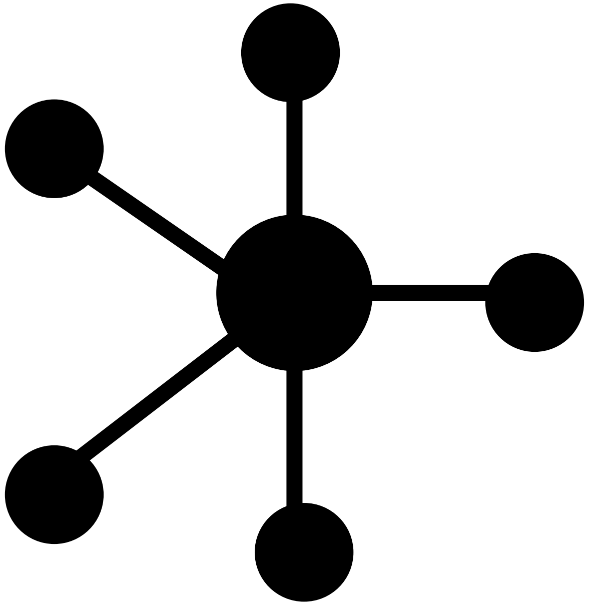
# net.tagger: Crowdsourcing Local physical network infrastructure



CAIDA AIMS Workshop

UCSD, 16 April, 2019

Justin P. Rohrer

Robert Beverly

Riqui Schwamm

Dan Woodman

Marie Rogers

**Naval Postgraduate School**

cMAND

# net.tagger

- Background and Motivation
- Our Solution
- Preliminary Results
- Future Work

# Topology Discovery

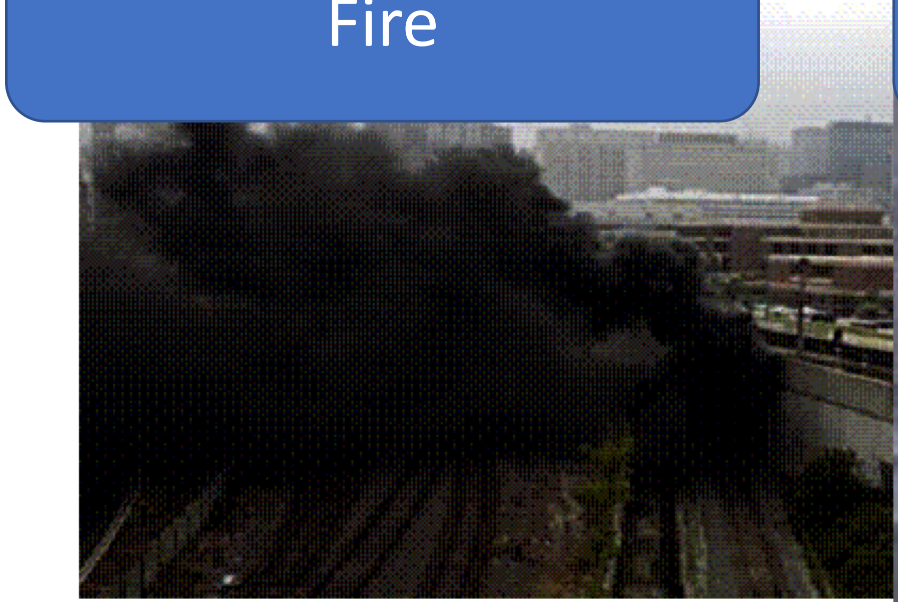
- Lots of work on *logical* topology discovery:
  - Active/passive measurements (traceroute, BGP, etc)
  - Finding IP, router, AS, or even organization-level graph
- Less work on *physical* topology in research space
  - Internet Atlas
  - Topology Zoo

net.tagger is a complementary project focusing on physical network infrastructure discovery

- Focus on microscopic detail, vs existing macroscopic efforts

# Why care about physical network?

- Identify logically independent, but physically dependent paths
- Improve critical infrastructure protectio



Howard Street Tunnel Fire

“Va
Ar

L3 California “Bad hole day”

# How well do we know the physical network

- Existing work focuses on:
  - PUC databases
  - Published network maps
- No aggregated database
  - Infrastructure is global
  - PUC databases are local
  - Existing maps are frequently incorrect

# How to map physical topologies?

- Latency-based geolocation from lots of vantage points?
  - Too inaccurate
- Buy maps from 3rd party companies?
  - Expensive, incomplete
- Have your grad students read the environmental impact statements at city hall?
  - Expensive, incomplete
- Or, just go look for it?

Make crowdsourced discovery easy
Available now on Android and IOS!

# Crowdsourcing Model

- Develop list of street-level indicators of Internet infrastructure
- Develop app that allows users to tag location, type, provider, and metadata for indicators
- Compile results, analyze

Users answer the question “What is here?”
Later, researchers can ask “Where is X?”

# Physical infrastructure markers everywhere

- Meta-data: provider name

**Qwest**

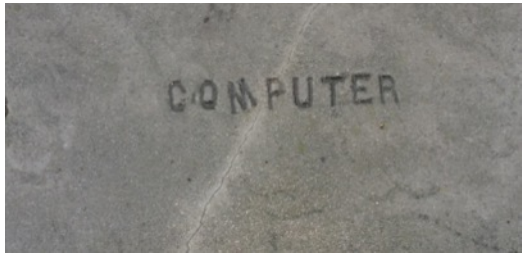
**AT&T**

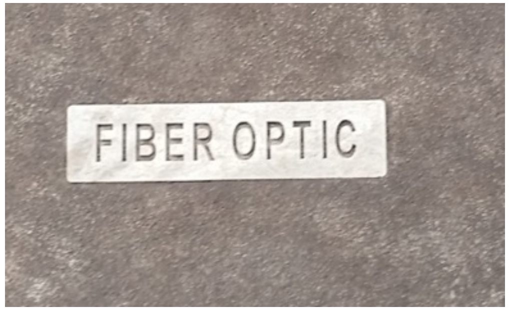
**newbasis**

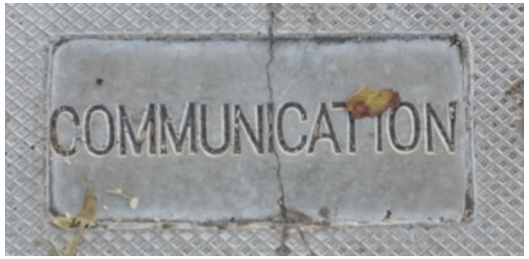
**SBC**

# Physical infrastructure markers everywhere

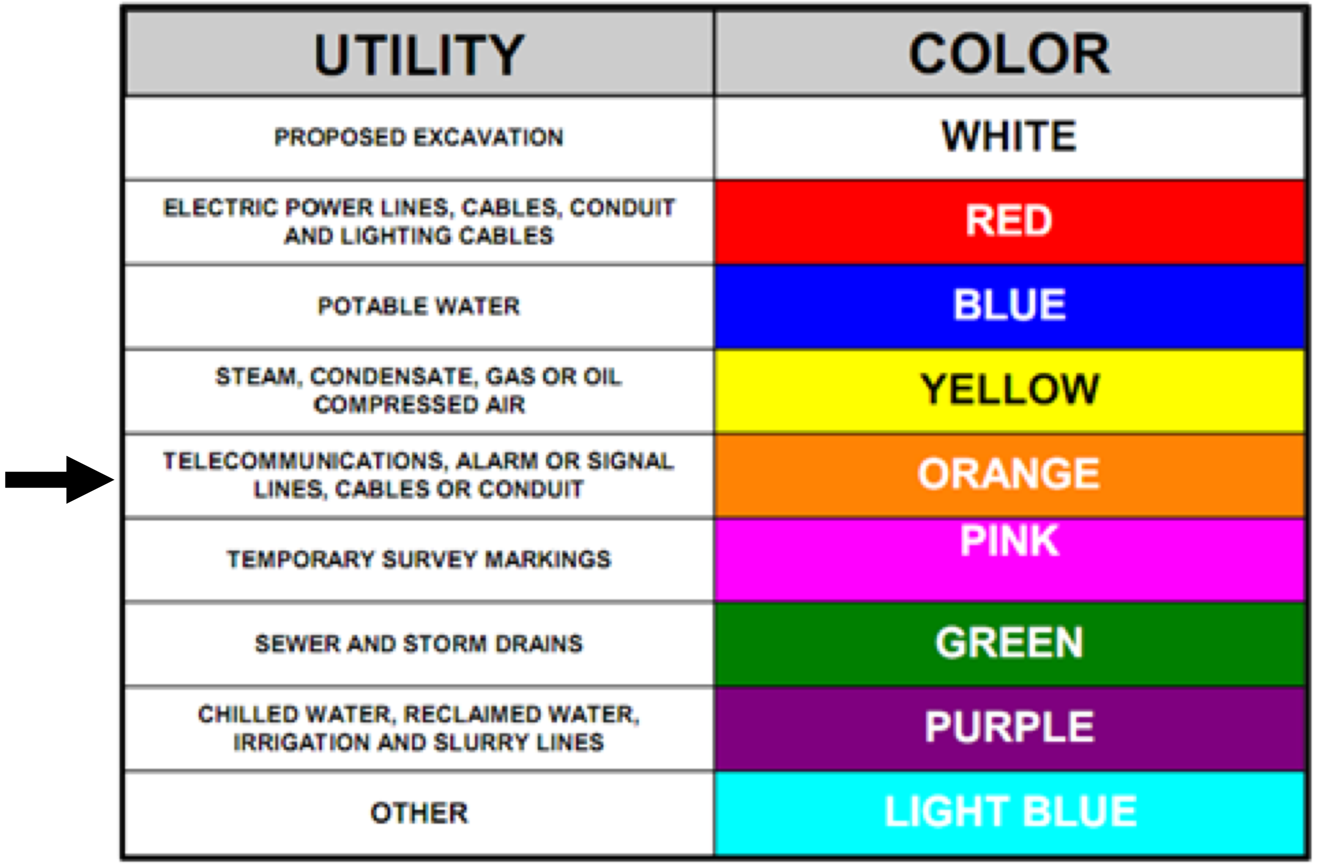
- Meta-data: keywords



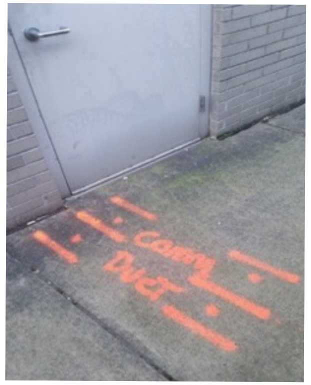


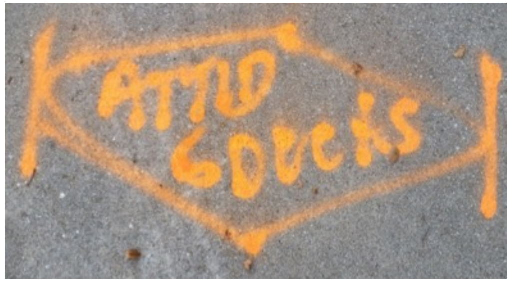


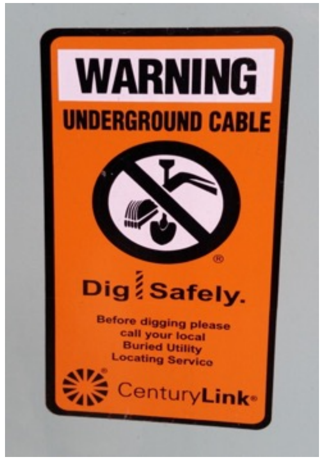
# Dig Markings, warnings



| UTILITY | COLOR |
|---|---|
| PROPOSED EXCAVATION | WHITE |
| ELECTRIC POWER LINES, CABLES, CONDUIT AND LIGHTING CABLES | RED |
| POTABLE WATER | BLUE |
| STEAM, CONDENSATE, GAS OR OIL COMPRESSED AIR | YELLOW |
| TELECOMMUNICATIONS, ALARM OR SIGNAL LINES, CABLES OR CONDUIT | ORANGE |
| TEMPORARY SURVEY MARKINGS | PINK |
| SEWER AND STORM DRAINS | GREEN |
| CHILLED WATER, RECLAIMED WATER, IRRIGATION AND SLURRY LINES | PURPLE |
| OTHER | LIGHT BLUE |

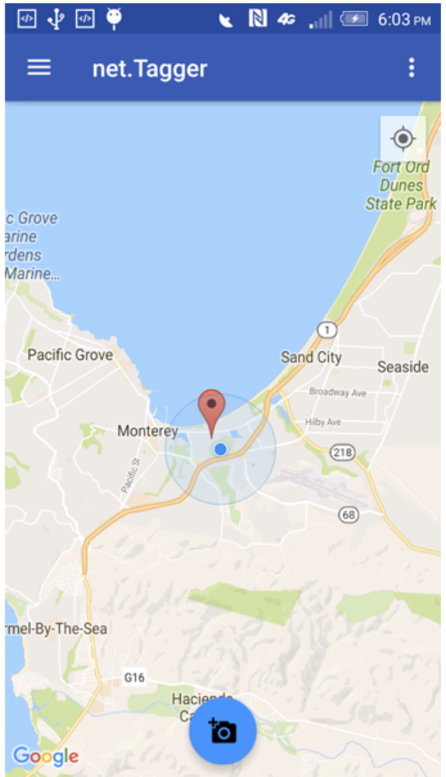


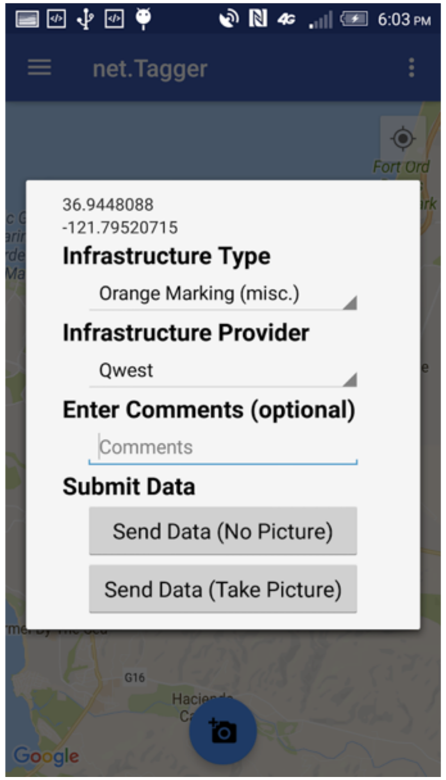



WARNING
UNDERGROUND CABLE
Dig Safely.
Before digging please call your local Buried Utility Locating Service
CenturyLink

# net.tagger app

- Crowdsource physical infrastructure discovery
- Users “tag” infrastructure using a free, easy-to-use mobile app
- Future:  Win points for tagging, verifying





36.9448088
-121.79520715

**Infrastructure Type**

Orange Marking (misc.)

**Infrastructure Provider**

Qwest

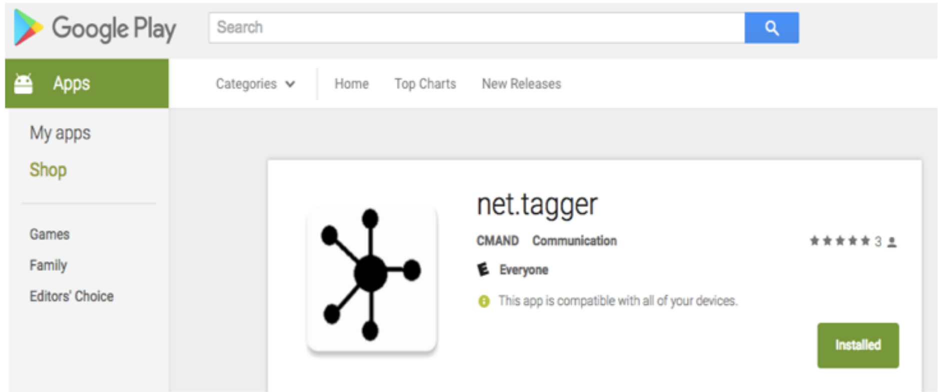
**Enter Comments (optional)**

Comments

**Submit Data**

Send Data (No Picture)

Send Data (Take Picture)



net.tagger

CMAND Communication

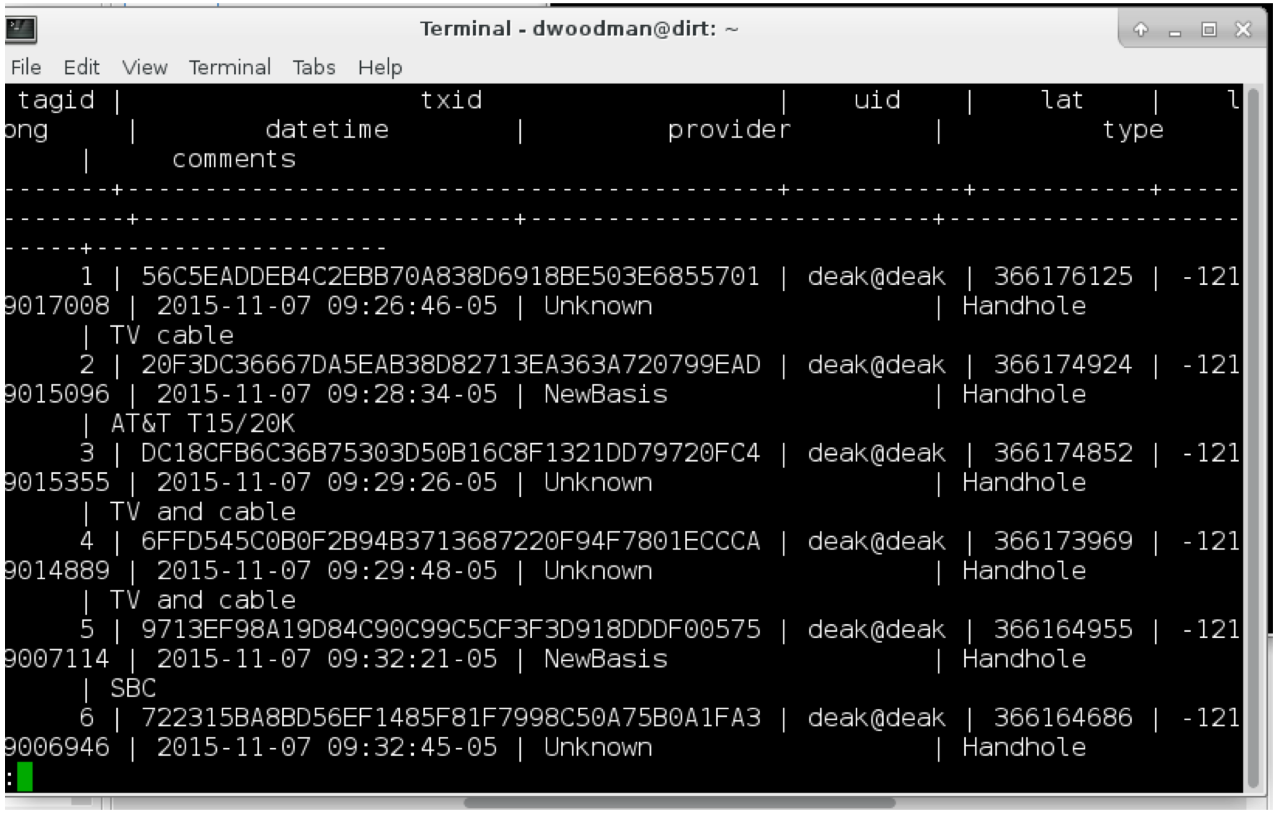
★★★★★ 3

E Everyone

This app is compatible with all of your devices.

# net.tagger app

- Aggregation and analysis on backend
- Postgres DB, based on Open StreetMaps schema



Terminal - dwoodman@dirt: ~
File Edit View Terminal Tabs Help

```
 tagid |                   txid                   |    uid    |    lat    |    l
ong     |        datetime        |         provider         |          type
     |     comments
-------+------------------------------------------+-----------+-----------+-----
--------+------------------------+--------------------------+-------------------
-----+-------------------
     1 | 56C5EADDEB4C2EBB70A838D6918BE503E6855701 | deak@deak | 366176125 | -121
9017008 | 2015-11-07 09:26:46-05 | Unknown                  | Handhole
     | TV cable
     2 | 20F3DC36667DA5EAB38D82713EA363A720799EAD | deak@deak | 366174924 | -121
9015096 | 2015-11-07 09:28:34-05 | NewBasis                 | Handhole
     | AT&T T15/20K
     3 | DC18CFB6C36B75303D50B16C8F1321DD79720FC4 | deak@deak | 366174852 | -121
9015355 | 2015-11-07 09:29:26-05 | Unknown                  | Handhole
     | TV and cable
     4 | 6FFD545C0B0F2B94B3713687220F94F7801ECCCA | deak@deak | 366173969 | -121
9014889 | 2015-11-07 09:29:48-05 | Unknown                  | Handhole
     | TV and cable
     5 | 9713EF98A19D84C90C99C5CF3F3D918DDDF00575 | deak@deak | 366164955 | -121
9007114 | 2015-11-07 09:32:21-05 | NewBasis                 | Handhole
     | SBC
     6 | 722315BA8BD56EF1485F81F7998C50A75B0A1FA3 | deak@deak | 366164686 | -121
9006946 | 2015-11-07 09:32:45-05 | Unknown                  | Handhole
:
```

# Quality of tags, mislabels

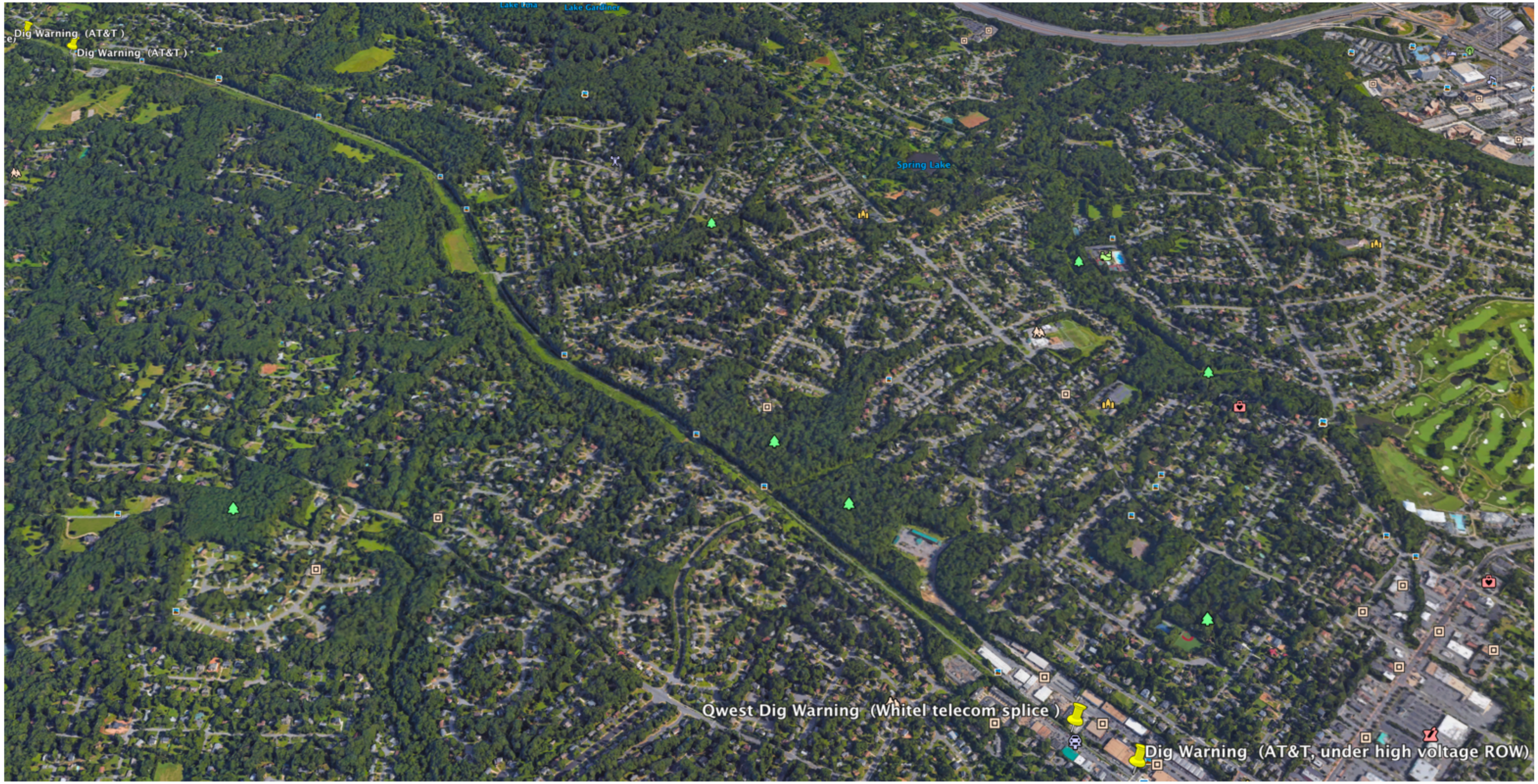
- Users may mislabel meta-data:
  - Wrong provider, wrong type
- Or even not infrastructure:
  - Mistake sewer for a telecom manhole
  - Mistake red dig markings for telecom
  - Mistake electrical vault for telecom
- Some tags are much more useful than others:

**No provider, no type, unclear direction**

# Inferential Power

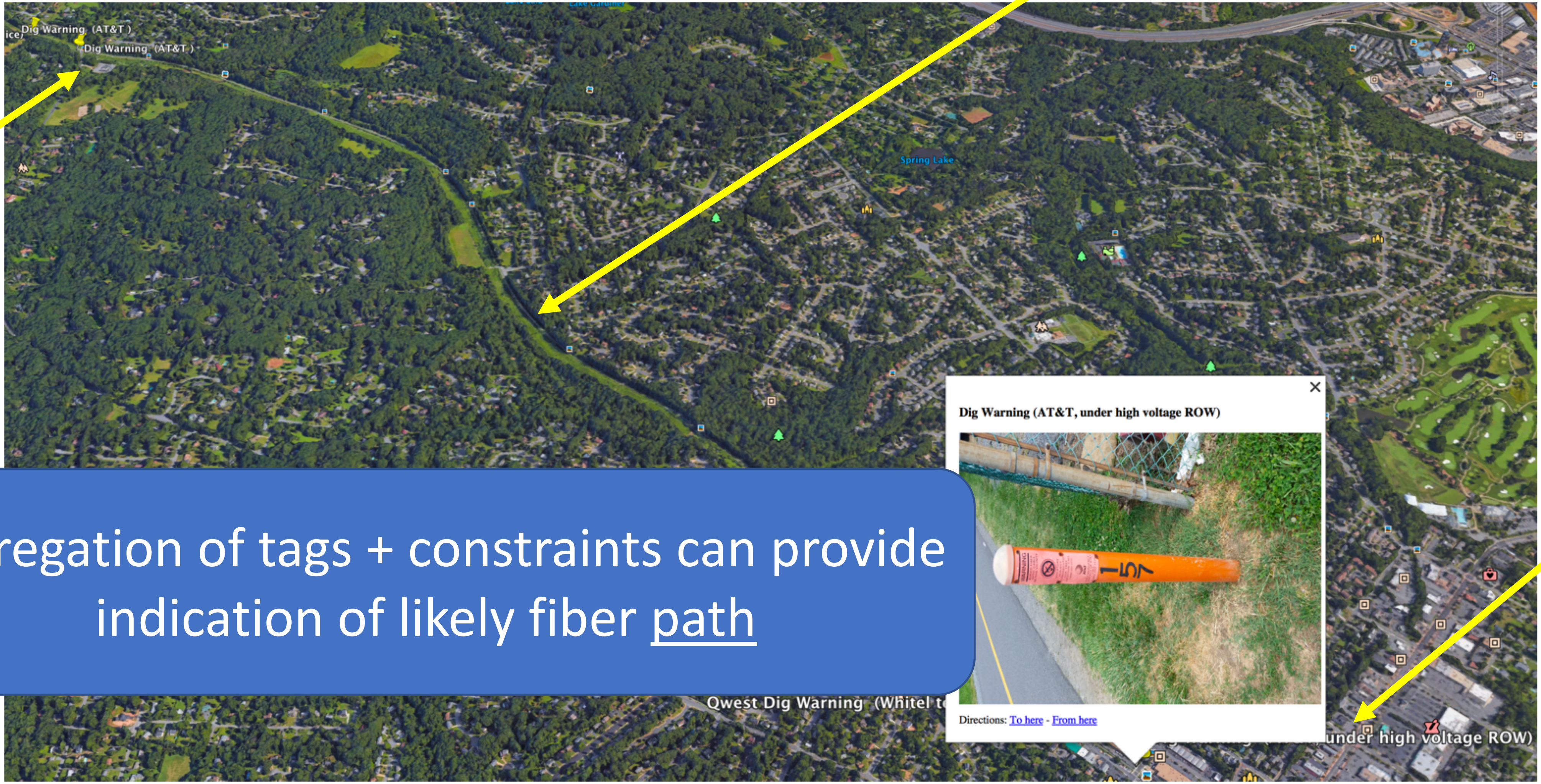
- Inferring likely points of infrastructure
    - “Connecting the dots”
    - Include physical constraints, e.g., transportation infrastructure, mountains, right-of-ways
- Data collected thus far suggests that there are lots of possible inferences
- Some case-studies:

# Example: Inferring Path



Lake Una
Lake Gardiner
Dig Warning (AT&T )
Dig Warning (AT&T )
Spring Lake
Qwest Dig Warning (Whitel telecom splice )
Dig Warning (AT&T, under high voltage ROW)

# Example: Inferring Path


Dig Warning (AT&T)
Dig Warning (AT&T)
Spring Lake
Dig Warning (AT&T, under high voltage ROW)
Directions: To here - From here
Qwest Dig Warning (Whitel t
under high voltage ROW)

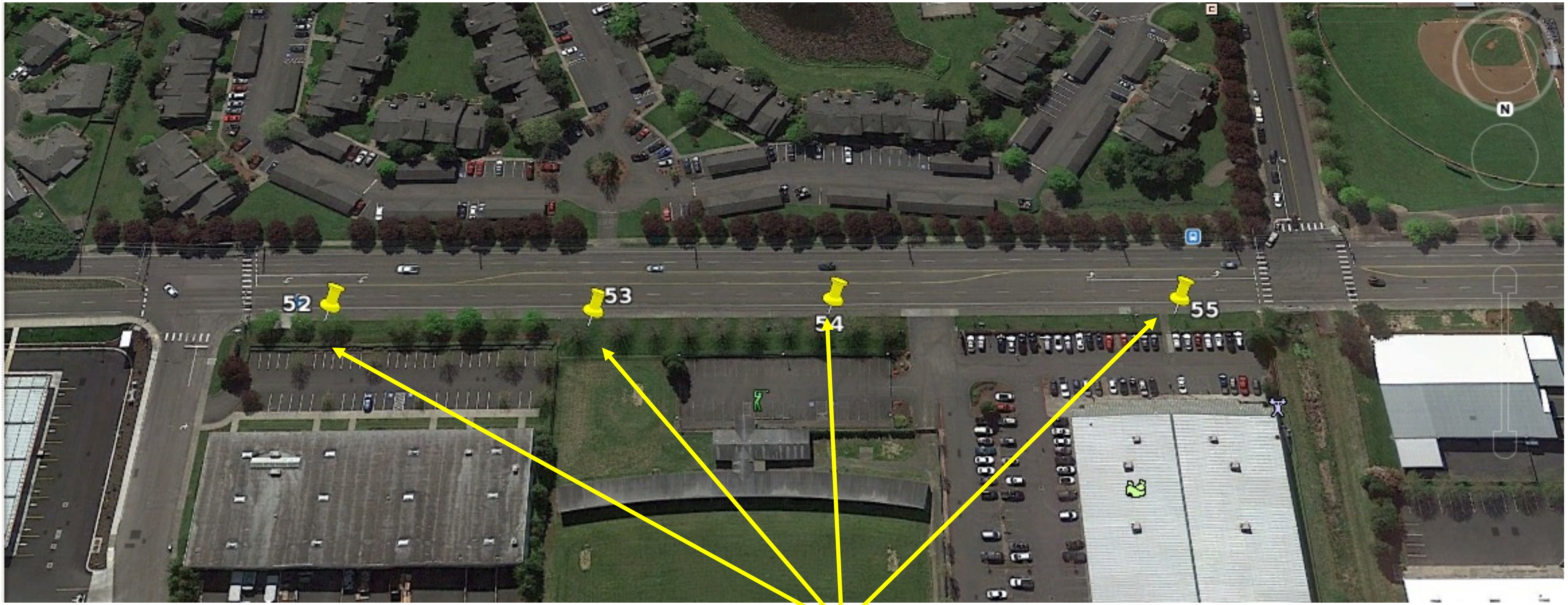
**Bike path (old railway ROW)**

**AT&T Dig Marker**

**AT&T Dig Marker**

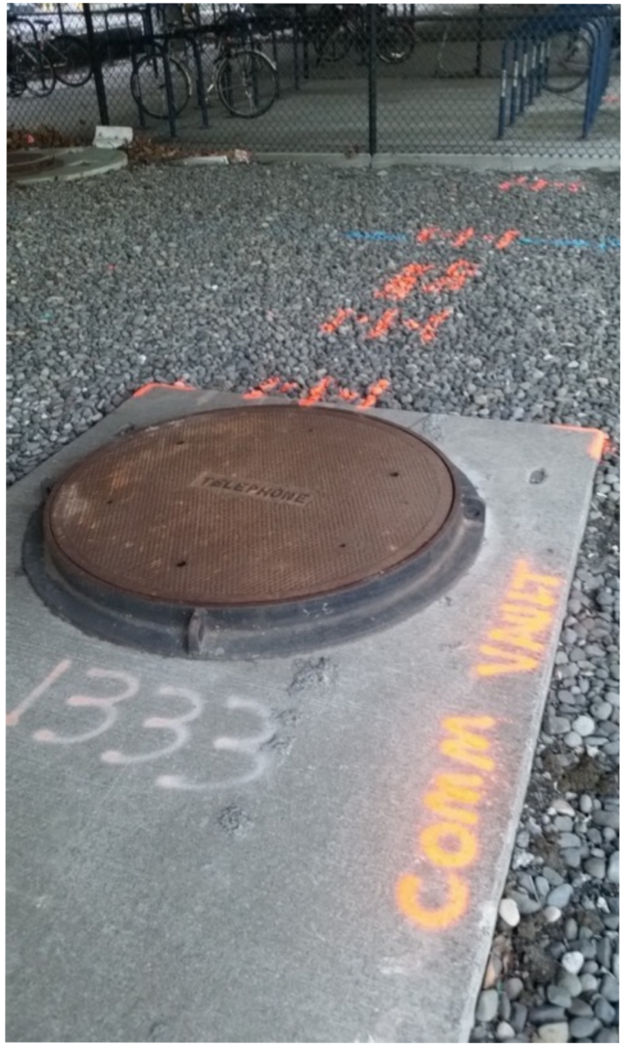
Aggregation of tags + constraints can provide indication of likely fiber path

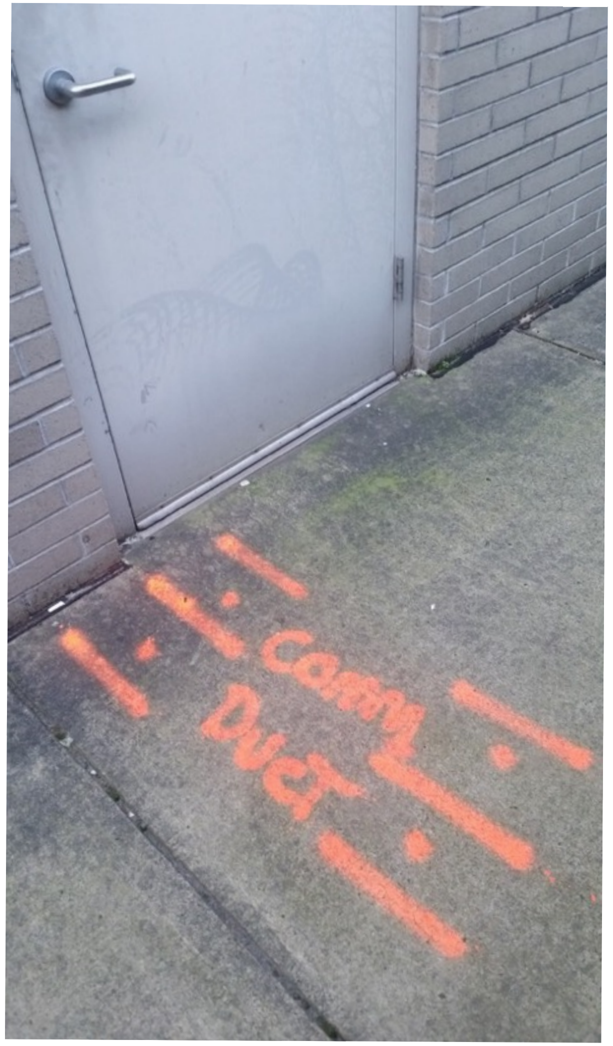
# Example: Dig Warnings + Road



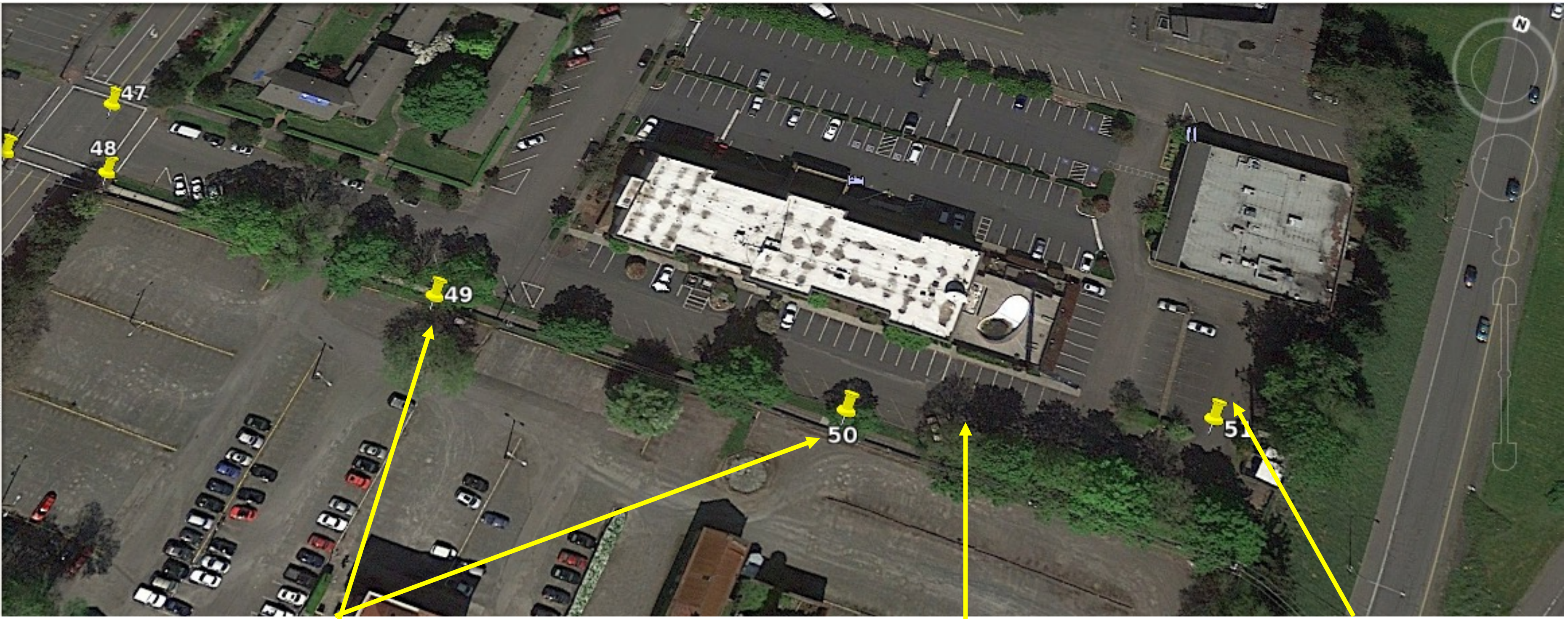
**All 4 registered to same provider**

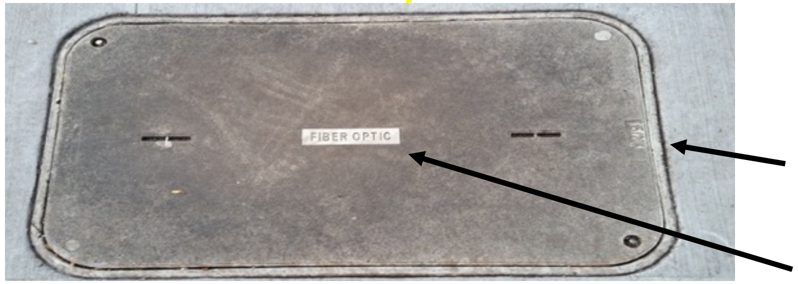
# Example: Duct + Features





# Example: Access Points + Structure





Dead-End Street

**"T15/20k"**

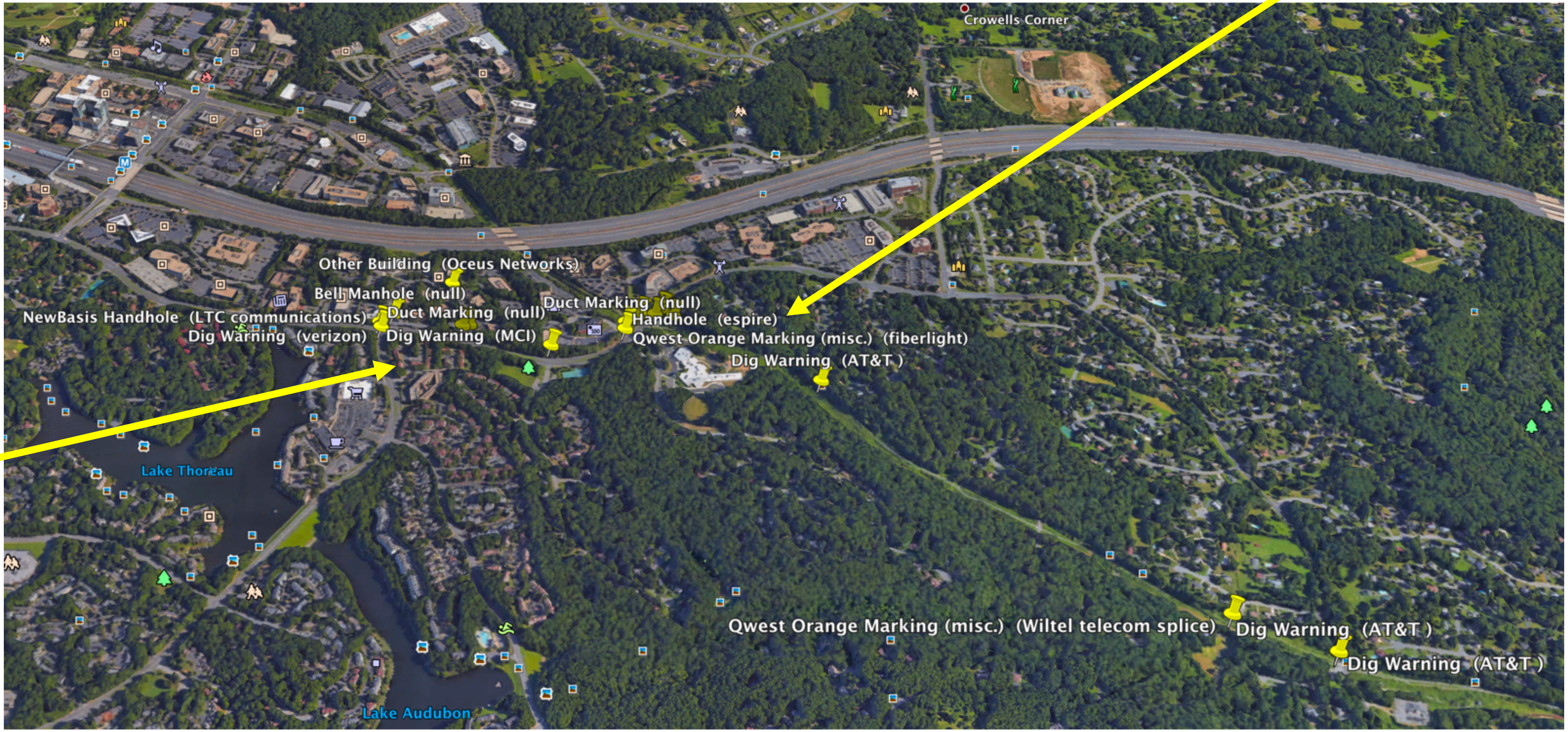
**"Fiber Optic"**

**Cell Tower**

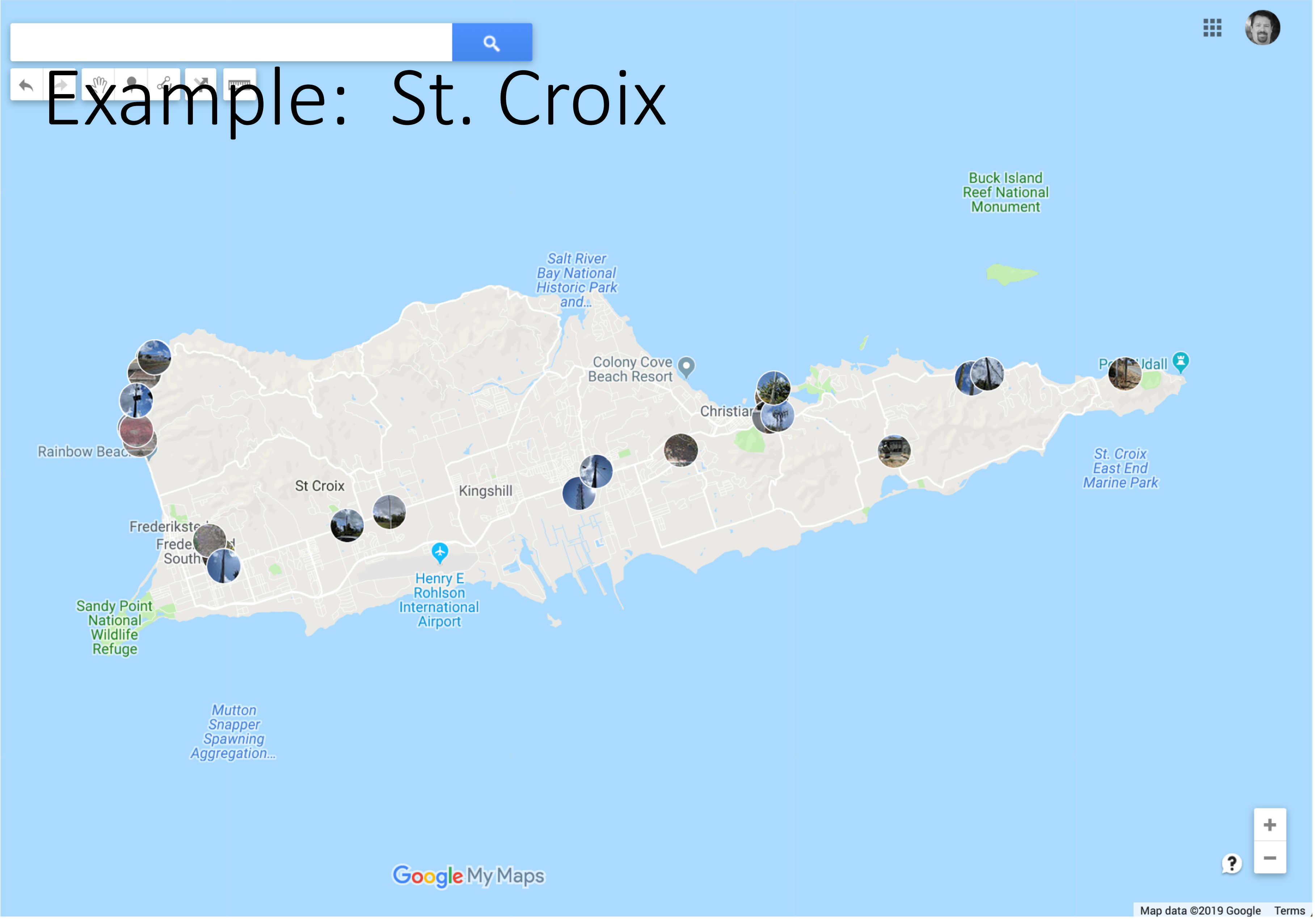
# Example: Shared Infrastructure

**Markers suggest shared infrastructure**

**Large density of infrastructure**



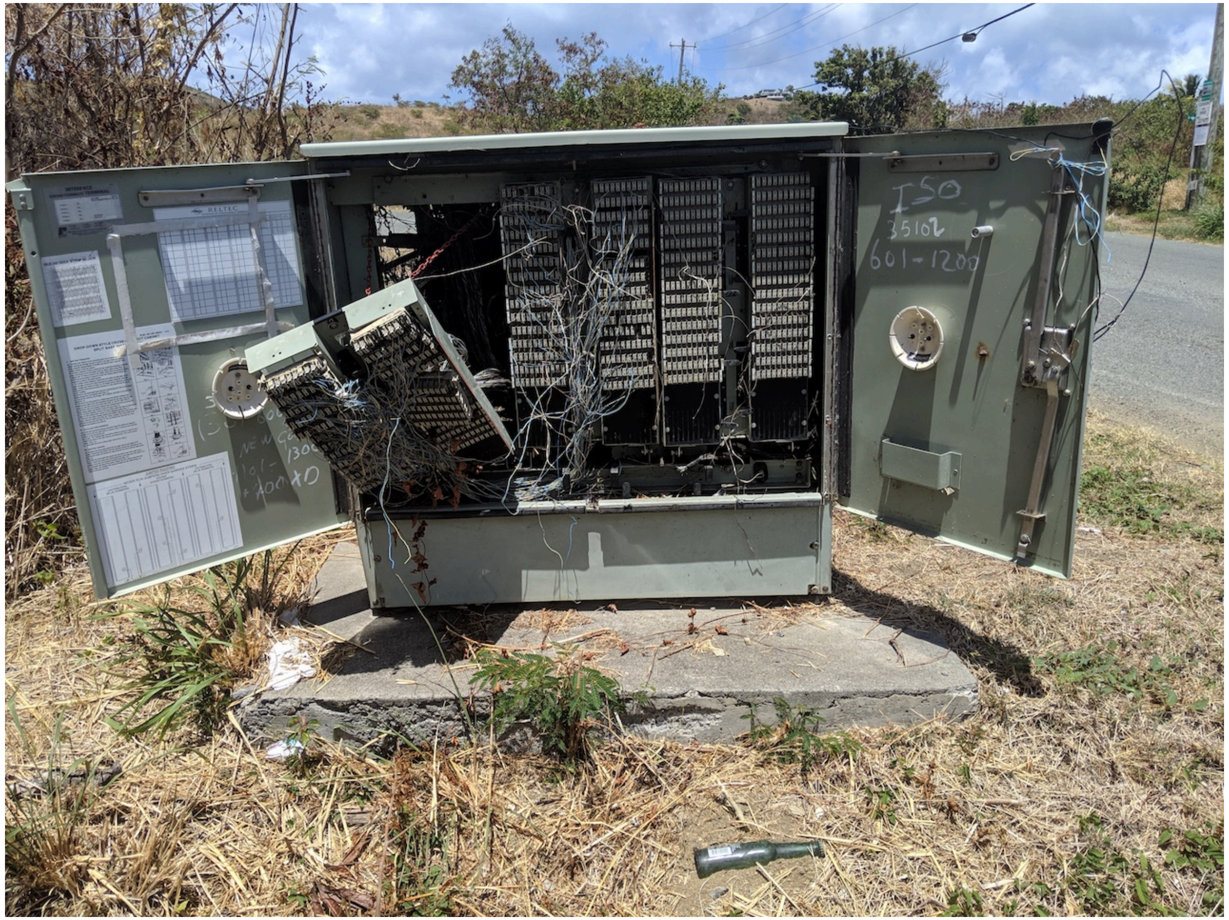
# Example: St. Croix



Buck Island Reef National Monument
Salt River Bay National Historic Park and...
Colony Cove Beach Resort
Christiar
Rainbow Beac
St Croix
Kingshill
Frederikste
Frede
South
Sandy Point National Wildlife Refuge
Henry E Rohlson International Airport
St. Croix East End Marine Park
Mutton Snapper Spawning Aggregation...
Google My Maps
Map data ©2019 Google Terms

- Minimal labeling
- No dig-marking program
- Most infrastructure above ground

# Example: State of infrastructure



Southside Rd, St. Croix, USVI

Butler Bay, St. Croix, USVI

# Preliminary deployments

- Available to anyone to beta-test
- In use as part of USVI disaster-recovery effort

- Actively bug-squashing and refining UI based on feedback from current users
- Significant maintenance to just keep pace with Android/IOS version and API changes

Rosecrans St, San Diego

# Open Questions:

- Capturing above-ground installations
- Integrating with OpenStreet Maps
- Correlation with pre-existing topology databases
  - Also helpful to seed tagging
- Incenting users
  - Bounties?
  - Leaderboards?
  - Point system?
- Sharing data
- Automated vision recognition

# Security Impact

- “We don’t want attackers to know where is critical infrastructure /weak points!!”
  - This is security through obscurity argument (and, attackers already know)
- Politico, Jun 1, 2017:

> In the throes of the 2016 campaign, the FBI found itself with an escalating problem: Russian diplomats, whose travel was supposed to be tracked by the State Department, were going missing.
>
> The diplomats, widely assumed to be intelligence operatives, would eventually turn up in odd places, often in middle-of-nowhere USA. One was found on a beach, nowhere near where he was supposed to be. In one particularly bizarre case, relayed by a U.S. intelligence official, another turned up wandering around in the middle of the desert. Interestingly, both seemed to be lingering where underground fiber-optic cables tend to run.
>
> According to another U.S. intelligence official, “They find these guys driving around in circles in Kansas. It’s a pretty aggressive effort.”

# Summary

- net.tagger app for crowdsourced physical infrastructure discovery
- Complementary to existing techniques
- Initial analysis demonstrates possible powerful inferences
- Looking for your participation and feedback!

https://cmand.org/tagger/