

# Geo-Location Forensics on Mobile Devices

Yi Sun

Meiya Pico Information Company Limited, Meiya Information Security Academy

Xiamen, Fujian Province, China

Geo.suny@gmail.com

**Abstract.** Nowadays, more and more people using smartphones such as iOS and Android handsets, a report from Nielsen<sup>1</sup> shows that, in the 4<sup>th</sup> quarter of 2011, 46.3% smartphone user choose android OS out of 75,000 users, while 30% surveyed iOS. Handsets with smart operating systems allow user to install all kinds of applications, provide high-speed wireless internet connections, and more useful features based on geo-location services such as GPS positioning and navigating. Thanks to that, now, digital forensic examiners can acquire not just logical data (For example, Call History, Contacts, SMS Messages, etc.), but data which give examiners exactly accurate locations. That is what we called “geo-location” forensic on mobile devices.

## 1 Geo-location forensic on iOS Devices.

iOS devices such as iPhone is one of the most popular handsets all around the world these years, in early 2011, researchers found that in particular model which using iOS 4.x version, the phone will save all cell tower information and WIFI information by default, both of them contains a large number of geo-location data, time range started from the first day the user purchase iPhone.

That file is named “Consolidated.db”, which can be found in any iOS 4.2 OS or any other version before.

---

<sup>1</sup> Nielsen Mobile Insights, Q4 2011

Database: consolidated Table: CellLocation File: C:\Users\Sun\Desktop\consolidated.db

Database SQL Builder SQL Data Design DDL

Refresh

RecNo	MCC	MNC	LAC	CI	Timestamp	Latitude	Longitude
1	460	0	22563	10419	320495514.680886	30.27861106	120.1639198
2	460	0	22303	33757	320495514.680886	30.27846801	120.16460508
3	460	0	22303	18639	320495514.680886	30.27834707	120.1647734
4	460	0	22563	18879	320495514.680886	30.27899098	120.1613695
5	460	0	22563	30086	320495514.680886	30.27654278	120.15977466
6	460	0	22298	25526	320495514.680886	30.27883553	120.16075879
7	460	0	22771	20124	320495514.680886	30.27735245	120.16625392
8	460	0	22298	10419	320495514.680886	30.279688	120.16237455
9	460	0	22298	18177	320495514.680886	30.27966445	120.161484
10	460	0	22298	20518	320495514.680886	30.2774074	120.16658711
11	460	0	22298	10429	320495514.680886	30.27902376	120.16562885
12	460	0	22298	10086	320495514.680886	30.27993041	120.16374105
13	460	0	22298	30086	320495514.680886	30.27840161	120.15964096
14	460	0	22298	10090	320495514.680886	30.27970337	120.16468101
15	460	0	22563	20128	320495514.680886	30.27793657	120.16655111
16	460	0	22303	28043	320495514.680886	30.27742612	120.15914857
17	460	0	22303	10090	320495514.680886	30.27959465	120.1650353
18	460	0	22563	10086	320495514.680886	30.28017842	120.16259938
19	460	0	22563	30082	320495514.680886	30.27974557	120.16068428
20	460	0	22298	30128	320495514.680886	30.27919971	120.16608685
21	460	0	22303	30086	320495514.680886	30.2794283	120.15978813
22	460	0	22303	10429	320495514.680886	30.27990639	120.1654694

Figure 1 Location data in Consolidated.db file.

The image above shows data stored in “Consolidated.db” file, we can see Cell network information such as MCC, MNC, LAC, Cell ID, Latitude, and Longitude, using this information, examiners can find the range of activity of the user.

MCC	MNC	LAC	CI	Timestamp	Latitude	Longitude	Horizontal ...	Altitude	Vertical Ac...	Speed	Course	Confidence
460	0	4254	10263	2-49-53 2011...	39.91797906	116.40148216	500.0	0.0	-1.0	-1.0	-1.0	70
460	0	4242	2308	2-49-53 2011...	39.91526901	116.40527039	1478.0	0.0	-1.0	-1.0	-1.0	65
460	0	4254	1043	2-49-53 2011...	39.91951149	116.40227937	500.0	0.0	-1.0	-1.0	-1.0	70
460	0	4377	2528	2-49-53 2011...	39.91740167	116.40808784	500.0	0.0	-1.0	-1.0	-1.0	65
460	0	4351	2003	2-49-53 2011...	39.91691231	116.40800887	1359.0	0.0	-1.0	-1.0	-1.0	65
460	0	4374	2528	2-49-53 2011...	39.91734158	116.40819942	500.0	0.0	-1.0	-1.0	-1.0	65
460	0	4242	2528	2-49-53 2011...	39.91779941	116.40828567	1131.0	0.0	-1.0	-1.0	-1.0	65
460	0	4212	2528	2-49-53 2011...	39.91733193	116.40827941	500.0	0.0	-1.0	-1.0	-1.0	65
460	0	4242	1786	2-49-53 2011...	39.91894763	116.4080587	1799.0	0.0	-1.0	-1.0	-1.0	65
460	0	4254	15190	2-49-53 2011...	39.91901171	116.40145176	1363.0	0.0	-1.0	-1.0	-1.0	65
460	0	4242	10262	2-49-53 2011...	39.91538542	116.40272384	531.0	0.0	-1.0	-1.0	-1.0	65
460	0	4254	51139	2-49-53 2011...	39.91979068	116.40205717	997.0	0.0	-1.0	-1.0	-1.0	65
460	0	4242	10268	2-49-53 2011...	39.91786932	116.40847998	806.0	0.0	-1.0	-1.0	-1.0	65
460	0	4359	52668	2-49-53 2011...	39.92070871	116.40493565	601.0	0.0	-1.0	-1.0	-1.0	65
460	0	4377	10267	2-49-53 2011...	39.91969293	116.40769958	1891.0	0.0	-1.0	-1.0	-1.0	65
460	0	4377	1787	2-49-53 2011...	39.91580468	116.40768736	661.0	0.0	-1.0	-1.0	-1.0	65
460	0	4242	2522	2-49-53 2011...	39.92062026	116.403219	500.0	0.0	-1.0	-1.0	-1.0	65
460	0	4408	52668	2-49-53 2011...	39.92077291	116.40573632	500.0	0.0	-1.0	-1.0	-1.0	70
460	0	4254	1473	2-49-53 2011...	39.91514724	116.40680783	500.0	0.0	-1.0	-1.0	-1.0	70
460	0	4242	4097	2-49-53 2011...	39.91774368	116.40874439	500.0	0.0	-1.0	-1.0	-1.0	65

Figure 2 Some free software can analyze Consolidated file and locate on Google Map

Examiner can also use some free forensic tools to analyze “Consolidated.db” file, one of them is “iStalkr<sup>2</sup>”.

iStalkr can read “Consolidated.db” and output all location data to a Google Map file, with a “kml” extension.

<sup>2</sup> iStalkr is a Evigator Digital Forensic product.

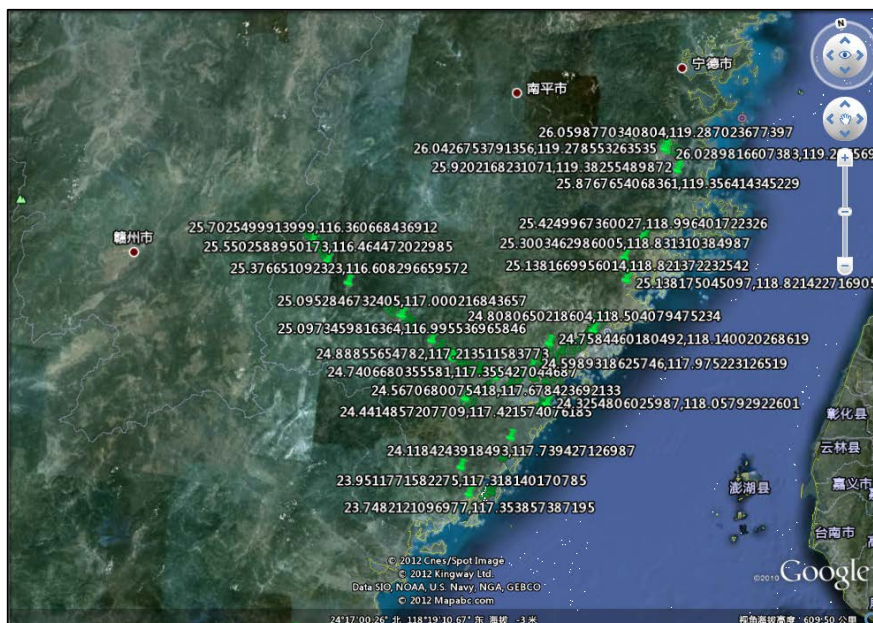


Figure 3 Consolidated.db shows on Google Earth

Besides, Camera on iOS device can save GPS location when taking photos, which is another resource of geo-location forensic on iDevices.

Output one image file that took by iPhone, in JPEG Exif information, we can see three kinds of GPS data, Latitude, Longitude and Altitude.

By using some software, for example, TAGView, in this case, GPS data in JPEG could be extract easily, and shows in a Map view.



Figure 4 GPS data in Exif of JPEG image.

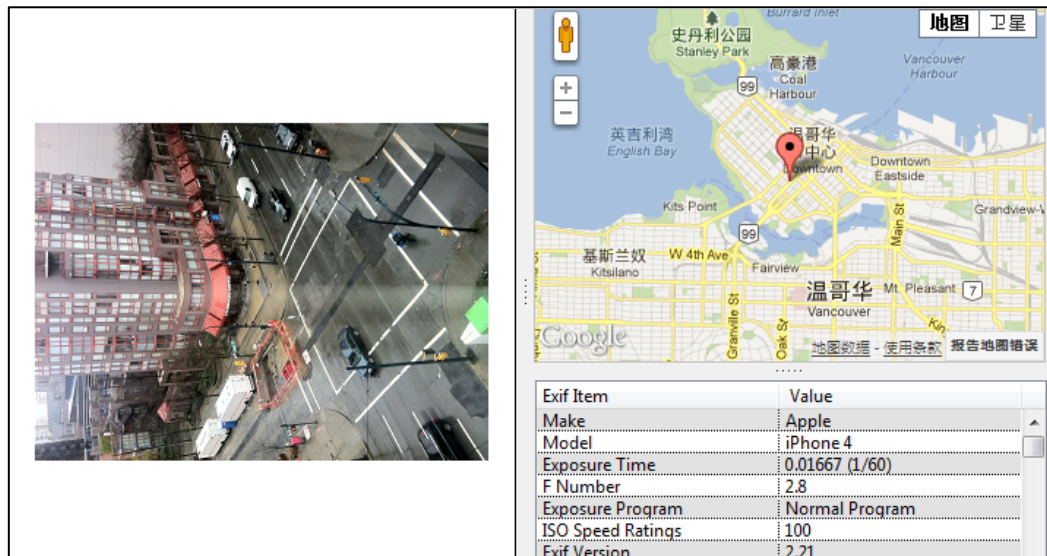


Figure 5 GPS data helps examiner to locate accurate location.

## 2 Geo-location forensic on Android Devices.

As I mentioned above, for iPhone, digital forensic examiners can acquire geo-location data easily in at least two ways, this is not an Individual phenomenon, Android, another most popular smartphone operating system present days, those location data also can be found by examiners.

Likely, Android save Cell network information and WIFI location information, but only the latest 50 for each.

Using ADB commands, examiners can acquire file from Android devices, files we want are named “cache.cell” and “cache.wifi”, generally, both file are less than 20 Kilobytes.

After converted, by Python scripts, we can get to GPS route file with “gpx” extension, the file type you convert is depends, of course, lie on what we need. In this demo, “gpx” file can be open in Google Earth, which provides an intuitionistic view.



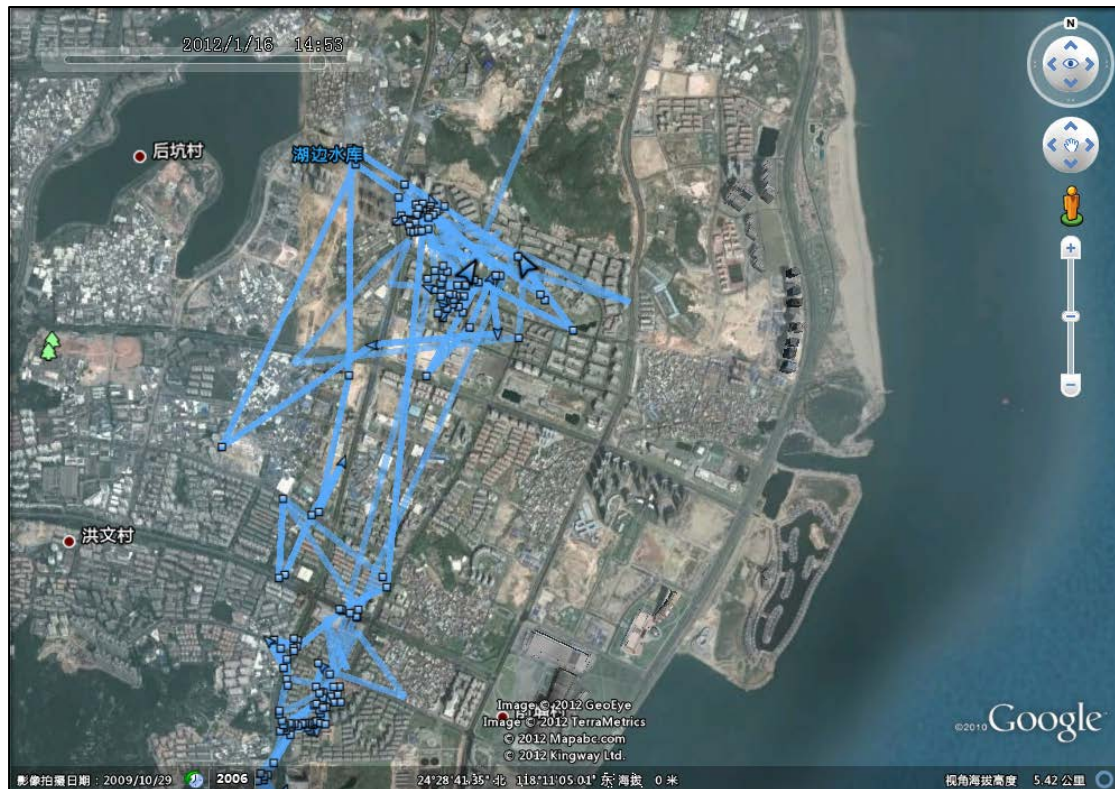


Figure 6 Cell and WIFI locations on Android devices.

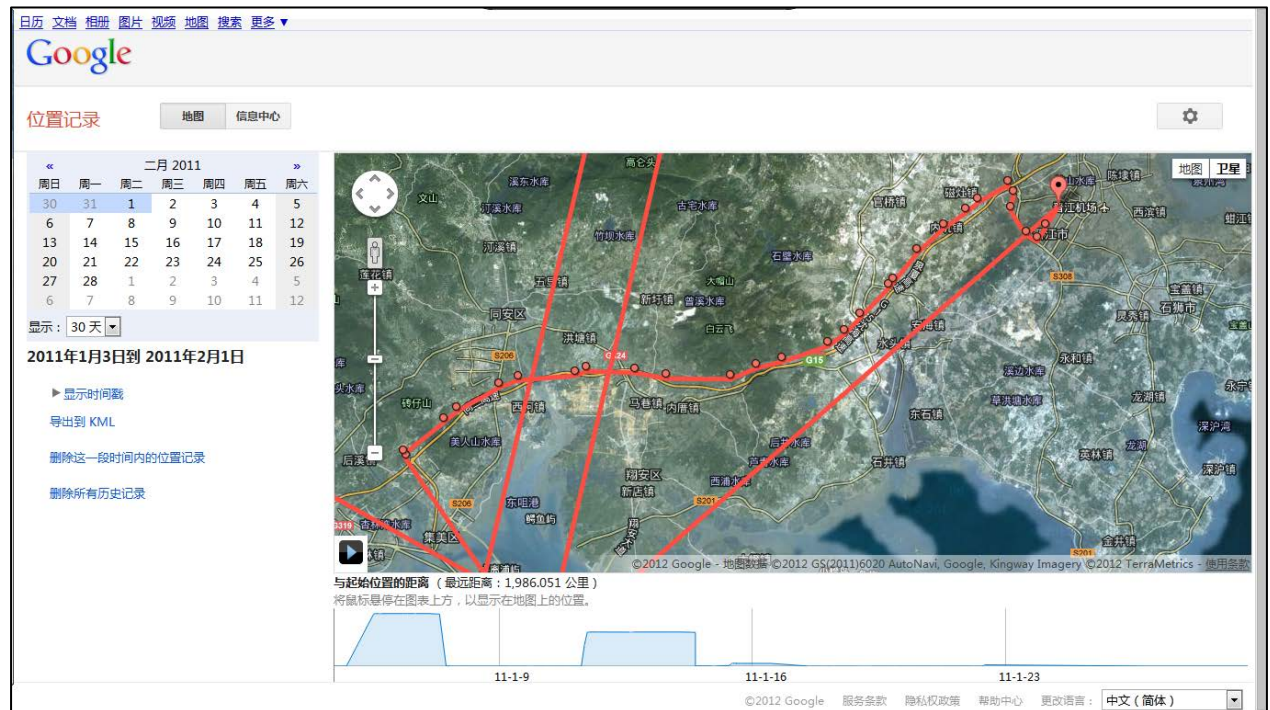
Some Android phone models such as Motorola<sup>3</sup>, allows user to take GPS-integrated image, just like iPhone, digital forensic examiners can perform exactly the same investigation as analyzing JPEG image on iPhone.

### 3 LBS Applications

If you are using a smartphone with Android OS, you may know lots of Google services were embedded on Android, such as Google Map, Google Search and Google Play (which was called Google App Market). As the default configuration of Android, each device required touch screen and GPS feature, with Google Map, Google provide a Location Based Services named “Google Latitude”, people who have a Google account can share location information with friends and any other person if they want.

But, people may not noticed that, Google latitude keep all location data on Google’s server, any authorized Google account access can obtain these data easily.

<sup>3</sup> Motorola Blur is an UI-modified Android OS.



Google Latitude is not the only application that store geo-location information, most popular SNS service provider now release their own mobile application, a trained forensic examiner can find you by a new tweet, a new personal status on Facebook, even an image.

#### 4 Locate without Geo-Location data.

Exif of JPEG contains GPS information, unless you upload image to a website, millions of image file are uploading at just this moment, but after they uploaded to the website, all file attributes will lost, include GPS information.

But there is another way we can try, Google Image Search allow user to upload their own image and find all related image files over the internet, images below shows this extraordinary method.



Figure 8 Step one, upload your image file.



Figure 9 Possible matches.

## 5 Conclusions

Compare with traditional logical data that we acquired from mobile phones, geo-location data is more visual and accurate, and more difficult to delete, forensic examiners must realize that forensics on mobile devices might give them much more

valuable evidence than ever.