# Lab03- Beacon Scavenger Hunt

In this lab, we will scan the 2.4 & 5ghz wifi space and capture beacon frames, analyze them, and find specific pieces of information. To complete this lab, you will need to use the Wireless environment in the IA Lab. Do NOT log into the Projects or Learn environments (https://ialab.dsu.edu, click Wireless). A standard Kali virtual machine is deployed for you (kali/kali user/pass), however it also has a physical 802.11 adapter connected. Using this adapter in your virtual machine, scan the area to detect networks. Use a combination of Wireshark and airodump-ng to complete the following things below. Make sure to include a screenshot for each one of the items. If your screenshot is big, make sure to circle or point out where the answer is in your screenshot.

## What to do

1. Locate a beacon that's hiding its SSID. What is the SSID length?
2. Locate two beacons that are operating on a channel other than 1, 6 or 11
3. The timestamps for the official DSU networks are all very consistent, find a non-DSU beacon containing a timestamp that is significantly different
4. Many AP's do not beacon any regulatory domain information, but one does. Can you find it?
5. Create two screenshots, one with the best, one with the worst signal strength you can find
6. Find a network that does not have the Privacy flag set
7. Display a list of all of the unique ESSID's you can detect in a given area
8. Display a list of all of the unique BSSID's you can detect in a given area
9. Many beacons contain "vendor specific" information, you can see this in Wireshark if you look at a beacon frame. What is this for?
10. Researchy question! 802.11ax, marketed to the muggles as WiFi 6, is pretty neat. It's introduced a lot of new features, they're really only useful in dense environments. Advice: don't bother upgrading to AX in order to improve your home's wifi performance. To that end, one of the neat features that are introduced is the notion of "spatial reuse". We achieve this through coloring (basic service set coloring or more broadly as a network color code). No crayons needed. What is this?

## Hints and Tips

- If airodump-ng gives you no results (as if there aren't networks), fear not: this is a regular thing that happens with airodump. Just reboot your VM (sudo reboot)
- If you find that you do not have a wireless card (iwconfig gives you no wireless adapter), gripe about it here: https://forms.gle/1waNYx55Cro9kPR96 That'll send a notice to a couple of us (Eric & myself) and we'll check it out!
- The "official" networks provided by DSU's ITS department are: GoTrojans, DSUGaming, eduroam, and Guest, other DSU networks include CubeFarm, DSUnix, CHP, IA_IOT. Other networks are available, but they may not be provided by the ITS department specifically (or, they're neighbors to campus).
- If for some reason you need network connectivity, your VM should have a 'wired' connection. You may connect via the wireless adapter, but the wired interface is your better bet. Hit captive.ialab.dsu.edu to trigger the captive portal.
- Many labs that we do are in a 'controlled environment'. This lab isn't—IE: you may be picking up wireless networks from some person that lives across the street from the building that your VMs are in. Be nice, if one of their networks happen to match a request for this lab, take a screenshot and go with it (that's not my intent, but it happens). Wireless beacons, with all their joy, aren't really considered "private" information (at least in the United States).