Hunting GPS Jammers

Vlad Gostomelsky

Do Good, Know Evil

BLACKHAT USA 2017

SPIRENT
Federal Systems

SPIRENT

Vlad Gostomelsky
SecurityLabs

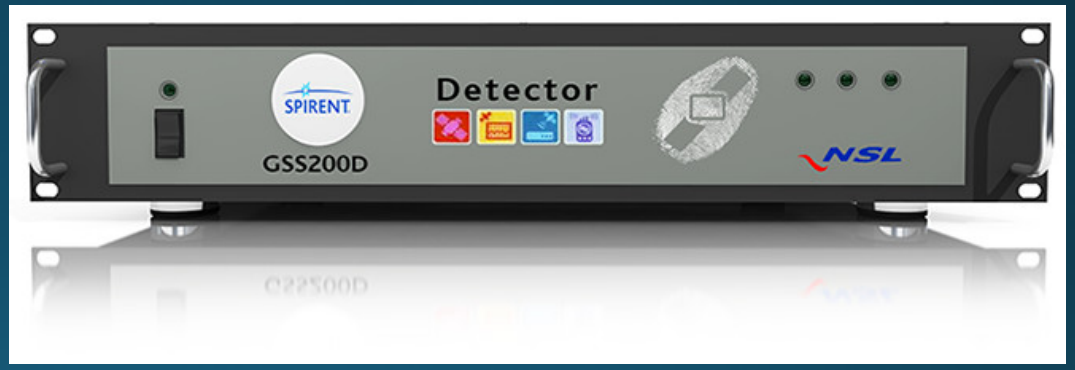
Hunting GPS Jammers

Vlad Gostomelsky

- Security Researcher
- Penetration Tester
- Radio
- Satellite
- SCADA
- Weapons Systems
- Mass Casualty

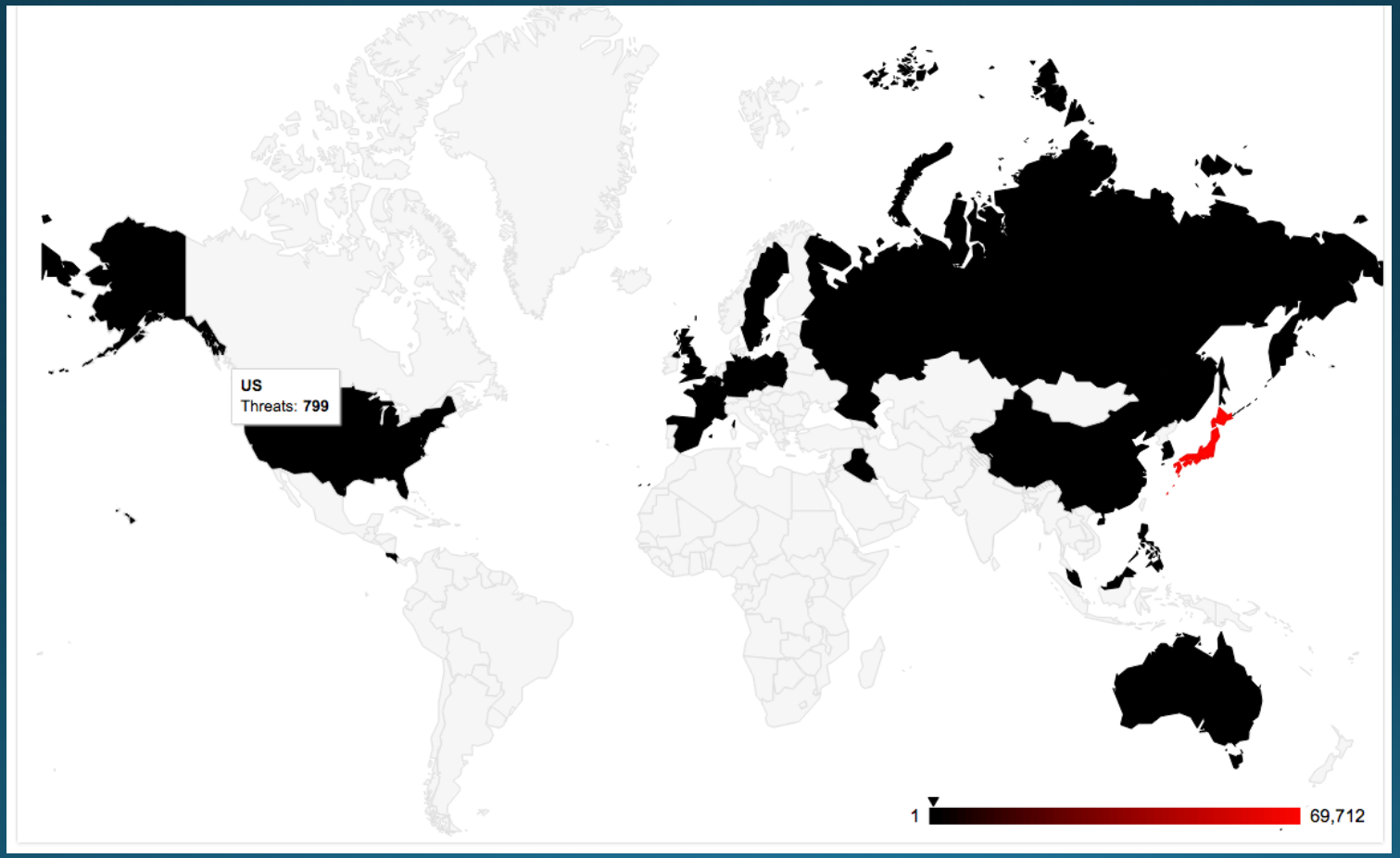
Beginning

- GPS Jamming detector demo



- Data highly sanitized
- Limited sensor placement
- Data from highly sensitive installations not included

US Threats



Global Threats

Jamming Types

- RF Jamming
- L1 (1575.42 MHz)
- L2 (1227.60 MHz)

- Protocol Jamming
- Accuracy Degradation
- Enhanced Accuracy
- Location Spoofing

Top Offenders

- Employer Vehicles
  - Off-hours
- Quad Flyers
  - Location Restrictions
- Advanced Threats
  - Sensitive Locations
  - L1 spoofing
  - L2 jamming
- Truckers
  - Toll Fraud
- A*holes
  - High Power
  - Wideband
- law enforcement

Laws

- **Federal law** prohibits the marketing, sale, or use of a transmitter (e.g., a jammer) designed to block, jam, or interfere with wireless communications. See Communications Act of 1934, as amended, 47 U.S.C. §§ 301, 302a(b), 333.
- Section 301 of the Communications Act: "No person shall use or operate any apparatus for the transmission of energy or communications or signals by radio…except under and in accordance with [the Communications] Act and with a license in that behalf granted under the provisions of this Act." 47 U.S.C. § 301.
- Section 302(b) of the Communications Act: "No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section." 47 U.S.C. § 302a(b).
- Section 333 of the Communications Act: "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under [the Communications] Act or operated by the United States Government." 47 U.S.C. § 333.
- **Jammers cannot be marketed or operated in the United States except in the very limited context of authorized, official use by the federal government.**

Consequences

- The unlawful use of a jammer is a criminal offense and can result in various sanctions, including a jail sentence. More specifically, the unlawful marketing, sale, or operation of cell phone, GPS, or other signal jammers in the U.S. can result in:
- significant fines (we call them "monetary forfeitures") – up to $16,000 for each violation or each day of a continuing violation, and as high as $112,500 for any single act;
- government seizure of the illegal equipment; and
- criminal penalties including imprisonment. See 47 U.S.C. §§ 401, 501, 503, 510; 47 C.F.R. § 1.80(b)(3).
- The FCC has taken action against various individuals and business entities for unlawfully operating and marketing jammers. You can find more information on jammer enforcement at www.fcc.gov/encyclopedia/jammer-enforcement.

Tools of the Trade

- GPS Jamming Detector
- Stalker

GPS Jamming Detector

- GSS100D
- GNSS Multi-Frequency Interference Detection and Analysis

Stalker 1.0

- 4 Microcomputers
- Power Distribution Board
- Ubertooth
- Cheap SDR x2
- WiFi dongle x2
- BladeRF
- GPS
- GoogleFi USB Dongle*
- Golf Cart Batteries
- Switch

- Host 1
  - Ubertooth
  - GPS
- Host 2
  - SDR
  - WiFi 2.4GHz
  - 4G Dongle
- Host 3
  - SDR
  - WiFi 5.8GHz
- Host 4
  - BladeRF

Cheap SDR

SDR1

- TPMS

SDR2

- VHF

Ubertooth

- BD_ADDR of the vehicle headunit
- BD_ADDR of the cellphone(s)
- Accessories
- Health wearables ;-)

WiFi Dongle

- 2.4Ghz
- 5.8Ghz
- Sniffing WiFi Association Frames
- Jagger/yes-man proxy (modified)

BladeRF

- Cellphone tower associations
- Cellphone EINs
- Similar concept to CreepyDOL but a lot of improvements

- It's not eavesdropping, it's just metadata ☺


EPA
TEAM
AIRCON
PELICAN
1650 CASE

Stalker 2.0

- 4 Microcomputers
- Power Distribution Board
- Ubertooth
- Cheap SDR x3
- WiFi dongle
- HackRF
- GPS x2
- Encrypted Storage
- GoogleFi USB Dongle*
- Golf Cart Batteries

- Host 1
  - Ubertooth
  - GPS
- Host 2
  - SDR
  - WiFi 2.4GHz and 5.8ghz
- Host 3
  - SDR
  - Encrypted Storage
  - 4G Dongle
- Host 4
  - HackRF
  - GPS

Switch Elimination

- Heat
- Size
- Power
- Needless complications

BladeRF to HackRF

- Power considerations
- $ of loss
- Overkill for listen only

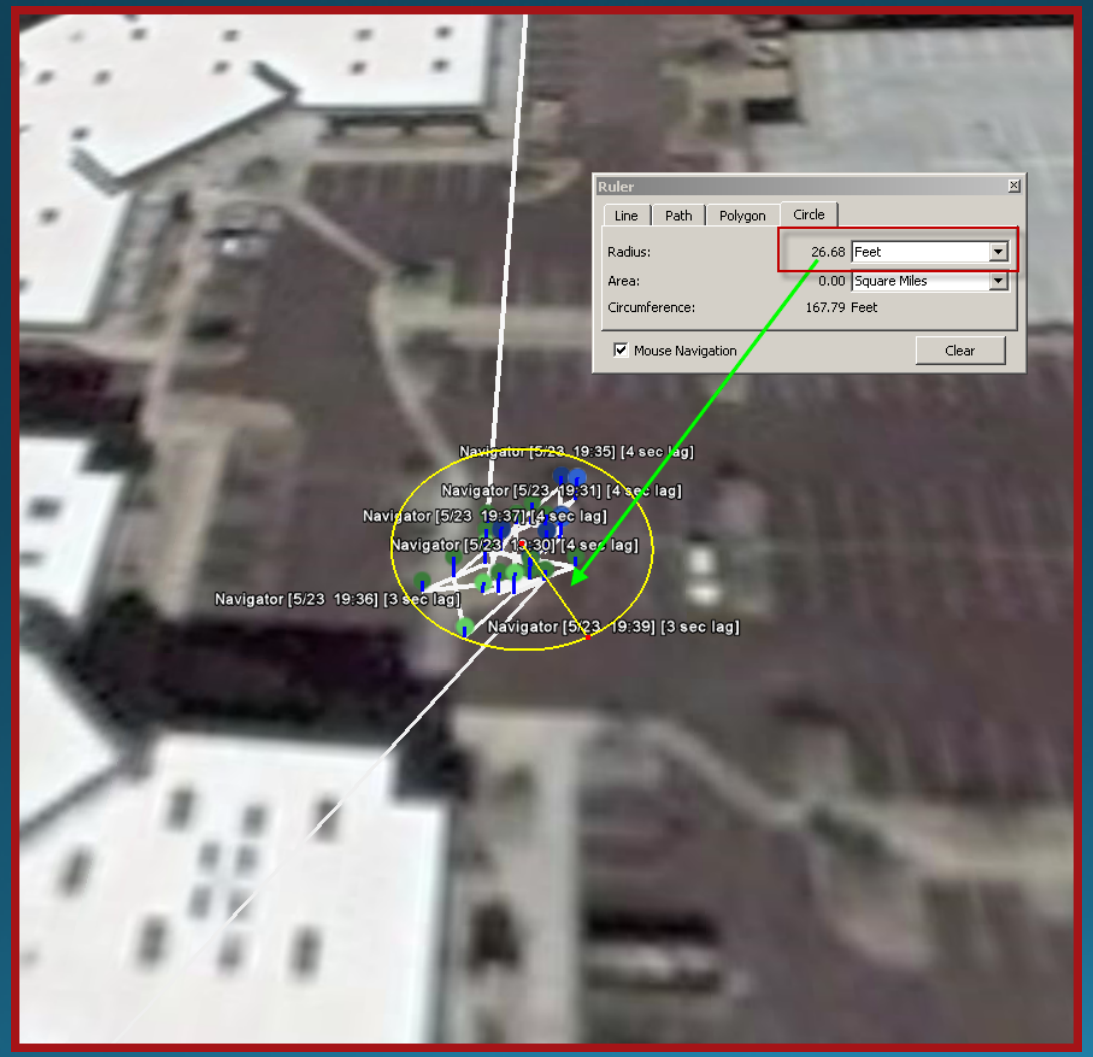
Encrypted Storage

- Selective Logging
- Rolling buffer
- ~2min in memory
- GSS100D trips alert write to USB
- FIPS 140-3

1 GPS -> 2 GPS

- Better measurement of GPS drift
- Data Integrity

GPS Drift


Ruler
Line
Path
Polygon
Circle
Radius:
26.68
Feet
Area:
0.00
Square Miles
Circumference:
167.79 Feet
Mouse Navigation
Clear
Navigator [5/23 19:35] [4 sec lag]
Navigator [5/23 19:31] [4 sec lag]
Navigator [5/23 19:37] [4 sec lag]
Navigator [5/23 19:30] [4 sec lag]
Navigator [5/23 19:36] [3 sec lag]
Navigator [5/23 19:39] [3 sec lag]

Other Improvements

- RF Chokes on every cable
- RF Shielding
- RF Shielding
- Bandpass filters
- Amphenol connectors
- Better antennas

Quadcopters in a Gym

- Washington DC
- stop calling them drones

Work Van

- Cigarette lighter plug unit

Apartment Building

- GPS Jammer
- Cellphone Jammer

- 4 antennas observed
- Intentions unknown
- *Investigation continues

Undercover officer

NSA Playset!

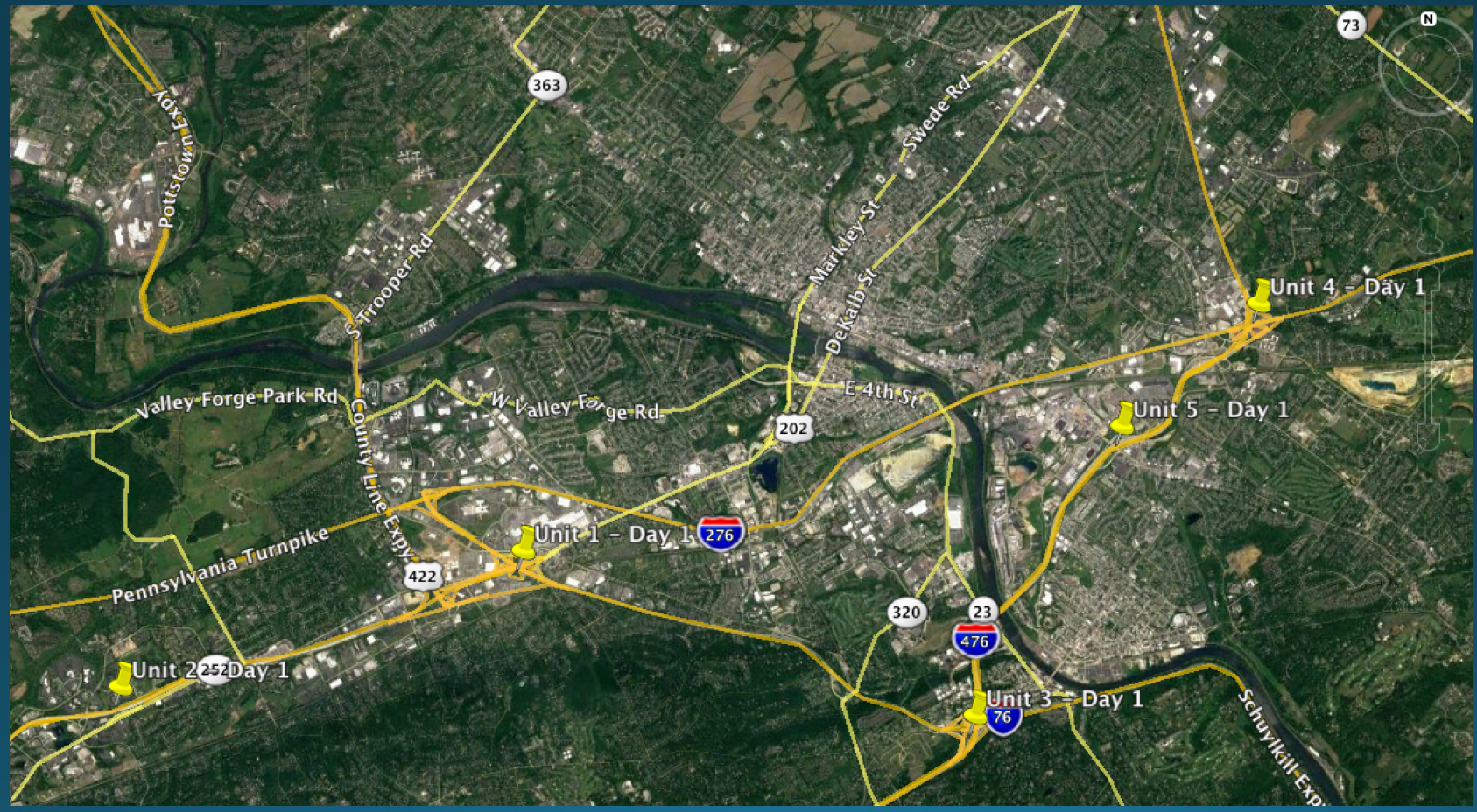
- Github

Lets Go Hunting!

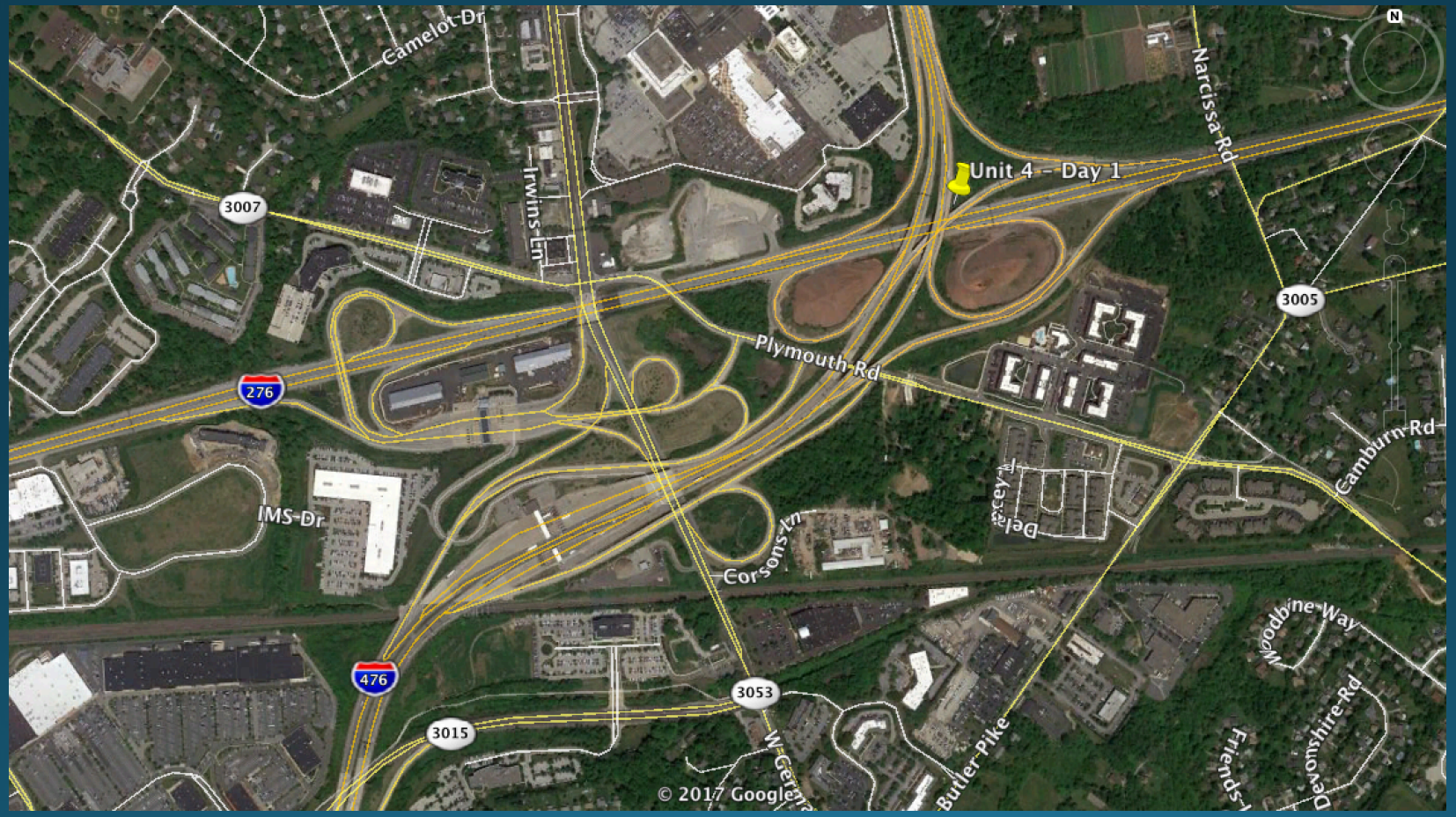
Inventory

- 5 Units
- Targeting 1 geographic area at a time
- Caterpillar search

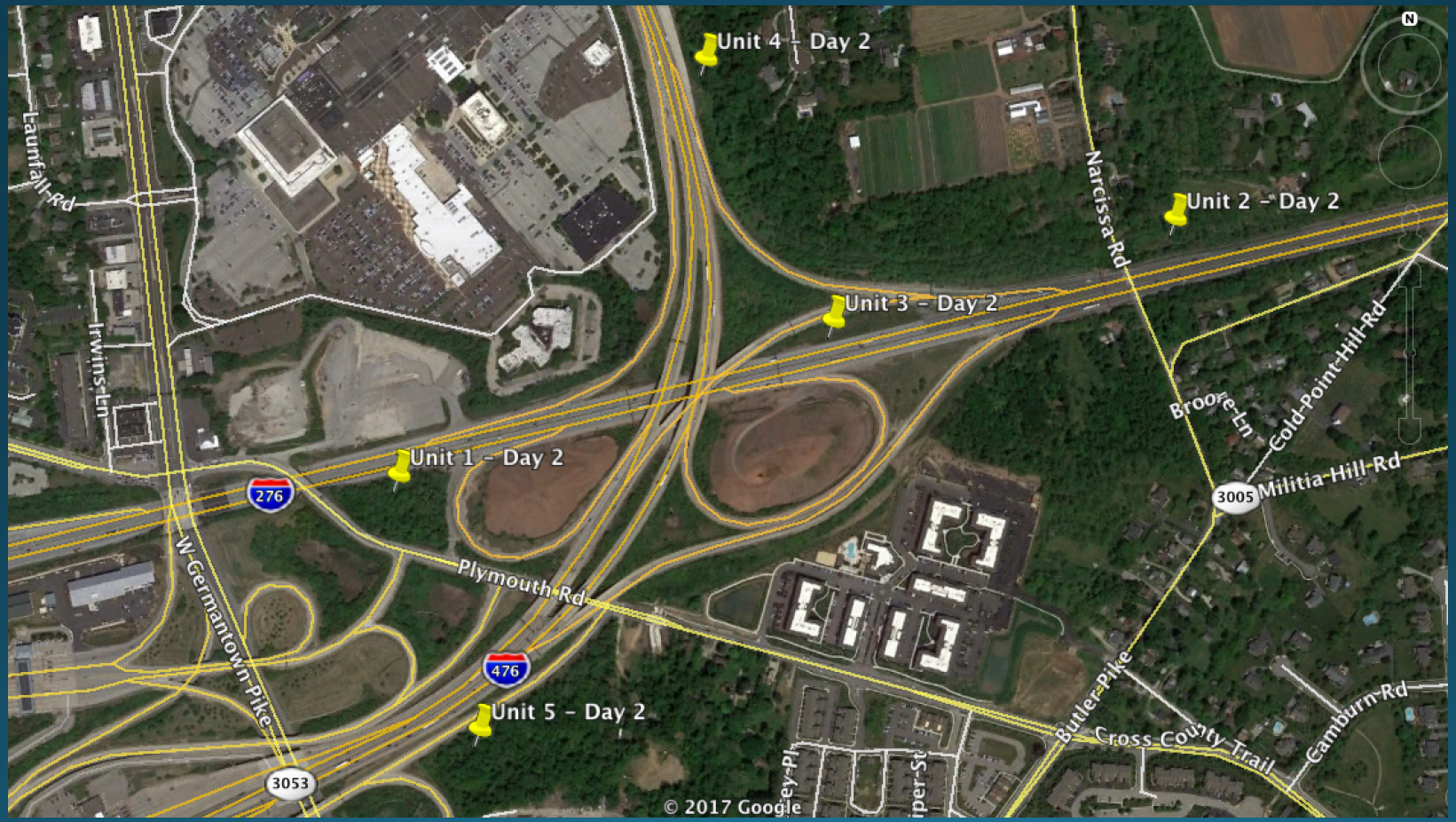
Day 1


Unit 4 – Day 1
Unit 5 – Day 1
Unit 1 – Day 1
Unit 2 – Day 1
Unit 3 – Day 1
Valley Forge Park Rd
W Valley Forge Rd
E 4th St
Pennsylvania Turnpike
Schuylkill Exp
363
202
422
276
320
476
76
73

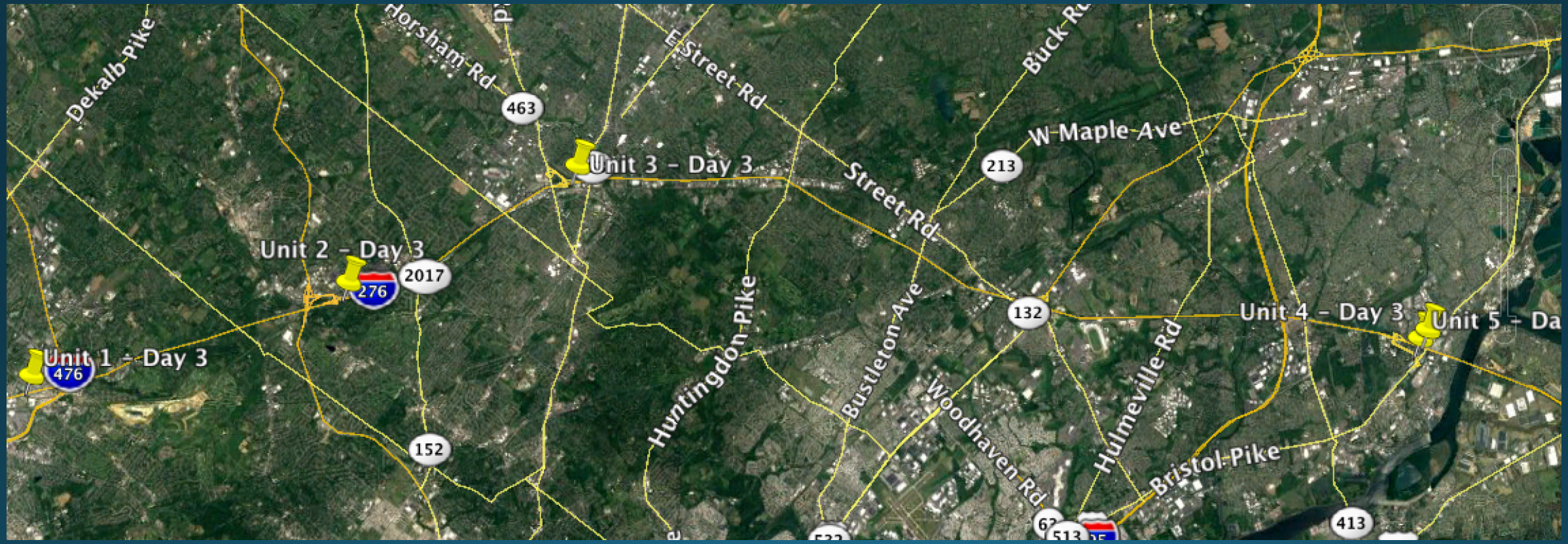
Success!


Camelot Dr
Irwins Ln
Unit 4 - Day 1
Narcissa Rd
3007
3005
Plymouth Rd
276
Cambum Rd
IMS Dr
Corsons Ln
476
3053
3015
Butler Pike
Devonshire Rd
© 2017 Google

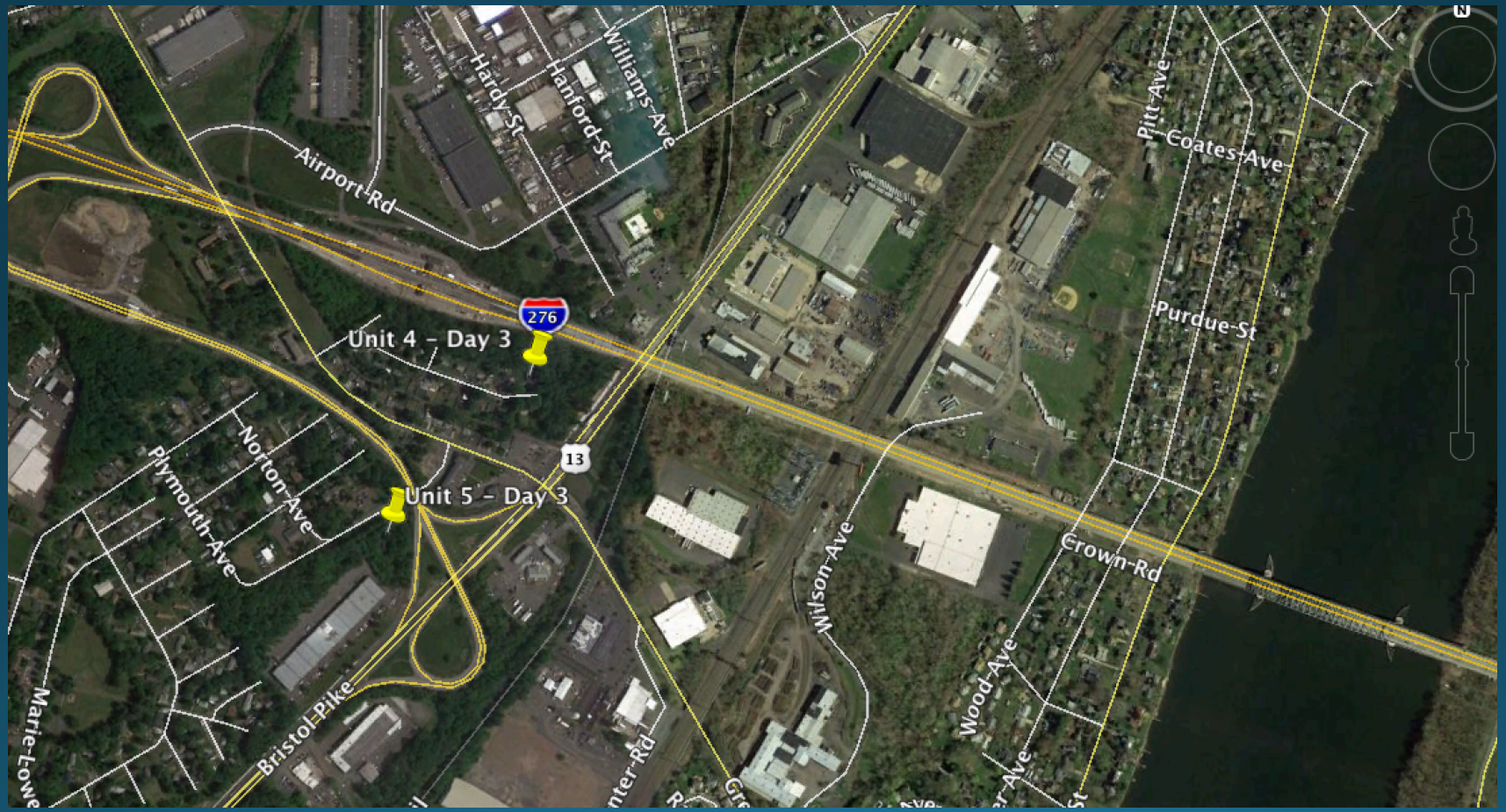
Day 2


Unit 4 - Day 2
Unit 2 - Day 2
Unit 3 - Day 2
Unit 1 - Day 2
Unit 5 - Day 2
Laurfall Rd
Irvins Ln
Narcissa Rd
Broore Ln
Gold Point Hill Rd
Militia Hill Rd
3005
276
476
3053
W Germantown Pike
Plymouth Rd
Butler Pike
Cross County Trail
Gamburn Rd
© 2017 Google

Day 3


Dekalb Pike
Horsham Rd
463
E Street Rd
Buck Rd
W Maple Ave
213
Unit 3 - Day 3
Street Rd
Unit 2 - Day 3
2017
276
Huntingdon Pike
Bustleton Ave
132
Unit 4 - Day 3
Unit 5 - Da
Unit 1 - Day 3
476
Woodhaven Rd
Hulmeville Rd
Bristol Pike
152
413

Don’t go to jersey



Day 4


Front St
7th St
Unit 1 - Day 4
River Rd
Cedar L
Delaware Ave
130
Kinkora Rd
Unit 4 - Day 4
Unit 3 - Day 4
660
678
658
276
Unit 2 - Day 4
Unit 5 - Day 4
Bordentown Rd
661
659

Closeup


WHELEN

No

- Dirty vest
- Dirty helmet
- Clipboard
- Pen
- camera

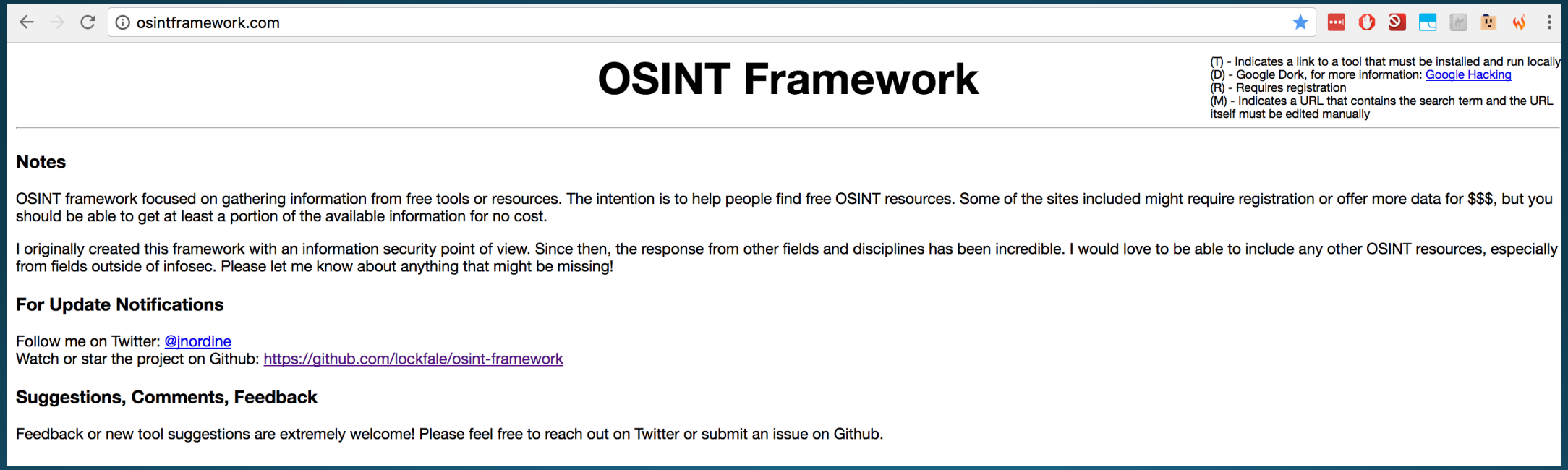
Day x

Gotcha


Unit 1 – gotcha
Unit 5 – gotcha
Unit 2 – gotcha
Unit 4 – gotcha
Unit 3 – Day x
Unit 3 – gotcha

What We know

- TPMS IDs of tires
- Vehicle type (tire pressure between 62PSI and 65PSI) – truck or SUV
- Hardware addresses of 2 cellphones
- Possibly SSID for the house
- Bluetooth mac address


osintframework.com
OSINT Framework
(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually
Notes
OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for $$$, but you should be able to get at least a portion of the available information for no cost.
I originally created this framework with an information security point of view. Since then, the response from other fields and disciplines has been incredible. I would love to be able to include any other OSINT resources, especially from fields outside of infosec. Please let me know about anything that might be missing!
For Update Notifications
Follow me on Twitter: @jnordine
Watch or star the project on Github: https://github.com/lockfale/osint-framework
Suggestions, Comments, Feedback
Feedback or new tool suggestions are extremely welcome! Please feel free to reach out on Twitter or submit an issue on Github.

Break!

- House tax records indicate a woman
- No public information on any males at the residense
- No public hits on marriages
- Photo time
- Google image hit!
- Agency photo from family day!

Observed OpSec

- GPS Jammer always on when engine is on
- Low end phone on until the bridge
- Stops pinging (hard off)
- iPhone 6s pinging ~30min until at the house
- Presumably off
- Onstar and Sirus xm
- Surveillance Detection Route

Next Version of Stalker

- Hardware with less crappy USB bus
- More powerful
- More RAM
- Ability to read EZ pass IDs
- V2V/V2X

Lessons Learned

- RF noise gets in everywhere
- Unlocked cases > locked cases
- $30 golf cart batteries > $700 SDR
- Clean helmet vs dirty helmet
- Google has you

Housekeeping

- All work done on dedicated laptops/hardware

- Wiped with a rag
- Wiped (FIPS 199)
- Wiped with 4lbs of tannerite

Future Work

- Investigate more locations

- Find advanced jamming sources
- pokemon gyms/portal locations?*

- Thank you!

Questions?

Demos at booth #754

blackhatgps@gmail.com

Related Civilian Projects

securitylabs@spirent.com

Related .mil/.gov projects

projects@spirentfederal.com