Discovering and Triangulating Rogue Cell Towers



Reddit: jaycrew

Eric Escobar, PE

Security Engineer

Barracuda

A bit about me:

- Started off in Civil Engineering (MS, PE)
- Always loved computers
- Nerded out on all things wireless
  - Licensed HAM
- I love to automate things
  - Chicken coop
  - Sprinklers
- Caught the DEF CON bug
  - Wireless CTF

Barracuda

A bit about what I do:

- Security Engineer for Barracuda Networks
  - Incident Response
  - Pentesting
  - Red Team, Blue Team
  - Social Engineering
  - Phishing Campaigns
  - Bug bounty
  - Infrastructure scanning
  - Product team relations
  - 2FA, IPAM



Here’s what we are going to cover:

- What is a rogue cell tower?
- Why should you care about rogue cell towers?
- How can you detect a rogue cell tower?
- How do you find a rogue cell tower?
- How do you build a detector at home?
- You’ve detected a rogue tower… now what?

Barracuda

What is a rogue cell tower?

- A device created (or purchased) by companies, governments or hackers that has the ability to trick your phone into thinking it's a real cell phone tower.
- Also known as IMSI catchers, interceptors, **cell-site simulators**, Stingrays, and probably a few more.
- Rogue cell towers have the ability to collect information about you indirectly through metadata (call length, dialed numbers)
- In some conditions can collect **content** of messages, calls, and data.

Barracuda

How are cell simulators used today?

In the United States:

- IMSI-catchers are used by US law enforcement agencies to help locate, track, and collect data on suspects.
- ACLU has identified 66 agencies and 24 states that own stingrays.
- Used to monitor demonstrations in the US
  - Used in Chicago political protests
  - IMSI Catcher Counter-Surveillance Freddy Martinez
- It's possible to make an IMSI-catcher at home
  - DEFCON 18: Practical Cellphone Spying - Chris Paget



How are cell simulators used today?

Further reading:

- EFF.org – Cell-site simulator FAQ
- ACLU – “Stingray Tracking Devices: Who’s Got Them”

Barracuda

How are cell simulators used today?

Abroad:

- Reported use in Ireland, UK, China, Germany, Norway, South Africa
- Chinese spammers were caught sending spam and phishing messages.
- Used by governments and corporations alike.

Barracuda

What's the IMSI in "IMSI-catcher"?

- IMSI stands for International Mobile Subscriber Identity.
- Is used as a means of identifying a device on the cell network.
- Typically 15 digits long
- Contains general information about you device (Country & Carrier)
  - Mobile Country Code – MCC
  - Mobile Network Code – MNC
  - Mobile Subscription Identification Number – MSIN

Barracuda

What’s the IMSI in “IMSI-catcher”?

MNC & MCC

- All country codes (MCC) are available on Wikipedia
- All network codes (MNC) are available on Wikipedia

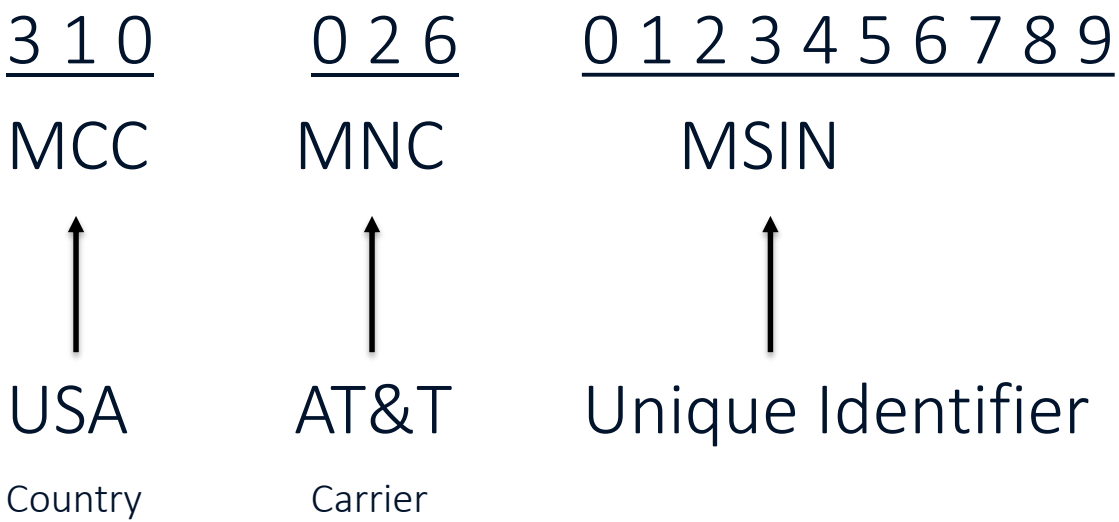
Barracuda

What’s an IMSI?

IMSI = Unique identifier to your device

Barracuda

Sample IMSI:



Barracuda

Why you should care? – A short story

- You are a fish about to be caught in one big net



Barracuda

Why you should care?

- Your phone will connect automatically to cell site simulators.
- Thieves can steal your personal information.
- Hacker's can track where you go, who you're talking to, and grab all sorts of other data about you.
- Your digital life can be sniffed out of the air by anyone with some technical chops, and a laptop, and some hardware that is CHEAP.
- Your company could be leaking trade secrets.
- Your privacy is at risk.



Why build a detector?

- There are some great apps for Android phones and that have the ability to detect cell tower anomalies.
  - You need specific phone models & root for this to work
- I wanted a device that met the following conditions:
  - Cheap ~$50/device
  - I wanted to set it and forget it.
  - I wanted to be alerted to any anomalies.
  - I wanted the ability to network multiple devices together.



How do you detect a rogue cell tower?

- Every cell tower (Base Transceiver Station, BTS) beacons out information about itself
  - ARFCN – Absolute radio frequency channel number
  - MCC – Mobile Country Code
  - MNC – Mobile Network Code
  - Cell ID – Unique identifier (within a large area)
  - LAC – Location area code
  - Txp – Transmit power maximum
  - Neighboring cells



How do you detect a rogue cell tower?

- Typically these values remain constant:
  - ARFCN – Absolute radio frequency channel number
  - MCC – Mobile Country Code
  - MNC – Mobile Network Code
  - Cell ID – Unique identifier (within a large area)
  - LAC – Location area code
  - Txp – Transmit power maximum
  - Neighboring cells
  - Power level

Barracuda

How do you detect a rogue cell tower?

- If values deviate from what's expected it can mean that there is maintenance taking place.
- It can mean changes are being made to the network.
- It could also mean that there is a rogue cell tower is nearby!
- The idea is to get a baseline of your cellular neighborhood over a period of time.
- It would be like keeping an eye on the cars that come in and out of your neighborhood, after a while you begin to know which doesn't belong.

Barracuda

How do you detect a rogue cell tower?



ARFCN	Channel	0694
MCC	Country Code	310
MNC	Network Code	026
Cell ID	Unique ID	1799
Power Level		Constant

Barracuda

How do you detect a rogue cell tower?

- Examples:
  - A new tower (Unknown Cell ID), high transmission power
  - Mobile country code mismatch
  - Mobile network code mismatch
  - Frequency change
  - Location Area Code mismatch

Barracuda

Why locate a tower?

- So you've found a tower
- Cell tower or white van?





Barracuda

How do you locate a tower?

- Combine unique cell tower data, receive power, and location.
- One detector can be moved around with an onboard GPS
  - Readings of unique tower identifiers, power level and GPS coordinates allow for a single detector to create a map.
  - Some math, open source GIS software, and pretty colors can approximate locations of towers or possible rogue towers

Barracuda

How do you locate a tower?



Barracuda

How do you locate a tower?

- Multiple detectors with known locations allow for trilateration of the suspected rogue tower.
- Receive power and distance are not inversely proportional
  - Regression formulas were required to be calculated in order to fine tune the results.
  - Less accurate but still pretty good
- TDOA – Time distance of arrival
  - I don’t have accurate enough timings

Barracuda

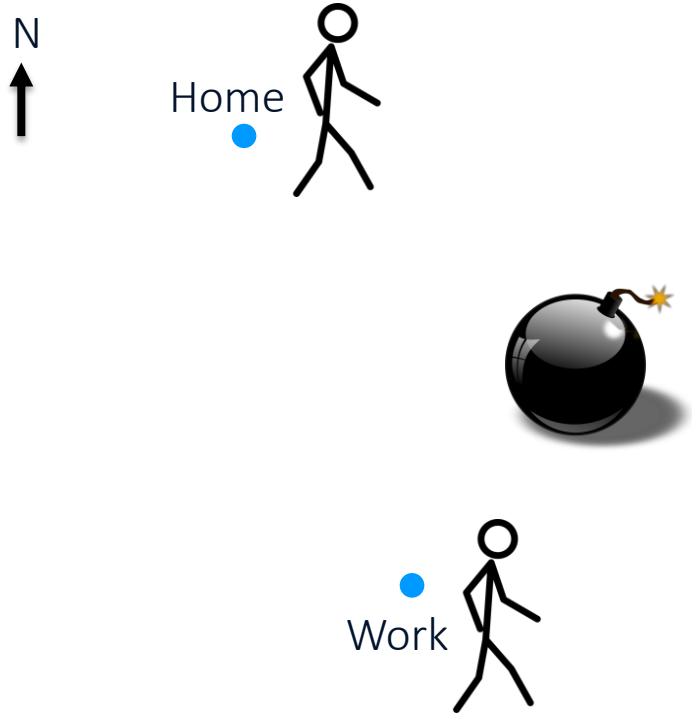
How do you locate a tower?

Trilateration vs Triangulation

(I get it, but some people don’t)

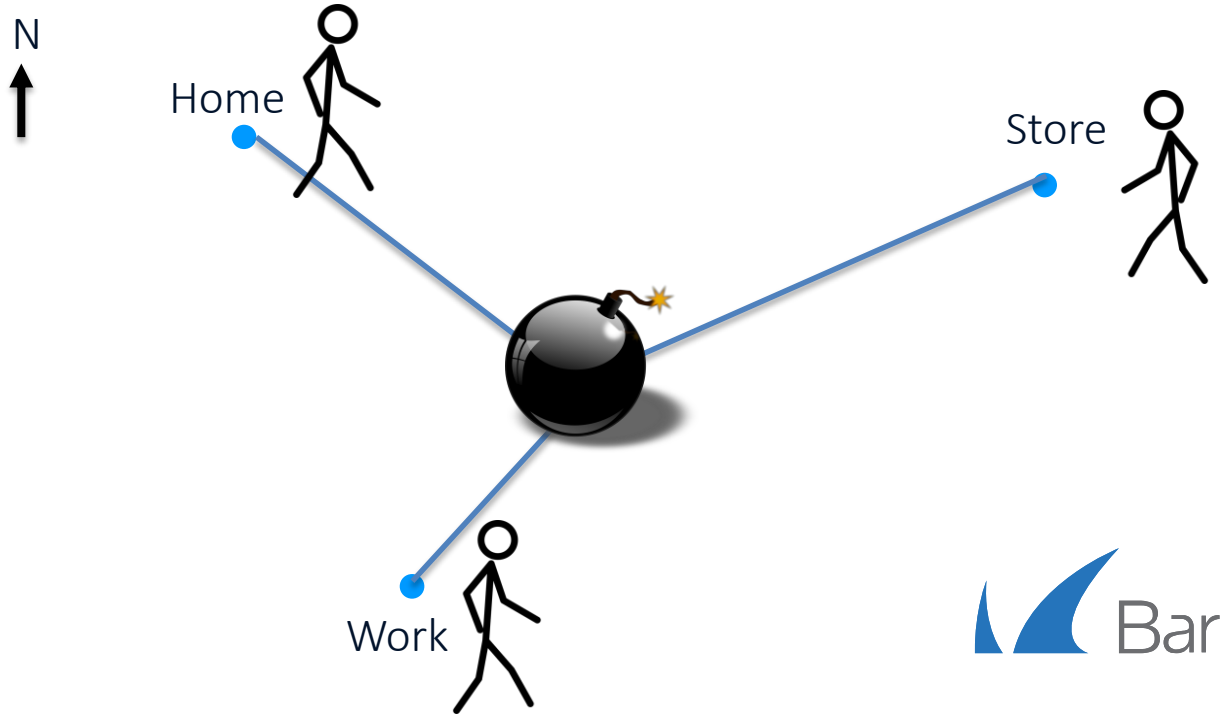
Barracuda

Triangulation



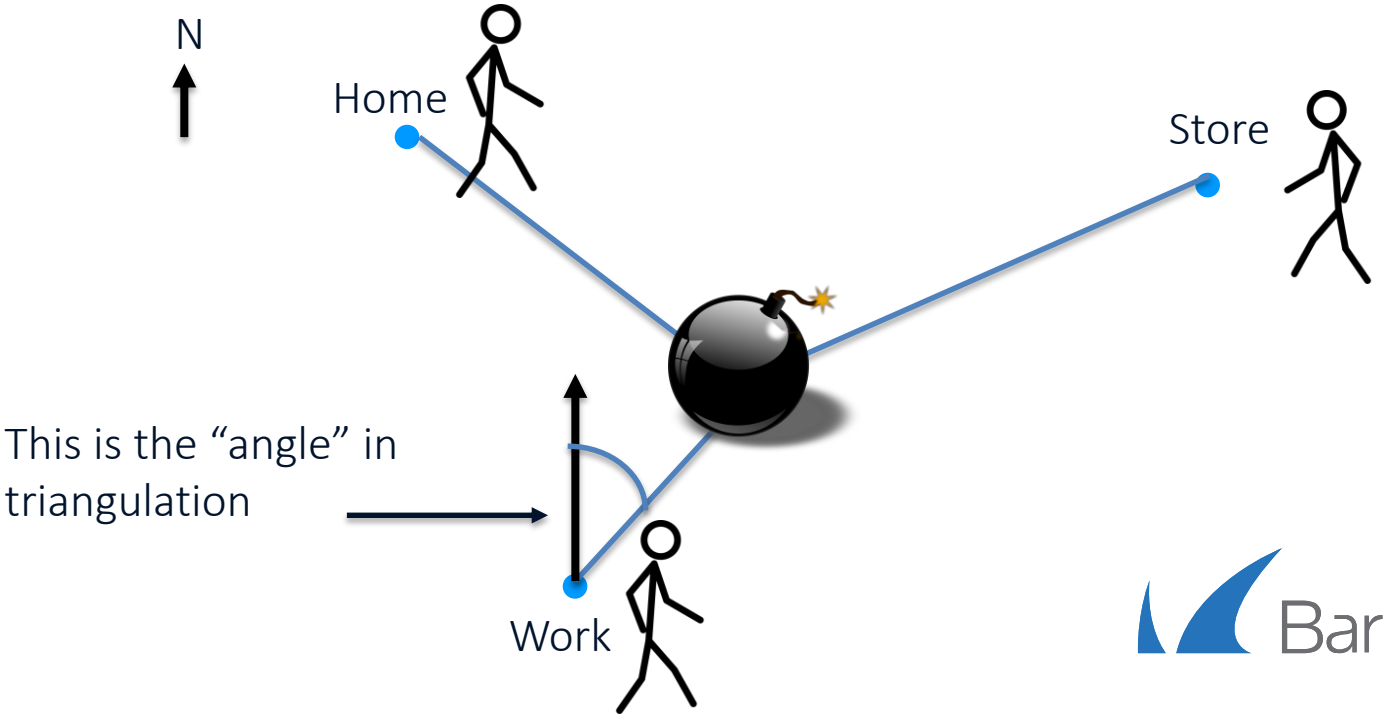
Barracuda

Triangulation



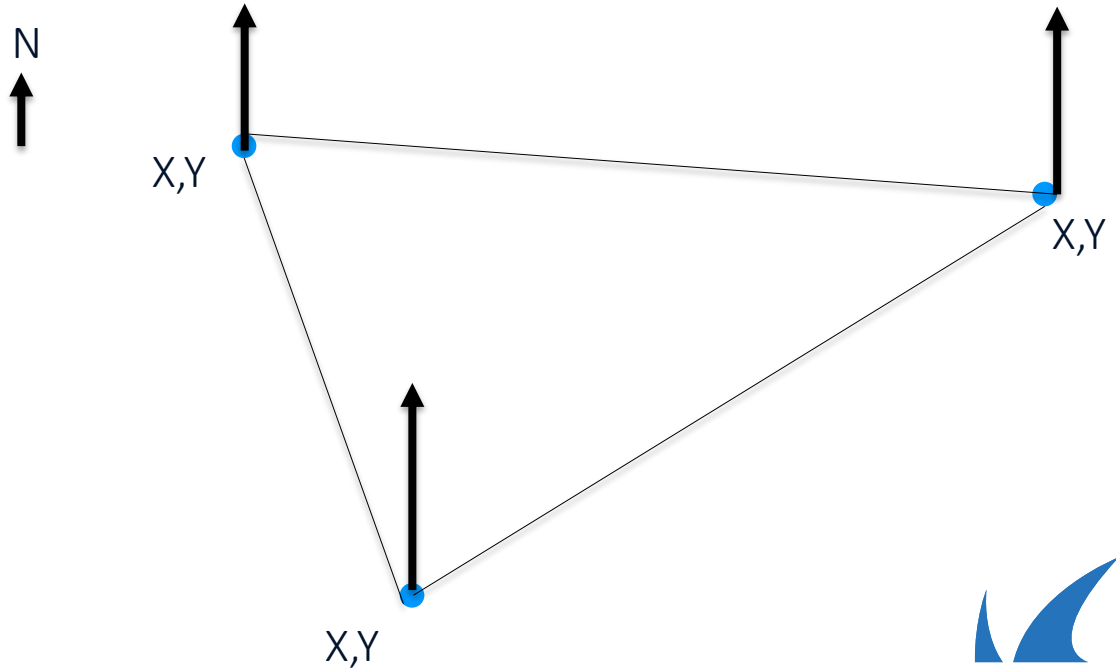
Barracuda

Triangulation



Barracuda

Triangulation



Barracuda

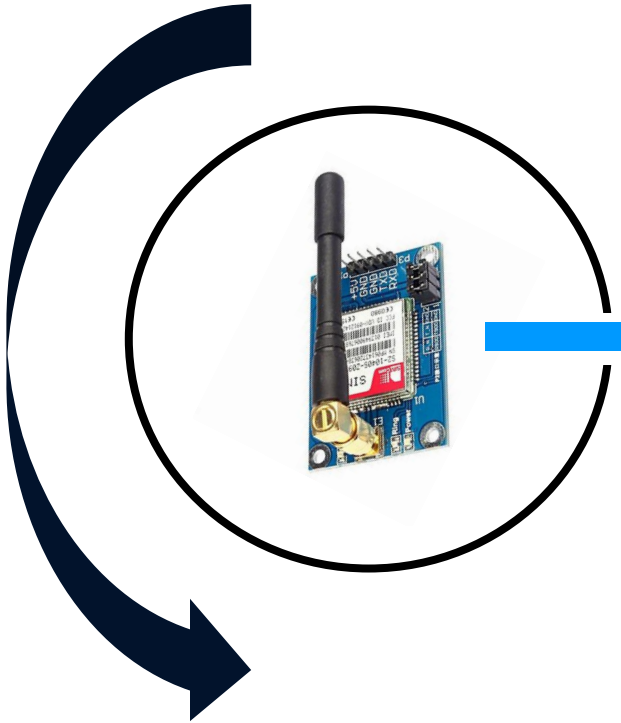
Triangulation

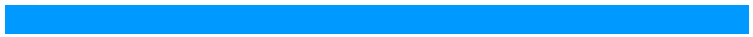
- Looking forward this is a feature I would like to add
- Conceptually makes sense, I haven’t tried it out



Barracuda

Triangulation







Barracuda

Triangulation







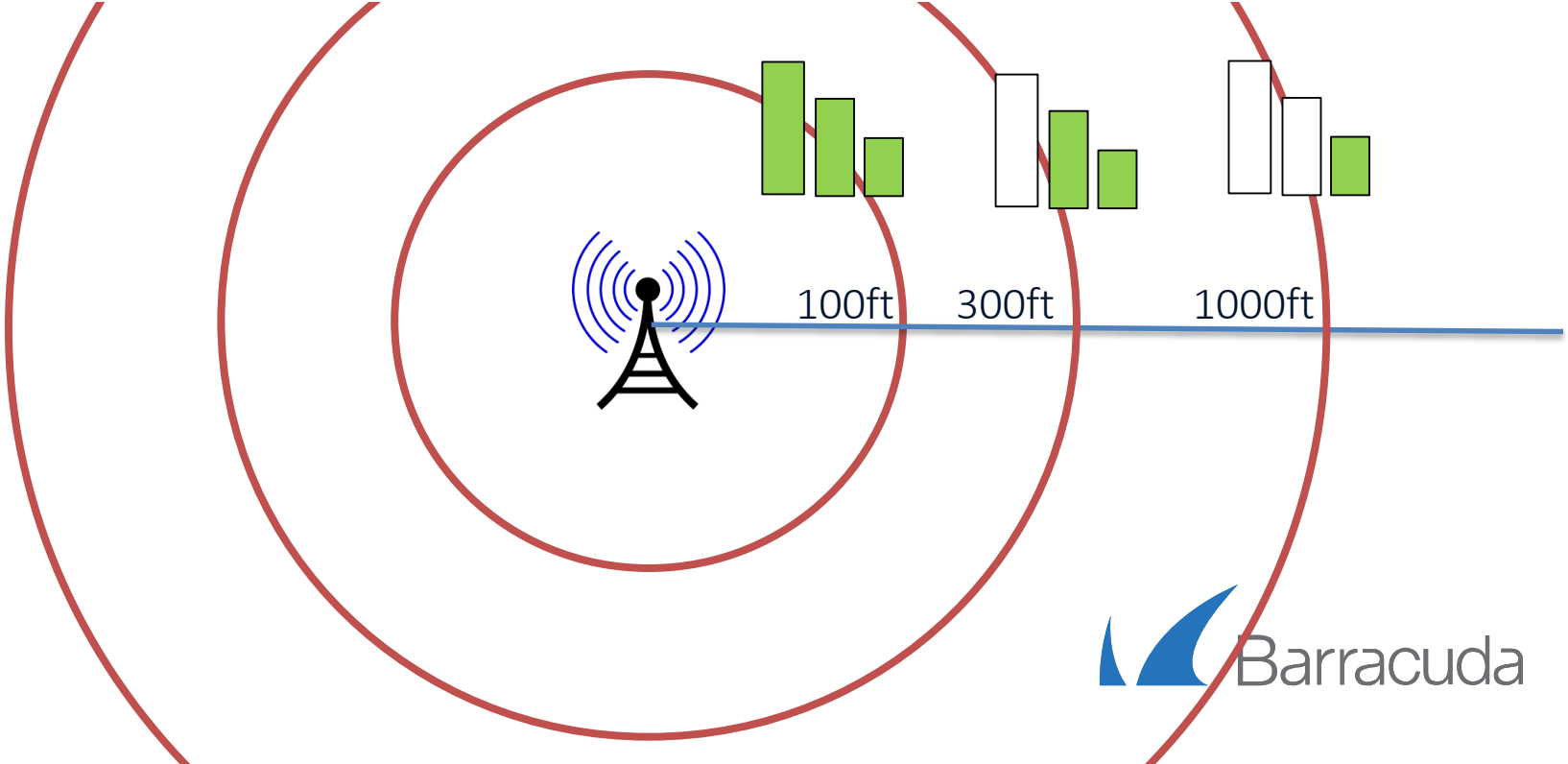
Barracuda

How do you locate a tower?

My detector **technically** uses trilateration

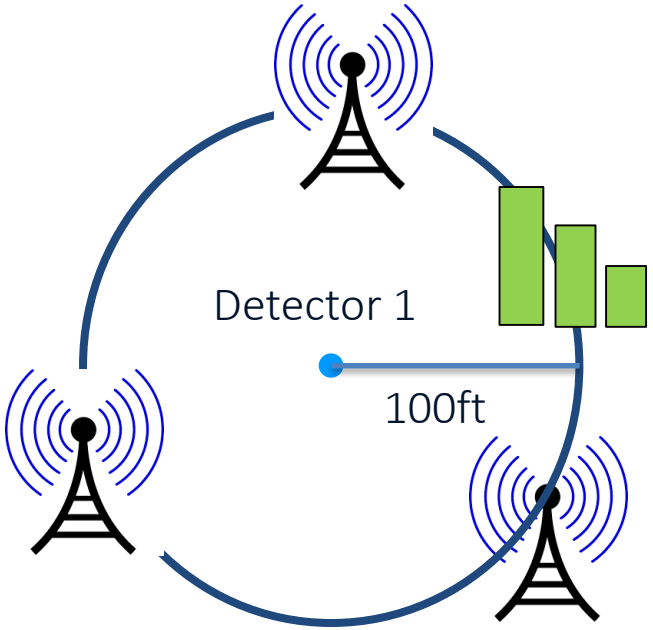


How do you locate a tower?



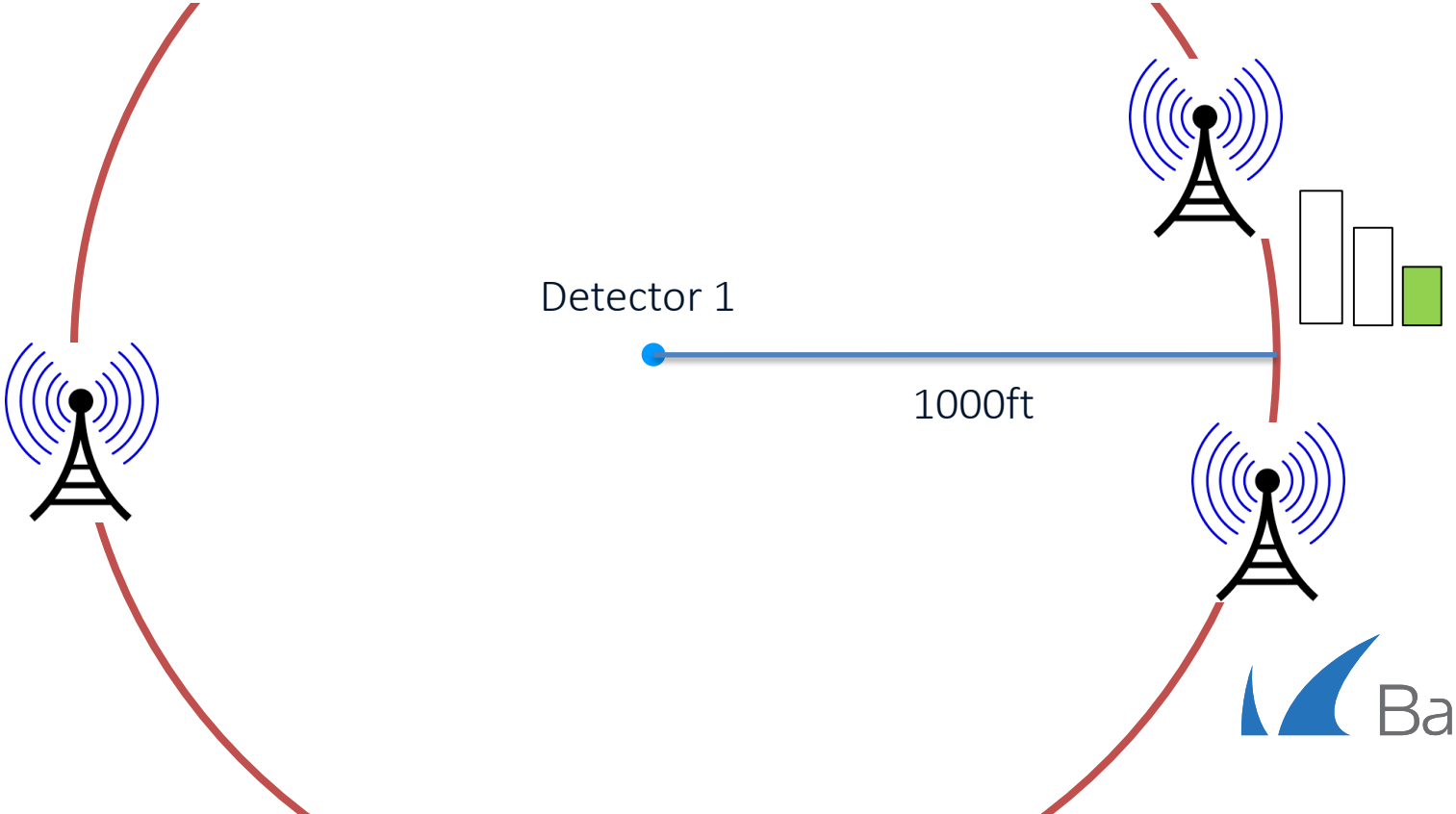
Barracuda

How do you locate a tower?



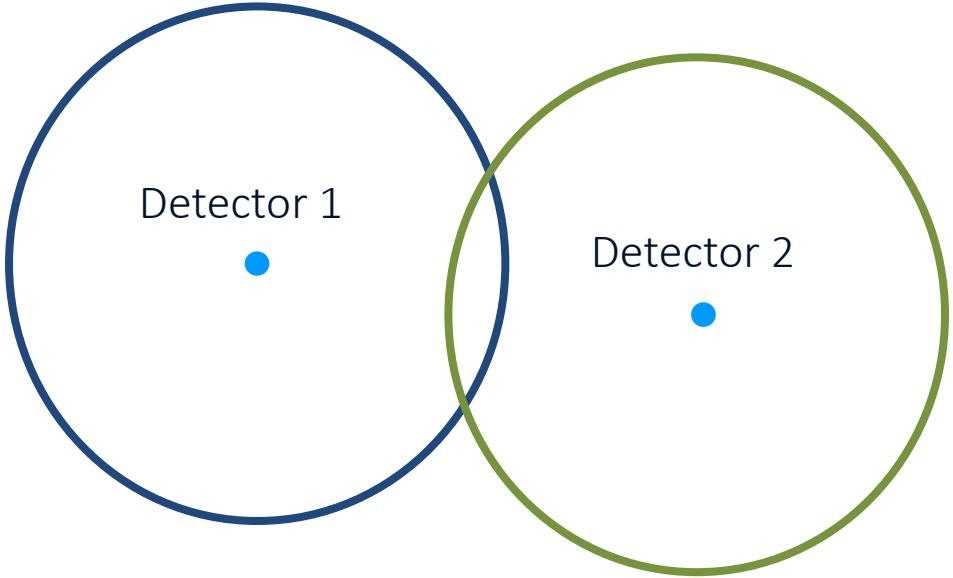
Barracuda

How do you locate a tower?



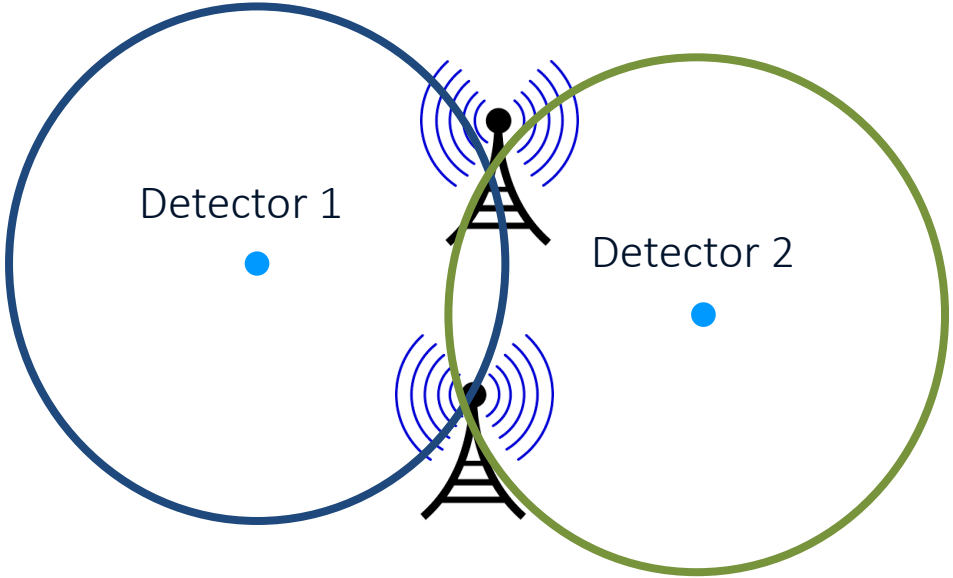
Barracuda

How do you locate a tower?



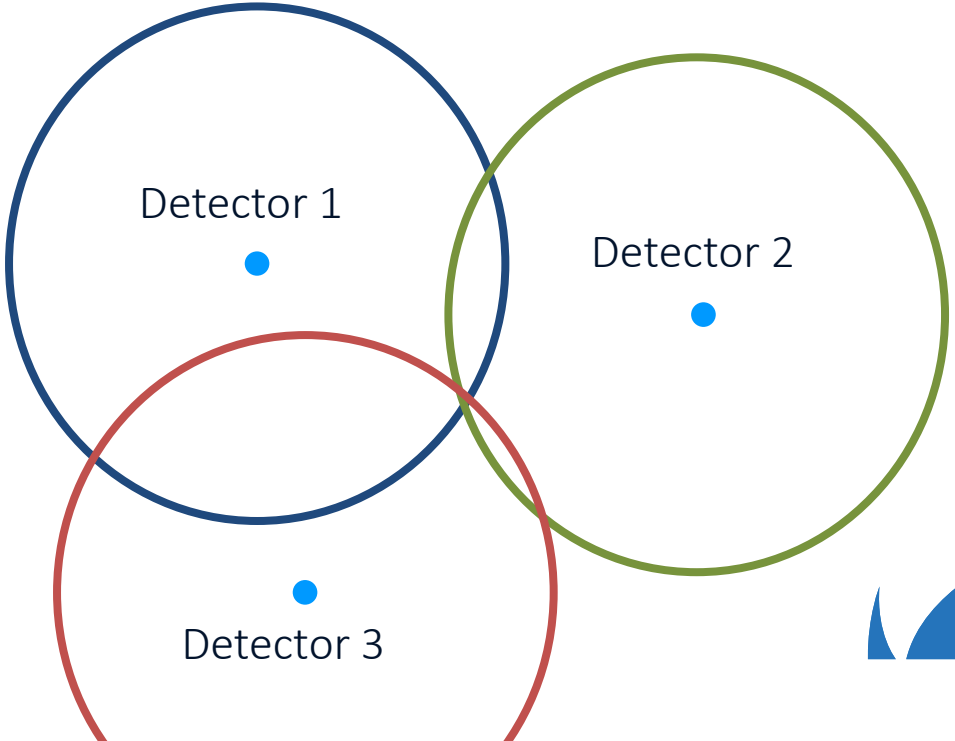
Barracuda

How do you locate a tower?



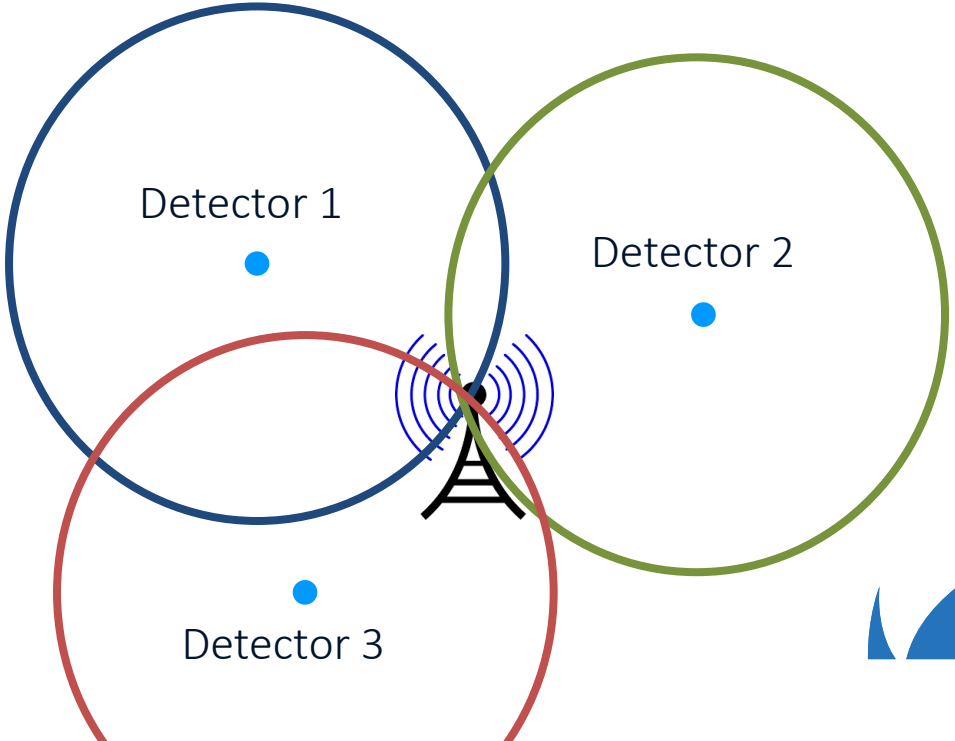
Barracuda

How do you locate a tower?



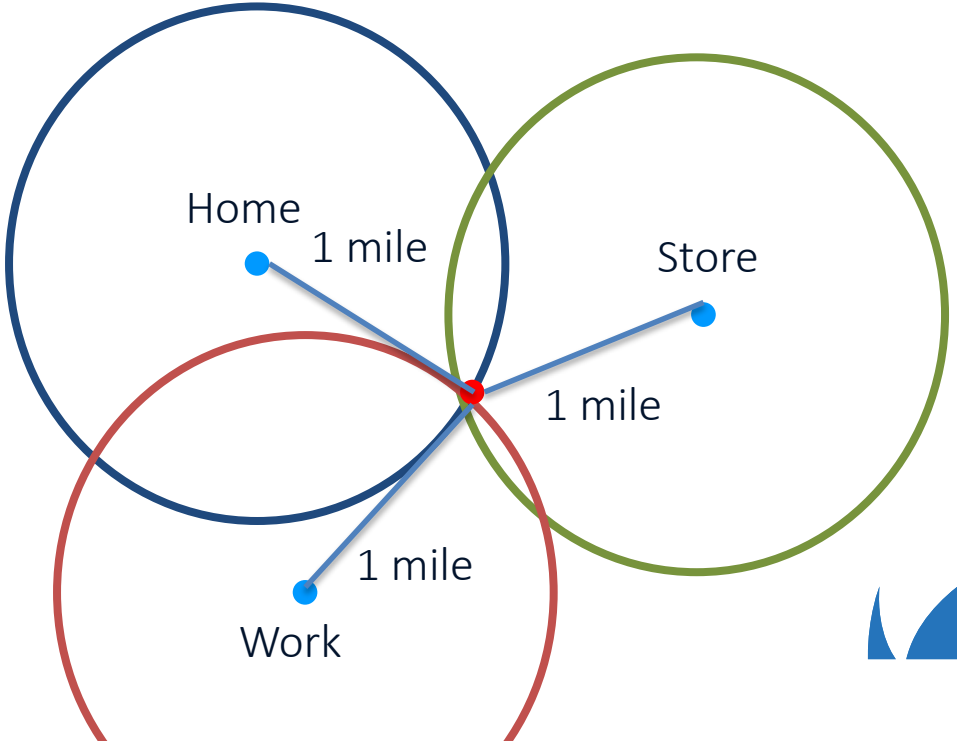
Barracuda

How do you locate a tower?



Barracuda

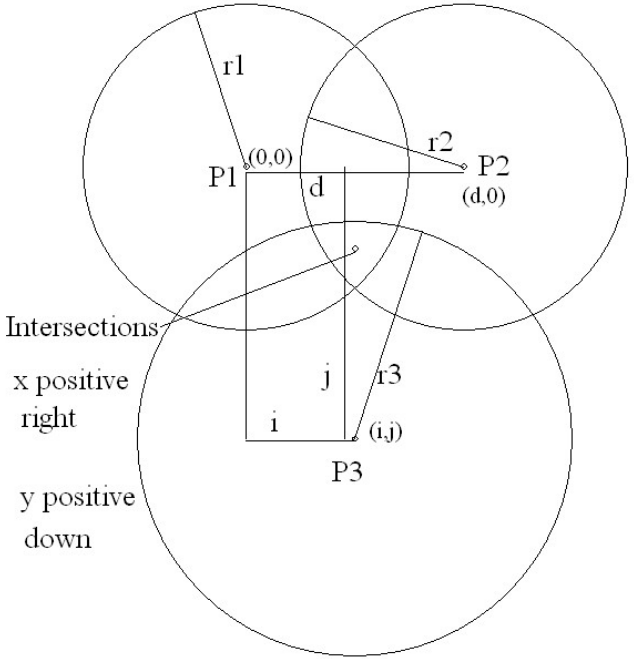
Trilateration



Barracuda

Trilateration

There are scripts that do the math…



Barracuda

How do you locate a tower?

Power is not linear

- More data
- More monitoring nodes
- Back of the envelope math
- Cell towers have different sectors



Barracuda

How do you locate a tower?

Multipoint trilateration

- Drive around collecting lots of data
- Gives you way more accurate results
- Tested on real towers



Barracuda

How do you locate a tower?



Barracuda

What’s the build?

- Raspberry Pi 3, power adapter, SD card (running stock Raspbian)
- SIM900 GSM Module
- Serial GPS module
- Software defined radio (depending where you are)
- *Scrap wood & hot glue*

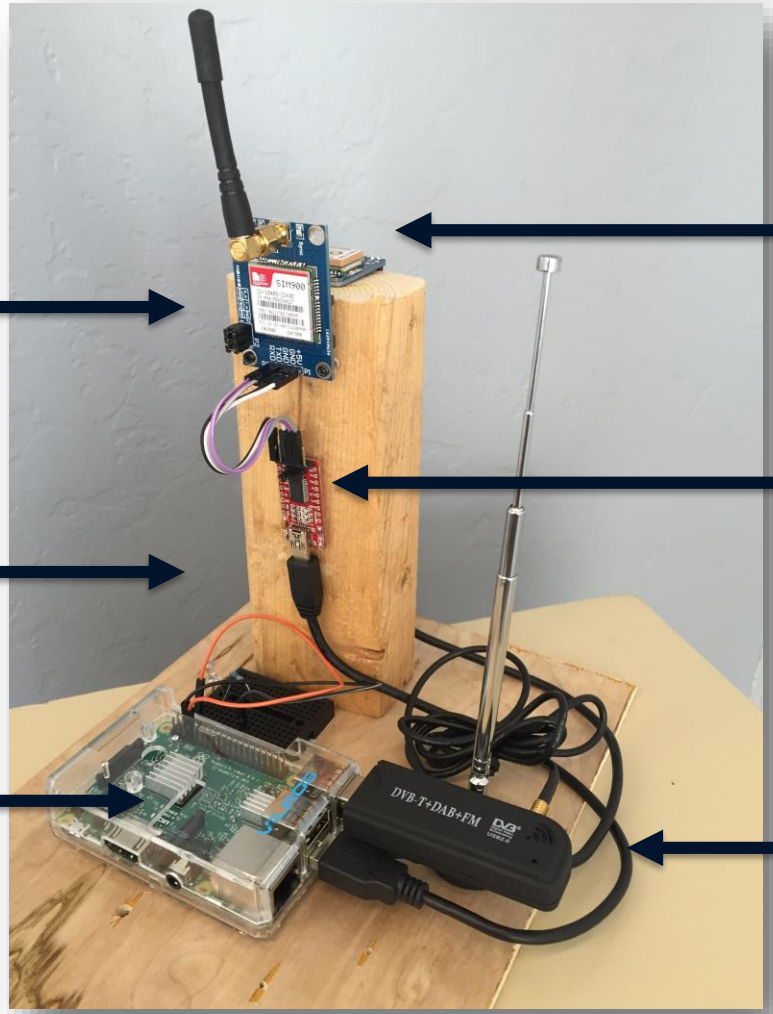


Brace yourself…
this is quite literally a hack.





Barracuda



SIM 900 Cell Module

GPS Module

Serial to USB

Scrap wood & hot glue

Raspberry Pi

Software defined radio (USB TV Tuner)

Barracuda

What's does it cost?

- $10 Raspberry Pi Zero
- $5 Wireless adapter
- $5 USB hub
- $5 SD card (running stock Raspbian)
- $27 SIM900 GSM Module
- $16 Serial GPS module (Optional)
- *Free? Scrap wood & hot glue*

$52 Total

Barracuda

SIM900

- SIM900
- Seven towers with the highest signal
  - Gives you a ton of information via a serial connection
  - No SIM card is required for engineering mode
  - Does not sniff traffic

Read Command **AT+CENG?**	Response Engineering Mode is designed to allow a field engi network information received by a handset, when th idle mode or dedicated mode (that is: with a call act engineer is able to view network interaction for the the handset is currently registered with) or for the n TA returns the current engineering mode. The netw including serving cell and neighboring cells are retu <mode>=1 or <mode>=2. <cell> carry with them c interaction. **+CENG: <mode>,<Ncell>** **[+CENG:** **<cell>,"<arfcn>,<rxl>,<rxq>,<mcc>,<mnc>,<bsic>,<cellid>,<ria>,** **<txp>,<lac>,<TA>"** **<CR><LF>+CENG:** **<cell>,"<arfcn>,<rxl>,<bsic>[,<cellid>],<mcc>,<mnc>,<lac>"…]** **OK**



Barracuda

SIM900 or Field test mode

- Many phones will let you see this information

- iPhones
  - Pretend to dial a number
  - *3001#12345#*
  - Hit call
- Android
  - Field test mode can vary phone to phone
  - Google for apps that let you see this info



SIM900

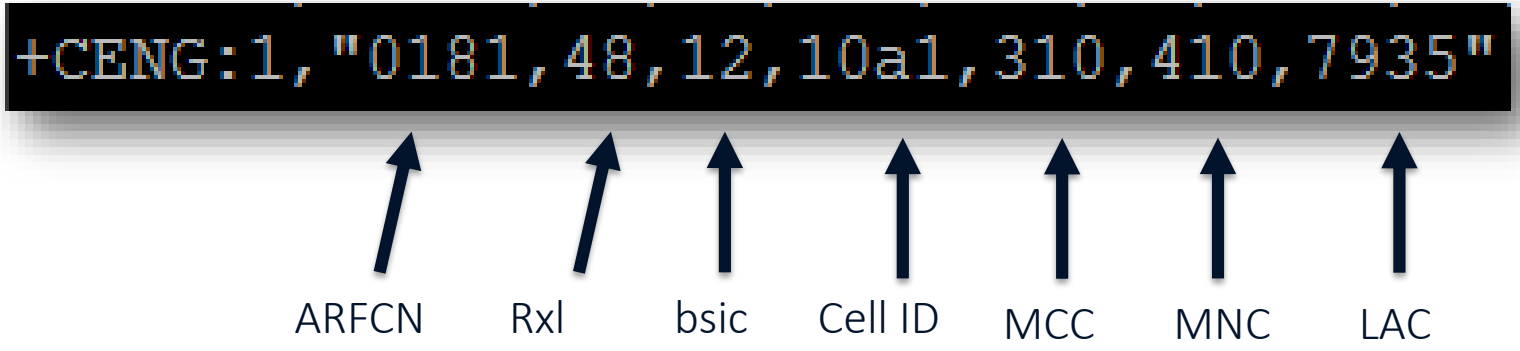
```
AT
OK
AT+CENG=1,1
OK
AT+CENG?
+CENG: 1,1

+CENG:0,"0235,63,99,310,410,36,109f,00,69,7935,255"
+CENG:1,"0181,48,12,10a1,310,410,7935"
+CENG:2,"0239,36,46,0109,310,410,7930"
+CENG:3,"0130,36,169,04d5,310,410,7935"
+CENG:4,"0233,32,180,10a0,310,410,7935"
+CENG:5,"0238,17,165,04d4,310,410,7935"
+CENG:6,"65535,255,00,0000,000,00,0"

OK
```

Barracuda

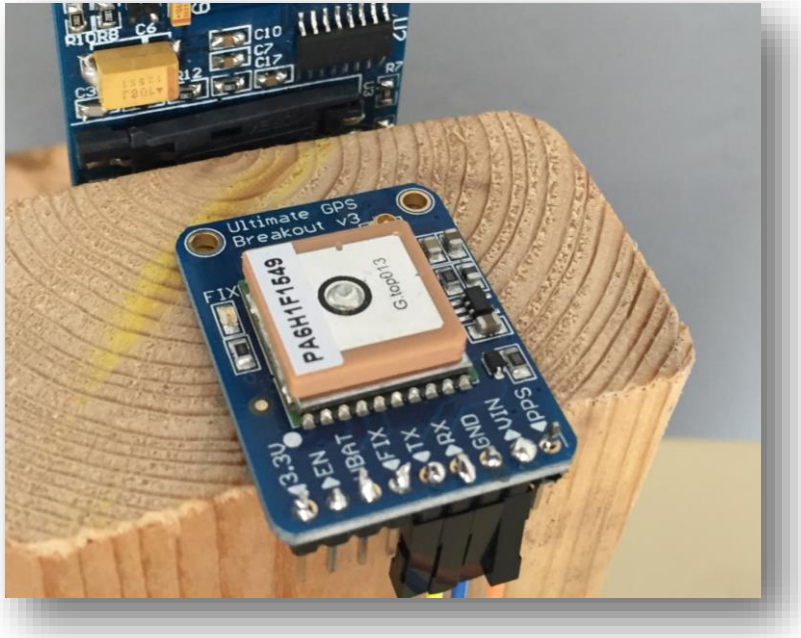
SIM900



Barracuda

GPS Serial

- Adafruit Ultimate GPS module
  - Fixes position quickly.
  - Good indoor reception
  - Works exactly how you would expect



Barracuda

GPS Serial

NMEA Data - National Marine Electronics Association

```
$GPGGA,151331.000,3606.7062,N,11510.2863,W,1,06,1.07,720.1,M,-24.4,M,,*5A
$GPGSA,A,3,17,13,01,15,19,07,,,,,,,1.42,1.07,0.93*07
$GPRMC,151331.000,A,3606.7062,N,11510.2863,W,0.12,237.19,070816,,,A*76
$GPVTG,237.19,T,,M,0.12,N,0.22,K,A*30
$GPGGA,151332.000,3606.7062,N,11510.2864,W,1,06,1.07,720.1,M,-24.4,M,,*5E
$GPGSA,A,3,17,13,01,15,19,07,,,,,,,1.42,1.07,0.93*07
$GPRMC,151332.000,A,3606.7062,N,11510.2864,W,0.27,211.93,070816,,,A*72
$GPVTG,211.93,T,,M,0.27,N,0.51,K,A*34
$GPGGA,151333.000,3606.7061,N,11510.2864,W,1,06,1.07,720.1,M,-24.4,M,,*5C
$GPGSA,A,3,17,13,01,15,19,07,,,,,,,1.42,1.07,0.93*07
$GPRMC,151333.000,A,3606.7061,N,11510.2864,W,0.46,221.19,070816,,,A*76
$GPVTG,221.19,T,,M,0.46,N,0.85,K,A*3B
$GPGGA,151334.000,3606.7060,N,11510.2865,W,1,06,1.07,720.1,M,-24.4,M,,*5B
$GPGSA,A,3,17,13,01,15,19,07,,,,,,,1.42,1.07,0.93*07
$GPRMC,151334.000,A,3606.7060,N,11510.2865,W,0.36,290.36,070816,,,A*71
$GPVTG,290.36,T,,M,0.36,N,0.67,K,A*37
$GPGGA,151335.000,3606.7061,N,11510.2866,W,1,06,1.07,720.0,M,-24.4,M,,*59
$GPGSA,A,3,17,13,01,15,19,07,,,,,,,1.42,1.07,0.93*07
$GPGSV,3,1,11,28,66,346,19,30,64,101,15,17,53,197,25,13,43,293,25*7F
$GPGSV,3,2,11,07,38,118,20,11,30,067,20,19,25,205,29,01,24,086,16*73
$GPGSV,3,3,11,15,16,313,24,08,07,041,,41,,,*72
$GPRMC,151335.000,A,3606.7061,N,11510.2866,W,0.43,297.19,070816,,,A*7A
$GPVTG,297.19,T,,M,0.43,N,0.79,K,A*30
$GPGGA,151336.000,3606.7061,N,11510.2867,W,1,06,1.07,720.0,M,-24.4,M,,*5B
$GPGSA,A,3,17,13,01,15,19,07,,,,,,,1.42,1.07,0.93*07
$GPRMC,151336.000,A,3606.7061,N,11510.2867,W,0.38,40.83,070816,,,A*4F
$GPVTG,40.83,T,,M,0.38,N,0.71,K,A*0F
$GPGGA,151337.000,3606.7062,N,11510.2866,W,1,06,1.07,720.0,M,-24.4,M,,*58
```



GPS Serial

```
$GPGGA,151332.000,3606.7062,N,
```

```
11510.2864,W,1,06,1.07,720.1,M,-24.4,M,,*5E
```

lat	lon	satellite	gps_quality	altitude	altitude_units
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770985	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M
36.84029	-119.770986	8	2	105.1	M

Barracuda

Raspberry Pi 3

- Stock Raspbian OS (debian for pi)
- Pi 3 has enough power to run a SDR
- Has four USB ports for serial adapters
- Easily powered by a USB battery pack



Barracuda

TV Tuner

- $20 Software defined radio
- Wide range of frequencies
- Github: Gr-Gsm
  - Can listen to raw GSM traffic***
  - See all the raw frames
  - Not necessary for locating cell towers
  - Provides deeper insights



WARNING!!!

Barracuda

Data collection:

- Everything dumps to a SQLite database for later use

```
lect * from CellData;
  time        arfcn       rxl         mcc         mnc         bsic        cellid      lac         l
  ----------  ----------  ----------  ----------  ----------  ----------  ----------  ----------  -
  1467249192  0694        14          310         260         35          1799        12c         3
  1467249192  0696        16          310         260         28          1cf3        12c         3
  146724919   lat         lon         satellite   gps_quality altitude    altitude_units 12c      3
  146724919   ----------  ----------  ----------  ----------  ----------  -------------- 12c      3
  146724919   36   029    -119.   1985 8           2           105.1       M              0        3
  146724919   36   029    -119.   1985 8           2           105.1       M              0        3
  146724919   36   029    -119.   1985 8           2           105.1       M              0        3
  146724920   36   029    -119.   1985 8           2           105.1       M              12c      3
  146724920   36   029    -119.   1985 8           2           105.1       M              12c      3
  146724920   36   029    -119.   1985 8           2           105.1       M              12c      3
  146724920   36   029    -119.   1985 8           2           105.1       M              12c      3
  146724920   36   029    -119.   1986 8           2           105.1       M              0        3
  146724920   36   029    -119.   1986 8           2           105.1       M              0        3
  146724920   36   029    -119.   1986 8           2           105.1       M              0        3
  146724921   36   029    -119.   1986 8           2           105.1       M              12c      3
  146724921   36   029    -119.   1986 8           2           105.1       M              12c      3
              36   029    -119.   1986 8           2           105.1       M
              36   029    -119.   1986 8           2           105.1       M
              36   029    -119.   1986 8           2           105.1       M
```

Barracuda

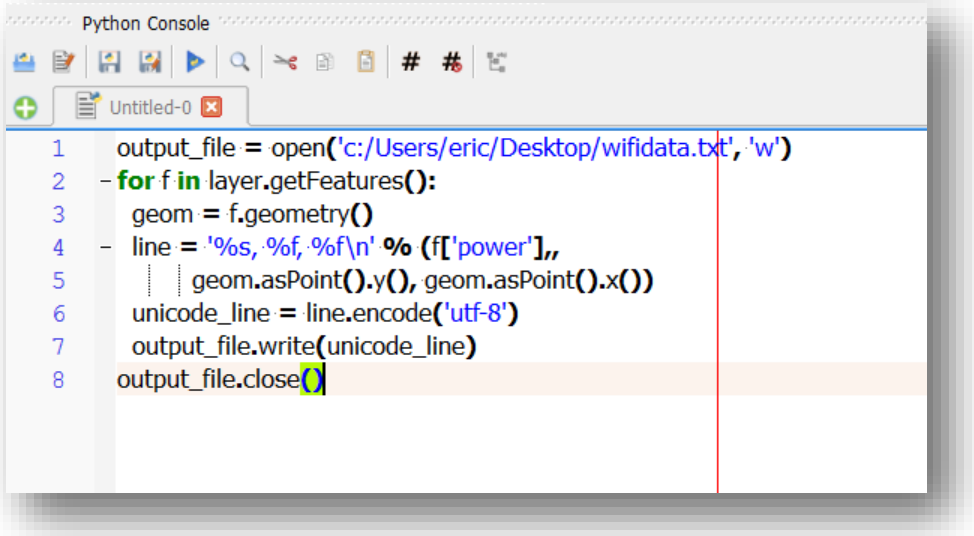
Let’s make it pretty:

- QGIS
  - Free and Open Source Geographic Information System
  - IDW – Inverse Distance Weighting
  - OpenLayers Plugin – Maps & GIS data
  - Python command line automation
  - Makes it very easy to visualize

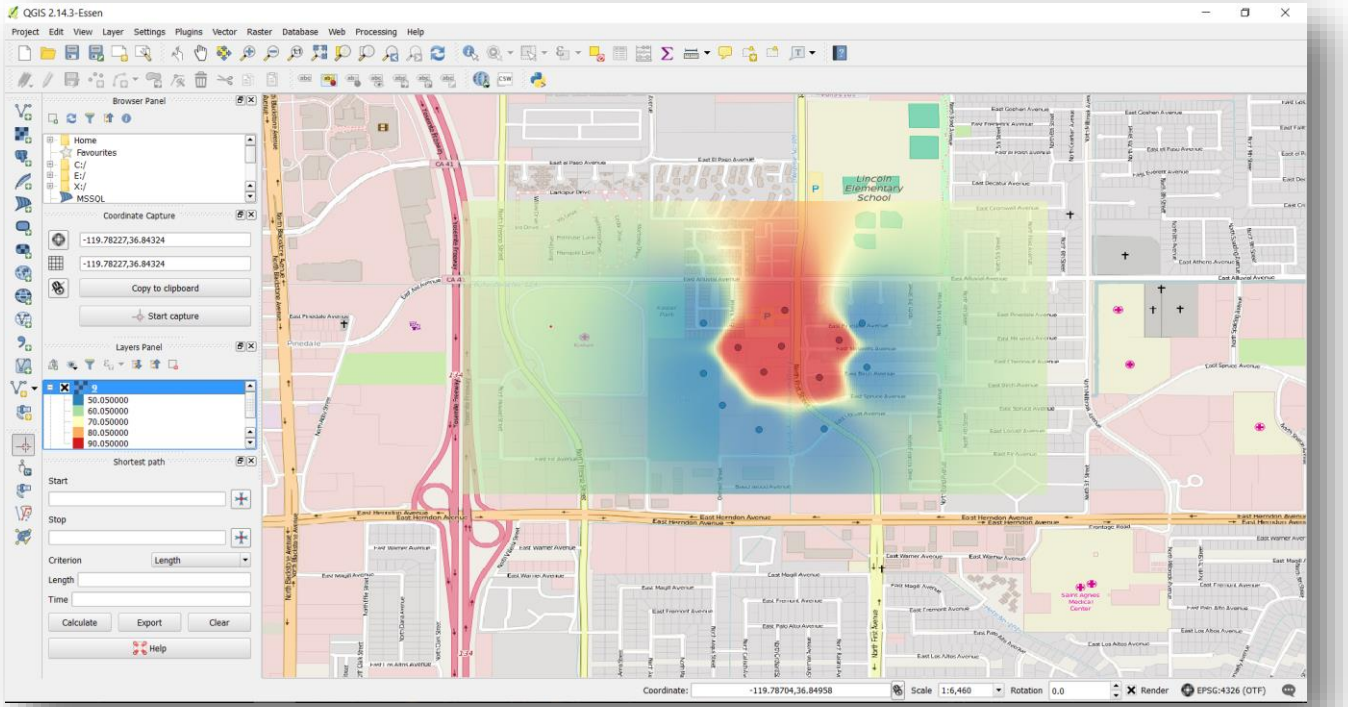


Let’s make it pretty:

- QGIS Python Console
  - Once you’re comfortable making maps manually you can begin automatically generating them



Let’s make it pretty:



There’s a disturbance in the force

- How do you get alerts?
  - Email
  - SMS - Twilio
  - Push notifications - PushOver



There’s a disturbance in the force

- Your detector goes off now what?
  - Turn off your phone
  - Start looking at the data
  - Go on a road trip



Want to help?
Questions?

defconjusticebeaver@gmail.com

RagingSecurity.Ninja

