

# Wardriving Project

Group: Satya Badde, Tasnimul Alam, and Johnny Hernandez

December 4, 2024

# Group Members

We were group #, consisting of:

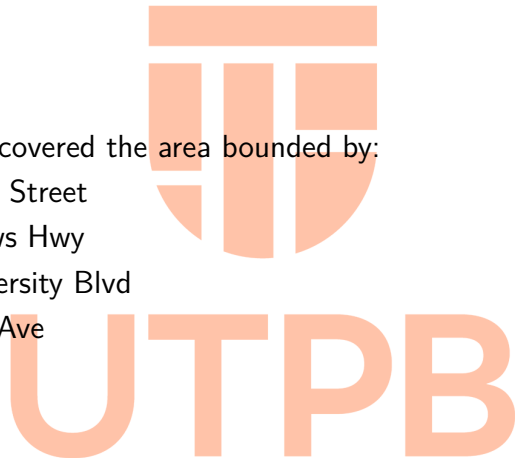
- Satya Badde, Tasnimul Alam, and Johnny Hernandez

UTPB

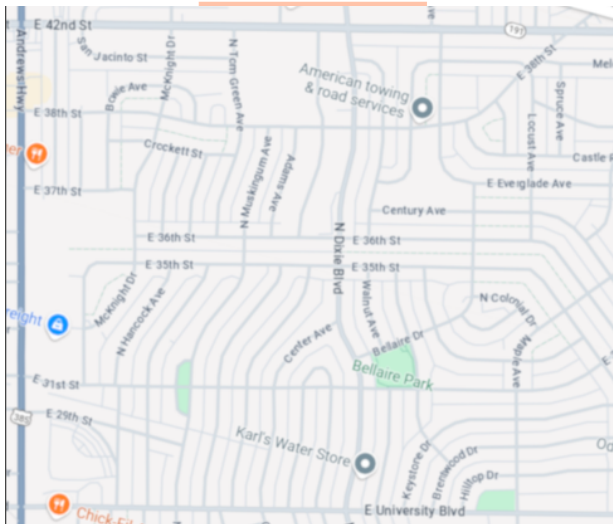
# Geographic Location

Our group covered the area bounded by:

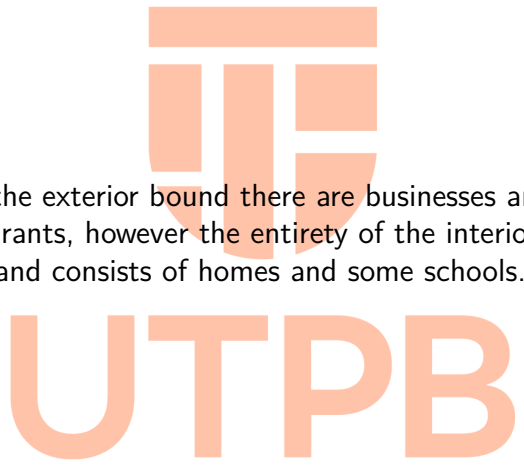
- E 42nd Street
- Andrews Hwy
- E University Blvd
- Maple Ave



# Map of Area



## Description of Area



Along the the exterior bound there are businesses and fast food restaurants, however the entirety of the interior is residential and consists of homes and some schools.

# Data

We found 6281 total access points (6264 of which fall under WIFI), falling into the following broad categories:

- Open: 527 presumed to be open or an extended service set (ESS)
- WEP: 40
- WPA: 1
- WPA2: 5246
- WPA3/WPA2 EAP Only: 88
- WPA2/SAE capability: 301

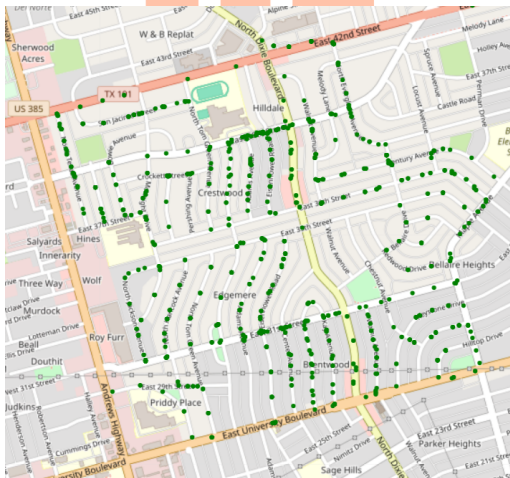
## Map of APs



There were some dead areas that we had planned to re-visit before the incident that caused us to stop occurred, however, most if not all roads were available for us to drive and take readings on.

# Open APs

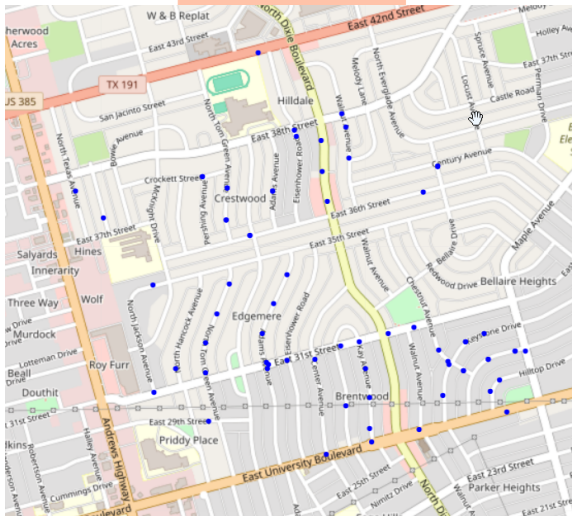
Of the open APs we found, these appear to have no security at all:





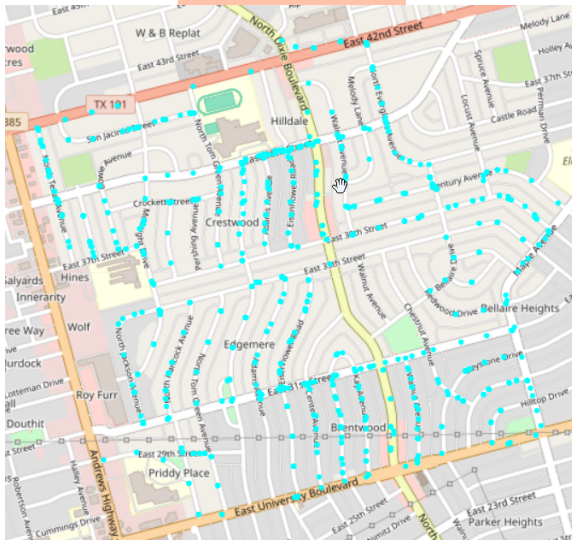
# WEP APs

These APs are operating in WEP mode only:



# Map of APs

These are the APs operating in WEP or are open:



These APs are operating in WPA mode only:



There were no inherent observations regarding vulnerabilities other than the APs operating in WEP or the APs that seem to be open, however, there are a large amount of APs with only ESS capability. Considering that APs that are ESS compatible are an extension of other APs there could be assumptions that those APs can be proxies.

UTPB

# Difficulties

The drive went perfectly fine for the most part and as a group we knew we wanted to go back and attempt to pick up more APs and streets we may have missed, however, by the end of the drive, the vehicle we were driving began to leak coolant at a rapid rate and we were not able to continue our capture. Due to network connectivity issues there were points in our section that would not continue capturing unless the vehicle was stationary.

# Mapping

The mapping of the APs was done using jupyter notebook and the pandas and folium packages. Pandas being a library in python used for data analysis of structures (in this case a csv). Folium is a python library used for visualizing geospatial data. An Example of that looks like:

```
import pandas as pd
import folium
df = pd.read_csv('C:/Users/jhern/Downloads/Capture1.csv', delimiter = ',', encoding='latin-1', headers=1)

mymap = folium.Map( locations[ df.CurrentLatitude.mean(), df.CurrentLongitude.mean() ], zoom_start=12)
|
for coord in df[['CurrentLatitude', 'CurrentLongitude', 'SSID', 'Type', 'MAC']].values:
    if (coord[3] == 'WIFI'):
        folium.CircleMarker(locations[coord[0], coord[1]], radius=1, color='red', popup=[ "SSID:", coord[2], "BSSID:", coord[4]]).add_to(mymap)

mymap.save('testone.html')
```

# What Can Someone do With This Information?

- Search for vulnerable access points and gain access.
- Gain access and sniff network traffic.
- Perform illegal activities on someone's network while using something like tails Linux, thereby leaving no trail.

UTPB

# Questions



UTPB