ISNIFF GPS

Virtual Wardriving

SyScan Singapore 2013

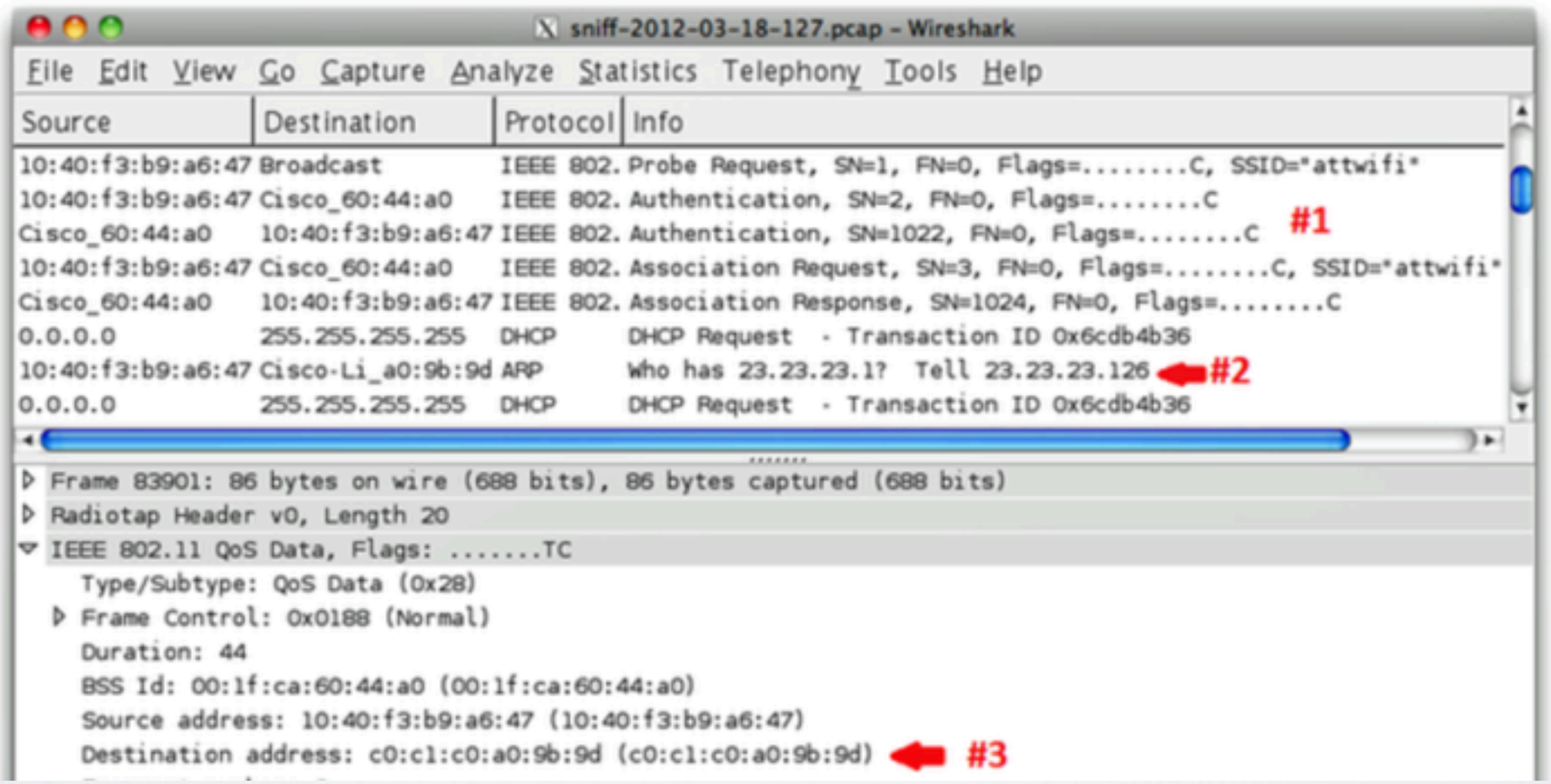
@hubert3
hubert(a)pentest.com

Anatomy of a leak: how iPhones spill the ID of networks they access

Yes, iPhones and other Apple devices routinely *do* expose the unique …

by **Dan Goodin** - Mar 27 2012, 6:30pm CEST

WHITE HAT 94



Ars Technica article - March 2012

Introducing iSniff GPS...

```
if p.haslayer(ARP):
    arp = p.getlayer(ARP)
    dot11 = p.getlayer(Dot11)
    mode = ''
    try:
        target_bssid = dot11.addr1 # on wifi, BSSID (mac) of AP currently connected to
        source_mac = dot11.addr2 # wifi client mac
        target_mac = dot11.addr3 # if we're sniffing wifi (mon0) the other-AP bssid disclosure will be here in 802.11 dest
        if dot11.FCfield == 1 and target_bssid != 'ff:ff:ff:ff:ff:ff' and arp.op == 1 and \
        target_mac != 'ff:ff:ff:ff:ff:ff' and source_mac != target_mac:
            print ('%s [%s] '+great_success('ARP')+' who has %s? tell %s -> %s [%s] on BSSID %s') % \
            (get_manuf(source_mac),source_mac,arp.pdst,arp.psrc,get_manuf(target_mac),target_mac,target_bssid)
            UpdateDB(clientmac=source_mac, time=p.time, BSSID=target_mac)
```

iSniff_import.py uses scapy to sniff:

- Client MAC addresses
- Unicast ARPs (RFC 4436)
- MDNS (Bonjour) broadcasts
- SSID probes (802.11 Probe Requests)

Stored in Django backend database / web interface

```
$ ./isniff_import.py -h
usage: isniff_import.py [-h] [-r PCAP] [-i INTERFACE]

iSniff GPS Server

optional arguments:
  -h, --help    show this help message and exit
  -r PCAP       pcap file to read
  -i INTERFACE  interface to sniff (default mon0)

$ ./isniff_import.py -r ../chan11-03.cap
Reading ../chan11-03.cap...
Intel [00:24:d7:e2:61:5c] probe for LabPrivate
Intel [00:24:d7:e2:61:5c] probe for pentestdmz
Intel [00:24:d6:5c:e4:b6] probe for 101
Apple [40:a6:d9:7a:fe:21] probe for hidd3n_from_U
Apple [40:a6:d9:7a:fe:21] probe for iSniff Channel 11
40:a6:d9:7a:fe:21 is Hans-Musters-iPhone
Updated name of 40:a6:d9:7a:fe:21 to Hans-Musters-iPhone
Apple [40:a6:d9:7a:fe:21] ARP who has 192.168.1.254? tell 192.168.1.14 ->
Cisco [00:16:c8:30:cf:f4] on BSSID 00:14:6c:6c:48:48
Murata [00:37:6d:a2:f1:4f] probe for MerPoular
Murata [00:37:6d:a2:f1:4f] probe for BIGPOND
Murata [00:37:6d:a2:f1:4f] probe for WLAN
```

Overview of clients detected

iSniff GPS v0.1

https pentest.com/isniff-gps/

Clients | Networks | Apple WiFi Geolocation | SSID Search | Stats

1337 devices probing for 3543 networks detected

MAC | Name	Manufacturer	Probed for
00:c0:ca:	ALFA	BlackHat
00:21:e9:	Apple	ARP:00:14:7f: ARP:00:14:6c: Open Test Secure WiFi iSniff Channel 11
00:23:6c:	Apple	BlackHat
00:23:df: Dannys-iPhone	Apple	
...		
74:e1:b6:	Apple	hhonors
74:e1:b6:	Apple	linksys majorhome
74:e1:b6:	Apple	BlackHat ARP:00:0b:86: iSniff Channel 11 home-down BTOpenzone-H BTHub3-CGF3 TALKTALK-69B453 SKY47597 fulwith BTHomeHub-85B2 ARP:00:b0:0c:
74:e1:b6:	Apple	gogoinflight SFO-WiFi testline AMT Claremont WiFi greenwood pier SPH SPH_244 Ratna Ling Public sandpiper house Gaia_Anderson9 The Cottages BCC-WiFi Larkspur fiend fiend_EXT

Overview by network...

1337 devices probing for 3543 networks detected

SSID / BSSID	Probed for by	Last probed for
BlackHat	612 | d0:23:db:a7:ea:a5 58:1f:aa:71:3b:35 00:f4:b9:3f:e1:99 e4:ce:8f:d1:92:06 78:d6:f0:8d:9e:f5 ...	July 26, 2012, 10:11 p.m.
linksys	55 | e4:ce:8f:39:0c:9a 5c:0a:5b:23:84:fc d4:20:6d:27:24:d7 b0:65:bd:45:fd:bf c8:aa:21:81:08:a3 ...	July 26, 2012, 10:09 p.m.
CaesarsLV-Convention-Cox	52 | d0:23:db:a7:ea:a5 e4:ce:8f:39:0c:9a d8:a2:5e:1f:74:1e ec:85:2f:07:b5:ce 00:27:10:09:d2:6c ...	July 26, 2012, 10:06 p.m.
Boingo Hotspot	49 | e4:ce:8f:39:0c:9a d0:23:db:a2:50:d4 28:6a:ba:63:5d:61 88:c6:63:3a:9a:39 34:51:c9:d3:81:3d ...	July 26, 2012, 10:06 p.m.
gogoinflight	49 | a4:67:06:06:94:8a d0:23:db:a2:50:d4 28:6a:ba:63:5d:61 a4:67:06:c0:b6:e6 d0:23:db:b4:7b:bc ...	July 26, 2012, 10:04 p.m.
ibahn	41 | a4:67:06:06:94:8a a4:67:06:c0:b6:e6 28:6a:ba:34:6f:08 7c:6d:62:cf:cf:5b b8:ff:61:7c:7f:f5 ...	July 26, 2012, 10:04 p.m.
hhonors	38 | d0:23:db:a2:50:d4 e0:b9:ba:4a:bd:de 8c:58:77:83:80:23 10:bf:48:ca:53:07 28:6a:ba:a6:9b:13 ...	July 26, 2012, 10:09 p.m.
McCarran WiFi	31 | e4:ce:8f:d1:92:06 64:b9:e8:61:b2:ef 60:fa:cd:71:56:c6 a4:67:06:40:ef:6b 3c:d0:f8:d5:d9:bf ...	July 26, 2012, 10:10 p.m.
Cox-CaesarsLV-Rooms	30 | e4:ce:8f:d1:92:06 a4:67:06:c0:b6:e6 9c:20:7b:61:62:f7 60:fa:cd:71:56:c6 70:56:81:8c:71:e1 ...	July 26, 2012, 10:06 p.m.
SFO-WiFi	28 | e4:ce:8f:e3:4d:b6 68:09:27:c2:1b:87 68:a8:6d:6f:16:09 b8:ff:61:7c:7f:f5 18:34:51:16:32:39 ...	July 26, 2012, 10:02 p.m.

Clients probing for a particular network

Clients probing for network HACKER (Unknown)

MAC	Name
7c:6d:62:	
7c:6d:62:	
f0:cb:a1:	

iSniff GPS v0.1

https pentest.com/isniff-gps/client/74:e1:b6 Reader

Clients | Networks | Apple WiFi Geolocation | SSID Search | Stats

Client 74:e1:b6: (Apple)

Probed for:

SSID	BSSID	Lat	Lon	Comment	Last probe observed	Locate
BlackHat		36.11669159	-115.18044281		July 26, 2012, 10:11 p.m.	
	00:0b:86:				July 26, 2012, 9:46 p.m.	
iSniff Channel 11					July 26, 2012, 9:31 p.m.	
home-down					July 25, 2012, 10:16 p.m.	
BTOpenzone-H					July 25, 2012, 10:16 p.m.	
BTHub3-CGF3					July 25, 2012, 10:16 p.m.	
TALKTALK-69B453					July 25, 2012, 10:16 p.m.	
SKY47597					July 25, 2012, 10:16 p.m.	
fulwith					July 25, 2012, 10:16 p.m.	
BTHomeHub-85B2					July 25, 2012, 10:16 p.m.	
	00:b0:0c:	53.	-2.		July 25, 2012, 10:21 p.m.	

Display a menu

WiGLE.net™

Wireless Geographic Logging Engine: Making maps of wireless networks since 2001

92,907,539 wifi 2,267,952 cellular 1,803,941,848 unique observations

Logged in as wigle909 Logout

news:

WiGLE and Google help locate stolen laptop
Sat Apr 20 11:05:01 2013

WiGLE and Google help **locate a stolen laptop**. Yay for data.
-bobzilla

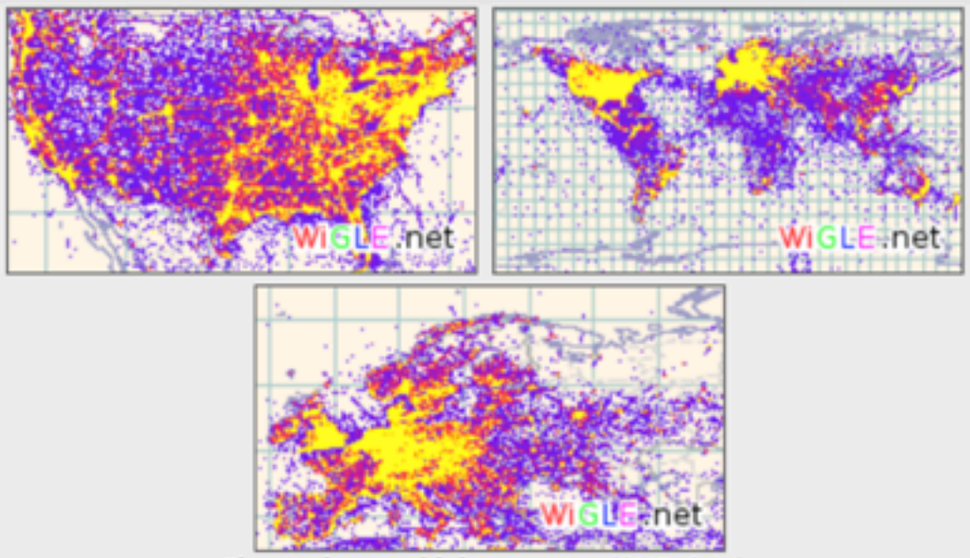
90 MEGANETS!
Wed Apr 3 18:18:34 2013

TROMOS has passed the 90M net mark, using WiGLEWiFi. I feel like sooner or later, we're destined for a scene like the one in ghostbusters, where we're forced to shut down the containment grid... AND ALL THE NETWORKS ESCAPE AND WREAK HAVOC!
-arkasha

New Geographic Statistics
Mon Feb 25 02:32:27 2013

It took 3 months of crunching, but we now have **Geographic Statistics** up. See what countries / states / postal codes have the most networks or the best crypto habits! Thanks to **Security B-Sides** at **DNA Lounge** for providing the

Help WiGLE: Please [**donate**] your points to the WiGLE commercial dataset



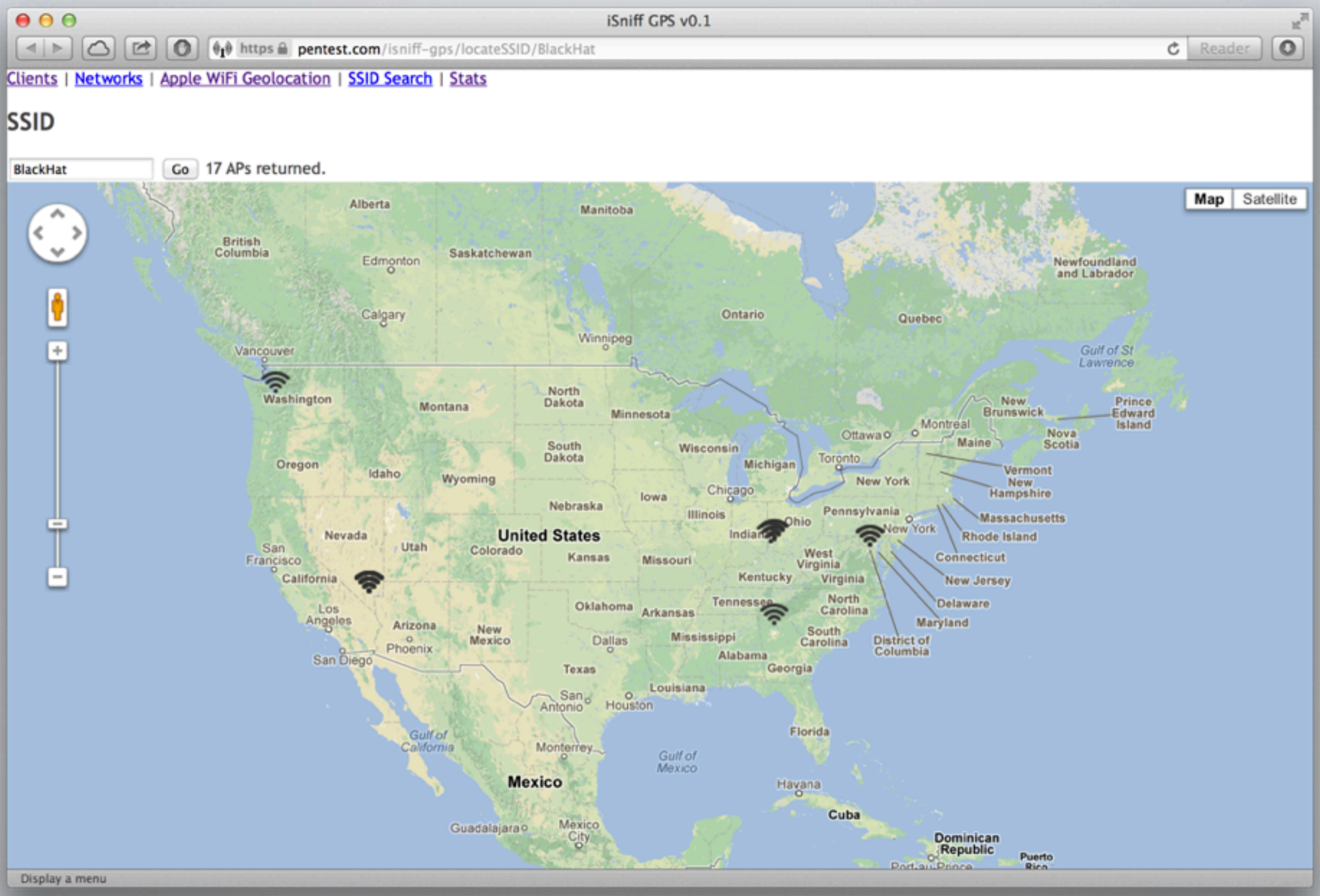
The wireless world this morning (GMT-6:00).

Find a wireless network by [searching] or [**browsing the interactive map**]

Add a wireless network to WiGLE [**from a stumble file**] or [**by hand**]

Add [**remarks**] to an existing network

Locations for SSID ‘BlackHat’ from wigle.net



How to locate a wifi router by MAC address?

Samy Kamkar "How I met your girlfriend"

DEF CON 18

Geolocation via XXXSS

- Upon MAC acquisition, ask the Google
- See FF source for Location Services

```
POST /loc/json HTTP/1.0
Host: www.google.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:
1.9.2b4) Gecko/20091124 Firefox/3.6b4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: none
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Length: 127
Content-Type: text/plain; charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache

{"version":"1.1.0","request_address":true,"wifi_towers":
[{"mac_address":"$mac","ssid":"g","signal_strength":-72}]}
```

How to locate a wifi router by MAC address?

- SKYHOOK WIRELESS
- Google (http://samy.pl/androidmap/)

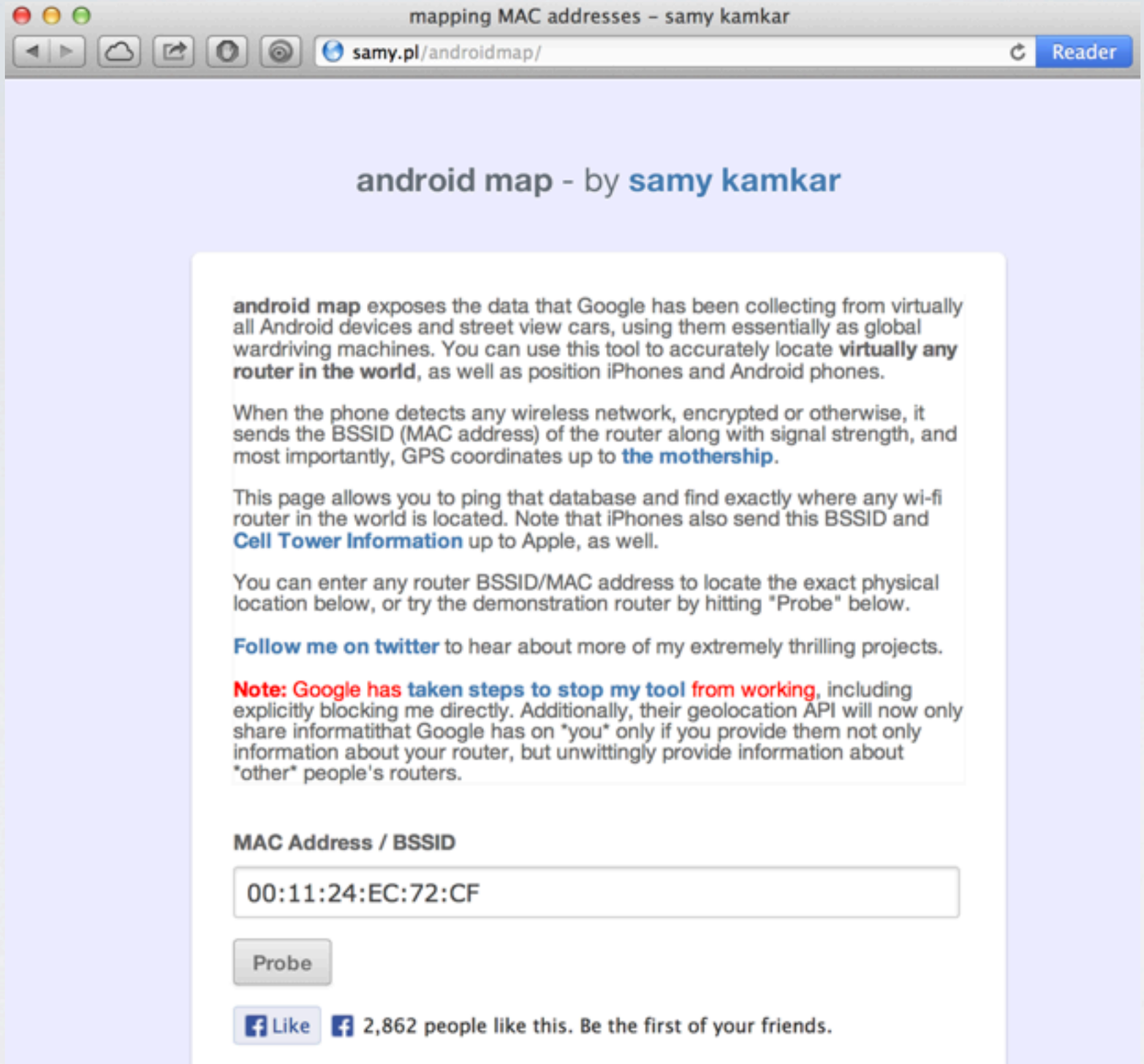
Google curbs Web map exposing phone locations

Google limits access to geolocation database linking Wi-Fi devices with physical locations after a CNET article highlights potential privacy concerns.

by Declan McCullagh | June 27, 2011 4:00 AM PDT

Follow

Google API restricted...



iOS device HTTPS request to Apple - Where am I?

Intercept | History | Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Modified	Status	Length
100	https://gs-loc.apple.com	POST	/clls/wloc	☑	☐	200	586

Request | Response

Raw | Params | Headers | Hex

```
POST /clls/wloc HTTP/1.1
Host: gs-loc.apple.com
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
Connection: keep-alive
Accept: */*
Content-Length: 236
User-Agent: locationd/1491.2.1 CFNetwork/609 Darwin/13.0.0

en_US com.apple.locationd 6.0.1.10A525[]
0:1c:28
0:1c:4a
0:22:3f
0:23:8:
0:23:8:
74:31:7
a2:5:43
e0:ca:9
e0:cb:4
```

Response from Apple

Intercept | History | Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Modified	Status	Length
100	https://gs-loc.apple.com	POST	/clls/wloc	☑	☐	200	586

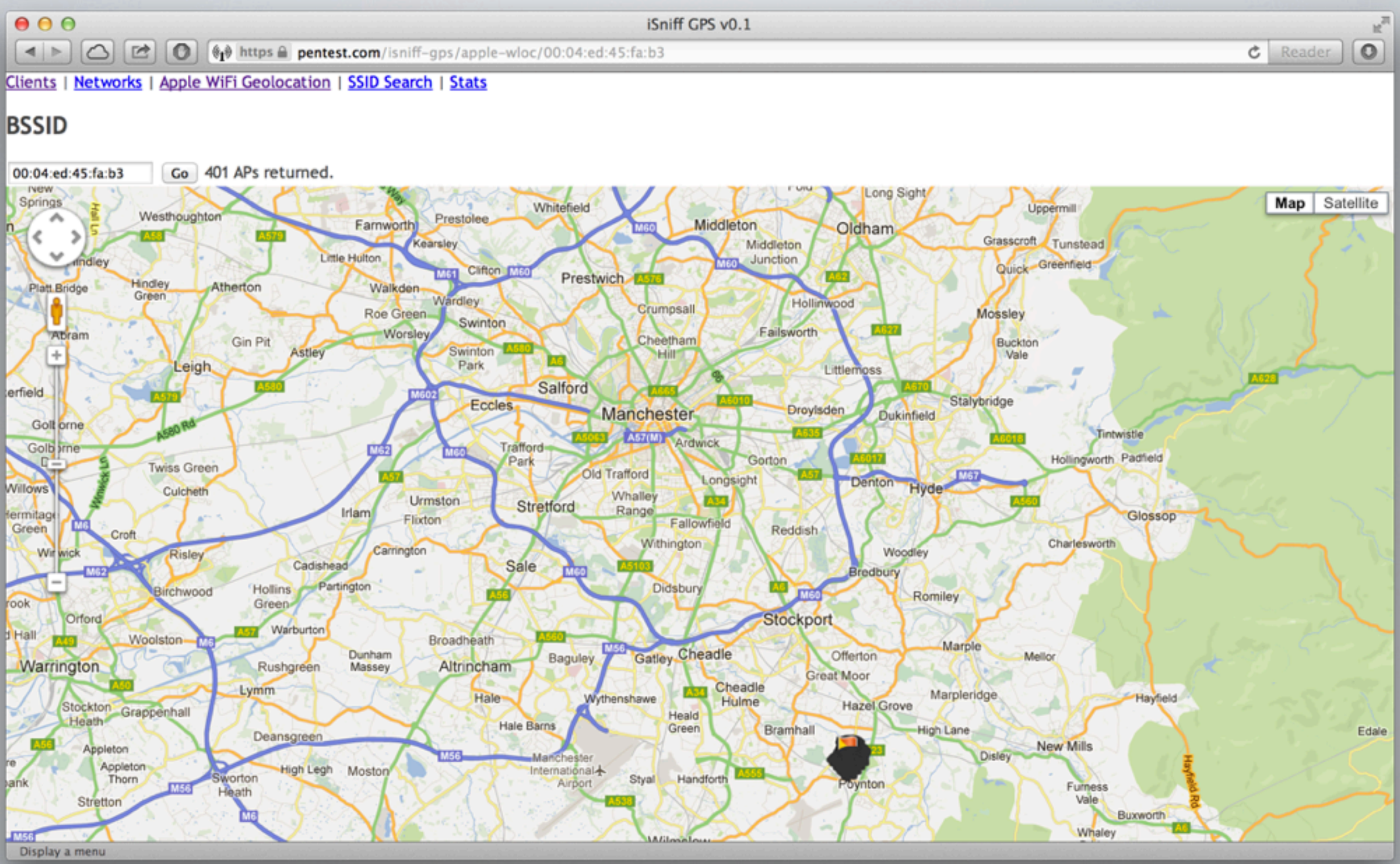
Request | Respo

Raw | Headers

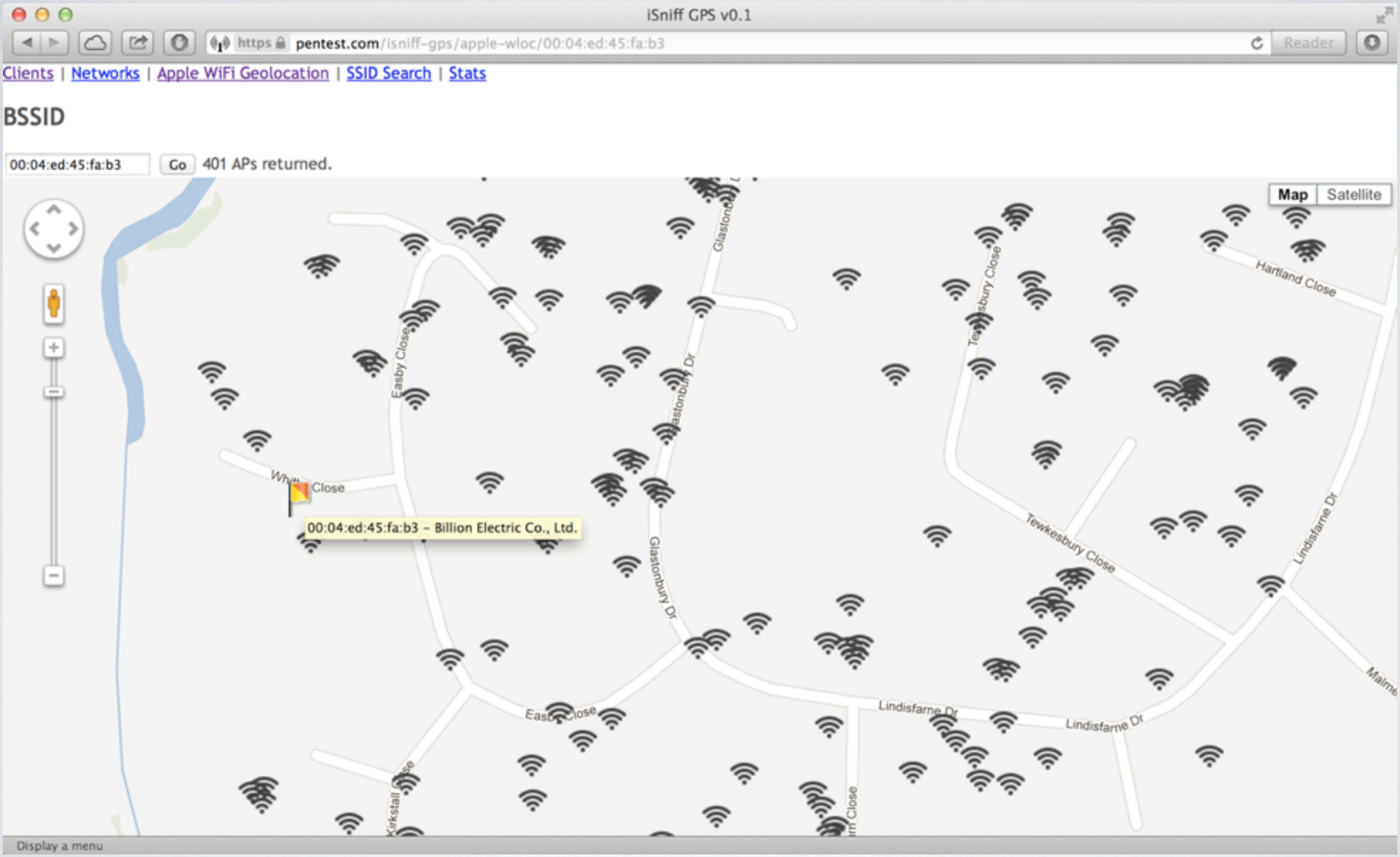
```
HTTP/1.1 200 OK
Server: Jetty(8.1.7.v20120910)
Content-Length: 514

- /
 0:1c:28:
 0:26:4d:
 0:1c:4a:
 0:22:3f:
 0:23:8:7
 0:23:8:f
 74:31:70
 a2:5:43:
 e0:ca:94
 e0:cb:4e
```

```
HTTP/1.1 200 OK

Wifi BSSID : e0:91:f5:fe:f6:60
Latitude : 48.87655264
Longitude : 2.32190334
Confiance : 42

------

Wifi BSSID : 0:1e:8c:4c:25:7b
Latitude : 48.87650626
Longitude : 2.32187509
Confiance : 42

------

Wifi BSSID : e0:a1:d7:73:94:0c
Latitude : 48.87662076
Longitude : 2.32189691
Confiance : 45

...
```

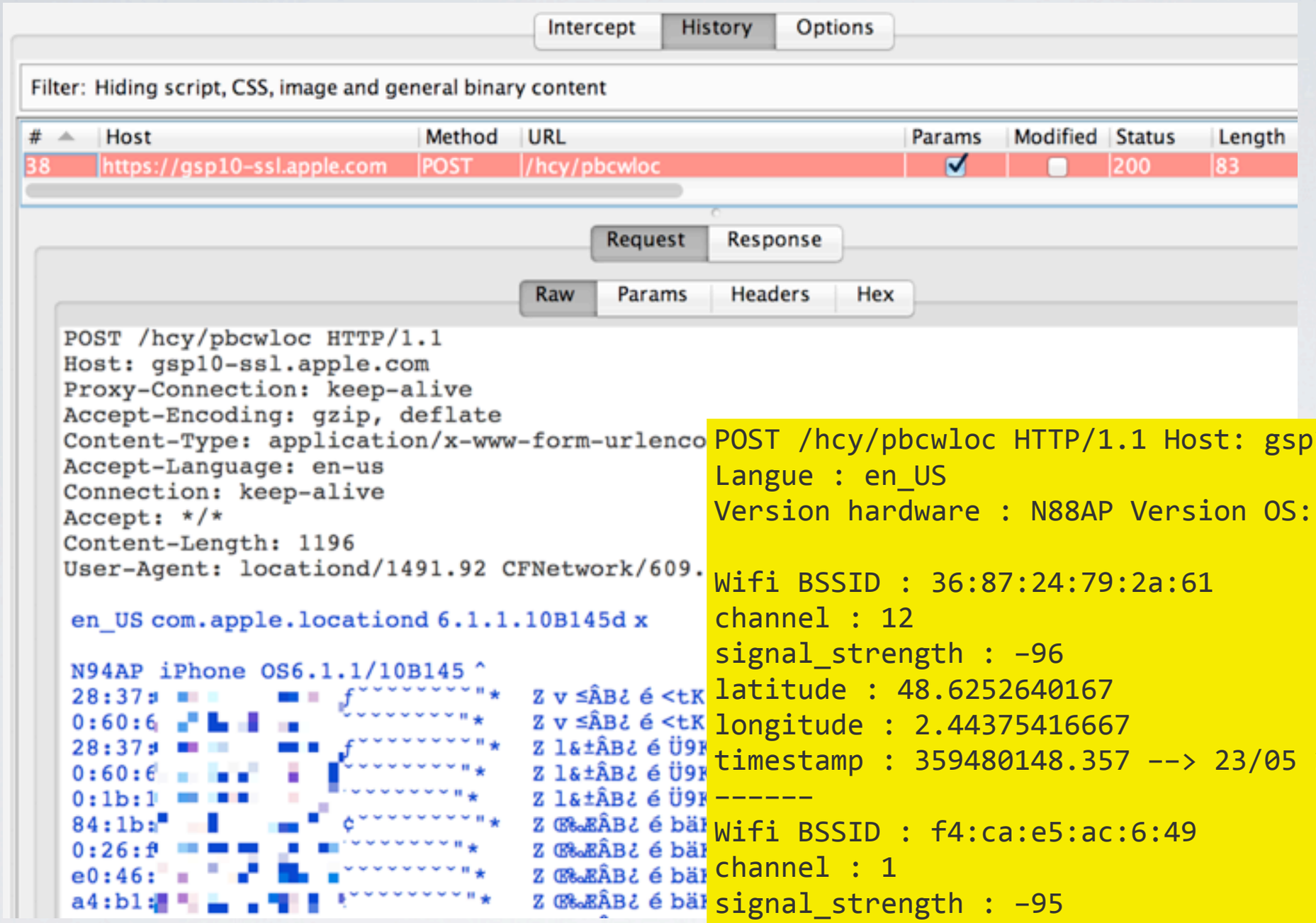
Response from Apple (Visualization)



Response from Apple (Visualization)



iOS device HTTPS request to Apple - Contributing data




```
POST /hcy/pbcwloc HTTP/1.1 Host: gsp10-ssl.apple.com
Langue : en_US
Version hardware : N88AP Version OS: iPhone OS5.1/9

Wifi BSSID : 36:87:24:79:2a:61
channel : 12
signal_strength : -96
latitude : 48.6252640167
longitude : 2.44375416667
timestamp : 359480148.357 --> 23/05 17:35:48
------
Wifi BSSID : f4:ca:e5:ac:6:49
channel : 1
signal_strength : -95
latitude : 48.6252640167
longitude : 2.44375416667
timestamp : 359480148.357 --> 23/05 17:35:48
------
```

Decoded sample request from http://fxaguessy.fr/rapport-pfe-interception-ssl-analyse-donnees-localisation-smartphones/

Opt Out?

Google Maps

Search M

Home | On Browser | On Android | On iPhone | Tips and Tricks | Blog | **Help**

Help home

Fix an issue

System requirements

Report a problem or fix the map

Issues while using Internet Explorer and Windows

Issues while using Firefox or other browsers

Configure access points with Google Location Service

Clear cache and cookies

Issues while using Street View in Windows 8

Configure access points with Google Location Service

To improve your use of location-based services, Google, as a location service provider, uses publicly broadcast Wi-Fi data from wireless access points, as well as GPS and cell tower data.

Location services play an important part in enabling many of today's most popular location-aware applications, in particular on smart phones, laptops and other devices that are WiFi enabled. The inclusion of your WiFi access point in the Google Location Service enables applications like Google Maps to work better and more accurately.

Only publicly broadcast Wi-Fi information is used to estimate the location of a device.

You can control whether or not your access point is included in GLS by following the steps below.

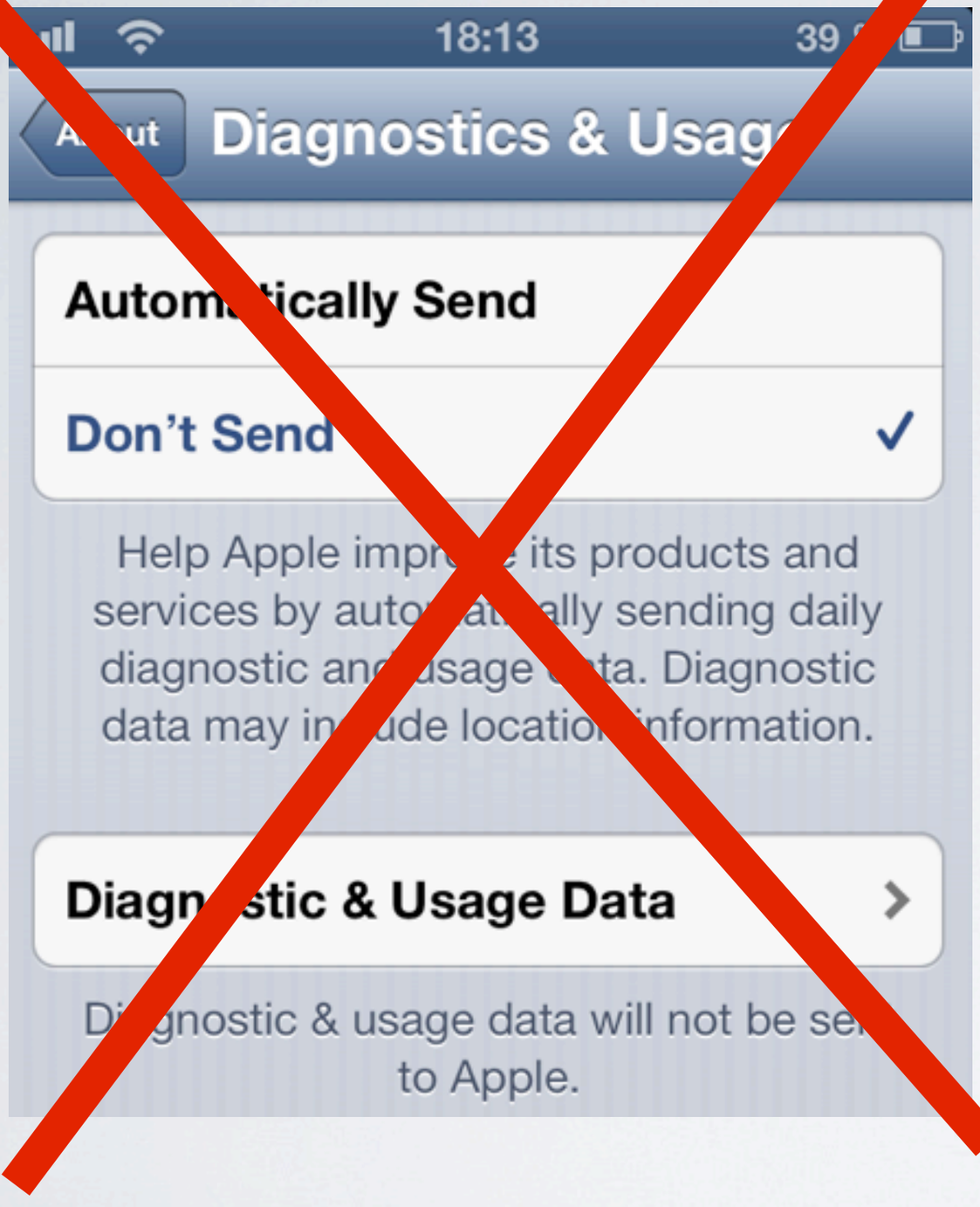
▼ How do I opt out?

You can opt out by changing the SSID (name) of your WiFi access point (your wireless network name) so that it ends with "_nomap". For example, if your SSID is "12345," you would need to change it to "12345_nomap".

You can click on the link below that corresponds to the manufacturer of your access point, to find specific instructions on changing your access point's SSID. If you received your access point from your ISP, you may wish to contact them to find out how to change the SSID.

- Apple
- Belkin
- Linksys (Cisco)
- Netgear

Apple iOS...



^ Makes no difference...

Experiment (Sample size = 2)

Netgear DG834 v3

Turned on 2013-02-27

SSID
"NETGEAR" (Broadcast disabled), no clients

First found in Apple Database 2013-03-15

~16 days

Netgear CG3100 Cable Modem

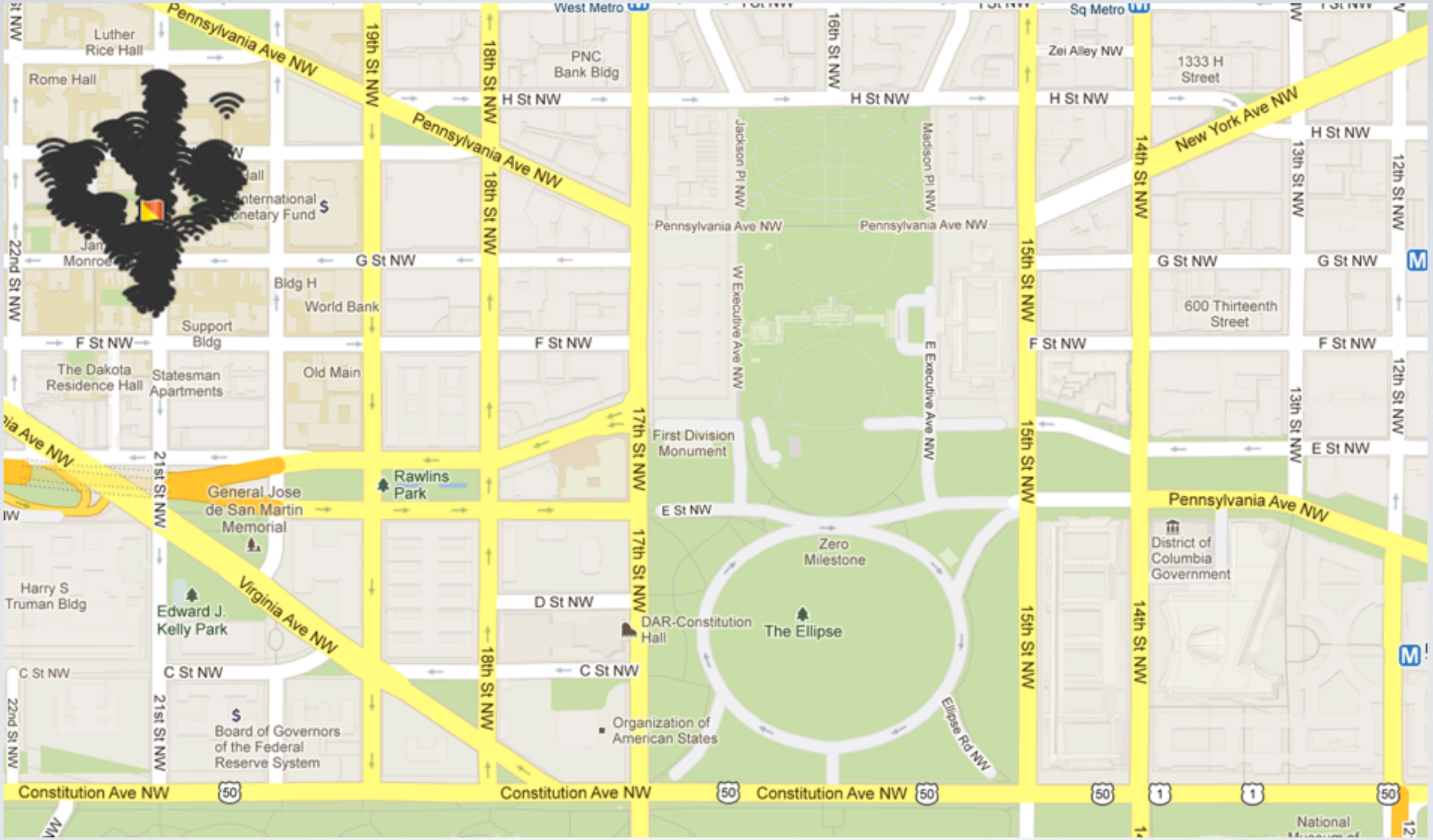
Turned on 2013-03-05

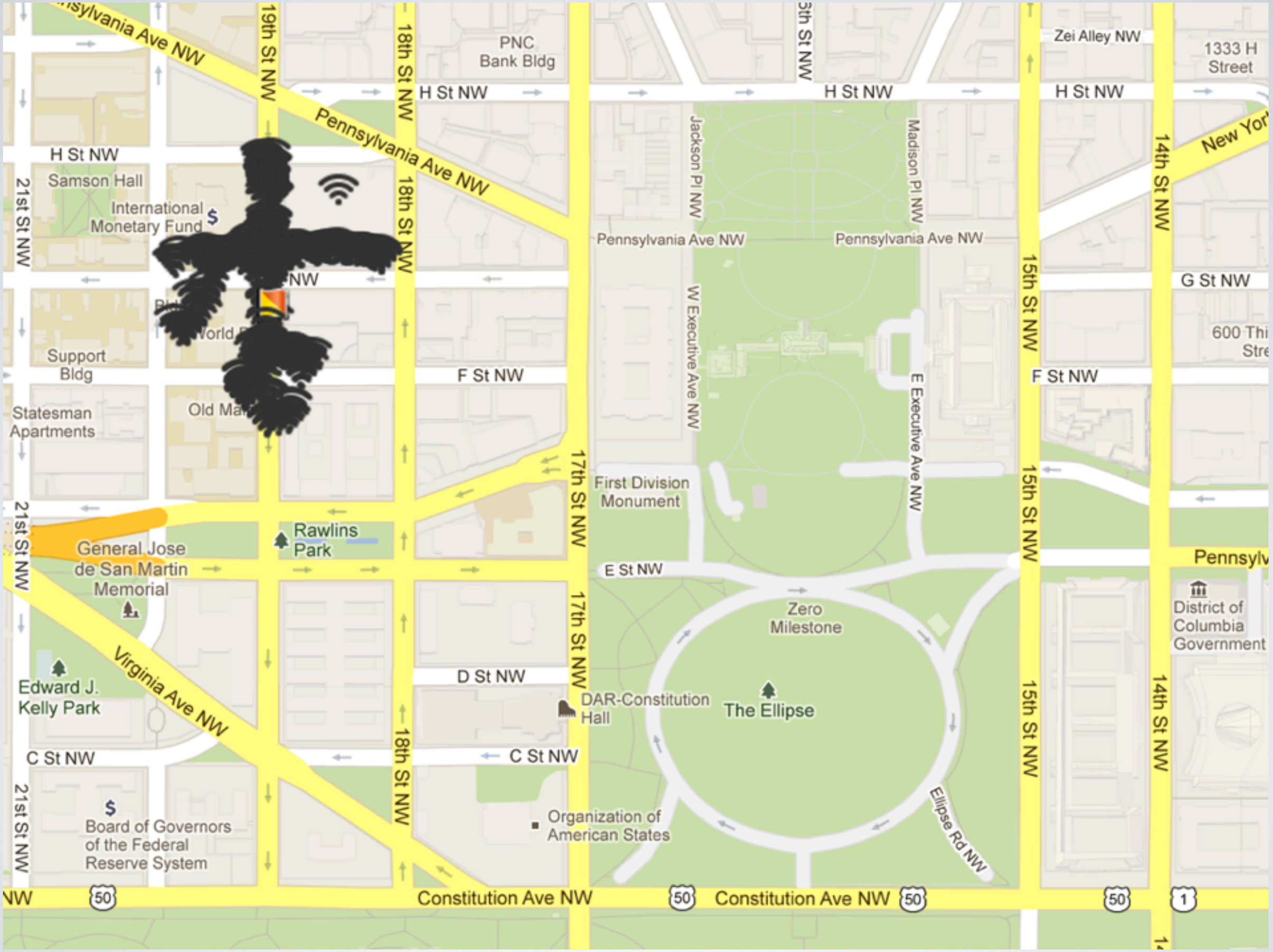
SSID broadcast enabled

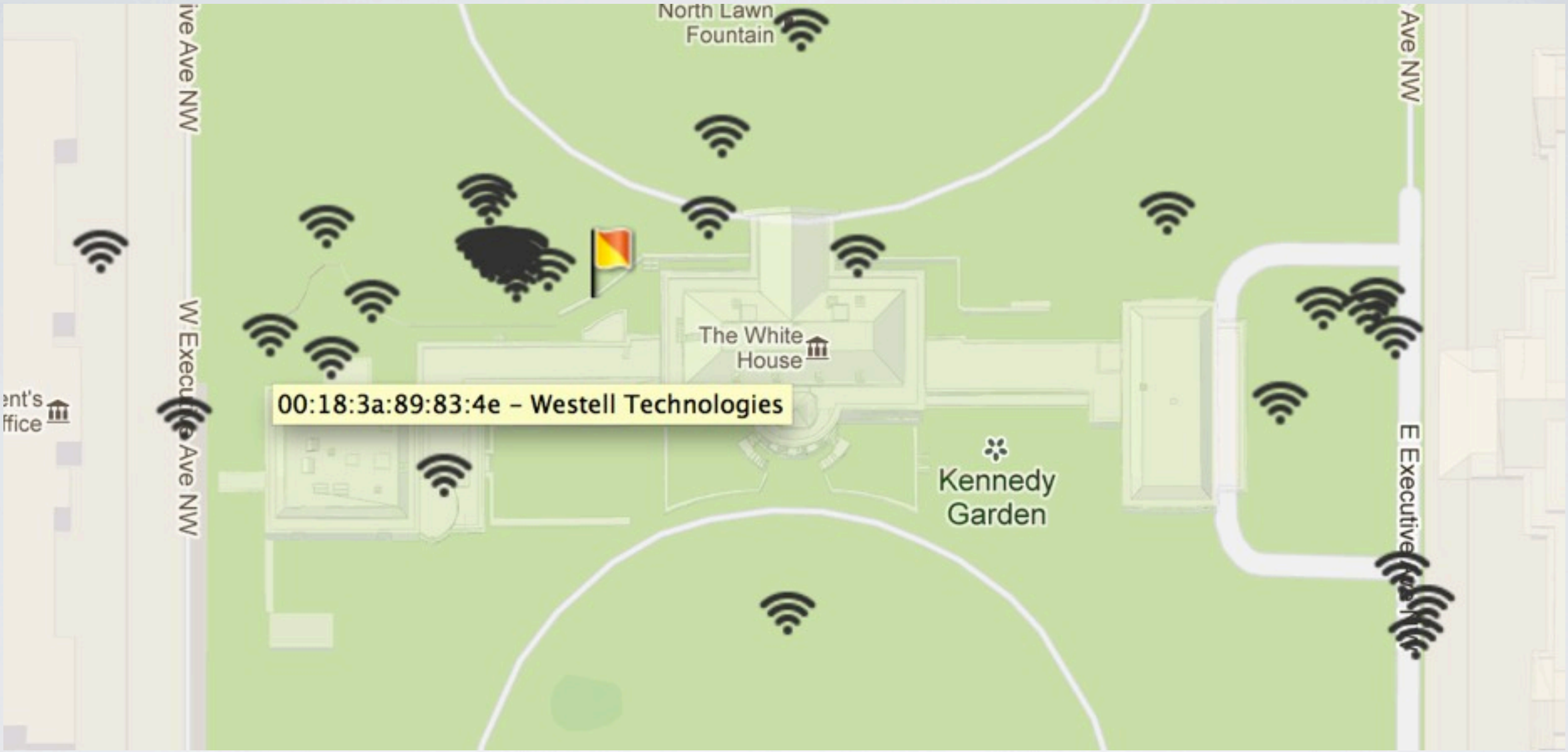
First found in Apple Database 2013-03-18

~13 days

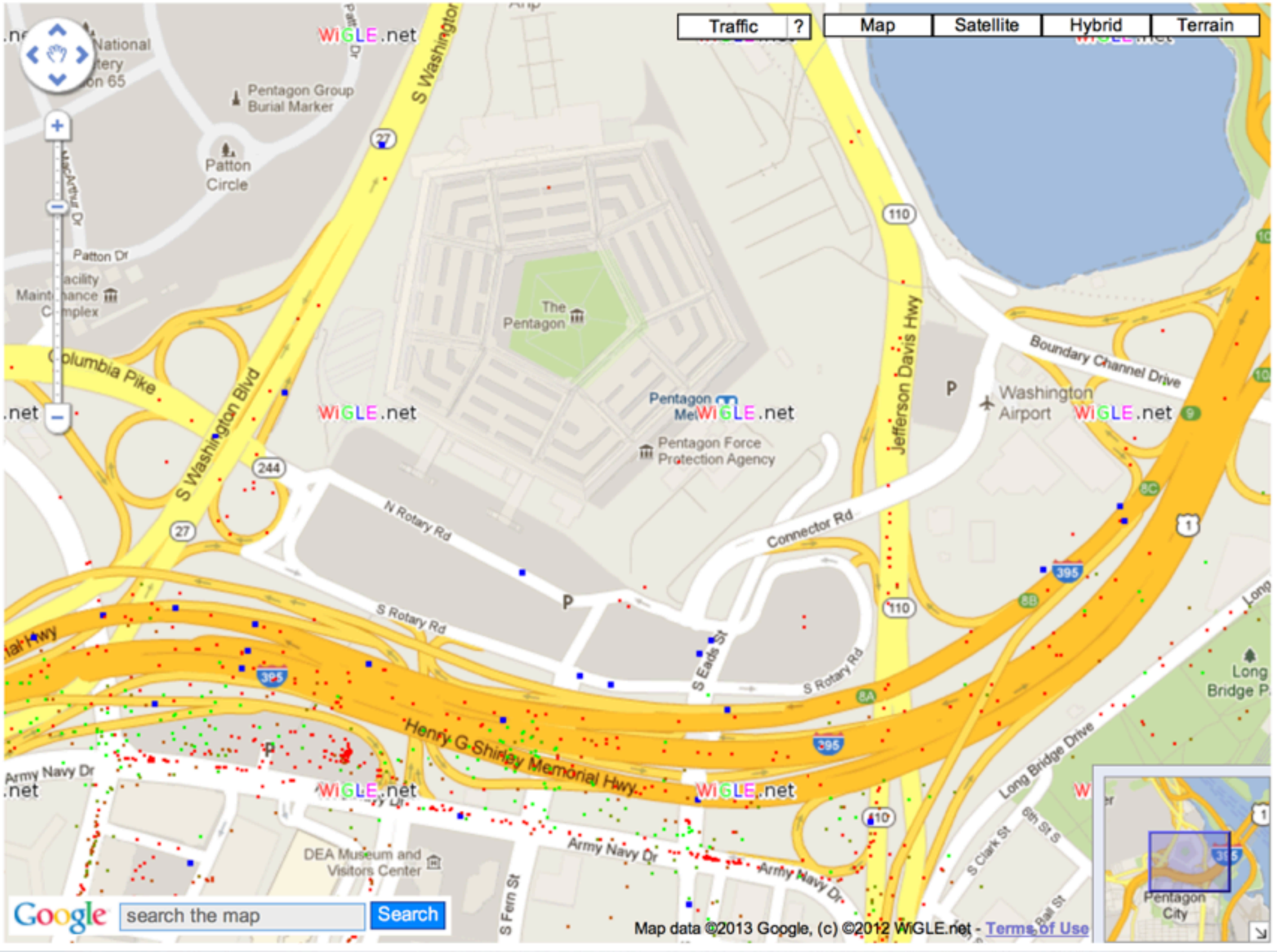
WiGLE.net
WiGLE.net
WiGLE.net
WiGLE.net
WiGLE.net
WiGLE.net
The White House
White House Rose Garden
The White House South Lawn
White House Basketball Court
White House Visitor Center
W Executive Ave NW
E Executive Ave NW
State Pl NW
E St NW
The Treasury
Free Public WiFi
WL-GUEST
ABCNEWS
Inauguration5
Inauguration4
Snapper
EIG-Internal
CNN ALBERTER
T-Mobile
Virgin Mobile
TWTWhiteHouse
hpsetup
bsnyden
ke_guest
Skadden-Guest
HTC Sensation 4G
B&D Tailors
Free Public WiFi
Silver Fox Bus 28A1E
Ramada
belkin.44
Booboo_Kitty


Pennsylvania Ave NW
West Metro
Sq Metro
Luther Rice Hall
Rome Hall
PNC Bank Bldg
Zei Alley NW
1333 H Street
H St NW
19th St NW
18th St NW
16th St NW
14th St NW
New York Ave NW
13th St NW
12th St NW
Jackson Pl NW
Madison Pl NW
G St NW
600 Thirteenth Street
F St NW
22nd St NW
Bldg H
World Bank
Support Bldg
The Dakota Residence Hall
Statesman Apartments
Old Main
17th St NW
15th St NW
First Division Monument
W Executive Ave NW
E Executive Ave NW
E St NW
Rawlins Park
General Jose de San Martin Memorial
Zero Milestone
District of Columbia Government
21st St NW
Harry S Truman Bldg
Edward J. Kelly Park
Virginia Ave NW
D St NW
DAR-Constitution Hall
The Ellipse
C St NW
Board of Governors of the Federal Reserve System
Organization of American States
Ellipse Rd NW
Constitution Ave NW
50
1
National


Pennsylvania Ave NW
19th St NW
18th St NW
PNC
Bank Bldg
H St NW
Samson Hall
21st St NW
International
Monetary Fund
$
Support
Bldg
F St NW
Statesman
Apartments
Old Ma
Jackson Pl NW
Madison Pl NW
Pennsylvania Ave NW
Pennsylvania Ave NW
W Executive Ave NW
E Executive Ave
17th St NW
First Division
Monument
15th St NW
Zei Alley NW
1333 H
Street
14th St NW
New Yor
G St NW
600 Thi
Stre
Pennsylv
District of
Columbia
Government
Rawlins
Park
General Jose
de San Martin
Memorial
E St NW
Zero
Milestone
Virginia Ave NW
Edward J.
Kelly Park
D St NW
DAR-Constitution
Hall
The Ellipse
C St NW
C St NW
Board of Governors
of the Federal
Reserve System
Organization of
American States
Ellipse Rd NW
Constitution Ave NW
Constitution Ave NW
50
1


North Lawn
Fountain
The White
House
00:18:3a:89:83:4e - Westell Technologies
Kennedy
Garden
E Executive
Ave NW
W Executive Ave NW

Browsable Map o' the World



Clients | Networks | Apple WiFi Geolocation | SSID Searc

Toggle markers | Filter | Show all | Toggle heatmap | Change gradient | Change radius | Change opacity

BSSID d8:c7:c8:d2:6a:21

2174 APs (0 added)

Clients | Networks | Apple WiFi Geolocation | SSID Search | Stats

Toggle markers | Filter | Show all | Toggle heatmap | Change gradient | Change radius | Change opacity

BSSID d8:c7:c8:d2:6a:21

114 APs matching aruba

iSniff GPS KML export in Google Earth

THANKS

iSniff GPS tool and slides by @hubert3
hubert(a)pentest.com

https://github.com/hubert3/isniff-gps

Using code published by François-Xavier Aguessy and Côme Demoustier

http://fxaguessy.fr/rapport-pfe-interception-ssl-analyse-donnees-localisation-smartphones/