C20 Go-Go Gadget, Smartwatch! An Investigation of Wearable Devices and Their Forensic Value

Nicole R. Odom, BS, Marshall University Forensic Science Center, Huntington, WV 25701; Jesse M. Lindmar, Virginia Department of Forensic Science, Richmond, VA 23219; Joshua L. Brunty, MS*, Marshall University, Huntington, WV 25701; Catherine G. Rushton, EdD, Marshall University Forensic Science Program, Huntington, WV 25701*

Learning Overview: After attending this presentation, attendees will better understand how smartwatch wearable devices with cellular network capability interact with companion mobile phones and where sensitive user data and forensic artifacts are stored, both through utilization as a standalone and as a connected device. This presentation will also provide a methodology for the forensically sound acquisition of data from a standalone wearable device.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by offering more insight into smartwatch wearable forensics, an area of research that is lacking. This presentation will provide an in-depth picture of not only what probative evidence each wearable may contain, but also the process of acquiring this data both directly from the smartwatch or through its companion mobile device, in order that analysts may most efficiently utilize their time and effort during investigations.

Smartwatch wearable devices allow users the ability to walk away from their mobile phone while remaining connected to the digital world. However, this freedom creates additional challenges for digital forensic investigators and analysts tasked with the examination, acquisition, identification, and analysis of probative data. Police departments are now finding that victims, suspects, and witnesses possess up to three smart devices each, as opposed to a singular mobile device.[1] This increase in smart device ownership leads to larger amounts of personal data being created, modified, and accessed. This personal data can be employed to establish causality in civil or criminal investigations. Features like standalone cellular network connectivity, automation through applications, and sensors that may result in persistent and invariable probative data, smartwatch wearable devices have the potential for an even broader scope and depth of information.[2] It has become imperative to understand how these devices operate and the challenges they present in order to provide insight into the implementation of data acquisition methodologies.

Very few studies have been performed on the acquisition of smartwatch data. Those that have been performed have utilized limited methods that are time-consuming, incomplete, or forensically unsound. One study has found that user data such as communication, app information, Personal Information Management (PIM) data, and calendar events are accessible through data acquired from various paired smartwatches. This indicates the forensic value of smartwatches is evident and warrants further exploration.[3] This preliminary research attempts to provide a better understanding of the sensitive user data and forensic artifacts stored directly on these wearable devices. User data observed is from devices connected with a companion mobile phone device or when utilized as a standalone device operating on a cellular network. The overall goal is to increase awareness of the valuable data these wearables are capable of storing and provide a methodology for how to access the data in future investigations.

For this research, the Samsung™ Gear S3 Frontier and Apple Watch® Series 3 were populated and examined. Two separate studies were conducted: data population in a connected state with a companion mobile phone device and data population in a standalone state operating on a cellular network connection. Following completion of both studies, two separate examinations were performed. The first involved the two mobile phone devices synced with the smartwatch wearables (i.e., the Samsung™ Galaxy S8 and Apple® iPhone® 6) to determine if any forensic artifacts were left from its respective smartwatch device and whether user data is stored when acting in a connected or standalone state. The second examination involved the smartwatch wearable devices and any identifiable data they may store that could be considered probative in a forensic investigation.

This presentation will provide the methodology implemented throughout the investigation, including data population and procedures for data acquisition, in an attempt to answer the following questions: what data can be found on the companion mobile phone device?; does the wearable device store data not found on the mobile phone?; and, in the case that a mobile phone is not present during forensic acquisitions, what probative data is available specifically on the wearable device? The results of this work will be presented, as well as general observations made throughout the investigation and any future directions or recommendations.

Reference(s):

1. Police Executive Research Forum. New National Commitment Required: The Changing Nature of Crime and Criminal Investigations. *PERF Reports: Critical Issues in Policing Series*. January 2018, http://www.policeforum.org/assets/ChangingNatureofCrime.pdf.
2. Rand Corporation. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. *RAND Research* Reports, 2015, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.
3. Ibrahim Baggili et al. Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. *2015 10th International Conference on Availability, Reliability and Security*, (August 2015): 303-311, https://doi.org/10.1109/ARES.2015.39.

Digital Forensics, Wearable Devices, Data Recovery