Messaging Application Analysis for Android and iOS Platforms

Katie Corcoran[1]*, Aaron Read, MS[2], Joshua Brunty, MS[1], and Terry Fenger, PhD[1]

[1]: Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701

[2]: Target Forensic Services Laboratory, 7000 Target Parkway, Brooklyn Park, MN 55445

ABSTRACT (for Marshall):

The proliferation of smartphones in the last several years presents forensically relevant challenges. One of the challenges is that of the application. Used to enhance the capabilities of the phone to something beyond that of a conventional phone or feature phone, applications can hold a wealth of useful information about the user's actions. This research focused on applications that had a messaging capability. They fall into four types: traditional, Push-to-Talk, multi-functional, and gaming. Using both an Android and iOS platform, seven applications were used, and then the phones were analyzed for usage information. Information looked for fell into six categories: text, photo, and audio messages, location information, timestamps, and sender/recipient information.

DISCLAIMER:

No claim is made to the exclusive rights to use the trademarks for Apple, Google, HTC, Sprint, Access Data, Cellebrite, Kakao, Facebook, Voxer, Loudtalks, Zynga, and WhatsApp or any of their associated products.

INTRODUCTION:

We live in a connected world. To imagine going a day without the internet or some form of technology is to strike fear into the hearts and minds of many Americans today. The

smartphone is one of the core mediums used to keep our world connected. They have been developed to offer more than just the traditional calls and messaging. Today's smartphones are phone, calendar, e-mail, and much more all wrapped up into one small, portable device. They are the merging of two very important technologies: the telephone and the internet.

The integration of the internet with the mobile phone in the consumer market was realized fully in 2007 when the iPhone was announced [1]. Running its own proprietary operating system, iOS, the iPhone represented the next generation of mobile devices. The iPhone came preloaded with a variety of applications that increased the functionality of the iPhone; they included a calendar, stocks, weather, music, and several other useful applications. It was an immediate success highlighted by the release of a new iPhone model as well as the launch of the App Store a year after the original iPhone release date. The App Store originally offered 500 third party applications [2]. Since its launch the App Store has grown exponentially, and now offers more than 650,000 third party applications for download and has had more than 30 billion downloads as of June 2012 [3].

The first competitor to the iPhone with a similar user interface (UI) and hardware was more than a year after the iPhone's initial release. In August 2008, Google announced the first Android phone, the HTC Dream, and released it later that year [4]. The Android operating system was different from iOS in that it was not proprietary; it is Linux-based and open-source (released under the Apache License). Because of its format, the Android operating system is able to be used by a range of manufacturers who can adapt it to their own environments. This feature of the Android system causes great variability between manufacturers and even the

phones of individual manufacturers. Similar to the iPhone, Android devices come preloaded with applications; these will also vary between carriers and phone/mobile device manufacturers. Google also launched the Android Market, renamed Google Play in March 2012 [5], concurrently with the HTC Dream. The Market experienced similar growth to the App Store going from 2300 apps 6 months after launch to more than 500,000 apps available and more than 15 billion downloads [3]. Google Play also offers many of the same applications available in the App Store allowing for cross-platform interaction.

Of all the changes to mobile devices that accompanied the smartphone, one of the most revolutionary would have to be the applications. They increase the capabilities and functionality of the phone to something more than that of a typical phone. Applications are able to do an almost unlimited number of processes; they can monitor stocks, manage banking, help navigate new places, be used for gaming and shopping, messaging, and enhance photos, just to name a small number of available functions. While many of these applications would and should be of forensic interest, this paper focuses mostly on the analysis of applications with messaging capabilities.

Applications with messaging capabilities present intriguing possibilities because they are an alternative to text messaging and will not show up in phone usage the same as traditional messaging. These applications are able to utilize Wi-Fi connections in place of the cellular network for calling and texting purposes. Applications with messaging capabilities come in many forms. Many of the applications used for messaging work similarly to traditional texting; they are able to send messages and pictures and may also have the additional ability to attach a

location. Another category of applications, known as Push-to-Talk (PTT), are capable of sending short messages using the Voice over Internet Protocol (VoIP) similar the functionality of walkie-talkies. Yet another category presents applications that combine all of these capabilities into one program; they can text, send photos, locations, voice messages, and may also have the ability to make phone calls. A final category of messaging applications is those used not primarily for messaging. Many gaming applications have the ability to send messages between players during gameplay. All of these application categories present different forensic information as well as the challenges in accessing such information.

Applications present a new era of consideration when performing mobile device examinations for a variety of reasons. First of all they are widely used among smartphone users [6]. Their ability to increase the functionality of the smartphone is indispensable. In addition, applications provide a wealth of information about a user's interactions when not using standard phone functions. The data usage can be used to show interaction between two people as well as give an accurate location that may be used to prove or disprove a claim by someone under suspicion. Also if the content of messages sent can be accessed, more information about interaction can be gained. While the message content may not be a so-called "smoking gun," the connection may be enough to move forward in an investigation. The potential for being able to associate people makes application analysis a valuable tool for investigations.

Using the information from several different apps on the phone, one study showed a hypothetical situation in which a general flow of events was developed using location

information, names of people communicated with, and timestamps [7]. One of the main obstacles encountered when applications are present is most information available in the literature is about the general file structure of where applications are stored. Very little is present on what information can be gained specifically from different applications. While this can vary greatly between iOS and Android, having a general idea of what information could potentially be present can only be helpful.

Some assessment has been done concerning how third party applications and their data are stored with both the iOS and Android platforms. viaForensics has gone through both systems and identified the path used to find the information for third party applications. In the iOS system, application information is kept in the /private/var/mobile/applications folder [8]. This folder is specifically used to hold information about third-party applications as the preloaded applications are standard and kept in a separate folder. In the Android system, application information is kept in the /data/data folder [9]. This folder holds every application on the phone due to the fact that every manufacturer and carrier has a slightly different OS with different preloaded applications.

For this research, a variety of applications with messaging capabilities were assessed. The applications chosen fell within one of the four categories previously discussed: traditional messaging (similar to texting), PTT, multi-functional messaging, and gaming applications. The applications were tested on both the iOS and Android platforms to locate stored data and compare what information the application stored in the physical phone. Several specific types

of information were looked for that at least two of the applications could potentially have a need to store.

METHODS AND MATERIALS:

To assess the information stored on the phone by messaging applications, both an Android and iOS device were used. Seven applications were used; each fell into one of the messaging application categories described previously.

To prepare the phones for the process a factory reset was initiated on each device in order to remove any information from previous users and applications. When they were ready, the phones were imaged with no applications added. The applications were then added to the phone but not used, and the phone was imaged again. Each of the applications was then used to test their functionality. After the applications were used, the phones were imaged again. Using forensic software both the physical and logical images of the phones were analyzed to determine what information the applications store on the physical phone.

Cell Phone Platforms:

Android For the Android Platform, the HTC EVO 3D (model PC86100) was used. The carrier for the phone was Sprint. The phone had 1 GB of internal memory with an additional 4GB microSD card. The phone was running the Android software version 2.3.4 ("Gingerbread"). The phone was not password protected, and the phone had USB debugging enabled and was rooted to allow complete access to the phone's operating system. The phone was rooted using a publicly

available method from HTCEvoHacks.com and the HTC Unlock Bootloader method from HTCDev (htcdev.com).

iOS For the iOS platform, the Apple iPhone 4 (model A1332) was used. The carrier for the phone was AT&T. The phone had 16 GB of internal memory and had no external memory. The phone was running iOS version 5.0.1. The device was not password protected.

Applications:

The applications chosen for this study were ones available from both the Apple App Store and Google Play. They were also chosen because of the number of downloads for the applications. All applications had been downloaded at least one million times and up to 100 million per the numbers listed on Google Play. The number of times an application had been rated and the value of the rating was also considered. The free version for each application was chosen if available as these are the versions most likely to be found on devices. All application versions were the most currently available versions at the time of the research. A summary of each application's capabilities can be found in Table 1.

Traditional Messaging Two applications were used that were similar to regular text and photo messaging: Facebook Messenger (developed by Facebook Inc.) and WhatsApp Messenger (developed by WhatsApp Inc.). Facebook Messenger allows users to send messages to one person or to a group. Users can also send photos and attach their location. The version used was 1.7.002 for Android and 1.7 for iOS. WhatsApp allows users to message similarly to Facebook Messenger. A phone number is required to set up the account. The versions used were 2.6.10 for iOS and 2.7.7532 for Android.

PTT Messaging Only one application was used that was strictly PTT. Zello Walkie-Talkie was released by Loudtalks Inc. The application allows users to send short voice messages using VoIP. The version of Zello used was 1.28 for Android and 1.2 for iOS.

Multi-Functional Messaging The applications used that combined traditional and PTT messaging were KakaoTalk Messenger (developed by Kakao Corp.) and Voxer (developed by Voxer Llc.). KakaoTalk includes all the features of traditional and PTT messaging as well as making real time voice calls. The version of Kakao used was 2.9.6 for iOS and 3.1.1 for Android. Voxer includes all of the features from traditional and PTT messaging apps with no additional features. The version of Voxer used was 2.4.2003 for iOS and 0.9.7.3.0004 for Android.

Gaming Applications The applications used that were primarily for gaming but also had a messaging function were Words with Friends (developed by Zynga Inc.) and Draw Something (developed by OMGPOP Inc.). Words with Friends allows users to hold a text conversation throughout the duration of a game. The version of Words with Friends used was 4.13 for iOS and 4.90 for Android. Draw Something allows users to send short messages between users with each drawing done. There is no continuous conversation. The version of Draw Something used was released on 15 May 2012 for iOS and on 21 May 2012 for Android.

Processing Tools:

Imaging Tools Images of the phones were taken using the CelleBrite UFED Ultimate (Cellebrite USA Corporation, 266 Harristown Rd, Suite 105, Glen Rock, NJ 07452). The software version used was 1.1.9.7.

Data Analysis Images obtained were analyzed using Cellebrite's UFED Physical Analyzer 3, a component of the UFED Ultimate system, and AccessData Forensic Toolkit (version 4.0.1.35151).

RESULTS:

When looking for what information was kept in the phone by the applications, six different criteria were looked at: text messages, location information, audio messages, time stamps, photo messages, and sender and recipient information. Each corresponds to a function that at least one of the applications was capable of performing. Unless otherwise noted, results for Android and iOS were similar. A summary of results can be found in Tables 2 and 3 for iOS and Android respectively. Table 4 contains detailed information about user information for each application as well as file locations.

Text Messages One of the most important components to the messaging applications are the messages themselves. Access to the content of the messages could lead to important information. Of the seven applications assessed on both iOS and Android all but one of the applications kept some or all of the message content on the phone. Only Zello, which only transmits audio messages, had no message content. Draw Something was different from the rest of the applications that kept message content in that only the last messages sent with a drawing or guess were kept on the phone. All other applications kept full message content and in the correct order sent or received.

Location Only three of the seven applications used the location information from the phone when sending or receiving messages. The apps with location tracking kept accurate records of

a sender's location when location services were enabled. Two of the apps recorded the location information with every message: Facebook Messenger and Voxer. The third application with location services was WhatsApp. This application only sent location information when the sender checked in at a location (while this is based on location services, the application does allow the user to select any location at which to check in).

Audio Messages Applications that had the PTT capability presented a unique challenge: How would an audio message be kept on a phone? Would it be playable? The answer for KakaoTalk and Voxer was that audio messages were indicated in the history of conversations however the content of the audio files were not available. Zello was different though because a file was found that may contain the voice messages. The problem for this though was that they were unplayable because they were in an uncommon Speex format that was missing the correct programming to be played. The file was stored on the microSD card instead of with the program files on the imbedded chip.

Timestamp Timestamps can provide useful information about when a conversation occurred. Almost all of the applications placed a timestamp on each message sent. The only application that did not accurately timestamp the messages sent or received was platform specific. The Android version of WhatsApp did not accurately timestamp each message.

Photo Messages Photos may not contain the most content information however their presence can provide good information. The files were searched to determine if the photos were viewable. All of the applications that had photo messaging capabilities had photo messages that were viewable.

Sender and Recipient Information Information kept by the application about the user on the phone was the most variable amongst applications and platforms. Some applications kept very little information about users, and others retained most pertinent information. Each application, except Zello, kept a list of contacts as well as an identifier of the contact with each message. For the purpose of this paper, the sender is the person sending the phone information, and the recipient is the person that owns the phone.

KakaoTalk Messenger On iOS the information about the users kept on the phone was the full name, user-generated nickname, username, user ID, and phone number used to activate account for both the sender and recipient. On Android the information about the users was the username and phone number for the sender and the user ID for both.

Zello Walkie-Talkie On both iOS and Android, the information about the users kept on the phone was the username, and this was only for the sender. On Android the information was kept on the microSD card (not with the other application data), similar to the audio messages.

Voxer On both iOS and Android, the information about the users kept on the phone was the username and full name, and this was for both the sender and recipient. The username corresponded to the day and time at which the user made the new account.

Facebook Messenger On both iOS and Android the information about the users kept on the phone was the full name and Facebook user ID for both sender and recipient. The Android version also kept the e-mail address and phone number of each contact.

WhatsApp Messenger On iOS the information about the users kept on the phone was user ID and full name, and these both applied only to the sender. The user ID corresponded to the cell phone number used to activate the account. On Android the same information was kept as on iOS as well as explicitly stating the cell phone number used to activate the account. The information kept corresponded to both sender and recipient.

Words with Friends On both iOS and Android the information about the users kept on the phone was the username, server ID, and e-mail address. The information was kept for both sender and recipient for the username and server ID, and the e-mail address was only kept for the recipient.

Draw Something On iOS and Android the information about the users kept on the phone was the username and user ID. The information was kept for both the sender and recipient.

DISCUSSION AND CONCLUSION:

From the results of this research, it can be observed that a wealth of information is available from third party applications if you know where to look. Having the capability to read the messages sent between two parties could be immensely valuable. Also, knowing the location from where messages were sent could also provide useful evidence. The information does, however, have some limitations, which are application-, research-, and device-dependent.

Application-dependent limitations outnumber the device-dependent limitations mostly because they come from a variety of developers. Because of the variability between the

applications and platforms for what information is kept about users, challenges are likely to occur. Unless the username or some other identifier specifically from the account of interest is known, it could be impossible to determine with whom a conversation was occurring. However, the applications that kept the number of the phone associated with the user, as with Kakao, WhatsApp, and Facebook, could provide easy identification of the message sender. Also, when considering the applications that had PTT capabilities, the audio messages were playable on the physical phone, and while the messages may prove to contain pertinent information, potentially altering the evidence on the phone to listen to the messages is something to be considered. Another consideration also involves the actual phone. If a manual examination is to be performed, some of the application content can only be accessed when connected to a network which poses a problem when SWGDE guidelines suggest that a phone be isolated [10]; Table 5 contains a list of the applications and whether they are able to be accessed in airplane mode with no Wi-Fi for both iOS and Android.

Other limitations apply to the devices and the research. Because the conversations only took place between two users and no others, it is difficult to predict how easy it would be to separate out isolated conversations occurring between different people. A final limitation concerns the devices used; they were not running the most recent operating systems, nor were they recently released phones both having been release in 2011 or earlier. At the time of this research version 5.1.1 was available for iOS, and the HTC EVO 3D was upgradable to version 4.0.3 (Ice Cream Sandwich) with a further version 4.0.4 available for Android.

Despite the limitations of the research, valuable information was gained. Knowing what information can be found in an application could be indispensable to an investigation. Because of this, future research in this area should focus on other commonly used applications. While they would not have to necessarily be messaging applications, any application that could potentially hold information of forensic interest would be useful. Another area of potential research would be to determine if there is a method that can be used to play the Speex files from Zello.

REFERENCES:

1: Honan, Matthew [Internet]. Macworld; c 1994-2012 [cited 2012 June 27] http://www.macworld.com/article/1054796/iphone.html

2: Apple Press Info [Internet]. Apple; c 2012 [cited 2012 June 27] http://www.apple.com/pr/library/2008/07/10iPhone-3G-on-Sale-Tomorrow.html

3: Mobile Statistics [Internet]. Mobile Statistics; c 2012 [cited 2012 June 27] http://www.mobilestatistics.com/mobile-statistics/

4: Holson, LM and Helft, M [Internet]. The New York Times; c 2012 http://www.nytimes.com/2008/08/15/technology/15hit-15google.15312776.html

5: Rosenberg, J [Internet]. Google Official Blog; c 2012 [cited 2012 June 27] http://googleblog.blogspot.com/2012/03/introducing-google-play-all-you.html

6: Our Mobile Planet [Internet]. Think With Google; c 2012 [cited 2012 June 27] http://www.thinkwithgoogle.com/mobileplanet

7: Levinson A, Stackpole B, and Johnson D. Third Party Application Forensics on Apple Mobile Devices. 44th Hawaii International Conference on System Sciences; 2011 Jan 4-7; Poipu, Kauai, Hawaii. 9 p.

8: Hoog A and Strzempka K. iPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices. Amsterdam: Syngress; 2011. 336 p.

9: Hoog A. Android Forensics: Investigation, Analysis, and Mobile Security for Google Android. Amsterdam: Syngress; 2011. 432 p.

10: SWGDE. Best Practices for Mobile Phone Examiners. SWGDE; 2009 May 21. Version 1.0. 10 p.

FIGURES:

Table 1. Overview of what functions the applications chosen are able to perform.

Application	Text Messaging	Voice Messaging	Photo Messaging	Calling	Location	Gaming
KakaoTalk	X	X	X	X		
WhatsApp Messenger	X		X		X	
Facebook Messenger	X		X		X	
Voxer	X	X	X		X	
Zello	X	X				
Words with Friends	X					X
Draw Something	X					X

Table 2. Overview of what information is stored on the phone by each application for the iPhone. Also the file location for application information is noted. Table notes: [1] sender and recipient information varied between applications and platforms; [2] voice messages were indicated in chat logs; content was not in obvious form; [3] located in a different location than the remainder of the usage data; [4] file present that may have contained messages but was in an unreadable Speex format;[5] only the last guess/draw comments were kept; [6] inaccurate timestamps kept for messages ; [7] location information only kept when user checks in.

Application Name	Text Messages	Lat/Lon Coordinates	Sender Info	Recipient Info	Audio Messages	Timestamp	Photo Messages
KakaoTalk	Y	N	Y[1]	Y[1]	Indicated No content[2]	Y	Y[3]
Zello	N	N	Y[1]	Y[1]	Y^	Y[6]	N/A
Voxer	Y	Y	Y[1]	Y[1]	Indicated No Content[2]	Y	Y[3]
Facebook Messenger	Y	Y	Y[1]	Y[1]	N/A	Y	N/A
WhatsApp Messenger	Y	Y[7]	Y[1]	N	N/A	N	N/A
Words with Friends	Y	N	Y[1]	Y[1]	N/A	Y	N/A
Draw Something	Y/N[5]	N	Y[1]	Y[1]	N/A	Y	N/A

Table 3. Overview of what information is stored on the phone by each application for the Android. Also the file location for application information is noted. Table notes: [1] sender and recipient information varied between applications and platforms; [2] voice messages were indicated in chat logs; content was not in obvious form; [3] located in a different location than the remainder of the usage data; [4] file present that may have contained messages but was in an unreadable Speex format;[5] only the last guess/draw comments were kept; [6] inaccurate timestamps kept for messages; [7] location information only kept when user checks in.

Application Name	Text Messages	Lat/Lon Coordinates	Sender Info	Recipient Info	Audio Messages	Timestamp	Photo Messages
KakaoTalk	Y	N	Y[1]	Y[1]	Indicated No Content[2]	Y	Y[3]
Zello	N	N	Y[1]	N	Y^	Y[6]	N/A
Voxer	Y	Y	Y[1]	Y[1]	Indicated No Content[2]	Y	Y[3]
Facebook Messenger	Y	Y	Y[1]	Y[1]	N/A	Y	Y
WhatsApp Messenger	Y	Y[7]	Y[1]	Y[1]	N/A	Y	Y
Words with Friends	Y	N	Y[1]	Y[1]	N/A	Y	N/A
Draw Something	Y/N[5]	N	Y[1]	Y[1]	N/A	Y	N/A

Table 4. Detailed user information for each application as well as file locations on each platform.

Application Name	iOS	Android
KakaoTalk	[1]- Name- for both, nickname- for both, User ID- for both [+]- Not in same place as other info Data>Data>mobile>Applications>578…>Documents>Talk.sqlite [+]Data>Data>mobile>Applications>578..>Library>Caches>Downloads	[1]- User ID- For sender, phone number used to activate account-for sender, Name- For sender, App ID- for both; [+]- Not stored in the same place as the rest of the info and doesn't show up in physical image but are in images Linux Native Partition (1)>Root>data>com.kakao.talk>databases>KakaoTalk.db [3]Linux Native Partition (1)>Root>data>com.kakao.talk>cache
Zello Walkie-Talkie	[1]- Username-only sender (found in index file); [6]- Timecode present but does not correspond to msgs, ^- Data present but unable to listen (missing container) Data>Data>mobile>Applications>B82…>Library>Preferences	[1]- Username- for sender, [6]- Time stamps do not correlate to the times messages were sent, ^- Data present but unable to listen (missing container) Linux Native Partition (1)>Root>data>com.loudtalks>databases>google_analytics.db

Voxer	[1]- Username (corresponds to when they joined the application)- for both, Name- for both, [3]- Not in same place as other info Data>Data>mobile>Applications>E44…>Documents>rv.db [3]Data>Data>mobile>Applications>E44>Documents>imageCache	[1]- Username (corresponds to when they joined application)- for both, Name-for both, E-mail address- for both, phone number- for recipient [3]- Not stored in the same place as the rest of the info Linux Native Partition (1)>Root>data>com.rebelvox.voxer> databases>rv.db [3]NO NAME_0>Voxer (SD card)
FB Messenger	[1]- Name- for both, Facebook User ID- for both Data>Data>mobile>Applications>390…>Library>Caches>orca2.db	[1]= FB ID- for both, Name- for both, E-mail Address- for both, Phone number- for both Linux Native Partition (1)>Root>data>com.facebook.orca> databases>threads_db2
WhatsApp Messenger	[7]- Only when sender checks in, [1]- User ID (which is cell phone's #)- for sender, Name- for sender Data>Data>mobile>Applications>5E9…>Documents> ChatStorage.sqlite	[7]- Only when user checks in, [1]- User ID (corresponds to phone number used to activate account)- for both, Display name- for both, phone number-for both Linux Native Partition (1)>Root>data>com.whatsapp>msgstore.db <&>wa.db
Words With Friends	[1]- Name- for both, Server ID- for both, e-mail address- for recipient Data>Data>mobile>Applications>6c2>Library>Application Support> WordsWithFriendsFree>chess_database.sqlite	[1]- User ID- for both, E-mail address- for recipient, Name- for both Linux Native Partition (1)>Root>data>com.zynga.words>databases> WordsFramework
Draw Something	[5]- Only the last guess/draw comments, [1]= ID- for both, Username- for both Data>Data>mobile>Applications>A78…>Documents>blobcache.db3>tables>objects>blobs	[5]- Only the last guess/draw comments, [1]= ID- for both, Username- for both Linux Native Partition (1)>Root>data>com.omgpop.dstfree> files> blobcache.db3

Table 5. Overview of which applications have accessible content when the phone is in Airplane Mode with no Wi-Fi broken down by platform.

Application	**iOS**		**Android**	
	Yes	**No**	**Yes**	**No**
KakaoTalk	X		X	
WhatsApp Messenger	X		X	
Voxer	X		X	
Facebook Messenger	X			X

Zello	X			X
Words with Friends		X		X
Draw Something		X		X