C38 A Forensic Comparative Analysis of a Fitness Tracking Application on Mobile Devices Assigned

Christina A. Malone, MSFS, Defense Forensic Science Center, Forest Park, GA 30305; Carl R. Kriigel, MA*, United States Army Criminal Investigation Laboratory, Forest Park, GA 30297; Seth M. Eisenberg, Army Educational Outreach Program, Forest Park, GA 30297; Hillary Lathrop, PhD, Defense Forensic Science Center, Forest Park, GA 30297*

Learning Overview: After attending this presentation, attendees will have an understanding of the current capabilities of extracting the mobile app, STRAVA™, Global Positioning System (GPS) data from mobile devices.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating the benefits and limitations of the extraction techniques used for obtaining GPS data that is recorded through the STRAVA™ app.

This presentation, a research project conducted by the Office of the Chief Scientist (the Research, Development, Testing, and Evaluation arm of the Defense Forensic Science Center), focuses on the benefits and limitations of the extraction techniques used for obtaining GPS data that is recorded through the discussed mobile fitness-tracking app.

Digital Forensic Examiners (DFEs) are responsible for extracting data from various electronic devices and performing analyses on different data types. It is the responsibility of the Digital and Multimedia Evidence (DME) community, including DFEs and researchers, to determine how to extract and interpret the data as well as discover if the data may be a potentially useful source of information. With the expansion of body-worn, fitness-tracker devices, the DME community searches for potentially pertinent data stored within fitness-tracking devices and the companion client devices that store the data.

The example body-worn, fitness-tracking app is used to track athletic activity via satellite navigation. It also works with GPS-enabled watches and head units. Tracking the user's activity may be forensically useful in establishing a suspect's location on a specific date and time. As such, understanding the data and establishing an extraction procedure will enable DFEs to successfully extract physical activity pattern data in cases where a suspect's or victim's location or activity may be important to establish.

Two companion client devices (iPhone® 7 Plus and iPhone® 6) were used for this research based on their availability to the researchers. The premium version of the mobile fitness-tracking app was loaded to the iPhone® 7 Plus. The basic version was loaded to the iPhone® 6. The companion clients were used to record a number of activities (e.g., running, walking, cycling, etc.) to generate data. Generated data included distances, locations, times, and dates to show each user's activity pattern. Recording only occurred when the app was activated. A manual log of each user's activities was kept for post-extraction data comparison. Data was collected over several months to establish the user's activity patterns and to collect various fitness activities. After several months, physical (full, including deleted data) and logical (partial) extractions were conducted on each device using standard computer forensic methods. Results were analyzed for accuracy by comparing the app's data to the user's manual log, as well as comparing the data recovered through the different extraction techniques. Through the evaluation of the app and the data extracted, investigators and examiners will be provided with relevant information on the steps to take when recovering and examining mobile devices and the GPS data that could be associated with a crime.

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 United States Army Criminal Investigation Command, the Office of the Provost Marshal General (OPMG), the DA, or the DoD.

Mobile Device Forensics, Cell Phone Forensics, Digital Extraction