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

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.

Introduction

Cell phones are a commonly encountered piece of evidence in any investigation in this day and age. With the spread of smartphones in the last several years, it is not uncommon to come upon one of these as opposed to a conventional phone or a feature phone. Most smartphones on the market in the United States have one of two platforms: iOS and Android.

Both of these operating systems are enhanced by a multitude of third party applications that can perform an almost infinite number of actions such as stock monitoring, banking, gaming, shopping, messaging, and photo enhancement. This research however focused mainly on applications that had messaging capabilities.

Applications with messaging capabilities come in many different forms. Some applications are able to only send text and photo messages, referred to as traditional messaging; others are strictly push-to-talk (PTT) and operate similarly to walkie-talkies and send only audio messages. Another type of application combines both traditional and PTT messaging, referred to as multi-functional. A final type of application is one primarily for gaming but allows players to send messages back and forth. The applications are attractive because they can be used strictly through Wi-Fi, which means they can be used on more devices and not require cellular service.

Using the number of ratings and number of downloads from Google Play, the Android application market, seven applications present in both Apple's AppStore and Google Play were chosen. Each one fell into one of the four types of messaging applications. For traditional messaging, WhatsApp Messenger and Facebook Messenger were chosen. For PTT messaging, Zello Walkie-Talkie was chosen. For multi-functional messaging, KakaoTalk and Voxer were chosen. For gaming applications, Words with Friends and Draw Something were chosen.

The applications were loaded onto an iPhone 4 (iOS platform) and a HTC EVO 3D (Android platform) and used to test out the different capabilities of each application. After imaging the phones, the images were searched for different information about the users of the application and the usage.

Methods and Materials

Phones:

- Apple iPhone 4: Carried by AT&T™, 16 GB of internal memory, iOS version 5.0.1, not password protected
- HTC EVO 3D: Carried by Sprint™, 1 GB of internal memory with a 4GB microSD card, Android software 2.3.4 (Gingerbread), not password protected, rooted

Applications:

- Facebook Messenger: developed by Facebook Inc., version 1.7 for iOS and version 1.7.002 for Android
- WhatsApp Messenger: developed by WhatsApp Inc., version 2.6.10 for iOS and version 2.7.7532 for Android
- Zello: developed by Loudtalks Inc., version 1.2 for iOS and version 1.28 for Android
- KakaoTalk Messenger: developed by Kakao Corp., version 2.9.6 for iOS and version 3.1.1 for Android
- Voxer Walkie-Talkie PTT: developed by Voxer Llc., version 2.4.2003 for iOS and version0.9.7.3.0004 for Android
- Words with Friends: developed by Zynga Inc., version 4.13 for iOS and 4.90 for Android
- Draw Something: developed by OMGPOP Inc., version released on 15 May 2012 for iOS and on 21 May 2012 for Android

Capabilities	Text Msgs.	Audio Msgs.	Photo Msgs.	Calls	Location	Games
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

Analysis Tools:

- Imaging Tool: CelleBrite UFED Ultimate, version 1.1.9.7
- Data Analysis: UFED Physical Analyzer 3, part of the UFED Ultimate system, and AccessData® Forensic Toolkit® (version 4.0.1.35151).

Results

iPhone	Text Msg.	Location	Sender	Recipient	Audio Msg.	Time	Photo Msg.
Kakao	Y	N	Y[1]	Y[1]	Indicated[2]	Y	Y[3]
Zello	N/A	N	Y[1]	N	Y[4]	N	N/A
Voxer	Y	Y	Y[1]	Y[1]	Indicated[2]	Y	Y[3]
FB Msngr.	Y	Y	Y[1]	Y[1]	N/A	Y	N/A
WhatsApp	Y	Y	Y[1]	N	N/A	N	N/A
Words WF	Y	N	Y[1]	Y[1]	N/A	Y	N/A
Draw ST	Y/N[5]	N	Y[1]	Y[1]	N/A	Y	N/A

[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

Android	Text Msg.	Location	Sender	Recipient	Audio Msg.	Time	Photo Msg.
Kakao	Y	N	Y[1]	Y[1]	Indicated[2]	Y	Y[3]
Zello	N/A	N	Y[1]	N	Y[4]	N	N/A
Voxer	Y	Y	Y[1]	Y[1]	Indicated[2]	Y	Y[3]
FB Msngr.	Y	Y	Y[1]	Y[1]	N/A	Y	Y
WhatsApp	Y	Y	Y[1]	Y[1]	N/A	Y	Y
Words WF	Y	N	Y[1]	Y[1]	N/A	Y	N/A
Draw ST	Y/N[5]	N	Y[1]	Y[1]	N/A	Y	N/A

Discussion and Conclusion

Limitations of Project:

- It could be impossible to determine with whom a conversation was occurring without a username or other identifier
- Only two users were messaging; it may be difficult to identify what messages apply to which users if more than two were present
- Audio messages were playable when a manual examination was done however some applications are not accessible when in airplane mode and not connected to Wi-Fi (important consideration for investigations)

Application	iPhone		Android	
Airplane Accessible?	Yes	No	Yes	No
KakaoTalk	X		X	
WhatsApp Messenger	X		X	
Facebook Messenger	X			X
Voxer	X		X	
Zello	X			X
Words with Friends		X		X
Draw Something		X		X

- Most recent operating systems for each operating system were not used; 5.1.1 was available for iOS and the EVO 3D could be upgraded to 4.0.3 (Ice Cream Sandwich) and version 4.0.4 was the most recent release for Android
- Applications updated frequently and may change what information is stored

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.

Future Work

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. Other research could look into finding a method for playing the Speex files.

References

Holson, Laura M and Helft, Miguel. "T-Mobile to be first to use Google's Android." The New York Times. Retrieved 27 June 2012

Honan, Matthew. "Apple unveils iPhone." Macworld.com. Retrieved 27 June 2012 http://www.macworld.com/article/1054796/iphone.html

Hoog, Andrew. *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android.* Syngress: Amsterdam. 2011.

Hoog, Andrew and Strzempka, Katie. *iPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices.* Syngress: Amsterdam. 2011.

"iPhone 3G on Sale Tomorrow." Apple.com. Retrieved 27 June 2012 http://www.apple.com/pr/library/2008/07/10iPhone-3G-on-Sale-Tomorrow.html

Levinson, Alex, Stackpole, Bill, and Johnson, Daryl. "Third Party Application Forensics on Apple Mobile Devices." Proceedings of the 44th Hawaii International Conference on System Sciences. 6 Jan 2011.

"Mobile Statistics." Mobilestatistics.com. Retrieved 27 June 2012 http://www.mobilestatistics.com/mobile-statistics/

http://www.nytimes.com/2008/08/15/technology/15hit-15google.15312776.html

Rosenberg, Jamie. "Introducing Google Play: All your entertainment, anywhere you go." Google™ Official Blog. Retrieved 27 June 2012 http://googleblog.blogspot.com/2012/03/introducing-google-play-all-you.html

Image Sources

http://nasa4ppc.files.wordpress.com/2011/09/htc-evo-3d-2.jpg

http://techleash.com/wp-content/uploads/2010/07/iPhone-4.jpg