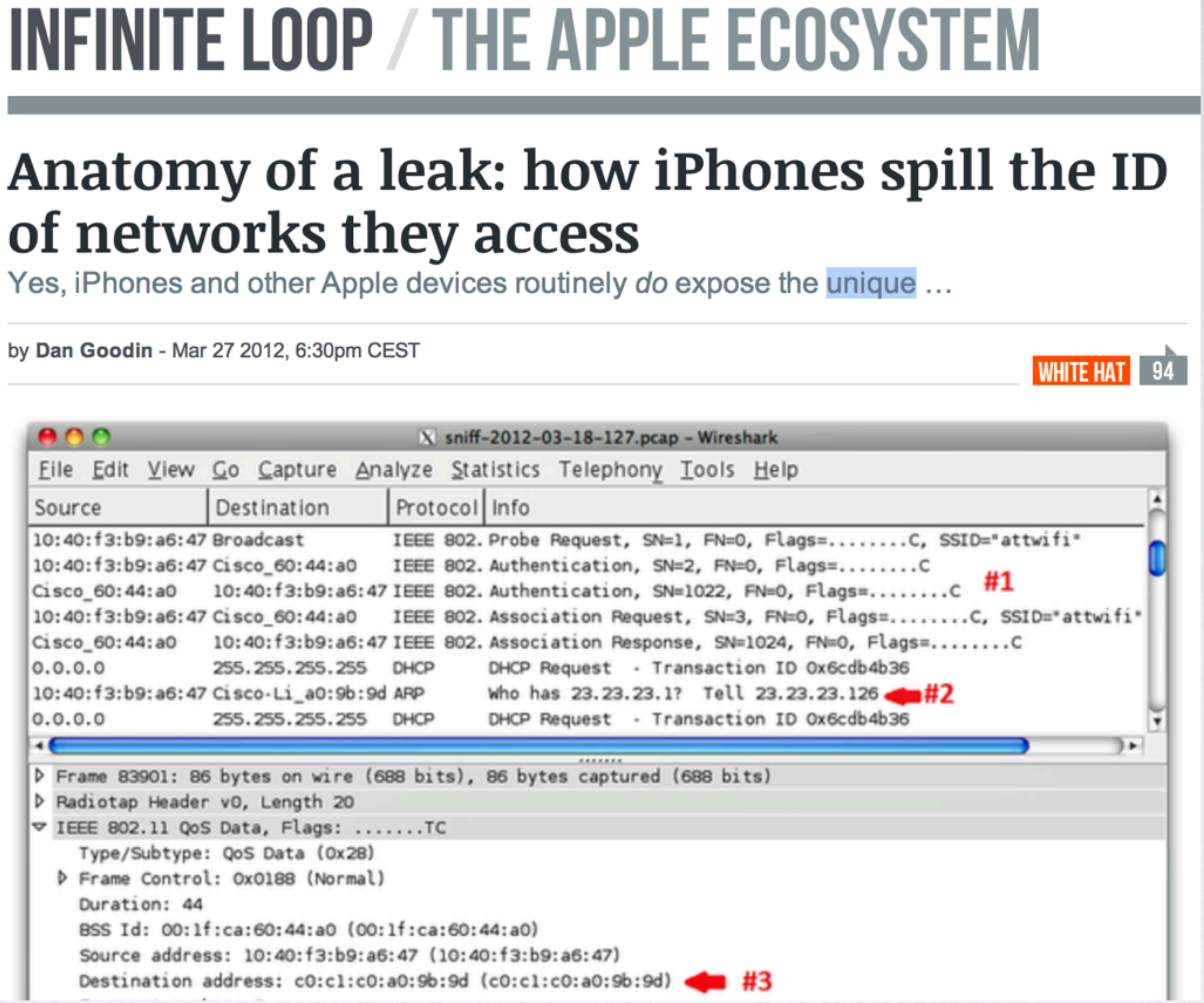
ISNIFF GPS

WHERE HAS YOUR IPHONE BEEN?

29c3 Lightning Talk
December 2012

@hubert3
hubert(a)pentest.com



INFINITE LOOP / THE APPLE ECOSYSTEM

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

sniff-2012-03-18-127.pcap - Wireshark

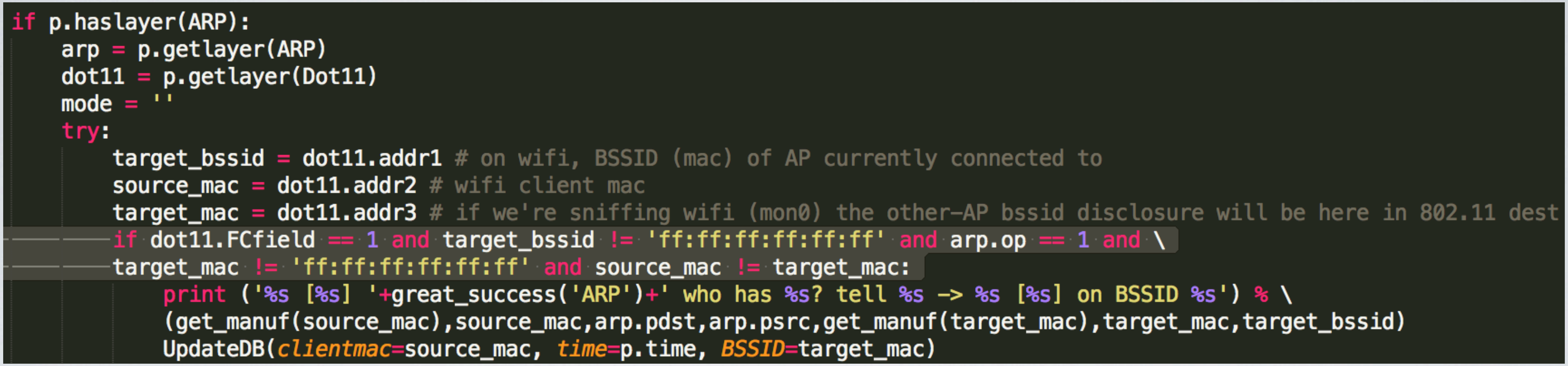
File Edit View Go Capture Analyze Statistics Telephony Tools Help

```
Source            Destination       Protocol Info
10:40:f3:b9:a6:47 Broadcast         IEEE 802. Probe Request, SN=1, FN=0, Flags=........C, SSID="attwifi"
10:40:f3:b9:a6:47 Cisco_60:44:a0    IEEE 802. Authentication, SN=2, FN=0, Flags=........C
Cisco_60:44:a0    10:40:f3:b9:a6:47 IEEE 802. Authentication, SN=1022, FN=0, Flags=........C
10:40:f3:b9:a6:47 Cisco_60:44:a0    IEEE 802. Association Request, SN=3, FN=0, Flags=........C, SSID="attwifi"
Cisco_60:44:a0    10:40:f3:b9:a6:47 IEEE 802. Association Response, SN=1024, FN=0, Flags=........C
0.0.0.0           255.255.255.255   DHCP      DHCP Request  - Transaction ID 0x6cdb4b36
10:40:f3:b9:a6:47 Cisco-Li_a0:9b:9d ARP       Who has 23.23.23.1?  Tell 23.23.23.126
0.0.0.0           255.255.255.255   DHCP      DHCP Request  - Transaction ID 0x6cdb4b36

▷ Frame 83901: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▷ Radiotap Header v0, Length 20
▽ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x28)
  ▷ Frame Control: 0x0188 (Normal)
    Duration: 44
    BSS Id: 00:1f:ca:60:44:a0 (00:1f:ca:60:44:a0)
    Source address: 10:40:f3:b9:a6:47 (10:40:f3:b9:a6:47)
    Destination address: c0:c1:c0:a0:9b:9d (c0:c1:c0:a0:9b:9d)
```

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

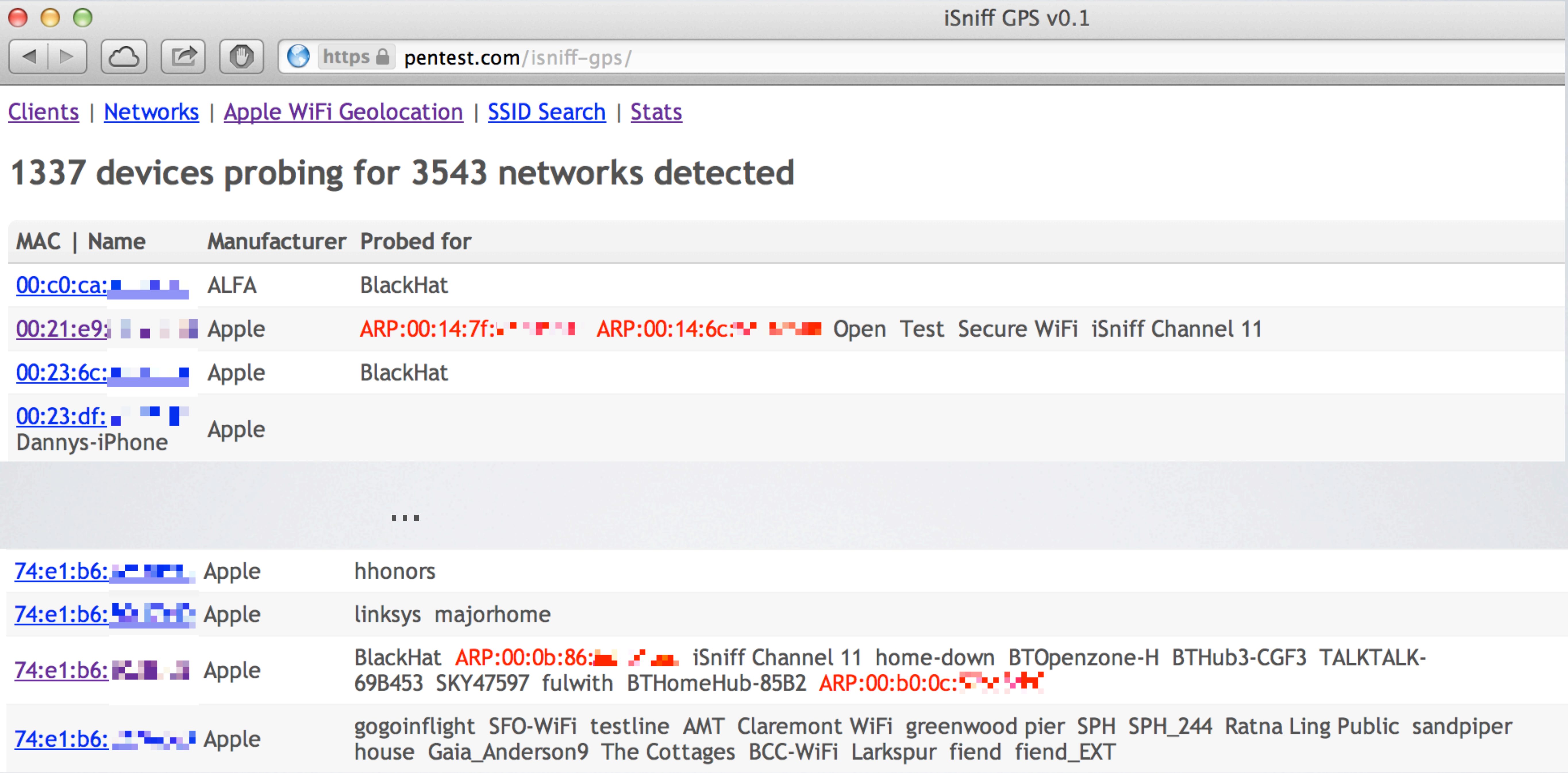
```
$ ./isniff_import.py -h
usage: isniff_import.py [-h] [-r PCAP] [-i INTERFACE]

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
```

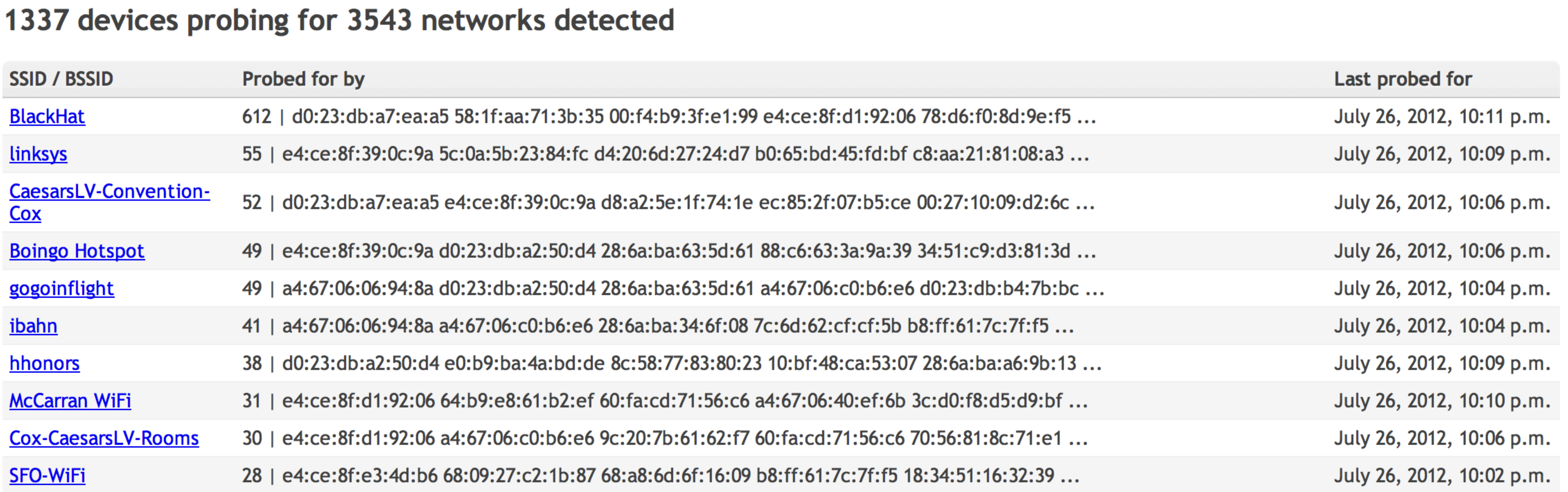
Overview of clients detected


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:[redacted]	ALFA	BlackHat
00:21:e9:[redacted]	Apple	ARP:00:14:7f:[redacted] ARP:00:14:6c:[redacted] Open Test Secure WiFi iSniff Channel 11
00:23:6c:[redacted]	Apple	BlackHat
00:23:df:[redacted] Dannys-iPhone	Apple	
		...
74:e1:b6:[redacted]	Apple	hhonors
74:e1:b6:[redacted]	Apple	linksys majorhome
74:e1:b6:[redacted]	Apple	BlackHat ARP:00:0b:86:[redacted] iSniff Channel 11 home-down BTOpenzone-H BTHub3-CGF3 TALKTALK-69B453 SKY47597 fulwith BTHomeHub-85B2 ARP:00:b0:0c:[redacted]
74:e1:b6:[redacted]	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

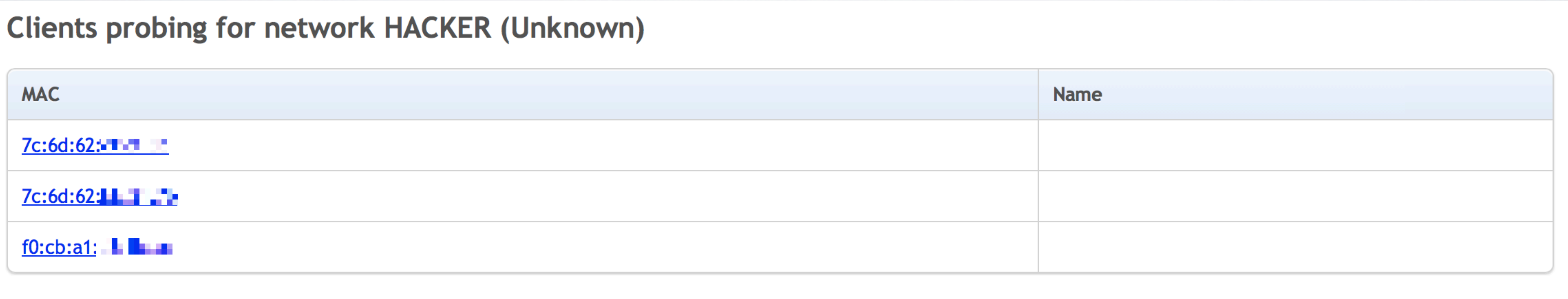
Overview by network...



1337 devices probing for 3543 networks detected

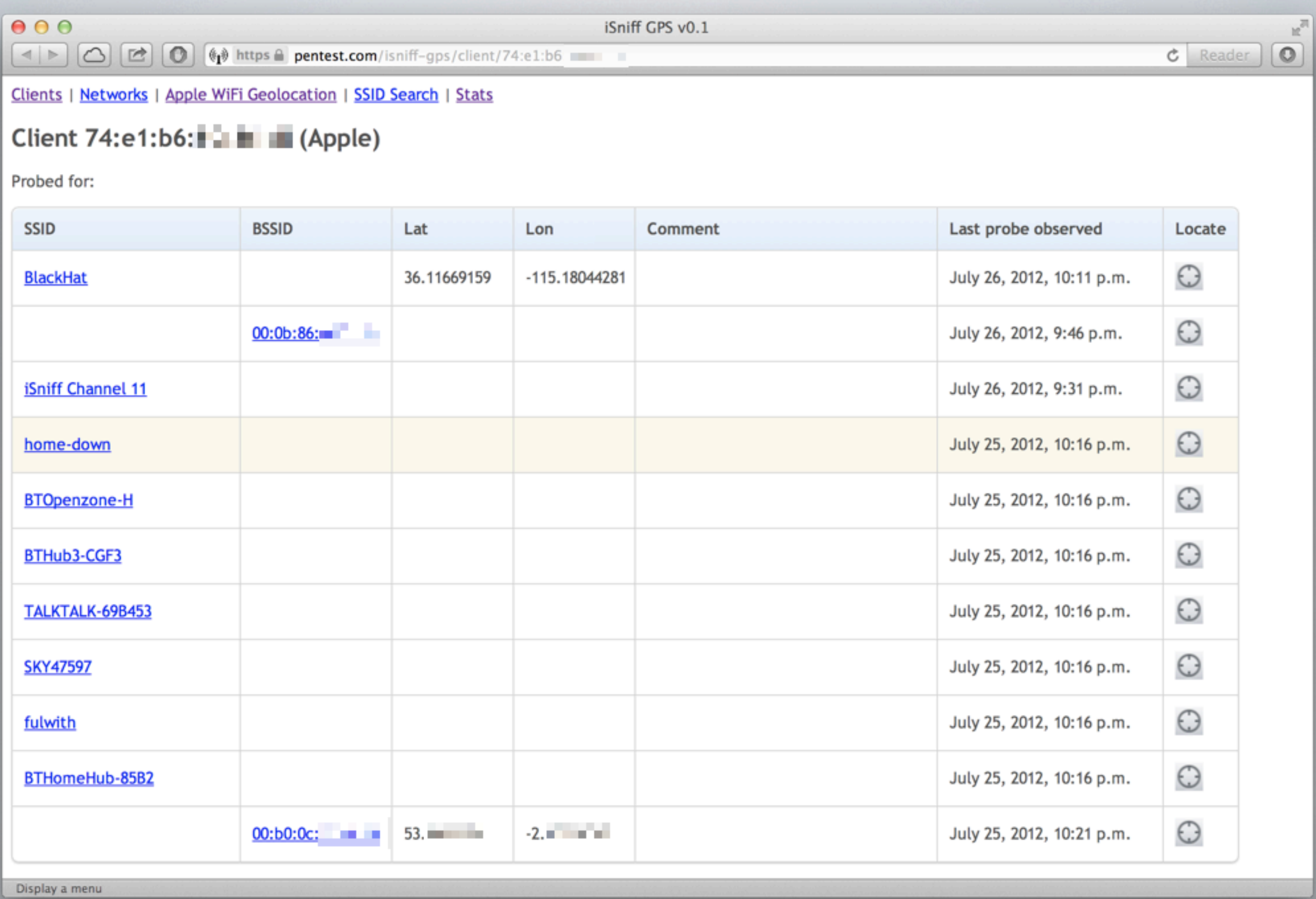
SSID / BSSID	Probed for by	Last probed for
BlackHat	612 | d0:23:db:a7:ea:a5 58:1f:aa:71:3b:35 00:f4:b9:3f:e1:99 e4:ce:8f:d1:92:06 78:d6:f0:8d:9e:f5 ...	July 26, 2012, 10:11 p.m.
linksys	55 | e4:ce:8f:39:0c:9a 5c:0a:5b:23:84:fc d4:20:6d:27:24:d7 b0:65:bd:45:fd:bf c8:aa:21:81:08:a3 ...	July 26, 2012, 10:09 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:[redacted]	
7c:6d:62:[redacted]	
f0:cb:a1:[redacted]	



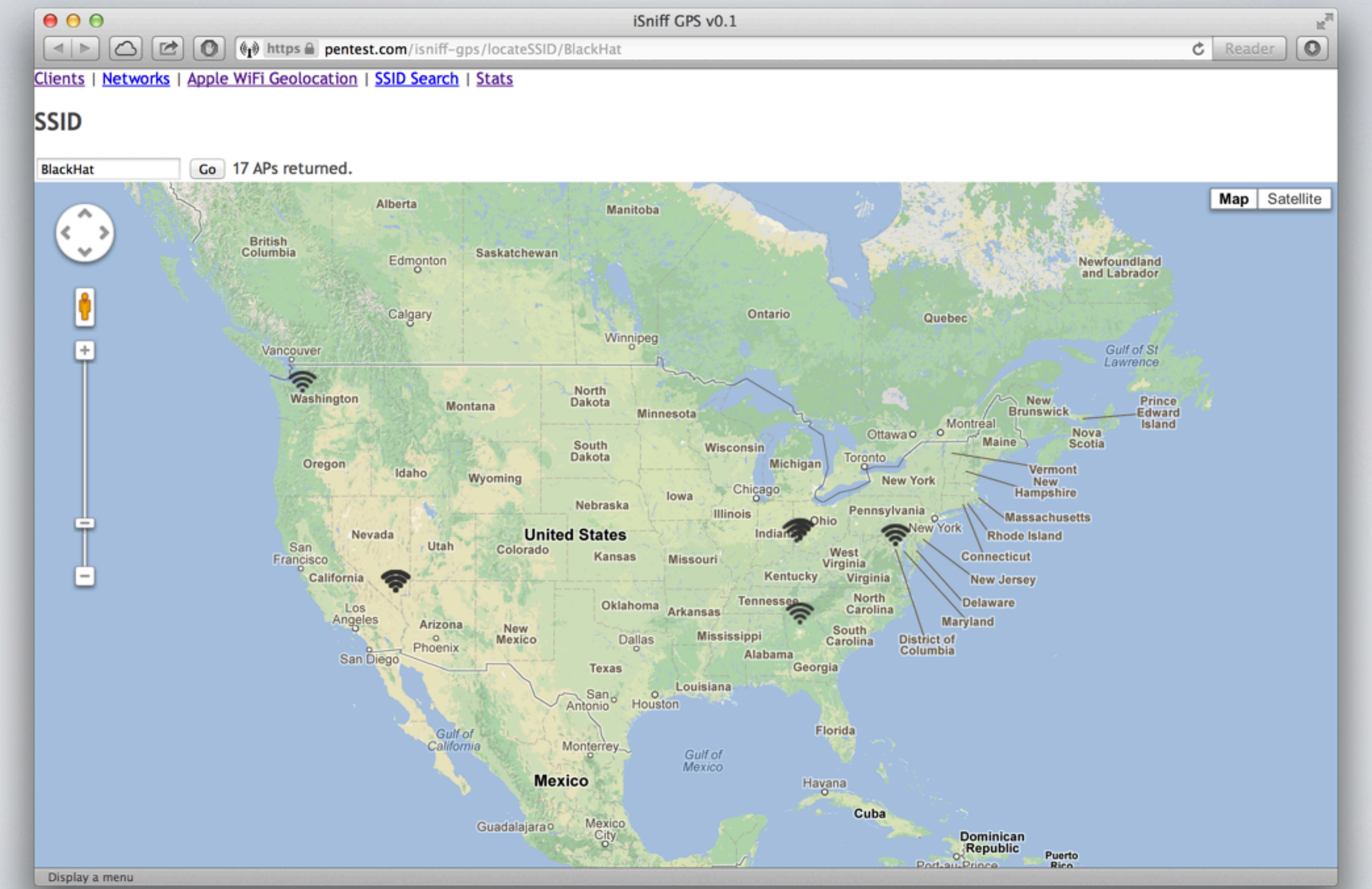
Clients | Networks | Apple WiFi Geolocation | SSID Search | Stats

Client 74:e1:b6:[redacted] (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:[redacted]				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:[redacted]	53.[redacted]	-2.[redacted]		July 25, 2012, 10:21 p.m.	⌖

Locations for SSID ‘BlackHat’ from wigle.net



iSniff GPS v0.1

https pentest.com/isniff-gps/locateSSID/BlackHat

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

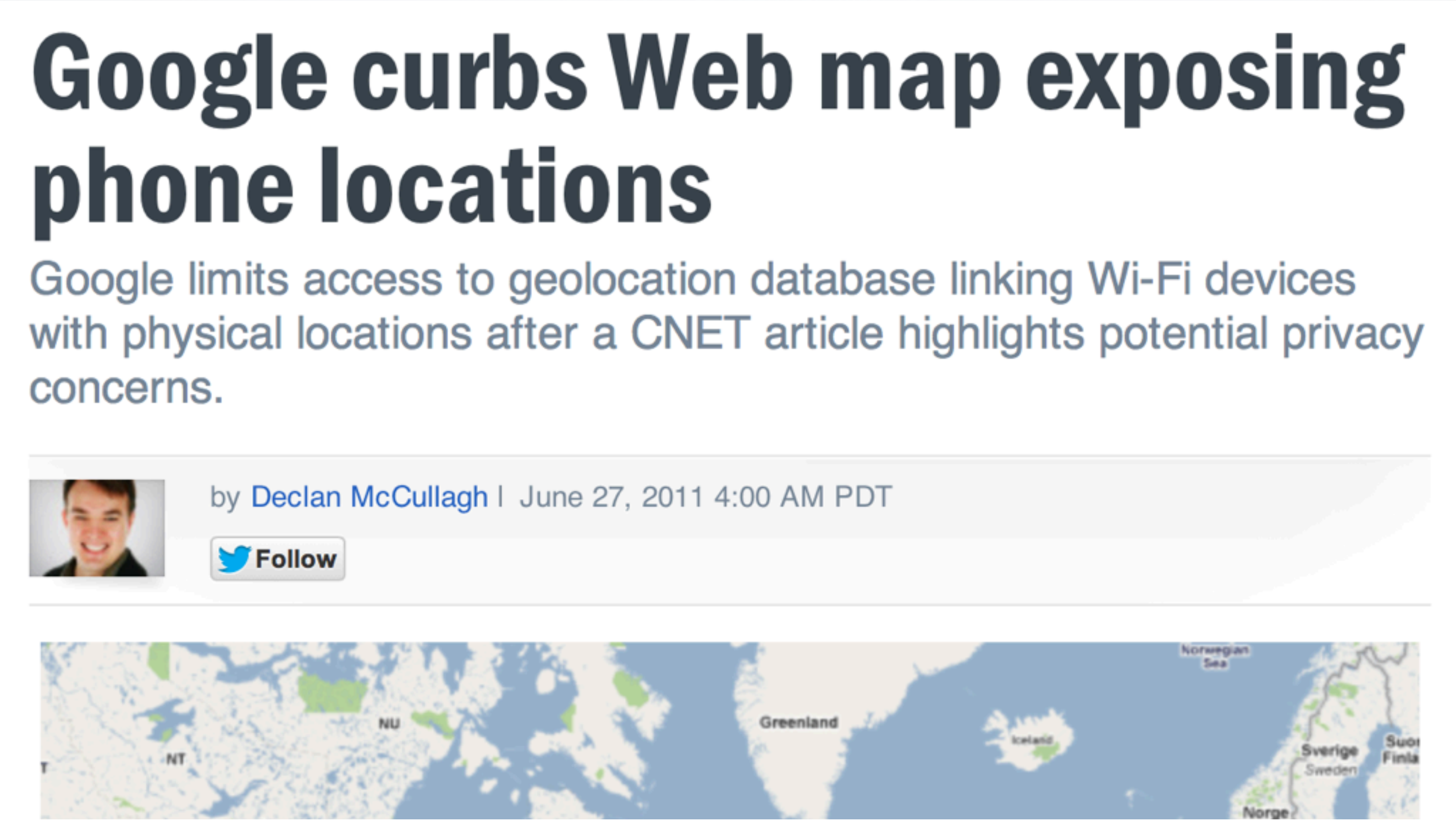
SSID

BlackHat Go 17 APs returned.

Display a menu

How to locate a wifi router by MAC address?

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

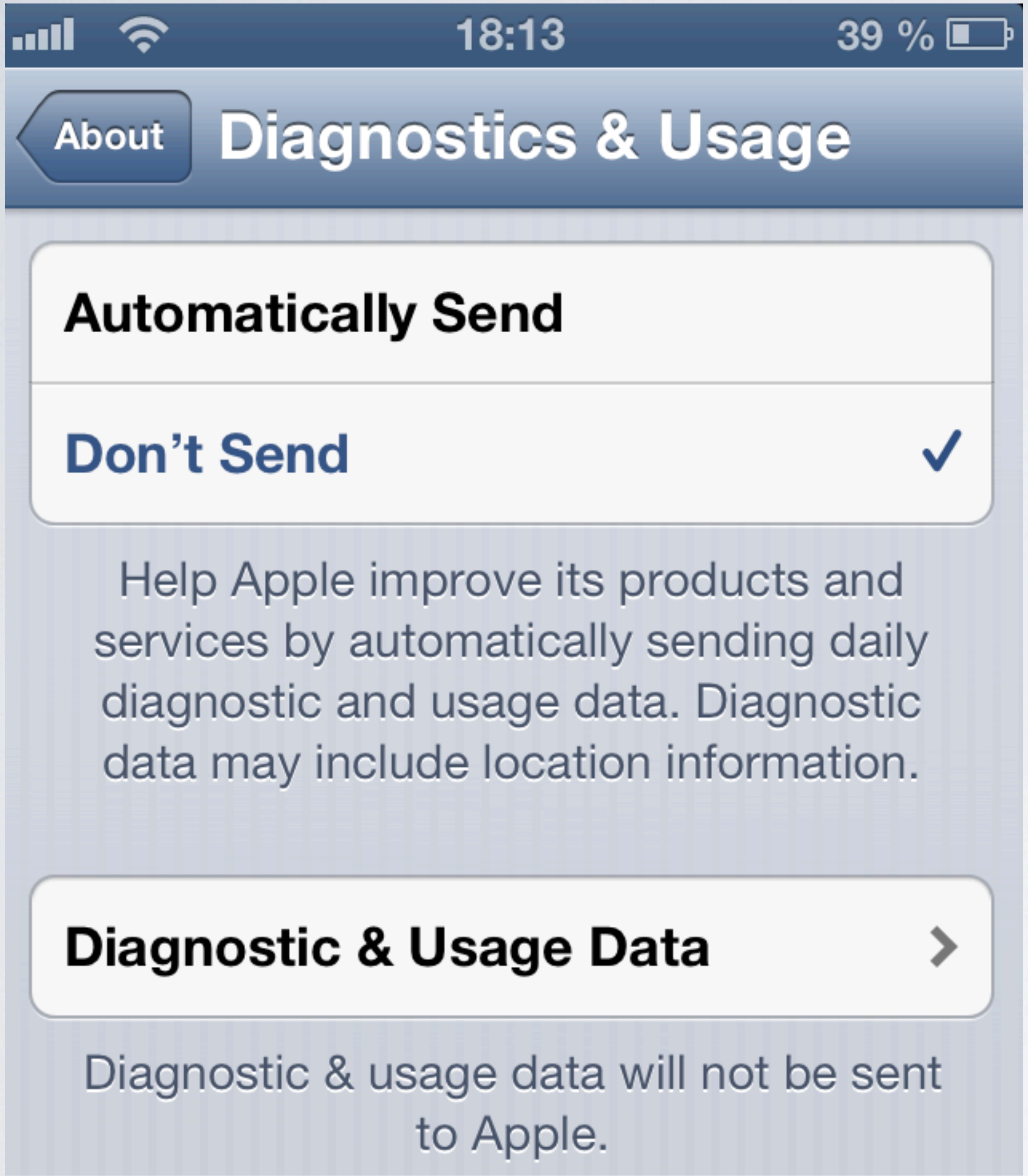


Google curbs Web map exposing phone locations

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

Apple iOS...



Diagnostics & Usage

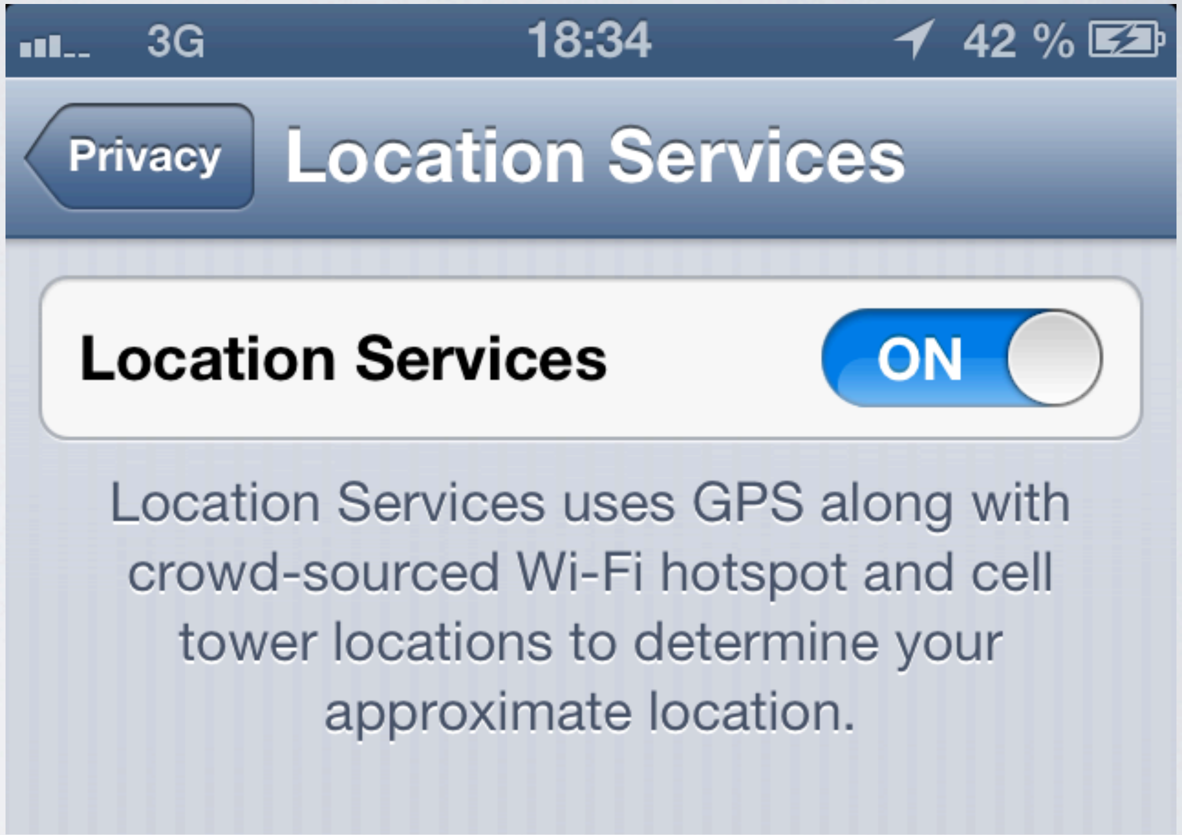
Automatically Send

Don't Send ✓

Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Diagnostic data may include location information.

Diagnostic & Usage Data >

Diagnostic & usage data will not be sent to Apple.

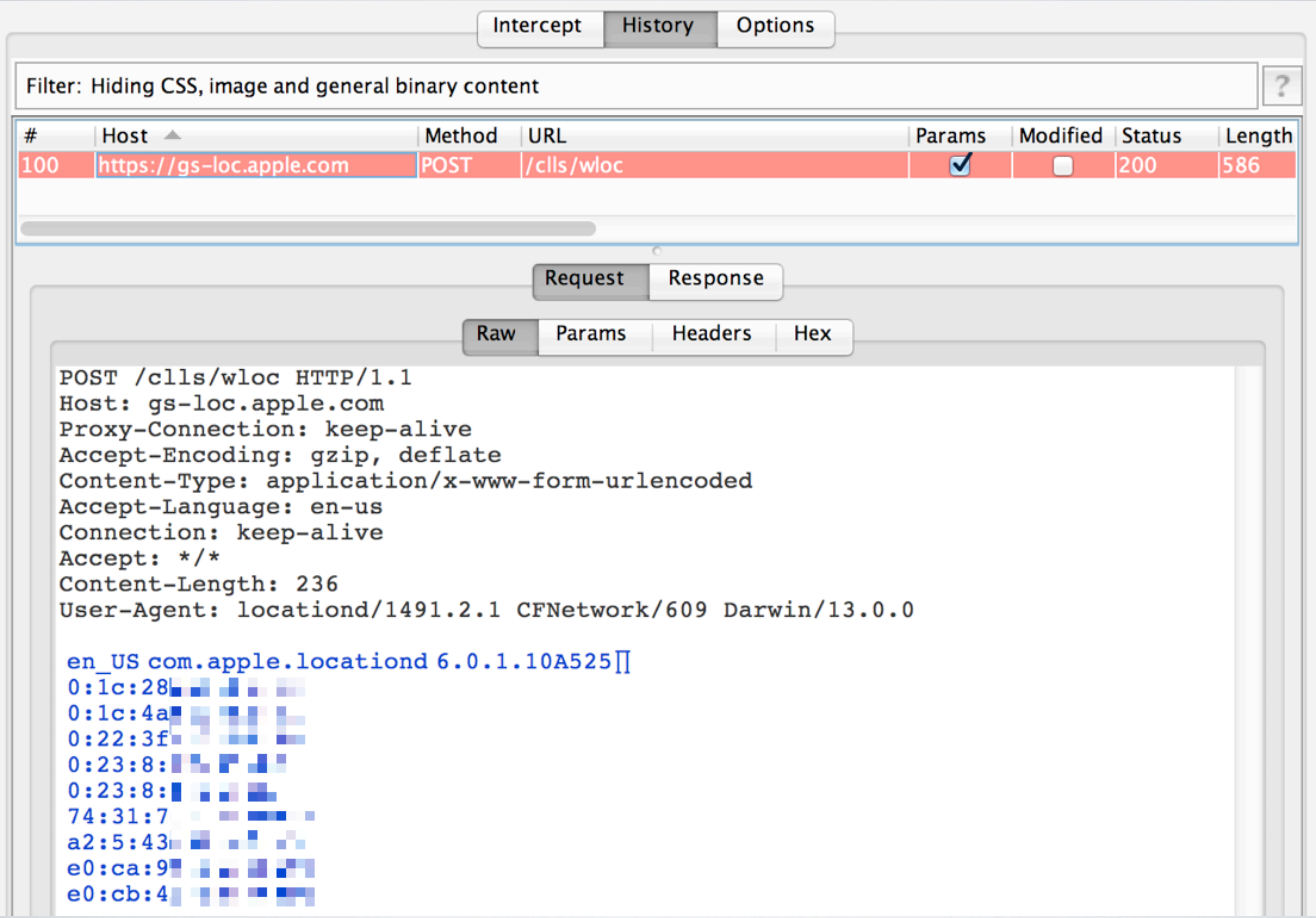


Location Services

Location Services ON

Location Services uses GPS along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location.

iOS device HTTPS request to Apple



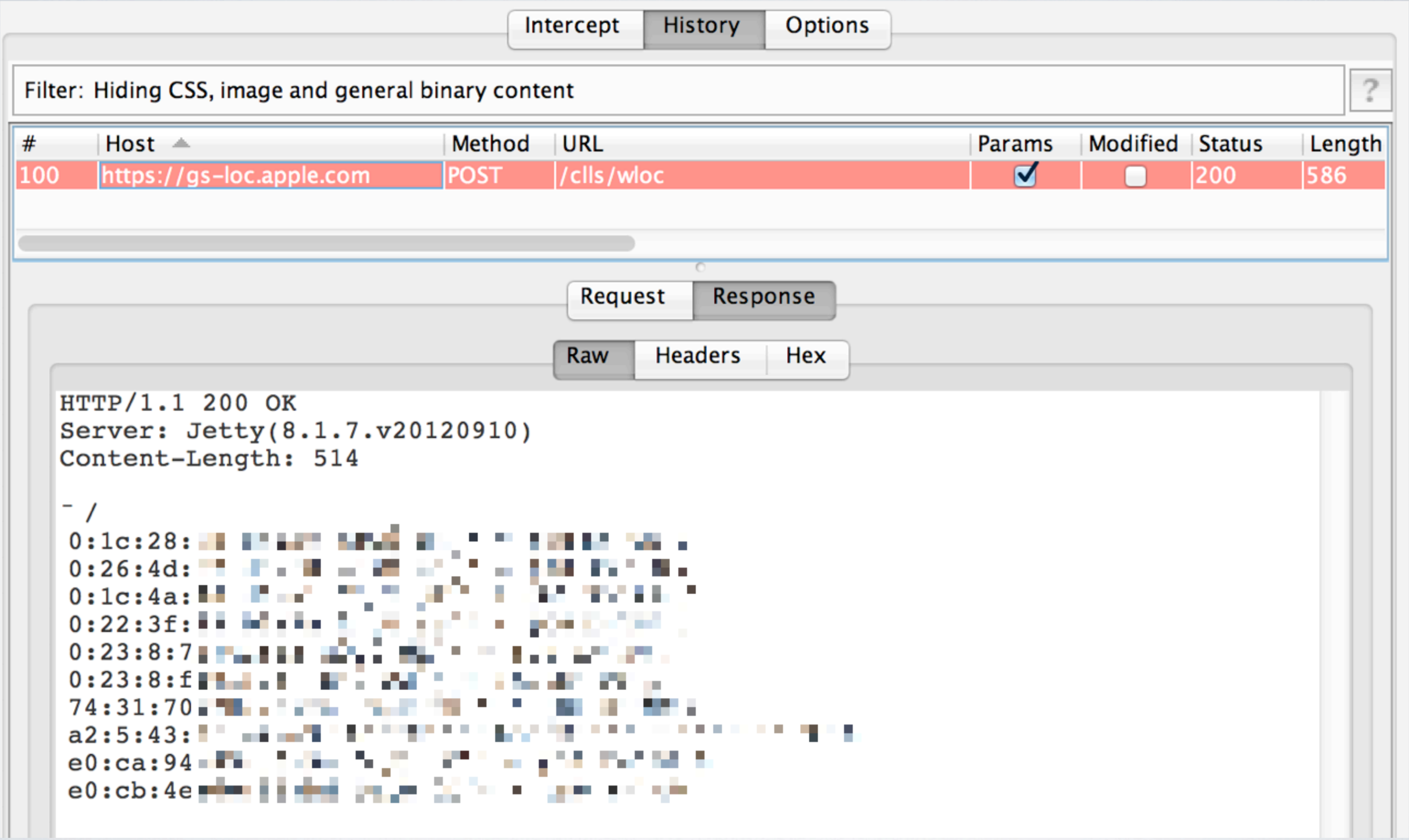
Filter: Hiding CSS, image and general binary content

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

```
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[redacted]
 0:1c:4a[redacted]
 0:22:3f[redacted]
 0:23:8:[redacted]
 0:23:8:[redacted]
 74:31:7[redacted]
 a2:5:43[redacted]
 e0:ca:9[redacted]
 e0:cb:4[redacted]
```

Response from Apple



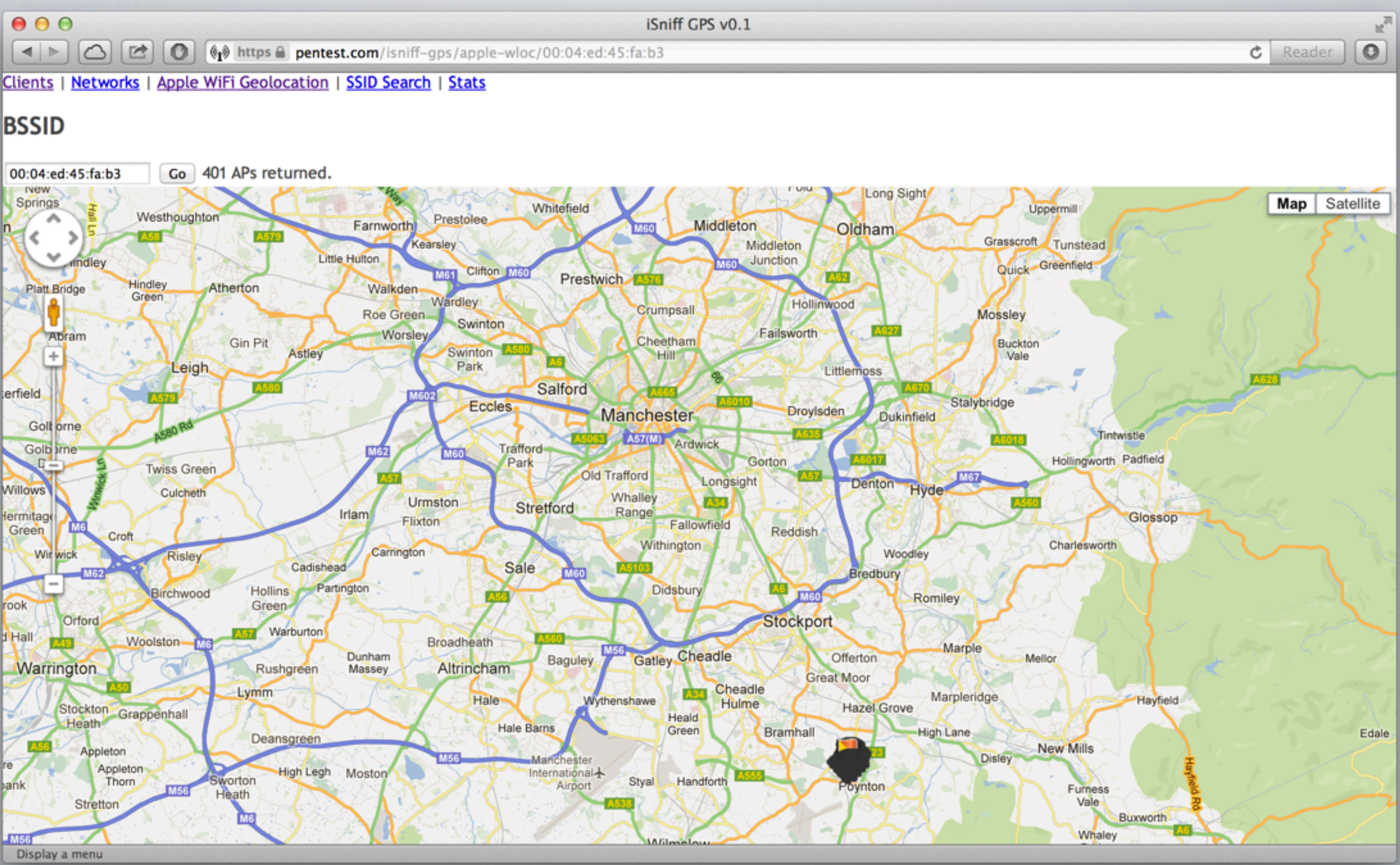
Filter: Hiding CSS, image and general binary content

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

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

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

Locating a wifi router MAC address



iSniff GPS v0.1

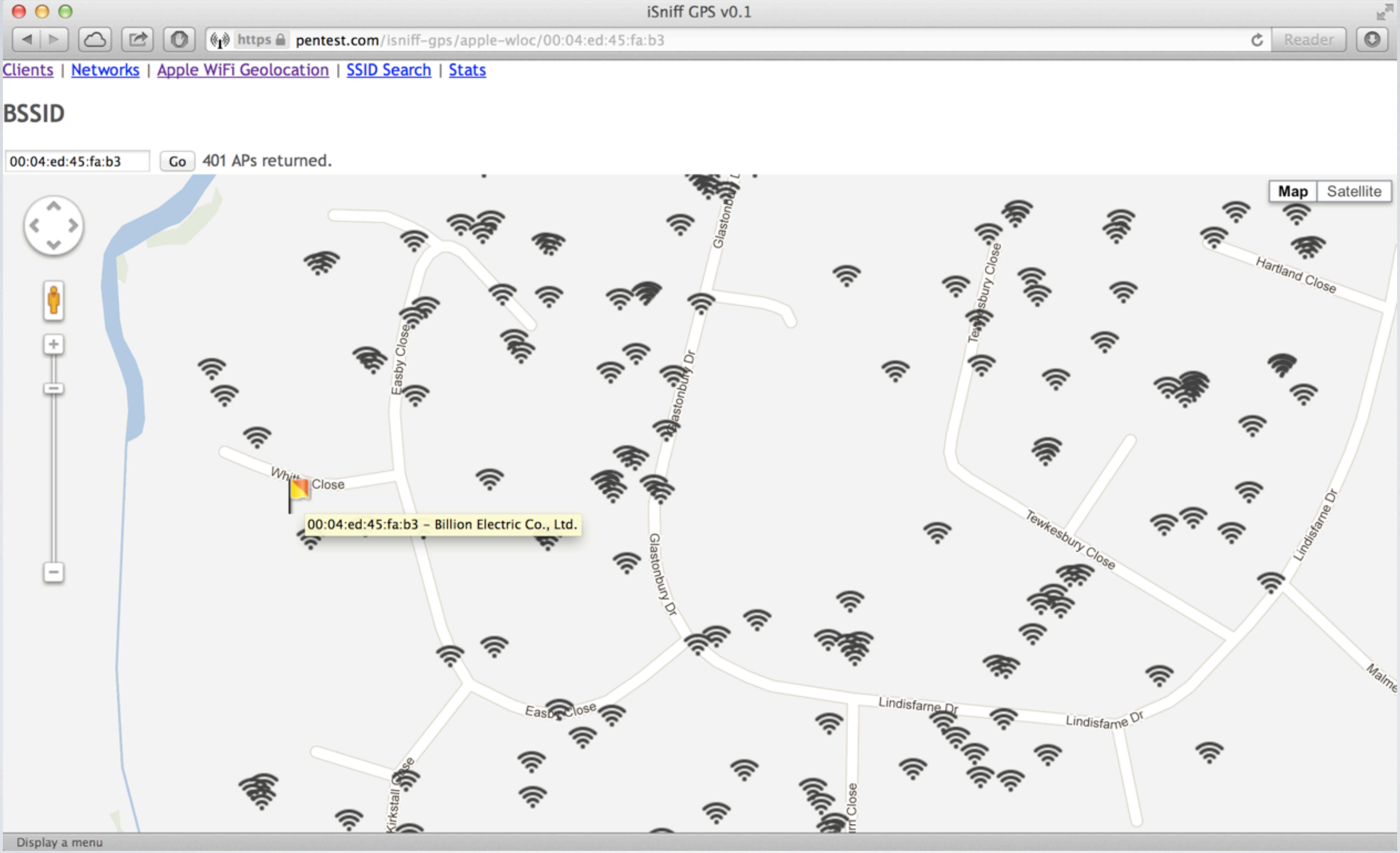
https pentest.com/isniff-gps/apple-wloc/00:04:ed:45:fa:b3

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

BSSID

00:04:ed:45:fa:b3 Go 401 APs returned.

Locating a wifi router MAC address



iSniff GPS v0.1

https pentest.com/isniff-gps/apple-wloc/00:04:ed:45:fa:b3

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

BSSID

00:04:ed:45:fa:b3 Go 401 APs returned.

00:04:ed:45:fa:b3 - Billion Electric Co., Ltd.

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/