

The Bluetooth Device Database

Ryan Holeman
@hackgnar

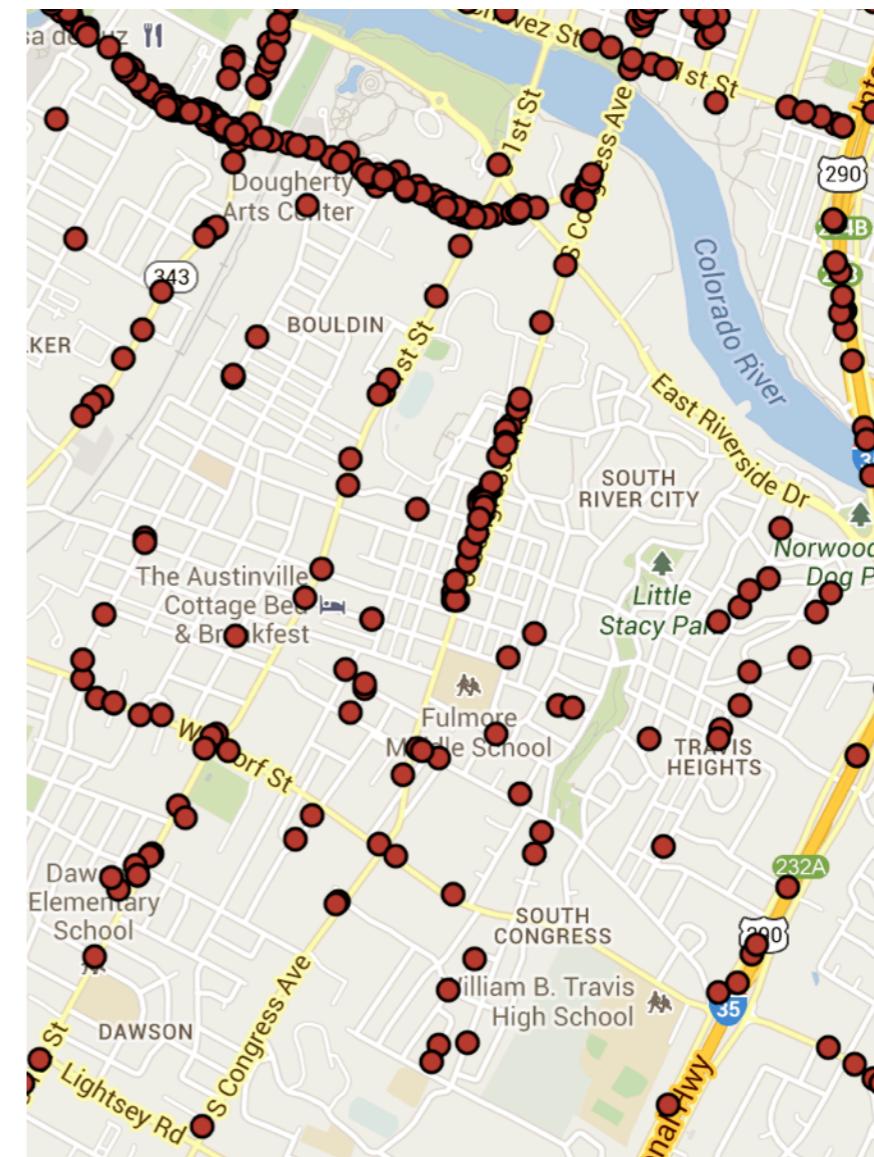
About Me

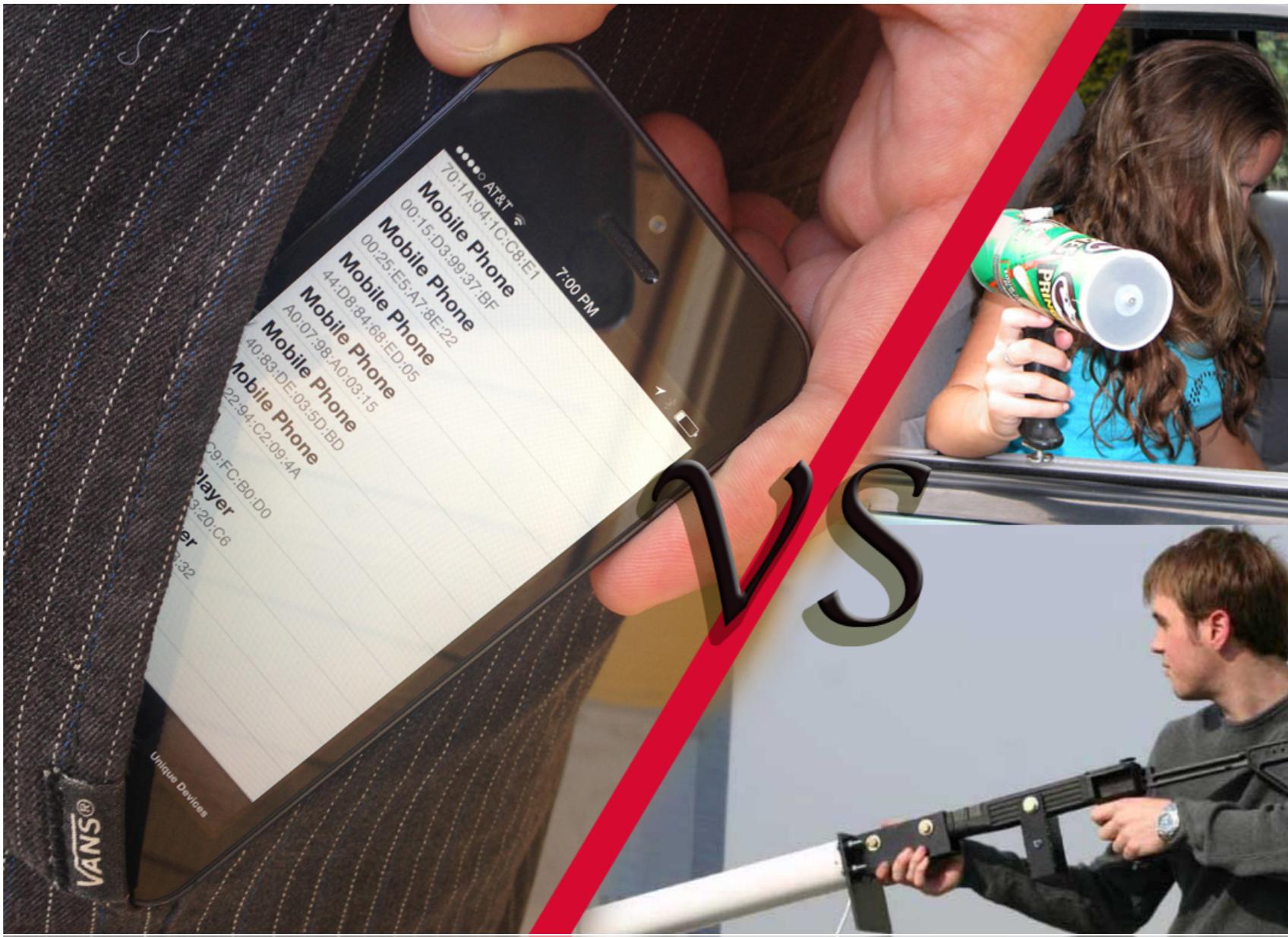
- Ziften Technologies
- Python & Ubertooth
 - github.com/hackgnar
- Twitter: @hackgnar



BT Device Survey

- Survey of discoverable bluetooth devices
- Curiosity
- Awareness
- Why only discoverable?

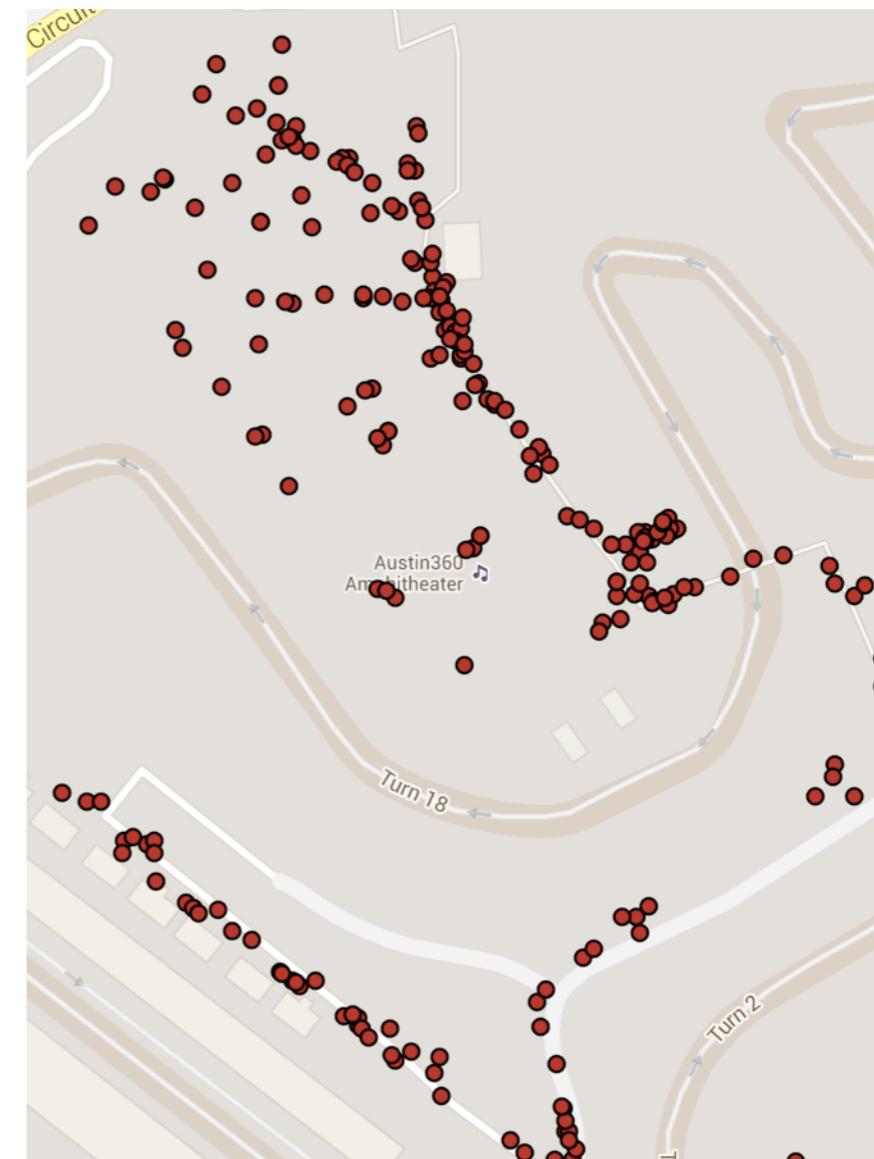




Convenience

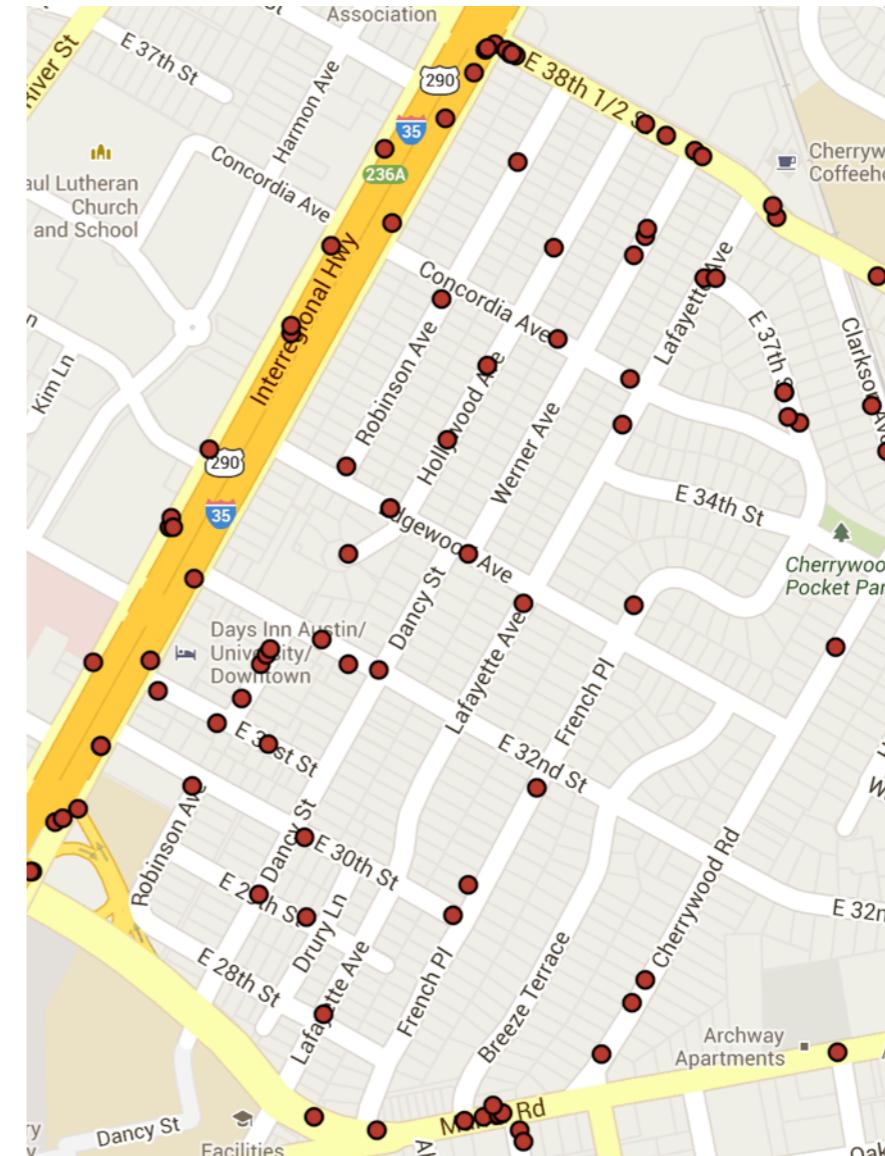
Data Collected

- Address
- Device name
- Geolocation
- Other metadata



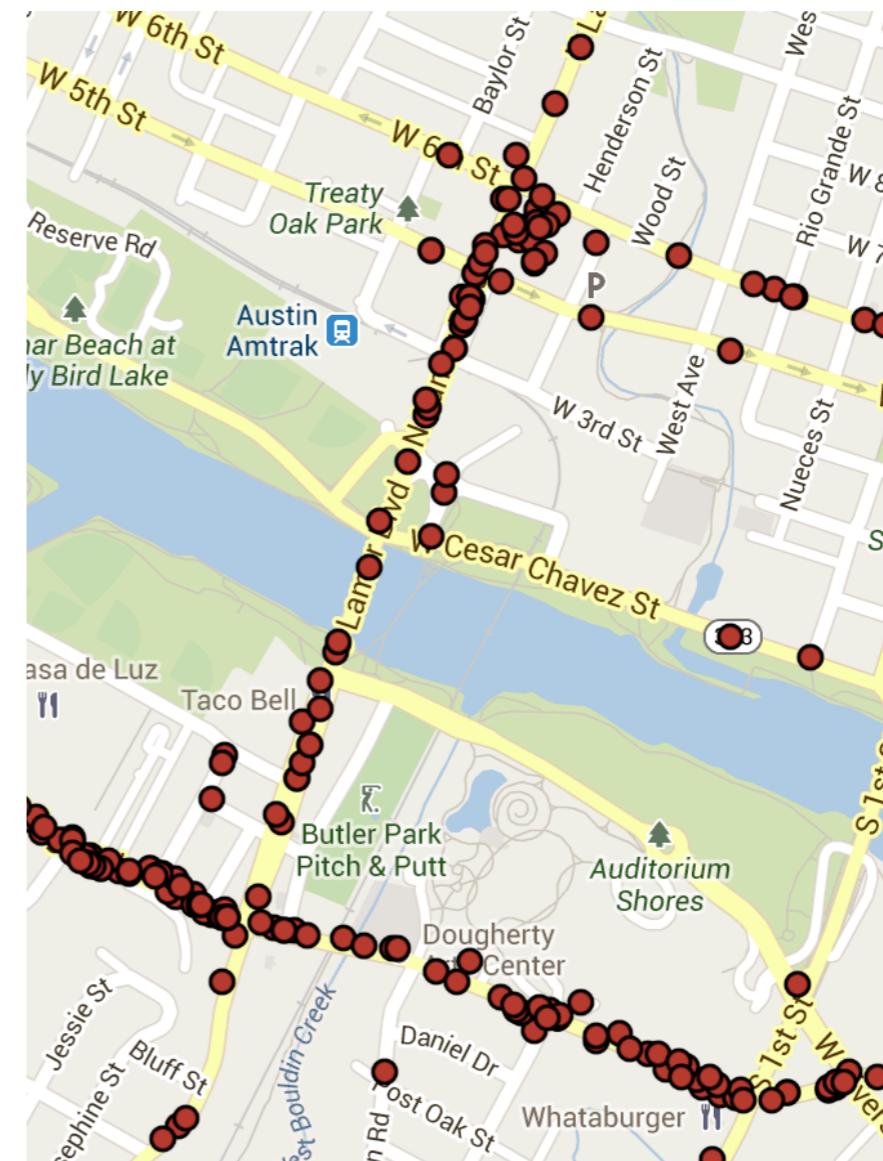
Tools and Data

- Open source
- Client
 - iOS, *nix, OSX, Win
- Server
 - DIY & managed
- Open data



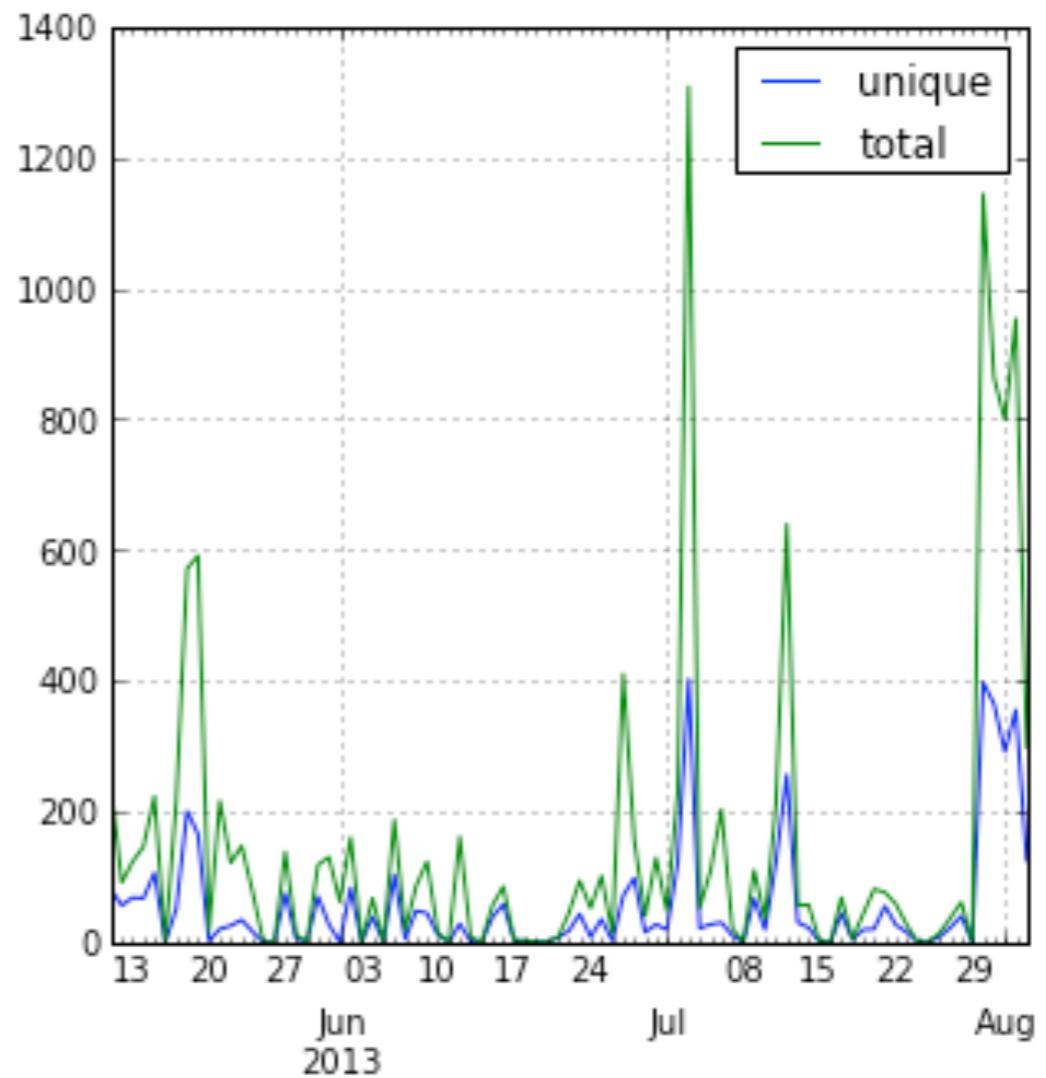
Similar Projects

- Open source
 - Bnap Bnap
 - Bluetooth Profiling Project
- Closed source
 - Wirelesswerx
 - Houston's TranStar



Whats Out There?

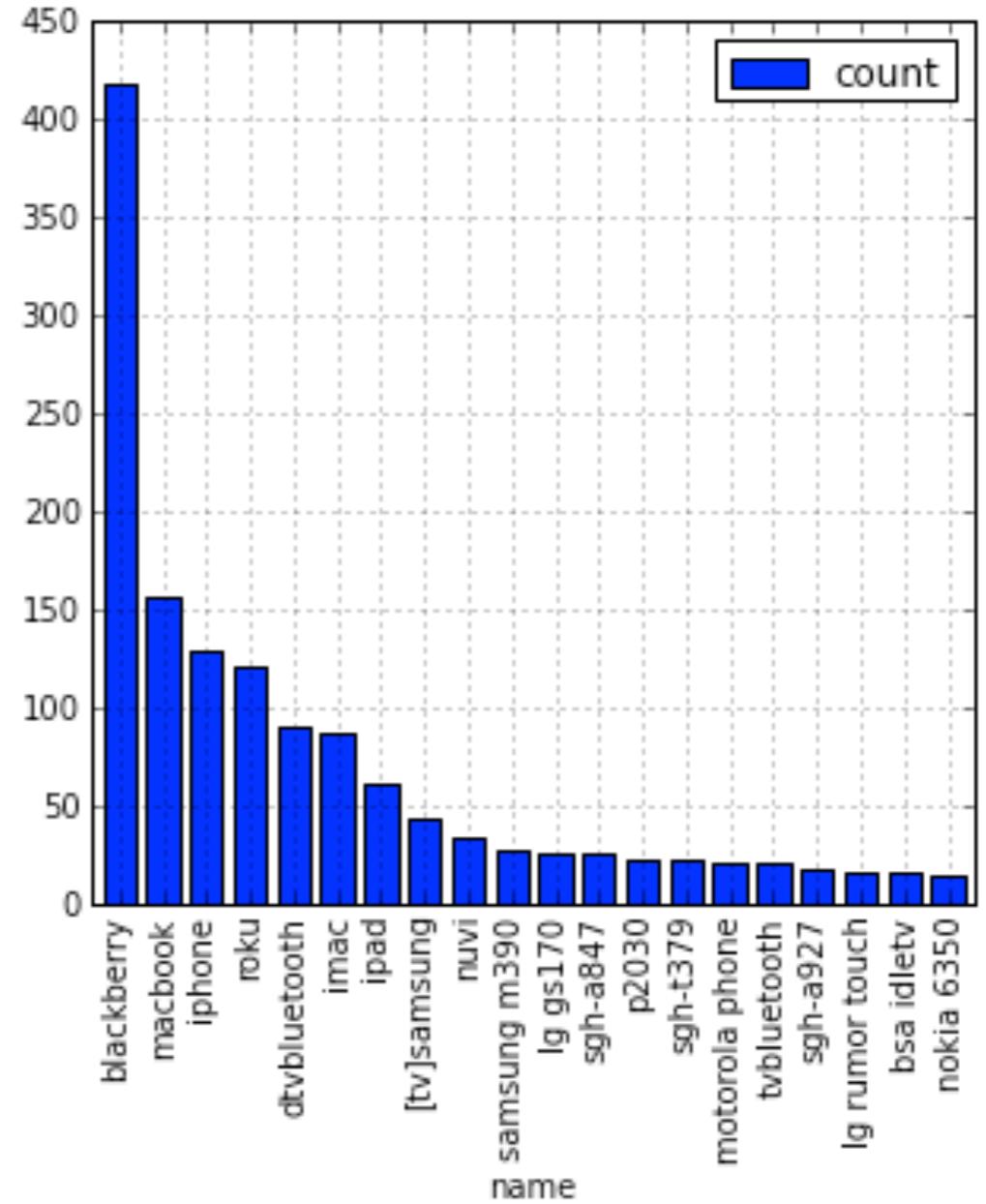
- Total device sightings:
12,860
- Unique devices address:
4,787



Most popular
discoverable bluetooth
device?

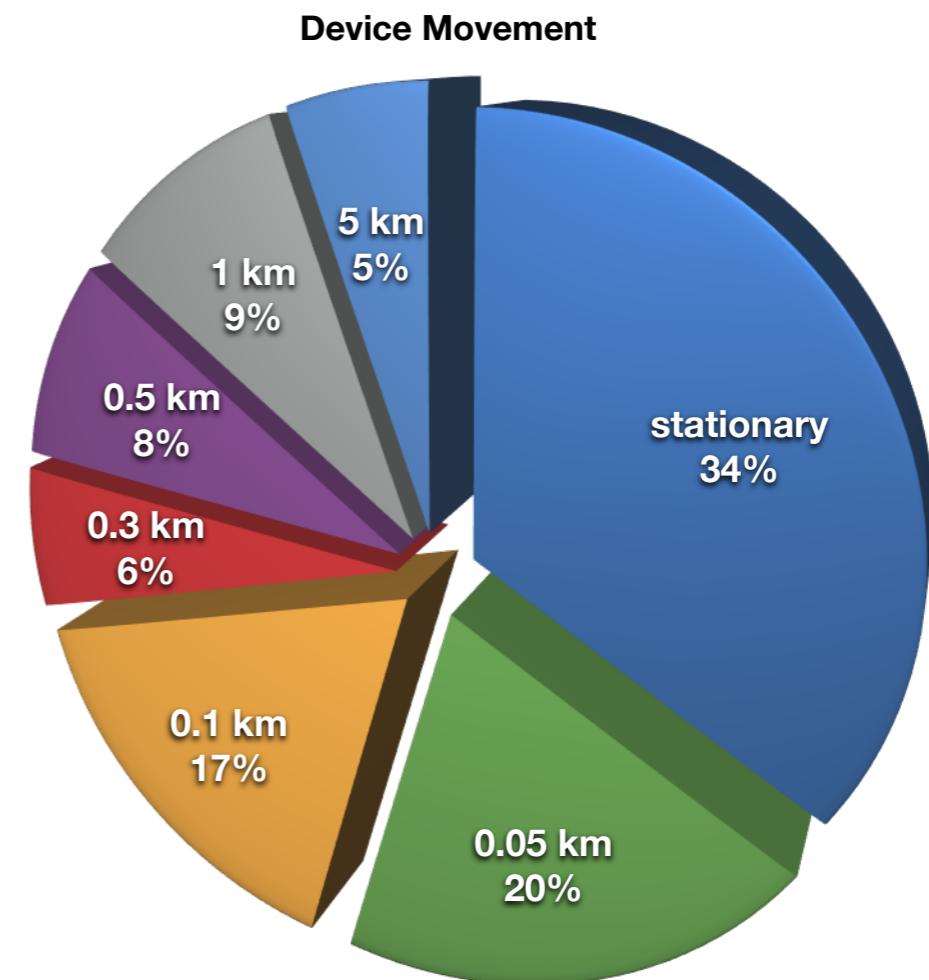
Prevalence

- Top 10 most prevalent discoverable BT devices by name
- Generic names removed
- Grouping required human interaction



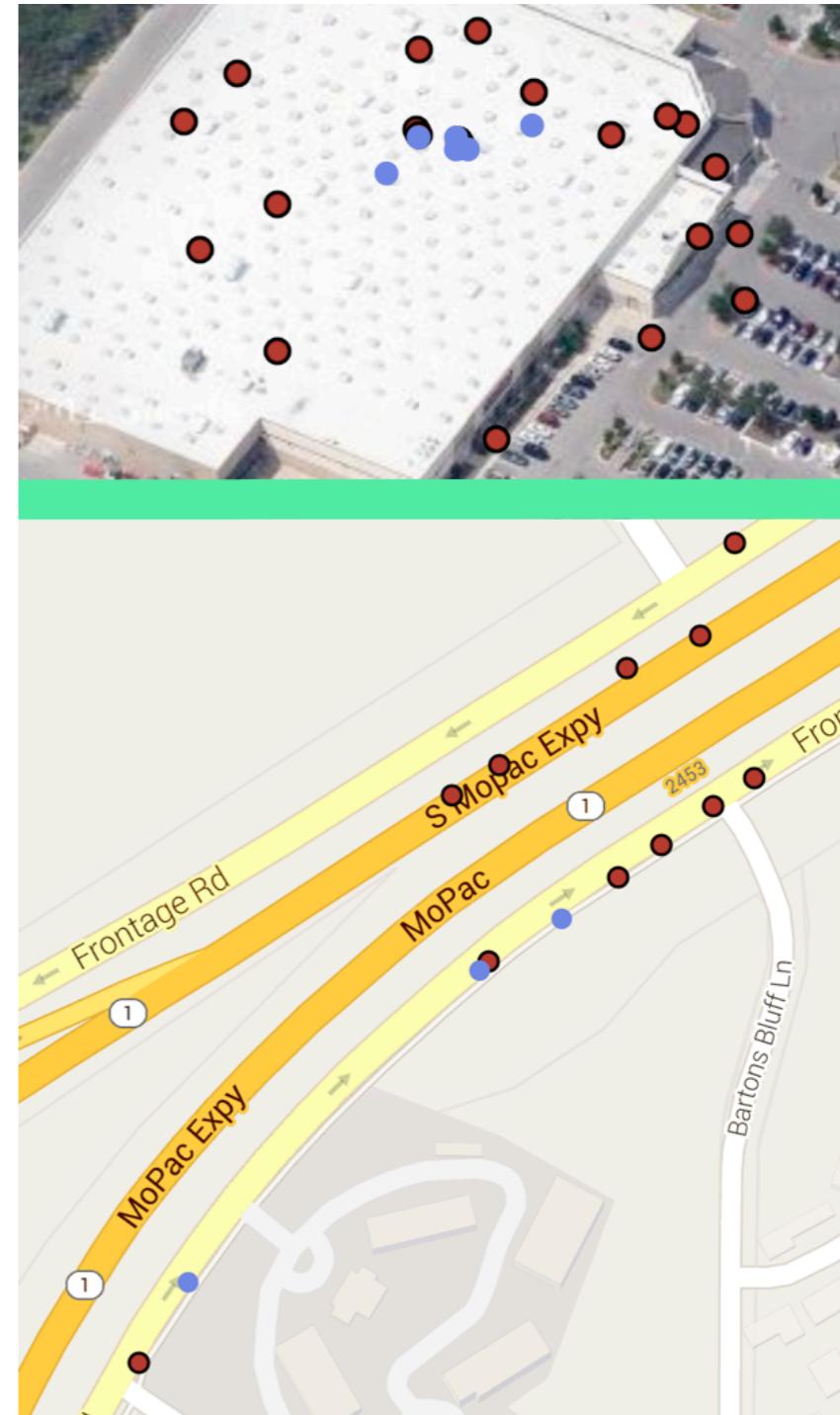
Movement

- Static vs moving sensor
- Multiple sightings required
 - 1,700 unique devices with 2+ sightings
- Computed by a devices 2 farthest points



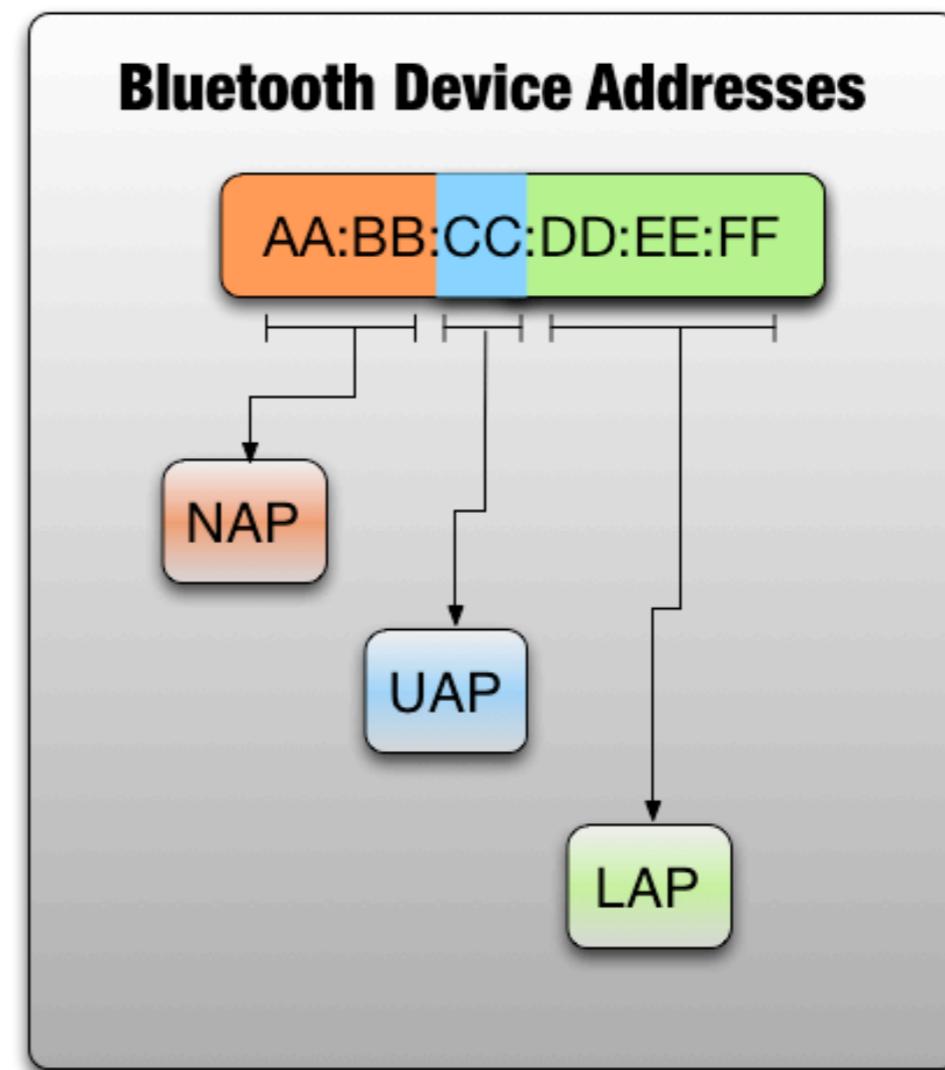
Reoccurrence

- What can we do with devices we see multiple times?
- Used for filtering out known devices
- Used for identifying small world phenomena



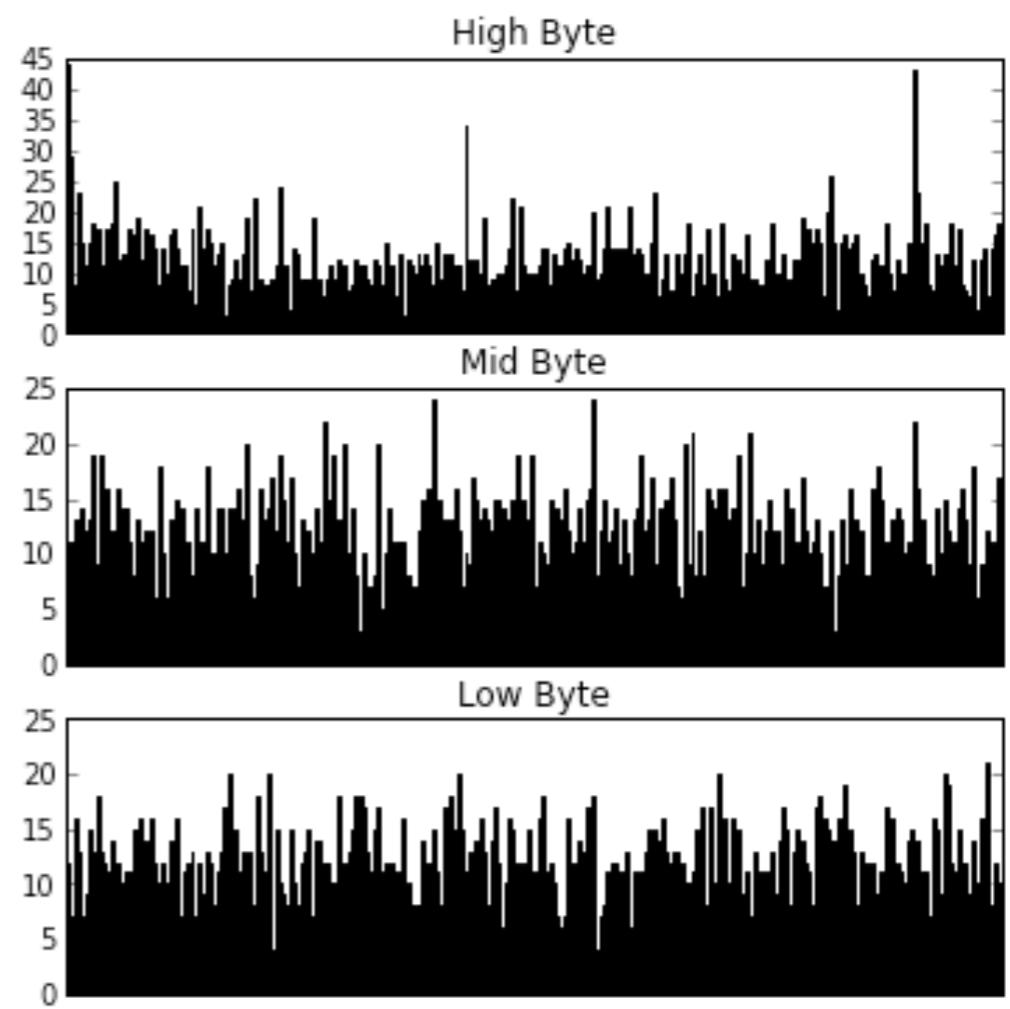
Bluetooth Addresses

- NAP
 - Vendor association
- UAP
 - Vendor association
- LAP
 - Device specific



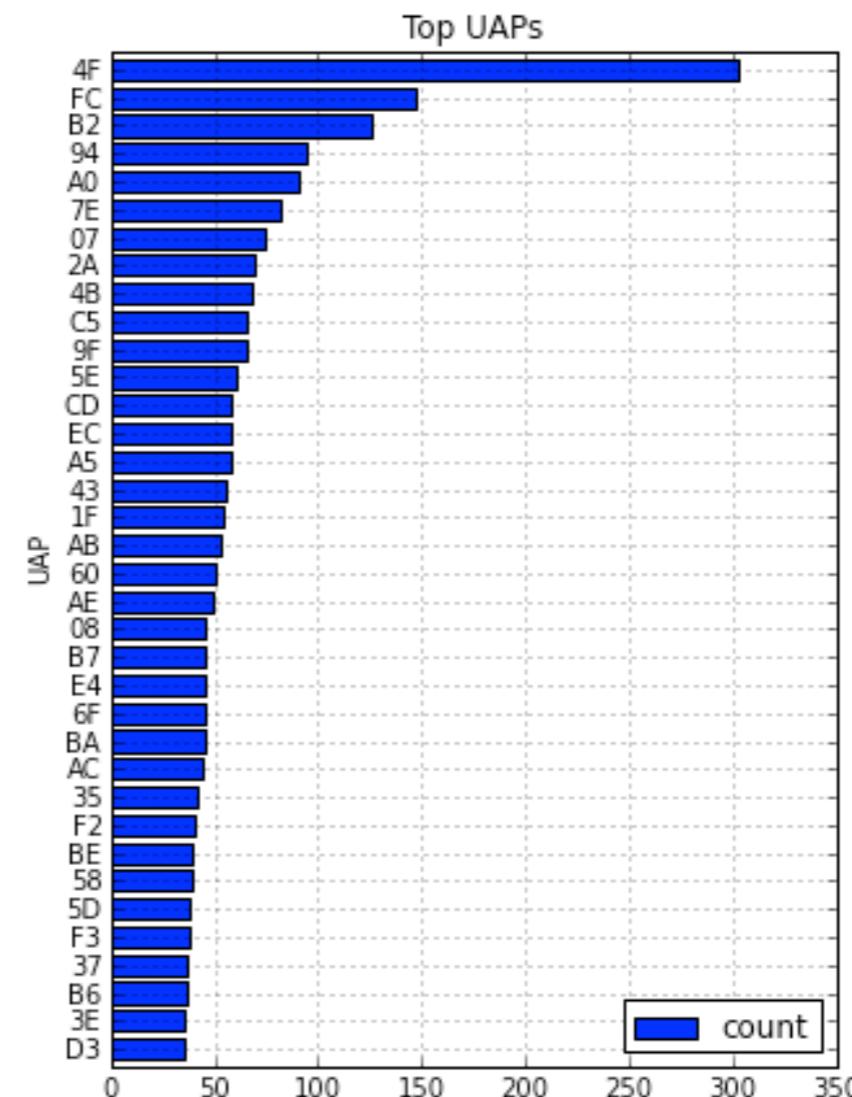
LAP Statistics

- 16,777,216 possible
- Collisions
 - Birthday paradox ~4k
 - First collision at 3,158
- Are peripherals worse?
- No apparent hot spots



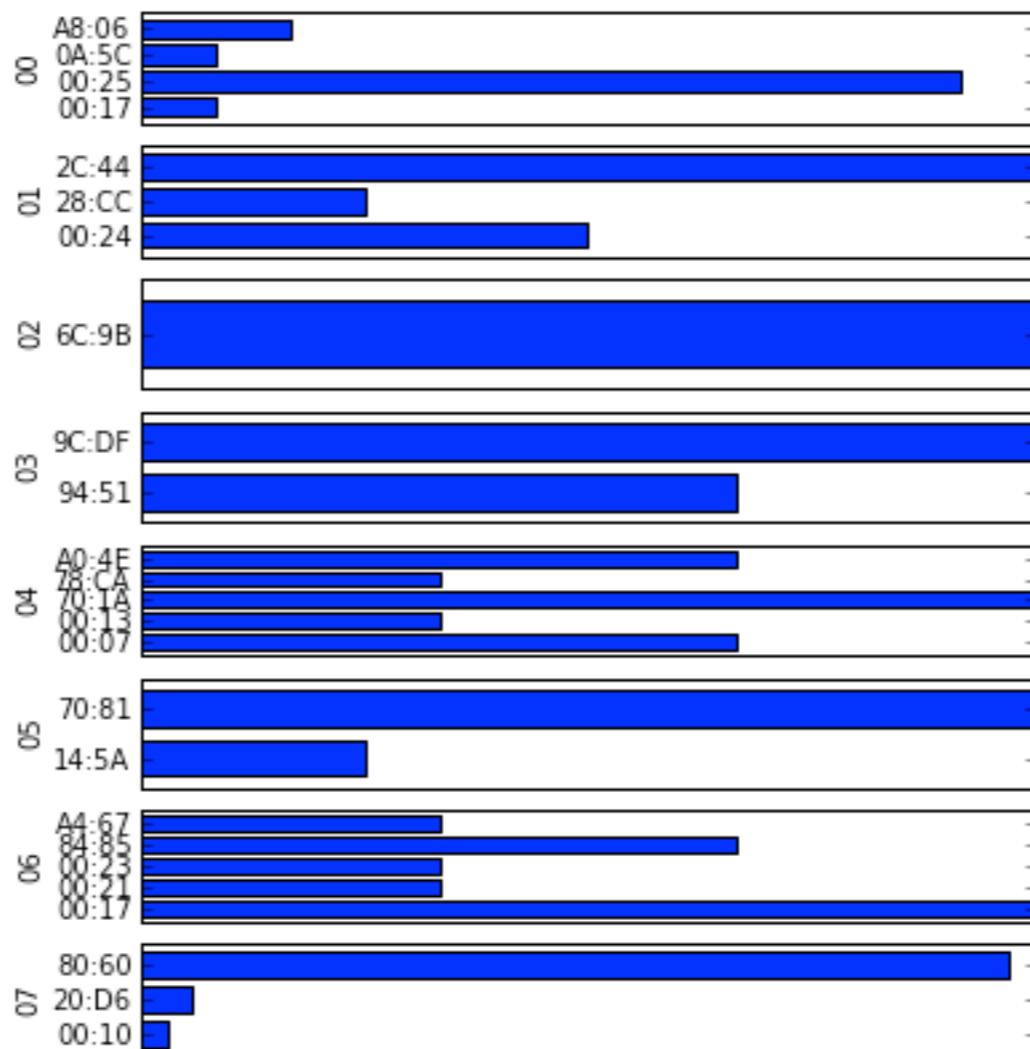
UAP Statistics

- 246 of 256 possible UAP's used
- Hot spots do exist
- High probability UAP can be used for passive detection



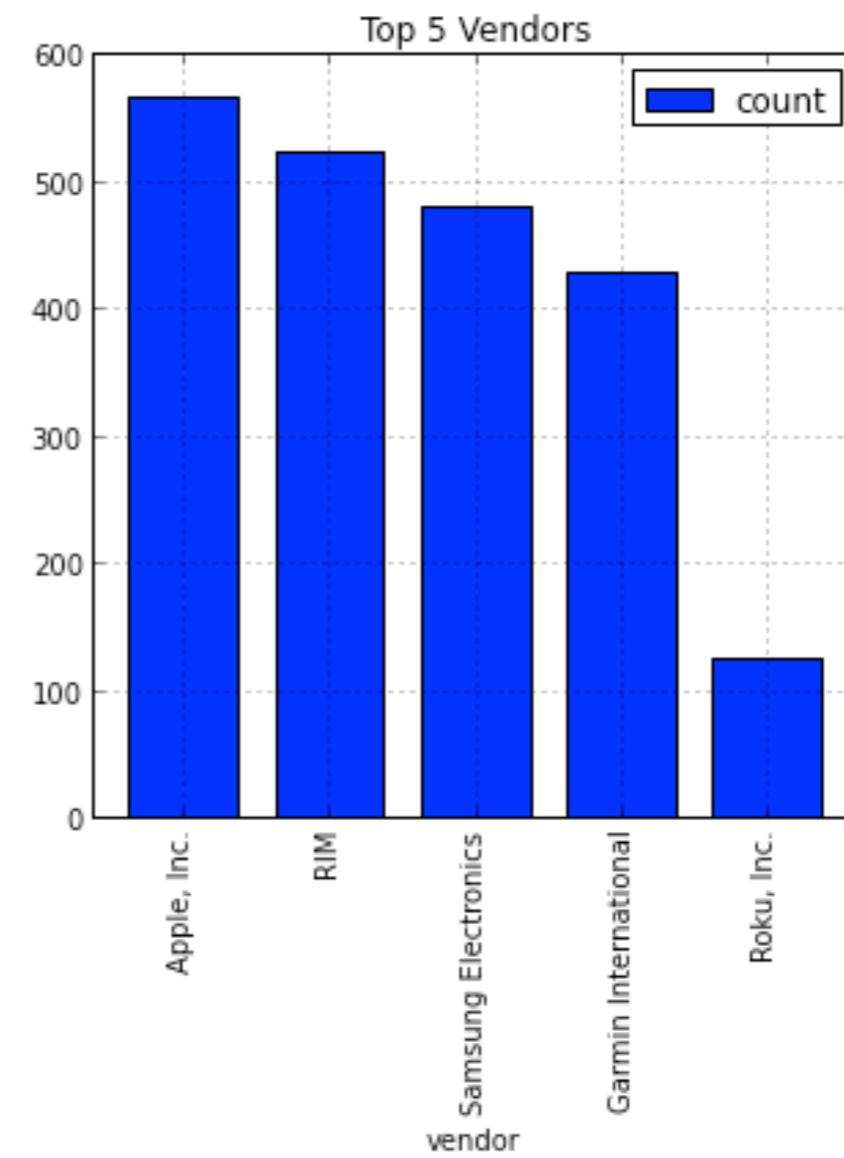
NAP Statistics

- Only a small amount of the address space is used 554 / 65,536
- Possible NAP probability by UAP
- Majority of UAP instances have only 1-3 associated NAP
- Worst case is 8 NAPs



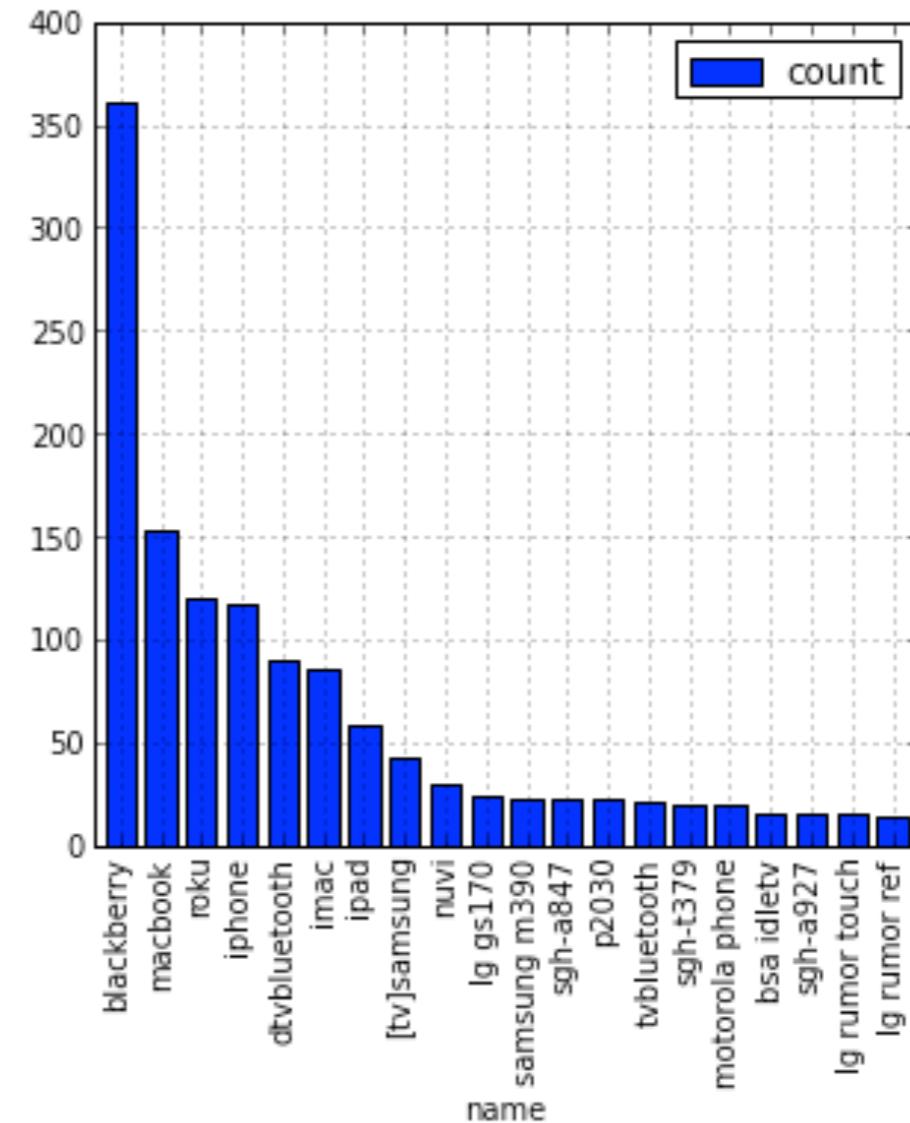
Vendor Statistics

- Top 5 vendors
- Can be used to improve NAP by UAP probability



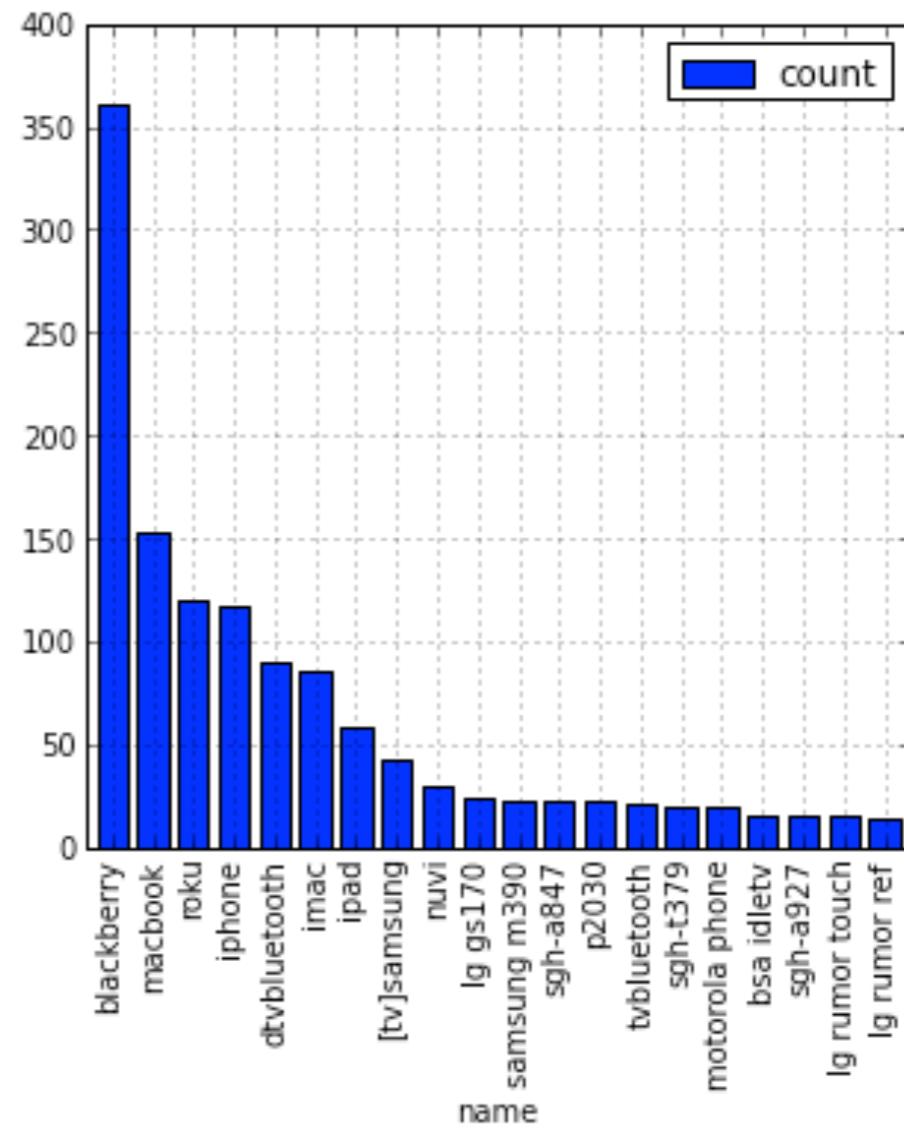
Security

- Is tracking an issue for you?
- Discoverable devices can assist targeted attacks
- Do you sweep for bluetooth during audits?



Awareness

- Hidden functionality
 - Car headsets
- Bugs
 - iOS
- Bad HCI
 - BlackBerry, OSX



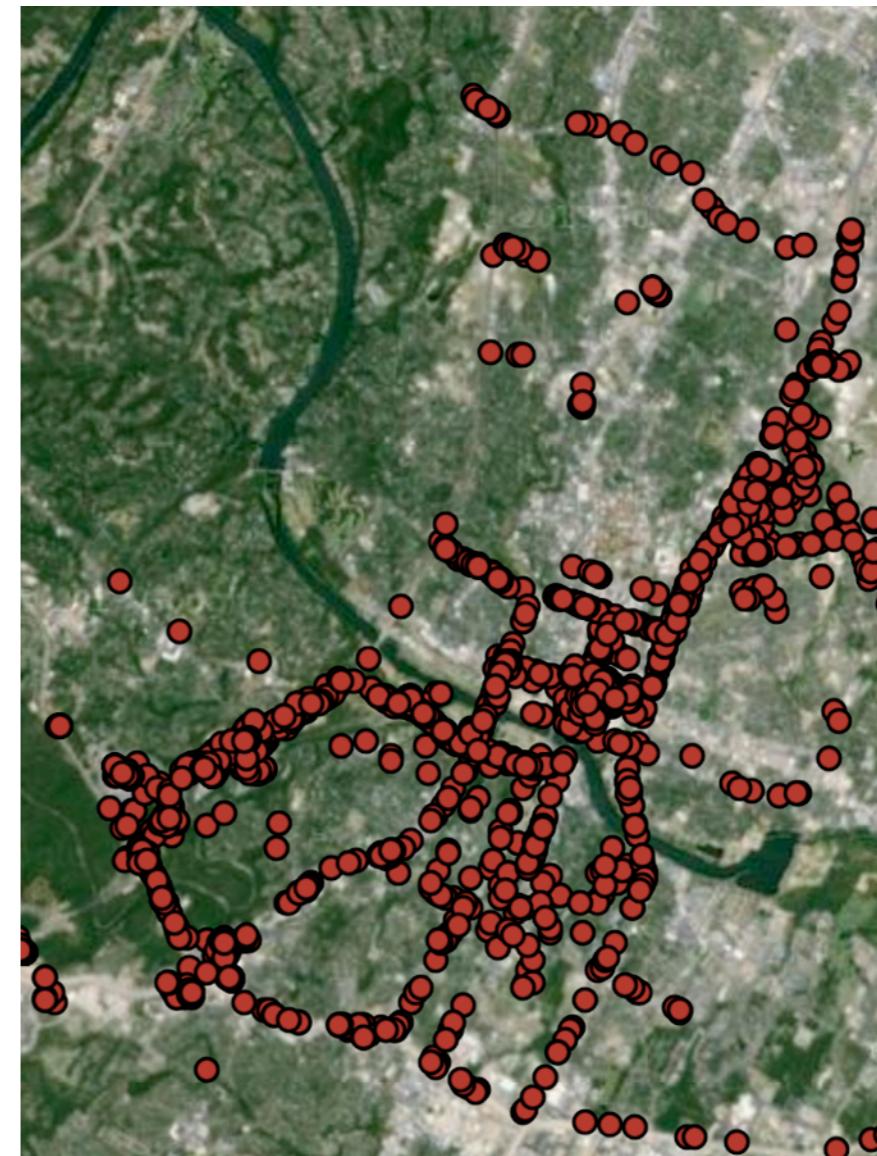
Legal Issues

- Are you aware of any?
- Same as WiFi?
- TranStar & Wirelesswerx



Participation

- Bluetoothdatabase.com
- [github.com/hackgnar/
bluetoothdatabase](https://github.com/hackgnar/bluetoothdatabase)



Future Work

- Real time statistics on bluetoothdatabase.com
- Community participation
- Service enumeration
- Passive survey
 - SR & BTLE

