Messaging Application Analysis for Android and iOS Platforms
Katie Corcoran¹; Aaron Read, MS²; Joshua Brunty, MS³; and Terry Fenger, PhD⁴
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.

Methods and Materials

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 Viber were chosen. For gaming applications, Words with Friends and Draw Something was 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.

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 Viber were chosen. For gaming applications, Words with Friends and Draw Something was 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

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 Viber were chosen. For gaming applications, Words with Friends and Draw Something was 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.

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 not 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)

Results

<table>
<thead>
<tr>
<th>Phone</th>
<th>Text Msg</th>
<th>Location</th>
<th>Sender</th>
<th>Recipient</th>
<th>Audio Msg</th>
<th>Time</th>
<th>Photo Msg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kakao</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Zello</td>
<td>N/A</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Viber</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/A</td>
<td>Y/A</td>
</tr>
<tr>
<td>FB Mgr.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/A</td>
<td>Y/A</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N/A</td>
<td>Y/A</td>
<td>Y/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Draw Sht</td>
<td>Y/N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y/A</td>
<td>Y/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone</th>
<th>Text Msg</th>
<th>Location</th>
<th>Sender</th>
<th>Recipient</th>
<th>Audio Msg</th>
<th>Time</th>
<th>Photo Msg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kakao</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Zello</td>
<td>N/A</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Viber</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/A</td>
<td>Y/A</td>
</tr>
<tr>
<td>FB Mgr.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/A</td>
<td>Y/A</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N/A</td>
<td>Y/A</td>
<td>Y/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Draw Sht</td>
<td>Y/N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y/A</td>
<td>Y/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 not 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)

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

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

Image Sources