BL(u)E CRAB:

RSSI Detection Pattern Analysis for Flagging System Development

Zhi Qu

Bluetooth Low Energy (BLE)

- Low power devices

- Application
    - Smart Home
    - Fitness devices
    - Trackers

Bluetooth Low Energy (BLE)

- Low power devices
- Application
  - Smart Home
  - Fitness devices
  - Trackers

- AirTag
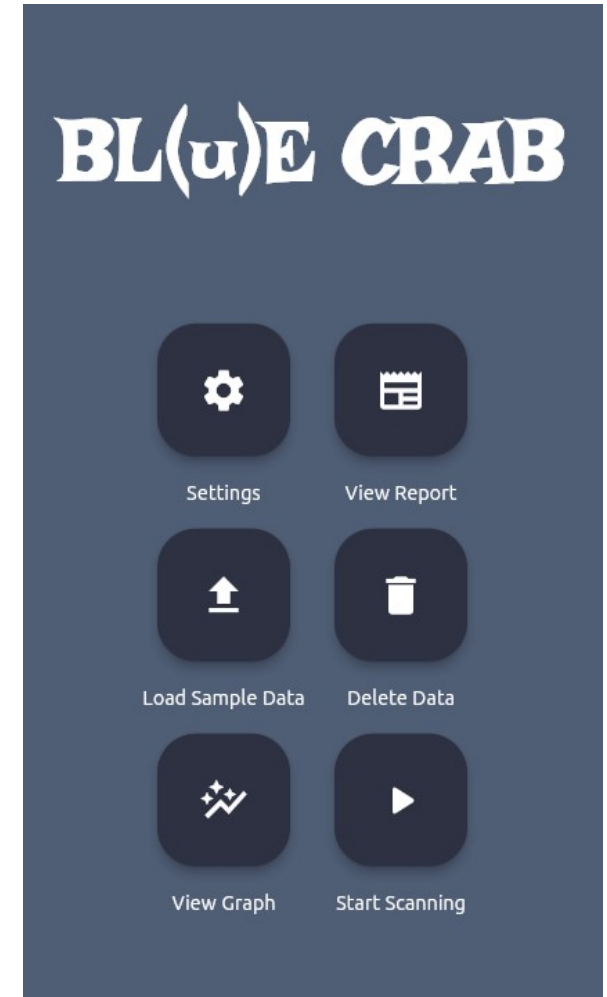- Tile
- Chipolo
- SmartTag

What is the Threat?

Stalking

- Making unwanted and persistent phone calls
- Approaching or showing up in places uninvited
- Following and watching the person
- Sending unwanted texts, emails, and social media messages
- Delivering unwanted gifts
- Utilizing technology for monitoring and tracking

Facing the Shadows: A Comprehensive Look at Stalking. (n.d.). https://safepass.org/2025/01/10/ facing-the-shadows-a-comprehensive-look-at-stalking

What is the Threat?

Stalking

- Making unwanted and persistent phone calls
- Approaching or showing up in places uninvited
- Following and watching the person
- Sending unwanted texts, emails, and social media messages
- Delivering unwanted gifts
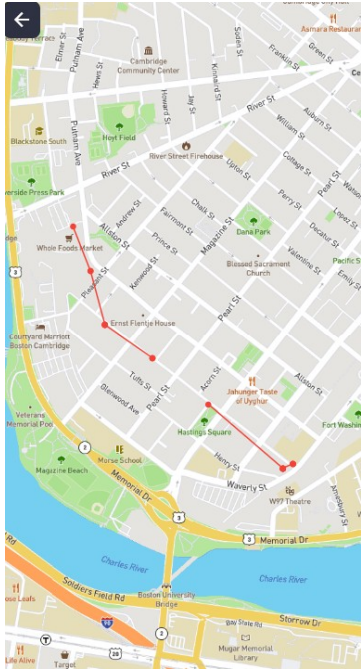- Utilizing technology for monitoring and tracking

Facing the Shadows: A Comprehensive Look at Stalking. (n.d.). https://safepass.org/2025/01/10/ facing-the-shadows-a-comprehensive-look-at-stalking

BL(u)E CRAB

- Flutter app

- Scans for BLE devices nearby

- Assess risk

- Flags device

- Logs device info

D. Conklin, P. Pappachan, and R. Yus, "Bl (u) e crab: A user-centric framework for identifying suspicious bluetooth trackers," in 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops). IEEE Computer Society, 2025, pp. 570–572.

Information Log

- location
- time
- RSSI

Information Log

- location
- time
- RSSI

Information Log
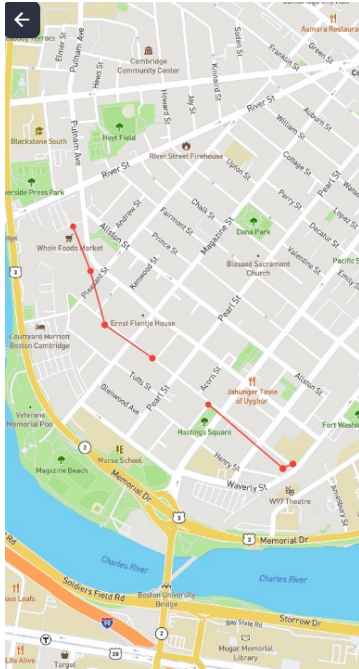
- location

- time

- RSSI

Device Details

UUID	00:00:00:00:00:06
Manufacturer	Ericsson AB
Duration Travelled	12 mins, 4 sec
Distance Travelled	748 meters
Incidence	9

Device Routes

RSSI Graph

What is this?

Information Log

- location
- time
- RSSI
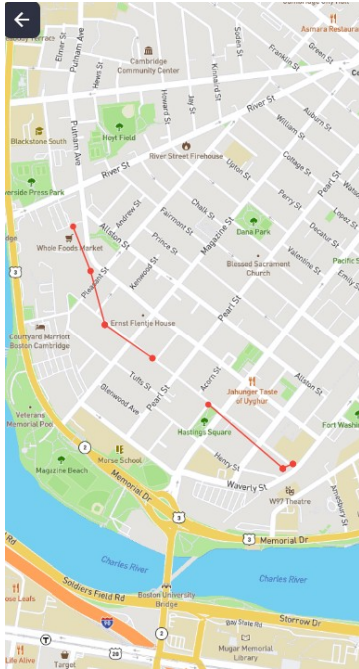
Device Details

UUID	00:00:00:00:00:06
Manufacturer	Ericsson AB
Duration Travelled	12 mins, 4 sec
Distance Travelled	748 meters
Incidence	9

Device Routes

RSSI Graph
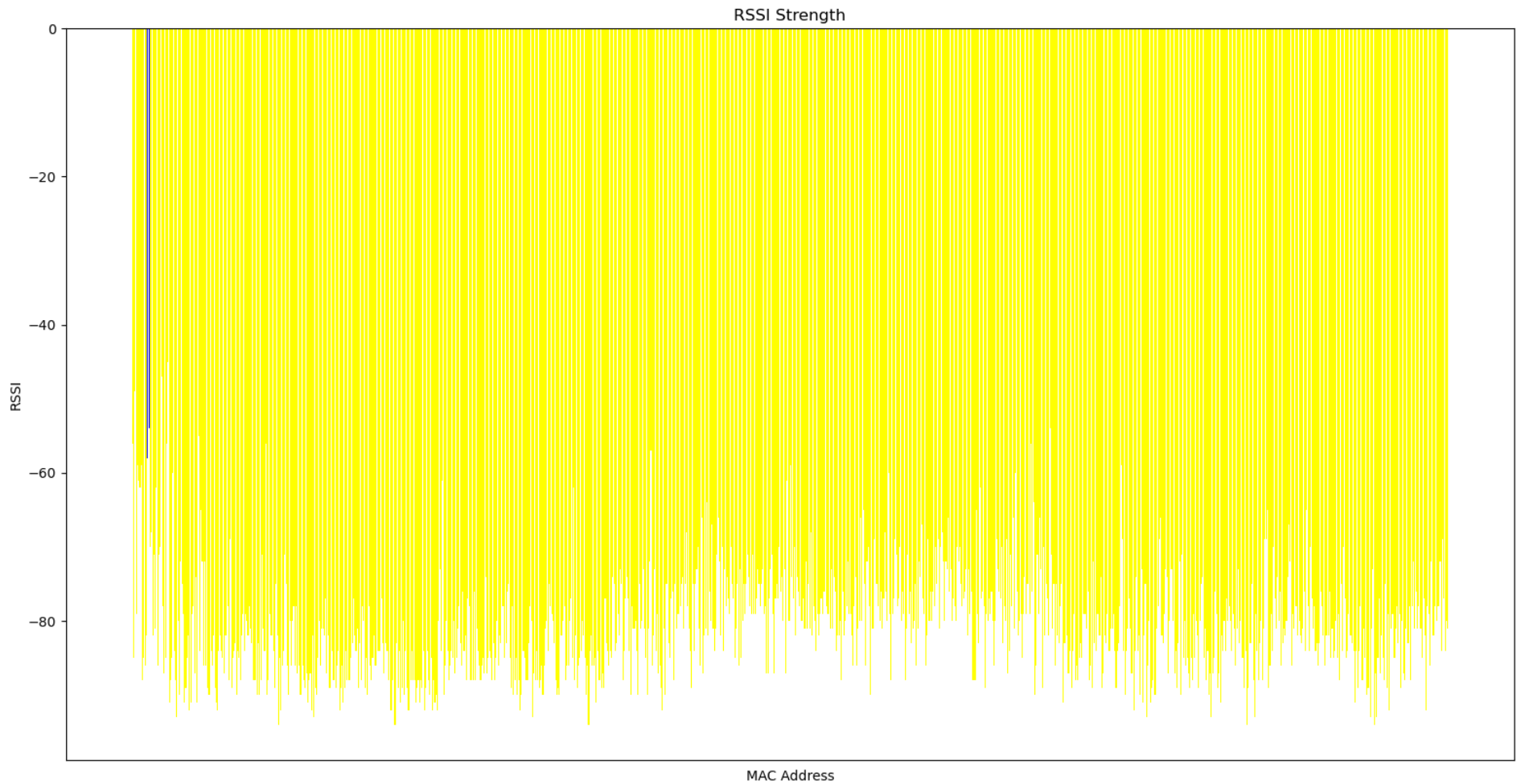
Received
Signal Strength
Indicator

Question

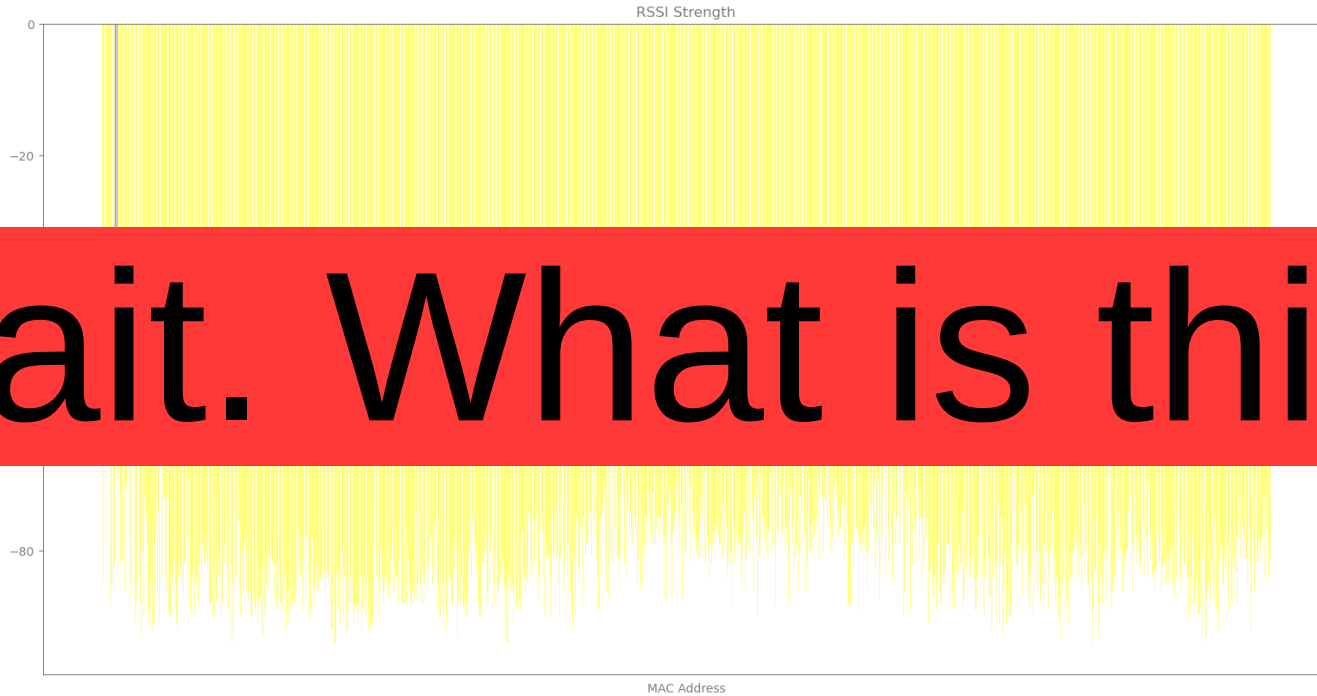How does the RSSI values differ for suspicious and non-suspicious devices?

Reading the data

- The data is from BLE-Doubt

- JSON

- Various travel and planted methods

- Ground truth

	Movement	Location
A	Walking	Backpack
B	Walking	Backpack
C	Walking	Pockets
D	Walking	Pockets
E	Car	Car
F	Jogging	Backpack
G	Walking	Backpack
H	Walking	Backpack
I	Train	Backpack
J	Train	Backpack
K	Walking	Pockets
L	Walking	Pockets
M	Train	
N	Car	Car

J. Briggs and C. Geeng, "Ble-doubt: Smartphone-based detection of malicious bluetooth trackers," in 2022 IEEE Security and Privacy Workshops (SPW). IEEE, 2022, pp. 208–214.

Graph

RSSI Strength

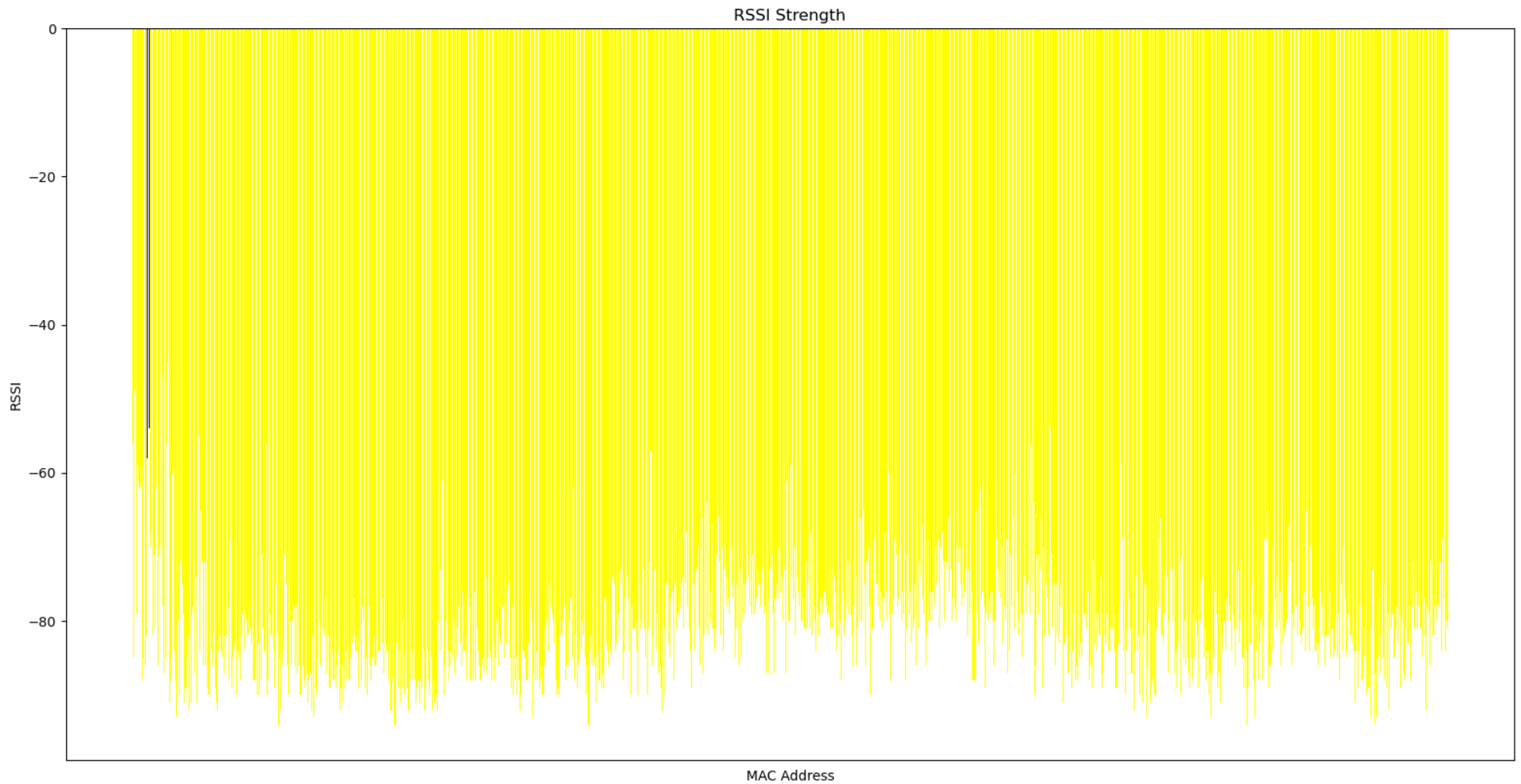# Graph

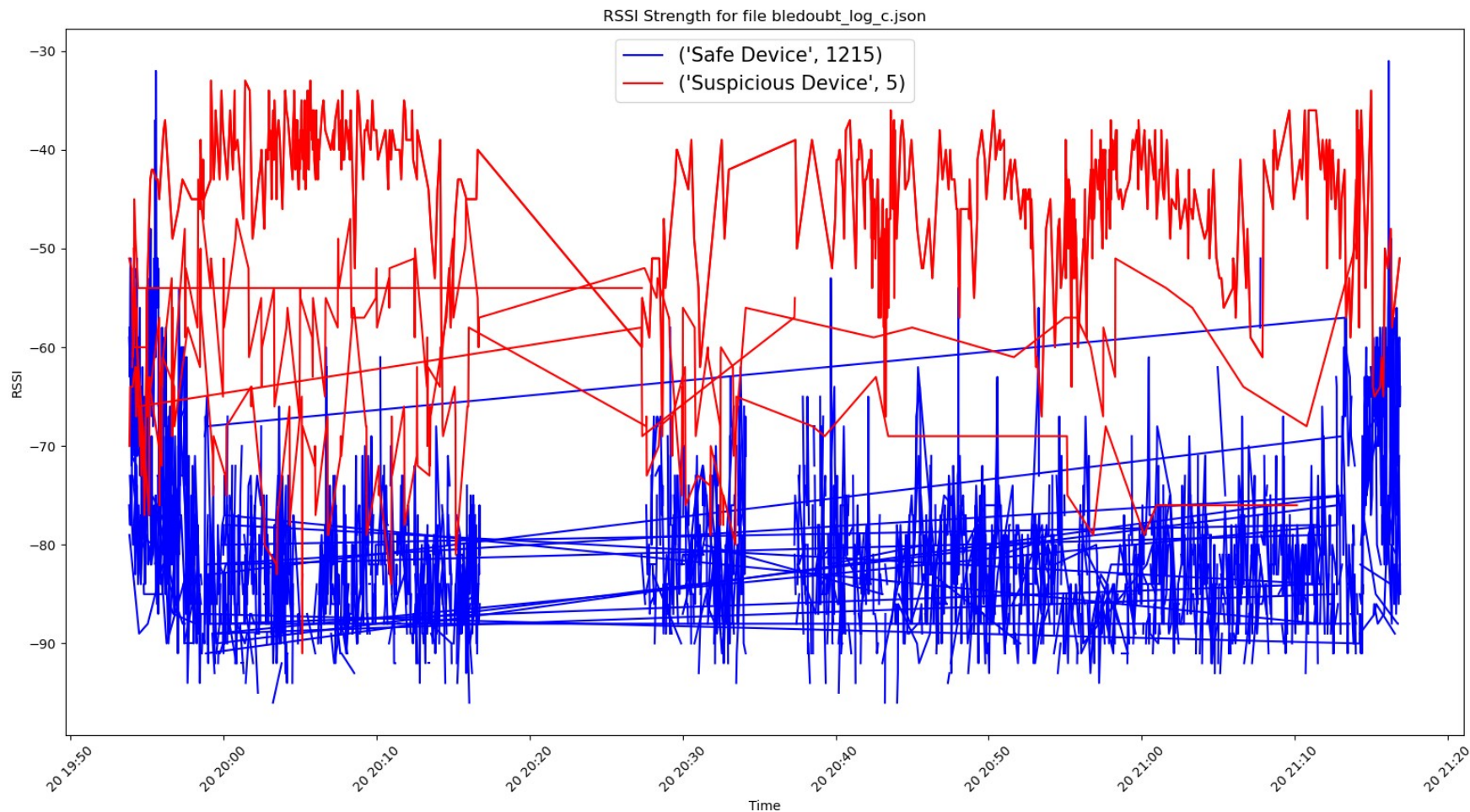RSSI Strength
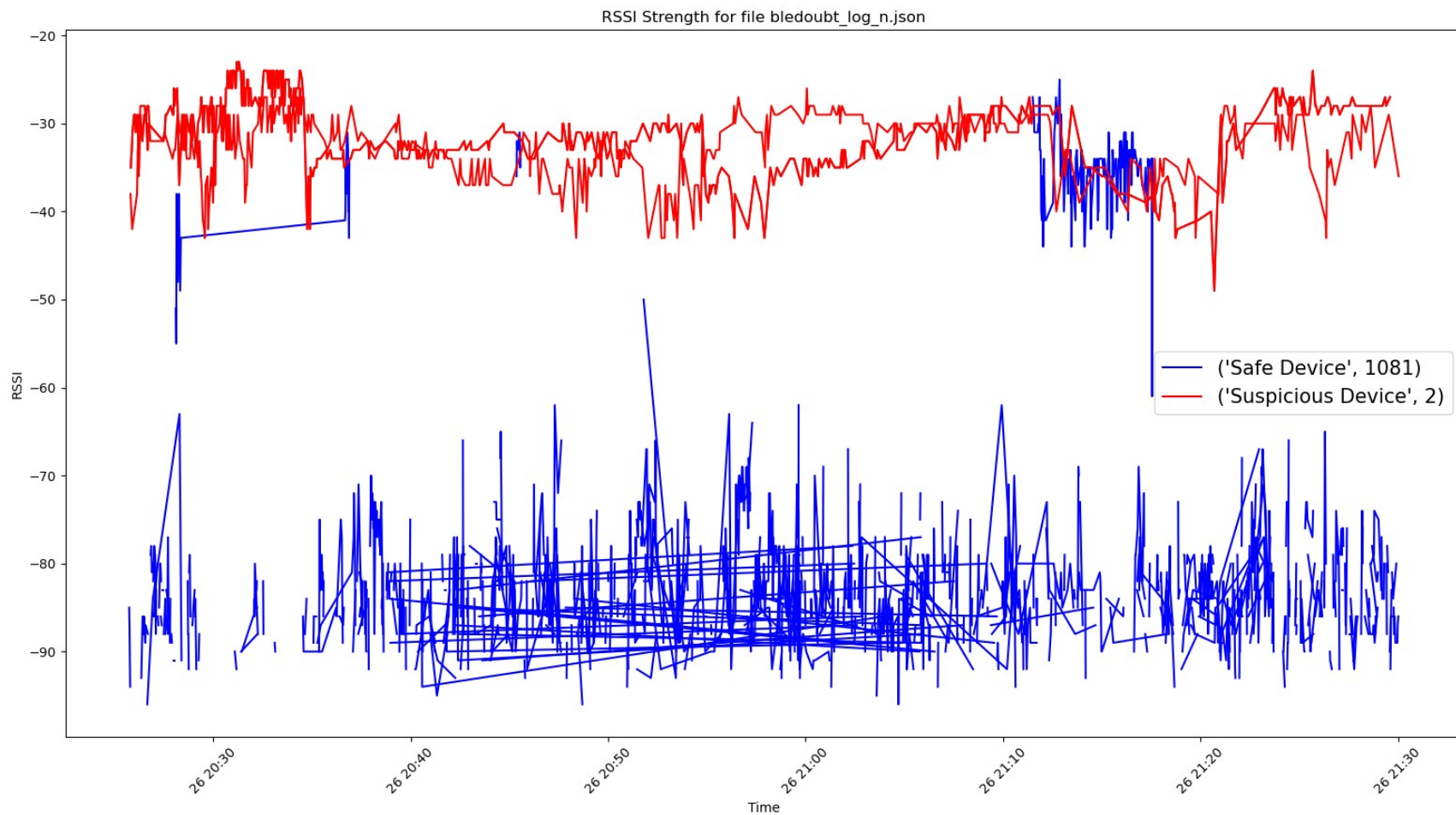
Wait. What is this?

MAC Address

Graph

Identifying each mac id

```python
     #note: change function to takes in variable
 def sort(mac, rssi, time):
     #list of unique mac addresses
     fmac = list(set(mac))
     #new lists to store RSSI and time as a list in list
     #for each unique mac address
     arssi = []
     atime = []
     for i in fmac:
         r = []
         t = []
     #loop through the original mac list to find each unique mac address
     #idx is the index of the original mac list
         for idx, e in enumerate(mac):
             if i == e:
                 r.append(rssi[idx])
                 t.append(time[idx])
         arssi.append(r)
         atime.append(t)
     return fmac, arssi, atime
```

Data file c – Walking, Pockets

RSSI Strength for file bledoubt_log_c.json

Legend: ('Safe Device', 1215), ('Suspicious Device', 5)

Data file n - Car

RSSI Strength for file bledoubt_log_n.json

Legend:
- ('Safe Device', 1081)
- ('Suspicious Device', 2)

Significant time Detected
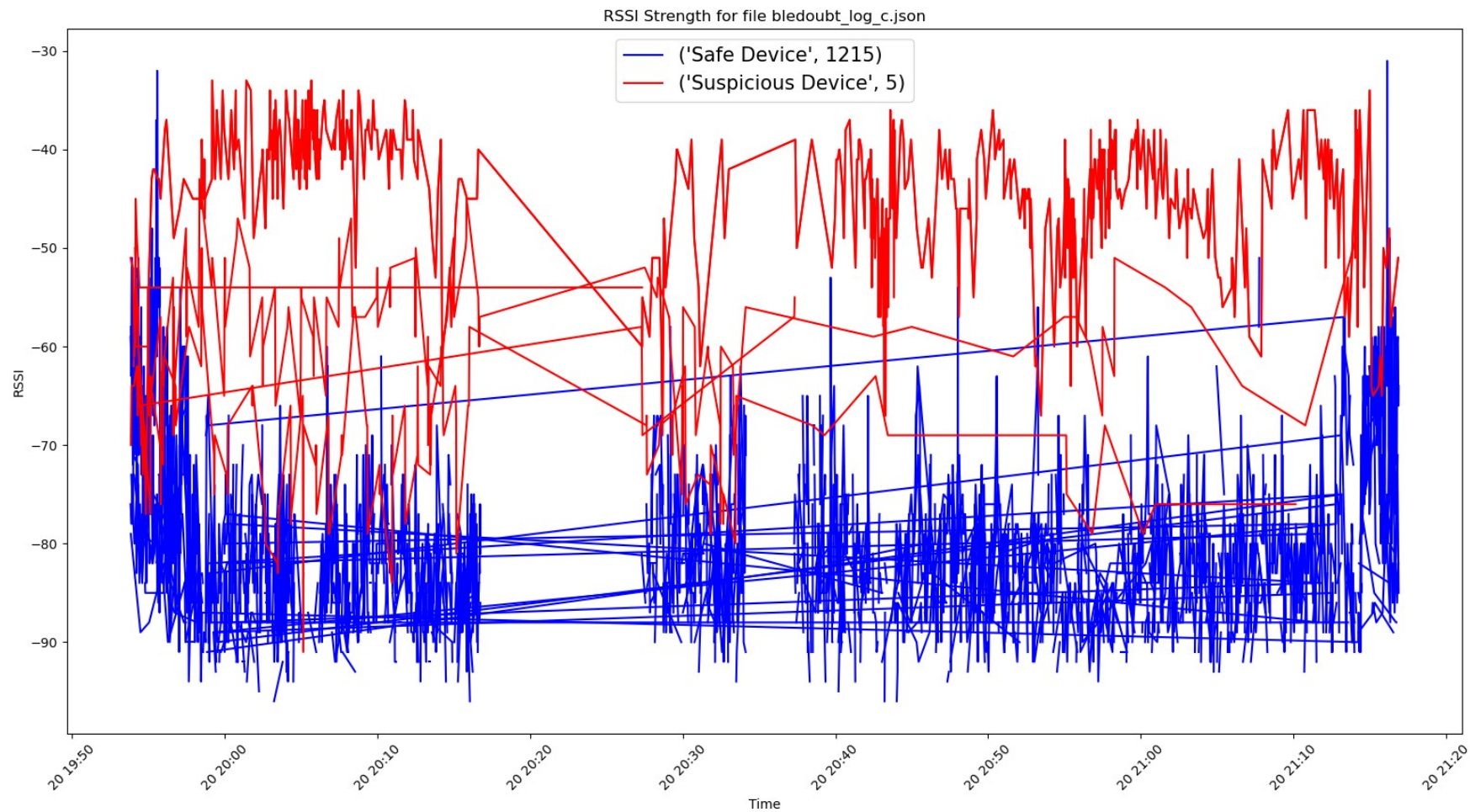
```
86      for a in macsafe:
87          idx = macsafe.index(a)
88          if len(timesafe[idx]) > 60:
89              labelsafe.append(a)
90              labelsafe_r.append(rssisafe[idx])
91              labelsafe_t.append(timesafe[idx])
92          else:
93              next
94      for a in macsus:
95          idx = macsus.index(a)
96          if len(timesus[idx]) > 60:
97              labelsus.append(a)
98              labelsus_r.append(rssisus[idx])
99              labelsus_t.append(timesus[idx])
100         else:
101             next
```
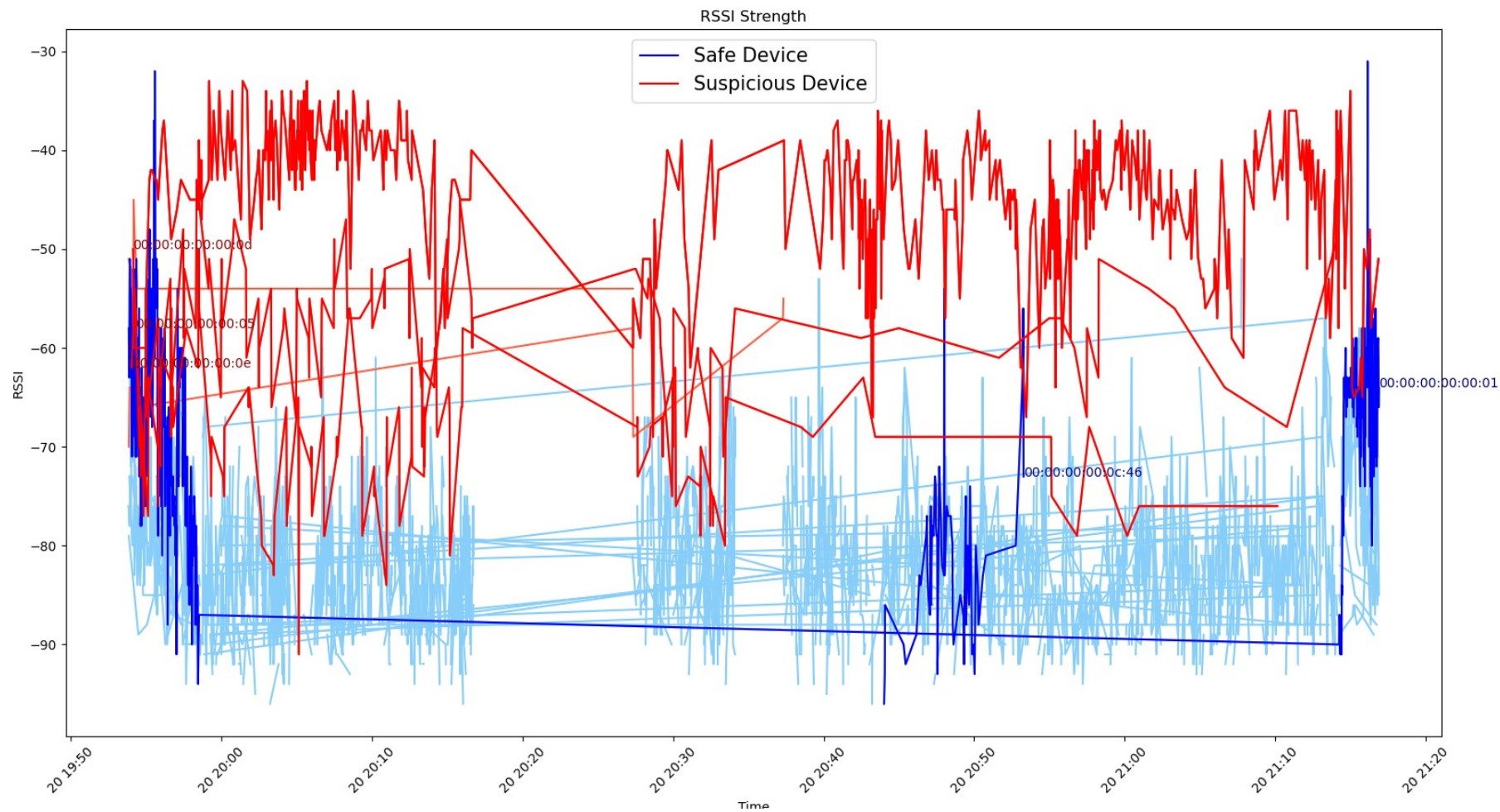
Setting threshold to 60 seconds

Plotting with different colors

```
130    #the colors were changed to be a lighter verson of the original colors
131        for i in range(len(macsafe)):
132            sorted_pairs = sorted(zip(timesafe[i], rssisafe[i]), key=lambda x: x[0])
133            timesafe_paired, rssisafe_paired = zip(*sorted_pairs)
134            plt.plot(timesafe_paired, rssisafe_paired, color="lightskyblue")
135
136    # specially plot significant devices with bold color
137        for i in range(len(labelsafe)):
138            sorted_pairs = sorted(zip(labelsafe_t[i], labelsafe_r[i]), key=lambda x: x[0])
139            timesafe_paired, rssisafe_paired = zip(*sorted_pairs)
140            plt.plot(timesafe_paired, rssisafe_paired, color = "blue")
141            plt.text(labelsafe_t[i][-1], labelsafe_r[i][-1], labelsafe[i], color="navy")
142
```
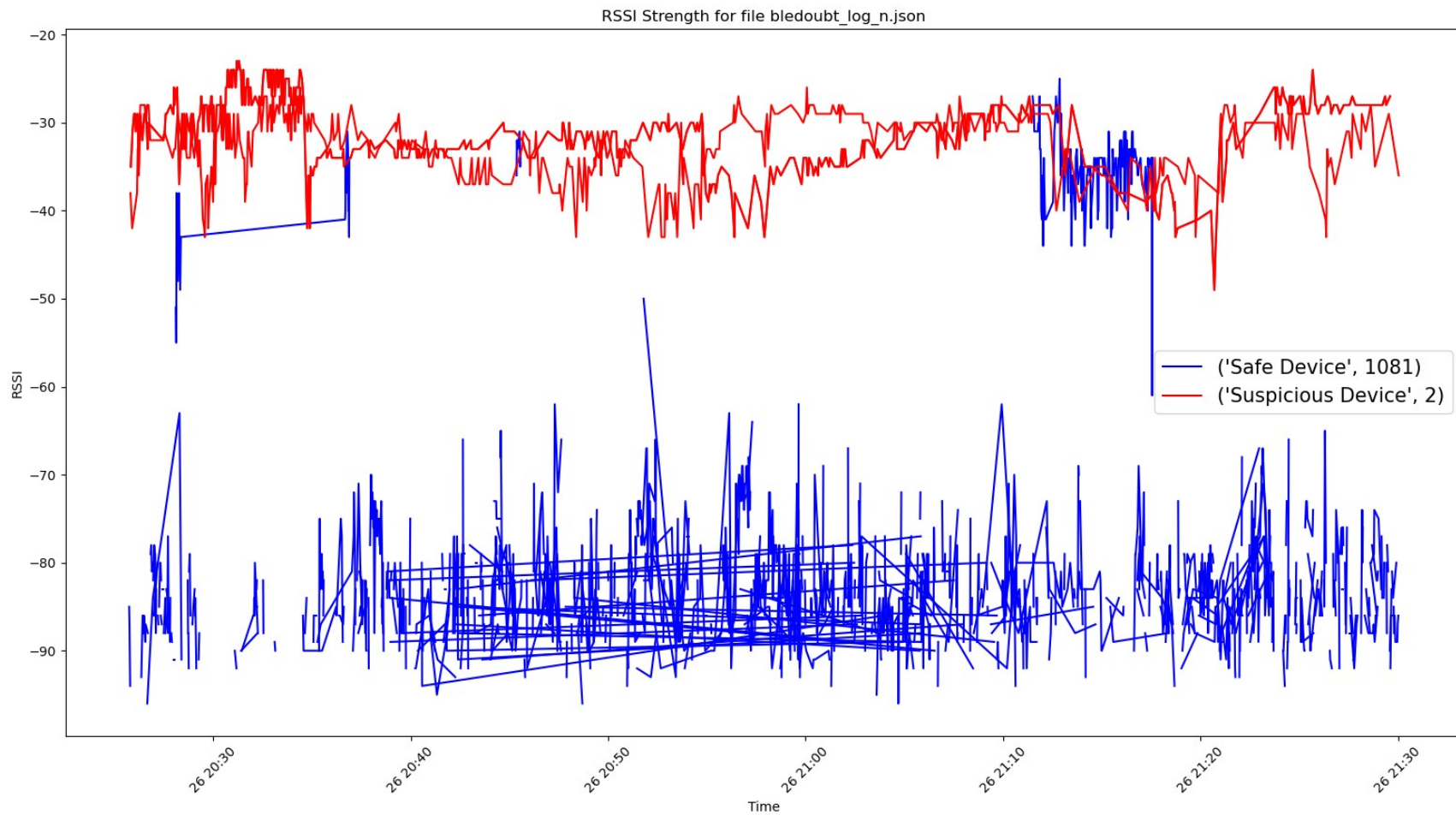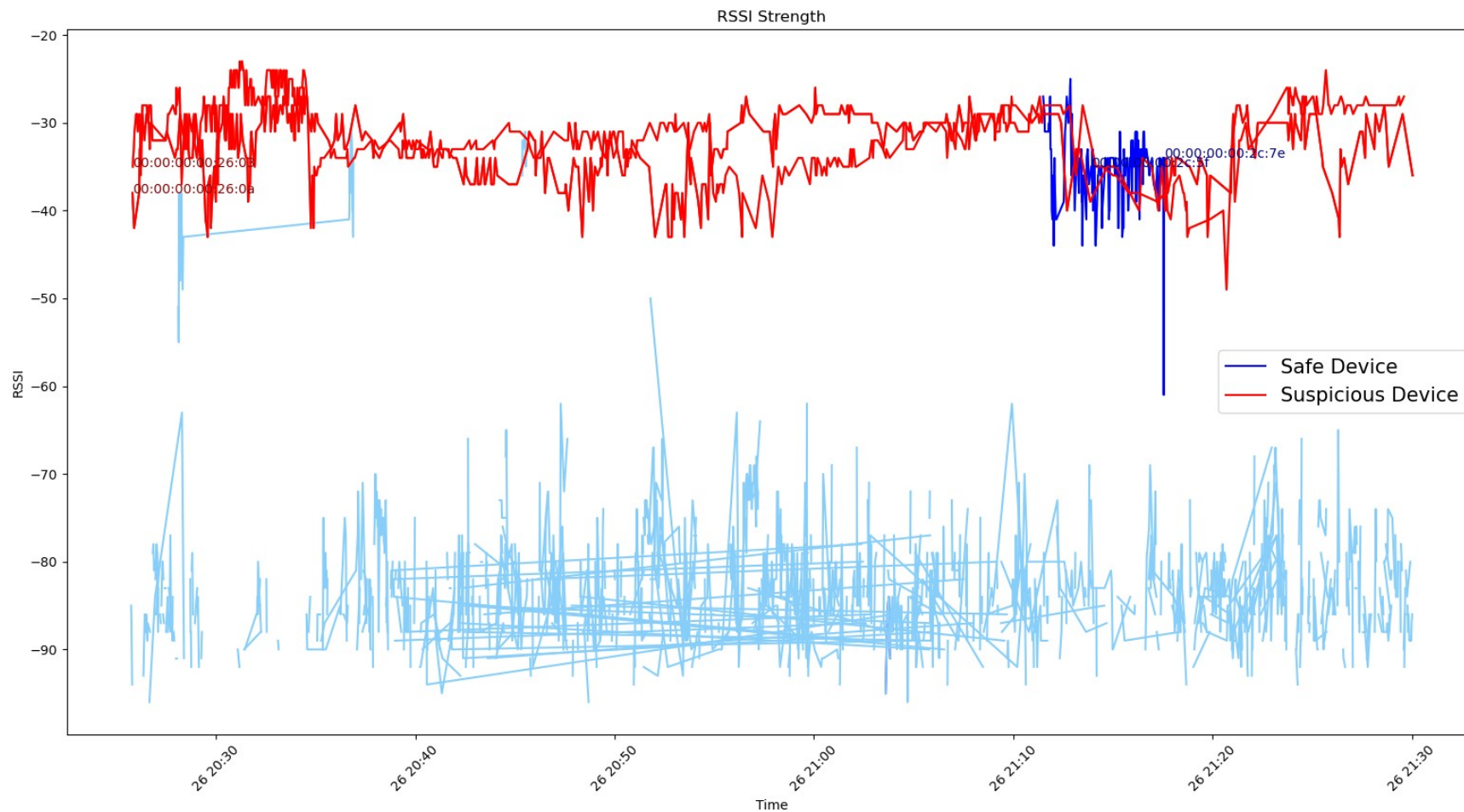
Data file c

RSSI Strength for file bledoubt_log_c.json

Legend:
- ('Safe Device', 1215)
- ('Suspicious Device', 5)

Y-axis: RSSI

X-axis: Time

Data file c – long detection

RSSI Strength

Data file n

RSSI Strength for file bledoubt_log_n.json

Data file n - long detection

RSSI Strength

Legend:
- Safe Device
- Suspicious Device
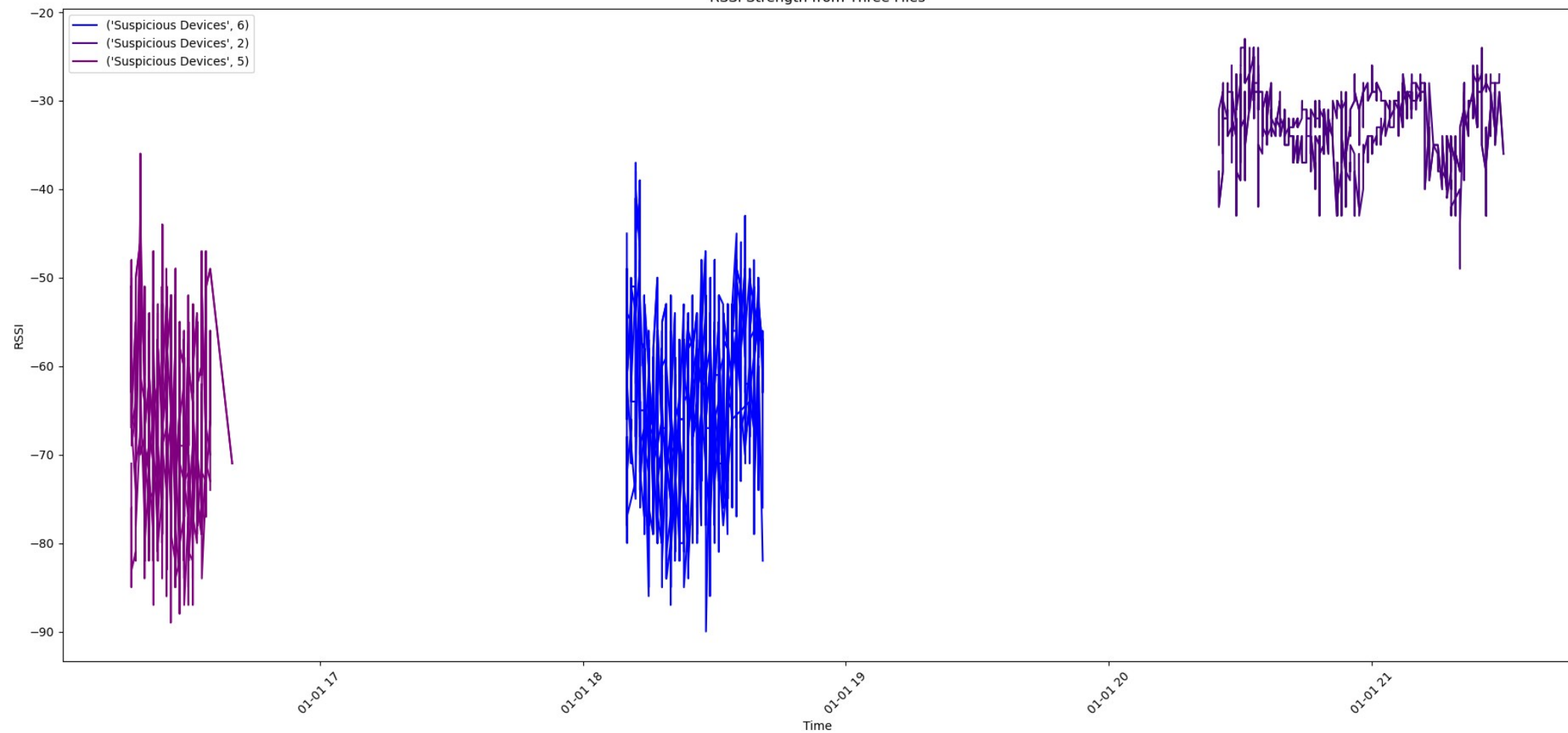
Time of Day

```python
88    #note: change function to takes in variable
89    # new plot function to simplify main()
90    def plot(data, setsus, color1):
91        mac, rssi, time = make_rssi(data)
92        fmac, arssi, atime = sort(mac, rssi, time)
93        macsus, rssisus, timesus, = findsus(setsus, fmac, arssi, atime)
94
95        plt.plot(timesus[0], rssisus[0], color=color1, label=("Suspicious Devices", len(macsus)))
96
97        for i in range(len(macsus)):
98            sorted_pairs = sorted(zip(timesus[i], rssisus[i]), key=lambda x: x[0])
99            timesus_paired, rssisus_paired = zip(*sorted_pairs)
100           plt.plot(timesus_paired, rssisus_paired, color=color1)
```
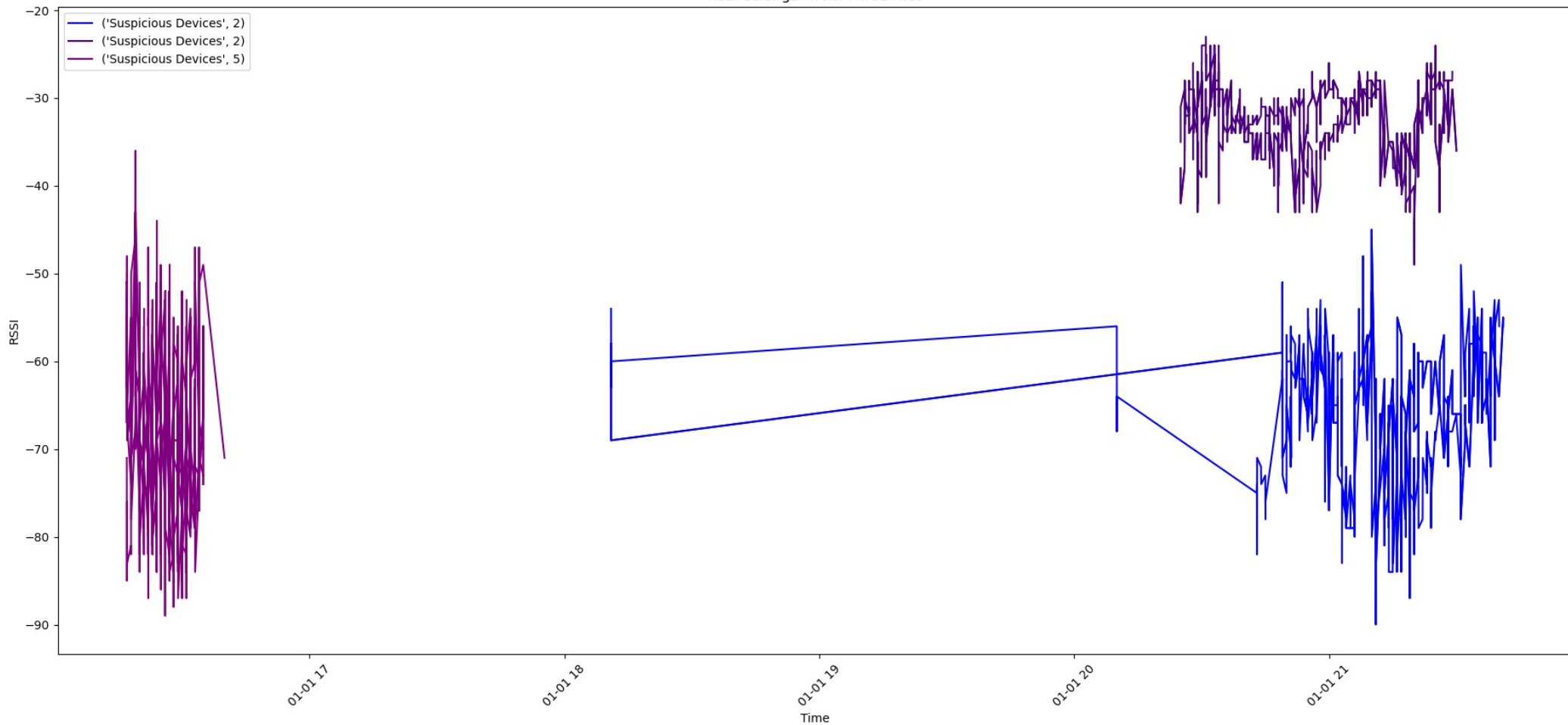
Time of day – G$_{(walking, backpack)}$,N$_{(Car)}$,J$_{(train, Backpack)}$

RSSI Strength from Three Files

Time of day – G(walking, backpack), N(Car), A(walking, backpack)

RSSI Strength from Three Files

Conclusion

- Suspicious devices have higher RSSI values

- Suspicious devices have long detection time

- Time of day has no statistically significant difference

Discussion

- Surrounding environment
- Time significance
- Time of day vs. location

Acknowledgments

- DIPr Lab
  - Primal Pappachan
  - Dylan Conklin
  - Orobosa Ekhator

- Institute for Computing in Research
  - Aaron Grinberg
  - Mark Galassi