



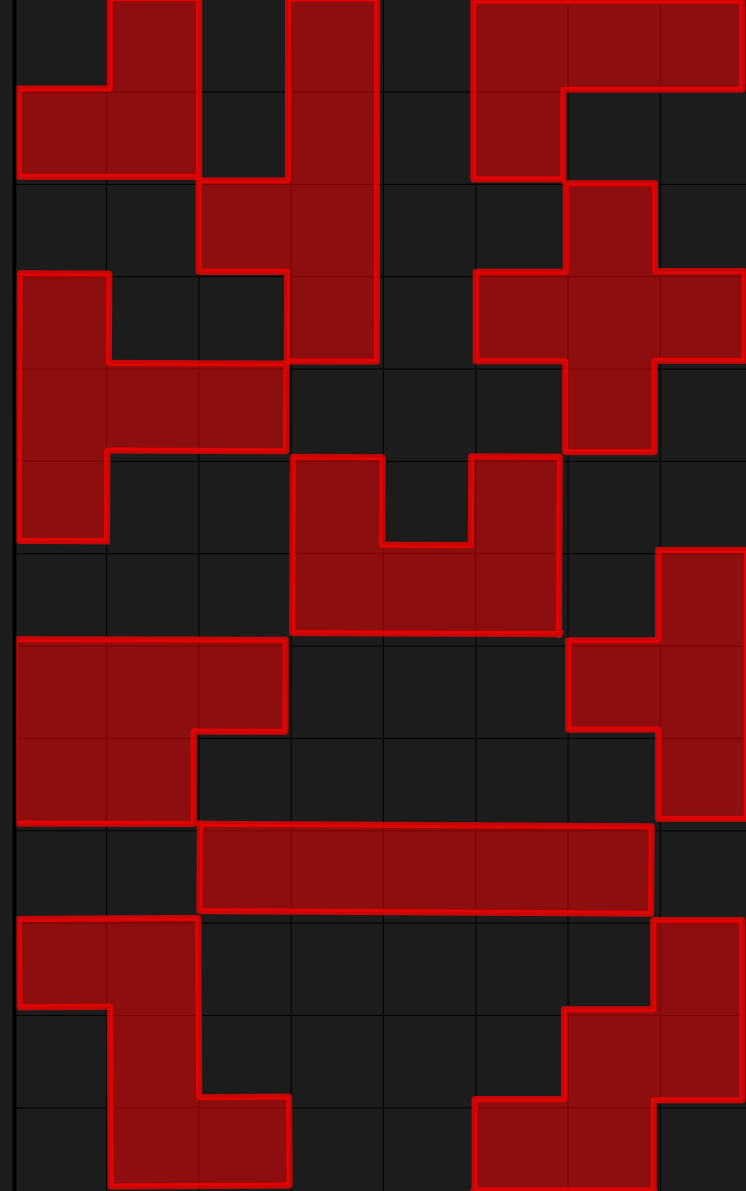
Eyes From The Street

Today

- ♦ Reading discussion
- ♦ Case Study: Dragnets
- ♦ Field trip: Warwalk!(6:40pm)
- ♦ Tools for Network Analysis (7pm)
- ♦ Project discussions

Readings

- ♦ AIUSA Decode Surveillance NYC
- ♦ We Hunted Hidden Police Signals at the DNC
 - ♦ Stingray/IMSI Catchers
 - ♦ Downgrade attack (ex 5G to 2G)
 - ♦ Easier decryption





Dragnets

Wide set of measures or points of collection for law enforcement investigation

- ◆ **Stop and Frisk/Terry Stop**

- ◆ On/Off, Multiple Lawsuits, Adams Approved, overwhelmingly racist in execution, LAPD pioneers in 1930s

- ◆ **Geofence/Reverse Search Warrants**

- ◆ Google Sensorvault + historical geo data

- ◆ **DNA Dragnets**

- ◆ Gathered secretly or by request (ENY 500+)

- ◆ Office of Medical Examiner's Permanent Database (65k+)

- ◆ Faulty (Lukis Anderson)

- ◆ Third-party companies + relative gene matching

- ◆ **ALPRs, Stringrays, FRT video network, ...?**

Warwalking

- ◆ Dynamically capturing network information across space (WiFi, towers, other networked devices)
- ◆ Google StreetView Controversy



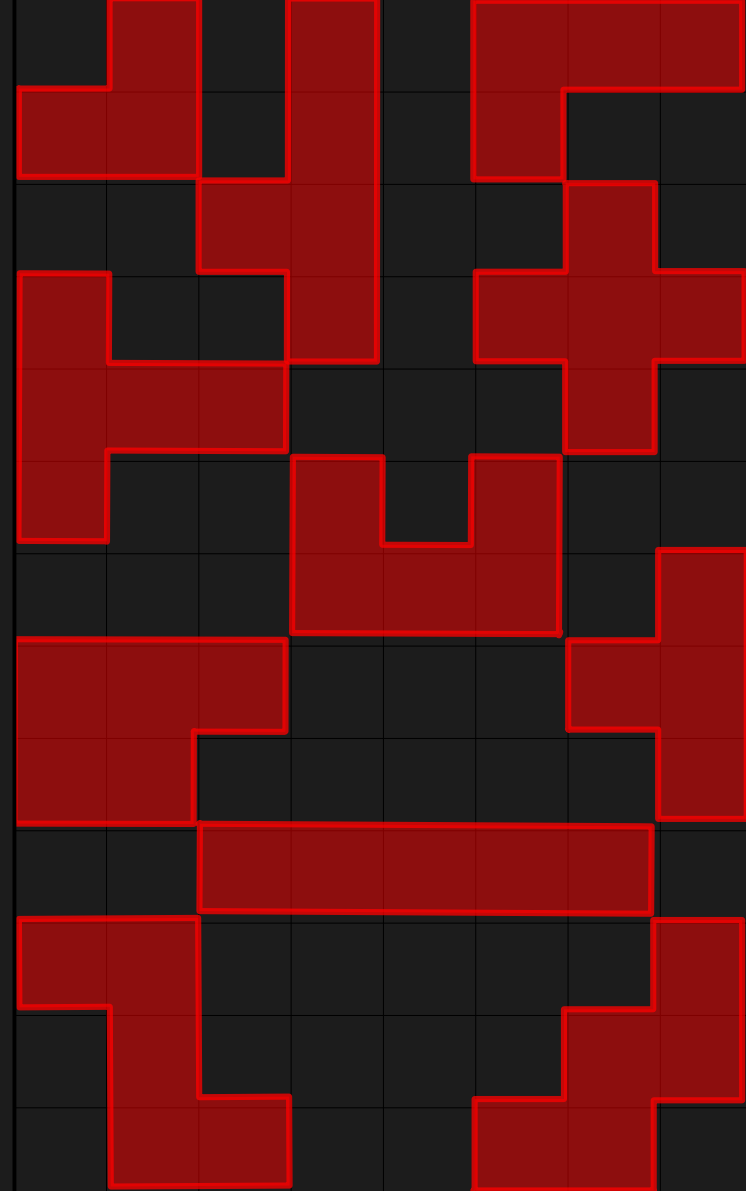
Let's Warwalk

- ◆Buddy up!
- ◆Download WiGLE WiFi Wardriving on Android or open network settings on Apple
- ◆Pick a nearby place (ex: gov't buildings, popular action spot, police station, etc) or routes
- ◆Observe network info on the way to and at the site
- ◆Keep track of time!
- ◆Look at the manufacturer names
- ◆If networks are named or not
- ◆Make note of any towers
- ◆Commonalities in MAC addresses
- ◆Screenshot anything of note!

Be back by 7pm pls!

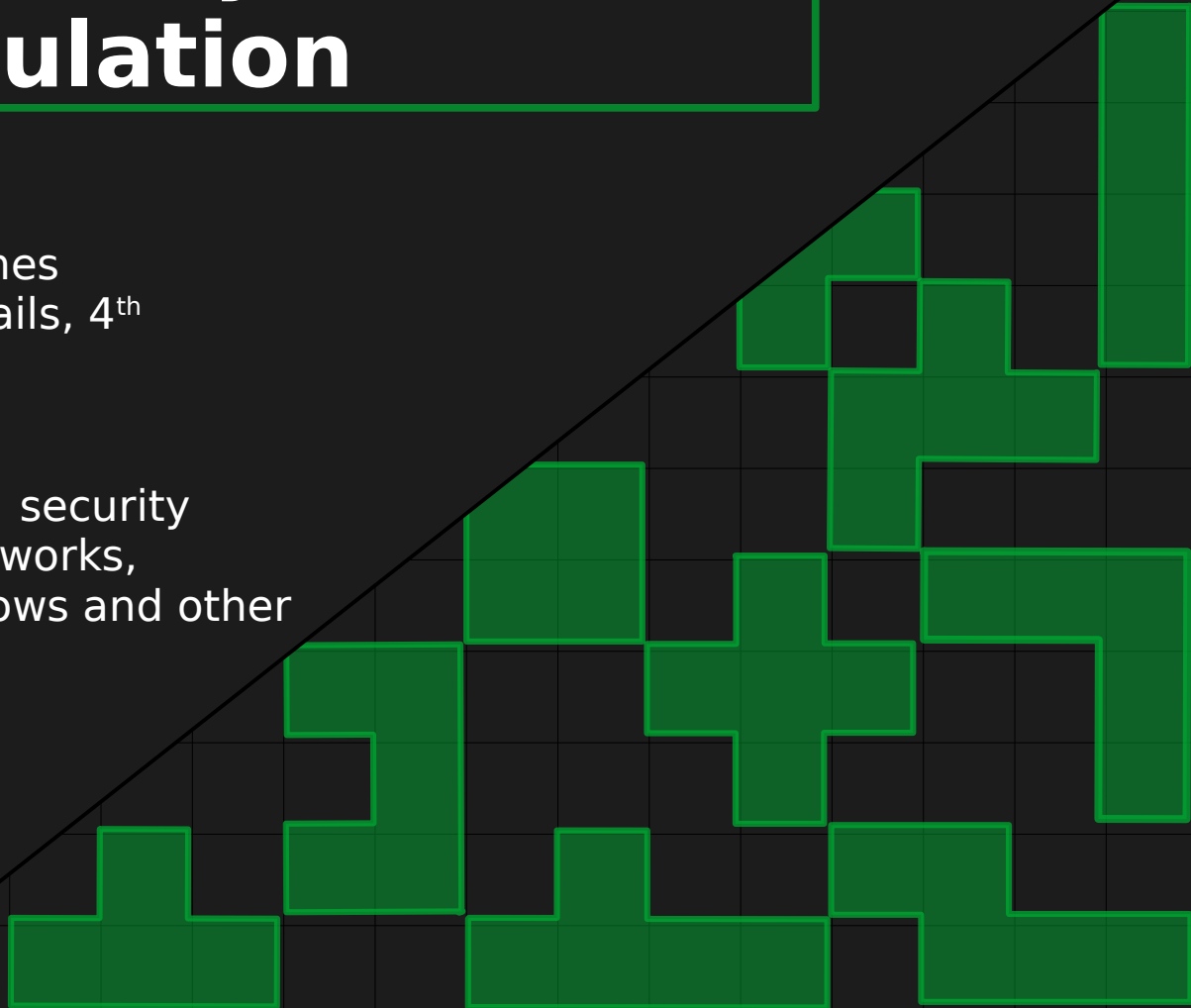
Unpack the net

- ♦ Did you find any towers?
- ♦ Rise in unnamed networks near certain areas?
- ♦ Any patterns in manufacture information or MAC addresses near those zones?
- ♦ Suspicious or funny network names?



Network Analysis + Manipulation

- ◆ Surveillance implications
 - ◆ TPMS, hard to detect (sometimes impossible), little legal guardrails, 4th amendment
- ◆ Accountability possibilities
 - ◆ Secret infrastructure spotting, security vulnerabilities on personal networks, transparency of information flows and other network connections

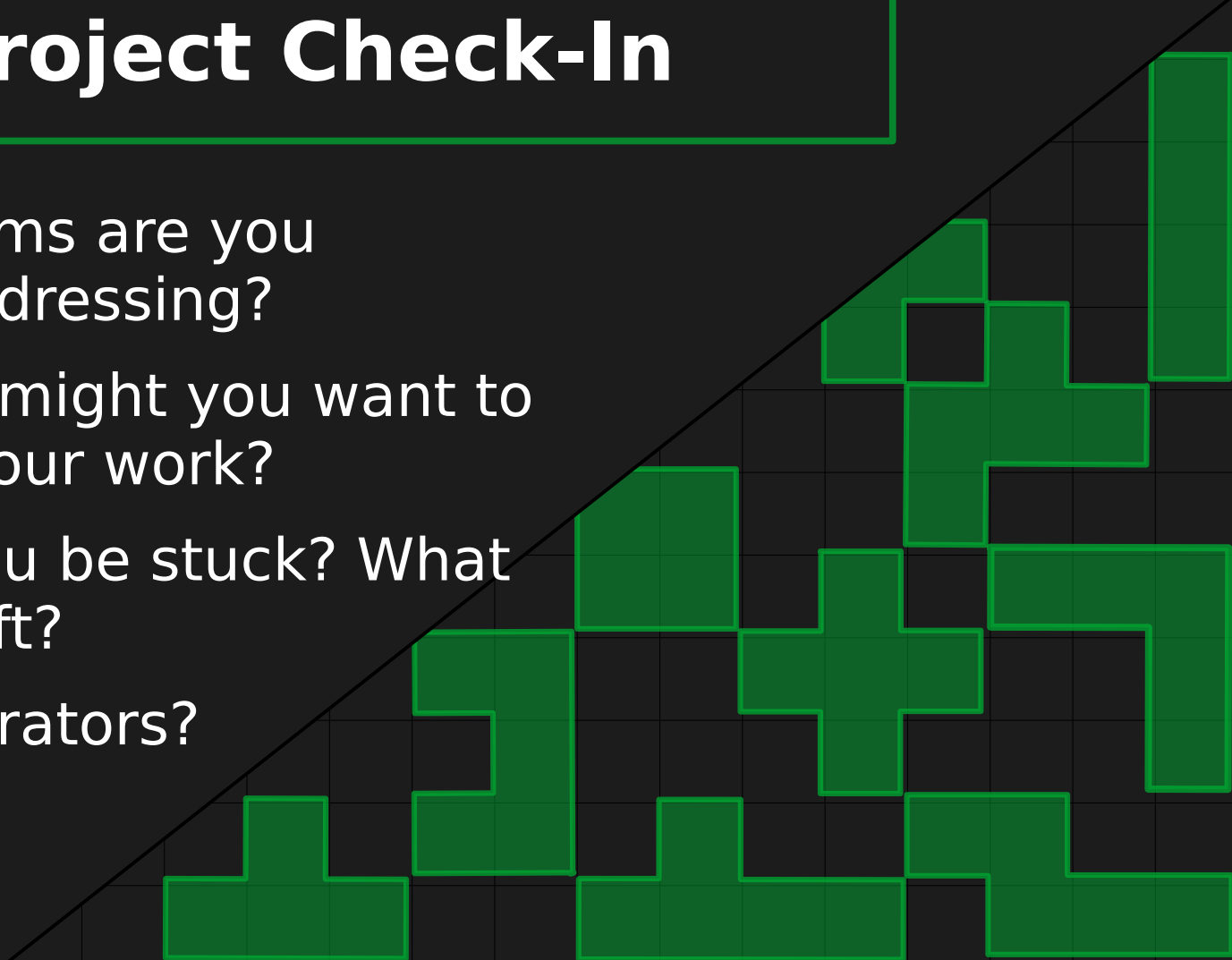




Tools for Network Analysis

- ♦ [Wireshark](#) / packet analysis
- ♦ [mitmproxy](#) / transparent proxy
 - ♦ View decrypted traffic locally or through proxy on a device you control
- ♦ [RFParty](#) / bluetooth stumbler
- ♦ [Aircrack ng](#)
- ♦ [Kismet](#)/[Kismac](#)

Final Project Check-In

- ♦ What mechanisms are you interested in addressing?
 - ♦ What mediums might you want to communicate your work?
 - ♦ Where might you be stuck? What decisions are left?
 - ♦ Open to collaborators?
- 



Next week

- ◆ Develop your project a bit more
 - ◆ Specify targets and scope
 - ◆ Identify medium for sharing (even if just for now)
 - ◆ Plot 4/30 presentation(s)

Thank you! Feel free to...

Find our syllabus online: <https://2nd.systems/efts>

Review and add to our class notes:
<https://efts.2nd.systems/notes>

Connect in our Signal group chat:
<https://efts.2nd.systems/chat>

POST Act Updated!