Privacy Issue of Using Wi-Fi

Sang Young 楊和生

Convenor, Internet Security & Privacy Working Group

Internet Society Hong Kong 香港互聯網協會

Topics

- Public Wi-Fi
- Privacy Threat
- Looking Forward …

Public Wi-Fi

- Everywhere (…, …, …)
  - SME Shop
  - Telecom providers
  - Government
- Free
- Paid

Public Wi-Fi Characteristics

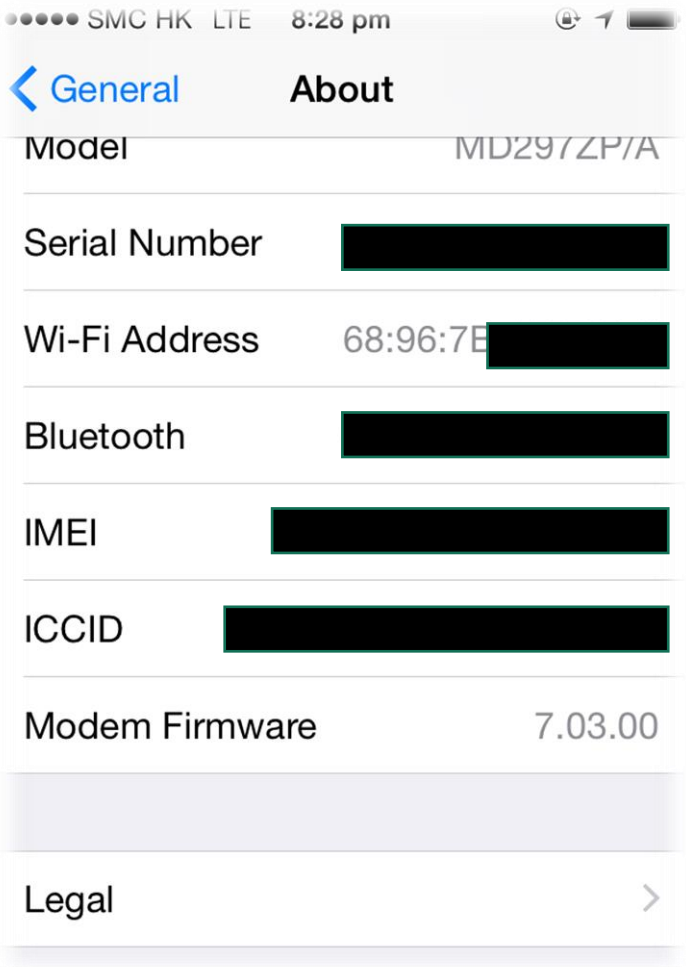
- Free
  - Accept Disclaimer
  - Simple registration
    - Collection your email address only? Really?

Public Wi-Fi

- Similar to CCTV
- Good or Bad ?

Data Collected from Public Wi-Fi

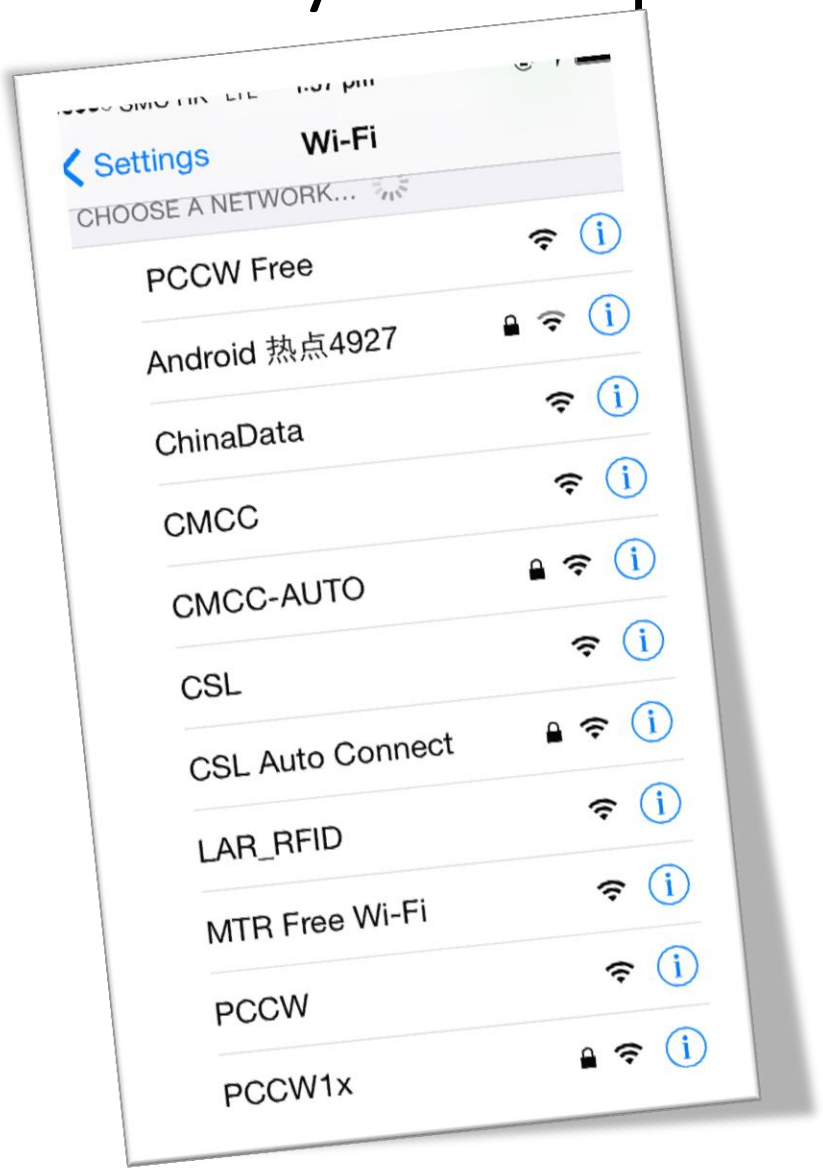
- Free Public Wi-Fi to customer
- In return, MAC Address of your mobile Device



How Does it Work?

- Wi-Fi enabled in mobile device
- It will make a survey on nearly Wi-Fi access point
  - i.e. MAC address can be logged
- When we try to access any free Wi-Fi
  - We have to accept the T&C
  - Maybe leaving your contact email
- In this case, MAC Address -> email

Survey Examples

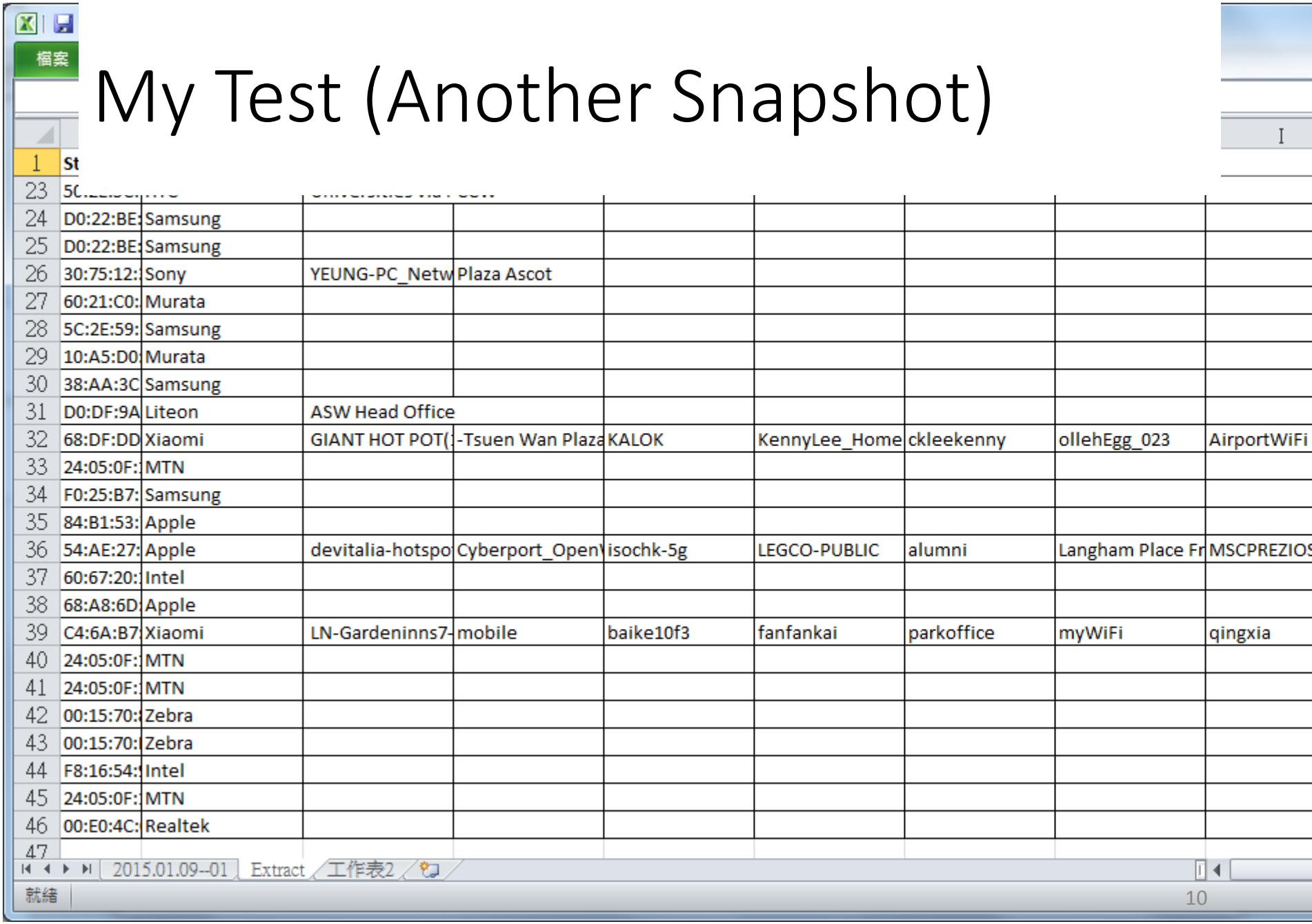


My Test

Source	Destination	Protocol	Length	Info
9c:02:9[redacted]	Broadcast	802.11	149	Probe Request, SN=414, FN=0, Flags=........C, SSID=bw-net
9c:02:9[redacted]	Broadcast	802.11	157	Probe Request, SN=426, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9[redacted]	Broadcast	802.11	153	Probe Request, SN=427, FN=0, Flags=........C, SSID=RC-KLNEAST
9c:02:9[redacted]	Broadcast	802.11	149	Probe Request, SN=428, FN=0, Flags=........C, SSID=bw-net
9c:02:9[redacted]	Broadcast	802.11	143	Probe Request, SN=1064, FN=0, Flags=........C, SSID=Broadcast
9c:02:9[redacted]	Broadcast	802.11	155	Probe Request, SN=2079, FN=0, Flags=........C, SSID=MegaBox_WiFi
9c:02:9[redacted]	Broadcast	802.11	157	Probe Request, SN=2227, FN=0, Flags=........C, SSID=TP-LINK_AEA99C
9c:02:9[redacted]	Broadcast	802.11	157	Probe Request, SN=2494, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9[redacted]	Broadcast	802.11	153	Probe Request, SN=2495, FN=0, Flags=........C, SSID=RC-KLNEAST
9c:02:9[redacted]	Broadcast	802.11	155	Probe Request, SN=2497, FN=0, Flags=........C, SSID=MegaBox_WiFi
9c:02:9[redacted]	Broadcast	802.11	157	Probe Request, SN=3654, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9[redacted]	Broadcast	802.11	157	Probe Request, SN=445, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9[redacted]	Broadcast	802.11	153	Probe Request, SN=446, FN=0, Flags=........C, SSID=RC-KLNEAST
9c:02:9[redacted]	Broadcast	802.11	149	Probe Request, SN=447, FN=0, Flags=........C, SSID=bw-net
9c:02:9[redacted]	Broadcast	802.11	155	Probe Request, SN=448, FN=0, Flags=........C, SSID=MegaBox_WiFi
9c:02:9[redacted]	Broadcast	802.11	149	Probe Request, SN=450, FN=0, Flags=........C, SSID=butbut

bits), 149 bytes captured (1192 bits)

My Test (Another Snapshot)



1	St								
23	5C								
24	D0:22:BE:	Samsung							
25	D0:22:BE:	Samsung							
26	30:75:12:	Sony	YEUNG-PC_Netw	Plaza Ascot					
27	60:21:C0:	Murata							
28	5C:2E:59:	Samsung							
29	10:A5:D0:	Murata							
30	38:AA:3C	Samsung							
31	D0:DF:9A	Liteon	ASW Head Office						
32	68:DF:DD	Xiaomi	GIANT HOT POT(	-Tsuen Wan Plaza	KALOK	KennyLee_Home	ckleekenny	ollehEgg_023	AirportWiFi
33	24:05:0F:	MTN							
34	F0:25:B7:	Samsung							
35	84:B1:53:	Apple							
36	54:AE:27:	Apple	devitalia-hotspo	Cyberport_Open	isochk-5g	LEGCO-PUBLIC	alumni	Langham Place Fr	MSCPREZIOS
37	60:67:20:	Intel							
38	68:A8:6D:	Apple							
39	C4:6A:B7:	Xiaomi	LN-Gardeninns7-	mobile	baike10f3	fanfankai	parkoffice	myWiFi	qingxia
40	24:05:0F:	MTN							
41	24:05:0F:	MTN							
42	00:15:70:	Zebra							
43	00:15:70:	Zebra							
44	F8:16:54:	Intel							
45	24:05:0F:	MTN							
46	00:E0:4C:	Realtek							
47									

Mobile OS Invading Privacy

- When a device associate an AP
- It collects the AP's Mac Address (i.e. BSSID)
- It collects the GPS location (i.e. latitude & longitude) from the device
- Upload to a vendor's website via https

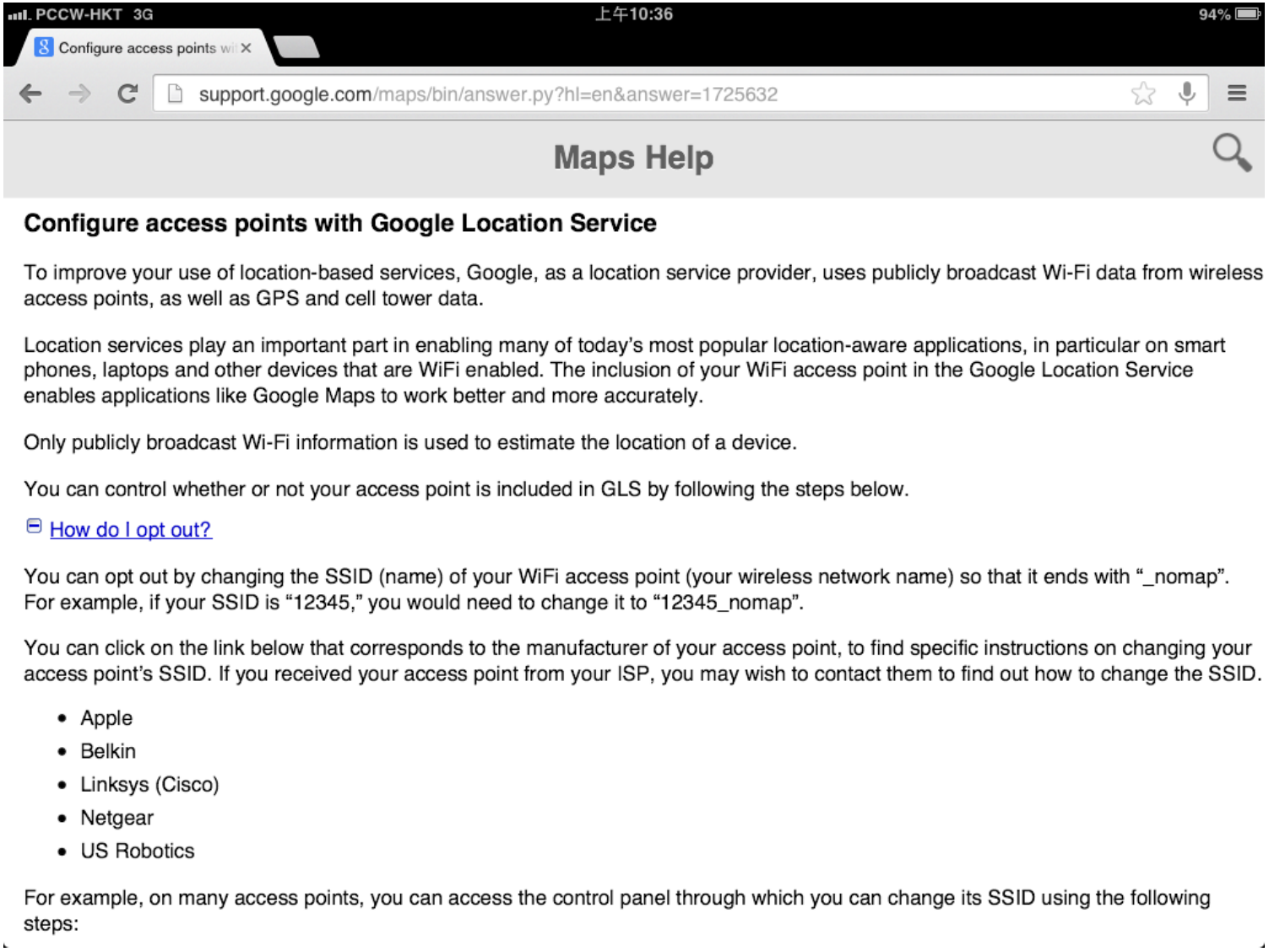
- Both Android & iOS

iOS Example

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

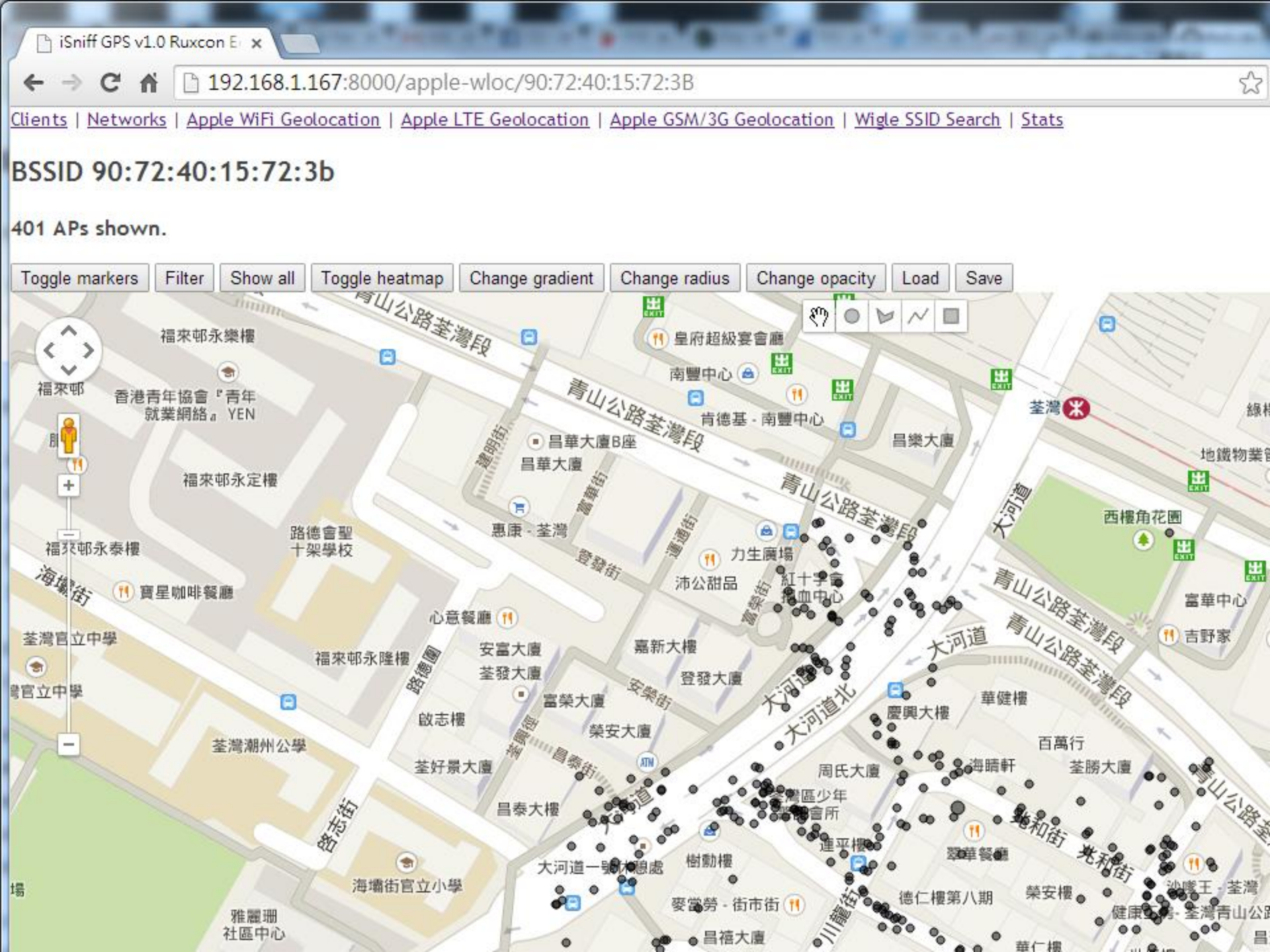
wifi BSSID : 36:87:24:79:2a:61
channel : 12
signal_strength : −96
latitude : 48.6252640167
longitude : 2.44375416667
timestamp : 359480148.357

Google


PCCW-HKT 3G
上午10:36
94%
Configure access points wi
support.google.com/maps/bin/answer.py?hl=en&answer=1725632
Maps Help
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
US Robotics
For example, on many access points, you can access the control panel through which you can change its SSID using the following steps:

Examples

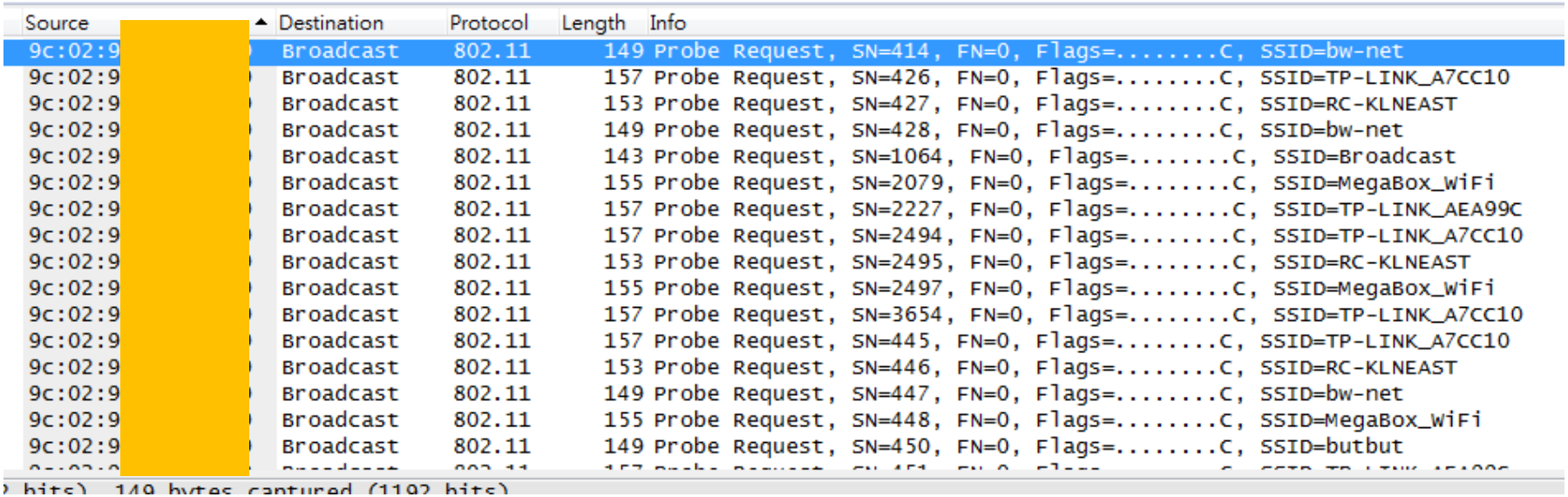
- iSniff-GPS
  - Passive sniffing tool for capturing and visualizing Wi-Fi location data disclosed by iOS devices
- Android Map
  - http://samy.pl/androidmap
  - Google blocked this site & changed the Geolocation API


iSniff GPS v1.0 Ruxcon E
192.168.1.167:8000/apple-wloc/90:72:40:15:72:3B
Clients | Networks | Apple WiFi Geolocation | Apple LTE Geolocation | Apple GSM/3G Geolocation | Wigle SSID Search | Stats
BSSID 90:72:40:15:72:3b
401 APs shown.
Toggle markers
Filter
Show all
Toggle heatmap
Change gradient
Change radius
Change opacity
Load
Save

Risks of Public Wi-Fi

- No encryption
- Honeypots
- Session Hijacking

No Encryption



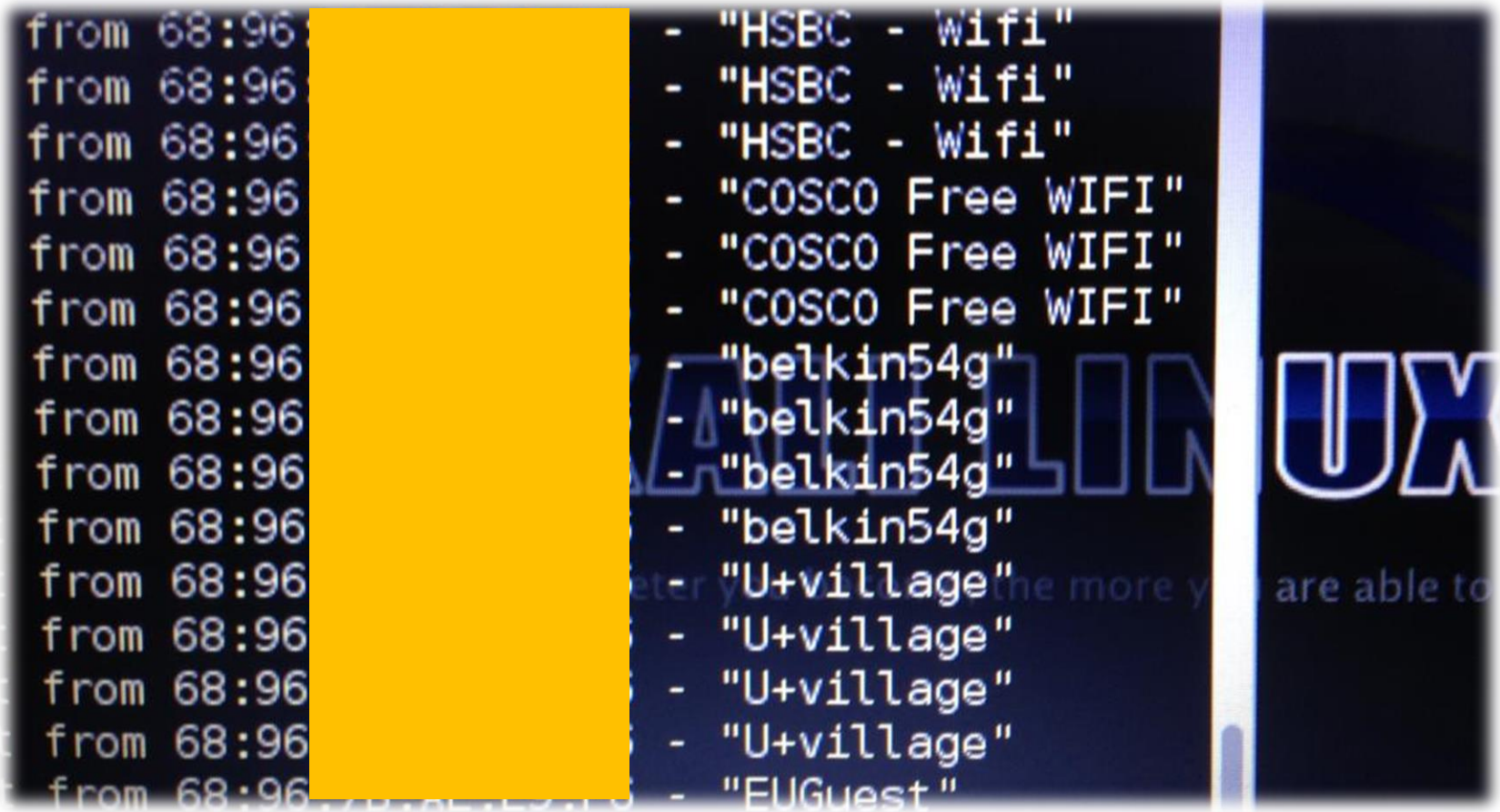
Source	Destination	Protocol	Length	Info
9c:02:9	Broadcast	802.11	149	Probe Request, SN=414, FN=0, Flags=........C, SSID=bw-net
9c:02:9	Broadcast	802.11	157	Probe Request, SN=426, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9	Broadcast	802.11	153	Probe Request, SN=427, FN=0, Flags=........C, SSID=RC-KLNEAST
9c:02:9	Broadcast	802.11	149	Probe Request, SN=428, FN=0, Flags=........C, SSID=bw-net
9c:02:9	Broadcast	802.11	143	Probe Request, SN=1064, FN=0, Flags=........C, SSID=Broadcast
9c:02:9	Broadcast	802.11	155	Probe Request, SN=2079, FN=0, Flags=........C, SSID=MegaBox_WiFi
9c:02:9	Broadcast	802.11	157	Probe Request, SN=2227, FN=0, Flags=........C, SSID=TP-LINK_AEA99C
9c:02:9	Broadcast	802.11	157	Probe Request, SN=2494, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9	Broadcast	802.11	153	Probe Request, SN=2495, FN=0, Flags=........C, SSID=RC-KLNEAST
9c:02:9	Broadcast	802.11	155	Probe Request, SN=2497, FN=0, Flags=........C, SSID=MegaBox_WiFi
9c:02:9	Broadcast	802.11	157	Probe Request, SN=3654, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9	Broadcast	802.11	157	Probe Request, SN=445, FN=0, Flags=........C, SSID=TP-LINK_A7CC10
9c:02:9	Broadcast	802.11	153	Probe Request, SN=446, FN=0, Flags=........C, SSID=RC-KLNEAST
9c:02:9	Broadcast	802.11	149	Probe Request, SN=447, FN=0, Flags=........C, SSID=bw-net
9c:02:9	Broadcast	802.11	155	Probe Request, SN=448, FN=0, Flags=........C, SSID=MegaBox_WiFi
9c:02:9	Broadcast	802.11	149	Probe Request, SN=450, FN=0, Flags=........C, SSID=butbut

hits), 149 bytes captured (1192 bits)

Honeypots - Evil Twins

- “Hacker” toolbox
  - Notebook
  - Kali Linux
  - Specialized USB Wi-Fi Adaptor
  - Antenna
  - Mobile Pocket Wi-Fi with Ethernet

Kali Linux – airbase-ng



Session Hijacking Example

楊和生指，黑客Apps可截取用戶訊息，模擬及冒充用戶身份，登入及操控用戶社交平台帳戶。

Stay Safe … …

- Know whose network
- Disable automatically connect
  - i.e forget the network
- HTTPS to websites, if possible
- VPN, particular …
  - business activities
- 2FA
- Disable sharing in Windows, Mac OS X etc.

Looking Forward …

- Transparency from service provider

Questions?