B12 Forensic Analysis of Data Transience Applications in iOS® and Android™

Cindy Wu, BS, 236 9th Avenue, Huntington, WV 25701; Chris Vance, BS, 1401 Forensic Science Drive, Huntington, WV 25701; Robert J. Boggs, 1401 Forensic Science Drive, Huntington, WV 25701; and Terry Fenger, PhD, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will understand the capabilities of data transience third-party applications and gain insight on potential factors that impact the recoverability of communication artifacts within the iOS® and Android™ device.

This presentation will impact the forensic science community by focusing on the recoverability of data from two popular third-party applications that might be used by criminals to circumvent the law. With mobile phones becoming a common piece of evidence to be investigated, recovered artifacts can potentially connect two individuals who otherwise would not be connected.

The availability of mobile applications has greatly enhanced the capabilities of mobile phone users. Among these applications are data transient apps such as Snapchat (Snapchat, Inc.) and Burner (Ad Hoc Labs, Inc.), which has become prevalent amongst mobile phone consumers. In Snapchat, users are able to share timed content that 'self-destructs' upon reaching the set duration, making it no longer accessible according to the privacy policies. The Burner application allows you to double a personal mobile phone as a burner phone, maintaining the privacy of the user. Upon expiration of those phone numbers, all history and logs associated with them are removed from the device.

Prefacing these applications with the ability of content termination, users may use these applications for the purposes of drug deals, distribution of child pornography, and other criminal activity, expecting any exchanged content to delete upon expiration. In these cases, the recoverability of artifacts becomes essential in investigations which includes, but is not limited to observing the transferred content, timestamps, and associations amongst individuals.

Using a LG® Nexus 4 E960 and a fourth generation Apple® iPod touch, a constant exchange of data was carried out. Physical extractions and file system extractions were conducted using the Celebrite® UFED Touch and the Celebrite® Physical Analyzer in order to study different factors impacting the recoverability in Snapchat and Burner. Snapchat factors focused on message status, time elapsed, and the "clear feed" option while Burner factors focused on time elapsed and expiration method. The differences between the Android device and iOS device proved to be significant.

In a case requiring investigation of Snapchat data, time is of the essence when it comes to the Android due to the server ability to remove received snaps from the given accounts after a certain time has elapsed. The iOS device showed no recoverability of any snaps. Both devices showed logs, which no longer existed upon using the 'clear feed' option. The recovery of Burner application data, however, seems to be dependent upon whether the burner number was expired or manually removed.

This research was supported by Award No. 2010-IJ-CX-K025 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice.

Snapchat, Burner, Mobile

 ** Presenting Author*