JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, 2019
doi: 10.1111/1556-4029.14109
Available online at: onlinelibrary.wiley.com

PAPER

DIGITAL & MULTIMEDIA SCIENCES

Nicole R. Odom,[1,2] *M.S.F.S. Jesse M. Lindmar,*[2] *B.S.; John Hirt,*[2] *B.S.; and Josh Brunty,*[1] *M.S.*

Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices[*,†]

ABSTRACT: Wearable devices allow users the ability to leave mobile phones behind while remaining connected to the digital world; however, this creates challenges in the examination, acquisition, identification, and analysis of probative data. This preliminary research aims to provide an enhanced understanding of where sensitive user data and forensic artifacts are stored on smartwatch wearable devices, both through utilization as a connected and standalone device. It also provides a methodology for the forensically sound acquisition of data from a standalone smartwatch wearable device. The results identify significant amounts of data on the Samsung™ Gear S3 Frontier, greater than that stored on the companion mobile phone. An Apple Watch® Series 3 manual examination method which produces native screenshots was identified; however, the companion mobile phone was found to store the greatest amount of data. As a result of this research, a data extraction tool for the Samsung™ Gear S3 Frontier was created.

KEYWORDS: forensic science, digital forensics, mobile forensics, smartwatch wearable devices, internet of things, forensic artifacts, data recovery

From the panels of Dick Tracy to cartoon episodes of Inspector Gadget, innovative writers have filled the minds of adolescents and adults alike with dreams of a connected future through wearable devices; after all these years, science fiction has become a reality. Although smartwatches have been in production for the past decade, the most recent releases have the capability of operating as standalone wearable devices, much like those seen in the cartoons. Being given the freedom to leave smartphones behind and remain connected to the digital world offers users the hands-free capability that has always been desired in a smart device, making it no wonder that smartwatch wearable devices are quickly becoming popular on the market. With manufacturers of mobile phone devices exploring their own versions of smartwatch wearable devices capable of connecting to major platforms like iOS and Android, the appeal among all users has risen. In fact, the International Data Corporation's (IDC) Worldwide Quarterly Device Tracker states that the overall wearables market is expected to grow from 113.2 million shipments in 2017 to 223.3 million in 2021, with anticipated smartwatch units equaling up to 71.5 million (1). Although this increased use of smartwatch wearable devices may lead to more convenience and efficiency for end-users, it also presents many new obstacles for forensic digital examiners to overcome as wearable use also becomes more prevalent in civil and criminal cases.

Police departments are now finding that victims tend to own up to three smart devices, as do suspects and witnesses, leading to greater amounts of personally sensitive probative data being created, modified, and accessed (2). A large part of this is due to automation, which may produce data that are persistent and invariable, allowing wearables to provide investigators the means to establish causation for investigations (3). Approximately 80% or more of current court cases contain some type of digital evidence, including those where smartwatch wearable data have been used to uphold or refute witness statements (4). In addition to these investigational advances, smartwatch wearable devices are also capable of interacting with multiple media sources through various modes of connection, making them big players in the Internet of Things (IoT) arena (2,5). Therefore, the collection and subsequent analysis of these devices is becoming increasingly more important, as is the study of their computing capabilities and modes of connection (6).

The IoT is currently of great interest for digital forensic investigators and researchers, as the networks created by these

[1] Marshall University Forensic Science Center, Huntington, WV 25705, USA.

[2] Virginia Department of Forensic Science, Digital & Multimedia Evidence Section, Richmond, VA 23219, USA.

Corresponding author: Nicole R. Odom B.S. E-mail: nicole.odom@dfs.virginia.gov

[*] Presented at the 71st Annual Scientific Meeting of the American Academy of Forensic Sciences, February 18–23, 2019, in Baltimore, MD.

[†] This paper is the result of an internship in the Digital & Multimedia Evidence Section of the Department of Forensic Science-Central Laboratory (DFS). At the time the research was conducted, the intern was a student at Marshall University and had no affiliation with the DFS; therefore, any conclusions are based on examination findings of the student and do not reflect upon the analysts of the DFS. This research is focused on two specific wearable devices and may be subject to change due to software updates or newer models. Given the wide range of compatibility of these devices, it is possible that other makes and models of companion mobile phones may produce different results than those found in this specific case. Dates and times associated with the data presented are dependent upon the settings of the device or data network and may not necessarily reflect the actual date and time of the recorded event. Due to the nature of electronically stored information, all data related to the research may not have been identified.

Received 23 Mar. 2019; and in revised form 19 May 2019; accepted 21 May 2019.

interconnected smart devices are huge repositories of information that produce digital evidence of a much broader scope and depth than physical evidence (7). Since smartwatch wearable devices essentially function as mini-computers, with communication functionalities as well as a variety of physiological and mechanical sensors, their storage capabilities warrant further exploration (8). In previous work, it has been shown that data such as messages, health and fitness information, e-mails, contacts, events, and notifications are accessible from datasets acquired from various paired smartwatch wearable devices, thus the forensic value from these devices is worthy of investigation (9). This work is imperative as it attempts to solve two key issues in digital forensics: the limited research performed on smartwatch wearable devices and the heavy workload that digital forensic investigators face on a daily basis. Very few studies have been performed on the acquisition of smartwatch wearable data, and those that have been performed utilized limited methods which are both time-consuming and either incomplete or forensically unsound (6,9). Most studies performed a manual review of a device's electronically stored information utilizing its native interface, restricting acquisition to what the examiner can see on the screen. One study performed a physical extraction, allowing for the information to be read from the flash memory of the device and deleted data to be accessed; however, rooting the device prior to physical extraction was required, which is often considered a less forensically sound approach due to system data and possible user data modifications (3,10). Therefore, a forensically sound methodology for the advanced acquisition of data directly from a smartwatch wearable device is needed. In addition, given the current backlogs resulting from the time required to parse through data from multiple devices in combination with the rate at which technology is updating and evolving, it has become crucial to triage items for examination within a case. In order to make these prioritizing decisions, it is necessary to understand what potential probative evidence each device contains so investigators can most efficiently use their time and effort (3).

This preliminary work takes a closer look at two separate smartwatch wearable devices, the Samsung™ Gear S3 Frontier and the Apple Watch® Series 3, in order to identify not only the significant user data and forensic artifacts each may contain, but also the process of acquiring this data as a standalone or connected device. These devices were populated and examined through two separate studies: data population in connected mode with a companion mobile phone device and data population in standalone mode operating on a cellular network connection. Following the completion of both studies, two separate examinations were performed. The first involved the two companion mobile phone devices (i.e., the Samsung™ Galaxy S8 and Apple® iPhone® 6), looking for any forensic artifacts left from its respective smartwatch wearable device, as well as possible user data stored when acting as a connected or standalone device. The second examination looked directly at the smartwatch wearable devices to determine whether any data were present that were not synced to the companion mobile phone device, as well as what probative data were available in the event that a mobile phone was not present during an acquisition. A forensically sound methodology for the acquisition of data from a standalone smartwatch wearable device has been outlined for future advanced extraction purposes, and a command-line-based data extraction tool for the Samsung™ Gear S3 Frontier has been created for use by law enforcement and analysts in the field.

Materials & Methodology

Testing Apparatus

For this research, two smartwatch wearable devices were forensically analyzed with respect to sensitive user data and forensic artifacts stored when acting as a standalone or connected device. The devices, Samsung™ Gear S3 Frontier (Model SM-R765A, Tizen v.3.0.0.2) and Apple Watch® Series 3 (Model A1860, iOS v.4.0.1), were chosen based on their market popularity and new cellular capabilities that have yet to be explored forensically. As per compatibility guidelines for each, these smartwatch wearable devices were connected with the Samsung™ Galaxy S8 (Model SM-G950U, Android v.7.0; Release Date June 13, 2017) and Apple® iPhone® 6 (Model MG492J/A, iOS v.11.3.1; Release Date April 24, 2018), respectively. At the time of research, the Samsung™ Galaxy S8 was chosen as the companion device for this study as it appeared to be a popular model commonly utilized and paired with the Samsung™ Gear S3 Frontier. Although it is recognized that an earlier version of Android may have allowed for increased acquisition capabilities among commercial tools, the decision was made to research a configuration that would most likely be encountered in the field.

The newest models of smartwatch wearable devices, including both of those tested in this research, are capable of utilizing three different types of connection: Bluetooth, Wi-Fi, and Cellular. These types of connections are employed differently based upon the mode in which the smartwatch wearable device is functioning. There are two modes in which the most recent smartwatch wearable devices can operate: connected and standalone. In the connected mode under default settings, Bluetooth connection for short-range activity has main priority, followed by Wi-Fi connectivity for longer range activity. Through these connections, the smartwatch wearable device acts as an extension of the paired mobile phone device, communicating and interacting directly through the phone (Fig. 1, Connected Mode).

Through this research, standalone mode for the Samsung™ Gear S3 Frontier was found to be a bit more complex than the connected mode, as it consists of three different states: Connected Remotely, Standalone Without Relay, and Standalone ((11)). The latter state is when the smartwatch wearable device operates entirely on its own, independent of a mobile phone; this state was not utilized for this research, as it appears to be severely limited in functionality and the least likely state to be encountered in the field. The former two states were utilized interchangeably during the standalone study of this research depending on whether the smartwatch wearable device was able to access a data connection. In standalone mode with the Connected Remotely state, cellular connection has main priority unless the user enables Wi-Fi, in which case the smartwatch wearable device will connect to previously trusted Wi-Fi networks; Wi-Fi was not enabled for the standalone study. In the Standalone Without Relay state, the smartwatch wearable device does not have an active wireless data connection, but is still able to forward calls and messages from the companion mobile phone (Fig. 1, Standalone Mode). The Apple Watch® Series 3 was slightly different than the Samsung™ Gear S3 Frontier, as it simply displays that it is connected to a cellular network when operating in the standalone mode; however, for both smartwatch wearable devices, standalone mode is enacted either through toggling by the user or upon roaming out-of-range of both Bluetooth and Wi-Fi connectivity. Through this mode, the smartwatch wearable device is the sole communicator,

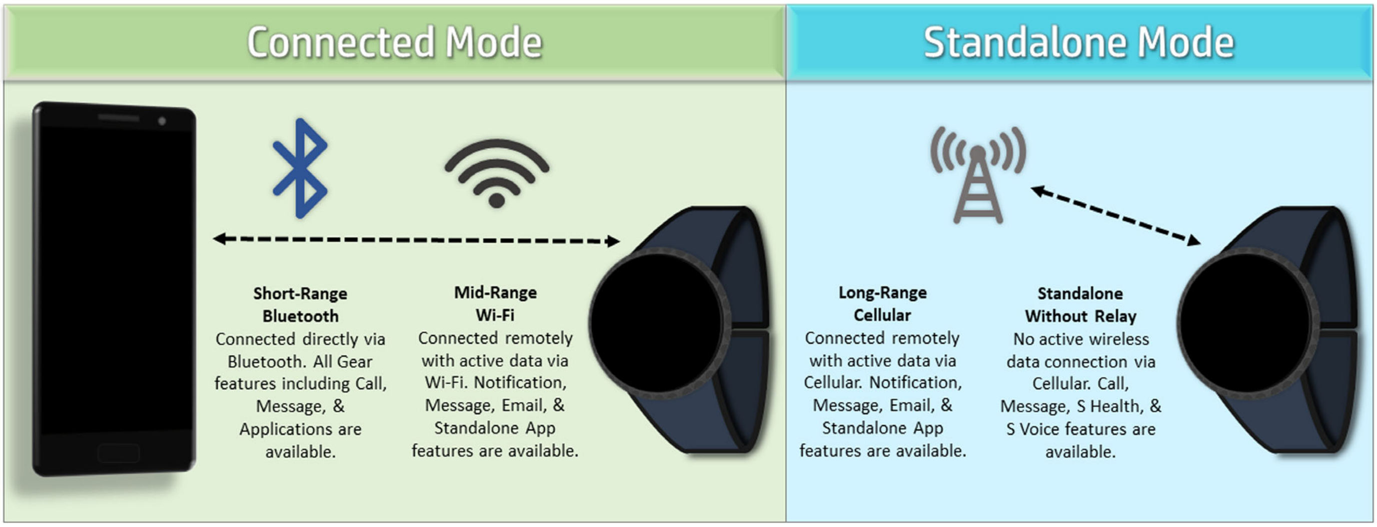

Connected Mode
Standalone Mode
Short-Range Bluetooth
Connected directly via Bluetooth. All Gear features including Call, Message, & Applications are available.
Mid-Range Wi-Fi
Connected remotely with active data via Wi-Fi. Notification, Message, Email, & Standalone App features are available.
Long-Range Cellular
Connected remotely with active data via Cellular. Notification, Message, Email, & Standalone App features are available.
Standalone Without Relay
No active wireless data connection via Cellular. Call, Message, S Health, & S Voice features are available.

FIG. 1—*Modes of operation & connectivity of the Samsung™ Gear S3 Frontier.*

interacting without the paired phone through the cellular network; however, in order to permit maximum functionality, the companion mobile phone devices must be left in the powered-on state as per each manufacturer's directions.

Experimental Setup

Two separate studies were performed for this research. The first study consisted of data population of each smartwatch wearable device in the connected mode, while the second study consisted of data population of each smartwatch wearable device in the standalone mode. Guidelines recommended by the National Institute of Standards and Technology (NIST) were utilized for data population (12). Each of these setups has been explained in further detail below, with Table 1 documenting each type of populated data and any loss of functionality for each smartwatch wearable device within the chosen data categories.

Study One—For this study, the Samsung™ Gear S3 Frontier was connected with the Samsung™ Galaxy S8, and the Apple Watch® Series 3 was connected with the Apple® iPhone® 6. Data for several areas of interest were populated, including Contacts, Calendar Events, Alarms, Reminders, Notes, Passwords, Email, Multimedia, Call Logs, Short Message Service (SMS)/ Multimedia Message Service (MMS), Messengers including Facebook Messenger (Android v.169.0/iOS v.167.0), Kik (Android v.13.3.1/iOS v.13.3.0), and WhatsApp (Android v.2.18.177/iOS v.2.18.61), Location including Google/Apple® Maps and Waze (Android v.4.39.0.4/iOS v.4.39.2), Web Browser Activity, Hey Google/Siri Commands, Fitness including Samsung™ Health and Apple® Activity/Health, and 3rd party applications including Facebook (Android v.175.0/iOS v.175.0) and Snapchat (Android v.10.34.0.0/iOS v.10.33.1). Within each of these categories, variable types of data were populated, including sent/received/deleted messages, outgoing/incoming/ missed calls and voicemails, Internet bookmarks, picture/video/ audio multimedia, daily and workout stats for fitness, and various activities for Facebook, including a profile picture upload, status update, life event post, and a video download. Connected data events originated both from the smartphone and smartwatch devices when permitted (e.g., two different calendar events were made while in the connected mode, one on the companion mobile phone and one on the smartwatch wearable device) in order to test the impact of data provenance. All populated data were recorded in detail, including content, date, and time stamps, and any additional settings made when populated for increased accuracy and identification in examination.

Study Two—For this study, the Samsung™ Galaxy S8 and the Apple® iPhone® 6 were moved outside of the Bluetooth and Wi-Fi ranges for the Samsung™ Gear S3 Frontier and the Apple Watch® Series 3 in order to enable independent operation of the smartwatch wearable devices, otherwise known as standalone mode. The mobile phone devices were left in the powered-on state to permit maximum functionality of both wearable devices as per each manufacturer's directions. This was also done to simulate the activity of an average end-user, given that most users utilizing their smartwatch wearable device in its standalone mode would simply leave their phone at home in the powered-on state. The Samsung™ Gear S3 Frontier and the Apple Watch® Series 3 were then populated with data similar to Study One where capability existed. Again, all populated data was recorded in great detail, including content, date, and time stamps, and any additional settings made when populated for increased accuracy and identification as standalone versus connected data in examination, including notes when functionality or similar additional settings did not exist. Following completion of data population, both smartwatch wearable devices and their respective companion mobile phones were powered off and kept apart throughout examination and acquisition to prevent sync or cross-talk events.

Acquisition Methods

Four separate acquisitions were performed for this work, following guidelines recommended by NIST for the extraction of forensic data (13). Both of the smartwatch wearable devices were studied and evaluated for their connection capabilities, and approaches for the acquisition of data directly from each standalone smartwatch wearable device were designed.

Samsung™ Galaxy S8—Forensic extractions of the Galaxy S8 were acquired through Cellebrite's UFED 4PC (v.7.5.0.845). A physical extraction was attempted using the Advanced Android Debugging Bridge (ADB) option; however, it yielded a security

TABLE 1—*Data population for connected study one & standalone study two*

Data Category	Content	Study One: Connected Origin	Study Two: Standalone Origin
Contacts	Add Contact	P, W^{-A}	W^{-A}
Calendar Events	Add Calendar Event	P, W	W
Alarms	Set Alarm	P, W	W
Reminders	Create Reminder	P, W	W
Notes	Create Note	P, W$^{-A,-G}$	W$^{-A,-G}$
Keychains	Lock Device	P, W	W
Email	Send Message	P, W	W
	Receive Message		
	Delete Message		
	Create Draft Message	P, W$^{-A,-G}$	W$^{-A,-G}$
Multimedia	Take Picture	P, W$^{-A,-G}$	W$^{-A,-G}$
	Record Video		
	Record Audio	P, W	W
Call Logs	Perform Outgoing Call	P, W	W
	Receive Incoming Call		
	Perform Missed Call		
SMS	Send Message	P, W	W
MMS	Receive Message		
	Delete Message		
Facebook Messenger	Send Message	P, W	W
Kik	Receive Message		
Messenger	Delete Message	P, W$^{-A,-G}$	W$^{-A,-G}$
WhatsApp Messenger			
Google/Apple® Maps	Perform Navigation Event	P, W^{-G}	W^{-G}
Waze			
Hey Google/Hey Siri Command	Ask Question	P, W	W
Browser Activity	Perform Web Search	P, W	W
	Create Bookmark		
Facebook	Add Profile Picture	P, W$^{-A,-G}$	W$^{-A,-G}$
	Create Status Update		
	Add Life Event		
Snapchat	Send Message	P, W$^{-A,-G}$	W$^{-A,-G}$
	Receive Message		
Samsung™ Health	Record Daily Health Stats	P, W	W
	Record Workout		

P: Data originated from companion mobile phone device.

W: Data originated from smartwatch wearable device.

-A: Apple Watch® Series 3 has a lack of functionality and is not capable of performing this data function.

-G: Samsung™ Gear S3 Frontier has a lack of functionality and is not capable of performing this data function.

patch level limitation error for this extraction type that could not be bypassed. Prior to this work, the researchers were unaware of the severe limitations in data acquisition possibilities that this mobile device currently presents to analysts. Through this research and further communication with other active analysts in the field, it was identified that acquisition is limited in the way of a physical extraction for the Galaxy S8 as it would need to be rooted to circumvent this type of error. Since rooting of a device elevates the user to the highest level of privileges and allows for modification of the software on that device, it is not a forensically sound or preferred method; however, even if it was a desirable method for acquisition, it would not be a possibility for this device due to its internal chipset. This specific mobile phone device contained a Snapdragon processor from the United States, which has a locked bootloader, preventing rooting of the device even with the installation of a custom Team Win Recovery Project (TWRP) bootloader. In-System Programming (ISP) and non-heat chip-off techniques were investigated for this device, but given the lack of known or available pinouts, the Universal Flash Storage (UFS)-memory chip, and the difficulties related to encryption, these techniques did not seem feasible nor recommended for this device at this time. Thus, all other possible extractions for this device were performed, including an Android Backup, Partial File System extraction, and Logical extraction. For each, the device was placed into Airplane mode with developer options made accessible, allowing the "USB debugging," "Stay awake," and "Media Transfer Protocol (MTP)" settings to be enabled. These images were analyzed using Cellebrite's UFED Physical Analyzer (v.7.6.0.83). SHA256 hash values were calculated and verified for all extractions.

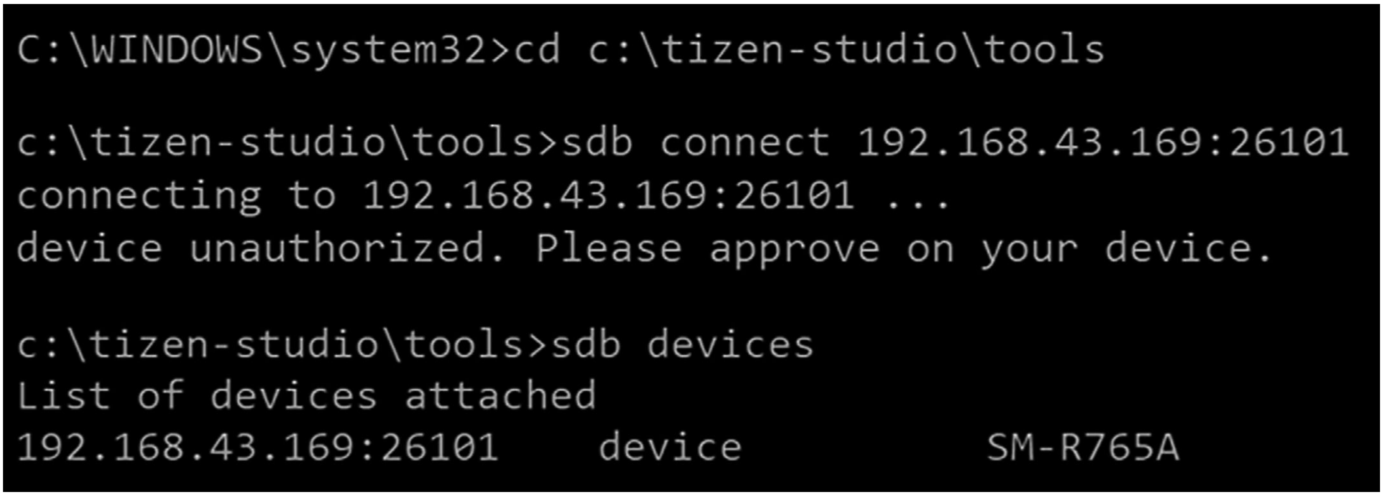
Apple® iPhone® 6—A Full Filesystem extraction of the iPhone® 6 was able to be acquired utilizing GrayShift's GrayKey (OS v1.3.30, App Bundle v1.9.10). A Physical extraction utilizing Cellebrite's UFED Physical Analyzer (v.7.4.0.103, iOS Support Package v.5.19) was not supported for the iPhone® 6; however, an Advanced Logical extraction was made for comparative purposes with the GrayKey extraction. For the Advanced Logical extraction, "Method 1" was chosen for the most inclusive data extraction. The GrayKey extraction was imported for analysis into Cellebrite's UFED Physical Analyzer utilizing the "Advanced Open" option and "iPhoneFS" chain. The Advanced Logical extraction was also analyzed using this software. SHA256 hash values were calculated and verified for both extractions.

Samsung™ Gear S3 Frontier—The Gear S3 Frontier smartwatch wearable device provides no physical connection ports, as it uses wireless connection for charging purposes; therefore, extracting any sensitive user data and forensically relevant artifacts directly from the device was slightly more difficult. The methodology used in this research for data extraction is outlined below.

Through the Tizen Studio (v.2.4, Release Date Apr 25, 2018) Software Development Kit (SDK), it is possible to connect a Gear S3 Frontier to a host PC via utilization of the Smart Development Bridge (SDB) device management tool. This process requires a Wireless Access Point (WAP), which acts as a USB-connection between the device and the host PC. In order to prevent any interference, Bluetooth connectivity on the Gear S3 Frontier was disabled. To allow connection, "Debugging mode" and Wi-Fi of the Gear S3 Frontier were enabled through the Settings/Connections menu, and the device was rebooted to initialize. At this point, the Gear S3 Frontier and the host PC were connected to the same WAP and an IP address received from the WAP for the smartwatch wearable device via Dynamic Host Configuration Protocol (DHCP) was noted. A terminal in the host PC was utilized to connect the previously assigned IP address to the Gear S3 Frontier port of 26101 via <sdb connect>, followed by <sdb devices> to verify the connection (Fig. 2).

The <sdb shell> command was run to activate a remote shell interactively, followed by <sdb shell ls -lah> to display the directory contents in a long list format, including hidden files (Fig. 3). Upon review of the device's directory and exit of the remote shell, <sdb pull> was run on the root-level directories in order to recursively copy the entire directory structure from the remote Gear S3 Frontier to the local host PC, resulting in a filesystem extraction. This filesystem extraction was brought into X-Ways Forensics (v.19.6 SR-4 x64), and each of the partitions of the smartwatch wearable device was labeled and examined for their content. This filesystem extraction was also brought into Cellebrite's UFED Physical Analyzer (v.7.6.0.83) for comparative purposes.

Apple Watch® Series 3—The Series 3 smartwatch wearable device also uses a wireless connection for charging purposes;

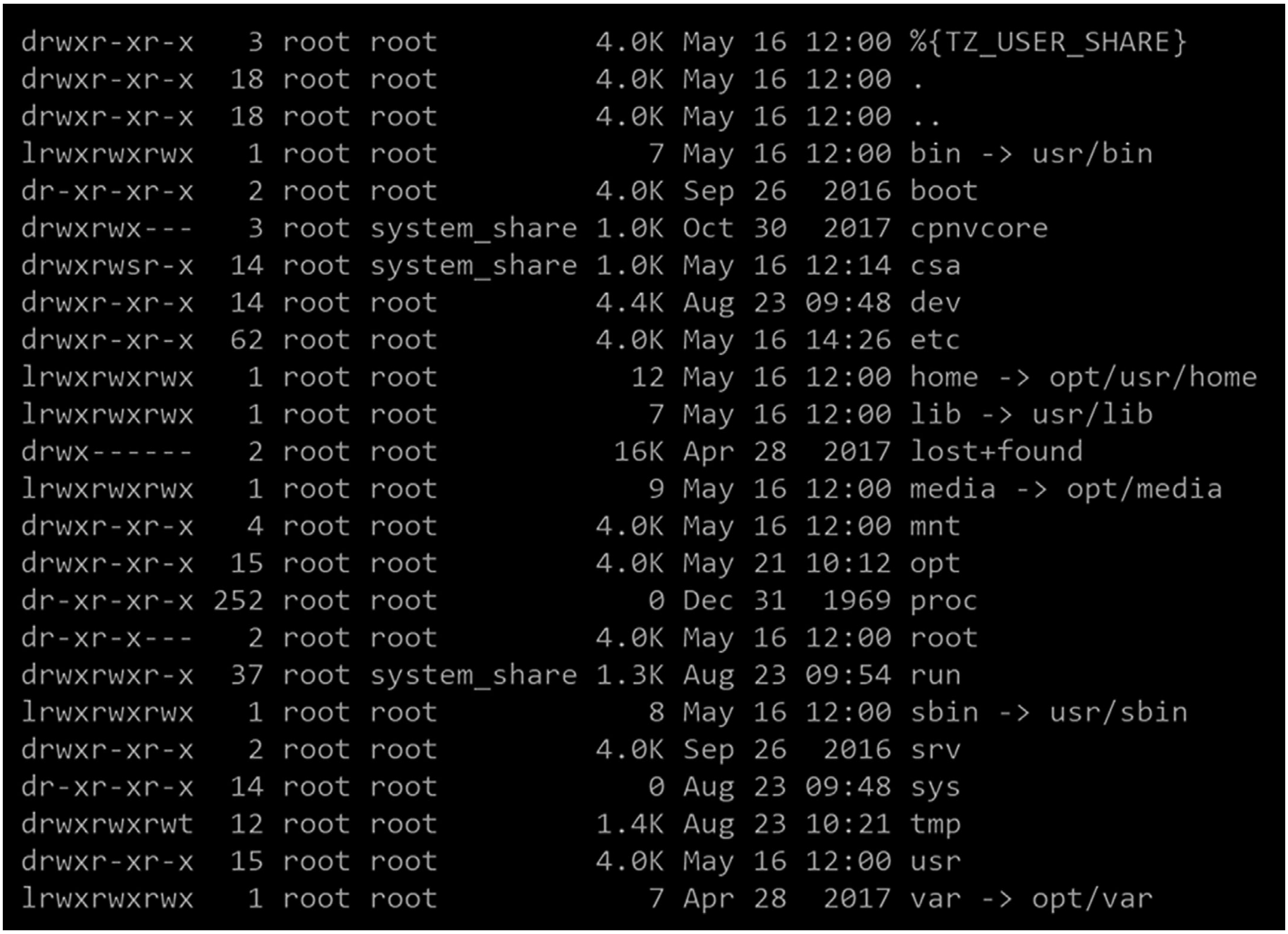


```
C:\WINDOWS\system32>cd c:\tizen-studio\tools

c:\tizen-studio\tools>sdb connect 192.168.43.169:26101
connecting to 192.168.43.169:26101 ...
device unauthorized. Please approve on your device.

c:\tizen-studio\tools>sdb devices
List of devices attached
192.168.43.169:26101    device          SM-R765A
```

FIG. 2—*Host PC connection to the Samsung™ Gear S3 Frontier in terminal.*



```
drwxr-xr-x   3 root root         4.0K May 16 12:00 %{TZ_USER_SHARE}
drwxr-xr-x  18 root root         4.0K May 16 12:00 .
drwxr-xr-x  18 root root         4.0K May 16 12:00 ..
lrwxrwxrwx   1 root root            7 May 16 12:00 bin -> usr/bin
dr-xr-xr-x   2 root root         4.0K Sep 26  2016 boot
drwxrwx---   3 root system_share 1.0K Oct 30  2017 cpnvcore
drwxrwsr-x  14 root system_share 1.0K May 16 12:14 csa
drwxr-xr-x  14 root root         4.4K Aug 23 09:48 dev
drwxr-xr-x  62 root root         4.0K May 16 14:26 etc
lrwxrwxrwx   1 root root           12 May 16 12:00 home -> opt/usr/home
lrwxrwxrwx   1 root root            7 May 16 12:00 lib -> usr/lib
drwx------   2 root root          16K Apr 28  2017 lost+found
lrwxrwxrwx   1 root root            9 May 16 12:00 media -> opt/media
drwxr-xr-x   4 root root         4.0K May 16 12:00 mnt
drwxr-xr-x  15 root root         4.0K May 21 10:12 opt
dr-xr-xr-x 252 root root            0 Dec 31  1969 proc
dr-xr-x---   2 root root         4.0K May 16 12:00 root
drwxrwxr-x  37 root system_share 1.3K Aug 23 09:54 run
lrwxrwxrwx   1 root root            8 May 16 12:00 sbin -> usr/sbin
drwxr-xr-x   2 root root         4.0K Sep 26  2016 srv
dr-xr-xr-x  14 root root            0 Aug 23 09:48 sys
drwxrwxrwt  12 root root         1.4K Aug 23 10:21 tmp
drwxr-xr-x  15 root root         4.0K May 16 12:00 usr
lrwxrwxrwx   1 root root            7 Apr 28  2017 var -> opt/var
```

FIG. 3—*The Samsung™ Gear S3 Frontier root directory in long list format.*

however, a diagnostic port exists for flashing firmware onto the device via connection to a proprietary Apple® cable and has yet to be explored for its ability to pull data from the device. Since research is limited in regard to acquisition from an Apple Watch®, the various methods attempted throughout this research will be discussed below, including those in which data extraction was not possible. Each method was explored for its capability to establish a point of connection between the Series 3 and a host

PC, which could be utilized for communication with the smartwatch wearable device.

Method One attempted to utilize the diagnostic port of the Apple Watch® Series 3 with a lightning-to-USB cable (Fig. 4). The wristband of the Series 3 was first removed, allowing access to the hidden diagnostic port. The door covering the diagnostic port was removed with the use of a needle, revealing five pins for connection to a proprietary Apple® cable for firmware flashing. The lightning-to-USB cable utilized consisted of a detachable lightning tip, which when removed revealed five pins for charging connection to a tablet, arranged in a similar layout to that of the diagnostic port. Since the frame of the cable was too bulky and the five pins were not aligned properly for direct connection to the smartwatch wearable device's diagnostic port, the frame was deconstructed through use of a cutoff wheel to allow access to the five respective soldering points. Short connecting wires were soldered to the exposed points and attached to a Chip On Data Extraction Device (CODED) by Forensic Navigation, which allows for ISP and Embedded MultiMediaCard (eMMC) chip reading without direct soldering. The needle tips of the CODED arms were inserted into the diagnostic port and the USB tip was connected to the port of the host PC. The Series 3 was powered on to check whether it was recognized by the PC; it was not. The Series 3 was then powered off and iTunes® was opened on the PC. The smartwatch wearable device was then booted into "Device Firmware Upgrade (DFU)" mode via holding down both the Side button and Digital Crown for ten seconds, followed by the release of the side button alone; still, no device was recognized by the PC.

Method Two also attempted to utilize the diagnostic port of the Apple Watch® Series 3 with a cable of similar build to the proprietary Apple® cable, the iBUS S2 (Fig. 5). The stabilization bar, included with this cable, was slid into the opening for the smartwatch wearable device's wristband and the opening was lined up with the diagnostic port. The iBUS S2 cable was then connected to the smartwatch wearable device through this opening and fastened with a simple rubber band to tighten the connection, and the USB tip of this cable was connected to the port of the host PC. Upon powering up the Series 3, the computer immediately began installing drivers for an Apple® device and the iTunes® application recognized the Apple Watch® by name; however, iTunes® offered no backup option for the smartwatch wearable device, only a few troubleshooting options for problematic devices. By running a <ioreg -p IOUSB -w0 -l> command on the host PC, a high-speed USB device was identified as "Watch," accompanied by a wide range of information pertaining to the device, including a port number and the serial number of the USB. Efforts to utilize this information for communication with the smartwatch wearable device through this cable, including attempts to mount the device for exploration, were unsuccessful.

Method Three attempted to utilize a wireless connection in similar fashion to the extraction method of the Samsung™ Gear S3 Frontier. Through use of a common WAP and the IP address of the smartwatch wearable device received from the WAP via DHCP, a Secure Shell (SSH) connection was attempted. It is important to note that this method requires knowledge of the username of the smartwatch wearable device. This method proved unsuccessful, as each attempt to connect to the device via <sshusername@ip.addr> resulted in either a "Connection timed out" or "Connection refused" response.

Method Four utilized Xcode® (v.10.1), a suite of software development tools that enable developers to build applications for Apple® devices, including the Apple Watch® Series 3. Through this software, it is possible to interact with both a USB-connected physical smartwatch wearable device and a

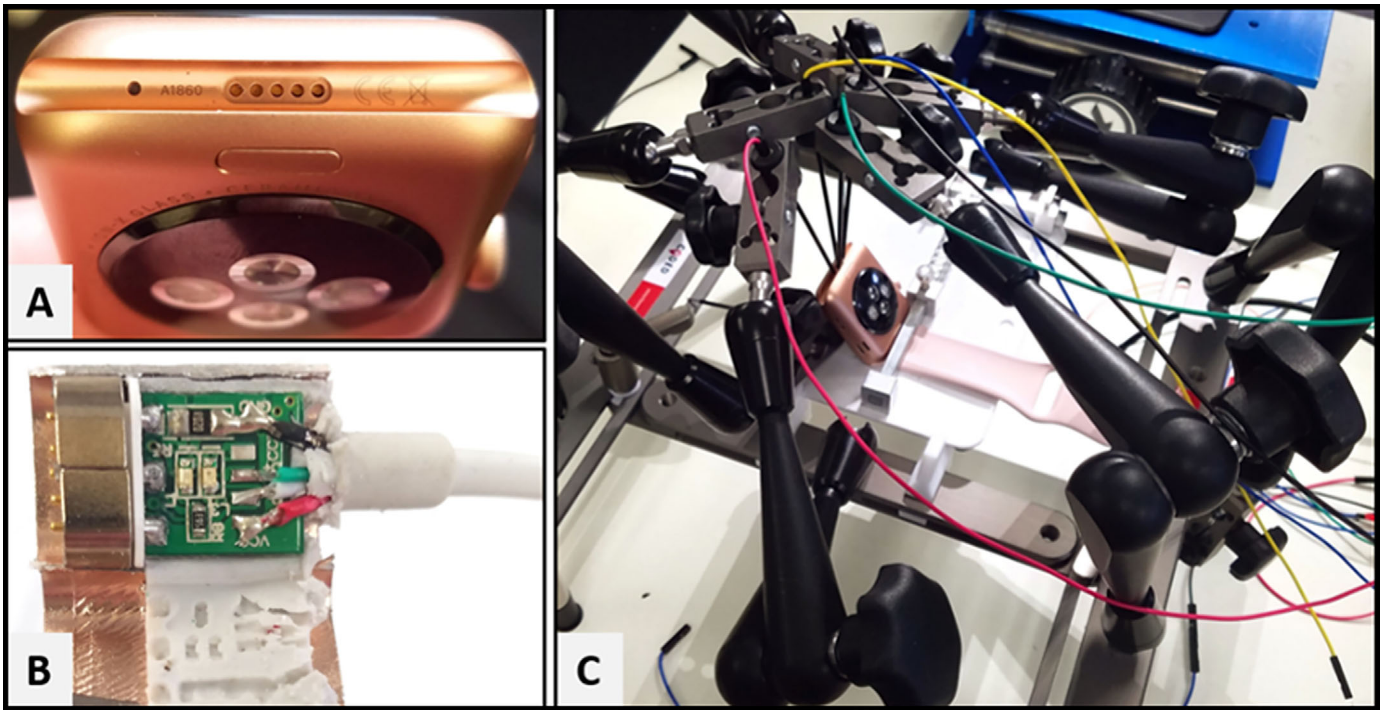
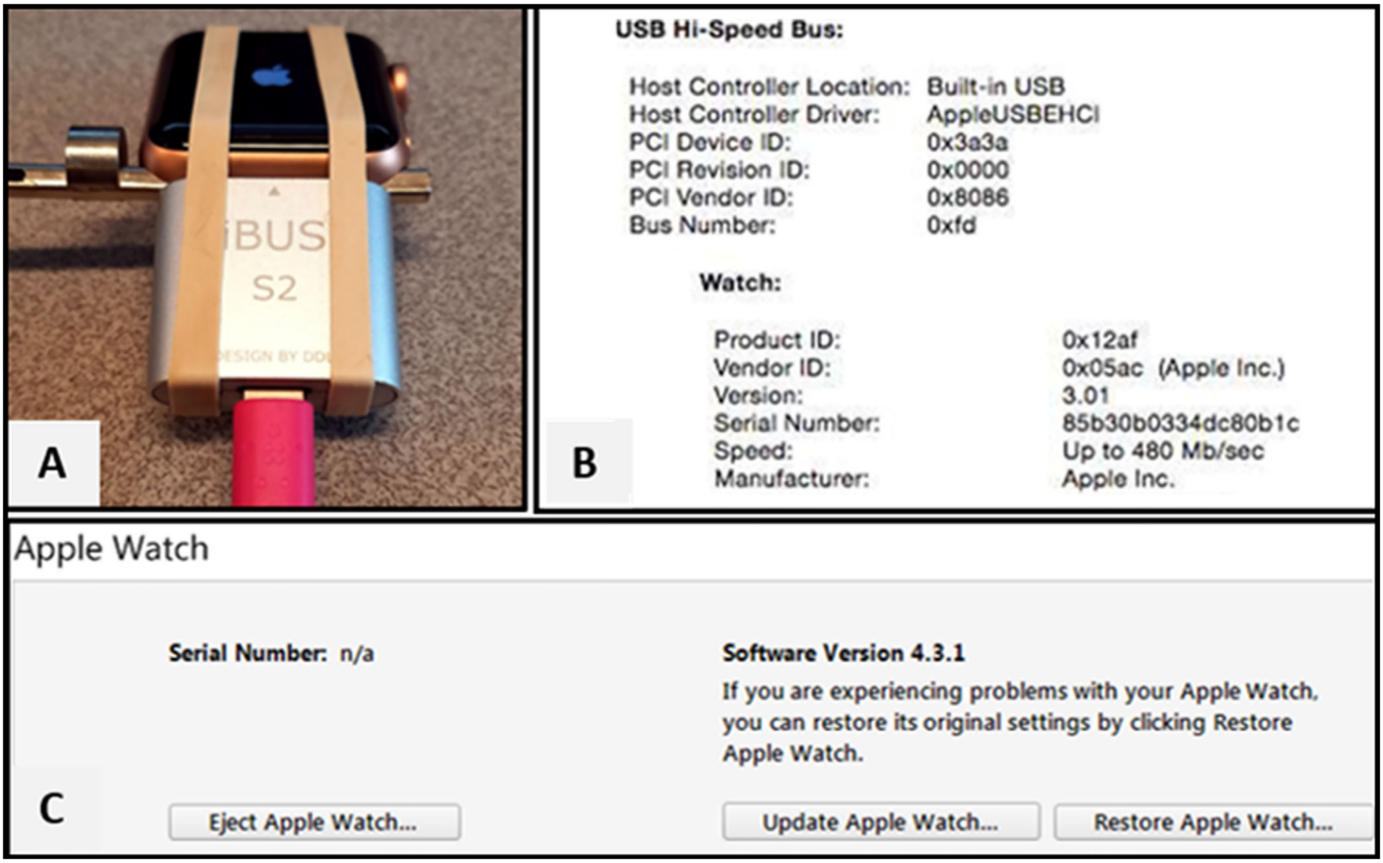


FIG. 4—*Utilizing a lightning-to-USB cable for extraction of data from the Apple Watch® Series 3. (a) Diagnostic port of the Series 3 smartwatch wearable device. (b) Deconstructed frame of the lightning-to-USB cable, revealing soldering points corresponding to pins. (c) CODED arms inserted into the diagnostic port of the Series 3.*



```
USB Hi-Speed Bus:

  Host Controller Location:  Built-in USB
  Host Controller Driver:    AppleUSBEHCI
  PCI Device ID:             0x3a3a
  PCI Revision ID:           0x0000
  PCI Vendor ID:             0x8086
  Bus Number:                0xfd

      Watch:

        Product ID:                 0x12af
        Vendor ID:                  0x05ac  (Apple Inc.)
        Version:                    3.01
        Serial Number:              85b30b0334dc80b1c
        Speed:                      Up to 480 Mb/sec
        Manufacturer:               Apple Inc.
```

Apple Watch

Serial Number: n/a

Software Version 4.3.1

If you are experiencing problems with your Apple Watch, you can restore its original settings by clicking Restore Apple Watch.

FIG. 5—*Utilizing the iBUS S2 cable for extraction of data from the Apple Watch® Series 3. (a) iBUS S2 cable attached to the diagnostic port of the Series 3 smartwatch wearable device. (b) USB Hi-Speed Bus identified as "Watch" with an additional list of information. (c) iTunes® recognizing the attached device as an Apple Watch®.*

smartwatch wearable simulator to directly test the functionality of a designed application; therefore, Method Four sought to determine whether it was possible to utilize this capability for the purposes of interacting with the Apple Watch® Series 3. Upon plugging in the Series 3 to the computer via the previously mentioned iBUS S2 cable and opening the Window/Devices & Simulators tab, the smartwatch wearable device was recognized by its user-assigned name. This window gave a list of useful information, including the watchOS version, serial number, model number, capacity, current storage, and an identifying string for the smartwatch wearable device. There were also three different options available for interaction with the Series 3, including the ability to take a screenshot of the native watch screen, view the device logs, and open the console for this smartwatch wearable device (Fig. 6). Although the latter two options appeared useful, upon further inspection it became apparent that both the device logs and console were only maintained from the moment of USB-connection to the computer. However, the screenshot option could prove convenient and greatly improve efficiency of manually documenting displayed content. Although Xcode® offers a command-line utility, "simctl," for interacting with smartwatch wearable simulators similar to ADB for Android, it would seem that this utility is unable to be applied to a physical device. The option of attempting to create a backup from the physical device to a simulated iPhone® or Apple Watch® was also explored, but this capability does not appear to be possible at this time.

Results

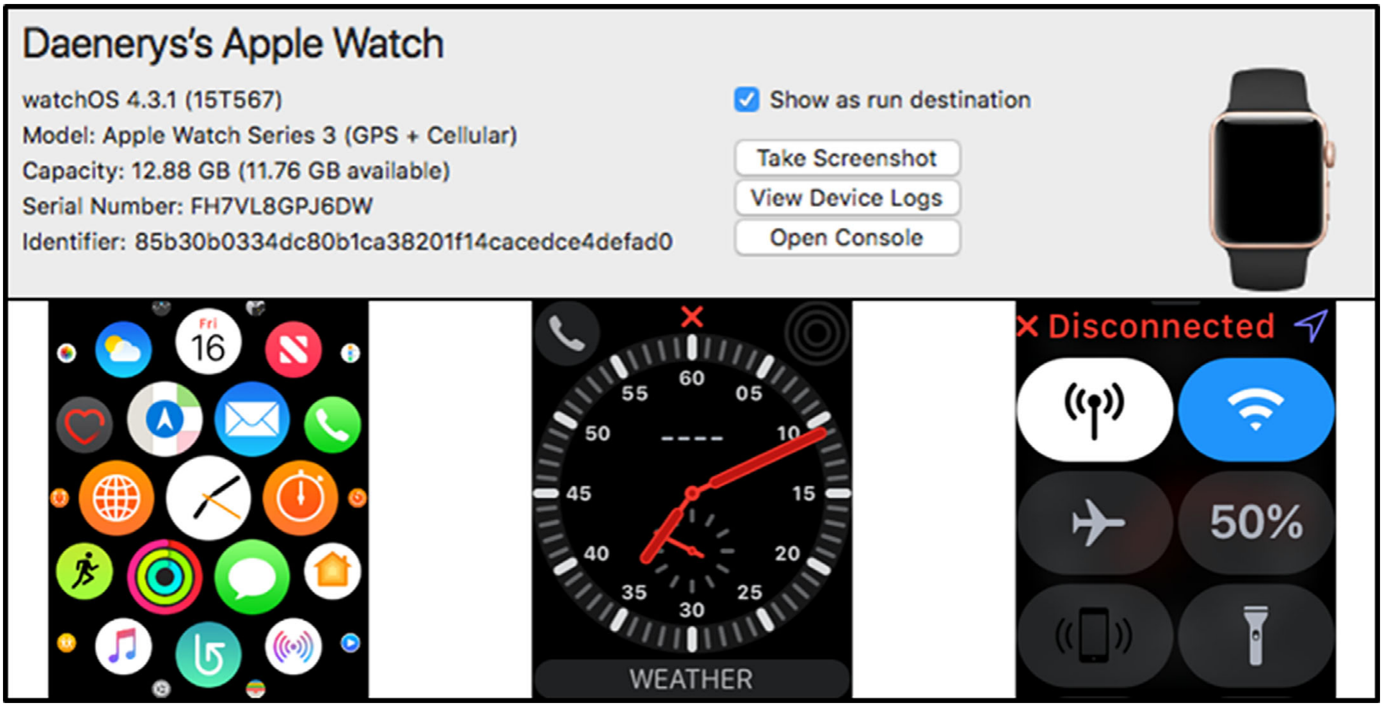
Four separate examinations were performed for this work, following guidelines recommended by NIST for the analysis of forensic data (13).

Mobile Phone Devices

In this section, the data identified and analyzed on each of the companion mobile phone devices over both studies, connected and standalone, are presented.

Samsung™ Galaxy S8—Since data population was thoroughly documented, the goal of this examination was to specifically look for any evidence related to the populated data, in addition to any indications of the paired smartwatch wearable device. Examination of the three forensic extractions (i.e., Android Backup, Partial File System, Logical) resulted in a number of log files, documents, applications, and plugins originating from connection with the Gear S3 Frontier, as well as a decent amount of populated user data.

When examining the file system of the Galaxy S8 for forensic artifacts left by the smartwatch wearable device, five different log files for the Gear S3 Frontier were located. Within these log files, there were specific references to the make and model of the smartwatch wearable device connected, as well as the device's alias name which references the user. Also listed was a transcription of the downloaded Gear application necessary for pairing the smartwatch wearable device to the mobile phone, the



Daenerys's Apple Watch

watchOS 4.3.1 (15T567)
Model: Apple Watch Series 3 (GPS + Cellular)
Capacity: 12.88 GB (11.76 GB available)
Serial Number: FH7VL8GPJ6DW
Identifier: 85b30b0334dc80b1ca38201f14cacedce4defad0

☑ Show as run destination

FIG. 6—*Utilizing Xcode® for extraction of data from the Apple Watch® Series 3.*

first connection made between the two devices, the last date of sync, and information regarding the cellular network service provider for the standalone smartwatch wearable device. In addition to these log files, different applications and plugins were found which show a direct connection between the devices, including <com.samsung.android.app.watchmanagerstub>, <com.samsung.android.gearoplugin>, an installation file under SmartThings, and the SamsungPayWearable.apk. A vast amount of multimedia related to the Gear S3 Frontier was also found in the Data Files section of Cellebrite's UFED Physical Analyzer under Images.

When examining the device for sensitive user data, the specification of connected versus standalone and the status of any communication became important. Table 2 depicts data identified on the Samsung™ Galaxy S8 mobile phone device. All data acquired in the connected mode contained entries originating from both devices. Due to limitations in the available acquisition methods for this device, no data were acquired regarding Alarms, Reminders, Notes, Email, Facebook or WhatsApp Messengers, Google Maps, Waze Navigation, Web Browser Activity, Hey Google Commands, Samsung™ Health, Facebook, or Snapchat as a standalone or connected device; however, of the data acquired, a decent amount of connected data and a limited amount of standalone data were able to be identified. With respect to acquired data in the connected mode, the Galaxy S8 appears to store everything regardless of population provenance. The only unrecoverable data were deleted SMS and Kik messages due to the methods of acquisition. With respect to acquired data in the standalone mode, data identified were much more limited. Of that identified, the only unrecoverable data were again deleted SMS and Kik messages; however, SMS messages deleted from the smartwatch wearable device were able to be recovered on the companion mobile phone device.

Apple® iPhone® 6—The goal of this examination was to specifically look for any evidence related to data population, as well as any indications of the paired smartwatch wearable device. Examination of the two forensic extractions (i.e., GrayKey Full Filesystem and Cellebrite Advanced Logical extraction) resulted in a sufficient amount of populated user data, as well as many documents, property lists, and databases regarding or originating from the Apple Watch® Series 3.

When examining the file system of the Apple® iPhone® 6 for forensic artifacts left by the smartwatch wearable device, many different files referencing "nano" and "gizmo" were identified. Within these files, information pertaining to the smartwatch wearable device's system and application registries, companion sync events, current state and history, backups, software updates, and device checks, as well as the WatchKit and Apple® System Logs were located. In addition to these files, many different property lists (plists) and databases for the wearable device were located which showed a direct connection between the devices, including <com.apple.private.alloy.watchconnectivity>, <com.apple.storeServices.watchAnalytics>, <com.apple.private.alloy.findmydevice.watch>, and <com.apple.private.alloy.companionproxy>. A vast amount of multimedia and watchfaces for the Series 3 were also identified.

When examining the device for sensitive user data, the specification of connected versus standalone and the status of any communication were again important variables to document. Table 3 depicts data identified on the Apple® iPhone® 6 mobile phone device. All data acquired in the connected mode contained entries originating from both devices, unless otherwise specified due to a lack of functionality by the smartwatch wearable device. No data were found regarding Alarms, Hey Siri Commands, Facebook, or Snapchat as a standalone or connected device; however, this could be due to limitations in the search methodology or the automated parsing capabilities of the version of Physical Analyzer utilized for analysis of the GrayKey acquisition, as these acquisitions were still relatively new at the time of analysis. Even with these possible

TABLE 2—*Data identified on Samsung™ Galaxy S8 mobile phone device*

Data	Connected	Standalone	Exclusions
Contacts	✓	X	
Calendar Events	✓	X	
Alarms	X	X	
Reminders	X	X	
Notes	X	-	
Keychains	✓^{E}	✓^{E}	
Email	X	X	
Multimedia	P	X	*
Call Logs	✓	✓	All Voicemails; Watch-Originating Outgoing Calls in Standalone Mode
SMS	✓	✓	Phone-Originating Deleted Messages in Connected Mode[†]
MMS	P	X	Deleted Messages in Connected Mode
Facebook Messenger	X	X	
Kik Messenger	✓	✓	All Deleted Messages
WhatsApp Messenger	X	X	
Location	X	-	
Browser Activity	X	X	
Hey Google Command	X	X	
Facebook	X	-	
Snapchat	X	-	
Samsung™ Health	X	X	

✓: Acquired data originating from all sources included in study.

P: Only acquired data which originated from companion mobile phone device.

X: No data acquired from either source included in study.

E: Encrypted data.

-: Smartwatch wearable device has a lack of functionality and is not capable of performing this type of data independently.

*Smartwatch-originating data only included audio files, as it could not add image or video files.

[†]All messages deleted from the smartwatch wearable device over both modes of population were recoverable on the companion mobile phone device.

TABLE 3—*Data identified on Apple® iPhone® 6 mobile phone device*

Data	Connected	Standalone	Exclusions
Contacts	P	-	
Calendar Events	✓	✓	
Alarms	X	X	
Reminders	✓	✓	
Notes	P	-	
Keychains	✓	✓	
Email	✓	✓	
Multimedia	P	X	*
Call Logs	✓	✓	Watch-Originating Outgoing Calls in Standalone Mode
SMS	✓	✓	Phone-Originating Deleted Messages in Connected Mode[†]
MMS	✓	✓	Phone-Originating Deleted Messages in Connected Mode[†]
Facebook Messenger	P	X	[‡]
Kik Messenger	✓	✓	
WhatsApp Messenger	✓	✓	
Location	P	X	Watch-Originating Navigation Events
Browser Activity	P	X	
Hey Siri Command	X	X	
Facebook	X	-	
Snapchat	X	-	
Apple® Activity	✓	X	

✓: Acquired data originating from all sources included in study.

P: Only acquired data which originated from companion mobile phone device.

X: No data acquired from either source included in study.

- : Smartwatch wearable device has a lack of functionality and is not capable of performing this type of data independently.

*Smartwatch-originating data only included audio files, as it could not add image or video files.

[†]All messages were able to be identified except for messages which were deleted from the companion mobile phone in the connected mode. All messages deleted from the smartwatch wearable device over both modes of population were recoverable on the companion mobile phone device.

[‡]Smartwatch wearable device had issues loading the Facebook Messenger application and therefore could not be populated with data; this is a common issue seen for many Apple Watch® devices.

limitations, the data acquired contained a significant amount of user data that was able to be identified over both modes of population. With respect to acquired data in the connected mode, the Apple® iPhone® 6 seems to store everything originating from the mobile phone device. When looking at Apple® Maps location data, any navigation information originating from the Series 3 was unable to be identified. In the connected mode, any SMS messages that were deleted from the mobile phone device were also unable to be recovered; however, SMS messages deleted from the smartwatch wearable device were able to be located on the companion mobile phone device. With respect to acquired data in the standalone mode, it would appear that the companion mobile phone does not store any data from outgoing calls.

Smartwatch Wearable Devices

In this section, the data identified and analyzed on each of the smartwatch wearable devices over both studies, connected and standalone, are presented.

Samsung™ Gear S3 Frontier—The goal of this examination was to look for any evidence related to the populated data, as well as any information that could be considered probative in an investigation. A filesystem extraction was performed on the Gear S3 Frontier, resulting in fourteen directories of user and system data including bin, csa, dev, etc., home, lib, media, opt, proc, sbin, sys, tmp, usr, and var. Due to a lack of root access, there were many files within the above-mentioned directories which were unable to be acquired during the data extraction; each of these files was documented in an output log. In addition, a few directories found at the root level of the Gear S3 (i.e., %{TZ_USER_SHARE}, boot, cpnvcore, lost+found, mnt, root, run, srv) were not copied over to the Host PC as a result of either being empty or requiring root access. It is important to note that even though a filesystem extraction was able to be performed, much of the data were acquired in duplicate; in fact, even though all system and user data are stored in the expected directory locations of the filesystem, the smartwatch wearable device unexpectedly utilizes the common Linux directory, opt, to store duplicates of most, if not all, user and device specific data. Further analysis of this opt directory revealed that two of the significant artifacts identified on the smartwatch wearable device, <.account.db> and <.CompanionInfo.db>, were identified in this unexpected storage location alone. These database files contain user identifiers and a large amount of information pertaining to the paired companion mobile phone device of the Gear S3, and are not found in any of the expected directories for user and system data storage. Therefore, the opt directory was the only directory analyzed in depth for the identification of all populated data in this research. The smartwatch wearable device's owner profile, located at opt/usr/home/owner, was made up of nine directories, two of which held a significant amount of probative data.

Under the <apps_rw> directory, many plugins were found containing information about the user, companion or host device, and the Gear S3 Frontier itself. Among these plugins were <com.samsung.w-manager-service> which stored two individual files about the Host and Wearable statuses, <com.samsung.samsungaccount> which contained a database of service applications and user information, and <com.samsung.gearstore> which listed identifying strings and specifications regarding the smartwatch wearable device. Under the <data> directory, a file pertaining to the user's Samsung™ cloud account was located.

When examining the device for sensitive user data, there were some significant differences between the Gear S3 Frontier and Galaxy S8 acquisitions. Table 4 depicts data identified on the Samsung™ Gear S3 Frontier smartwatch wearable device. All data acquired in the connected mode contained entries created by both devices, unless otherwise specified in the comments. Location data identified for the smartwatch wearable device does not include any data pertaining to the Waze navigation application, as the Gear S3 Frontier had a lack of functionality for this application at the time of testing. No data were found regarding Notes, Facebook Messenger, Kik Messenger, WhatsApp Messenger, Hey Google Commands, Facebook, or Snapchat as a standalone or connected device; however, vast amounts of data were still able to be identified for many other data categories over both modes of population. When looking at Samsung™ Health data in either mode of population, the vast majority of the identified data was in an undecipherable format. With respect to acquired data in the connected mode, the Samsung™ Gear S3 Frontier does not store any Alarms, Keychains, Email, or video/audio Multimedia local to the companion mobile phone device. In addition, the smartwatch wearable device does not appear to store any SMS messages, MMS messages, or Browser Activity when operating in the connected mode. With respect to acquired data in the standalone mode, it would appear that the Gear S3 Frontier stores at least a portion, if not all, of the populated data; the only areas where this is not the case are the exclusion of voicemails and deleted data. In particular, when looking at Browser Activity, only the search results were able to be located; none of the typed queries to bring up these search results were identified.

TABLE 4—*Data identified on Samsung™ Gear S3 Frontier smartwatch wearable device*

Data	Connected	Standalone	Exclusions
Contacts	✓	✓	
Calendar Events	✓	✓	
Alarms	W	✓	Phone-Originating Alarms in Connected Mode
Reminders	✓	✓	
Notes	X	-	
Keychains	X	W^{E}	Encrypted
Email	✓	✓	Phone-Originating Draft Email in Connected Mode
Multimedia	P	✓	Phone-Originating Video & Audio in Connected Mode[*]
Call Logs	✓	✓	All Voicemails
SMS	X	✓	All Deleted Messages
MMS	X	✓	All Deleted Messages
Facebook Messenger	X	X	
Kik Messenger	X	X	
WhatsApp Messenger	X	X	
Location	P^{E}	-	
Browser Activity	X	✓	[†]
Facebook	X	-	
Snapchat	X	-	
Samsung™ Health	✓	✓	[‡]

✓: Acquired data originating from all sources included in study.

P: Only acquired data which originated from companion mobile phone device.

W: Only acquired data which originated from smartwatch wearable device.

X: No data acquired from either source included in study.

E: Encrypted data.

- : Smartwatch wearable device has a lack of functionality and is not capable of performing this type of data independently.

[*] Smartwatch-originating data only included audio files, as it could not add image or video files.

[†] Although viewed pictures or visited webpages were able to be identified, the specific typed queries to pull up these results were unable to be identified.

[‡] Only partial data identification, which included mapped workouts over both modes of population; the remainder of the Samsung™ Health database was undecipherable.

Apple Watch® Series 3 — The goal of this examination was to look for any evidence related to the populated data, as well as any information that could be considered probative in an investigation. Many methods were attempted for the extraction of data from the Series 3, and although none were wholly successful, connection possibilities were discovered which allowed for the manual documentation of displayed content.

Physical connection of the Series 3 revealed that iTunes® recognizes an Apple Watch® and offers assistance with technical issues in the form of a software update or a complete restoration of the device's original settings. In addition, an examination of the PC's connected devices identified the Series 3 as a USB Hi-Speed Bus labeled "Watch," with supplementary information including the host controller driver, the device's serial number, and the port number of the smartwatch wearable device.

When examining the device for sensitive user data, it quickly became apparent that due to the limited extraction methods and lack of functionality for the origination of certain data on the smartwatch wearable device, the Series 3 does not store a significant amount of data which is detailed enough to be effectively probative. Table 5 depicts data identified on the Apple Watch® Series 3 smartwatch wearable device through manual examination of displayed content. All data acquired in the connected mode contained entries originating from both devices, unless otherwise specified due to a lack of functionality by the smartwatch wearable device. Location data identified for the smartwatch wearable device does not include any data pertaining to the Waze navigation application, as the Series 3 had a lack of functionality for this application at the time of testing. No data were found regarding Calendar Events, Notes, Keychains, MMS, Browser Activity, Facebook Messenger, Kik Messenger, WhatsApp Messenger, Hey Siri Commands, Apple Activity, Facebook, or Snapchat as a standalone or connected device; however, a small amount of data was still able to be examined manually for other data categories over both modes of population. With respect to identified data in the connected mode, the Apple Watch® Series 3 seems to largely exclude data originating from the mobile phone device, with the exception of Contacts. Although the Series 3 lacks the functionality to create Contacts, it does store those which originated from the mobile phone device; however, when displayed on the Series 3, the information is limited to the individual's name and excludes the number, email, or any additional information pertaining to the entry. In the connected mode, Email messages which were sent from either device were unable to be identified. In addition, when examining Call Logs, only voicemails were identified in the connected mode. With respect to identified data in the standalone mode, the smartwatch wearable device does store Call Logs additional to voicemails; however, only the most recent log per individual is retained with no identifiable directionality of incoming or outgoing.

TABLE 5—*Data identified on Apple Watch® Series 3 smartwatch wearable device*

Data	Connected	Standalone	Exclusions
Contacts	✓	-	*
Calendar Events	X	X	†
Alarms	W	✓	Phone-Originating Alarms in Connected Mode
Reminders	W	✓	Phone-Originating Reminders in Connected Mode
Notes	X	-	
Keychains	X	X	
Email	✓	X	Phone-Originating Draft & Sent Emails in Connected Mode
Multimedia	P	X	Phone-Originating Video & Audio in Connected Mode[‡]
Call Logs	✓	✓	All Phone-Originating Call Data in Connected Mode[§]
SMS	✓	X	Deleted Messages in Connected Mode
MMS	X	X	
Facebook Messenger	X	X	
Kik Messenger	X	X	
WhatsApp Messenger	X	X	
Location	P	X	Watch-Originating Navigation Events
Browser Activity	X	X	
Facebook	X	-	
Snapchat	X	-	
Apple® Activity	X	X	¶

✓: Acquired data originating from all sources included in study.

P: Only acquired data which originated from companion mobile phone device.

W: Only acquired data which originated from smartwatch wearable device.

X: No data acquired from either source included in study.

E: Encrypted data.

- : Smartwatch wearable device has a lack of functionality and is not capable of performing this type of data independently.

*Only the contact name is displayed on the smartwatch wearable device; all additional information is not shown.

†Calendar data are time-sensitive, as the smartwatch wearable device only displays the current month.

‡Smartwatch-originating data only included audio files, as it could not add image or video files.

§The only phone-originating data able to be identified in the connected mode were voicemails; all other call data were unable to be identified. Standalone Call Logs, displayed on the smartwatch wearable device, only show the most recent call per individual number and indicate no directionality of incoming/outgoing.

¶: All fitness data populated on the smartwatch wearable device is transferred immediately to companion mobile phone device.

Discussion

Samsung™ Galaxy S8

A significant amount of data was unidentified; however, this is most likely due to the type of extractions that were able to be acquired. With each extraction performed (i.e., Android Backup, Partial File System, Logical), data accessibility is dependent upon the device's make, model, OS version, and security measures, and therefore could be limited for this device. Since no physical extraction was acquired, it is difficult to determine if the data that was not identified was due to its physical absence or the limitations which these types of extractions presented; however, given the documented content provided by a physical extraction and the general consensus among analysts familiar with using this type of extraction every day, it is more probable that the latter is the underlying reason for the nonexistent data.

The forensic artifacts identified contained a significant amount of information regarding the Gear S3 Frontier, including specifications for the smartwatch wearable device and the dates and times of its utilization. These artifacts could not only inform investigators of additional evidence items that may need to be acquired, but could also provide useful information about the user's utilization habits of the smartwatch wearable device, alternate phone numbers to inquire about with the cellular network provider, and whether the smartwatch wearable device is up-to-date in sync with the companion mobile phone.

When examining the results, it can be concluded that extraction capabilities for the Samsung™ Galaxy S8 are severely limited at this time. Although all of the acquired connected data was able to be identified, there is still a significant amount of populated data which was unable to be acquired or identified. Given that all acquired connected data was transferred back to the companion mobile phone, it can be concluded that the smartwatch wearable device simply acts as an extension of the smartphone when operating in this mode. With respect to the acquired standalone data, identification was even more limited. The Galaxy S8 does not seem to store anything local to the Gear S3 Frontier, such as Personal Information Management (PIM) data or multimedia. However, the data that is capable of communicating with and being transferred through a cellular network or a specific application's cloud source appears to be able to be identified, including messages which were deleted from the local smartwatch wearable device. The only source where this does not seem to be the case is with the Kik Messenger application, which does not allow for deleted messages to be recovered in either mode. This points to the way in which these messenger applications work, storing only the conversation currently present in the downloaded application on the device instead of all messages sent, received, and deleted.

Samsung™ Gear S3 Frontier

Although a few root-level directories and many files within the acquired directories of the smartwatch wearable device were skipped upon use of the pull command, either due to a lack of root access or the directory being empty, a significant amount of data was still able to be extracted from the Gear S3 Frontier. The smartwatch wearable device does not appear to store data from any third-party applications like Facebook, Snapchat, or alternative messaging applications; data including Hey Google Commands and Notes made on the companion device were also unidentifiable. However, it would seem that it is possible to extract, identify, and recover at least a portion of all other data created in the standalone mode, excluding some deleted SMS messages. The Location and Samsung™ Health data were identified on the device for the range of dates in which data were populated; some of which was readable and interpretable, with the remainder being in a format that could not be interpreted. With further testing and/or research, there is a high possibility that location data and health statistics would be fully available if needed. The results for Web Browser Activity were a bit different; although a specifically typed search query could not be located or identified, the results of the query were attainable and offered a snapshot of the user's intent.

When it comes to connected data, there was also a significant amount of data identification. Most of the same information identified in the standalone analysis was found, with a few exclusions. It would appear that most PIM data originating from either device is present, with the exception of Alarms. Connected Alarms were found, but only those that were created from the smartwatch wearable device. This implies that the Gear S3 Frontier is capable of storing information originating from either source device, and allows for personally sensitive data to be acquired. In the special case of Alarms, none were found on the Samsung™ Galaxy S8, which means that the smartwatch wearable device may in fact be the only source of this data. It is important to note that the Gear S3 Frontier does not seem to store any passwords apart from its own security lock, meaning that no security information for the companion smartphone device, emails, or additional applications can be acquired. Since all emails, existing or pre-existing, in both population modes were identified excluding the draft message created and then deleted by the companion mobile phone device, there are two possibilities for email storage: the smartwatch wearable device either never received the draft message as a result of the default sync interval settings of the device's email application or the smartwatch wearable device is simply unable to store any messages which are local to the companion mobile phone. No SMS or MMS messages populated during the connected mode were identified, suggesting that when the Gear S3 Frontier has a connection to the companion mobile phone, no texting data is stored on the device; it is simply used as a pass through. Similar to the standalone analysis, some Location and Samsung™ Health data were found either readable and interpretable, or undecipherable; however, tracked maps of both connected and standalone workout routes were fully available. With connected Web Browser Activity, nothing could be located on the smartwatch wearable device, which suggests that the Gear S3 Frontier is not at all involved in this process and merely mirrors the companion mobile phone device as warranted.

Although limited in its storage of SMS/MMS messages and third-party messenger application data, it is evident that the Samsung™ Gear S3 Frontier is capable of storing similar amounts of accessible data, if not more, compared to the Samsung™ Galaxy S8.

Apple® iPhone® 6

The two extractions performed on the Apple® iPhone® 6 were not equivalent; although both extractions were sufficient for acquiring sensitive user data from the device, Grayshift's GrayKey was able to acquire slightly more information than Cellebrite's Advanced Logical extraction at this time. In addition to identifying the passcode of the mobile phone, the GrayKey was also able to acquire source files containing all emails, deleted MMS messages, Facebook Messenger conversations, and partial Apple® Maps location data; all of which were unable to be acquired with an Advanced Logical Extraction. As stated previously, data which was unable to be identified for the GrayKey extraction could be due to the relative newness of these acquisitions at the time of analysis, meaning that the available version of Cellebrite's Physical Analyzer may not have been equipped to fully parse the given data. It would be advantageous to reload the data extraction into the newest version of Physical Analyzer in order to confirm that this data were unable to be parsed or found manually. It would also be interesting to explore whether jailbreaking the Apple® iPhone® 6 would allow a Cellebrite extraction to acquire these additional items.

Although an abundant number of documents, property lists, and databases were located which show a direct connection between the two devices, these files are limited in the amount of information they provide about the "nano" or "gizmo" smartwatch wearable device. However, the Apple® System Logs identified in reference to the smartwatch wearable device did contain some key clues to the directory structure of the Apple Watch® Series 3, making them significant in communicating with the smartwatch wearable device.

When examining the results, it can be concluded that although acquisition of data from the Apple® iPhone® 6 does not present a complete picture of all user data populated in both modes, the device clearly stores the vast majority of the data. The only area of acquired connected data that was limited in extraction due to storage capabilities was that of the Apple® Maps location data, which excluded data originating from the smartwatch wearable device. To ensure this data were unable to be identified due to its physical absence and not an inability of the software to parse the material, a series of known information about the populated data was searched across the entirety of binary data, including GPS coordinates and names of locations, date and times of navigation, and specific search queries typed. The inability to identify any location data related to Apple® Maps which originated from the connected smartwatch wearable device suggests that this navigation is not stored on the companion mobile phone, and therefore no record of navigational events logged by Apple® Maps on the Series 3 would exist within the mobile phone acquisition. All SMS messages deleted from the mobile phone device were also unable to be identified; the cause of this could be due to the limitations of the types of extractions performed on the device and not a physical absence of the data, or the data could simply no longer be available within the respective source file. The only area of acquired standalone data that was limited in extraction was related to calls initiated by the smartwatch wearable device. Since the call logs included everything except for outgoing calls, it can be concluded that the companion mobile phone device during standalone mode stores only calls which are directly connected to its registered mobile phone number. Although the smartwatch wearable device mirrors the companion mobile phone's dialing number in order to receive calls, and this same number appears on the receiving user's screen when performing an outgoing call from the smartwatch wearable device, the Series 3 is in fact registered under a separate dialing number with the cellular network provider. The inability of the companion mobile phone to store any outgoing calls initiated from the smartwatch wearable device during standalone mode suggests that the Series 3 is in fact using its registered dialing number to perform these calls, while indirectly mirroring the mobile phone's number on the receiving user's phone. It is important to note that the Apple Watch® Series 3 is not capable of performing some functions, including Contacts, Notes, and Web Browser Activity; therefore, no conclusions can be drawn about these functions in regards to the smartwatch wearable device.

Apple Watch® Series 3

Although a significant amount of data was unable to be acquired or identified due to the current inability to communicate and interact with the Apple Watch® Series 3 at a deeper level than a manual examination, some key observations were still able to be made in regards to both the identified and unidentified data.

The Series 3 was recognized by iTunes®; however, the ability to view data in a manner similar to when an iPhone® device is accessed through the application was not possible, as only options for update or recovery were available. At this time, it would appear that the additional information obtained from viewing the PC's connected devices is not helpful in offering a wireless point of connection. Although Xcode® allows for interaction with the smartwatch wearable device through a physical connection, any efforts made to take advantage of developer commands or simulated devices in order to perform an extraction of the data is also not possible at this time.

When examining the results, it can be concluded that manual examination of the Apple Watch® Series 3 offers an extremely limited amount of information due to the smartwatch wearable device's method of storage and display functionalities. Storage of both Browser Activity and Apple® Activity/Health was not identified on the Series 3. Although searches and fitness activity were viewable and interactive on the smartwatch wearable device during population, data from both categories were automatically transferred to the companion mobile phone device and are not accessible on the Series 3. It is possible this smartwatch-originating data is stored in local databases, but is not available due to the limited extraction methods. In addition, it quickly became apparent that the amount of time spanning from the intake of the smartwatch wearable device to the acquisition of its data is a primary concern for Calendar Events due to the limited display functionality of the Series 3; no conclusions can be drawn in regards to this data category, as the Series 3 is only able to manually display the current month.

With respect to identified data, it is evident that the Apple Watch® Series 3 offers much less than the Apple® iPhone® 6 at this time. In addition, what is accessible on the Series 3 through a manual examination is not well-detailed, and therefore lacks probative impact. Even though there was little success with this smartwatch wearable device, it is still important to publish the methods attempted not only to shine light on different avenues for future researchers to further pursue, but also to increase awareness about some methods that may prove futile.

Future Work

This investigation shone a light on the lack of current research being performed on smartwatch wearable devices. It is the hope that publication of both successful and failed attempts on data acquisition will spur future work to be performed on the identification of new methodology for data acquisition from current smartwatch wearable devices, or the furtherance of the listed methods attempted in this research. It would be of particular interest to explore the possibility of altering smartwatch wearable device settings prior to acquisition, in order to allow for more files to be accessible through nonrooted acquisition or to disable any encryption so that chip-off techniques may be performed. Specifically, for the Apple Watch® Series 3, further exploration of wireless connection possibilities, including low-energy Bluetooth, could prove beneficial in the acquisition of data from these devices. In addition, further research into full Standalone acquisitions and acquisitions involving rooting of the Samsung™ Gear S3 Frontier should be pursued, as it would allow both upper and lower limits to be more firmly established for this device.

Conclusions & Contributions

This research sought to provide an enhanced understanding of 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 connected device. It also sought to provide a methodology for the forensically sound acquisition of data from a standalone smartwatch wearable device. Through the two studies, this work has shown that there are a significant amount of artifacts stored on both the smartwatch wearable devices and their companion mobile phone devices over both modes of connectivity, some of which could prove especially valuable during cases where one of the paired devices may not be present.

Additionally, this work addresses the location of storage for different applications and various sensitive user data when utilizing a connected or standalone device; and although there were categories of data population that were unable to be acquired for every device, a substantial amount of information can be garnered with respect to probative data. For the Samsung™ Galaxy S8 mobile phone device, acquisition capabilities were limited; however, it stored all identified connected data and any standalone data that is capable of cellular communication, including messages deleted from the smartwatch wearable device. For the Samsung™ Gear S3 Frontier, acquisition was equivalent, if not better, than its companion mobile phone device. Although this smartwatch wearable device is limited in the amount of data stored when utilized in the connected mode, it stores the vast majority of data populated in the standalone mode, making it a valuable device to collect for digital investigations. For the Apple® iPhone® 6 mobile phone device, acquisition was substantial in both the connected and standalone modes. At this time, there only appear to be two areas of identified data which are incompletely acquired, being the location data originating from the smartwatch wearable device in connected mode and the outgoing calls made in standalone mode. As for the Apple Watch® Series 3, more work needs to be done in order to determine its probative capabilities during a digital investigation. Current acquisition methods are limited to a manual examination, which not only offers no additional data to the companion mobile phone, but also data which are time sensitive or incomplete.

As a result of the work performed, a data extraction tool for the Samsung™ Gear S3 Frontier was created, coined GearGadget. This tool allows for law enforcement and analysts in the field to easily connect to and extract data from a seized Gear S3 Frontier through a command-line interface. A Graphical User Interface (GUI)-based version may be explored in the near future; however, the current version consists of an automated shell script built into an .OVF virtual machine containing all necessary software and components for a data extraction. An operating system of Ubuntu Linux (v.18.04) was chosen for this virtual machine, and Tizen Studio (v.2.4) was installed to enable operation of the Smart Development Bridge (SDB). A shell (bash) script was written which, once initiated through <bash.GearGadget.sh>, allows the user to assign a unique identifier to their smartwatch wearable device and input the IP address for the device as allocated by the WAP. Once the user has specified these variables, the script enacts a series of pull commands, as outlined in the Acquisition Methods section, to extract data from the identified source device to the connected target PC. Upon completion, this tool results in a filesystem data extraction, which can be brought into most popular tools for analysis. The GearGadget tool also outputs both a log file documenting the acquired/skipped data and an MD5 hash value for data verification. This extraction tool package is available for download at https://www.marshall.edu/cyber/geargadget/. It is also important to note that any novel artifacts found on all devices studied in this research have been submitted for reference to the Artifact Genome Project (AGP), in an effort to better aid analysts and researchers in knowing what content is available on these smartwatch wearable and paired devices, as well as its location. The AGP is accessible at https://agp.newhaven.edu/.

Acknowledgments

Thank you to the Virginia Department of Forensic Science (DFS) and the Digital & Multimedia Evidence Section analysts at the DFS Central Laboratory for the opportunity and resources for this project, as well as guidance and advice. Thank you to Dr. Catherine G. Rushton of the Marshall University Forensic Science Center (MUFSC) for lending her time and assistance throughout the entirety of this research project. In addition, special thanks to Dr. Ian Levstein of the MUFSC for his tremendous amount of financial support and confidence; thank you for being an amazing advisor and teaching me all about the wonderful world of computers.

References

1. Shirer M, Llamas R, Ubrani J, editors. IDC forecasts shipments of wearable devices to nearly double by 2021 as smart watches and new products categories gain traction. Framingham, MA: International Data Corporation Insights Press, 2017. https://www.idc.com/getdoc.jsp?containerId=prUS43408517 (accessed June 1, 2018).
2. Police Executive Research Forum. New national commitment required: the changing nature of crime and criminal investigations. Critical Issues in Policing Series. Washington, DC: Police Executive Research Forum, 2018. http://www.policeforum.org/assets/ChangingNatureofCrime.pdf (accessed June 8, 2018).
3. Goodison SE, Davis RC, Jackson BA. Digital evidence and the U.S. criminal justice system: identifying technology and other needs to more effectively acquire and utilize digital evidence. Santa Monica, CA: RAND Corporation, 2015.
4. Rogers M. DCSA: a practical approach to digital crime scene analysis. In: Tipton HF, Krause M, editors. Information security management handbook, 5th edn. vol. 3. Boca Raton, FL: Auerbach Publications, 2006;601–14.
5. Alabdulsalam S, Schaefer K, Kechadi T, Le-Khac NA. Internet of things forensics: challenges and case study. In: Peterson G, Sehnoi S, editors. Advances in digital forensics XIV. Proceedings of DigitalForensics 2018: 14th IFIP WG 11.9 International Conference on Digital Forensics; 2018 Jan 3-5; New Delhi, India. New York, NY: Springer, 2018;35–48.
6. Seneviratne S, Hu Y, Nguyen T, Lan G, Khalifa S, Thilakarathna K, et al. A survey of wearable devices and challenges. IEEE Commun Surv Tutor 2017;19(4):2573–620.
7. Arshad H, Jantan AB, Abiodun OI. Digital forensics: review of issues in scientific validation of digital evidence. J Inf Process Syst 2018;14 (2):346–76.
8. Karakaya M, Bostan A, Gökçay E. How secure is your smart watch? Int J Info Secur Sci 2016;5(4):90–5.
9. Baggili I, Oduro J, Anthony K, Breitinger F, McGee G. Watch what you wear: preliminary forensic analysis of smart watches. In: O'Conner L, editor. ARES 2015: Proceedings of the 2015 10th International Conference on Availability, Reliability and Security; 2015 Aug 24-27; Toulouse, France. Piscataway, NJ: IEEE, 2015; 303–11.
10. Al Barghouthy N, Marrington A. A comparison of forensic acquisition techniques for Android devices: a case study investigation of Orweb browsing sessions. In: Badra M, Alfandi O, editors. NTMS 2014: Proceedings of the 2014 6th International Conference on New Technologies, Mobility and Security; 2014 Mar 30-Apr 2; Dubai, United Arab Emirates. Piscataway, NJ: IEEE, 2014; 1–4.
11. AT&T. Saint Louis, MO: AT&T Services, Inc.; c1986-2019. Samsung Gear S3 frontier (R765A): connection status. https://www.att.com/devicehowto/index.html#!/tutorials/topic/9006081 (accessed January 1, 2019).
12. Ayers RP, Livelsberger BR, Guttman B. Quick start guide for populating mobile test devices. Gaithersburg, MD: National Institute of Standards and Technology, 2018. May; Report No.: SP 800-202.
13. Kent K, Chevalier S, Grance T, Dang H. Guide to integrating forensic techniques into incident response. Gaithersburg, MD: National Institute of Standards and Technology, 2006. Aug.; Report No.: SP 800-86.