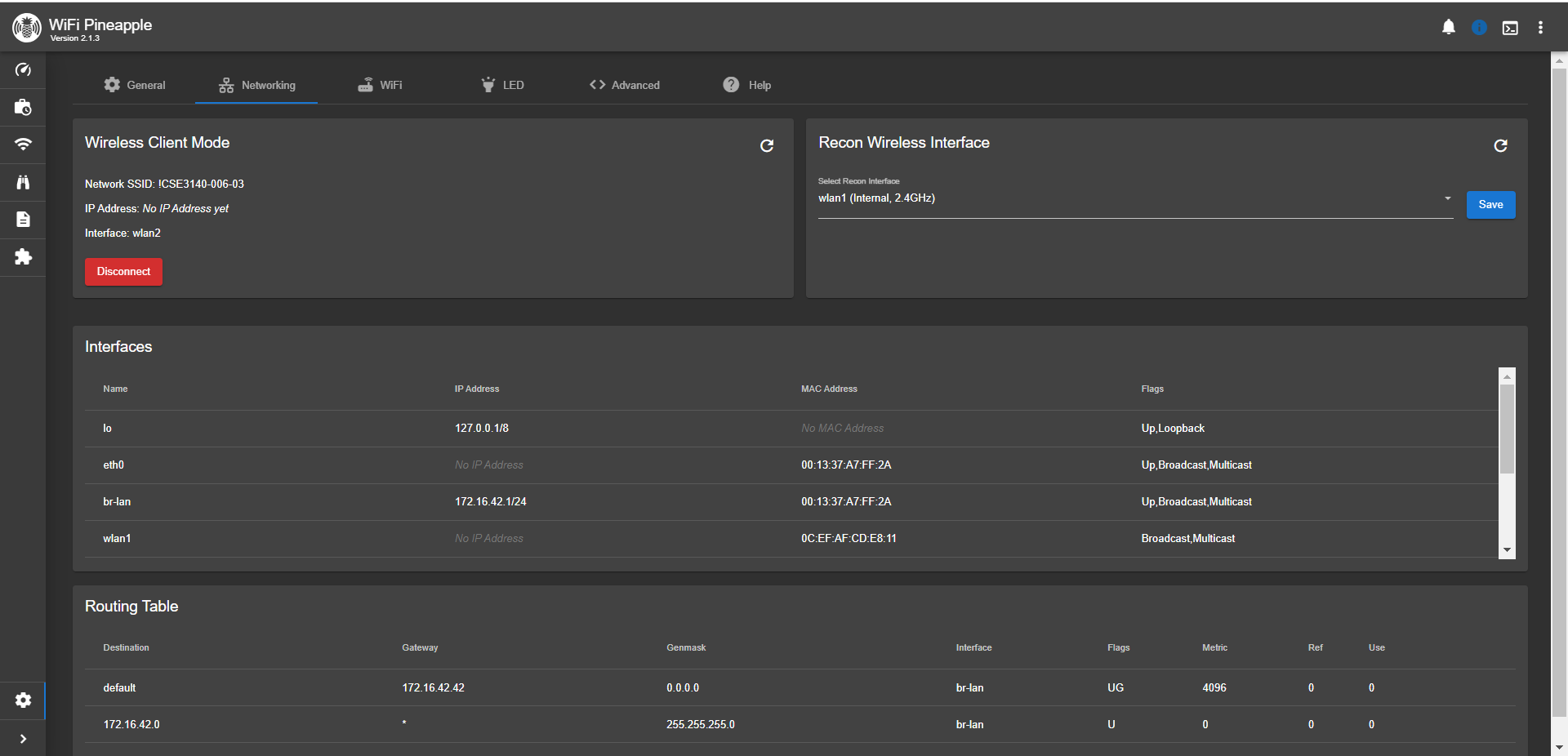
Name: Truc Ho Nguyen

NetID: thv20002

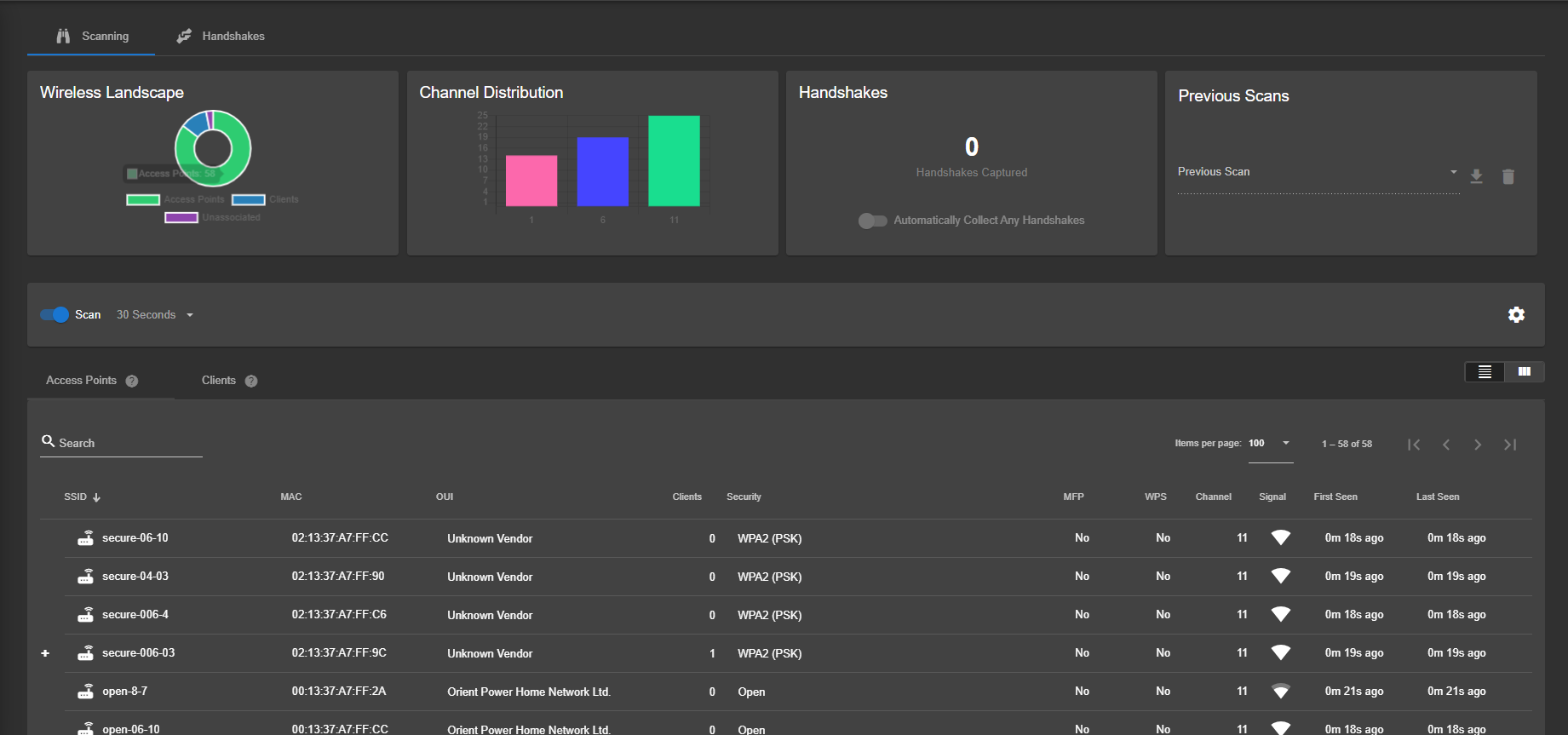
Section: 8

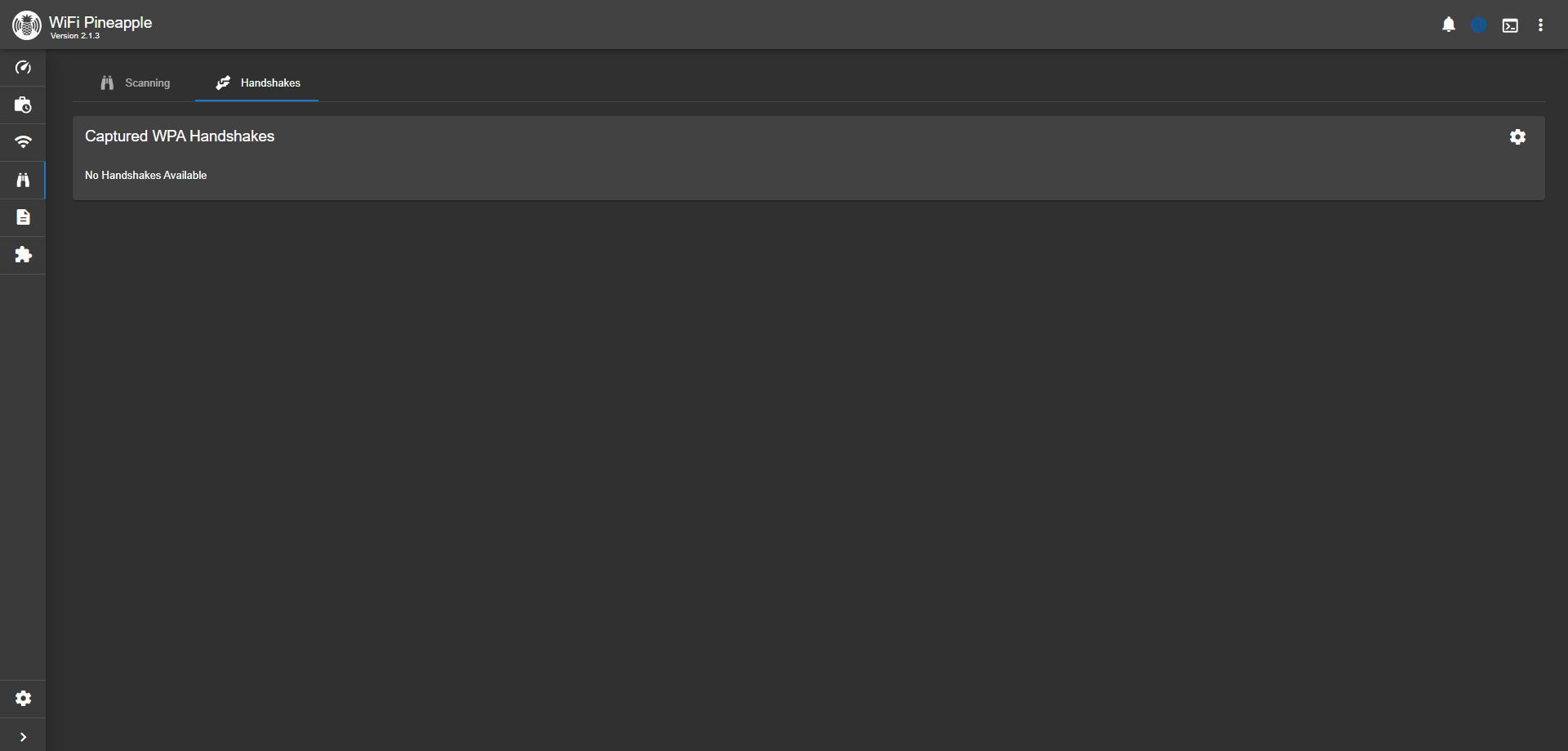
VM IP Address: 172.16.49.54

1. Attached below is a screenshot of the Wi-Fi administration console and dashboard. The Recon Wireless Interface box is used to scan and gather information on nearby networks. The Interfaces box shows the components that are able to connect the device to the network. The Routing Table box guides data packets as they travel throughout the network.

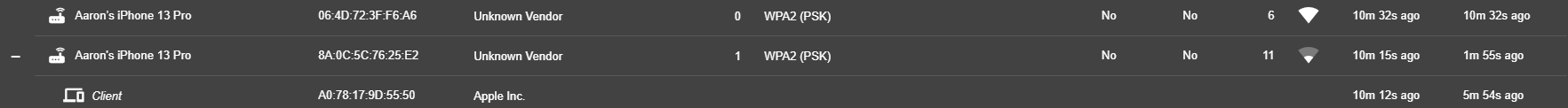


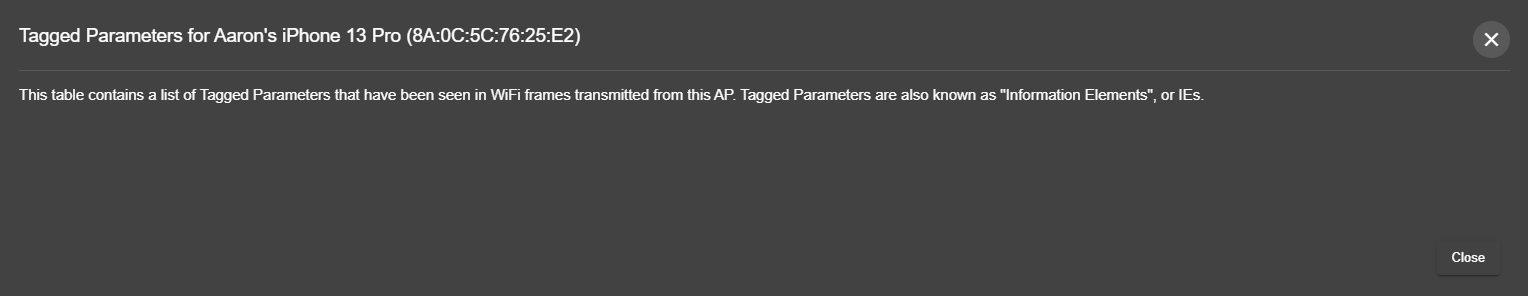
2. Attached below are screenshots of the Scanning and Handshakes tabs. The SSID represents the names of the access points. The MAC addresses are used to uniquely identify devices within a local network. The OUI is used to identify the manufacturer of the device. The clients represent how many devices are connected to a certain access point. The security refers to the certain protocols used to encrypt the network. The MFP enhances security by protecting management frames. The WPS simplifies the proces of connecting devices to a secure network. The channel refers to the frequency range that is used to transmit data.

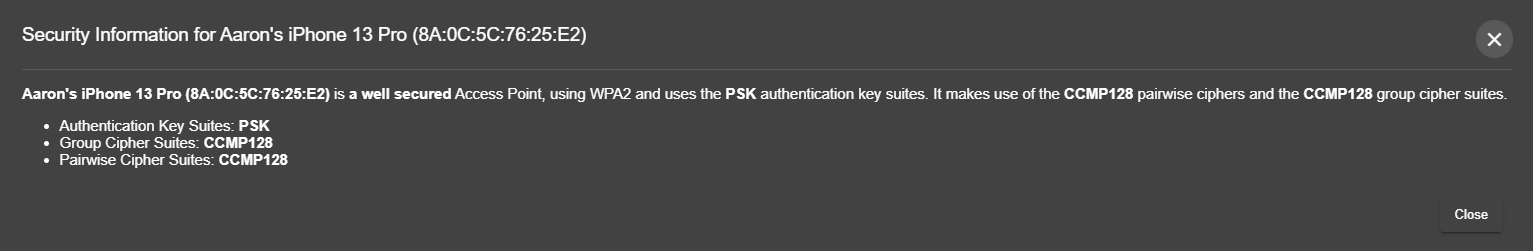




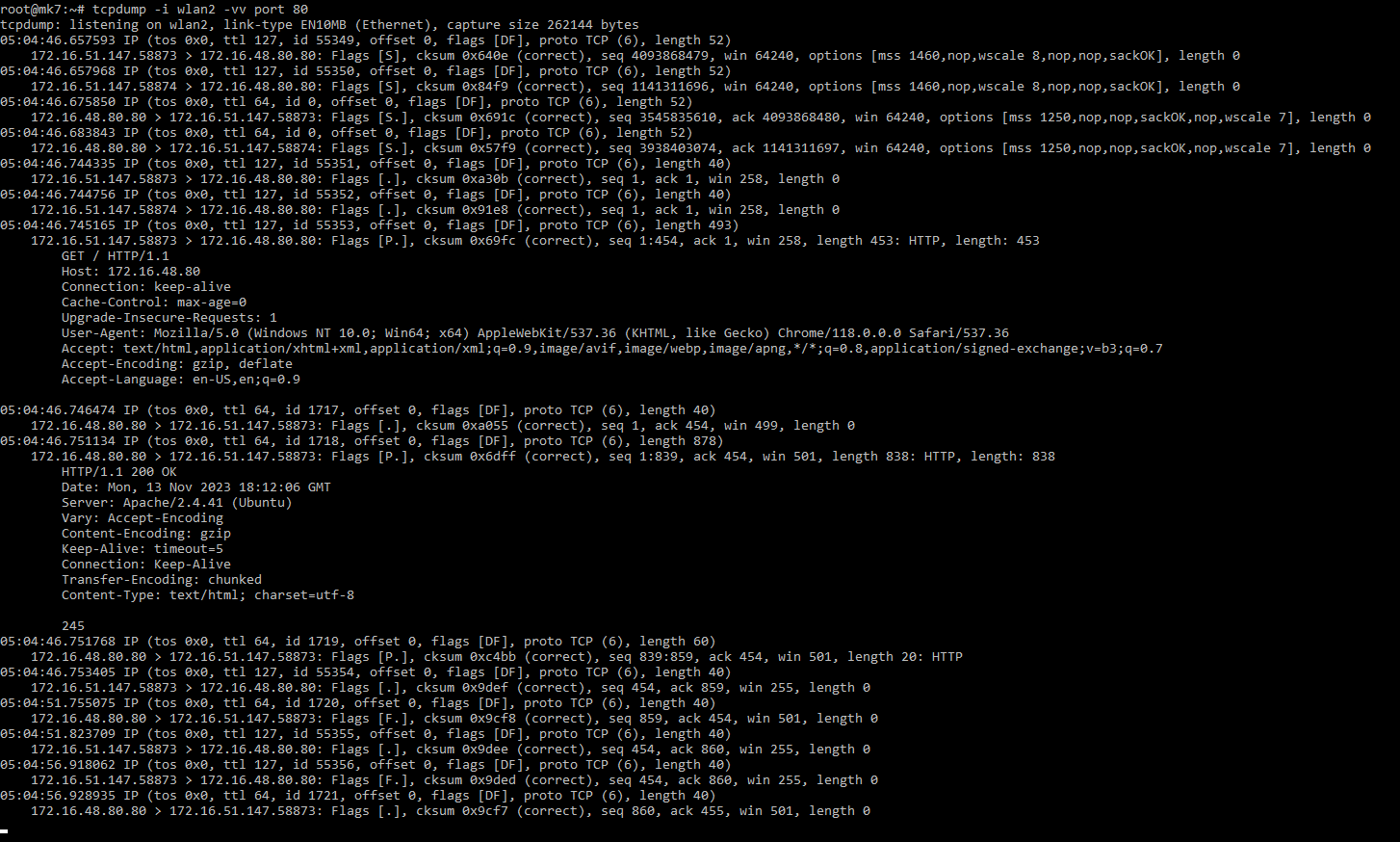
3. Attached below are screenshots of the Scanning tab after connecting a laptop to the personal hotspot (the TA allowed me to use his phone’s hotspot). From the Scanning tab, I could click on an access point to see clients using the network, such as my laptop. I could also view the access point’s tagged parameters and security information.



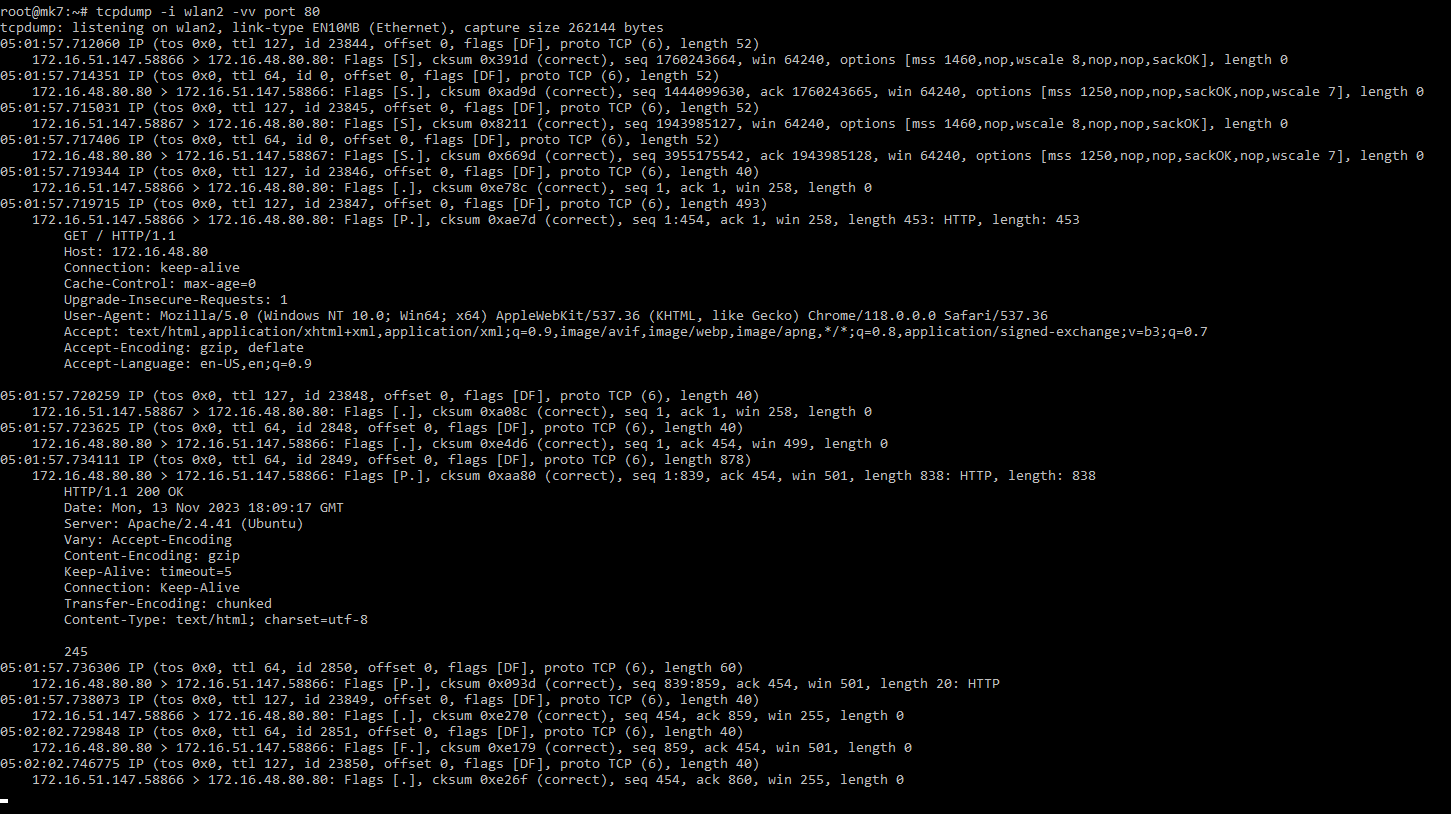




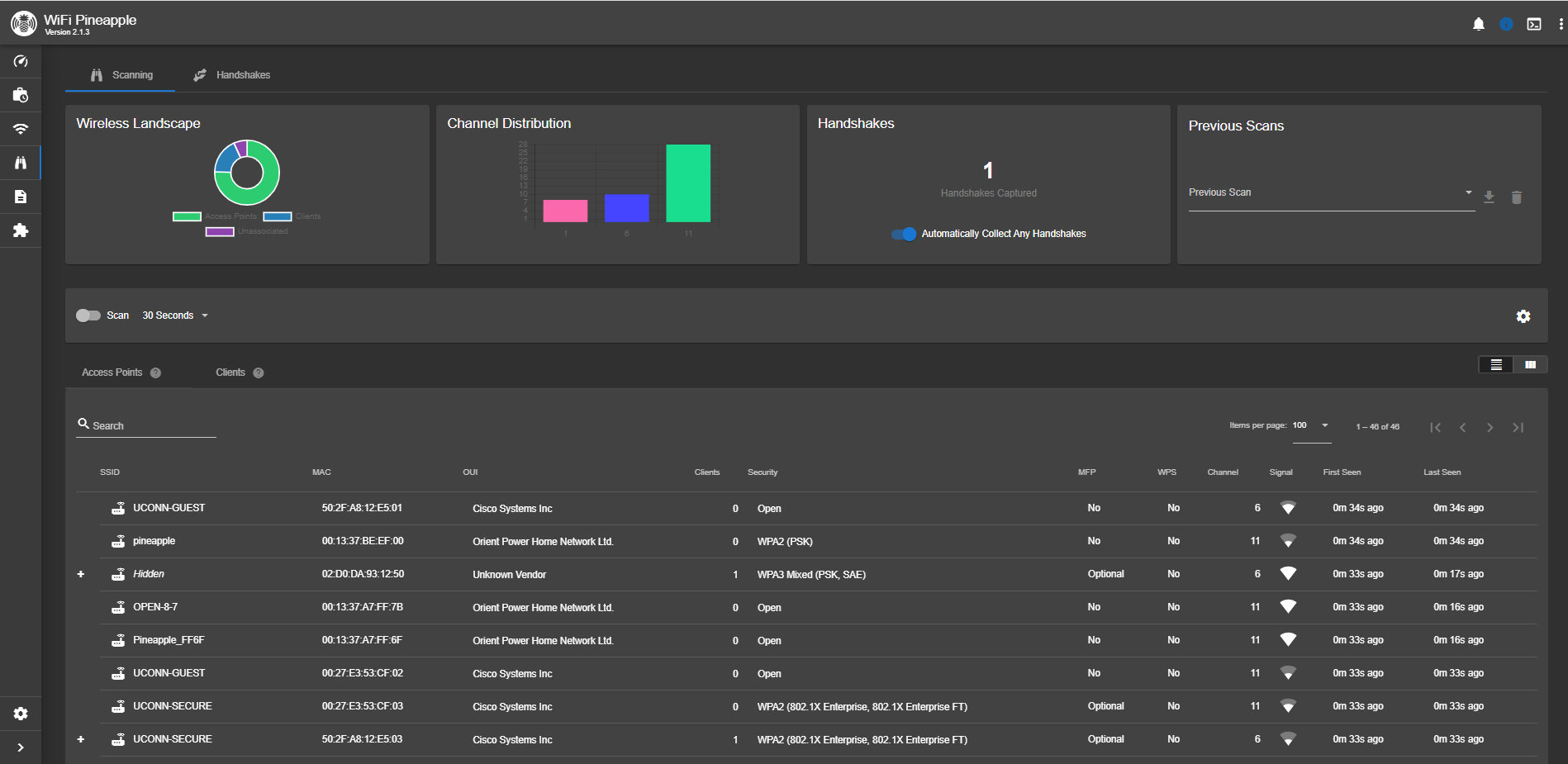
4. Attached below are results of the tcpdump while my laptop was connected to the unprotected network. I was able to view the traffic over the network. Two IP addresses sending HTTP traffic were 172.16.51.147.58873 (corresponds to my laptop) and 172.16.48.80.80 (corresponds to the banking website).



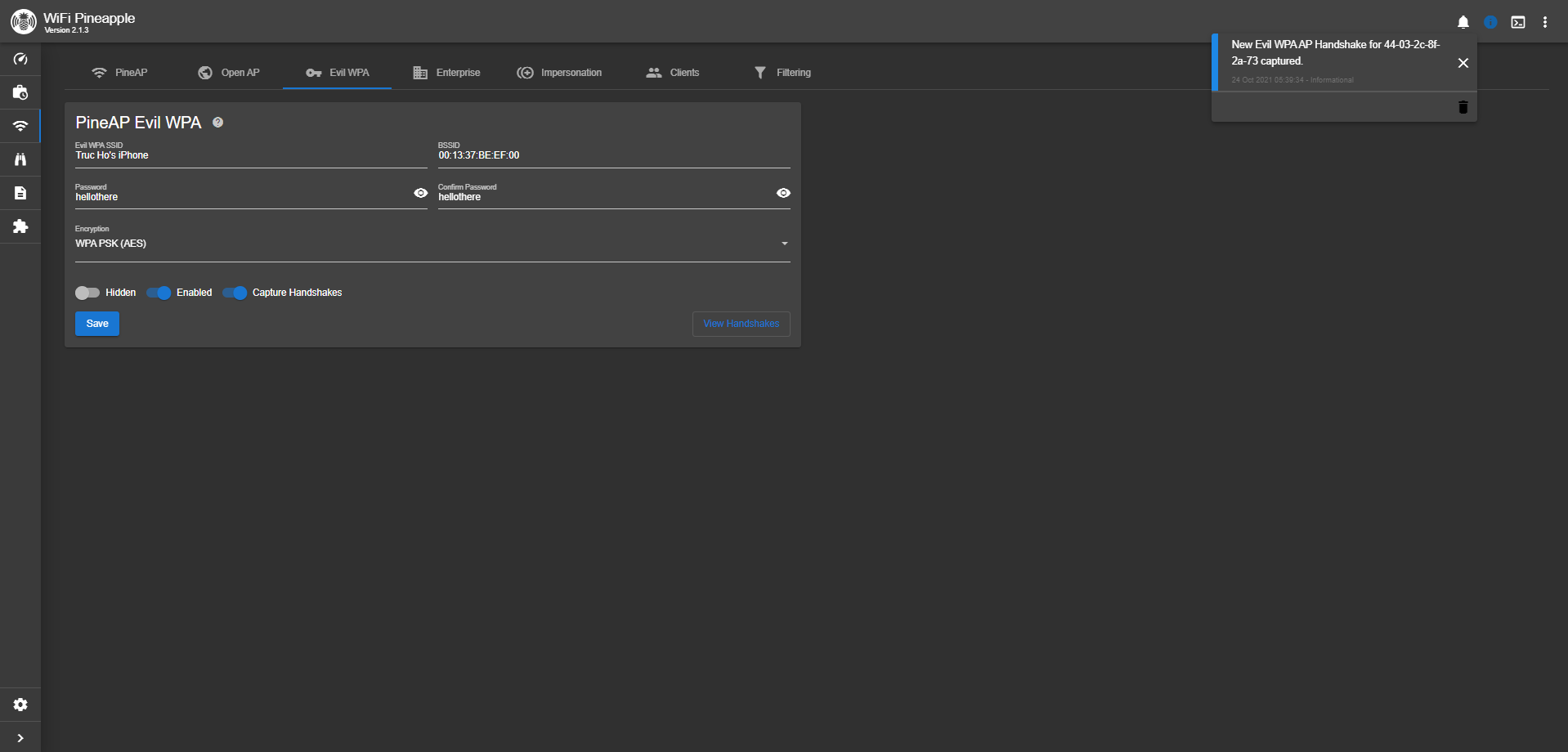
5. Attached below are results of the tcpdump while my laptop was connected to the secure network. I was still able to see traffic over the network. Thus, being on a protected network does not fully protect you from people attempting to view your information.

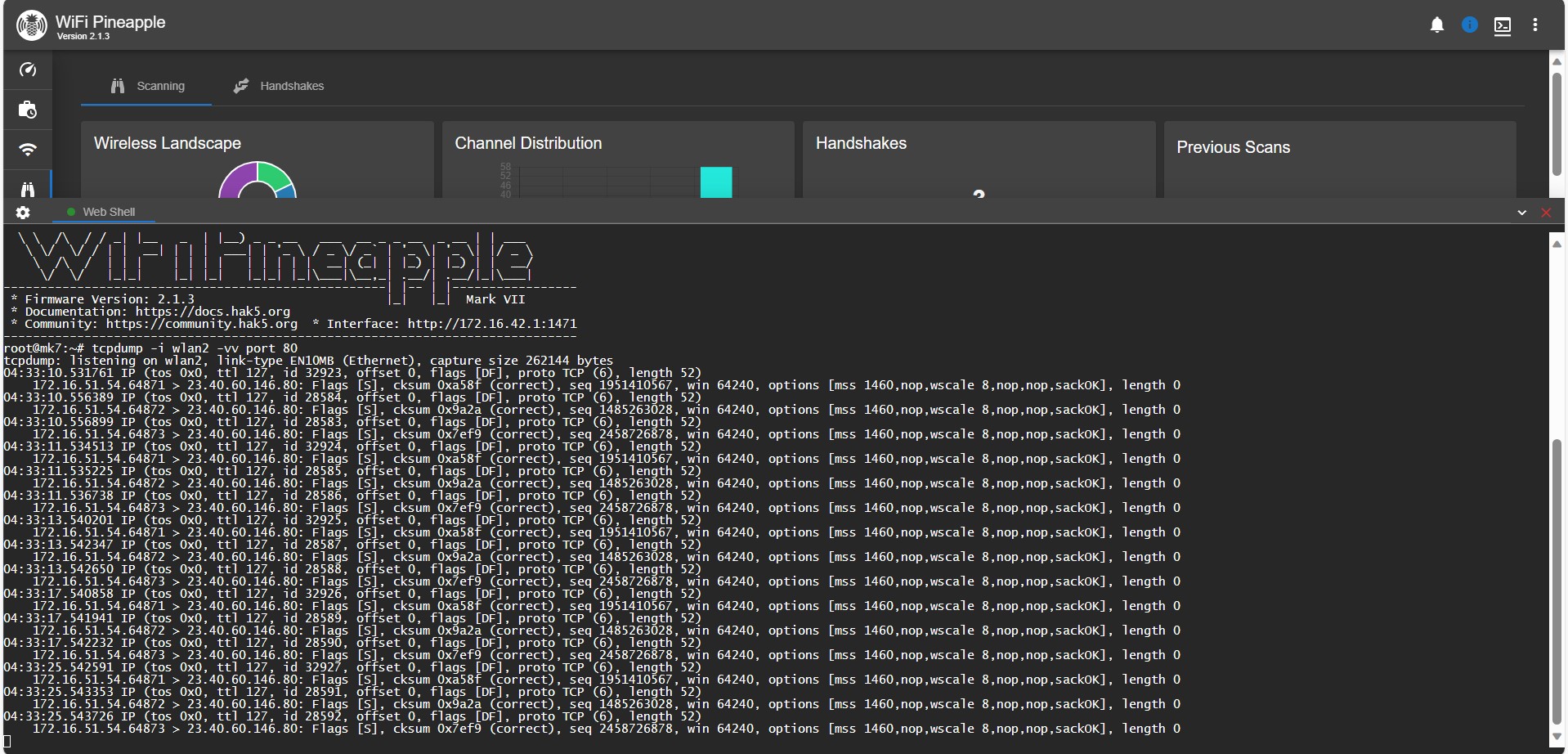


6. Attached below are results of a 30 second scan in the Recon tab. All of the wireless networks in the lab were visible including the official UConn Wi-Fi, other students’ open/secure networks, and other students’ personal hotspots. In this picture, UCONN-SECURE is an access point with more than one network, since it has multiple rows on the page. The security column shows what protocols were used to encrypt the network (Open refers to no security).



7. Attached below is the information I used to impersonate my phone’s personal hotspot, and the handshake that was captured after my laptop reconnected to it. I was able to find my phone’s encryption information through the Recon scanning. Also attached is the results of the tcpdump on the network, showing that the Pineapple can view the laptop’s traffic after impersonating a network. I was not able to do a screen recording since this required multiple devices.





8. Attached below is the tab I used to deauthenticate the clients on my phone’s hotspot. Once the laptop disconnected, I reenabled the Evil WPA and the laptop reconnected to the impersonating network. Also attached below are some handshakes captured from the attack. I was not able to do a screen recording since this required multiple devices.

