A Comparison of Geo-tagging in Mobile Internet Browsing Applications on iOS and Android

Samantha Comer, Dr Petra Leimich
Abertay University
Dundee, Scotland, DD1 1HG

July 2014

Abstract

Nowadays there is almost no crime committed without a trace of digital evidence, and since the advanced functionality of mobile devices today can be exploited to assist in crime, the need for mobile forensics is imperative. Many of the mobile applications available today, including internet browsers, will request the user's permission to access their current location when in use. This geolocation data is subsequently stored and managed by that application's underlying database files. If recovered from a device during a forensic investigation, such GPS evidence and track points could hold major evidentiary value for a case.

The aim of this paper is to examine and compare to what extent geolocation data is available from the iOS and Android operating systems. We focus particularly on geolocation data recovered from internet browsing applications, comparing the native Safari and Browser apps with Google Chrome, downloaded on to both platforms. All browsers were used over a period of several days at various locations to generate comparable test data for analysis. Results show considerable differences not only in the storage locations and formats, but also in the amount of geolocation data stored by different browsers and on different operating systems.

Keywords: geolocation data, GPS, Android forensics, iOS forensics

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

1 Introduction

Mobile devices have developed unimaginably over the last decade. The times when a mobile phone could merely make a phone call or send a text message have ceased, and now these portable devices can perform a vast range of functions. Amongst all generations across the globe today, mobile phones and tablets are becoming a part of daily life. Due to popular demand, constant improvements in technology and most importantly reductions in cost, their scope and usage in society seem limitless. According to Reiber [6], 91% of the global population today make use of a mobile device, and 82% of device usage is expended on some sort of application. It is estimated that Google alone processes more than 200,000 searches every minute, illustrating just how much data is transferred worldwide, all of which leaving traces of digital evidence. With the number of active mobile devices around the world forecast to reach 7.3 billion in 2014, greater than the global population [7], this fast developing industry is set to continue to thrive. It can, therefore, be seen that the need for mobile forensics is imperative.

Many integrated and downloadable applications use the owner's location when in operation, obtained from the device's Global Positioning System (GPS). Such geolocation evidence could prove invaluable to law enforcement, as it could allow an investigator to pinpoint where a user may have been at a particular point in time and thus, for example, prove or disprove a suspect's alibi.

In this paper, we examine to what extent geolocation data is available from the iOS and Android operating systems. We focus on the comparison of geolocation data recovered from Internet browsing applications Safari, Browser and Google Chrome. An iOS and Android device were used at various locations to generate comparable test data for analysis. It was expected that the two operating systems stored geolocation data in different ways, ranging from differences in data structure and architecture to the amount of data stored by each system, and in-depth analysis showed that there is a considerable difference in the amount of geolocation data that is

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

stored by the two mobile operating systems, particularly with regards to Google Chrome and Browser on Android.

Section 2 provides an overview of the iOS and Android operating systems' architecture, and reviews the current methods available for forensically analysing GPS data on each OS. In Section 3, we discuss the approaches taken to generate the evidence and perform the analysis. The results are presented in Section 4 and discussed in Section 5.

2 Background

2.1 Device Architecture

Both the iOS and Android platforms make use of partitions to structure and organise files and folders on devices.

2.1.1 iOS

The iOS platform makes use of two partitions; *firmware* and *user data* [4]. The *firmware* partition is used to perform system upgrades and contains system files, upgrade files and basic applications used to allow the device to function. The *user data* partition will be central to most investigations since, as the name suggests, contains all of the user data generated on the device. The *user data* partition will be the focus of this investigation on iOS.

2.1.2 Android

The Android platform makes use of six different partitions; */boot*, */system*, */recovery*, */data*, */cache*, and */misc* [5]. The */boot* partition is required to allow the device to boot. The */system* partition stores the entire Android operating system. This partition also contains the Android user interface and all of the native system applications used on the device. The */recovery* partition can be regarded as an alternative /*boot* partition. This allows the device to be booted into recovery mode and can be used for carrying out advanced recovery and maintenance tasks. The */data* partition contains the user generated data. This partition is where evidence relating to contacts, messages, settings and installed applications are stored. Wiping this partition can also be considered a factory reset of the device, restoring it to its original settings. The */cache* partition contains the frequently accessed data for improved device efficiency. Finally, the */misc* partition contains miscellaneous system settings. It is an essential partition for device functionality and if it becomes corrupt or is missing, some of the device's

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

features will not function correctly [5]. The */data* partition is considered the most valuable to a forensic examiner, as it contains the user generated data. The */data* partition will be the focus of this investigation on Android. Many android devices also allow for removable storage; however, as iOS devices do not, this is not investigated here.

2.2 Storage of geolocation data

Many applications on the iOS and Android platforms, including the Internet browsers, will ask the user if they can use their current location, and if the user agrees, their current location will be cached and the GPS data stored into an SQLite database, as SQLite databases are used by both operating systems to manage application data. SQLite databases are used primarily for structured data storage and have become a well-used method in smartphones and mobile devices today. Both the iOS and Android platforms allow developers to use SQLite for the creation of apps, therefore much of the application data can be found in these SQLite databases and so they are often a rich source of forensic evidence.

2.2.1 iOS

The iOS platform makes use of a single SQLite database file called *consolidated.db*, which stores all GPS data generated on the device. The file was introduced with iOS version 4. It is believed that GPS data is stored only in this file to allow for one centralised location, with the hope of increasing device efficiency. One centralised location is also useful to mobile forensics investigators since only a single file has to be examined for GPS data [3].

2.2.2 Android

In android, forensically valuable data will typically be found in the /*data* partition. Each application stores its data in a subdirectory named after the package [1], typically */data/data/<packageName>/databases*. However, SQLite files are not limited to this part of the file system, so a comprehensive search for database files needs to be conducted for a full analysis, rather than simply searching the /*data*/*data*/ path [2].

For example, Hoog [2] conducted an investigation on an Android HTC Incredible mobile device and found two SQLite databases in the subdirectory *app_geolocation* concerning GPS data and permissions. In this

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

investigation, these databases were *CachedGeoposition.db* and *GeolocationPermissions.db*.

3 Methodology

Given the differences in system architecture, we expected that the two operating systems would store geolocation data in different ways, and suspected that differences might also arise depending on whether the devices could use GPS only on WiFi or also on cellular data networks. In order to explore this as fully as possible given the constraints of the study, the two devices chosen for this research project were one phone and one tablet, and one of each OS. We decided that analysis of an Apple iPhone and an Android tablet would produce the most diverse, yet interesting results, and an iPhone 3GS and Motorola XOOM tablet were the devices of choice (see Table 1 for specifications).

Device	**Motorola XOOM**	**iPhone 3GS**
OS Version	Android Ice Cream Sandwich version 4.0.4	iOS Version 6.1.3
Cellular Network	N/A	Orange/EE
WiFi	Yes	Yes
Capacity	32GB internal storage (no additional SD cards would be used)	8GB internal storage

Table 1: Device specifications

Many apps may store geolocation information during use, including camera, web browsers, social networking apps, Skype and messaging. In order to focus on geolocation data that could be recovered from web browsers, we decided to compare the native web browsing applications, iOS Safari and Android Browser with each other and with the corresponding mobile versions of one of the most popular desktop browsers, Google Chrome.

The first phase of the project involved generating data on both devices. Since only the geolocation evidence was being analysed, it was important that both devices performed the same data-gathering activities, for example, browsing to the same Internet sites all in the same location. This avoided the

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

problem of confounding and ensured effective comparisons could be made about the recovered geolocation evidence.

The preliminary stages of any computer forensic investigation require that devices are imaged before being analysed, to avoid any evidence being accidentally modified by the examiner. Forensically imaging mobile devices is significantly different to that of traditional computer systems: Since a mobile device's built-in storage media cannot be removed safely, the device must be worked with directly [2, 3]. The use of specialised mobile forensic toolkits designed to extract data from these embedded systems is the most straightforward method of imaging mobile devices. For this research project, the XRY mobile forensics toolkit, created by Micro Systemation, was the tool of choice. XRY was chosen as it is a commercial tool and well recognised within the forensics community. A logical image was acquired from the iOS device using the XRY toolkit. Only logical images were required for this research project since no data was being deleted from the devices, and the analysis of deleted evidence would not be necessary. Unfortunately, the XRY toolkit proved incompatible with the Android device, the reasons for which remained unknown. Therefore, another method of imaging was required and since no other commercial tools were available, rooting the device became the only feasible option, and was carried out successfully. Manual rooting is not considered a desirable method of data acquisition within the forensics community. One of the major risks include potentially "bricking" the device. If this had occurred, all data generated during the previous phase of the project would have been lost, emphasising its risky nature.

4 Results

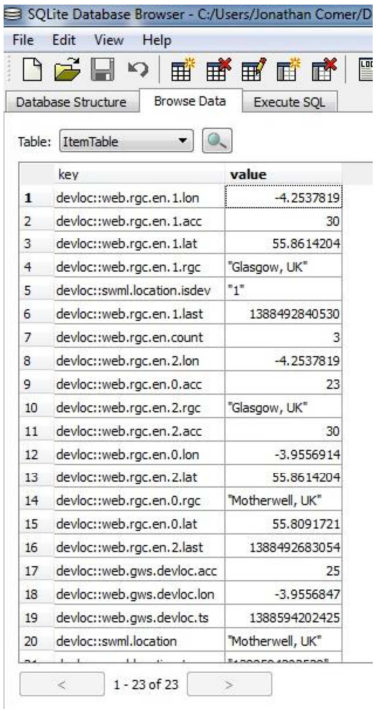
4.1 Native browsers: Safari and Browser

During the data-gathering phase, the Browser application was permitted to update its location automatically, without prompt, whenever it was opened. As the android device did not have a mobile data connection, any update was on WiFi. An SQLite database file of particular interest recovered from Browser was *http_www.google.co.uk_0.localstorage*. This contains latitude and longitude coordinates for the places where the Google

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

search engine updated the device's location. All expected records were found within this file.

Figure 1 shows an extract of the *localstorage* database file. "Glasgow, UK" and "Motherwell, UK" are represented with two records each. Copying and pasting the latitude and longitude values into Google Maps for the first “Glasgow, UK” record correctly revealed the location of the device at that time, which was in a Starbucks on Buchanan Street. It can be seen from Figure 2 that the accuracy of the result is extremely high.



	key	value
1	devloc::web.rgc.en.1.lon	-4.2537819
2	devloc::web.rgc.en.1.acc	30
3	devloc::web.rgc.en.1.lat	55.8614204
4	devloc::web.rgc.en.1.rgc	"Glasgow, UK"
5	devloc::swml.location.isdev	"1"
6	devloc::web.rgc.en.1.last	1388492840530
7	devloc::web.rgc.en.count	3
8	devloc::web.rgc.en.2.lon	-4.2537819
9	devloc::web.rgc.en.0.acc	23
10	devloc::web.rgc.en.2.rgc	"Glasgow, UK"
11	devloc::web.rgc.en.2.acc	30
12	devloc::web.rgc.en.0.lon	-3.9556914
13	devloc::web.rgc.en.2.lat	55.8614204
14	devloc::web.rgc.en.0.rgc	"Motherwell, UK"
15	devloc::web.rgc.en.0.lat	55.8091721
16	devloc::web.rgc.en.2.last	1388492683054
17	devloc::web.gws.devloc.acc	25
18	devloc::web.gws.devloc.lon	-3.9556847
19	devloc::web.gws.devloc.ts	1388594202425
20	devloc::swml.location	"Motherwell, UK"

Figure 1: Latitude and longitude coordinates stored by the Google search engine in the Android http_www.google.co.uk_0.localstorage file of the native Browser

Exporting the latitude and longitude values into Google Maps from the records correctly thus revealed the location of the device at those times, with high accuracy for all but one records. While this local storage file gave the coordinates of where the Browser application updated the location, no timestamps were found within the file, thus making it difficult for a forensic

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

investigator to use the information in a timeline. The file can, however, infer order, as location updates were stored sequentially, oldest first.

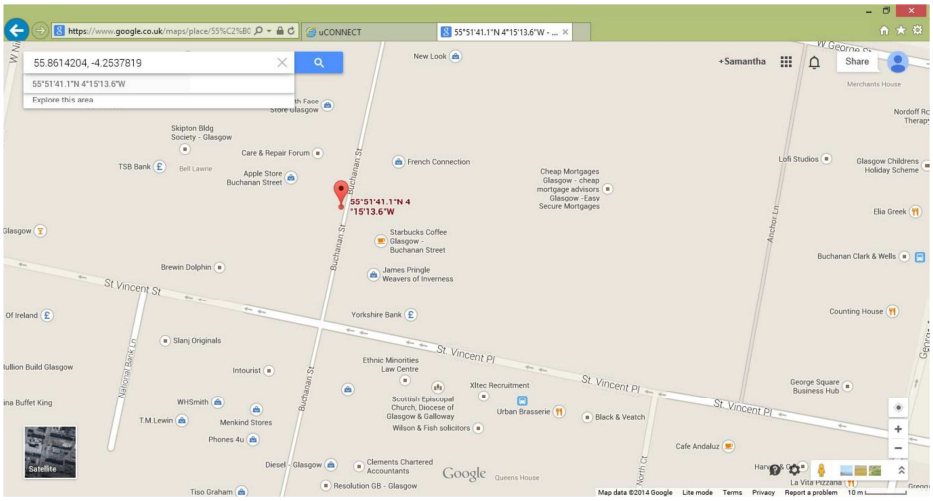


Figure 2: Google Maps representation of the coordinates taken from the first "Glasgow, UK" record, as described by entries 1 and 3 in Figure 1 above

The iOS platform uses a single, centralised database file, *consolidated.db*, which is used by all apps. We expected this file to store Safari's app data, including geolocation information, but this was not the case. It was thus established that the *consolidated.db* SQLite database contained no geolocation data. As Safari stored no data elsewhere on the system, no geolocation data for Safari could be retrieved.

4.2 Google Chrome

Google Chrome was installed on both devices, and used in the data gathering phase for the same activities in the same locations. The only geolocation data that was recovered from the Google Chrome application on Android were a set of GPS coordinates for the device's last cached position, acquired from the *CachedGeoposition.db* SQLite database file. No GPS coordinates could be found within the standard SQLite database files used by Google Chrome, despite setting the app to use the device's location when

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

in use. This result was very surprising, as it shows that the two internet browsing applications Browser and Chrome differ fundamentally with regard to location information, despite both having the location updated in each visited setting, and despite both being developed by Google. Even on the same Android device, Browser was able to provide highly accurate coordinates of where each update occurred whereas Google Chrome did not store these coordinates.

Android's Google Chrome History SQLite file contained no GPS coordinates either. However, a forensic investigator may be able to extract some more abstract, circumstantial location evidence from the browsing information that is stored. For example, an entry in the SQLite database file revealed through the URL visited and corresponding title field that weather information was requested for the Strathclyde region from the Met Office web site. While insufficient on its own, this could suggest that the requester was in the Strathclyde area when combined with other evidence.

The iOS Chrome History SQLite file contained comparable data to the Android Chrome History SQLite file. Again, no coordinates were stored in the table but the Glasgow region searched for on the Met Office web site was found, and therefore the same circumstantial location information could be inferred. Table 2 summarises the results.

OS	Application	Evidence	Extent of GPS Data
Android	**Browser**	*http_www.google.co.uk_0.localstorage* SQLite file	GPS coordinates for the places where the Google search engine had been set to use the device's location.
	Google Chrome	i) *CachedGeoposition* SQLite file ii) *History* SQLite file	i) No GPS coordinates. ii) Circumstantial location evidence. E.g. "Strathclyde"
iOS	**Safari**	*Consolidated.db* SQLite file	No GPS coordinates.
	Google Chrome	i) *Consolidated.db* SQLite file ii) *History* SQLite file	i) No GPS coordinates. ii) Circumstantial location evidence. E.g. "Strathclyde"

Table 2: Summary of results

In addition to SQLite, iOS apps use property lists for data storage. Several such plists were examined, particularly GeolocationSites.plist. No

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

coordinates were found in this plist. It did contain an entry for imdb.com, one of the websites accessed in the data generation phase of the project, but all that was available was a "ChallengeDate" and a "ChallengeCount", a timestamp and access count respectively.

5. Conclusion

There is a considerable difference in the amount of geolocation data that is stored by the two mobile operating systems, and a fundamental difference between the storage architecture on the two platforms. With regards to the Internet browsing applications in particular, both Browser and Google Chrome on the Android platform used application-specific SQLite databases to manage data and store browsing history. Surprisingly, despite both apps being operated by Google, and both having the location updated in each visited setting, they differed fundamentally with regard to location information. Browser was able to provide highly accurate coordinates of where each update occurred whereas Google Chrome did not store these coordinates.

iOS applications use SQLite database files and property lists to manage data. While property lists are application-specific, all geolocation data is centralised in one single iOS-managed SQLite database file, *consolidated.db*, which provided no valuable GPS information in this investigation. Certain tables, such as the CellLocation and WifiLocation tables, which were expected to be present within the *consolidated.db* database file did not exist, nor could these tables be found anywhere else on the iOS forensic image. The *consolidated.db* file simply contained two tables for compass calibration and details regarding the orientation of the device. As explained previously, we found no Safari data stored elsewhere on the system. This would warrant further investigation.

Our project had two main limitations in that slightly older versions of both operating systems were used, and only one device of each. With regard to the former, we used Android Ice Cream Sandwich, 4.0.4, despite Jelly Bean 4.1 – 4.3.1 being available and KitKat 4.4 being released in November 2013, shortly after the start of the project. We used iOS 6.1.3 while 7.0.1 was available. However, our findings should be applicable to a range of versions, past and future, as the underlying architecture of both operating systems and the apps themselves changes very rarely. With regard to only

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158
Author contact: p.leimich@abertay.ac.uk

one of each device being used, this means that we were unable to compare WiFi and 3G or 4G devices of the same OS. We were also limited to a single manufacturer. Android is used by many manufacturers, some of whom implement their own "dialect", which could affect the results. This is possible because Android is open source. iOS on the other hand is unlikely to be affected by such issues as it is used only by Apple.

References

[1] H. Chu, C. Lo and H. Chao. The disclosure of an Android smartphone's digital footprint respecting the Instant Messaging utilizing Skype and MSN. 2013. Electronic Commerce Research, pp. 399-410.

[2] A. Hoog. Android forensics: investigation, analysis and mobile security for Google Android. Elsevier. MA. 2011.

[3] A. Hoog and K. Strzempka. iPhone and iOS forensics: investigation, analysis and mobile security for Apple iPhone, iPad and iOS devices. Elsevier. MA. 2011.

[4] T. Proffitt. Forensic analysis on iOS devices. SANS White Paper. 2012. From http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

[5] H., Q. Raja. Android partitions explained: boot, system, recovery, data, cache & misc. 2011. From http://www.addictivetips.com/mobile/android-partitions-explained-boot-system-recovery-data-cache-misc/

[6] L. Reiber. Building a solution to today's problem: mobile device application overload. 2014. From http://blog.mobileforensicsinc.com/

[7] Silicon India. World to have more cell phone accounts than people by 2014. 2013. From http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

CFET 2014.
7th International Conference on Cybercrime Forensics Education & Training. Canterbury Christ Church University, 10-11 July.
ISBN 97801909067158

Author contact: p.leimich@abertay.ac.uk