B30 Messaging Application Analysis for Android and iOS Platforms

Katie Corcoran, BS, 1106 11th Ave, Apt 4, Huntington, WV 25701; Aaron Read, MS, 7000 Target Pkwy, Brooklyn Park, MN 55445; and Joshua L. Brunty, MS, and Terry Fenger, PhD, 1401 Forensic Science Dr, Huntington, WV 25701*

After attending this presentation, attendees will have a better understanding of how to access information relevant to mobile device application usage and what remains in a smartphone's memory.

This presentation will impact the forensic science community by providing a straightforward explanation of what information can be found in the presence of specific applications on the two most common smartphone operating systems, Android™ and iOS™. This could help analysts efficiently process a smartphone found during an investigation by having knowledge of the type of information each application contains.

Mobile devices are a commonly encountered piece of evidence in today's investigations. The majority of the operating systems found on smartphones include versions of Android™ and iOS™. 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 which 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 only send 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. These 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™ App Store™ 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 Messenger™ 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 artifacts about content and user information. The types of information searched were: text, audio and photo messages, sender/recipient information, location information, and timestamp information and were present in various forms. Text and photo messages were completely accessible except in Draw Something™. When enabled, all applications with location functions kept accurate tracking records and attached latitude and longitude coordinates to each message. Most applications also kept accurate timestamps. Audio messages were mostly unrecoverable, with Zello™ being the only application that could potentially have kept the original messages on the phone (denoted by a Speex file header). The greatest variability was in the user information kept. Not only did each application retain different information, but it also varied between platforms. The platform that generally kept more information was Android™; the Facebook Messenger™ app for Android™ recorded more information than seemed applicable to the scope of the application storing the phone number and e-mail address for each of the contacts.

Despite some limitations in the methods used, most of the information available from analysis of the messaging applications could be helpful in an investigation. Future research on mobile device applications would expand beyond just messaging applications to other types commonly found on seized phones. Another area of potential research would be to find a method that can be used to play the audio files from Zello™.

Smartphone, Messaging, Applications

 ** Presenting Author*