

# War-Driving 战争驾驶攻击

## War Driving 缘由

看过黑客电影的朋友们有没有留意到最后抓捕大哥组织里面那群人时候他们开着货车移动式攻击有没有印象？

这里有个词叫 War Driving

War Driving(驾乘式攻击)：是驾驶攻击也称为接入点映射,这是一种在驾车围绕企业或住所邻里时扫描无线网络名称的活动。

总而言之，通过多个 SSID 地理位置和用户最近所连接 WiFi 的路由器的 MAC 地址，就基本可以确定曾经所在的具体地理位置。

## WarXing 概念

### WarXing

是指探测公共可访问计算机或网络节点等行为的总称。这个‘X’可以被很多种方式名词所替代，下面列举了主要的方式。

**Wardriving**—也称之为“战争驾驶”，指通过驾驶车辆、在目标区域往返等行为来进行 Wi-Fi 无线接入点探测，可在车辆内部使用诸如 PDA、笔记本电脑等设备。

**Warbiking** — 指通过骑自行车、电动车、摩托等行为来进行 Wi-Fi 无线接入点探测，可使用设备有 PDA、笔记本电脑等。

**Warwalking** —指通过散步、穿插、长途穿越等个人行为来进行 Wi-Fi 无线接入点探测，可使用设备有 PDA、笔记本电脑等。

**Warchalking** —也称之为“作战标记”，指将无线接入点位置等基本情况，用事先定义的标识来区分，并用粉笔绘制到墙上的行为。

**Warflying** —通过使用飞行器如乘坐飞机来进行 Wi-Fi 无线接入点探测，可使用设备有 PDA、笔记本电脑等。

**Warspying** — 指探测并查看无线视频的行为。通常会在车辆上使用接收器来进行。和 Wardriving 比较相似，区别只是将无线网络换成了无线视频。

## 1.1 Wardriving

**Wardriving** 称之为“战争驾驶”，指通过驾驶车辆、在目标区域往返等行为来进行 Wi-Fi 无线接入点探测，可在车辆内部使用诸如 PDA、笔记本电脑等设备。

战争驾驶中用到的软件绝大部分都可以从 Internet 上找到，Windows 下常用的是 NetStumble，而 Kismet 及 SWScanner 是使用在 Linux、FreeBSD、NetBSD 和 OpenBSD 系统的，对于 MacOS 而言，主要是 KisMac。

类似的，还有 Warbiking、WarWalking 等。

## 1.2 Warbiking

**Warbiking** 从字面就可以理解，指通过骑自行车、电动车、摩托等行为来进行 Wi-Fi 无线接入点探测，可使用设备有 PDA、笔记本电脑等。进行 War-Wabiking 所使用到的软件和 War-Driving 基本一致。War biking 源自于无线黑客术语 War driving。

无线黑客及无线爱好者们有的采用在骑车时使用背包里开启的笔记本电脑进行无线接入点搜寻，还有的会不时停下来尝试连接无线 AP，再有的甚至直接对自行车前面进行了改装，通过加装固定器以便固定掌上电脑及 GPS，这样在骑行过程中就可以随时查看无线扫描报告。

## 1.3 Warwalking

**Warwalking** 从字面意思可知，该方式指通过散步、穿插、长途穿越等个人行为来进行 Wi-Fi 无线接入点探测，可使用设备有 PDA、笔记本电脑等。进行 War-Walking 所使用到的软件和 War-Driving 基本一致。Warwalking 源自于无线黑客术语 War driving。

作为民间的爱好者，会采用手持笔记本电脑，将天线随身携带等方式来进行 War-Biking 无线探测。不过在长时间的手持探测下，似乎笔记本的重量还是不那么令人乐

观的。所以对于单纯的无线接入点信号探测，War-Walking 爱好者们也会使用 PDA 之类的便携式电脑来实现。

## War-Driving 能做什么？

不知道大家清楚不清楚 wifi 定位原理, 摘自网上的一段话: **WiFi 定位: 靠的是侦测附近周围所有的无线网路基地台(WiFi Access Point)的 MAC Address (类似 10-78-D2-93-58-C2 这样的格式), 去比对资料库中该 MAC Address 的座标, 交叉连集出所在地。此法尚须有网路连线做资料库查询才能完成定位。**

War-Driving 会记录 MAC 地址, 利用 GPS 可以获取到经纬度, 这样的情况下可以进行定位。

这样的事情已经很多的大型互联网公司都在做了, 定位你当前的位置, 发送你位置经纬度和 MAC 地址到云端的服务器, 当然公安肯定不落后, 他们也有这样的设备采集车采集到信息之后进行入库, 定位来抓犯罪嫌疑人。

总而言之, 通过多个 SSID 地理位置和用户最近所连接 WiFi 的路由器的 MAC 地址, 就基本可以确定曾经所在的具体地理位置。

曾有 google apple 采集 wifi 事件

[谷歌就收集 WiFi 网络用户个人信息道歉](#)

[苹果官方解释收集用户位置信息问题](#)

## War-Driving 攻击准备

要想进行驾驶攻击你就要具备一辆车、一台电脑（膝上型电脑）、一个工作在混杂模式下的无线以太网网卡, 还有一个装在车顶部或车内的天线。

因为一个无线局域网可能仅局限于一栋办公楼的范围内, 外部使用者就有可能入侵网络, 获得免费的企业内部网络连接, 还可能获得公司的一些记录

和其他一些资源。用全方位天线和全球定位系统 (GPS), 驾驶攻击者就能够系统地将 802.11b/g/n 无线接入点映射地址映射。

驾乘式攻击，其实在现实当中用来收集信息才是比较使用的。那么收集到的信息有哪些？如下图

些？如下图

A	B	C	D	E	F	G	H	I	J	K
WigleWi-1.4	appRelease=1.57	model=HTC	release=4	device=m7	display=JZ054K	board=unk	brand=htccn_chs_ct			
MAC	SSID	AuthMode	FirstSeer	Channel	RSSI	CurrentLc	CurrentLc	Altitude	Accuracy	Type
6c:e8:13:29:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-71	40.0729	116.3628	26.4	39	WIFI
14:75:83:d8:9e	Doreen	[WPA-PSK- #####		11	-78	40.0729	116.3628	26.4	39	WIFI
ec:88:13:6a:4e:b0	banyue	[WPA-PSK- #####		6	-88	40.0729	116.3628	26.4	39	WIFI
c8:3a:35:4a:b5:b8	Tenda_4AB5B8	[WPA-PSK- #####		7	-86	40.0729	116.3628	26.4	39	WIFI
28:2c:b2:68:f5:0c	TP-LINK_68F50C	[WPA-PSK- #####		1	-89	40.0729	116.3628	26.4	39	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.0729	116.3628	26.4	39	WIFI
13824_11490	????	CDMA - Ev	#####	0	-48	40.0729	116.3628	26.4	39	CDMA
08:10:77:15:86:59	Netcore	[WPA-PSK- #####		6	-91	40.07293	116.3628	28.5	22	WIFI
38:83:45:15:fb:da	ouou	[WPA-PSK- #####		5	-93	40.07292	116.3628	28.5	47	WIFI
74:ad:b7:13:03:cb	CM512-6803cb	[WPA2-PSK #####		6	-92	40.07292	116.3628	28.4	182	WIFI
c0:61:18:13:d7:48	Lee	[WPA-PSK- #####		6	-92	40.0729	116.3628	28.9	51	WIFI
6c:e8:73:19:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-73	40.07461	116.3669	0	4.646787	WIFI
14:75:90:13:d8:9e	Doreen	[WPA-PSK- #####		11	-78	40.07461	116.3669	0	4.646787	WIFI
c8:3a:35:4a:b5:b8	Tenda_4AB5B8	[WPA-PSK- #####		7	-86	40.07461	116.3669	0	4.646787	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.07461	116.3669	0	4.646787	WIFI
28:2c:b2:68:f5:0c	TP-LINK_68F50C	[WPA-PSK- #####		1	-90	40.07461	116.3669	0	4.646787	WIFI
6c:e8:73:19:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-67	40.07455	116.3667	0	4.646787	WIFI
14:75:90:13:d8:9e	Doreen	[WPA-PSK- #####		11	-80	40.07455	116.3667	0	4.646787	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.07455	116.3667	0	4.646787	WIFI
6c:e8:73:19:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-67	40.07449	116.3666	0	4.646787	WIFI
14:75:90:13:d8:9e	Doreen	[WPA-PSK- #####		11	-80	40.07449	116.3666	0	4.646787	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.07449	116.3666	0	4.646787	WIFI
c8:3a:35:4a:b5:b8	Tenda_4AB5B8	[WPA-PSK- #####		7	-82	40.07447	116.3665	0	4.646787	WIFI
28:2c:b2:68:f5:0c	TP-LINK_68F50C	[WPA-PSK- #####		1	-89	40.07447	116.3665	0	4.646787	WIFI
ec:88:8f:6a:4e:b0	banyue	[WPA-PSK- #####		6	-90	40.07447	116.3665	0	4.646787	WIFI
6c:e8:73:19:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-68	40.07443	116.3664	0	4.646787	WIFI
14:75:90:13:d8:9e	Doreen	[WPA-PSK- #####		11	-81	40.07443	116.3664	0	4.646787	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.07443	116.3664	0	4.646787	WIFI
c8:3a:35:4a:b5:b8	Tenda_4AB5B8	[WPA-PSK- #####		7	-82	40.07441	116.3664	0	4.646787	WIFI
28:2c:b2:68:f5:0c	TP-LINK_68F50C	[WPA-PSK- #####		1	-90	40.07441	116.3664	0	4.646787	WIFI
ec:88:8f:6a:4e:b0	banyue	[WPA-PSK- #####		6	-90	40.07441	116.3664	0	4.646787	WIFI
38:83:45:15:fb:da	ouou	[WPA-PSK- #####		5	-92	40.07441	116.3664	0	4.646787	WIFI
6c:e8:73:19:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-70	40.07437	116.3663	0	4.646787	WIFI
14:75:90:13:d8:9e	Doreen	[WPA-PSK- #####		11	-87	40.07437	116.3663	0	4.646787	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.07437	116.3663	0	4.646787	WIFI
c8:3a:35:4a:b5:b8	Tenda_4AB5B8	[WPA-PSK- #####		7	-84	40.07435	116.3662	0	4.646787	WIFI
38:83:45:15:fb:da	ouou	[WPA-PSK- #####		5	-92	40.07435	116.3662	0	4.646787	WIFI
ec:88:8f:6a:4e:b0	banyue	[WPA-PSK- #####		6	-91	40.07435	116.3662	0	4.646787	WIFI
6c:e8:73:19:d5:e2	TP-lantianyuan	[WPA-PSK- #####		1	-70	40.07431	116.3661	0	4.646787	WIFI
e0:05:c5:a1:f0:3c	kid	[WPA-PSK- #####		11	-68	40.07431	116.3661	0	4.646787	WIFI
a8:57:4e:f7:a4:cc	FAST_A4CC	[WPA-PSK- #####		6	-88	40.07431	116.3661	0	4.646787	WIFI
c8:3a:35:4a:b5:b8	Tenda_4AB5B8	[WPA-PSK- #####		7	-82	40.07429	116.3661	0	4.646787	WIFI

上图是 Wigle 无线攻击到处 XLS 格式的数据进行的一个联合查询的结果, 也是收集到信息达一部分。

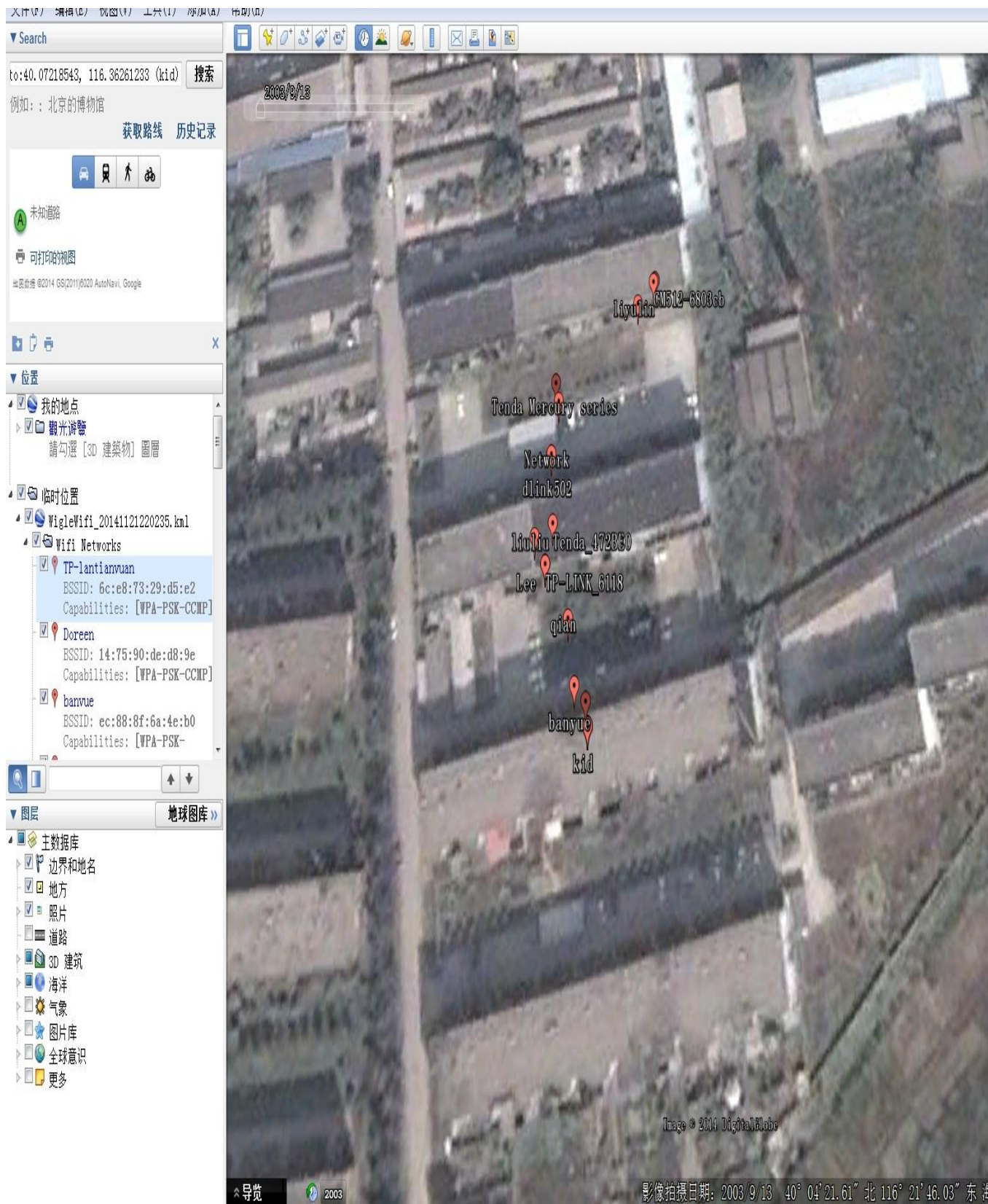
MAC: 是无线路由或者说是无线设备的 MAC 地址

lat; lon :是此无线设备达经纬度 GPS 信息

ssid: 是无线设备达名称

authmode:可以明显的看到这个是无线设备达加密方式

看看这张图片:



上图中，所有绿色为没有加密的无线网络，黄色达为 wep 加密方式，红色的是 wpa/wpa2 加密方式。

## War-Driving 花样式攻击

首先我们看了以上图 考虑的问题是如何得到的信息在地球中显示，其实需要两样东西 一个 GPS 记录当前所在位置，另外一个就是用于收集 wifi 信息的设备。

## 设备需求 攻击方式

一般情况下如果要做专业点并且比较精确信息量大，那么就需要一个外接 USB GPS、笔记本一台、wifi 增益天线、车子一辆。

大家熟知的 bt5 就自带一个 kismet，有需要的可以 google youtube 上有视频演示。

这样的设备不一定人人都有，但是别忘记了 android ios 等智能手机手机也存在 GPS 定位功能和 wifi 功能。

当然这样的工具已经存在了, 已经有别人写好了。Wigle

安装成功之后名字是 wigle 无线驾驶攻击





麦子学院



QQ



滴滴打车



nfc



Wifi 分析仪



NFCClassic



WIFI密码查看器



WiGLE無線駕駛攻擊



GPS轨迹记录仪



多点GPS户外导航



Mifare Classic Tool



下图安装之后打开的界面



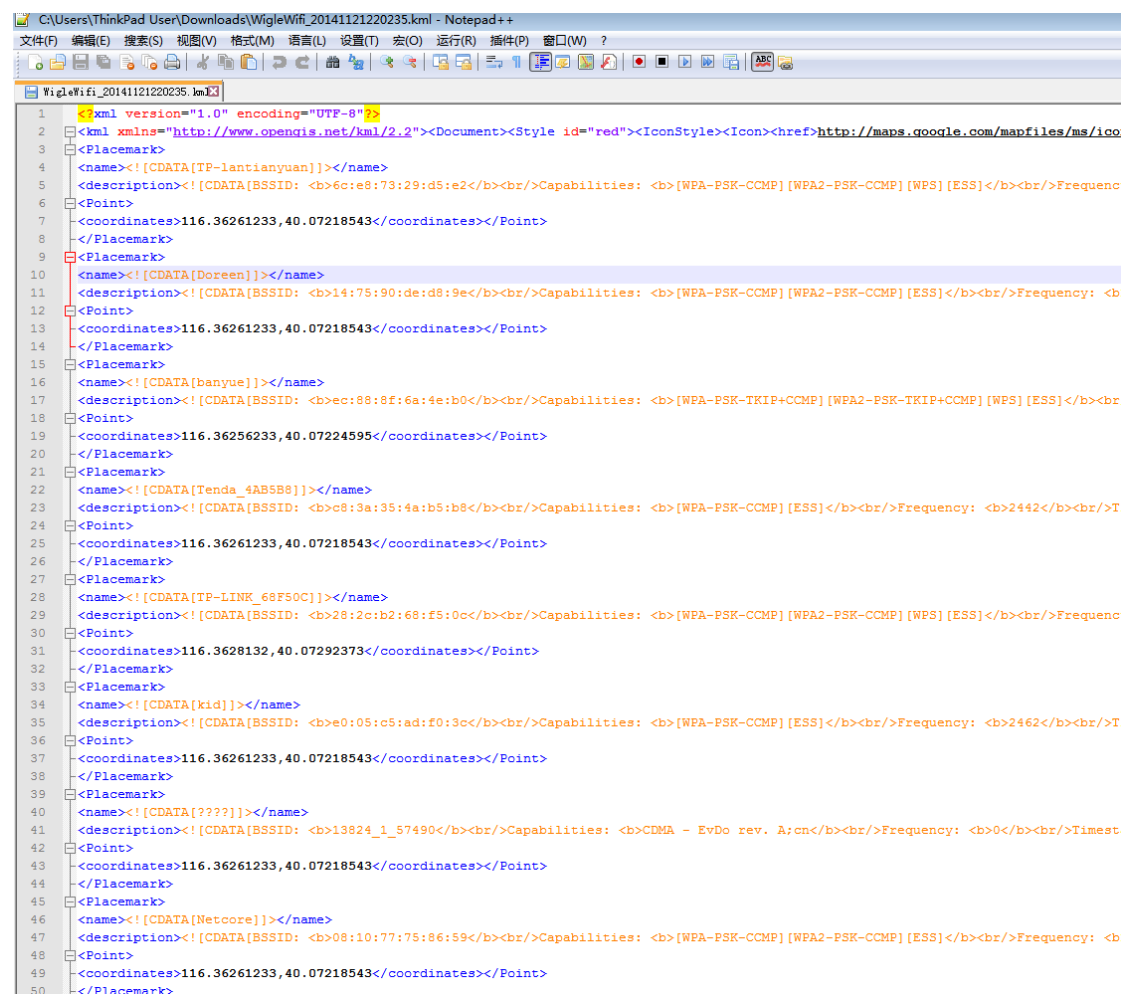


从上图可以清晰到

1. ssid
2. mac 地址
3. wifi 加密方式
4. GPS 位置信息
5. 已抓取数据

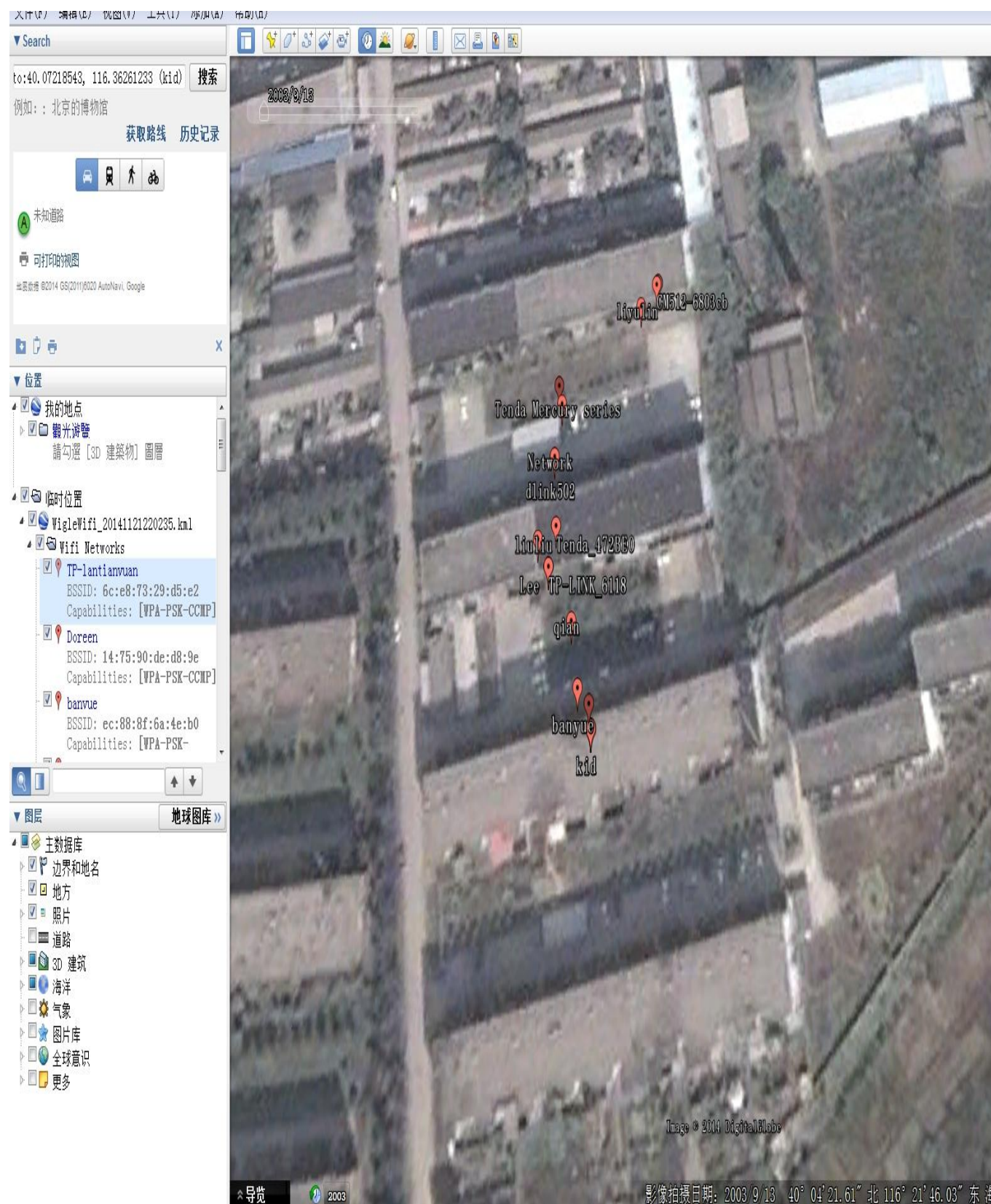
**wigle 无线驾驶攻击**支持从数据库中导出 kml, XLS 格式（google 地图标记用的就是这个）

KML 格式数据



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <kml xmlns="http://www.opengis.net/kml/2.2"><Document><Style id="red"><IconStyle><Icon><href>http://maps.google.com/mapfiles/ms/ico
3 </Placemark>
4 <name><![CDATA[TP-lantianyuan]]></name>
5 <description><![CDATA[BSSID: <b>6c:e8:73:d5:e2</b><br/>Capabilities: <b>[WPA-PSK-CCMP] [WPA2-PSK-CCMP] [WPS] [ESS]</b><br/>Freque
6 <Point>
7 <coordinates>116.36261233,40.07218543</coordinates></Point>
8 </Placemark>
9 <Placemark>
10 <name><![CDATA[Doreen]]></name>
11 <description><![CDATA[BSSID: <b>14:75:90:de:d8:9e</b><br/>Capabilities: <b>[WPA-PSK-CCMP] [WPA2-PSK-CCMP] [ESS]</b><br/>Frequency: <b
12 <Point>
13 <coordinates>116.36261233,40.07218543</coordinates></Point>
14 </Placemark>
15 <Placemark>
16 <name><![CDATA[banyue]]></name>
17 <description><![CDATA[BSSID: <b>ec:88:8f:6a:4e:b0</b><br/>Capabilities: <b>[WPA-PSK-TKIP+CCMP] [WPA2-PSK-TKIP+CCMP] [WPS] [ESS]</b><br/>
18 <Point>
19 <coordinates>116.36256233,40.07224595</coordinates></Point>
20 </Placemark>
21 <Placemark>
22 <name><![CDATA[Tenda_4AB5B8]]></name>
23 <description><![CDATA[BSSID: <b>c8:3a:35:4a:b5:b8</b><br/>Capabilities: <b>[WPA-PSK-CCMP] [ESS]</b><br/>Frequency: <b>2442</b><br/>T
24 <Point>
25 <coordinates>116.36261233,40.07218543</coordinates></Point>
26 </Placemark>
27 <Placemark>
28 <name><![CDATA[TP-LINK_68F50C]]></name>
29 <description><![CDATA[BSSID: <b>28:2c:b2:68:f5:0c</b><br/>Capabilities: <b>[WPA-PSK-CCMP] [WPA2-PSK-CCMP] [WPS] [ESS]</b><br/>Freque
30 <Point>
31 <coordinates>116.3628132,40.07292373</coordinates></Point>
32 </Placemark>
33 <Placemark>
34 <name><![CDATA[kidj]]></name>
35 <description><![CDATA[BSSID: <b>e0:05:c5:ad:f0:3c</b><br/>Capabilities: <b>[WPA-PSK-CCMP] [ESS]</b><br/>Frequency: <b>2462</b><br/>T
36 <Point>
37 <coordinates>116.36261233,40.07218543</coordinates></Point>
38 </Placemark>
39 <Placemark>
40 <name><![CDATA[????]]></name>
41 <description><![CDATA[BSSID: <b>13824_i_57490</b><br/>Capabilities: <b>CDMA - EvDo rev. A;cn</b><br/>Frequency: <b>0</b><br/>Timest
42 <Point>
43 <coordinates>116.36261233,40.07218543</coordinates></Point>
44 </Placemark>
45 <Placemark>
46 <name><![CDATA[Netcore]]></name>
47 <description><![CDATA[BSSID: <b>08:10:77:75:86:59</b><br/>Capabilities: <b>[WPA-PSK-CCMP] [WPA2-PSK-CCMP] [ESS]</b><br/>Frequency: <b
48 <Point>
49 <coordinates>116.36261233,40.07218543</coordinates></Point>
50 </Placemark>
```

接着我们打开 GoogleEarth 显示图



由于天太冷，下楼的时候采集了一些 wifi 信息，来做演示, 看起来效果不是很明显。

2014 年 12 月 2 日