

# Joshua Schroeder

Meeting People via Wifi

@JoshInGeneral

JoshInGeneral@gmail.com

# About JoshInGeneral

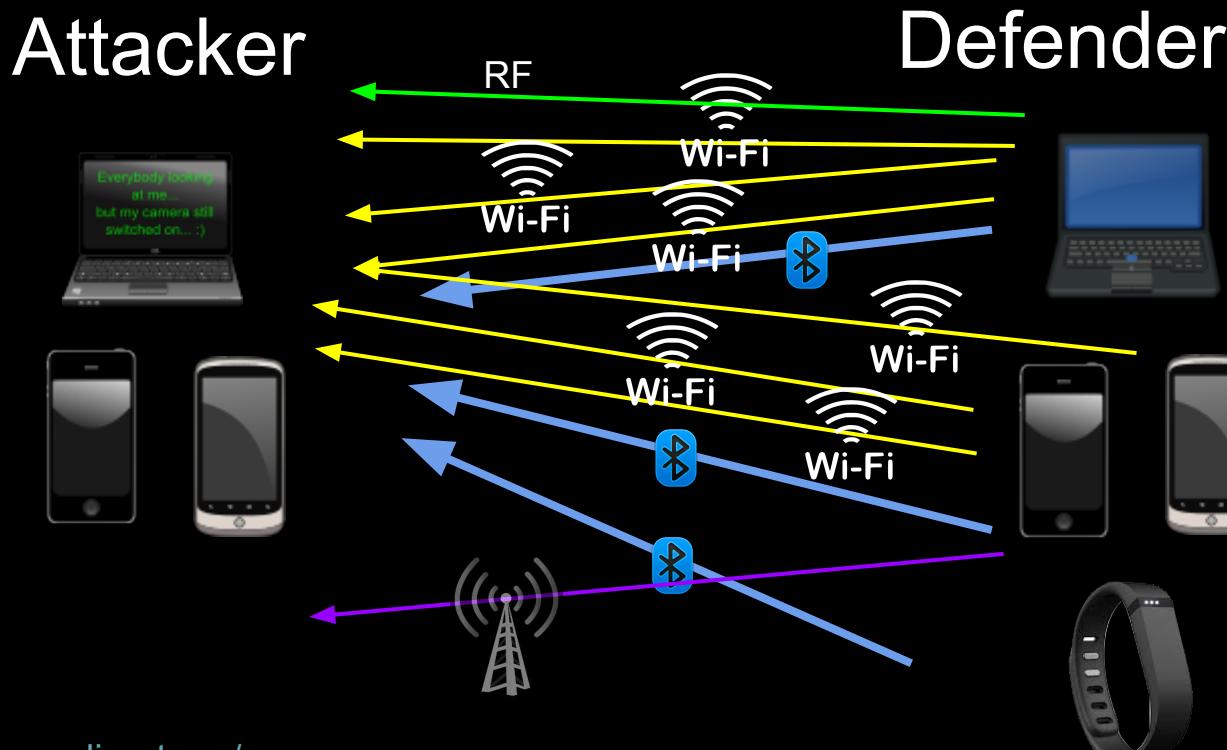
- NovaHacker ~3 years
- From NC, UNCC,  
49th Security Division
- Most research in Web Vulnerabilities,  
Dabble in Legal, CCTV hacking, 3rd Year  
WCTF
- Currently work doing IR in NoVA
- Research not related to job



# Agenda

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

# Overview



YOU  
LOSE

You can't hide your signals...

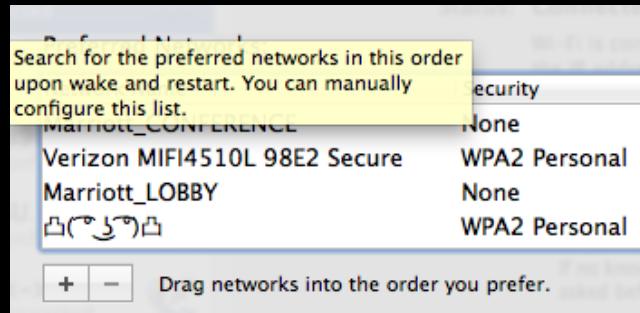
# Overview: Bluetooth Scanning for Device Association

- 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



# 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



# Hardware Needed - Wifi

Showing Today on Linux and Android + OTG Adapter



# 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

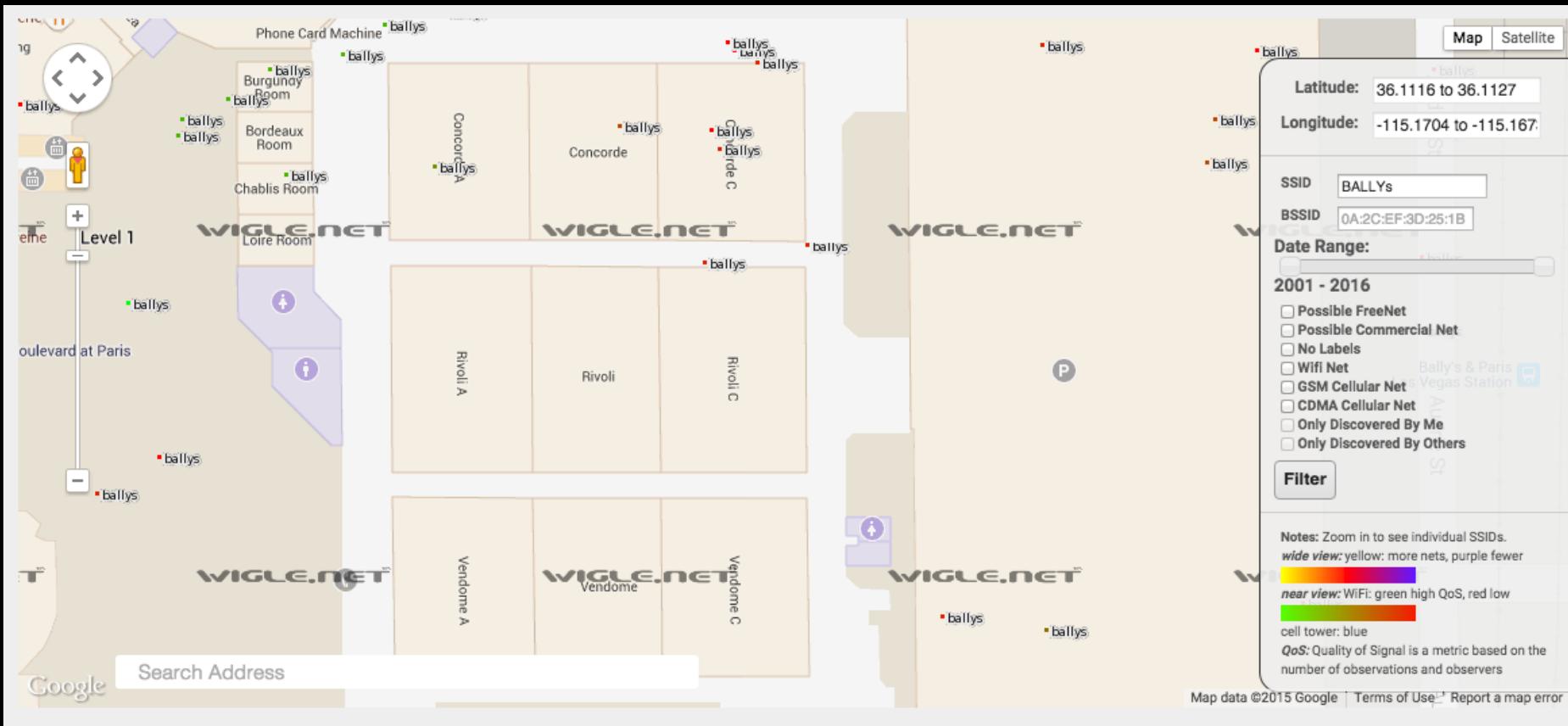


WiGLE WiFi a>z

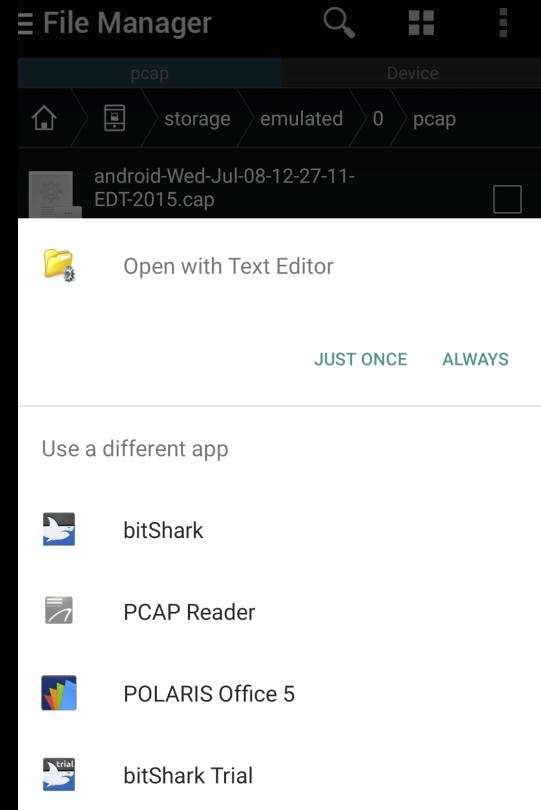
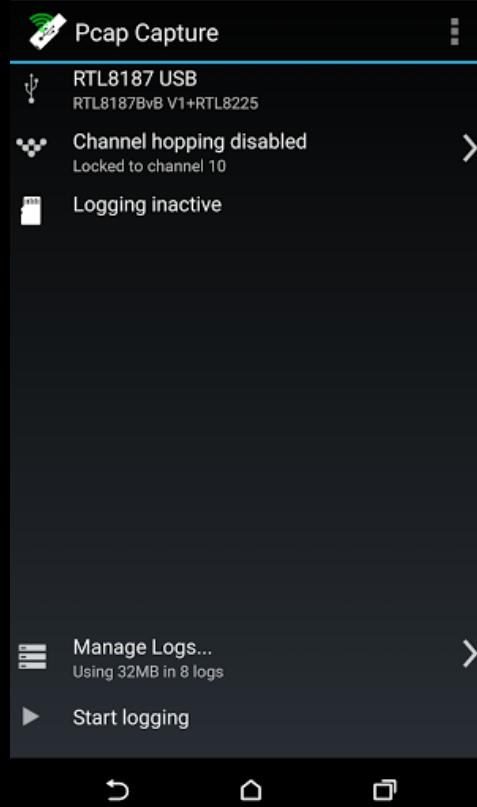
LIST MAP DASH DATA

<p>Run: 3</p> <p><b>UPLOAD TO WIGLE.NET</b></p>	<p>New: 2</p> <p>Lat: 35.70493654 Lon: -114.47711369 Speed: 71.1 mph</p>	<p>DB: 4715 +/- 39 ft Alt: 2,385 ft Sats: 15</p>
<p>2 scanned in 2012ms. DB Queue: 0 <span style="float: right;">MUTE</span></p> <p> MiFi4620LE Jetpack 527C Secure 20:41:32 45   00:15:ff - [WPA2][ESS]</p>		

# Software Needed - WiGLE Wifi



# Software Needed - PCAP Scanner



# Software Needed - BitShark Scanner



WIGLE WIFI



PCAP CAPTURE



BITSHARK



RAMBLE



BLUESCAN



FILE MANAGER



SDRTOUCH



OCLOUD24



WIFI ANALYZER

(android-Fri-Jul-24-17-18-15-EDT-201...)		
#75	To: 00:00:08:00:69:00 2015-07-24 14:18:15.988657	36B
ETH2	From: 00:00:B4:00:AC:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.98906	24B
ETH2	From: 00:00:94:00:24:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.989519	36B
ETH2	From: 00:00:B4:00:F8:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.989974	24B
ETH2	From: 00:00:94:00:24:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.99043	36B
ETH2	From: 00:00:B4:00:C8:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.990822	24B
ETH2	From: 00:00:94:00:24:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.991215	36B
ETH2	From: 00:00:B4:00:50:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.99917	24B
ETH2	From: 00:00:C4:00:24:00 To: 00:00:08:00:69:00 2015-07-24 14:18:15.999625	18B
ETH2	From: 00:00:B4:00:50:00 To: 00:00:08:00:69:00 2015-07-24 14:18:16.000041	24B

Packet #713, 219 bytes

Packet Info

Packet #713  
Packet Size: 219 Bytes (219 Bytes)  
Timestamp: 2015-07-24 14:18:25.784293  
Time Since Start: 0h:0m:10.287s

Ethernet: 14 bytes

```
Eth: ***** Ethernet - "Ethernet" - offset=0 (0x0) length=14
Eth:
Eth: destination = 00:00:08:00:69:00
Eth: .....0..... = [0] LG bit
Eth: .....0..... = [0] LG bit
Eth: source = 00:00:08:00:00:00
Eth: .....0..... = [0] LG bit
Eth: .....0..... = [0] LG bit
Eth: type = 0xFFFF (65535)
Eth:
```

Data Hex: 205 bytes

```
ff ff ff 00 24 a5 b5 1c 4f 00 24 a5 b5 1c 4f
50 15 80 c1 29 11 00 00 00 00 64 00 11 04 00 05
64 6c 69 6c 6b 01 08 82 84 8b 96 0c 12 18 24 03
01 06 05 04 00 02 00 00 2a 01 04 32 04 30 48 60
6c 30 14 01 00 00 f0 ac 04 01 00 00 0f ac 04 01
00 00 f0 ac 02 0c 00 dd 16 00 50 f2 01 01 00 00
50 f2 04 01 00 00 50 f2 04 01 00 00 50 f2 02 2d
1a cc 11 b1 ff ff 00 00 00 00 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 17
```

# Software Needed - Kismet

Kismet Sort View Windows					
Name	T	C	Ch	Pkts	Size
. BETA	A	O	11	45	0B
. BETA	A	O	1	22	0B
Ballys-Convention-Co	A	N	6	1	0B
! Ballys-Rooms-Cox	A	N	6	84	0B
EISWireless	A	O	6	11	0B
+ Autogroup Probe	P	N	---	86	0B
BSSID: 00:00:00:00:00:00 Last seen: Aug 9 10:45:29 Crypt: None Manuf: Mixed					
FBI_Surveillance_Van	A	O	6	3	0B
Focus\342\200\231s i	A	O	1	8	48B
. Francis's iPhone	A	O	1	6	0B
MAC	Type	Freq	Pkts	Size	Manuf
90:8D:6C:BE:14:B9	Wireless	2457	3	0B	Unknown
18:F6:43:18:19:FA	Wireless	2447	2	0B	Unknown
00:0E:8E:47:0C:28	Wireless	2427	2	0B	Sparklan
9C:F3:87:21:2D:7F	Wireless	2442	10	0B	Unknown
00:02:6F:5F:26:20	Wireless	2462	5	0B	SenaoInt
E8:92:A4:94:48:BD	Wireless	2452	6	0B	LgElectr
00:C0:CA:1A:91:47	Wireless	2447	5	0B	Alfa
! 00:02:6F:5F:24:C2	Wireless	2452	8	0B	SenaoInt
. C8:BC:C8:EE:52:3E	Wireless	2427	4	0B	Apple
A4:77:33:08:FD:5D	Wireless	2457	2	0B	Google
F4:09:D8:F5:75:8A	Wireless	2462	2	0B	Unknown
No GPS data (GPS not connected) Pwr: AC (Charging)					
123					

# Software Needed - Aircrack-ng

```
aircrack.conf    airodump-ng.sh          CTF16-02.cap           Kis
airMenu.sh       CTF16-01.cap           CTF16-02.csv           Kis
airodump-ng2.sh  CTF16-01.csv          CTF16-02.kismet.csv   Kis
airodump-ng3.sh  CTF16-01.kismet.csv   CTF16-02.kismet.netxml Kis
airodump-ng4.sh  CTF16-01.kismet.netxml Kismet-20150123-21-50-55-1.alert Tes
      :~/Projects/aircrackScripts$ ./airMenu.sh
Type help for commands
Enter command:
help
You seem to be lost, please consult the droids for help
Type 'mon [start | stop]' to enter monitor mode
Type 'config' to edit the aircrack.conf file
Type 'capture [ nobssid | all ]' to start monitoring on config channel
Type 'handshakes [ fileprefix | test ]' to see what wifi have been proccessed
Type 'screen' to list and show running screens
Type 'list [SEARCH]' to see current wireless networks being captured
```

# 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
K[phy0]wlan0mon ath9k[mac80211]-N/A
```

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

```
Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
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  
[profile](#) | [home page](#) | [map](#) | [special programs](#)

[3020 Gallows Rd](#)  
Falls Church, VA 22042

2 Gunston Alternative School - South County Juvenile Court  
[profile](#) | [home page](#) | [map](#) | [special programs](#)

[8350 Richmond Hwy](#)  
Suite 119  
Alexandria, VA 22309

3 Hillwood School - East County Juvenile Court  
[profile](#) | [home page](#) | [map](#) | [special programs](#)

[2812 Old Lee Hwy](#)  
Suite 100  
Fairfax, VA 22031

4 Chantilly High School Academy  
[profile](#) | [home page](#) | [map](#)

[4201 Stringfellow Rd](#)  
Chantilly, VA 20151

CenturyBuilding11A

Web Maps Shopping Images News More ▾ Search tools

2 results (0.28 seconds)

Did you mean: [Century Building 11A](#)

**211 E 51st St APT 11A, New York, NY 10022 is Off Market ...**  
[www.zillow.com](#) › ... › New York › Manhattan › Turtle Bay ▾ Zillow ▾  
Situated at the quiet northwest corner of a classic mid-century building, 11A is perhaps the perfect two bedroom apartment. A lovely entry foyer welcomes you ...

**211 East 51st Street 11A - Blocksy.com**  
[www.blocksy.com/nyc/sale/2026477-211-east-51st-street-11a](#)  
Situated at the quiet northwest corner of a classic mid-century building, 11A is perhaps the perfect two bedroom apartment. A lovely entry foyer welcomes you ...

# Attribution Wifi - FCC

FCC building

Web Maps Images News Shopping More ▾ Search tools

About 68,700,000 results (0.87 seconds)

Images for FCC building Report images



More images for FCC building

---

Federal Communications Commission  
[www.fcc.gov/](http://www.fcc.gov/)  
3.9 ★★★★☆ 10 Google reviews · Write a review

 445 12th Street Southwest, Washington, DC 20554  
(888) 225-5322

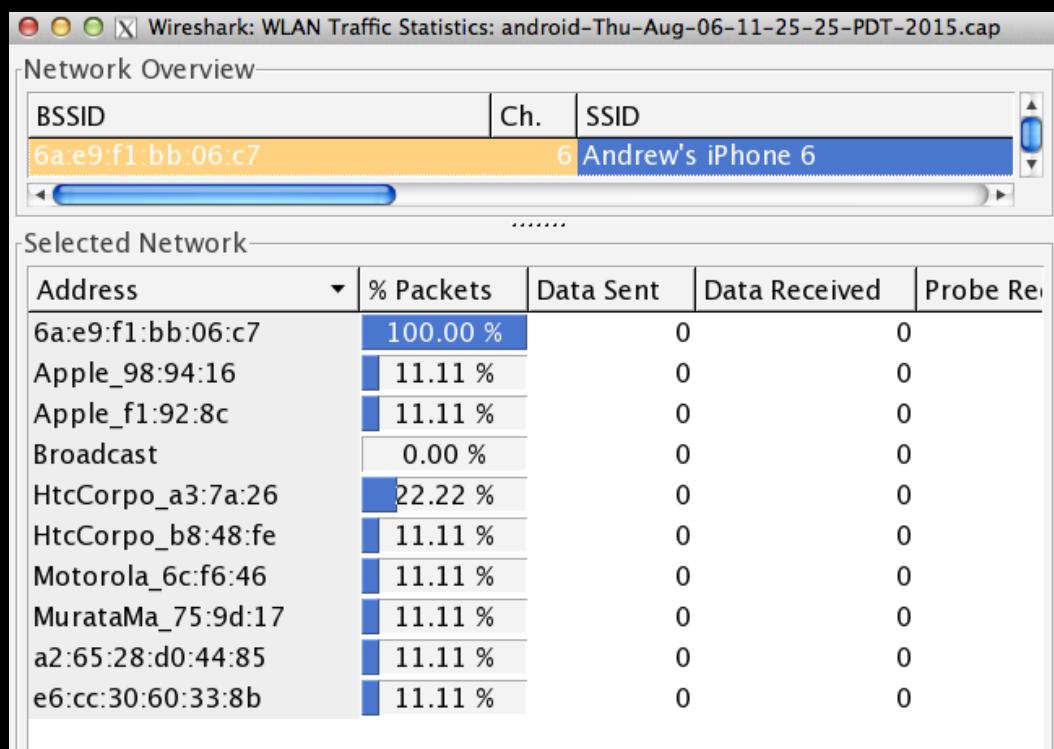
# Attribution Wifi - FCC



# Software Needed - Wireshark/tcpdump

Statistics -> WLAN Summary

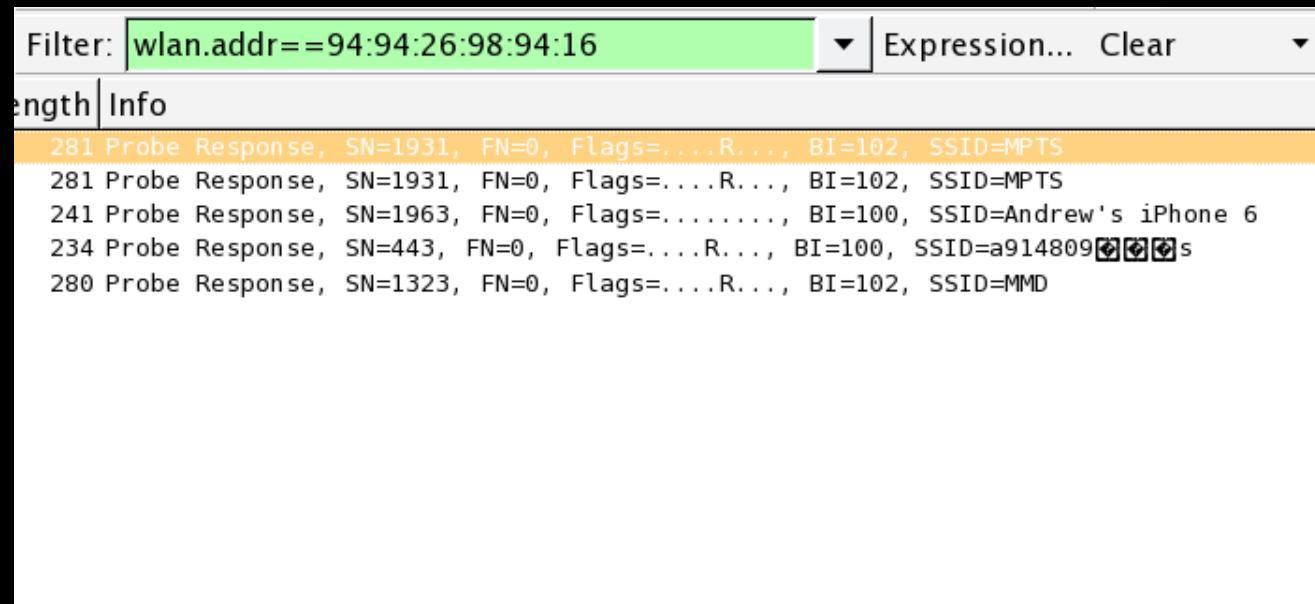
Make a filter for the MAC



# Software Needed - Wireshark/tcpdump

Statistics -> WLAN Summary

Make a filter for the MAC



A screenshot of the Wireshark interface. The top bar shows a filter: "wlan.addr==94:94:26:98:94:16". Below the filter, there are two tabs: "length" and "Info", with "Info" selected. The main pane displays a list of wireless frames:

- 281 Probe Response, SN=1931, FN=0, Flags=....R..., BI=102, SSID=MPTS
- 281 Probe Response, SN=1931, FN=0, Flags=....R..., BI=102, SSID=MPTS
- 241 Probe Response, SN=1963, FN=0, Flags=....., BI=100, SSID=Andrew's iPhone 6
- 234 Probe Response, SN=443, FN=0, Flags=....R..., BI=100, SSID=a914809■■■■s
- 280 Probe Response, SN=1323, FN=0, Flags=....R..., BI=102, SSID=MMD

# 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

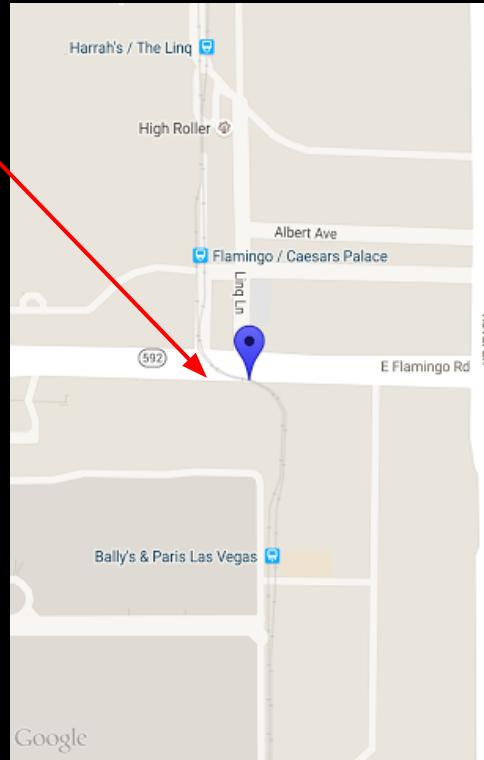
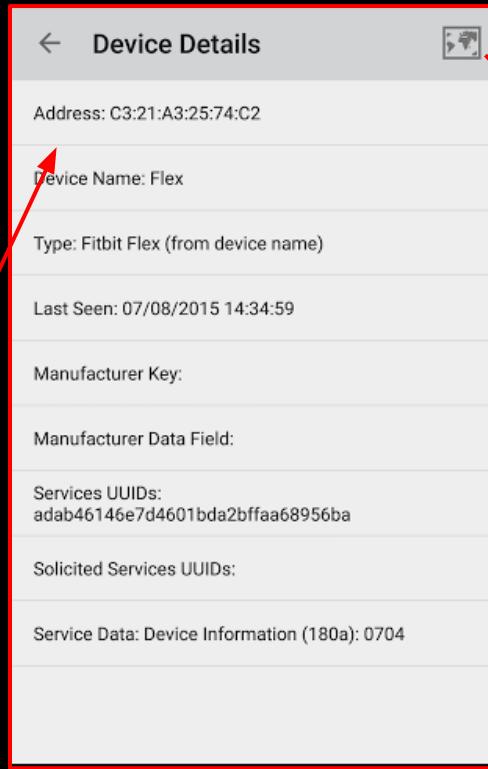
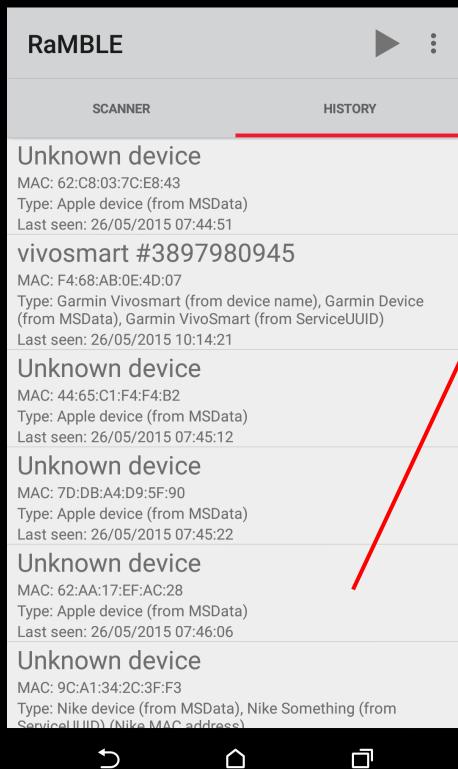
- Ramble (Android)
- BlueScan (Android)
- Bluetooth Smart Tool (iPhone)
- Kali: hcitool lescan

# Hardware Needed - BT UberTooth

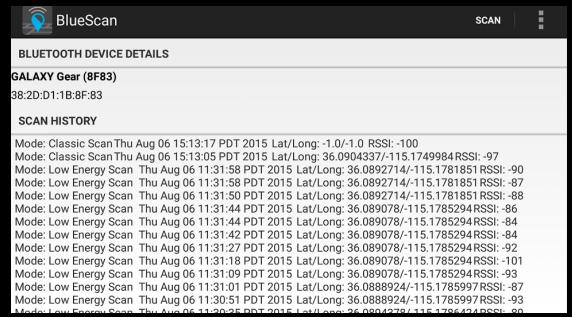
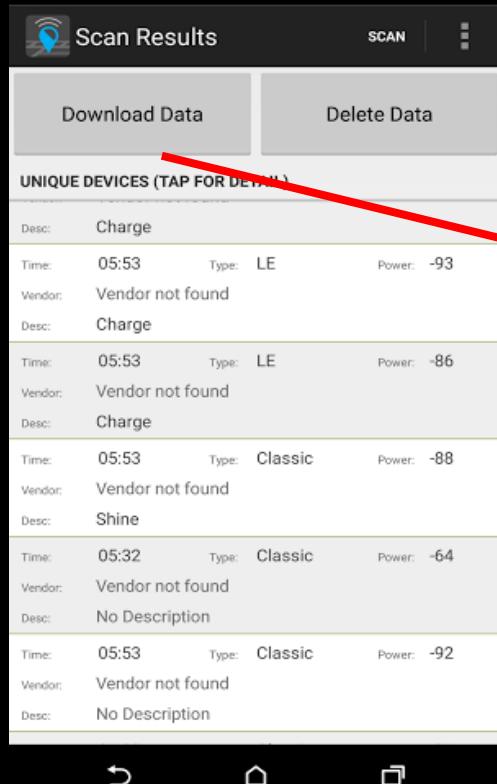


Source: <http://www.amazon.com/UCEC-USB-2-0-Adapter-Plug/dp/B00WHWKD60>

# 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"
```

# 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).

# 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
```

Convert epoch to human readable date and vice versa

The screenshot shows a timestamp conversion tool. At the top, a text input field contains the value "1438428920509". To its right is a button labeled "Timestamp to Human date". Below this, a message says "Assuming that this timestamp is in milliseconds:" followed by "GMT: Sat, 01 Aug 2015 11:35:20 GMT". Underneath, it says "Your time zone: 8/1/2015, 4:35:20 AM GMT-7:00". At the bottom, there's a date and time picker with fields for Mon, Day, Yr, Hr, Min, Sec, and a dropdown for GMT/Human.

## Epoch Batch Conversion Tool

Tools on this page

1. Convert FROM epoch/timestamp (make it readable)
2. Convert TO epoch/timestamp (create timestamps)

Now with CSV/Excel export! Always double-check your results.

# Software Needed - BlueScan

Get All Data by MAC

```
cat bluescan.json | egrep 5C:58:03 -B3 -A8
```

2C:8A:72

49:A1:FA

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
```

54:05:FE

5C:58:03

6F:F7:F4

7C:C3:C8

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
```

# 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
```

**OUI Lookup Tool**

The Wireshark OUI lookup tool provides an easy way to look up OUIs and other MAC address prefixes. It uses the [Wireshark manufacturer database](#), which is a list of OUIs and MAC addresses compiled from a number of sources.

Directions:  
Type or paste in a list of OUIs, MAC addresses, or descriptions below. OUIs and MAC addresses may be colon-, hyphen-, or period-separated.

Examples:  
0000.0c  
08:00:20  
01-00-0C-CC-CC-CC  
missouri

**OUI search**

DC:E6:09  
E4:5A:1E  
E6:62:9A  
F0:E4:6F  
F2:2A:9F  
F2:FA:03  
F5:AE:F9  
F9:5E:C4  
FA:7D:DE  
00:26:08

**Results**

00:26:08 Apple  
2C:8A:72 HTC Corporation  
5C:31:3E Texas Instruments

Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation

Source: <https://www.wireshark.org/tools/oui-lookup.html> | [https://code.wireshark.org/review/gitweb?p=wireshark.git;a=blob\\_plain;f=manuf](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
```

Sat Aug 1 04:35:20 MST 2015

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](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/\//\n/' | 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",
```

# 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

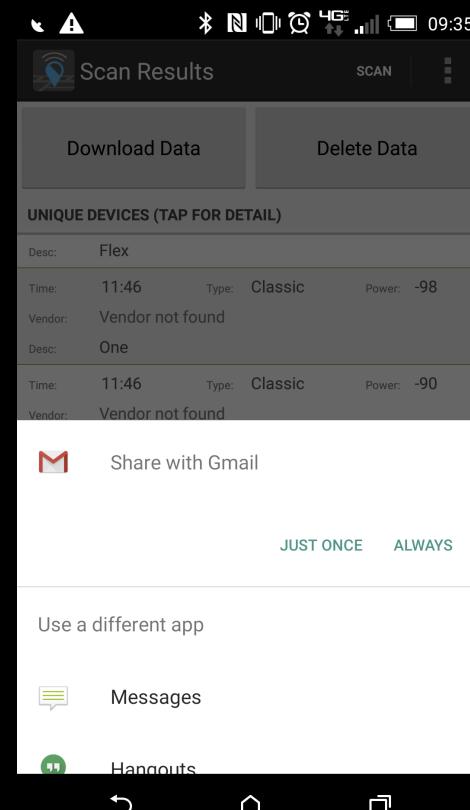
Email the database from bluescan

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

```
        "company": "",  
        "date_seconds": "1438428963138",  
        "timestamp": "143842896275",  
        "latitude": "39.1802898",  
        "longitude": "-76.6722784",  
        "altitude": "13.0",  
        "provider": "fused",  
        "rssi": "-93"  
    },  
    {  
        "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"  
    },  
    {  
        "local_mac": "2C:8A:72:19:17:86",  
        "device_type": "1",  
        "id": "2",  
        "mac": "6F:F7:F4:E6:70:84",  
        "company": "",  
        "date_seconds": "1438428890346",  
        "timestamp": "1438428941683",  
        "latitude": "39.1802885",  
        "longitude": "-76.6722627",  
        "altitude": "10.0",  
        "provider": "fused",  
        "rssi": "-95"  
    },  
    {  
        "local_mac": "2C:8A:72:19:17:86",  
        "device_type": "1",  
        "id": "1",  
        "mac": "7C:C3:C8:58:CF:AF",  
        "company": "",  
        "date_seconds": "1438428832597",  
        "timestamp": "1438428832597",  
        "latitude": "39.1802511",  
        "longitude": "-76.6726002",  
        "altitude": "0.0",  
        "provider": "fused",  
        "rssi": "-92"  
    }  
}  
-- INSERT --
```

# 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

```
longitude": "-76.6722620",
"mac": "6F:F7:F4:E6:70:84",
"company": "",
"date": "Sat Aug  1 04:35:41 MST 2015"
"latitude": "39.1802885",
"longitude": "-76.6722627",
"mac": "7C:C3:C8:58:CF:AF",
"company": "",
"date": "Sat Aug  1 04:33:52 MST 2015"
"latitude": "39.1802511",
"longitude": "-76.6726002",
bash-3.2$ ls output.csv
output.csv
bash-3.2$
```

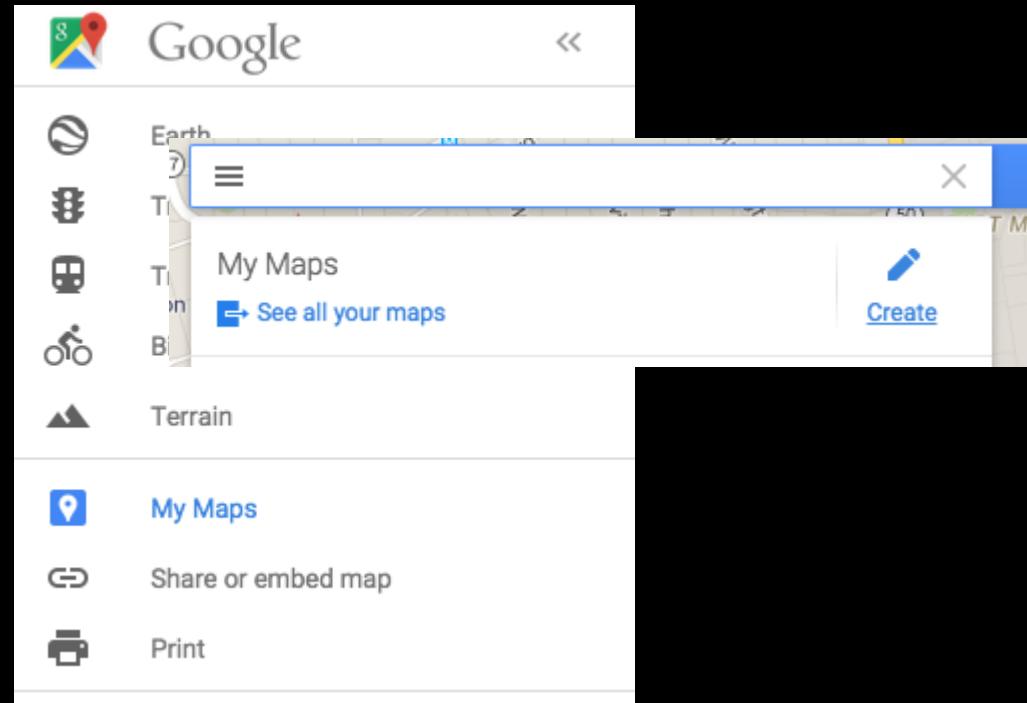
# Software Needed - Bluetooth Mapping

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

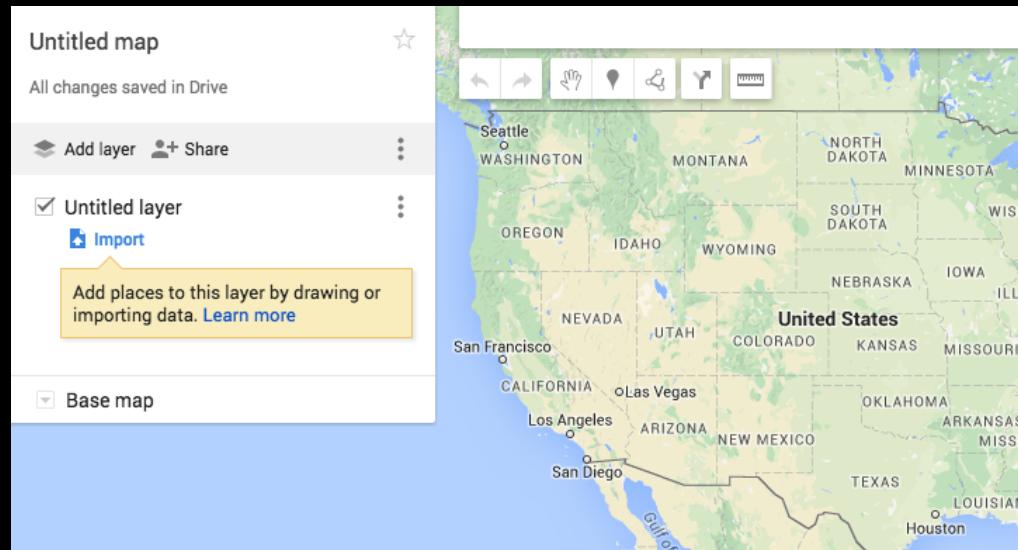
Email the database from bluescan

Download the database to a json file

Run the parser on the file:

```
./blueScanParserMaps.sh [file]
```

Upload to google maps



# Software Needed - Bluetooth Mapping

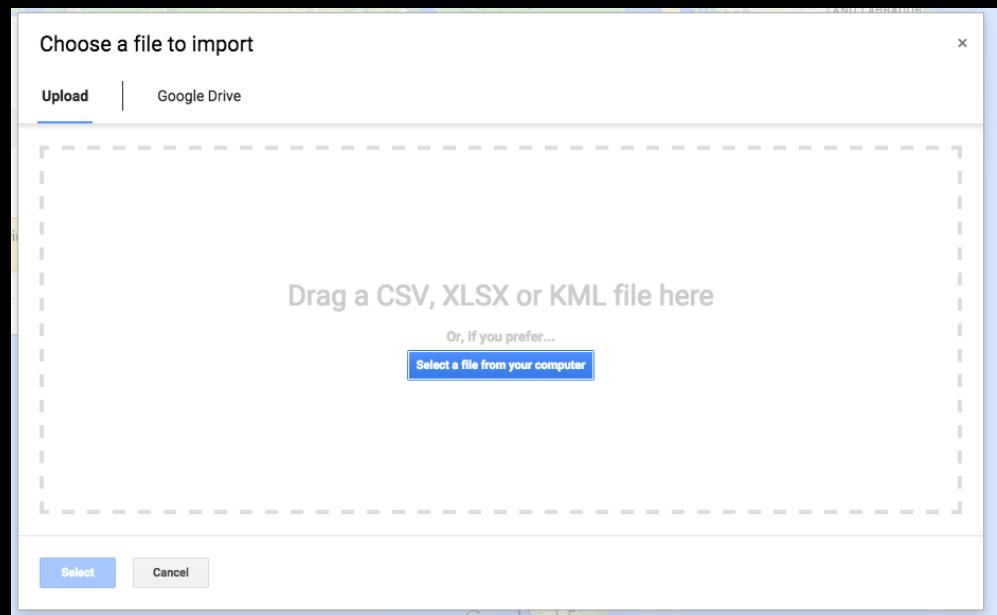
Email the database from bluescan

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

Choose columns to position your placemarks

Select the columns from your file that tell us where to put placemarks on the map, such as addresses or latitude-longitude pairs. All columns will be imported.

Name ?  
 Latitude (latitude) ?  
 Longitude (longitude) ?

Continue Back Cancel

Choose a column to title your markers

Pick a column to use as the title for the placemarks, such as the name of the location or person.

Name ?  
 Latitude ?  
 Longitude ?

Finish Back Cancel

Edit map title and description

Map title  
Defcon

Description  
Wifi Bluetooth Data

Save Cancel

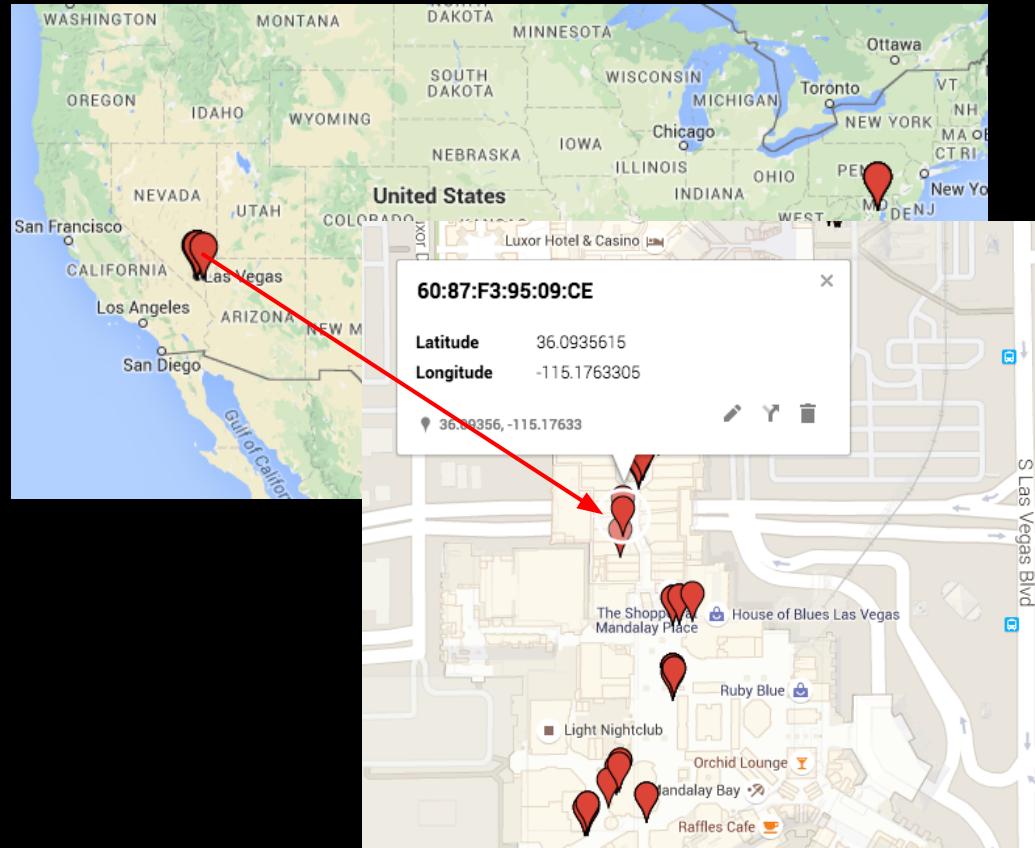
# Software Needed - Bluetooth Mapping

Email the database from bluescan

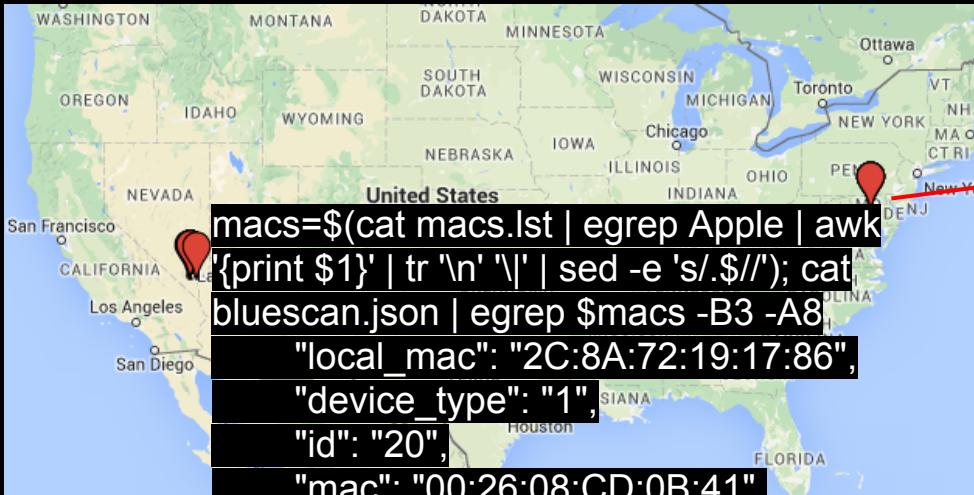
Download the database to a json file

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

Upload to google maps



# Attribution Bluetooth - Girl on a plane



# Attribution BT - People in Security Detail



# Attribution BT - People in Security Detail



The screenshot shows a search results page from a mobile browser. The search query is "SALT-CARD bluetooth". The results include a navigation bar with links for "Web", "Shopping", "Images", "Videos", "News", "More", and "Search tools". Below the navigation bar, it says "About 489,000 results (0.35 seconds)". The first result is a link to a Kickstarter page for "SALT - Keyless entry for your phone - Kickstarter". The link is <https://www.kickstarter.com/.../salt-keyless-entry-for-you...>. The snippet of the page content reads: "Kickstarter, Inc. ▾ Sep 22, 2014 - It's great to hear that some backers have started receiving their SALT Cards already! That's exciting news and we hope the majority of the SALT ...".

# Attribution BT - People in Security Detail

The screenshot shows the BlueScan application interface. At the top, there is a header bar with a location icon, the text "BlueScan", a "SCAN" button, and a three-dot menu icon. Below the header, the title "BLUETOOTH DEVICE DETAILS" is displayed. Under this title, the device "GALAXY Gear (8F83)" is listed with its MAC address "38:2D:D1:1B:8F:83". To the right of the device name are icons for a clipboard, a house, and a circular arrow. The main content area is titled "SCAN HISTORY" and lists numerous entries of scan data. Each entry includes the mode ("Mode: Classic Scan" or "Mode: Low Energy Scan"), the date and time ("Thu Aug 06 15:13:17 PDT 2015" or "Thu Aug 06 11:31:58 PDT 2015"), the latitude and longitude ("Lat/Long: -1.0/-1.0" or "Lat/Long: 36.0892714/-115.1781851"), the RSSI value ("RSSI: -100" or "RSSI: -97"), and the timestamp ("RSSI: -90" through "RSSI: -93").

Mode	Date/Time	Lat/Long	RSSI
Mode: Classic Scan	Thu Aug 06 15:13:17 PDT 2015	Lat/Long: -1.0/-1.0	RSSI: -100
Mode: Classic Scan	Thu Aug 06 15:13:05 PDT 2015	Lat/Long: 36.0904337/-115.1749984	RSSI: -97
Mode: Low Energy Scan	Thu Aug 06 11:31:58 PDT 2015	Lat/Long: 36.0892714/-115.1781851	RSSI: -90
Mode: Low Energy Scan	Thu Aug 06 11:31:58 PDT 2015	Lat/Long: 36.0892714/-115.1781851	RSSI: -87
Mode: Low Energy Scan	Thu Aug 06 11:31:50 PDT 2015	Lat/Long: 36.0892714/-115.1781851	RSSI: -88
Mode: Low Energy Scan	Thu Aug 06 11:31:44 PDT 2015	Lat/Long: 36.089078/-115.1785294	RSSI: -86
Mode: Low Energy Scan	Thu Aug 06 11:31:44 PDT 2015	Lat/Long: 36.089078/-115.1785294	RSSI: -84
Mode: Low Energy Scan	Thu Aug 06 11:31:42 PDT 2015	Lat/Long: 36.089078/-115.1785294	RSSI: -84
Mode: Low Energy Scan	Thu Aug 06 11:31:27 PDT 2015	Lat/Long: 36.089078/-115.1785294	RSSI: -92
Mode: Low Energy Scan	Thu Aug 06 11:31:18 PDT 2015	Lat/Long: 36.089078/-115.1785294	RSSI: -101
Mode: Low Energy Scan	Thu Aug 06 11:31:09 PDT 2015	Lat/Long: 36.089078/-115.1785294	RSSI: -93
Mode: Low Energy Scan	Thu Aug 06 11:31:01 PDT 2015	Lat/Long: 36.0888924/-115.1785997	RSSI: -87
Mode: Low Energy Scan	Thu Aug 06 11:30:51 PDT 2015	Lat/Long: 36.0888924/-115.1785997	RSSI: -93
Mode: Low Energy Scan	Thu Aug 06 11:30:25 PDT 2015	Lat/Long: 36.0894278/-115.1786424	RSSI: -89

# 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](mailto:JoshInGeneral@gmail.com)