Detecting Fake 4G Base Stations in Real Time

Cooper Quintin - Senior Security Researcher - EFF Threat Lab

Black Hat USA 2020

Intro

- Cooper Quintin
  - Senior security researcher
  - Has a toddler (dad jokes)
  - Former teenage phone phreak
- EFF
  - Member supported non profit
  - Defending civil liberties
  - 30 years
- Threat lab

Yomna!

None of this research would have been possible without her hard work. This is as much her project as mine.

Twitter: @rival_elf

Actual photo of Yomna

Technology that Targets At Risk People

- Activists, human rights defenders, journalists, domestic abuse victims, immigrants, sex workers, minority groups, political dissidents, etc…
- Goals of this technology
  - Gather intelligence on opposition
  - Spy extraterritorially or illegally
  - Locate and capture
  - Extortion
  - Harass and intimidate
  - Stifle freedom of expression

Jeff Bezos Can Afford a Security Team

Cybersecurity and AV companies care about the types of malware that affects their customers (usually enterprise.)

We get to care about the types of technology the infringe on civil liberties and human rights of at risk people.

This guy is not at risk.

Our Goals

- Protect people
- Broaden our communities` understanding of threats and defenses
- Expose bad actors
- Make better laws

Previous Project

Stalkerware

COALITION AGAINST STALKERWARE

Dark Caracal

What We are Going to Talk About Today

- Cell-site simulators AKA Stingrays or IMSI Catchers
- How they work
- Previous efforts to detect them
- A new method to detect them
- How to fix the problem

Cell Technology Overview

- UE - The phone - User Equipment
- IMSI - International Mobile Subscriber ID - ID for the SIM card
- IMEI - International Mobile Equipment ID - ID for the hardware
- eNodeB - Base station, what the UE is actually communicating with.
- EARFCN - The frequency a UE/EnodeB is transmitting on
- Sector - A specific antenna on the base station

Cell Technology Overview

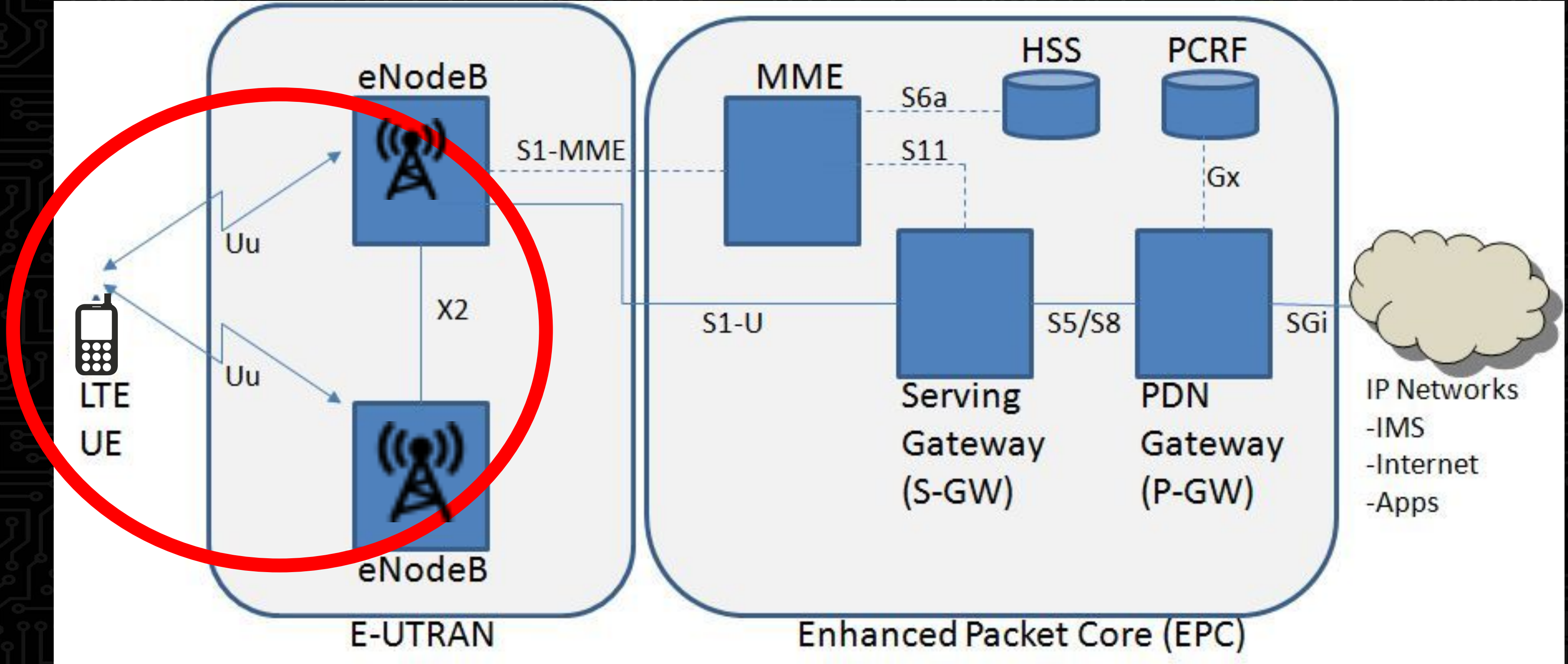
- MIB - Master Information block, broadcast by the enodeb and tells where to find the SIB
- SIB - System information block, contains details about the enodeb
- MCC / MNC / TAC - Mobile Country Code, Mobile Network Code, Tracking Area Code
- PLMN = MCC + MNC, Public Land Mobile Network

Cell Technology Overview

IMSI catcher, Stingray, Hailstorm, fake base station == cell-site simulator (CSS)

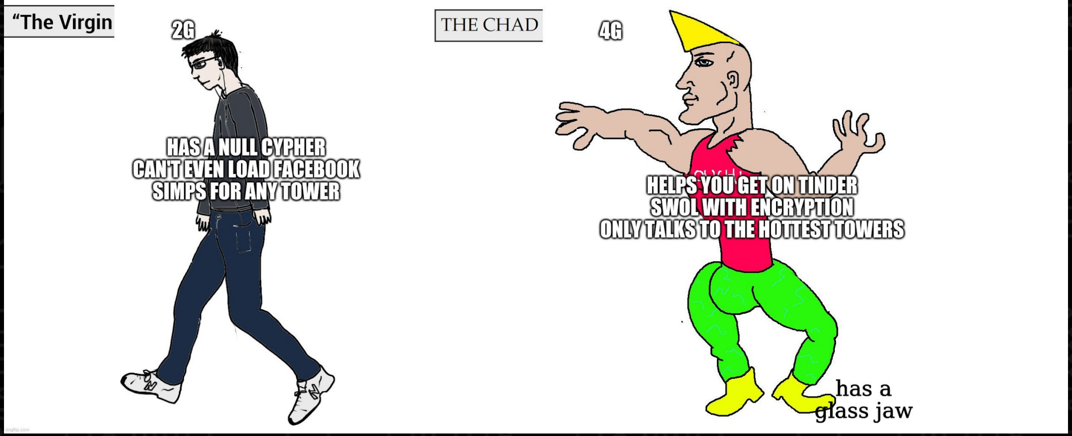
This is acronym hell and I’m sorry.

Cell Technology Overview



What Changed between 2G and 4G

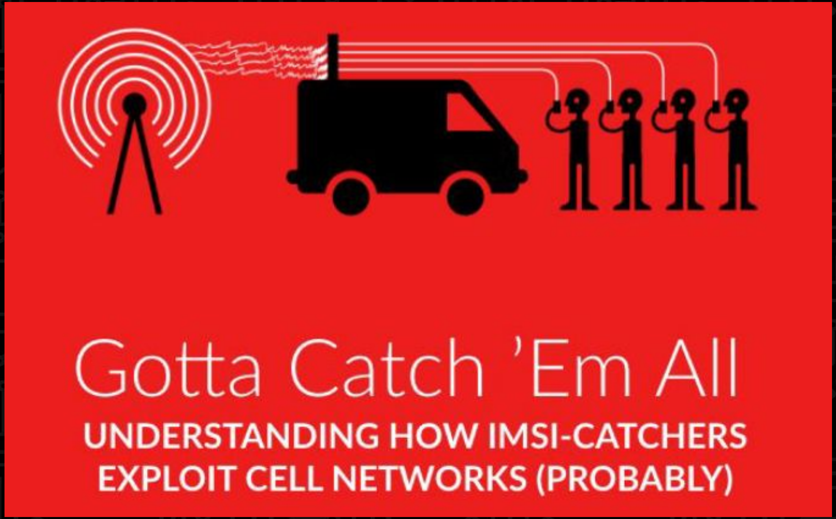
- eNodeB and UE mutually authenticate
- Better encryption between eNodeB and UE
- No longer naively connect to the strongest tower



What Changed Between 2G and 4G

- eNodeB and UE mutually authenticate
- Better encryption between eNodeB and UE
- No longer naively connect to the strongest tower

How do 4G CSS Work



Gotta Catch ’Em All

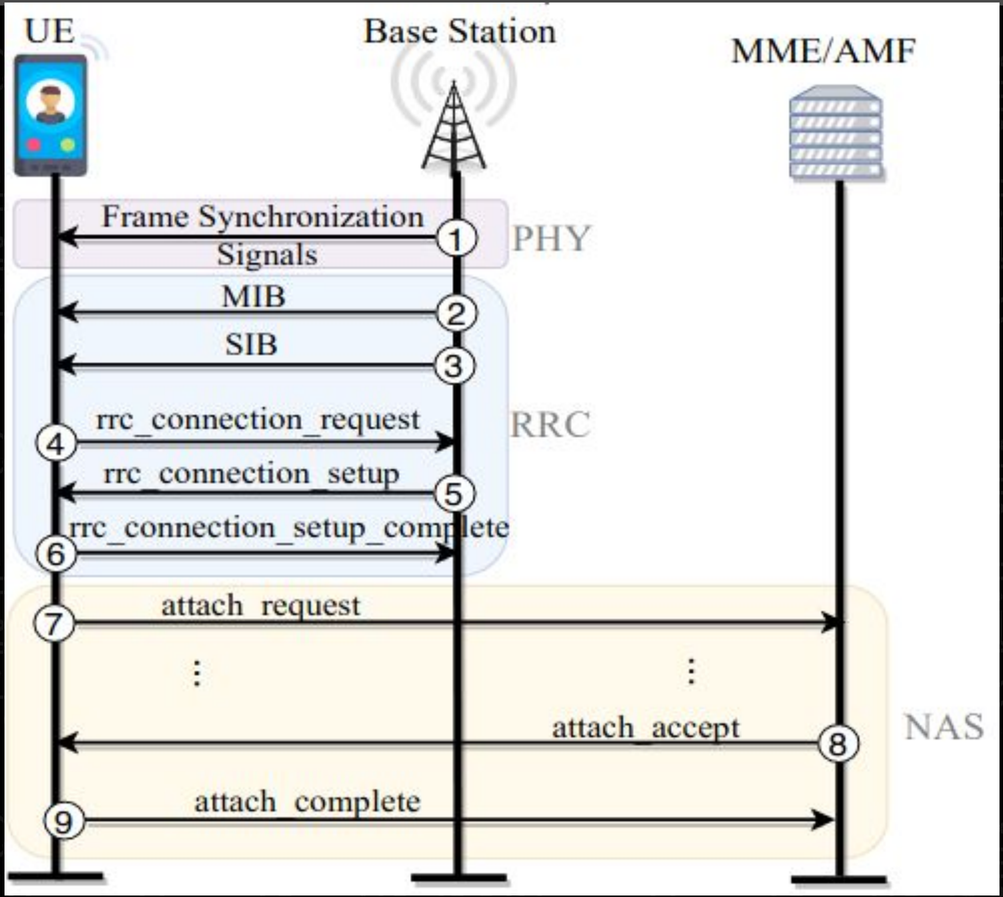
UNDERSTANDING HOW IMSI-CATCHERS EXPLOIT CELL NETWORKS (PROBABLY)

Gotta catch em all whitepaper by Yomna

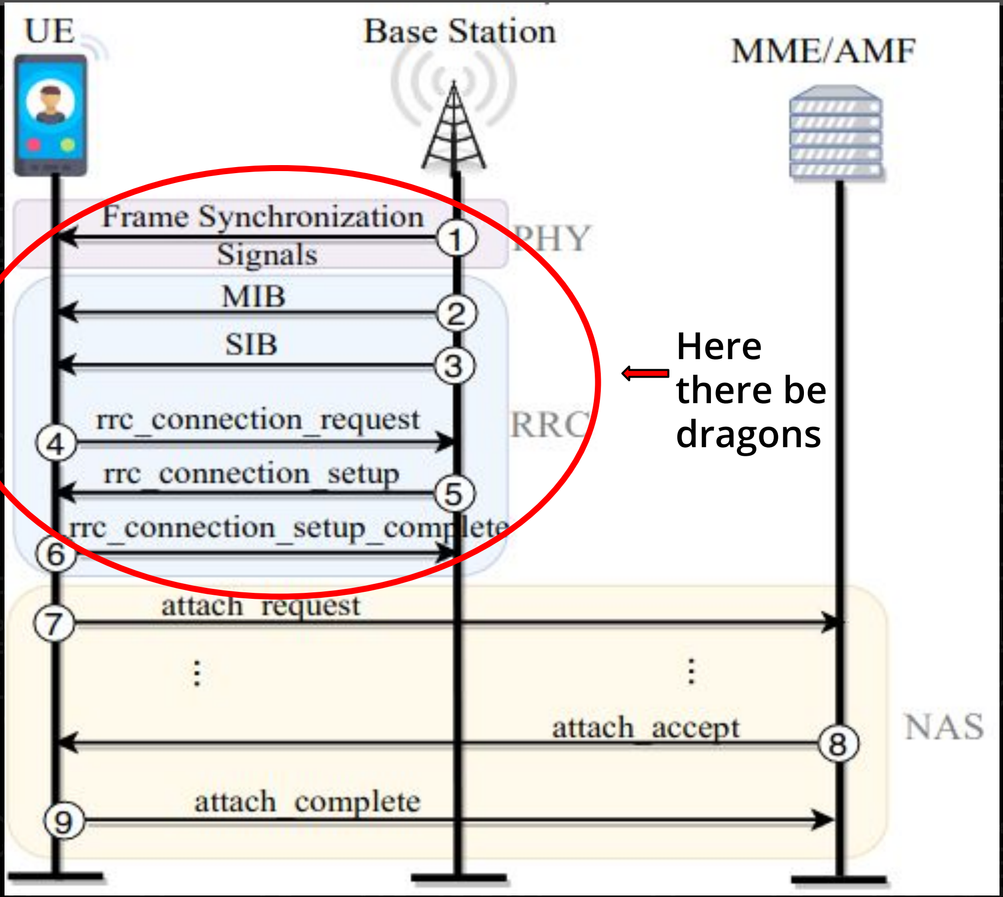
- What are the vulns next gen CSS are taking advantage of?
- Pre authentication handshake attacks
- Downgrade attacks

Pre-Authentication Vulnerabilities

- 4G has a glass jaw
- Even though the UE authenticates the tower there are still several messages that it sends, receives, and trusts before authentication happens or w/o authentication
- This is the weak spot in which the vast majority of 4G attacks happen



Insecure Connection Bootstrapping in Cellular Networks:The Root of All Evil - Hussein et al 2019



Here there be dragons

Insecure Connection Bootstrapping in Cellular Networks:The Root of All Evil - Hussain et al 2019

How Often are CSS Being Used

- ICE/DHS - hundreds of times per year
  - https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices/
- Local law enforcement
  - Oakland - 1-3 times per year
    - https://oaklandprivacy.org/oakland-privacy-sues-vallejo/
  - Santa Barbara PD - 231 times in 2017
    - https://www.eff.org/deeplinks/2019/05/eff-asks-san-bernardino-court-review-device-search-and-cell-site-simulator

How Often are CSS Being Used

- Foreign Spies
  - IMSI Catchers in DC
- Cyber Mercenaries
  - NSO Group https://www.amnestyusa.org/wp-content/uploads/2020/06/Morocco-NSO-Group-report.pdf
- Criminals
  - https://venturebeat.com/2014/09/18/the-cell-tower-mystery-gripping-america-has-now-been-solved-or-has-it/

Previous Efforts to Detect CSS

App Based

- AIMSICD
- Snoop Snitch
- Darshark

Strengths

- Cheap
- Easy to use

Weaknesses

- Limited data
- Lots of false positives
- False negatives?

Previous Efforts to Detect CSS

Radio Based

- Seaglass
- SITCH
- Overwatch

Strengths

- Better data
- Lower level information

Weaknesses

- Harder to set up, use, interpret
- Cost of hardware
- Can’t transmit

Previous Efforts to Detect CSS

Can we detect 4G IMSI Catchers?

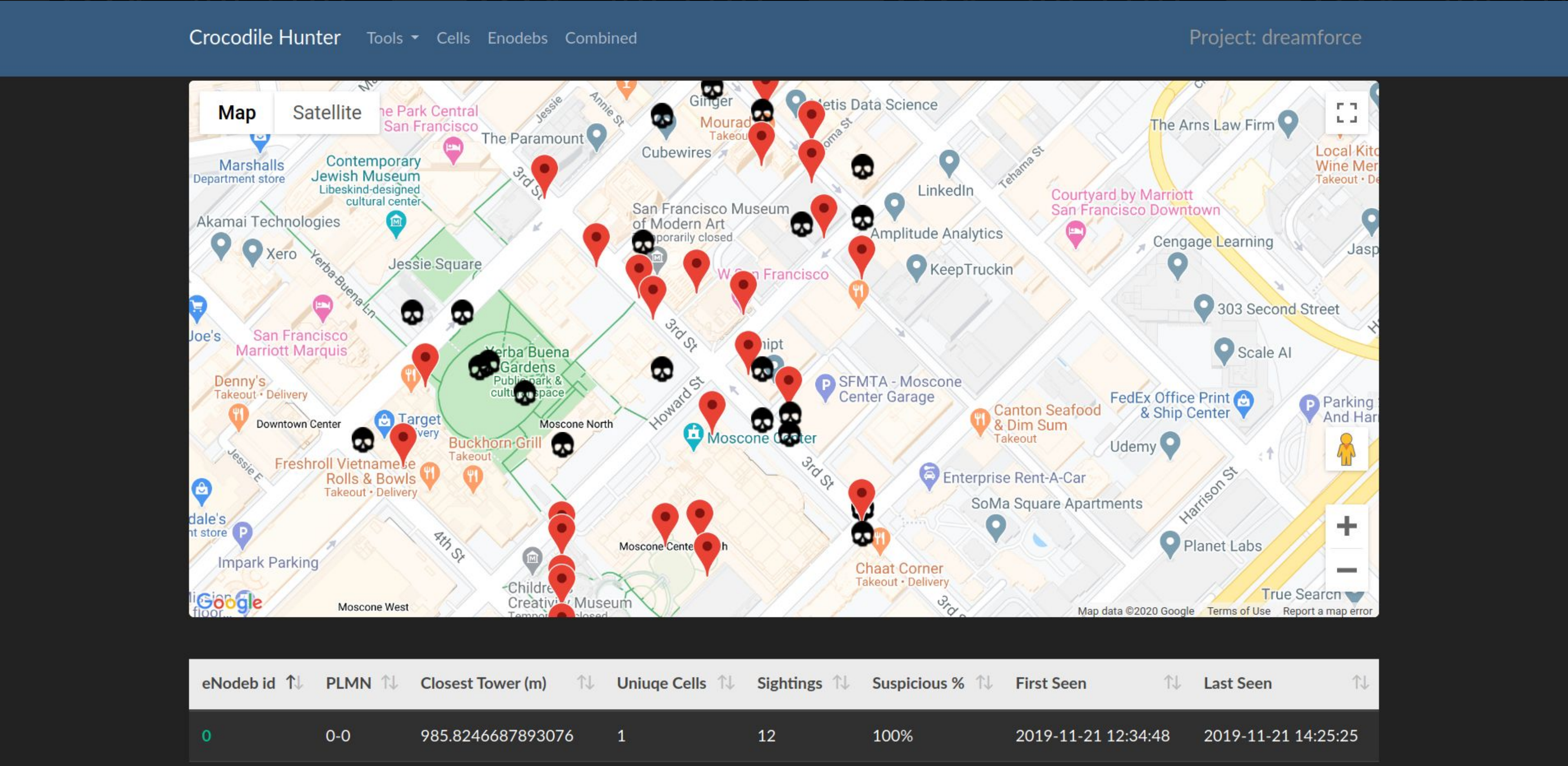
- How can we improve on previous attempts
  - Lower level data
  - See all towers not just what we are connecting to
  - Compare that data over time
  - **Look at 4G antennas!**
  - **Verify results!**

Introducing Crocodile Hunter

CROCODILE HUNTER

Crocodile Hunter Software Stack

- **Backend based on SRSLTE**
  - Open source LTE software stack
  - Written in C++
  - Communicates with frontend over a local socket
- **Python for heuristics, database and frontend**
  - Get data from socket
  - Add it to database
  - Run heuristics
  - Display tower locations
- **API for sharing data**



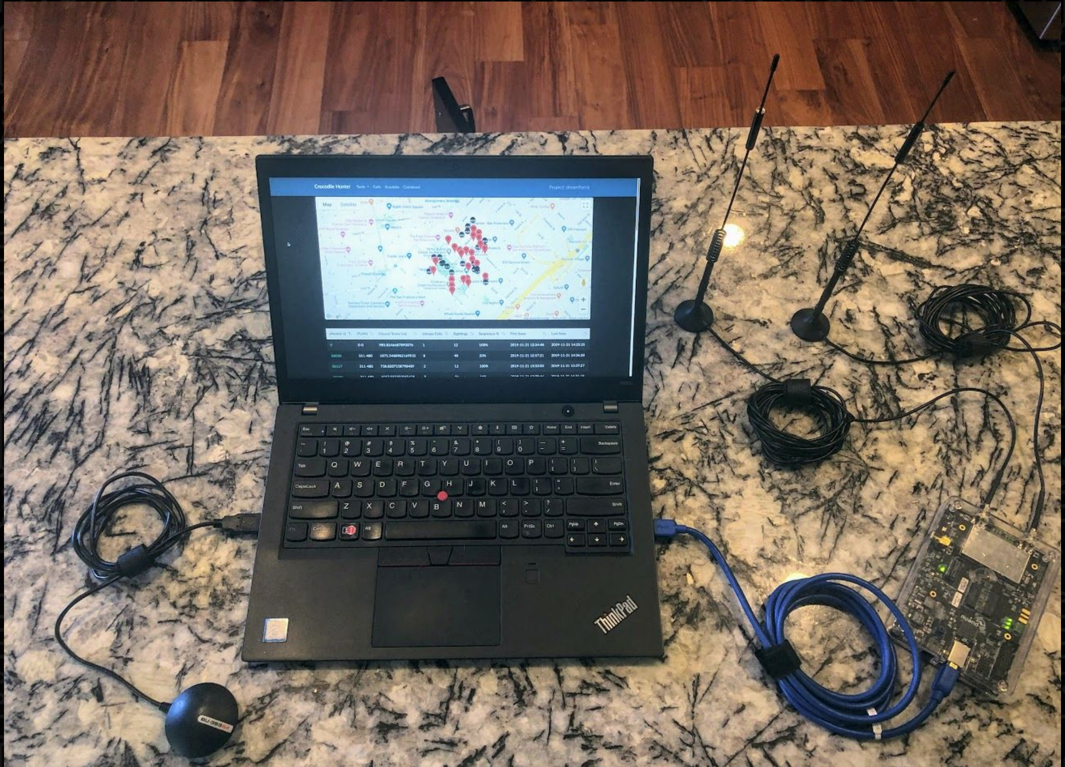
Crocodile Hunter · Tools · Cells · Enodebs · Combined · Project: dreamforce

eNodeb id	PLMN	Closest Tower (m)	Uniuqe Cells	Sightings	Suspicious %	First Seen	Last Seen
0	0-0	985.8246687893076	1	12	100%	2019-11-21 12:34:48	2019-11-21 14:25:25

Crocodile Hunter Hardware Stack

- Laptop / Raspberry Pi
- USB GPS Dongle
- SDR compatible with SRSLTE: BladeRF, Ettus B200
- LTE Antennas
- (Battery for Pi)

Crocodile Hunter Hardware Stack

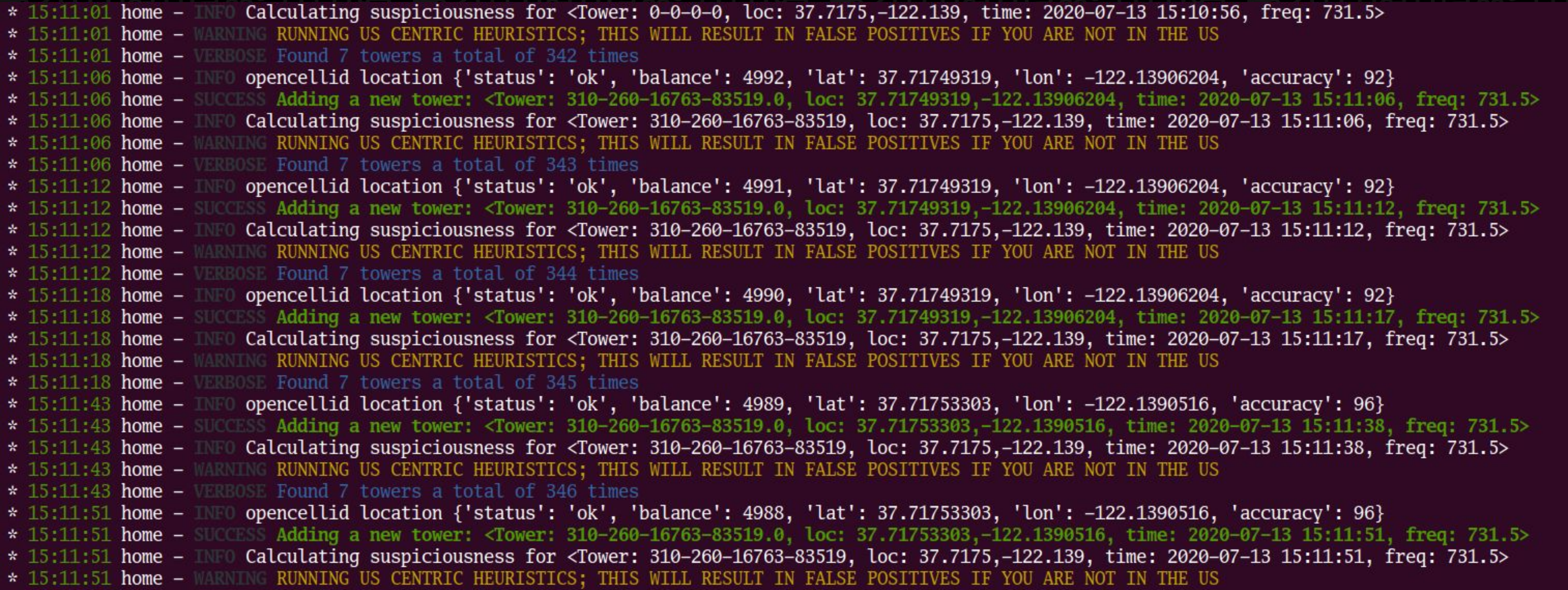


Workflow

1. Decode MIB and SIB1 for all the cells that we can see and record them.
2. Map the probable location of cells
3. Look for anomalies in the readings
4. Locate suspicious cells and confirm results

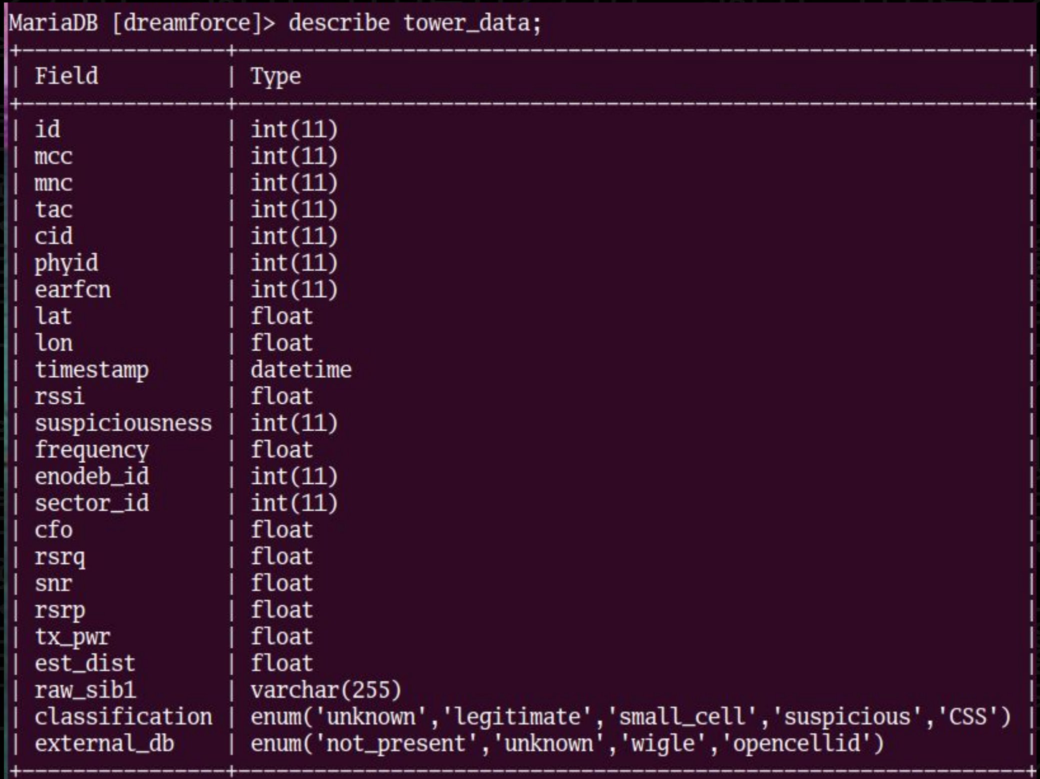
Decode MIB and SIB1

- SRSLTE scans a list of EARFCNS
- If we find a mib we decode mib and sib and send over socket



```
* 15:11:01 home - INFO Calculating suspiciousness for <Tower: 0-0-0-0, loc: 37.7175,-122.139, time: 2020-07-13 15:10:56, freq: 731.5>
* 15:11:01 home - WARNING RUNNING US CENTRIC HEURISTICS; THIS WILL RESULT IN FALSE POSITIVES IF YOU ARE NOT IN THE US
* 15:11:01 home - VERBOSE Found 7 towers a total of 342 times
* 15:11:06 home - INFO opencellid location {'status': 'ok', 'balance': 4992, 'lat': 37.71749319, 'lon': -122.13906204, 'accuracy': 92}
* 15:11:06 home - SUCCESS Adding a new tower: <Tower: 310-260-16763-83519.0, loc: 37.71749319,-122.13906204, time: 2020-07-13 15:11:06, freq: 731.5>
* 15:11:06 home - INFO Calculating suspiciousness for <Tower: 310-260-16763-83519, loc: 37.7175,-122.139, time: 2020-07-13 15:11:06, freq: 731.5>
* 15:11:06 home - WARNING RUNNING US CENTRIC HEURISTICS; THIS WILL RESULT IN FALSE POSITIVES IF YOU ARE NOT IN THE US
* 15:11:06 home - VERBOSE Found 7 towers a total of 343 times
* 15:11:12 home - INFO opencellid location {'status': 'ok', 'balance': 4991, 'lat': 37.71749319, 'lon': -122.13906204, 'accuracy': 92}
* 15:11:12 home - SUCCESS Adding a new tower: <Tower: 310-260-16763-83519.0, loc: 37.71749319,-122.13906204, time: 2020-07-13 15:11:12, freq: 731.5>
* 15:11:12 home - INFO Calculating suspiciousness for <Tower: 310-260-16763-83519, loc: 37.7175,-122.139, time: 2020-07-13 15:11:12, freq: 731.5>
* 15:11:12 home - WARNING RUNNING US CENTRIC HEURISTICS; THIS WILL RESULT IN FALSE POSITIVES IF YOU ARE NOT IN THE US
* 15:11:12 home - VERBOSE Found 7 towers a total of 344 times
* 15:11:18 home - INFO opencellid location {'status': 'ok', 'balance': 4990, 'lat': 37.71749319, 'lon': -122.13906204, 'accuracy': 92}
* 15:11:18 home - SUCCESS Adding a new tower: <Tower: 310-260-16763-83519.0, loc: 37.71749319,-122.13906204, time: 2020-07-13 15:11:17, freq: 731.5>
* 15:11:18 home - INFO Calculating suspiciousness for <Tower: 310-260-16763-83519, loc: 37.7175,-122.139, time: 2020-07-13 15:11:17, freq: 731.5>
* 15:11:18 home - WARNING RUNNING US CENTRIC HEURISTICS; THIS WILL RESULT IN FALSE POSITIVES IF YOU ARE NOT IN THE US
* 15:11:18 home - VERBOSE Found 7 towers a total of 345 times
* 15:11:43 home - INFO opencellid location {'status': 'ok', 'balance': 4989, 'lat': 37.71753303, 'lon': -122.1390516, 'accuracy': 96}
* 15:11:43 home - SUCCESS Adding a new tower: <Tower: 310-260-16763-83519.0, loc: 37.71753303,-122.1390516, time: 2020-07-13 15:11:38, freq: 731.5>
* 15:11:43 home - INFO Calculating suspiciousness for <Tower: 310-260-16763-83519, loc: 37.7175,-122.139, time: 2020-07-13 15:11:38, freq: 731.5>
* 15:11:43 home - WARNING RUNNING US CENTRIC HEURISTICS; THIS WILL RESULT IN FALSE POSITIVES IF YOU ARE NOT IN THE US
* 15:11:43 home - VERBOSE Found 7 towers a total of 346 times
* 15:11:51 home - INFO opencellid location {'status': 'ok', 'balance': 4988, 'lat': 37.71753303, 'lon': -122.1390516, 'accuracy': 96}
* 15:11:51 home - SUCCESS Adding a new tower: <Tower: 310-260-16763-83519.0, loc: 37.71753303,-122.1390516, time: 2020-07-13 15:11:51, freq: 731.5>
* 15:11:51 home - INFO Calculating suspiciousness for <Tower: 310-260-16763-83519, loc: 37.7175,-122.139, time: 2020-07-13 15:11:51, freq: 731.5>
* 15:11:51 home - WARNING RUNNING US CENTRIC HEURISTICS; THIS WILL RESULT IN FALSE POSITIVES IF YOU ARE NOT IN THE US
```

Database



```
MariaDB [dreamforce]> describe tower_data;
+----------------+--------------------------------------------------------------+
| Field          | Type                                                         |
+----------------+--------------------------------------------------------------+
| id             | int(11)                                                      |
| mcc            | int(11)                                                      |
| mnc            | int(11)                                                      |
| tac            | int(11)                                                      |
| cid            | int(11)                                                      |
| phyid          | int(11)                                                      |
| earfcn         | int(11)                                                      |
| lat            | float                                                        |
| lon            | float                                                        |
| timestamp      | datetime                                                     |
| rssi           | float                                                        |
| suspiciousness | int(11)                                                      |
| frequency      | float                                                        |
| enodeb_id      | int(11)                                                      |
| sector_id      | int(11)                                                      |
| cfo            | float                                                        |
| rsrq           | float                                                        |
| snr            | float                                                        |
| rsrp           | float                                                        |
| tx_pwr         | float                                                        |
| est_dist       | float                                                        |
| raw_sib1       | varchar(255)                                                 |
| classification | enum('unknown','legitimate','small_cell','suspicious','CSS') |
| external_db    | enum('not_present','unknown','wigle','opencellid')           |
+----------------+--------------------------------------------------------------+
```

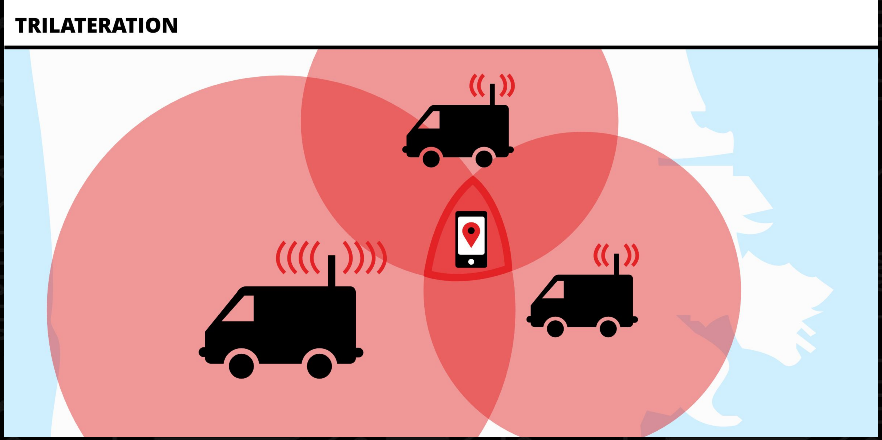
Mapping out antennas in real time

- Using trilateration and distance estimates we can figure out where all the towers are
- Compare this to a ground truth such as wigle or opencellid

Trilateration vs Triangulation

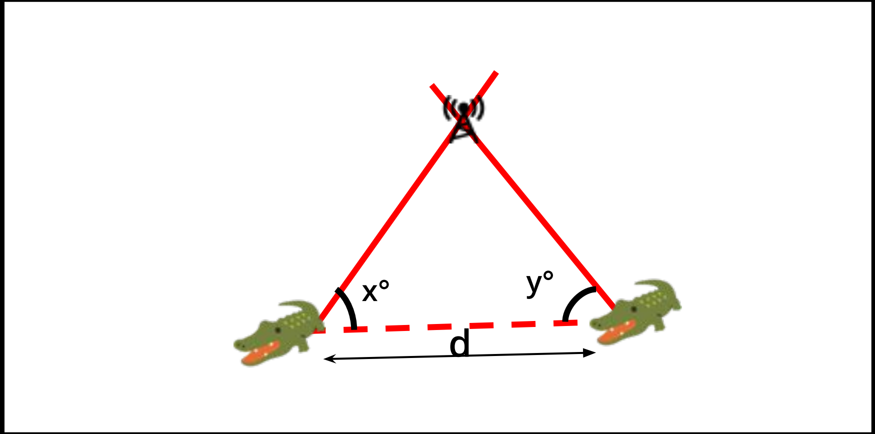
Trilateration

$L = R_1 \cap R_2 \cap R_3$



Triangulation (Bearing)

$L = B_1 \cap B_2 \cap B_3$



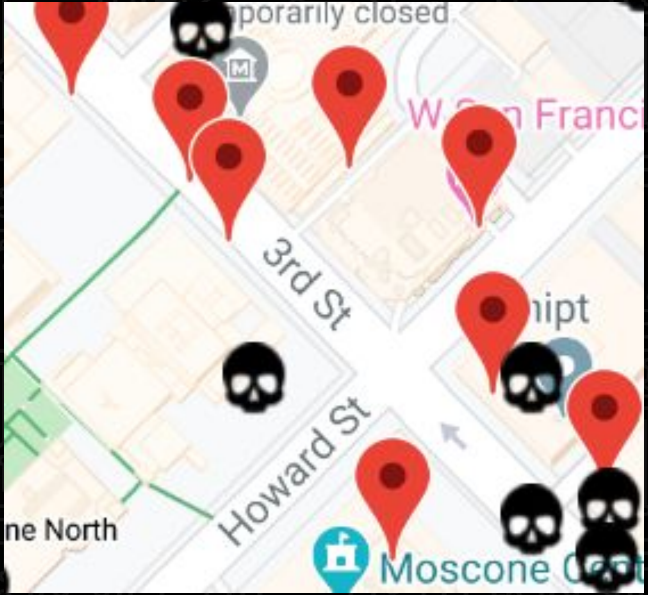
Looking for Anomalies

- Cells moving
- Cells that change signal strength
- Cells that aren’t where they should be
- Cells changing parameters
- Cells missing parameters
- New cells
- **Anomaly != CSS, that's why we have to verify**

Why Don’t we Transmit?

What we Found so Far

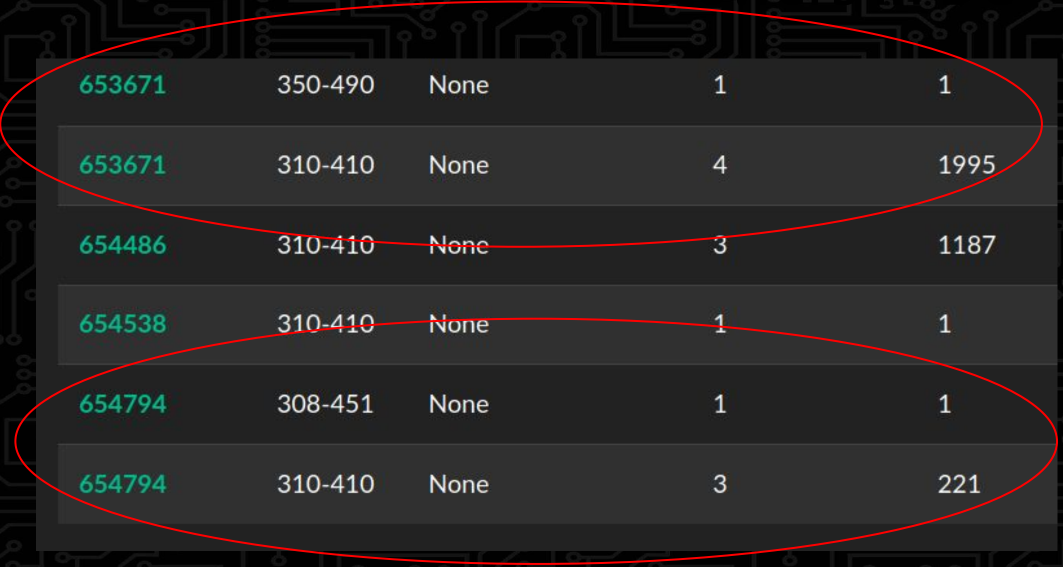
Cell on wheels at Dreamforce



CELL SITE SIMULATORS AREN'T ALWAYS THIS OBVIOUS
SignalWire
THAT'S WHY WE HAVE CROCODILE HUNTER
imgflip.com

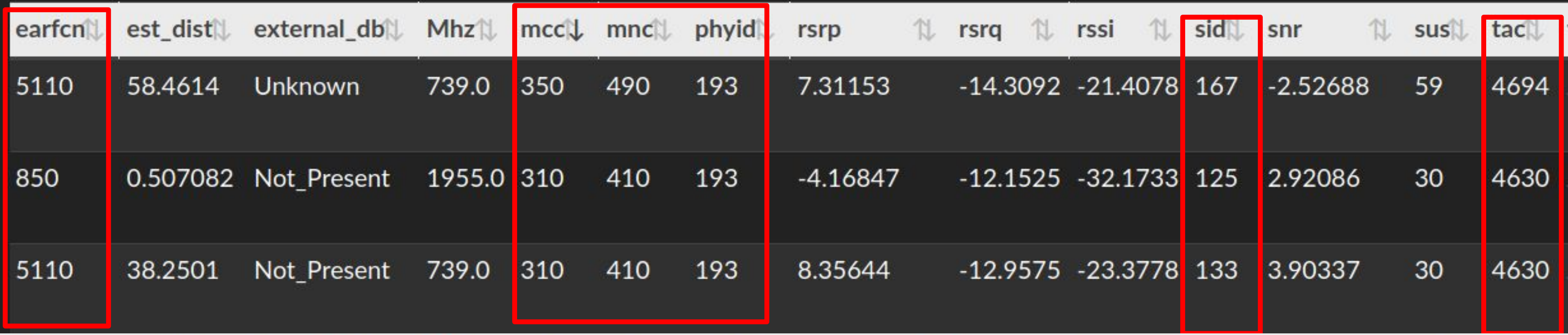
What we Found so Far

Suspicious eNodeBs in Washington DC

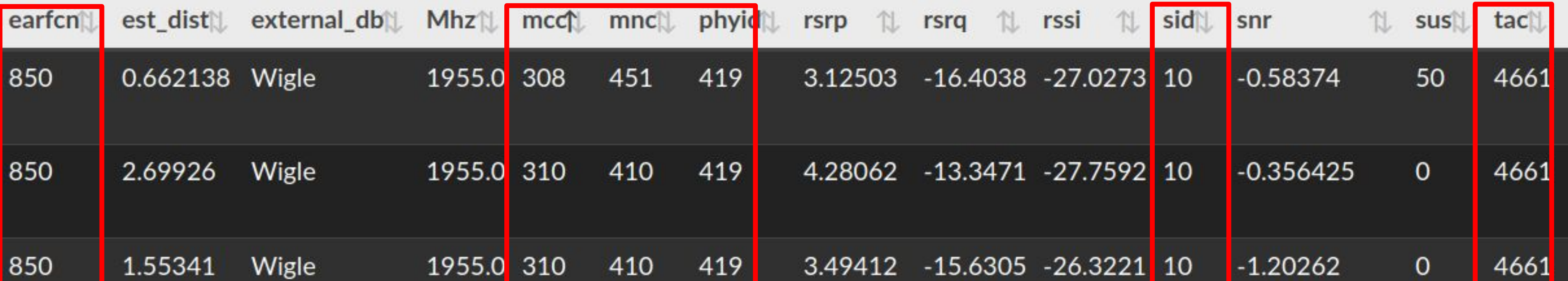


653671	350-490	None	1	1
653671	310-410	None	4	1995
654486	310-410	None	3	1187
654538	310-410	None	1	1
654794	308-451	None	1	1
654794	310-410	None	3	221

Washington DC



earfcn	est_dist	external_db	Mhz	mcc	mnc	phyid	rsrp	rsrq	rssi	sid	snr	sus	tac
5110	58.4614	Unknown	739.0	350	490	193	7.31153	-14.3092	-21.4078	167	-2.52688	59	4694
850	0.507082	Not_Present	1955.0	310	410	193	-4.16847	-12.1525	-32.1733	125	2.92086	30	4630
5110	38.2501	Not_Present	739.0	310	410	193	8.35644	-12.9575	-23.3778	133	3.90337	30	4630



earfcn	est_dist	external_db	Mhz	mcc	mnc	phyid	rsrp	rsrq	rssi	sid	snr	sus	tac
850	0.662138	Wigle	1955.0	308	451	419	3.12503	-16.4038	-27.0273	10	-0.58374	50	4661
850	2.69926	Wigle	1955.0	310	410	419	4.28062	-13.3471	-27.7592	10	-0.356425	0	4661
850	1.55341	Wigle	1955.0	310	410	419	3.49412	-15.6305	-26.3221	10	-1.20262	0	4661

Ongoing Tests

- Latin America (FADe Project)
- DC
- NYC
- Your hometown (coming soon…)

Future Work

- Better heuristics
- Better location finding
- Machine learning for detection of anomalies
- Port to cheaper hardware

What’s With the Name?

Press F to pay respects to Steve

How Can we Stop Cell-Site Simulators

- End 2G support on iOS and Android now!
  - https://www.eff.org/deeplinks/2020/06/your-phone-vulnerable-because-2g-it-doesnt-have-be
- Eliminate pre-authentication messages
  - TLS for the handshake with towers
- More incentives for standards orgs (3GPP), carriers, manufacturers, and OEMs to care about user privacy
- Nothing is foolproof but we aren’t even doing the bare minimum yet.

Key Takeaways

- We have a pretty good understanding the vulns in 4G which commercial cell-site simulators might exploit
- None of the previous IMSI catcher detector apps really do the job any more.
- We have come up with a method similar to established methods but targeting 4G.
- The worst problems of CSS abuse can be solved!

Thanks to the following people

- Yomna!
- The whole EFF crew
- Andy and Bob at Wigle
- Roger Piqueras-Jover
- Nima Fatemi with Kandoo, Surya Mattu, Simon
- Carlos and the FADE Project
- Karl Kosher, Peter Ney, and others at UW (SEAGLASS)
- Ash wilson (SITCH) and Eric Escobar (Defcon Justice Beaver)
- Kristin Paget

Thank you!

Cooper Quintin
Senior Security Researcher
EFF Threat Lab
cooperq@eff.org - twitter: @cooperq
https://github.com/efforg/crocodilehunter

References

1. https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks
2. https://github.com/srsLTE/srsLTE
3. https://arxiv.org/pdf/1710.08932.pdf
4. https://www.usenix.org/system/files/conference/woot17/woot17-paper-park.pdf
5. https://seaglass-web.s3.amazonaws.com/SeaGlass___PETS_2017.pdf
6. https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf