C8 Case Study: Snapchat™ Picture Recovery From Mobile Device Unallocated Space

Joseph L. White, MS, US Army Criminal Investigation Laboratory, Digital Evidence-CFI, 4930 N 31st Street, Forest Park, GA 30297*

After attending this presentation, attendees will expand their general understanding of the value of utilizing multiple forensic tools and techniques to recover deleted graphical content from mobile devices, specifically those utilizing the Snapchat™ application, which is designed to not retain multimedia content.

This presentation will impact the forensic science community by providing an overview and example of picture recovery procedures utilized when recovering deleted Snapchat™ pictures from mobile devices utilizing multiple forensic analysis tools and techniques.

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, the content is allegedly erased. Security features of the Snapchat™ application are also designed to prevent users from taking screen captures of received content through other mobile device applications.

This presentation will discuss these issues through the results of an 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. The mobile device submitted to the USACIL belonged to an individual accused of soliciting nude photographs from underage girls through the Snapchat™ application. The accused admitted to sending and receiving content through Snapchat™, but insisted the received content did not contain underage nudity. The actual content of the Snapchat™ pictures became vital to the case. Joint Test Action Group (JTAG) data extraction resulted in a copy of the full device memory for analysis. Initial analysis indicated several snaps were received from the user names utilized by the young girls using the Snapchat™ application, but none of the content was viewable using the default settings of traditional mobile forensics software. Multiple forensic software packages were utilized in an attempt to recover the deleted content. Several illicit pictures apparently depicting the underage girls were eventually recovered from the unallocated space of the mobile device and provided for investigative agency review.

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 or the Department of Defense.

Snapchat™, Data Recovery, Digital Evidence

*Presenting Author