C21 Snapchat® Data Recovery Capabilities

Joseph Levi White, MS, US Army Criminal Investigation Laboratory, Digital Evidence-CFI, 4930 N 31st Street, Forest Park, GA 30297; and Christina A. Malone, MSFS, Defense Forensic Science Center, Forest Park, GA 30305*

After attending this presentation, attendees will expand their general understanding of the methods used to recover Snapchat® content from mobile devices, comparing the ability to recover data from both Apple® and Android™ platforms.

This presentation will impact the forensic science community by providing an outline of the current capabilities for the recovery of mobile device Snapchat® data.

Forensic analysis of mobile devices is one of the most quickly evolving areas of Digital and Multimedia Sciences (DMS). With the development and release of mobile devices occurring at a very rapid pace, Digital Forensic Examiners (DFEs) and mobile forensic software companies are faced with the task of determining how to extract and interpret data from the constantly evolving hardware and software of mobile devices. As each new iteration of mobile device and/or mobile device Operating System (OS) is released, it must be determined how to not only extract data from the device, but how to convert the raw data into a format that makes sense to the end user. The use of mobile device applications, or apps, further complicates data analysis of mobile devices. Not only is the base OS of mobile devices under constant development, but individual application developers release and update apps at a surprising pace.

Snapchat® is a mobile device application that allows users to send and receive multimedia content, such as pictures and video, between specified individual contacts. The transferred multimedia is termed a "Snap." Settings within the sender's Snapchat® application determine how long the sent content will be viewable on the receiver's mobile device, from one to ten seconds. After the time limit has expired on the receiver's device, an attempt is made by the Snapchat® software to delete the data. Security features of the Snapchat® application are also designed to prevent users from taking screen captures of received content through other mobile device applications.

A previous presentation on this topic provided an overview of the examination of an Android™-based mobile device submitted for examination to the United States Army Criminal Investigation Laboratory (USACIL) in a case involving the Snapchat® application. Upon completion of the case, it was determined that traditional *mobile device* forensic software packages were at that time unable to extract any deleted Snapchat® pictures from the mobile device; however, traditional *computer forensic* software was successful at recovering the pertinent content. Further research determined that additional functionalities of the Android™ OS, such as facial recognition capabilities, may be responsible for capturing Snapchat® image data independent of the Snapchat® application on the particular device under examination.

This presentation will provide the outcomes of a research study developed as a result of the aforementioned case and the previously conducted research, comparing the ability (or lack thereof) to recover Snapchat® data from both Android™ and Apple® devices. This research takes into account the potential additional functionalities of the Android™ and Apple® operating systems that may circumvent the data deletion design of the Snapchat® application.

The opinions or assertions contained herein are the private views of the author and are not to be construed as official or as reflecting the views of the Department of the Army (DA) or the Department of Defense (DoD). Names of commercial manufacturers or products included are incidental only, and inclusion does not imply endorsement by the authors, the Defense Forensic Science Center (DFSC), the Office of the Provost Marshal General (OPMG), the DA, or the DoD.

Mobile Device, Snapchat®, Data Recovery

*Presenting Author