**CTF Write-up**

1. **Task 1:**
   1. We started off with using the GNU radio FM receiver given as well as the receiver from lab4 to record the different frequency peaks that were mentioned in the manual, i.e between 922 - 925 MHz.
   2. The observed peaks were at:
      1. 922.992
      2. 923.947
      3. 924.121
      4. 923.55
   3. Of these recorded peaks we received the first clue on **923.947MHz** which gave us our next clue: To check for vendor specific information in wifi packet frames and also something about the IP -  **192.168.2.1**
2. **Task 2:**

1. We then use the setup script provided to use monitor mode on the Wi-Fi USB adaptor.
2. On capturing the necessary traffic and viewing packet info that said “nothing to view here” we observed data strings like “GROUPX=”
3. This is where we found our first flag:

**GROUP3=e45ee7ce7e88149af8dd32b27f9512ce**

1. Further to find the password to connect to the network: wireless\_ctf we filtered the packet captured to show the string starting with pwd= and came across the password **spring2023**.

**3. Task 3:**

1. After retrieving the password and knowing which network to connect to, we used spring2023 to connect to wireless\_ctf.
2. We then used nmap -sV 192.168.2.1 to view what ports are open
3. It was seen that HTTP was running on port 80 and the next step was to use the browser to spin up <http://192.168.2.1:80>
4. We came across a secret\_tx\_util.zip folder and on downloading the zip file we discovered the secret\_flag\_tx.py file and the tx\_library.py.
5. The tx\_library had the frequency variable value set as **923.55**, which confirmed there is a hidden flag on it.
6. We specified this value in the secret\_flag\_tx.py file, gave the team id as 3, and modified the flag above