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[1] shows that, in the 4th 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.

[1] Nielsen Mobile Insights, Q4 2011

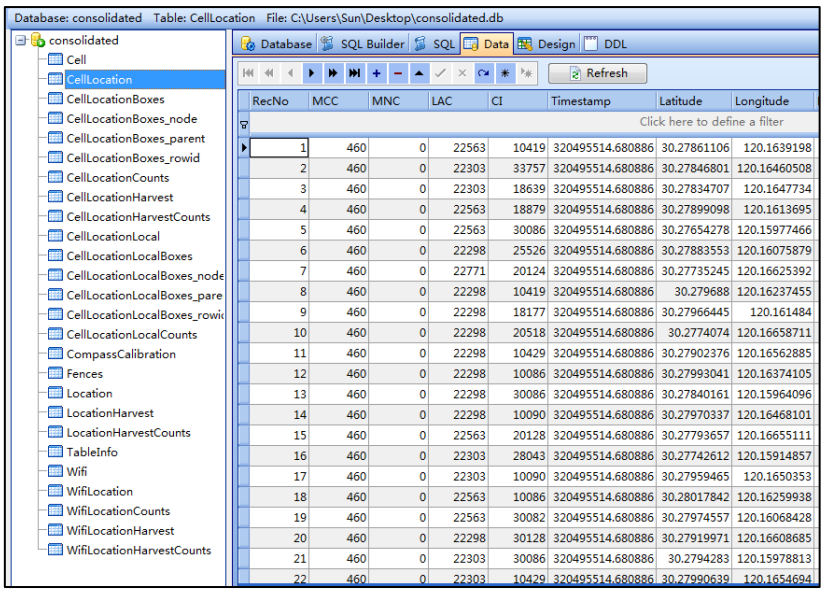

Figure 1 Location data in Consolidated.db file.

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.

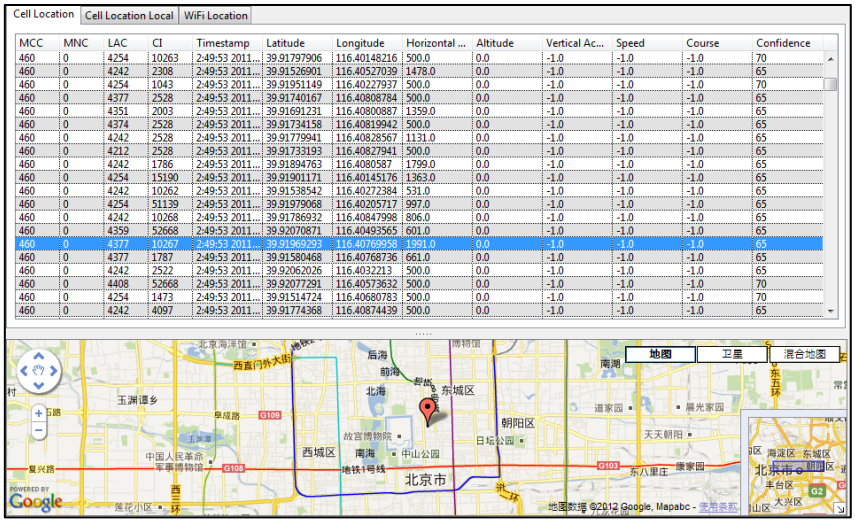

Figure 2 Some free software can analyze Consolidated file and locate on Google Map

Examiner can also use some free forensic tools to analyze "Consolidated.db" file, one of them is "iStalkr[2]".

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

[2] iStalkr is a Evigator Digital Forensic product.

http://www.evigator.com

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.

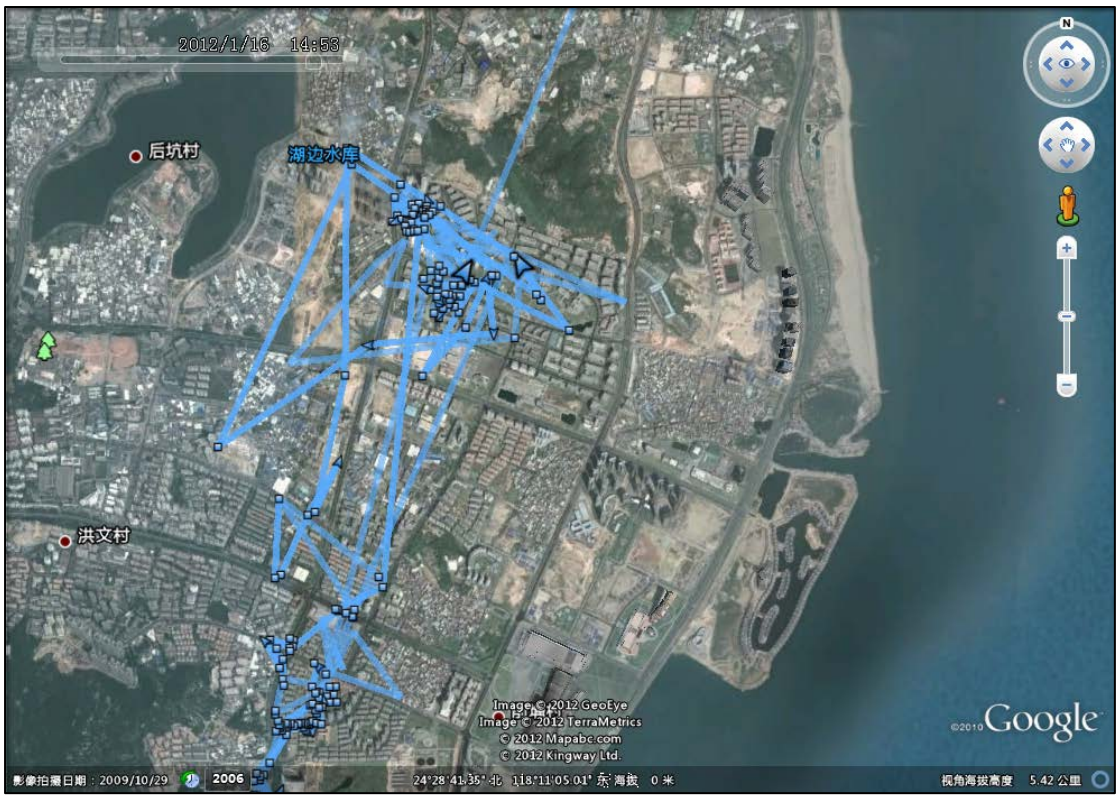

Figure 6 Cell and WIFI locations on Android devices.

Some Android phone models such as Motorola[3], 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.

[3] Motorola Blur is an UI-modified Android OS.

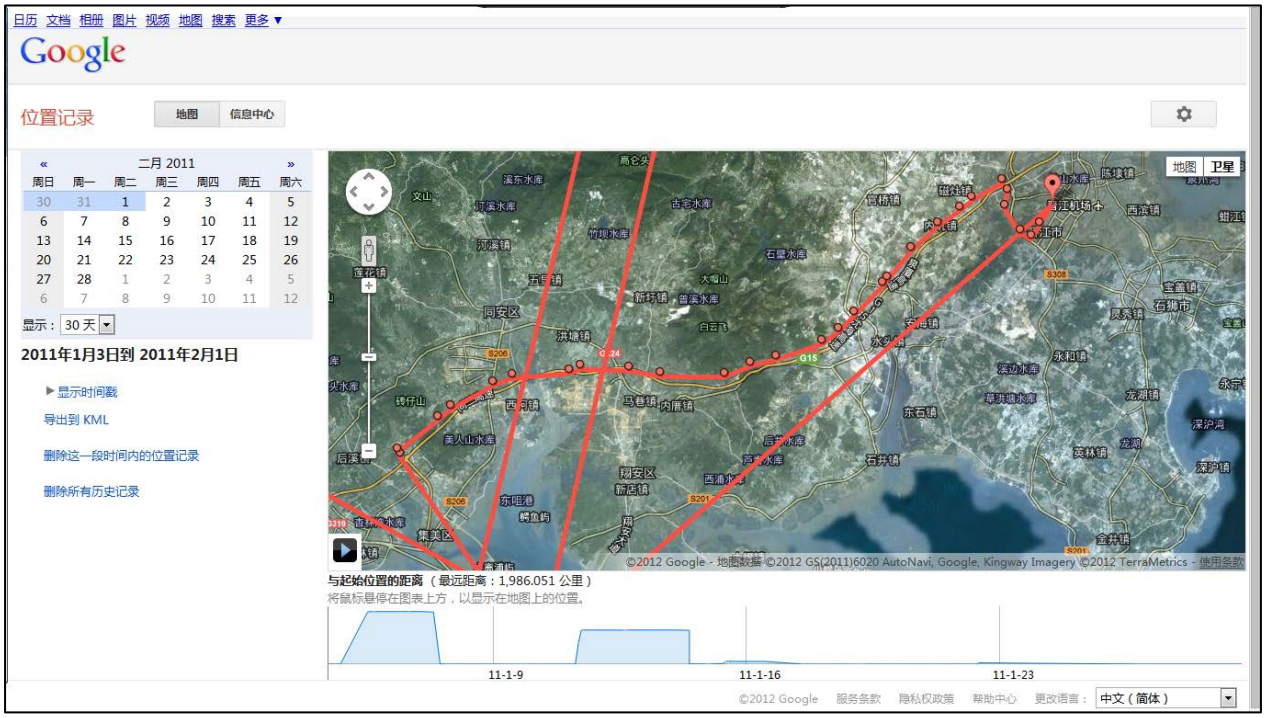

Figure 7　Google Latitude logs

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.