# Joshua Schroeder

Meeting People via Wifi

@JoshInGeneral

JoshInGeneral@gmail.com

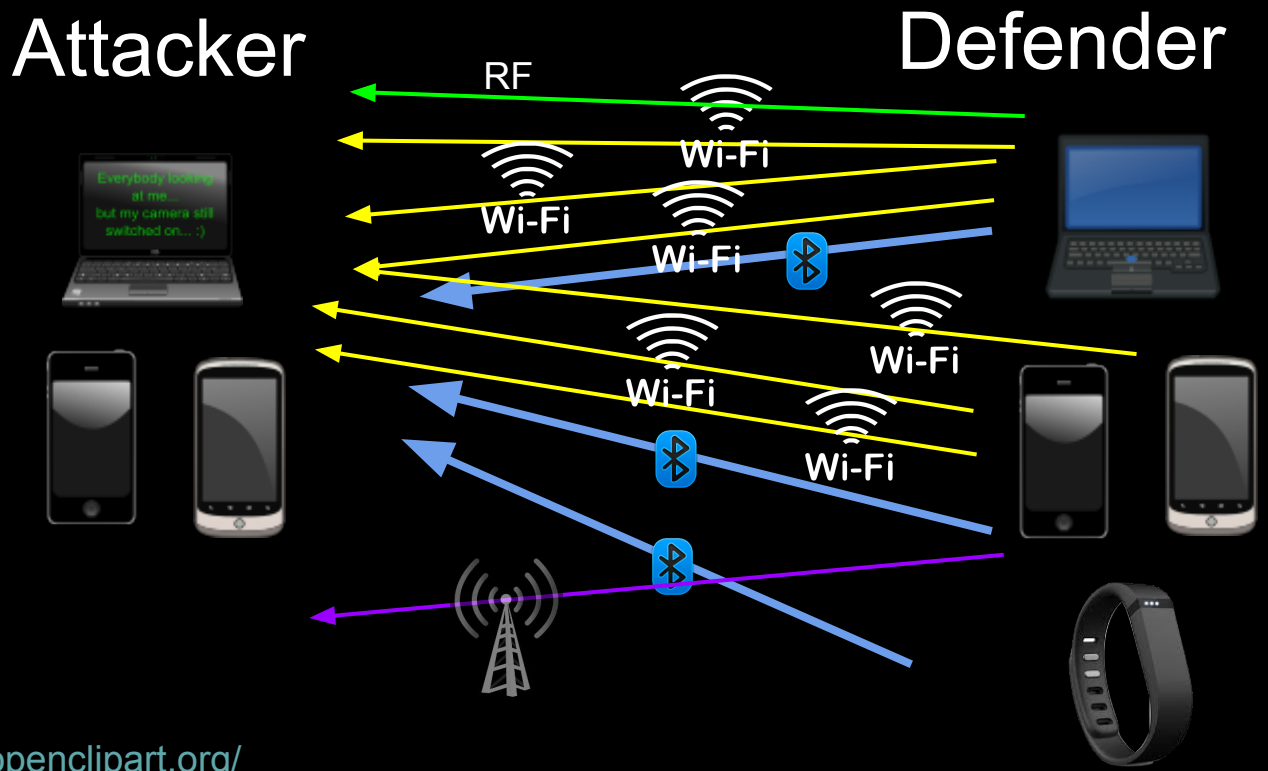
# About JoshInGeneral


- NovaHacker ~3 years
- From NC, UNCC,
  49th Security Division
- Most research in Web Vulnerabilities,
  Dabble in Legal, CCTV hacking, 3rd Year
  WCTF
- Currently work doing IR in NoVA
- Research not related to job

# Agenda

- Overview
- Wifi
  - Hardware and Software needed
  - Attribution
  - Tips for Protection
- BlueTooth
  - Hardware and Software needed
  - Attribution
  - Tips for protection

# Overview




Source: https://openclipart.org/

# YOU LOSE

You can’t hide your signals...

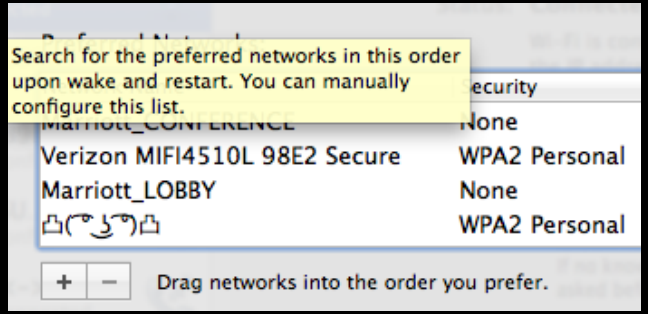
# Overview: Bluetooth Scanning for Device Association

- Discovery mode name, MAC etc
- Good OPSEC, just sniff no connect
- Use decibel to hone in (closer to 0, closer you are)
- Low Energy (Battery) vs Classic
- Most common devices:
  Fitbits, iPhones, Androids, Entertainment systems

Source: http://www.vivapets.com/upload/Image/snifferdog.jpg

# Overview: Wifi Scanning for Device Association

- Previous APs stored in list
- Search for APs they broadcast SSID
- We can pick this up via sniffing tools
- SSID names give away home, work or friends networks



# Hardware Needed - Wifi

Alfa 1000mW 1W 802.11b/g USB Wireless WiFi Network Adapter - RTL8187


Source: http://www.amazon.com/gp/product/B001O9X9EU

# Hardware Needed - Wifi

Showing Today on Linux and Android + OTG Adapter


Source: http://www.amazon.com/UCEC-USB-2-0-Adapter-Plug/dp/B00WHWKD60

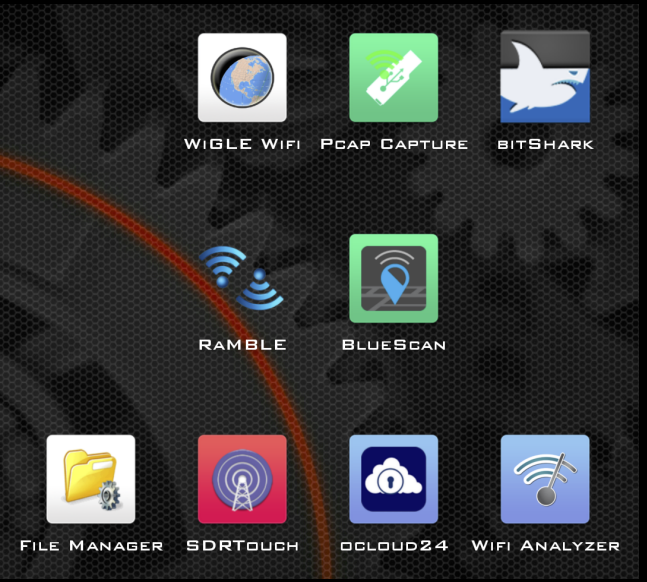
# Software Needed - Wifi

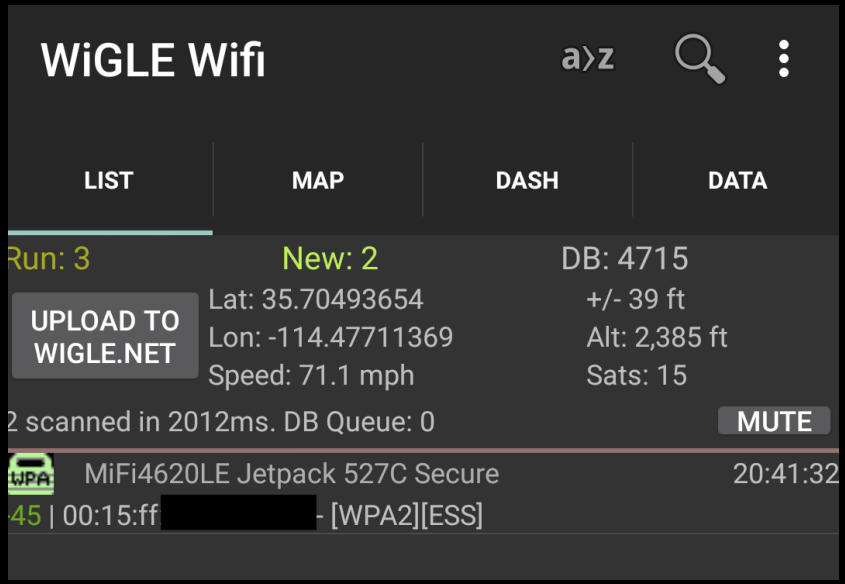
- Wiggle Wifi (Android)
- PCAP Scanner (Android)
- BitShark Share (Android)

- Kismet ( Linux | Win)
- Aircrack-ng ( Linux | Win )
- On Mac just use a VM

- Wireshark/tcpdump (Mac | Linux | Win)

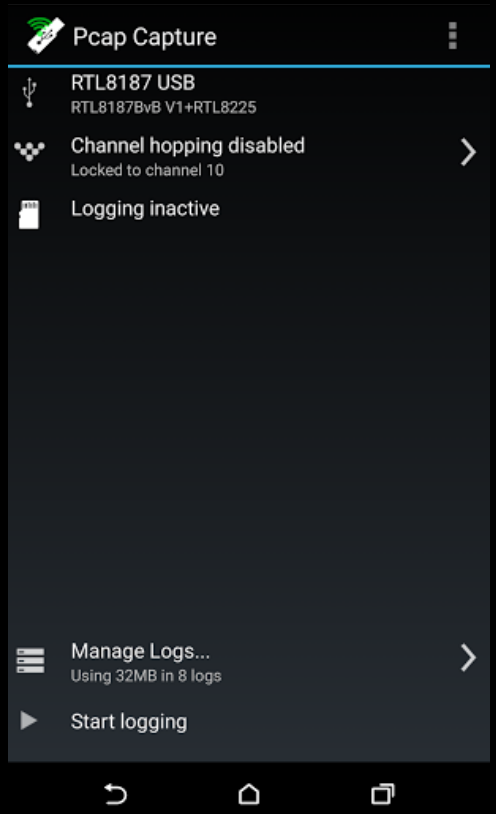
# Software Needed - WiGLE Wifi

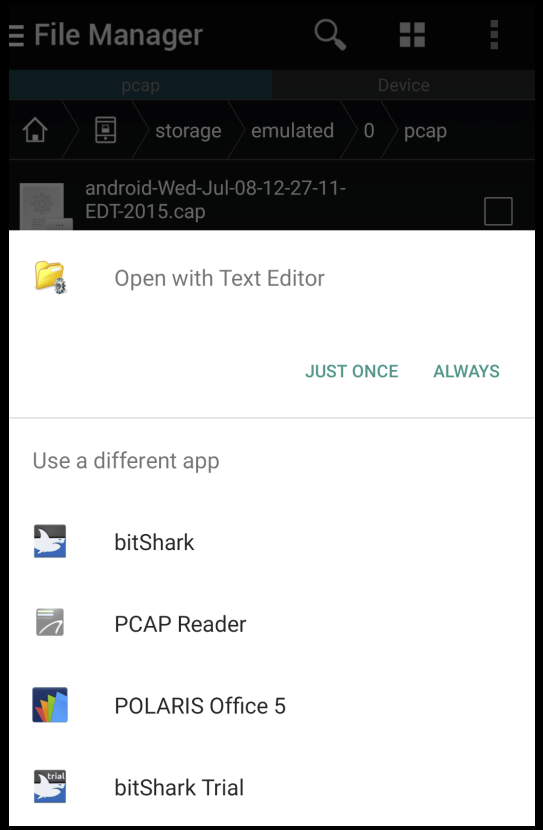


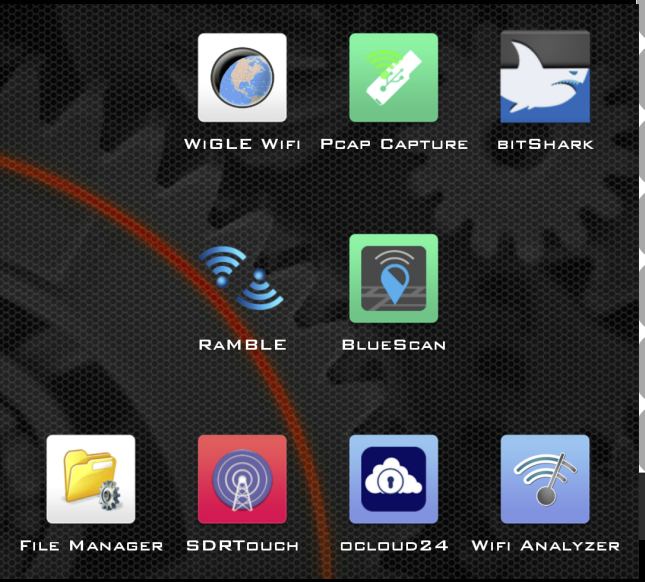
# Software Needed - WiGLE Wifi

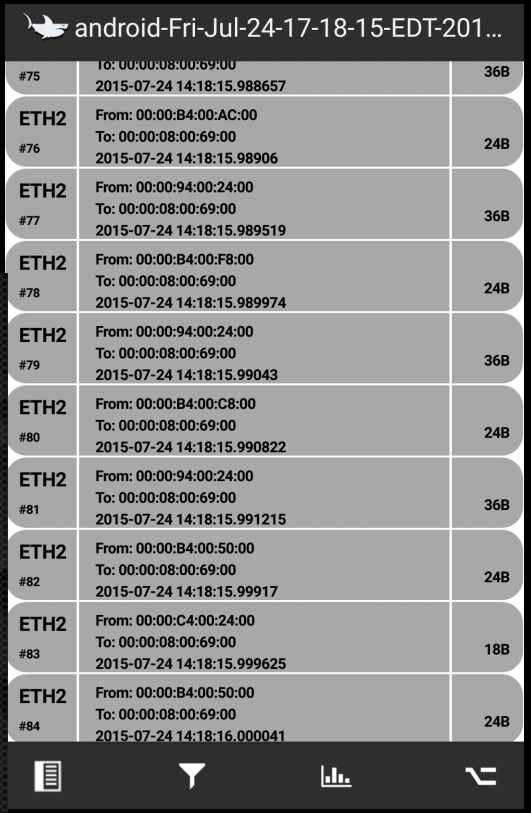
# Software Needed - PCAP Scanner

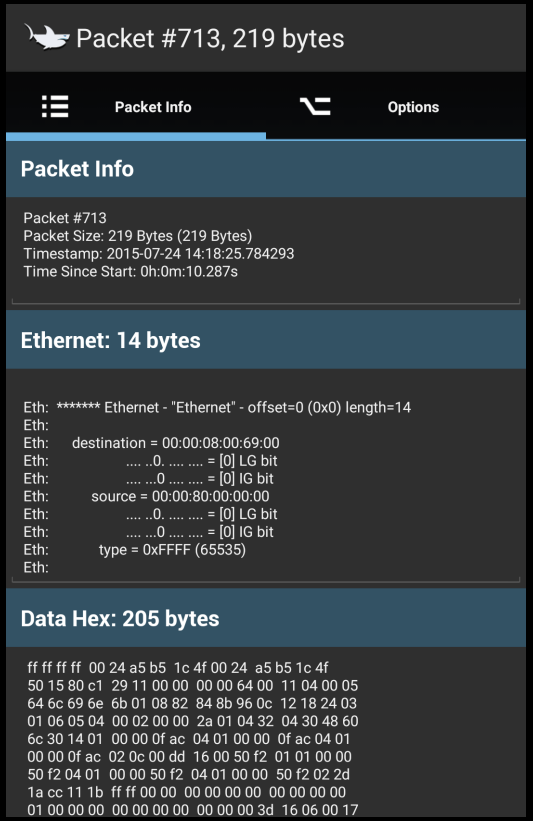



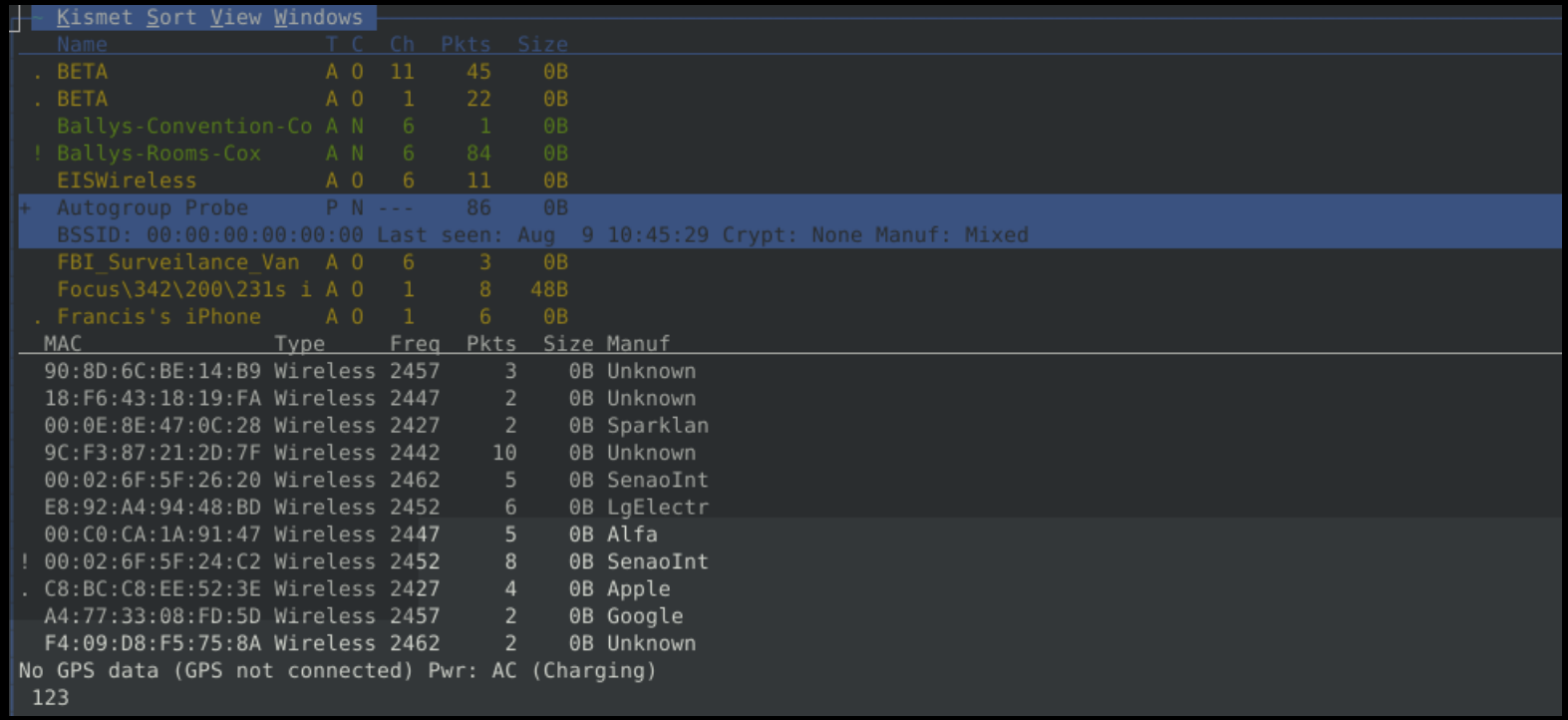
# Software Needed - BitShark Scanner



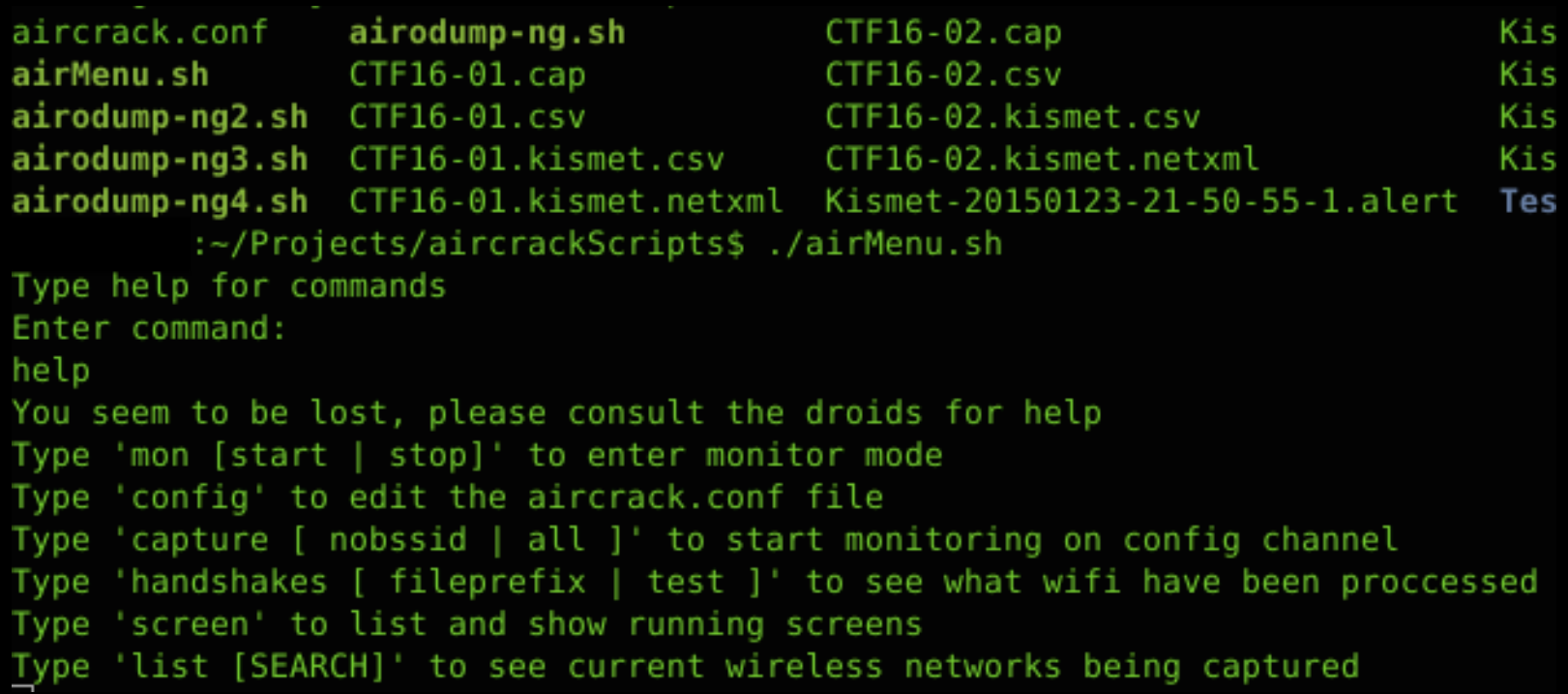



# Software Needed - Kismet



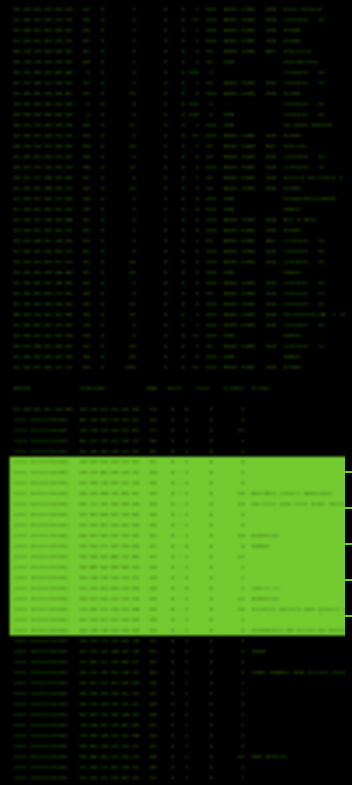
# Software Needed - Aircrack-ng



# Software Needed - Aircrack-ng

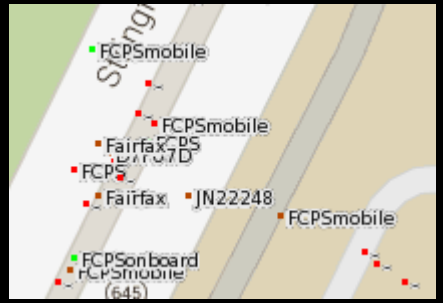
```
We are now starting to monitor the lasers
CHANNEL:11
BSSID:00:26:62:9E:25:FA
FILEPREFIX:test3
config load error
[sudo] password for ael:
Sorry, try again.
[sudo] password for ael:


X[PHY]Interface Driver[Stack]-FirmwareRev       Chipset                                                 E

K[phy0]wlan0    ath9k[mac80211]-N/A             Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
K[phy0]wlan0mon ath9k[mac80211]-N/A             Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)

interfaces:wlan0 wlan0mon
ath9k=Internal Card Asus
rtl8187=Alfa Card Asus
count:2
Attempting to start monitoring...
Checking interface named: wlan0
Checking interface named: wlan0mon
Loop done, showing results:


X[PHY]Interface Driver[Stack]-FirmwareRev       Chipset                                                 E

K[phy0]wlan0    ath9k[mac80211]-N/A             Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
K[phy0]wlan0mon ath9k[mac80211]-N/A             Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)

interfaces:wlan0 wlan0mon
count:2
```

# Attribution Wifi - FairFax County

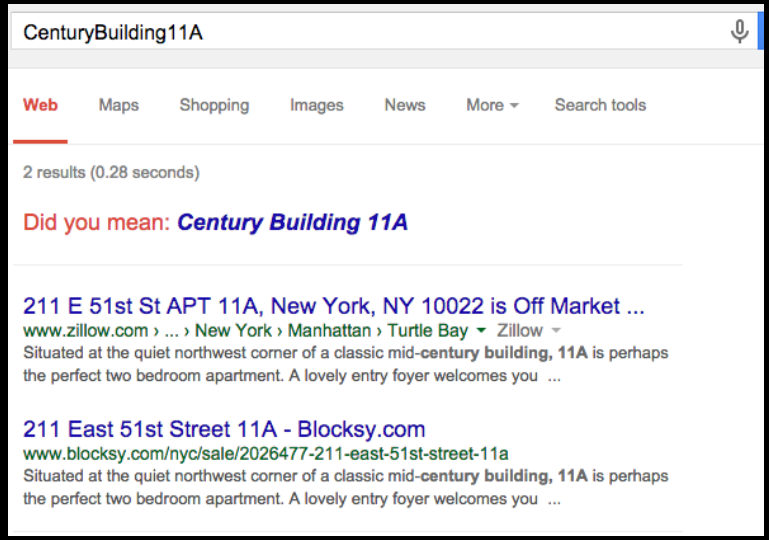


FC:0A:81:A7:2A:B8 64:C6:67:21:46:60 -76 0 - 6 3 3
(not associated) BC:20:A4:78:65:FC -52 0 - 1 0 2
(not associated) 20:7D:74:38:2F:DC -71 0 - 1 0 12
(not associated) BC:4C:C4:C7:4E:7F -80 0 - 1 0 1
(not associated) 8C:3A:E3:18:77:54 -81 0 - 1 0 3
(not associated) 3E:6F:39:43:12:A2 -81 0 - 1 0 3
(not associated) F0:25:B7:4A:1A:7F -83 0 - 1 0 4
(not associated) 92:68:C3:03:5C:19 -84 0 - 1 0 3
(not associated) E8:50:8B:36:BF:31 -84 0 - 1 0 18 BestBuy,ronali,WPATubez
(not associated) A4:77:33:08:FD:5D -84 0 - 1 0 24 Verizon SCH-LC11 9f61 Secure
(not associated) 4C:BC:A5:37:40:D5 -85 0 - 1 0 6
(not associated) 9C:F3:87:55:6C:EF -85 0 - 1 0 3
(not associated) 00:02:6F:5F:29:00 -87 0 - 1 0 16 EnGenius
(not associated) 68:09:27:AA:AE:FA -87 0 - 6 0 8 PARIS
(not associated) 90:8D:6C:BE:14:B9 -87 0 - 1 0 12
(not associated) 90:B6:86:DE:D0:29 -88 0 - 1 0 2
(not associated) E0:CB:1D:58:79:3F -88 0 - 5 0 1
(not associated) FC:0A:81:D9:75:A0 -89 0 - 6 0 1 smart-rf
(not associated) 00:02:6F:5F:26:20 -89 0 - 1 0 21 EnGenius
(not associated) C8:AA:21:1A:13:6B -89 0 - 1 0 10 attwifi,belkin.4b4.guests,ccc-wifi,CoffeeBeanWiFi
(not associated) A4:4E:31:92:98:98 -89 0 - 1 0 7
(not associated) E0:CB:1D:99:29:4A -89 0 - 1 0 4 FCPSGuest,HP-Print-92-Photosmart 6520,FCCPub
CenturyBuilding11A

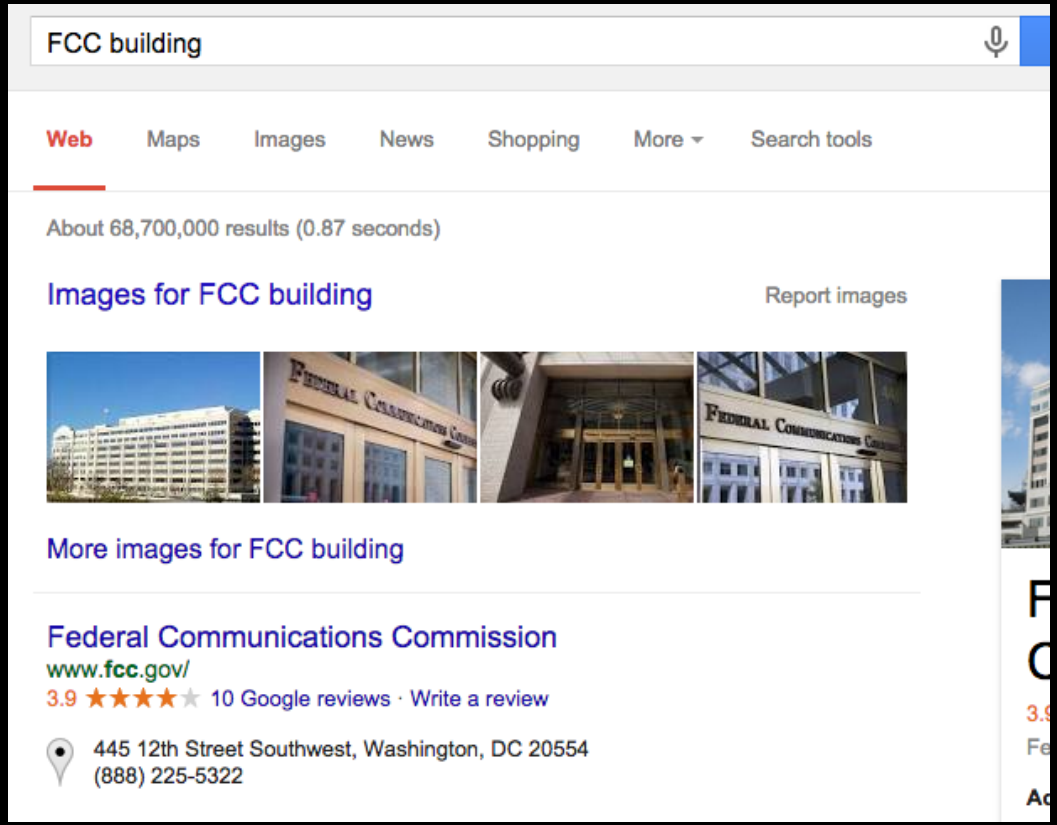
# Attribution Wifi - FairFax County



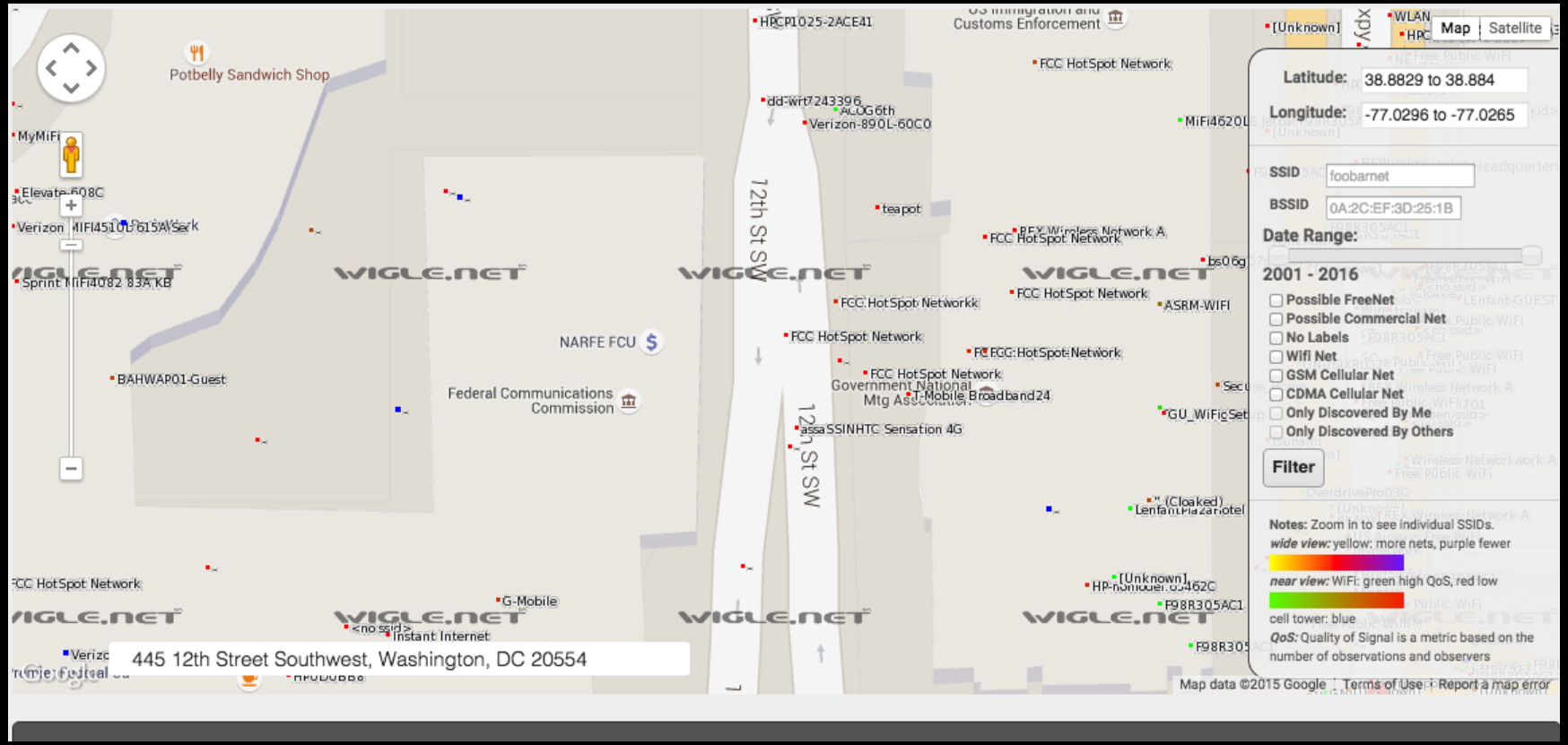

| | | |
|---|---|---|
| 1 | **School Board Room at Jackson Middle**<br>profile \| home page \| map \| special programs | 3020 Gallows Rd<br>Falls Church, VA 22042 |
| 2 | **Gunston Alternative School - South County Juvenile Court**<br>profile \| home page \| map \| special programs | 8350 Richmond Hwy<br>Suite 119<br>Alexandria, VA 22309 |
| 3 | **Hillwood School - East County Juvenile Court**<br>profile \| home page \| map \| special programs | 2812 Old Lee Hwy<br>Suite 100<br>Fairfax, VA 22031 |
| 4 | **Chantilly High School Academy**<br>profile \| home page \| map | 4201 Stringfellow Rd<br>Chantilly, VA 20151 |



# Attribution Wifi - FCC



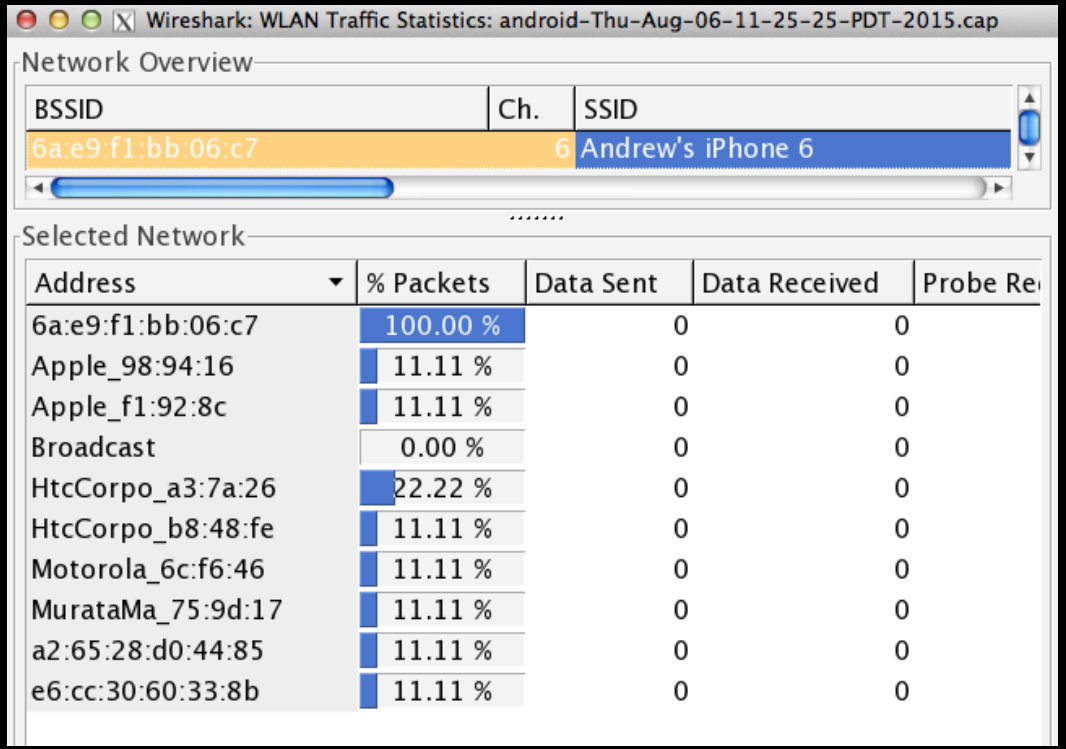
# Attribution Wifi - FCC



# Software Needed - Wireshark/tcpdump

Statistics -> WLAN Summary

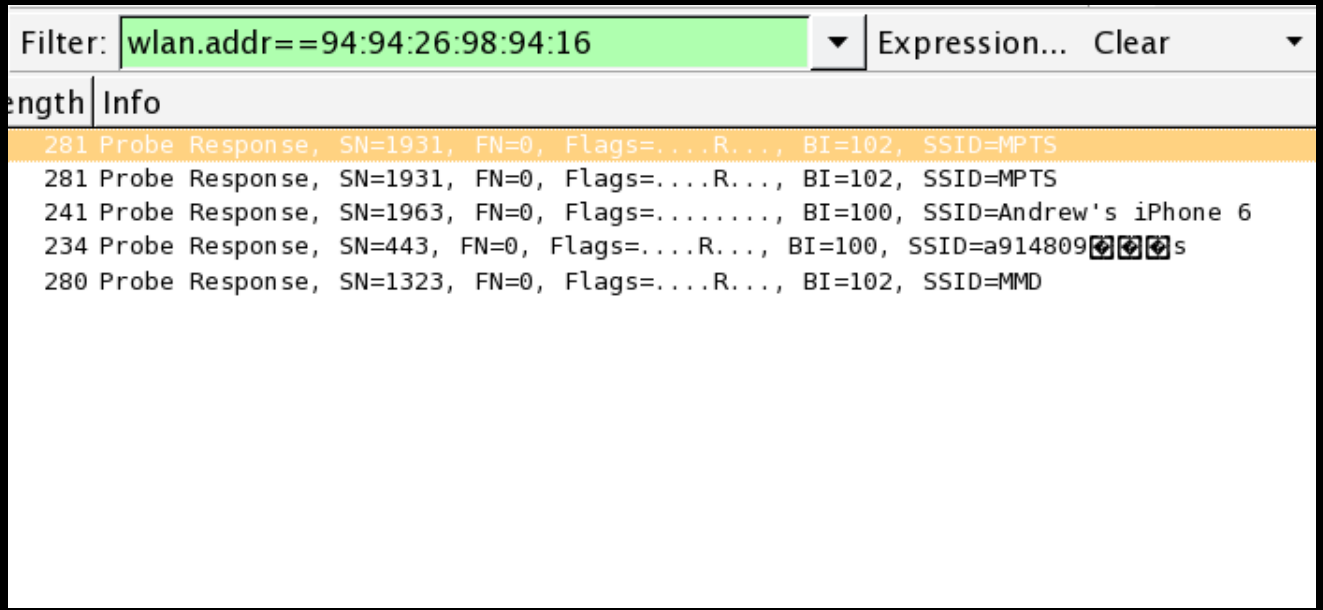
Make a filter for the MAC



# Software Needed - Wireshark/tcpdump

Statistics -> WLAN Summary

Make a filter for the MAC



# Software Needed - Wireshark/tcpdump

```
0x0040:  8c92 98a4 b0c8 e0ec 0301 0b05 0400 0200  ................
0x0030:  0000 0104 0204 0b16 3208 0c12 1824 3048  ........2....$0H
0x0040:  606c 0301 0b2d 1a21 0017 ff00 0000 0000  `l...-.!........
0x0030:  05b1 5f71 0100 0000 2c01 1104 0011 4154  .._q....,.....AT
0x0040:  542d 484f 4d45 4241 5345 2d38 3836 3001  T-HOMEBASE-8860.
0x0030:  805b fb2d 0200 0000 6400 3104 0000 0108  .[.-....d.1.....
0x0040:  8c92 98a4 b0c8 e0ec 0301 0b05 0400 0200  ................
0x0030:  80d1 1154 0100 0000 6400 2104 0006 4241  ...T....d.!...BA
0x0040:  4c4c 5953 0108 8c92 98a4 b0c8 e0ec 0301  LLYS............
0x0030:  8011 95ea 0100 0000 6400 2104 0005 5041  ........d.!...PA
0x0040:  5249 5301 088c 9298 a4b0 c8e0 ec03 010b  RIS.............
0x0030:  80e3 8586 0000 0000 6400 3104 0005 414c  ........d.1...AL
0x0040:  5048 4101 088c 9298 a4b0 c8e0 ec03 010b  PHA.............
0x0030:  8091 7c12 7007 0000 6400 1184 0005 414c  ..|.p...d.....AL
0x0040:  5048 4101 078c 1824 3048 606c 0301 0b05  PHA....$0H`l....
0x0030:  8033 1254 0100 0000 6400 3104 0005 414c  .3.T....d.1...AL

:~$ tcpdump -nnr Kismet-20150809-10-43-34-1.pcapdump | egrep "0x0030|0x0040"
```

# Software Needed - BlueTooth

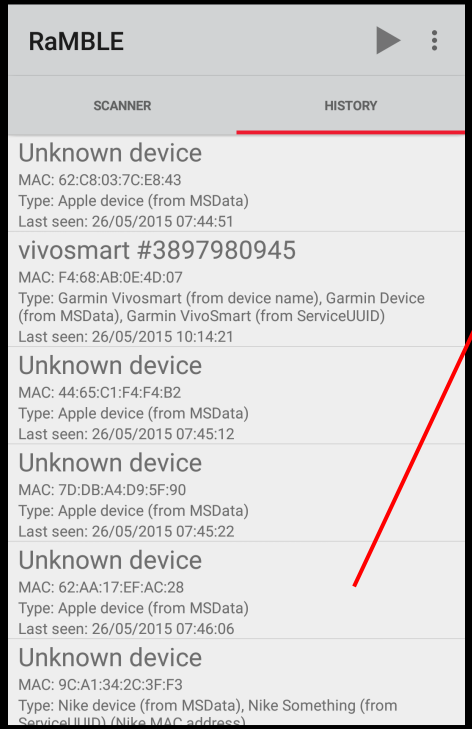
- Ramble (Android)
- BlueScan (Android)
- Bluetooth Smart Tool (iPhone)

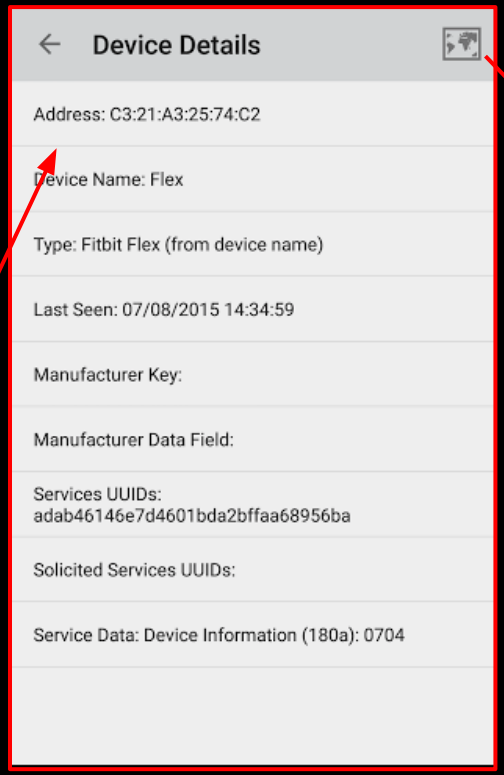
- Kali: hcitool lescan

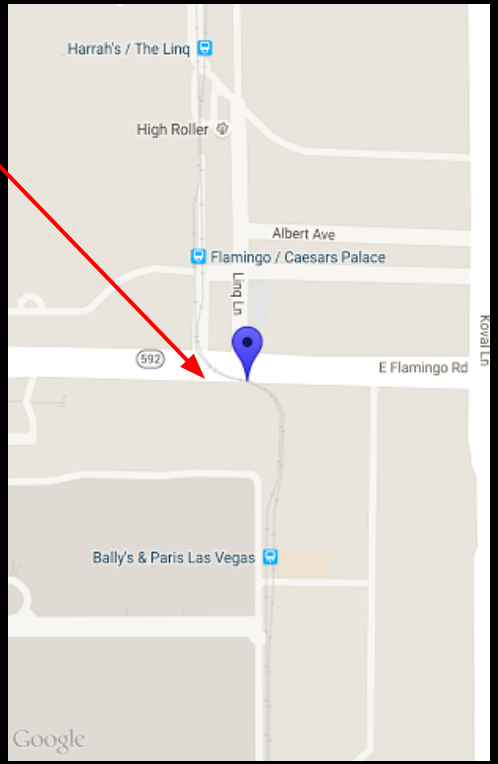
# Hardware Needed - BT UberTooth


Source: http://www.amazon.com/UCEC-USB-2-0-Adapter-Plug/dp/B00WHWKD60

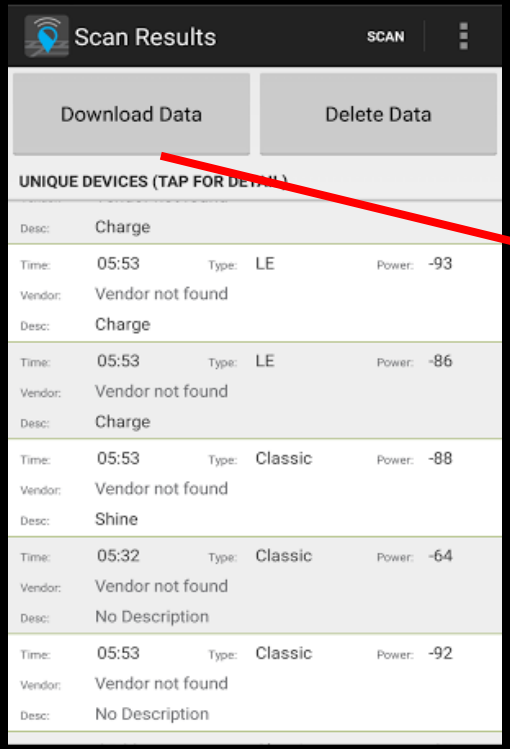
# Software Needed - Ramble



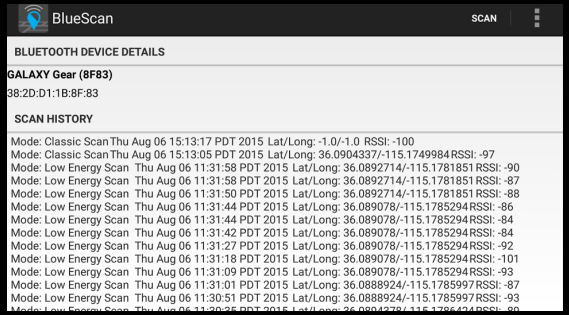



# Software Needed - BlueScan







# Software Needed - BlueScan

Get All Data by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8

Find MAC by Time
cat bluescan.json | egrep 143842.* -B3 -A8 | egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq

TIME by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8 | egrep "[0-9]{10}" -o | head -n1| xargs date -r

Find Bluetooth Type
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8


"local_mac": "2C:8A:72:19:17:86",
"device_type": "1",
"id": "3",
"mac": "5C:58:03:B1:EB:7D",
"company": "",
"date_seconds": "1438428920509",
"timestamp": "1438428983124",
"latitude": "39.1802517",
"longitude": "-76.6721928",
"altitude": "22.0",
"provider": "fused",
"rssi": "-96"


Source: http://www.epochconverter.com/

# Software Needed - Epochconverter

Get All Data by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8

Find MAC by Time
cat bluescan.json | egrep 143842.* -B3 -A8 | egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq

TIME by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8 | egrep "[0-9]{10}" -o | head -n1| xargs date -r

Find Bluetooth Type
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8

The **Unix epoch** (or **Unix time** or **POSIX time** or **Unix timestamp**) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT), not counting leap seconds (in ISO 8601: 1970-01-01T00:00:00Z).

Source: http://www.epochconverter.com/

# Software Needed - Epochconverter

Get All Data by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8

Find MAC by Time
cat bluescan.json | egrep 143842.* -B3 -A8 | egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq

TIME by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8 | egrep "[0-9]{10}" -o | head -n1| xargs date -r

Find Bluetooth Type
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8



Source: http://www.epochconverter.com/

# Software Needed - BlueScan

Get All Data by MAC
```
cat bluescan.json | egrep 5C:58:03 -B3 -A8
```

Find MAC by Time
```
cat bluescan.json | egrep 143842.* -B3 -A8 |
egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:
[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq
```

TIME by MAC
```
cat bluescan.json | egrep 7C:C3:C8 -B3 -A8 |
egrep "[0-9]{10}" -o | head -n1| xargs date -r
```

Find Bluetooth Type
```
macs=$(cat macs.lst | egrep Apple | awk
'{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat
bluescan.json | egrep $macs -B3 -A8
```

2C:8A:72
49:A1:FA
54:05:FE
5C:58:03
6F:F7:F4
7C:C3:C8

Source: http://www.epochconverter.com/

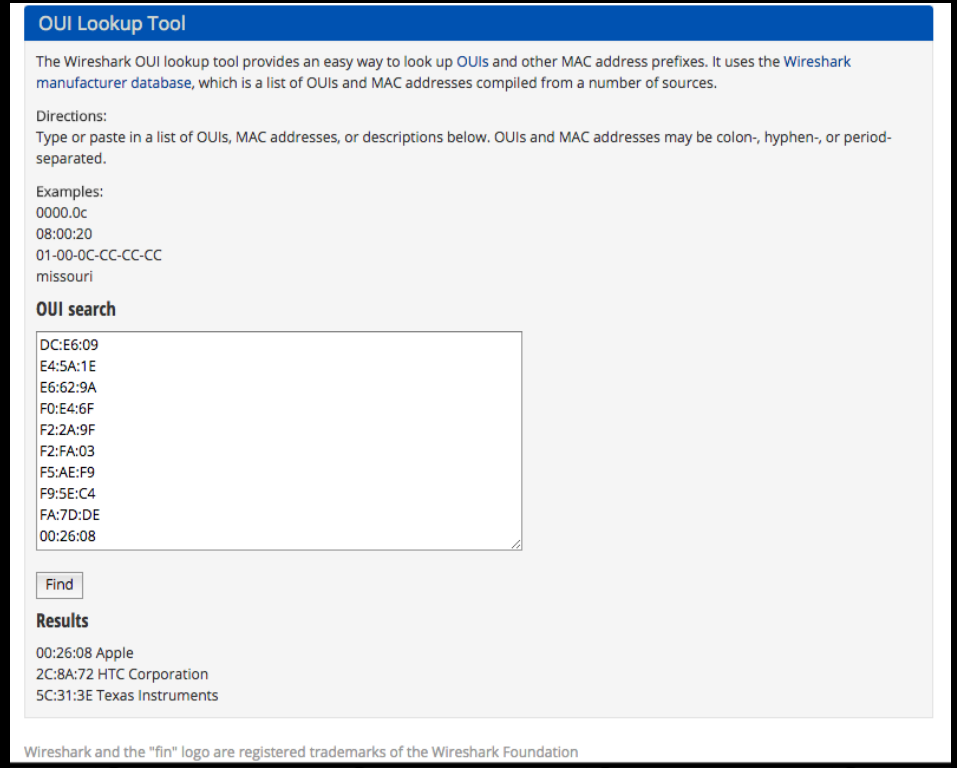
# Software Needed - WireShark

Get All Data by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8

Find MAC by Time
cat bluescan.json | egrep 143842.* -B3 -A8 | egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq

TIME by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8 | egrep "[0-9]{10}" -o | head -n1| xargs date -r

Find Bluetooth Type
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8




Source: https://www.wireshark.org/tools/oui-lookup.html | https://code.wireshark.org/review/gitweb?p=wireshark.git;a=blob_plain;f=manuf

# Software Needed - Meet BlueScan

Get All Data by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8

Find MAC by Time
cat bluescan.json | egrep 143842.* -B3 -A8 |
egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq

TIME by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8 |
egrep "[0-9]{10}" -o | head -n1| xargs date -r

Sat Aug  1 04:35:20 MST 2015

Find Bluetooth Type
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8

Source: https://www.wireshark.org/tools/oui-lookup.html | https://code.wireshark.org/review/gitweb?p=wireshark.git;a=blob_plain;f=manuf

# Software Needed - Meet BlueScan

Get All Data by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8

Find MAC by Time
cat bluescan.json | egrep 143842.* -B3 -A8 | egrep mac | egrep "\"[A-F0-9]{2}:[A-F0-9]{2}:[A-F0-9]{2}" -o | sed -e 's/\"//' | sort | uniq

TIME by MAC
cat bluescan.json | egrep 5C:58:03 -B3 -A8 | egrep "[0-9]{10}" -o | head -n1| xargs date -r

Find Bluetooth Type
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8

```
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8
        "local_mac": "2C:8A:72:19:17:86",
        "device_type": "1",
        "id": "20",
        "mac": "00:26:08:CD:0B:41",
        "company": "Apple, Inc",
        "date_seconds": "1438747584608",
        "title": "fire",
        "timestamp": "1438748098395",
        "latitude": "36.0143379",
        "longitude": "-114.7530405",
        "altitude": "457.0",
        "provider": "fused",
```

Source: https://www.wireshark.org/tools/oui-lookup.html | https://code.wireshark.org/review/gitweb?p=wireshark.git;a=blob_plain;f=manuf

# Software Needed - Bluetooth Mapping

- Unlike Wiggle Wifi bluetooth data no good geo database
- With a little json > csv parsing we can do it ourself
- In this example google maps was our choice

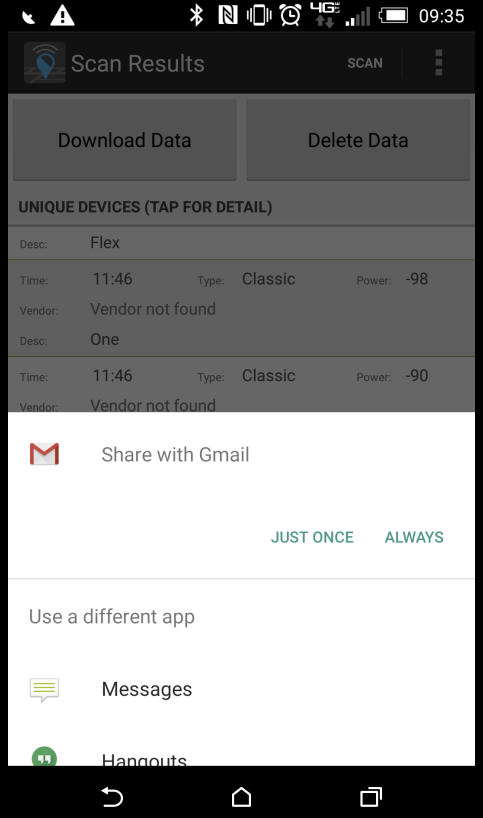
# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps

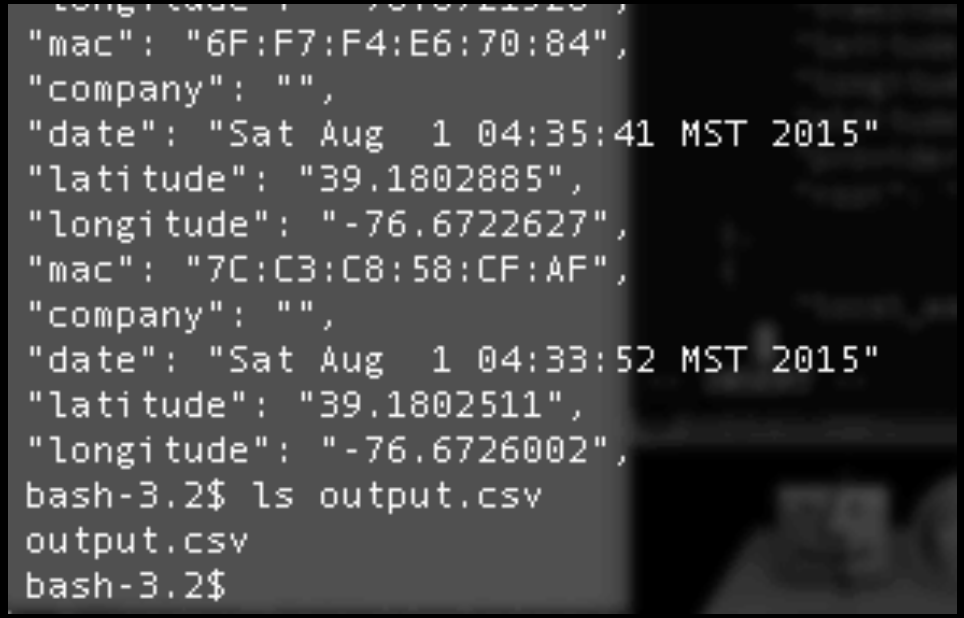
# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



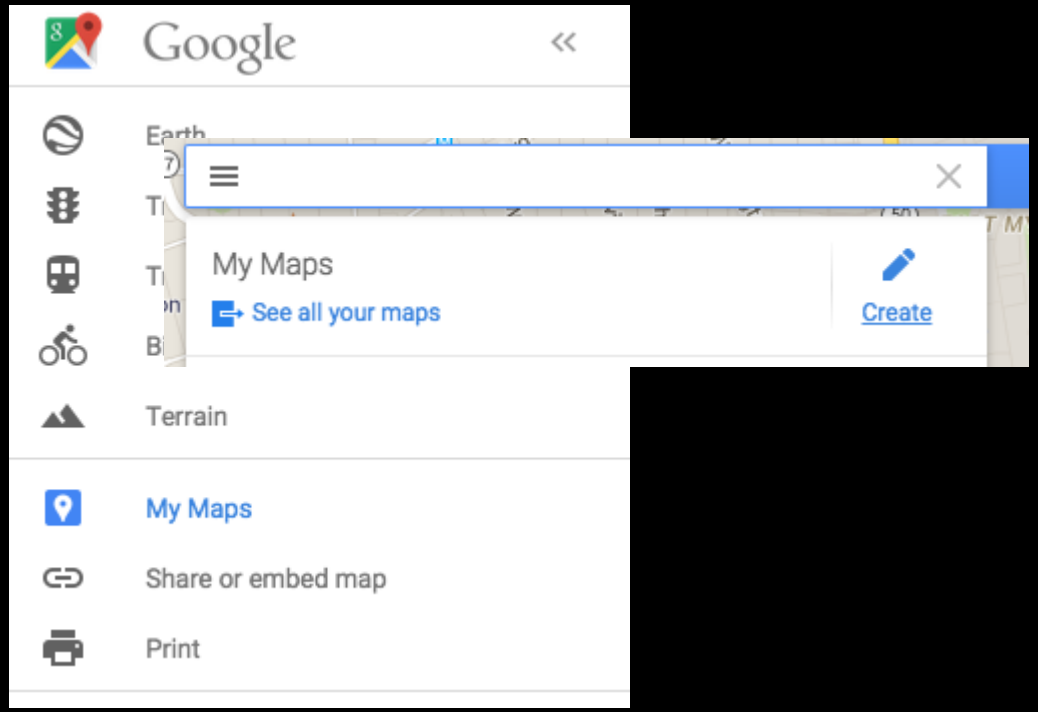
# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



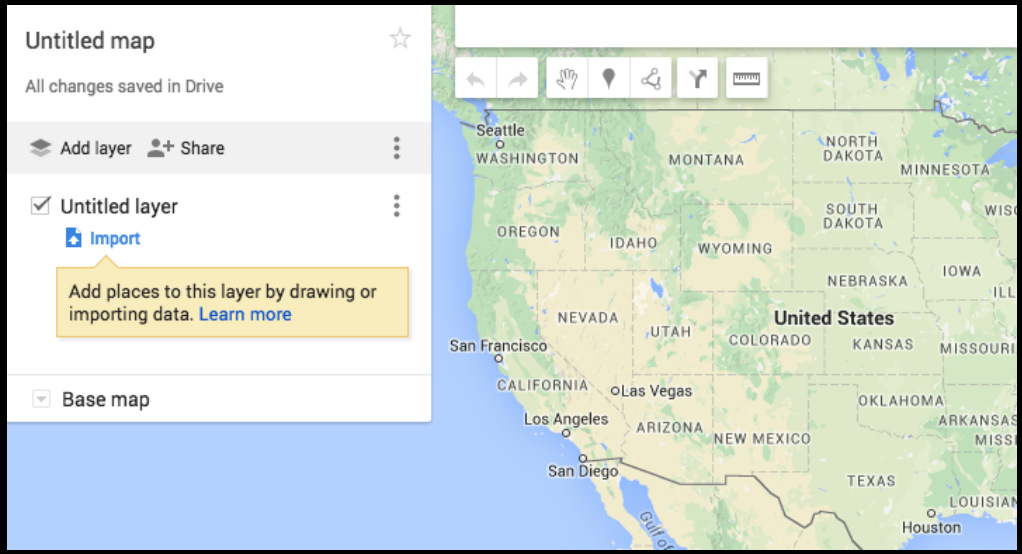
# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



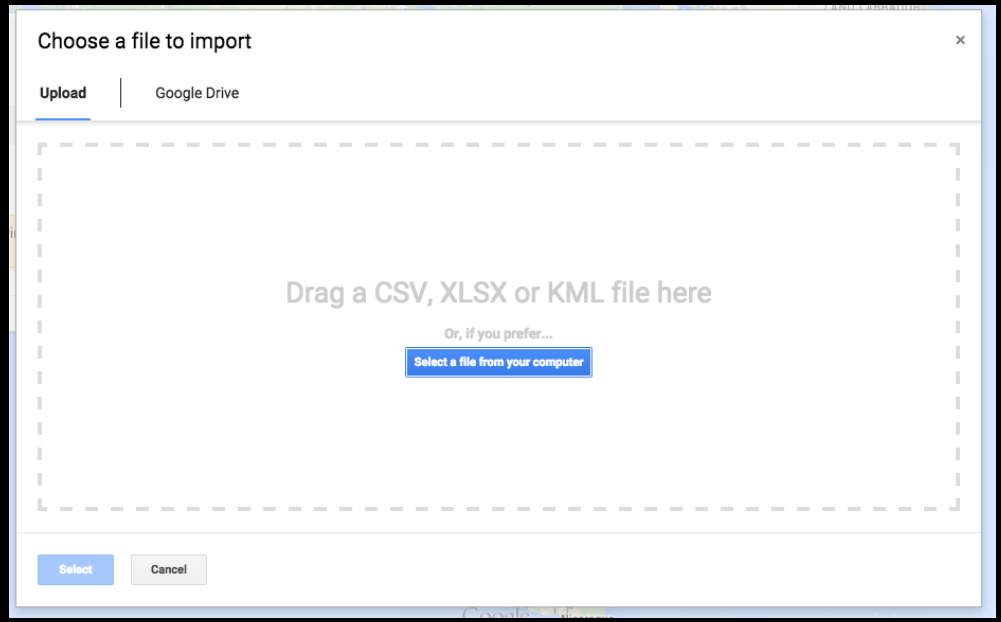
# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



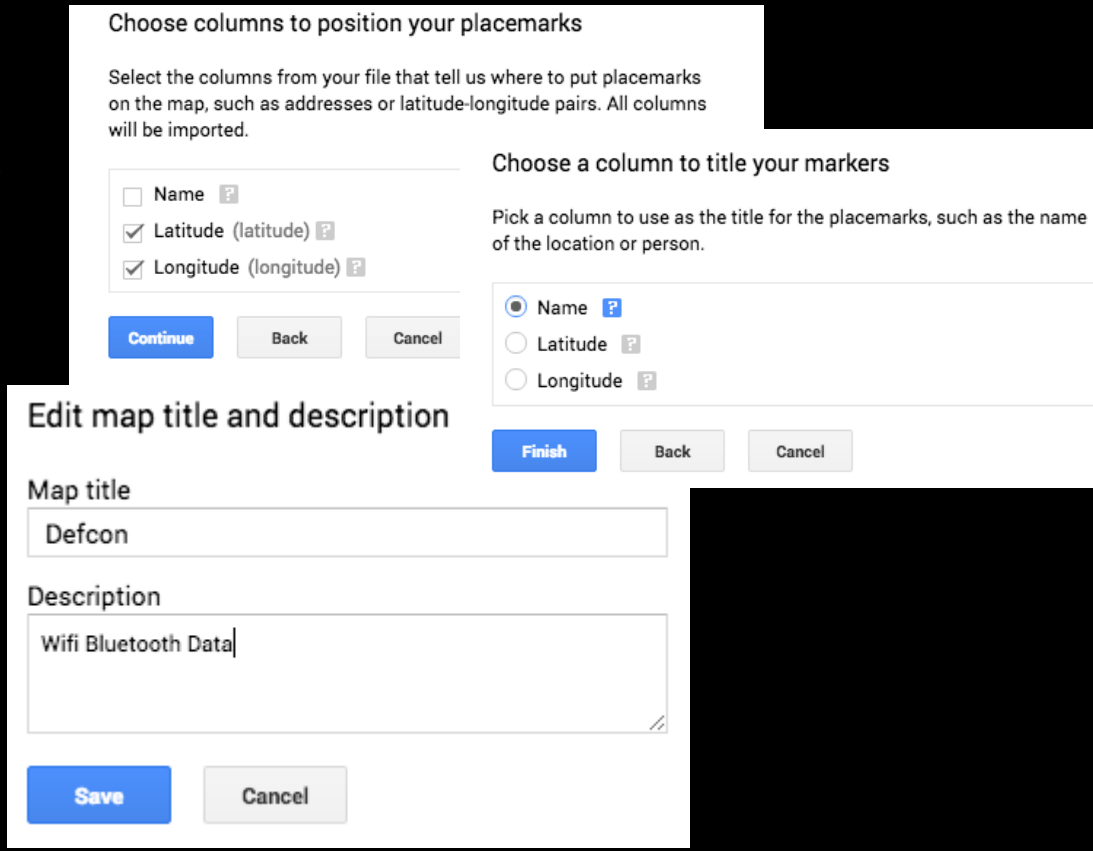
# Software Needed - Bluetooth Mapping

Email the database from bluescan

Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



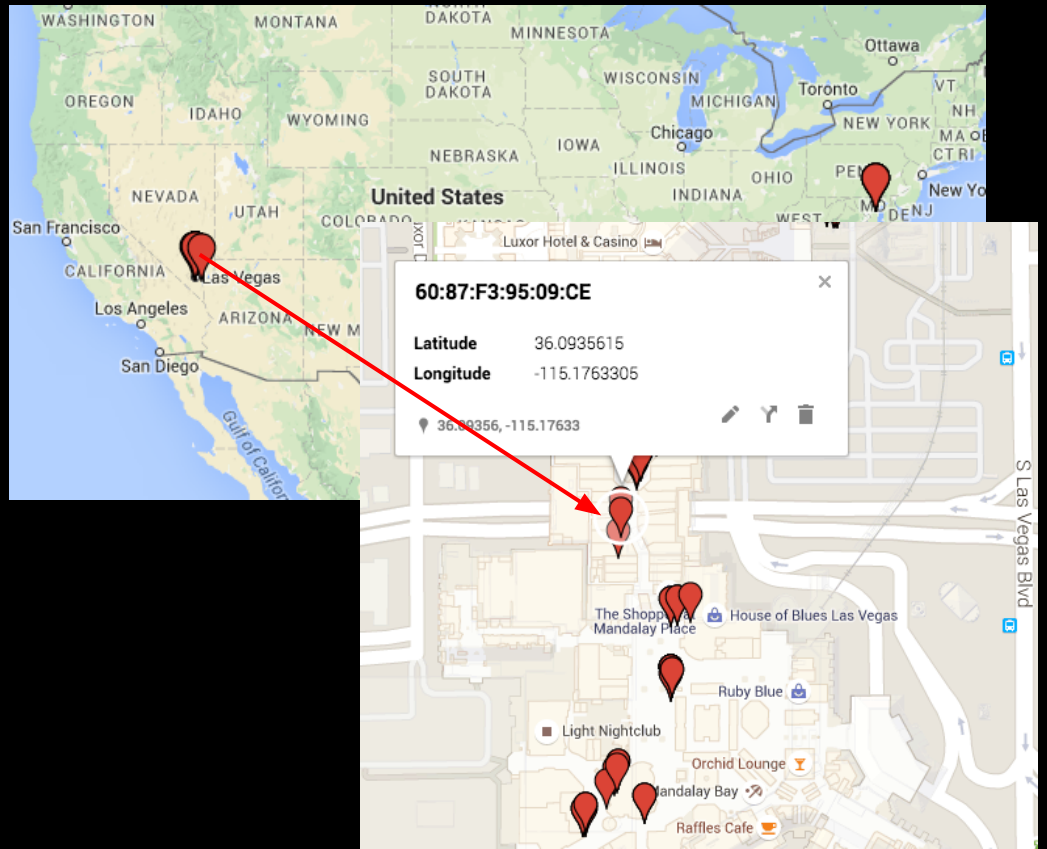
# Software Needed - Bluetooth Mapping

Email the database from bluescan

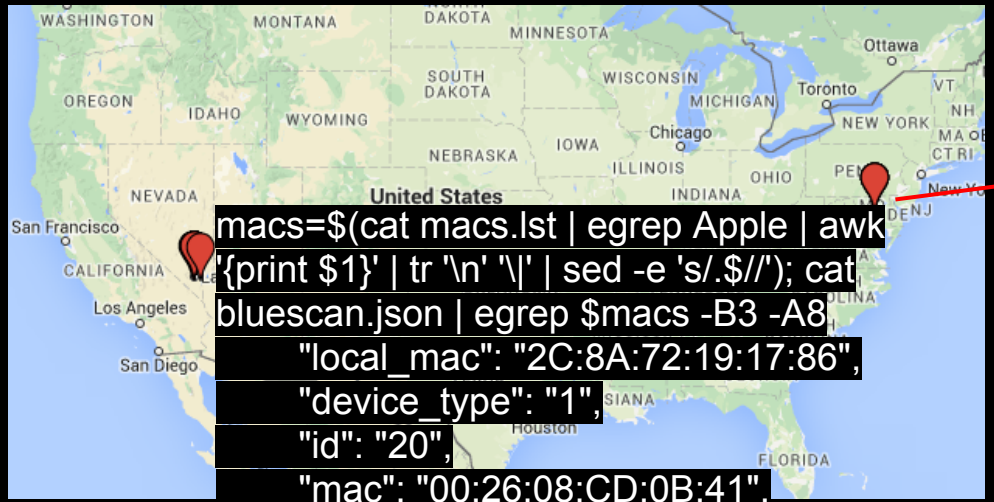
Download the database to a json file

Run the parser on the file:
./blueScanParserMaps.sh [file]

Upload to google maps



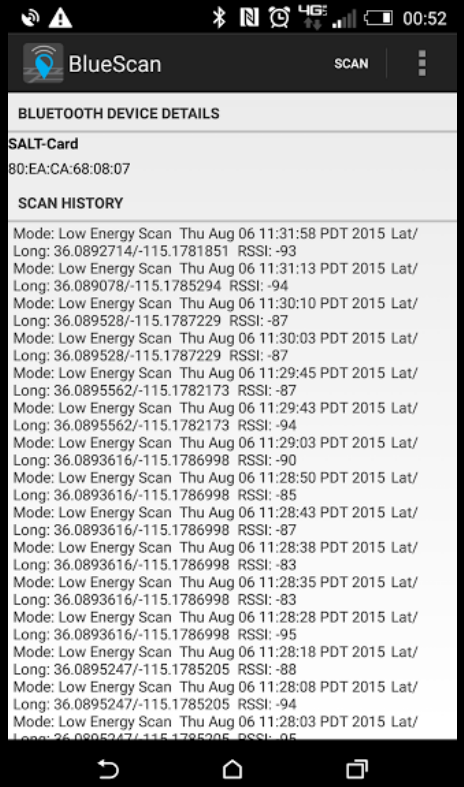
# Attribution Bluetooth - Girl on a plane

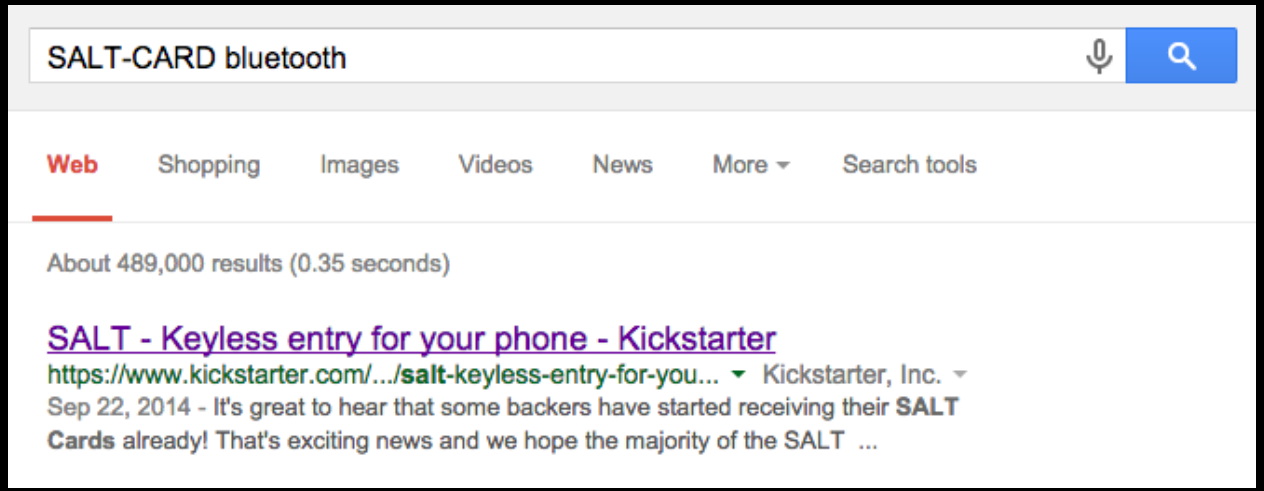



```
macs=$(cat macs.lst | egrep Apple | awk '{print $1}' | tr '\n' '\|' | sed -e 's/.$//'); cat bluescan.json | egrep $macs -B3 -A8
        "local_mac": "2C:8A:72:19:17:86",
        "device_type": "1",
        "id": "20",
        "mac": "00:26:08:CD:0B:41",
        "company": "Apple, Inc",
        "date_seconds": "1438747584608",
        "title": "fire",
        "timestamp": "1438748098395",
        "latitude": "36.0143379",
        "longitude": "-114.7530405",
        "altitude": "457.0",
        "provider": "fused",
```

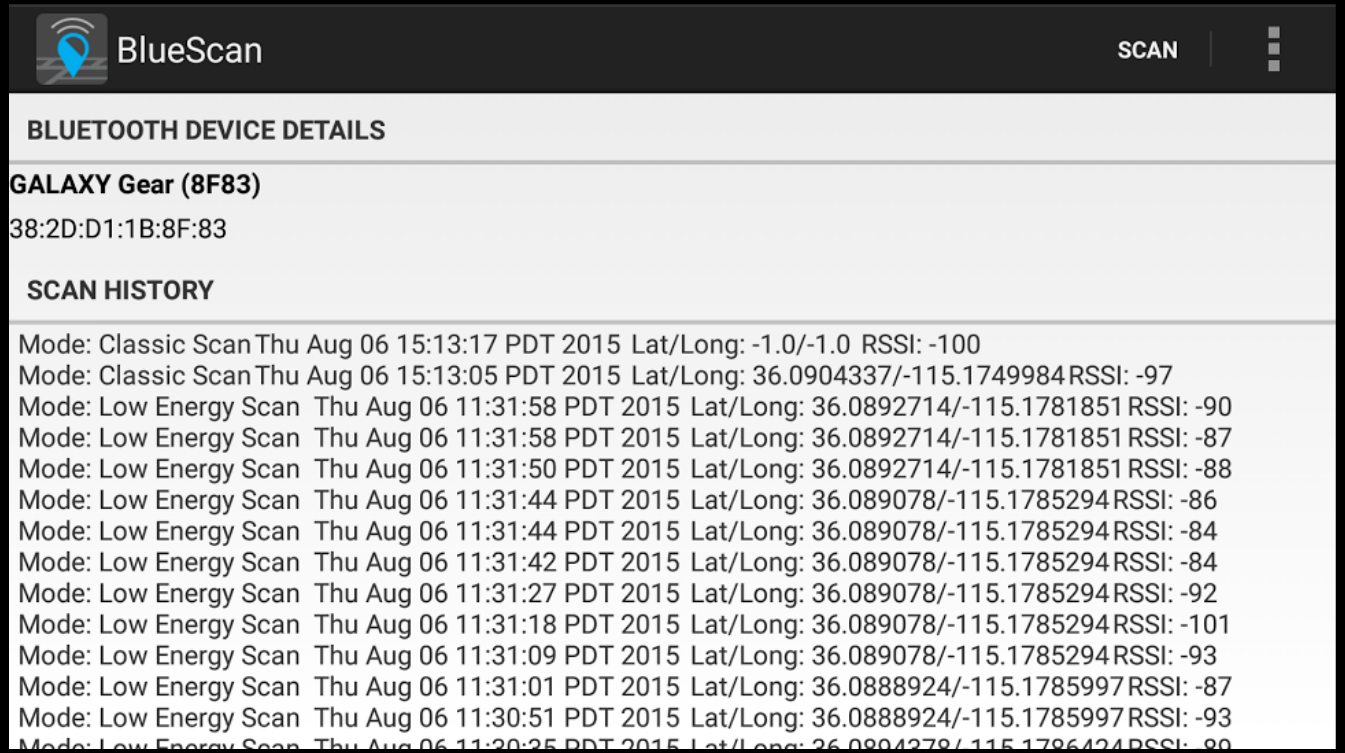
# Attribution BT - People in Security Detail


# Attribution BT - People in Security Detail



# Attribution BT - People in Security Detail



# Tips for Protection

- Turn off bluetooth when not needed
- Clean up your wifi
- Be aware of who is around you
- Scan yourself

# Thanks!

SPAM, Phish and Other Things Good to Eat.

@JoshInGeneral

JoshInGeneral@gmail.com