Go-Go Gadget, Smartwatch! An Inspection of Wearable Devices & Their Forensic Value

Nicole R. Odom*, BS[1]; Jesse M. Lindmar, BS[2]; John Hirt, BS[2]; Joshua L. Brunty, MS[1]; Dr. Catherine G. Rushton, EdD[1]

[1] Marshall University Forensic Science Center, Huntington, WV; [2] Virginia Department of Forensic Science- Digital & Multimedia Evidence, Richmond, VA

Abstract

Wearable devices allow users the ability to walk away from mobile phone devices while remaining connected to the digital world; however, this freedom creates additional challenges for digital forensic investigators and analysts in the examination, acquisition, identification, and analysis of probative data. This preliminary research attempts to provide an enhanced understanding of not only what sensitive user data and forensic artifacts a smartwatch may contain, but also the process of acquiring this data directly from the wearable or through its companion mobile phone device. The results identify significant amounts of data on the Samsung™ Gear S3 Frontier device; greater than that stored on the companion mobile phone. An Apple Watch® Series 3 manual examination method which produces high-quality native screenshots was identified; however, the companion mobile phone was found to store the greatest amount of data.

Introduction

Innovative writers have filled the minds of adolescents and adults alike with dreams of a connected future through wearable devices; and after all these years, science fiction has become a reality. Police departments are now finding that victims, suspects, and witnesses tend to have up to three smart devices each.[1] This increase in smart device use leads to greater amounts of personally sensitive data which can be employed to establish causality in investigations.[2] Few studies have been performed on the acquisition of smartwatch data, and those performed have utilized limited methods that are time-consuming, incomplete, or forensically unsound.[3]

For this research, the Samsung™ Gear S3 Frontier and Apple Watch® Series 3 were 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 completion of both studies, two separate examinations were performed. The first involved the two mobile phone devices synced with the wearable smartwatches (i.e., the Samsung™ Galaxy S8 and Apple® iPhone® 6), looking for any forensic artifacts left from its respective smartwatch device and possible user data stored when acting as a connected or standalone device. The second examination looked at the smartwatch wearable devices and any identifiable data they may store that could be considered probative in a forensic investigation.

Methods

Data Population

1. Connected: wearable utilized Bluetooth & Wi-Fi with companion phone.

2. Standalone: wearable utilized cellular network connection.

Data consisted of:

Contacts	Reminders	Email	Browser Activity
Calendar Events	Keychains	Messengers	3rd Party Apps
Notes	Call Logs	Fitness Apps	Multimedia
Alarms	SMS/MMS	Location	Commands

Data Acquisition

Each companion mobile phone was examined for populated data in both states and any indications of its respective paired wearable. Extractions were as follows:

- Samsung™ Galaxy S8 - UFED Logical, Partial File System, & Android Backup
- Apple® iPhone® - GrayKey Full File System & Cellebrite Advanced Logical

Each smartwatch wearable device was examined for populated data in both states and any probative content. Methods were as follows:

- Samsung™ Gear S3 Frontier - The Software Development Bridge of Tizen's Software Development Kit was used to connect the wearable to a Host PC wirelessly. The root file of the wearable was extracted through <sdb pull>.
- Apple Watch® Series 3 - An iBUS S2 cable was connected to the diagnostic port of the wearable, and Xcode® was used for a manual examination, resulting in native screen captures.

UFED Physical Analyzer, SQLite Viewer, & Notepad++ were used for analyses.

GearGadget

A command-line based data extraction tool for the Samsung™ Gear S3 Frontier, which extracts the opt folder of the Linux directory, was created as a result of this research. GearGadget is available for download at *forensics.marshall.edu/.*

Results

Samsung™ Galaxy S8

Forensic artifacts

Five log files for wearable, containing:
- Make, model, and alias
- Gear application download
- First connection & last date of sync
- Cellular network service provider

Plugins, Documents, & Applications, including:
- <com.samsung.android.app.watchmanagerstub>
- <com.samsung.android.gearoplugin>
- SmartThings installation file
- SamsungPayWearable.apk

Sensitive user data

Acquired data is listed in Table 1. No data was found regarding Alarms, Reminders, Notes, Email, Facebook & WhatsApp Messengers, Google Maps, Waze, Browser Activity, Hey Google Commands, Samsung Health, Facebook, and Snapchat.

Table 1. Samsung™ Galaxy S8 Recoverable Data

Data	C	S	Comments
Contacts	X		
Calendar Events	X		
Keychains	X	X	Encrypted
Multimedia	X		
Call Logs	X	X	No Voicemails
SMS	X	X	No Connected Deleted Messages*
MMS	X		
Kik Messenger	X	X	No Deleted Messages

† Data recovered in connected (C) state contains entries originating from both devices for testing of provenance impact. The standalone (S) state involves only the wearable device.
* Although no deleted SMS messages were found in the connected state, all deleted messages in the standalone state were recoverable on the companion mobile device.

Table 2. Samsung™ Gear S3 Frontier Recoverable

Data	C	S	Comments
Contacts	X	X	
Calendar Events	X	X	
Alarms	X	X	Connected Excluded Phone Originating Alarms*
Reminders	X	X	
Keychains		X	Encrypted
Emails	X	X	Connected Excluded Draft Email
Multimedia	X	X	Connected Excluded Phone Originating Video & Audio**
Call Logs	X	X	No Voicemails
SMS		X	No Deleted Messages
MMS		X	
Location	X	X	Encrypted
Browser Activity		X	Only Search Results, No Typed Queries
Samsung Health	X	X	Partial Identification, Remainder Undeciphered***

† Data recovered in connected (C) state contains entries originating from both devices for testing of provenance impact. The standalone (S) state involves only the wearable device
* Alarms populated in connected state originating from companion mobile phone were not recoverable.
** Standalone recovery included connected pictures originating from phone and all standalone multimedia.
*** Partial Recovery: mapped workouts populated in both states were recovered. Health App database was encrypted.

Samsung™ Gear S3 Frontier

Forensic artifacts

Plugins & Documents, including:
- <com.samsung.samsungaccount>
- Host Status.xml & Wearable Status.xml
- Product identifiers & specifications
- Data/samsung-cloud/.samsung_cloud_data_list

Sensitive user data

Acquired data is listed in Table 2.
No data was found regarding:
- Notes
- All Messengers
- Hey Google Commands
- 3rd Party: Facebook, Snapchat

Apple® iPhone® 6

Forensic artifacts

Files for 'Nano' & 'Gizmo', regarding:
- Device & App Registries
- Event & Companion Sync
- State & history of wearable
- Backups, updates, & device checks
- WatchKit & Apple System Logs

Plists & Databases, including:
- com.apple.private.alloy.watchconnectivity
- com.apple.private.alloy.findmydevice.watch
- com.apple.private.alloy.companionproxy
- com.apple.storeServices.watchAnalytics

Sensitive user data

Acquired data is listed in Table 3. No data was found regarding Alarms, Hey Siri Commands, Facebook, and Snapchat.

Table 3. Apple® iPhone® 6 Recoverable

Data	C	S	Comments
Contacts	X	-	*
Calendar Events	X	X	
Reminders	X	X	
Notes	X	-	*
Keychains	X	X	
Emails	X	X	
Multimedia	X		
Call Logs	X	X	No Standalone Outgoing Calls; Did Identify Voicemails
SMS	X	X	Connected Excluded Phone Originating Deleted Messages
MMS	X	X	
Kik Messenger	X	X	
Facebook Messenger	X	X	
WhatsApp Messenger	X	X	
Location	X		Connected Excluded Watch Originating Locations
Browser Activity	X	-	*
Apple Activity	X		

† Data recovered in connected (C) state contains entries originating from both devices for testing of provenance impact. The standalone (S) state involves only the wearable device
* Standalone mode does not allow for functionality.

Table 4. Apple Watch® Recoverable Data

Data	C	S	Comments
Contacts	X		Connected Only Displays Name
Alarms	X	X	Connected Excluded Phone-Originating Alarms
Reminders	X	X	Connected Excluded Phone-Originating Reminders
Emails	X		Connected Excludes Phone-Originating Draft & All Sent Messages**
Multimedia	X		Connected Excluded Phone-Originating Video & Audio
Call Logs	X	X	Connected Only Included Voicemails; No Indication of Outgoing/Incoming for Standalone Call Logs**
SMS	X		Connected Excluded Deleted Messages
Location	X		

† Data recovered in connected (C) state contains entries originating from both devices for testing of provenance impact. The standalone (S) state involves only the wearable device
* Apple Watch® is not capable of adding contacts natively; addition is only possible via the companion phone.
** Standalone Call Logs only show the most recent call to a particular contact, not all outgoing and incoming. Therefore, only one call log per contact is listed, except in the case of a missed call.

Apple Watch® Series 3

Forensic artifacts

Extraction was limited to a manual examination; therefore, no artifacts were identified.

Sensitive user data

Acquired data is listed in Table 4. No data was found regarding Calendar Events, Notes, Keychains, MMS Messages, All Messengers, Browser Activity, Apple Activity, Hey Siri Commands, Facebook, and Snapchat.

Discussion/Conclusion

Samsung™ Galaxy S8

No physical extraction was performed due to an unsupported security patch level, locked bootloader, & UFS memory-chip.

- It is difficult to determine if the data not acquired was due to a physical absence or limitations of the extractions able to be performed; although, the latter is more probable.

Acquired connected data: Device stores all data regardless of origin.

- Suggests that the connected device simply acts as an extension of the smartphone.

Acquired standalone data: Device doesn't store data local to the wearable; however, data capable of transfer through a cellular network or cloud source is acquired, even when deleted locally.

- One exclusion: Kik Messenger; stores only messages currently present on the device.
- Special note: SMS deleted on wearable remain on the companion mobile phone.

Samsung™ Gear S3 Frontier

Lack of a root connection caused some files to be inaccessible; however, a significant amount of data is still able to be acquired. It appears that the wearable device uses a common Linux directory, opt, to store all user and device specific data, making a full file system extraction unnecessary.

Acquired connected data: Device presents some limitations.

- Only the local device password can be identified; therefore, wearable does not appear to store any passwords related to the companion mobile phone, email, or 3rd party applications.
- All emails except a draft created by the companion mobile phone were found, suggesting either an issue with default sync interval settings or an inability to store email data local to the mobile phone.
- Connected SMS, MMS, & Browser Activities were not identified, suggesting that the wearable does not store any data for these functions.

Acquired standalone data: At least a portion of all data can be identified.

- Location/Samsung Health data for the range of dates populated exists, but is encrypted; however, tracked routes for both workouts were found.
- Specifically typed search queries could not be identified; however, results of queries were attainable and offered a snapshot of the user's intent.

Special notes: The wearable is the only source of Alarm data, both connected and standalone.

It is evident that the Samsung™ Gear S3 is capable of storing similar amounts of data, if not more, compared to the Samsung™ Galaxy S8.

Apple® iPhone® 6

Although most of the artifacts found were limited in information, the Apple System Logs contained insight into the directory structure of the Apple Watch Series 3.

Acquired connected data: Device stores the majority of data with two exceptions.

- Apple Maps location data originating from the wearable device could not be identified, suggesting that the companion mobile phone does not store these events and no record of them would exist.
- Phone-originating deleted SMS could not be identified; however, SMS deleted on the wearable remain on the companion mobile phone.

Acquired standalone data: Device stores all data except outgoing calls originating from the wearable device.

- The wearable device is assigned its own phone number by the cellular network provider and simply mirrors the companion mobile phone's number. The above result suggests that when dialing from the wearable, calls are utilizing the wearable's assigned number while under the guise of the companion mobile phone; therefore, nothing is stored.

Apple Watch® Series 3

As a result of the limited extraction methods able to be performed at this time, only data which can be manually examined on the wearable device's screen is able to be identified.

- Xcode®, an open-source application development tool, allows for native screen captures to be taken, which can greatly improve efficiency of manually documenting displayed content.

References

[1] PERF Reports. Washington (DC): Police Executive Research Forum; 2018. New National Commitment Required: The Changing Nature of Crime and Criminal Investigations.
[2] RAND Research Reports. Santa Monica (CA): RAND Corporation; 2015. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence.
[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.

Acknowledgements

Thank you to the Virginia Department of Forensic Science and the Digital & Multimedia Evidence analysts at the DFS Central Laboratory for this opportunity and resources, as well as guidance and advice. 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.