Watch Your Smartwatch

Manal Al-Sharrah*, Ayed Salman†, Imtiaz Ahmad‡
Department of Computer Engineering, Kuwait University
Email: *manal.alsharah@grad.ku.edu.kw, †ayed.salman@ku.edu.kw, ‡imtiaz.ahmad@ku.edu.kw

***Abstract*— Smartwatches are trending devices that give its users the ability to be connected, send/receive emails and messages, keep track of health and fitness, and even make calls on the go. Despite these benefits, the disadvantages of smartwatches can be equally terrifying. Smartwatches contain sensitive data and useful information that could be misused if a smartwatch gets lost or stolen. This paper develops a framework to do forensics for smartwatches according to three analysis stages: physical, backup, and wireless communication. We followed the proposed framework using Apple Watch. We found that the watch stores a lot of personal information such as contacts details, text messages, calendar details, Emails, pictures, and wallet data including: stored payment cards, gate passes, and event tickets, if any. In addition, the logical acquisition of the backup files revealed to us that more sensitive information such as the user's secure ID, Wi-Fi, Bluetooth, and MAC addresses can be extracted directly from the backup. Therefore, users must encrypt their backup files to keep their personal data secured. Based on our experiment, we believe that a smartwatch can be used as a valuable evidence for forensic investigators and a more advanced framework must be further developed in this emerging field.**

Keywords— smartwatch; smartwatch forensic; wearable devices; wearable forensics; artifact analysis; Apple smartwatch

I. Introduction

The field of wearable technology is one of the most trending fields to emerge these days and it is forecasted to continue growing due to the high increasing demands. Along with the growth in this field, the trends in consumer applications development is also increasing. The first growth period in the development of wearable technology was from 1980s to 1997 where it was known as the technology driven period [1]. The spreading of wearable applications continues to grow over a range of products and even as applications instances over the body area such as: smart jackets, smart gloves, smartwatches …etc. The survey in [1] evaluates different wearable technology applications and shows how smartwatches have become dramatically dominant in the current market trends capturing 35% of the market size compared to its old value of 8.7%. Smartwatches are devices that are capable to be linked to your smartphone, or even function as standalone devices, and perform many functions that go beyond timekeeping such as: messaging, making/receiving calls, playing media, monitoring health through a range of sensors, and provide alert notifications [2].

Many scholars have investigated how and why consumers use smartwatches in their daily life. There are a lot of factors that can affect the consumer's option in adopting a smartwatch in which some could be psychological reflecting the consumer beliefs that owning a wearable technology device will enhance their status in a social system [3]. While some people buy smartwatches as a fashion accessory to improve their image, others care to obtain a smartwatch for technical reasons. The usage of smartwatch can alternate between a general usage or specific user case scenarios. A survey in [4] explores the daily use of smartwatch. The researchers used wearable cameras to monitor the daily activities of smartwatch for 12 participants. It was found that most smartwatch consumers use their smartwatches as an augmented traditional watch. Other usage is to check notification, monitor health, or to use the smartwatch as an entertainment device. While the general use of smartwatches reflects the standard functionalities that the smartwatch is built for, the second type of usage can be more scenario-specific as found in [5] and [6].

Considering such high functionalities led to a great potential in the wearables market. The increasing demands on the global smartwatch market will give the market a potential to reach $32.9 billion by 2020 [7]. While the rapid growth of smartwatches continues to bring numerous benefits, the hidden risks are also need to be considered. A smartwatch can contain and store valuable data that could also comprise personal user information. Many of these smartwatches keep track of its users' activities such as: GPS locations, heart rate monitoring, personal information, and many more. Therefore, if a smartwatch is misused, it could reveal sensitive information. An experiment in [8] proves how a smartwatch could be used to capture user's information and computing activities using the smartwatch's ambient light sensors. The results of this experiment show the security vulnerabilities in smartwatches.

The sensitivity of the personal user information is highly important and it must be extremely secure. Unfortunately, a study done by Fortify, HP's security testing group, shows that most of the smartwatches in the market suffer from major security vulnerabilities that make them an easy target for hackers [9]. Because wearables are very limited in size, this lead to many difficulties in establishing a good authentication techniques. The researchers in [10] classify the authentication methods in wearables into three categories: tokens, passwords, and biometrics. Such authentication procedures are needed since wearables are mostly on and they are located closely to the users. Therefore, they carry rich-full information as they directly sense and measure data using built-in sensors. From this point, one can imagine how much sensitive data is carried in wearables and how important it is to keep such devices secure and safe.

In this digital era, we have more information stored in digital forms. Therefore, the field of cyber security is becoming more demanding since digital information is being used in criminal activities. Digital forensic will help in analyzing important data efficiently and highlight any critical

978-1-5386-4680-9/18/$31.00 ©2018 IEEE

information that can assist investigators in their work. We can assume that almost every case has digital aspects whether directly related to a crime, or can help in solving it. Computer forensic science is the field of science which studies and investigates data found on digital devices. The history of this field goes back in 1984 where the FBI Laboratory, along with other agencies, started developing programs to inspect computer evidence [11]. When dealing with a digital evidence, it must be taken into consideration that data should be not changed or modified in order to be forensically accepted as an evidence in any case. Thus, when data is being acquired for an investigation, it must be preserved, copied, and then the copied data will be analyzed for investigation. Digital evidence can expose how a crime was committed, help in any investigation process, and expose possible suspect [12]. Nowadays we can find wearables scattered everywhere. Hence, the chances of using such devices as evidence is very high.

At the time of writing this paper, there are many forensic analysis works done for wearable devices but very few on smartwatch forensics, especially on Apple Watch. Since smartwatches are one of the most trending technologies, it will be very important to define a methodology on how to obtain valuable evidence that are forensically accepted. This paper focuses on smartwatch forensic and investigates what type of information smartwatches could store. A methodology along with the process for extracting data will be explained in details. The organization of the remainder of the paper is as follow: section II will survey the literature and lists similar conducted works and studies on the security analysis of smartwatches. Section III will briefly lists the technical specs and explain a high-level architectural diagram of Apple Watch. Section IV will introduce the proposed methodology of smartwatch forensics to explore what hidden files or meaningful data could be retrieved from smartwatches while section V will show the proposed methodology applied on Apple Watch. Section VI concludes the paper with a summary and recommendations.

II. Literature Survey

A preliminary work demonstrated in [13] proposed a forensic mechanism for acquiring data from two different smartwatches. The aim of the research was to identify security mechanism of LG-G and Samsung Gear 2 Neo smartwatches to explore data management and propose a method for data acquisition. The study focuses on extracting data from the connected smartphone and the smartwatch itself. The researchers were able to recover most of the data along with other useful information. They also concluded that obtaining the image from Samsung Gear 2 Neo is more forensically acceptable than the method used to acquire data from LG-G watch where they had to reset it to its factory settings. On the other hand, the paper in [14] extracts a physical image from Samsung Galaxy Gear without resting it, using the mini-USB port. The analysis result of the image shows that there is data stored in the internal memory of the watch such as: event log tags, calendar information, pictures, web bookmarks, and encryption keys. Similarly, another analysis for an Android smartwatch is done in [15] in which a Sony smartwatch is used in an experiment to explore the stored information and analyze it forensically. The researches determine the location that Android Wear device stores information which is in the \dev partition and the memory chunks in running operating system with names like `mmcblk[#]p[#]`. The image analysis is captured in three locations: cache memory, system memory, and user data memory where the latter is the crucial location in which the users' settings and applications are included. The paper analyzes important artifacts such as: paired device information, Bluetooth packet analysis, logging system, notifications, and DropBox artifacts.

One can notice that most of the forensic analysis work done for smartwatch was based on Android Wear operating system. This is due to the flexibility of the Android system and the open source model that it follows. In general, the analysis process of imaging an Android smartwatch contains four stages. First, preparing the smartwatch access. During this step, the smartwatch must be connected with a permitted device and mostly an application need to be installed on the mobile to manage the settings of the watch. Next, the synchronization between the mobile and the smartwatch must be carried out using the available communication methods, either NFC or Bluetooth. The third stage is rooting the smartwatch in order to gain root access or in case the smartwatch contains a USB port, the USB debugging mode must be activated. The final stage is where the actual imaging is performed and analyzed using the available tools summarized in Table I.

A blog in [16] investigates Apple Watch forensically and conducts an advanced logical acquisition with the synced iPhone to study the offline activities of the watch. The result of the acquisition shows that the watch stores inbound and outbound messages, screenshots, and stored Apple Pay cards. Examining Apple watch closely has lead the investigator to notice that the watch syncs the information to the cloud even when it's not connected to the iPhone. One can notice how important it is to study and look at the device architecture in order to have a general knowledge of how the device is behaving as a one unit. The next section will introduce a high-level architectural overview of Apple Watch series 1 that is carried out in this study.

III. Technical Specs and Architectural Review

The first Apple Watch [17] is designed with 8 GB memory, 512 MB RAM, and a dual-core processor running watchOS 1, upgradable to v3.1, allowing great multitasking capabilities. Unfortunately, there is no input port, like mini-USB, to exchange data with the computer so the watch depends highly on its communication with the iPhone using Bluetooth 4.0 or Wi-Fi. The watch features heart rate sensor, accelerometer, gyroscope, and ambient light sensor giving it a great ability to collect personal data. Its worthy to mention that Apple didn't officially announce about the existence of a diagnostic port in the watch which is a six-pin hidden port located inside one of the watch's sides under the removable band. This port is completely covered with a metal panel, most probably to secure its functionality. To investigate more about this hidden port to know whether it can be used to transfer data, we contacted Apple support team but they assured that they kept this port hidden intentionally for their diagnostic usage only and not to be used by end users in any forms.

The Apple S1 is the brain of the Apple watch. Its identified as System in Package (SiP) where the single chip contains

TABLE I: Summary of Helpful Tools for Digital Forensic

Tools	Function	Found in Resources
.XRY Logical	Logical image acquisition from a smartphone	[13]
Access Data FTK Imager	Forensic toolkit for creating and analyzing forensic image.	[14, 15]
Android ADT Bundle	Android developer tools.	[14]
Android SDK tool	Android software development kit	[14, 15]
Autopsy	Open source forensic image analyzer.	[13, 14]
Cellebrite Case with Accessories	Cellebrite forensic kit containing additional tools.	[13]
Cellebrite Physical Analyzer	Physical image analyzer.	[13, 16]
Cellebrite UFED 4 PC	Physical image acquisition from a smartphone.	[13]
HEX editor	Software for reading and analyzing hexadecimal files.	[15]

multiple integrated devices. The Apple S1 chip contains many components like: CPU, GPU, memory, sensors …etc. The chip is equipped with a 520 MHz CPU and the main memory contains 2 levels of cache with 32 KB and 256 KB respectively along with an 8 GB Flash memory [18]. With this great storage, we can hypothesize that the watch will be able to store a good amount of data internally and independently from the synced mobile device.

IV. Methodology

In order to perform a forensic analysis for smartwatches, we suggest a framework to do forensic according to three different stages listed and explained below.

A. *Physical Analysis*

When a smartwatch is found as a piece of evident, it should be kept safe to be forensically accepted as an approved evidence in the court. In order to prevent any data changes, imaging techniques shall be performed to do data acquisition. The imaged copy then will be examined after being validated with the calculated encryption keys to guarantee that there are no data modifications during the imaging process. Investigating the copied image of the evidence will require the examiner to trace every file, look-up for any hidden data, or even extract deleted files. In the physical analysis stage in this experiment, we will explore all the internal stored information to examine what type of data one could retrieve if he/she gets a physical access to the watch itself.

B. *Backup Analysis*

Having the possibility to explore the backup data of any smartwatch could reveal a lot of useful stored information. Since most of the smartwatches require to be synchronized and connected with a smartphone, the backup of a smartphone that is synced with the watch will contain useful data. In the backup analysis stage, we will examine what type of data in Apple Watch is being synced with the iPhone through investigating the iOS backup of the iPhone in depth.

C. *Wireless Communication Analysis*

Since wearables are mostly always-on devices, the Wi-Fi and Bluetooth in Apple Watch is always activated for synchronization purposes with iPhone. Exploring what data is communicated wirelessly is important to see the transferred data and how secure the packets are. Hence, we suggest that a wireless communication network analysis is important to be carried out in any forensic investigation.

V. Forensic Analysis For Apple Watch

In this experiment, we carried out the previously suggested methodology using Apple Watch series 1. The investigation of each stage along with our findings will be discussed and listed in detail in the following sections.

A. *Physical Analysis*

If one gets a physical access to Apple Watch, a lot of information can be viewed even when the watch is disconnected from the synced iPhone. Since investigators can't work directly on the evidence, the first step in the acquisition is to take a complete physical image of Apple Watch to analyze it. Apple Watch lacks any input/output ports to extract data directly from the computer. Hence, a logical acquisition must be performed. A blog in [16] conducts an advanced logical acquisition for iPhone to examine data in Apple Watch. The researcher proves that the watch contains data independently of its synced iPhone and it can be used as a standalone communication device. Most of the data on the Apple Watch were all retrieved including the pictures, messages, and the stored payment credit cards. The examiner was also able to send and receive messages using the iMessage application even though the synced iPhone was off since the watch stores the network data of the pre-authenticated Wi-Fi network from the synced iPhone. Exploring more about Cellebrite Physical Analyzer capabilities revealed to us that the software can even performs a logical extraction even on a locked iPhone using the `.plist` files. The lockdown folders are found on MAC in:

```
/private/var/db/lockdown
```

In the second part of the physical analysis method, we examined the data on the Apple Watch as a standalone device. We set Apple Watch on airplane mode to avoid any network connections with other devices, we even turned off the paired iPhone. Once we guaranteed the access to Apple Watch, we were able to access all the pre-installed application along with the 3rd party applications. However, most of the 3rd party applications required a connection with the synced iPhone to retrieve data. On the other hand, the data of Apple's preinstalled applications, such as iMessage, were all viewable because it's stored internally on the watch. We were able to view all the chats in iMessage including the attached links in the chats and pictures. An interesting finding is that we were able to view old messages although they were deleted from the iMessage application on the iPhone before syncing it with the watch. We repeated the experiment and opened the iPhone to re-sync it again with the watch to make sure that the last data will be synced but we were still able to see some old deleted messages in the watch. Therefore, we can conclude that Apple Watch keeps the old data in its internal cache memory. In addition to the messages, we were able to access the following data:

- Phone book information; full access for contacts data including favorite contacts name and numbers
- All stored media, remainders, tasks, calendar details, and activity information
- Emails inbox messages
- Wallet data; including the stored payment cards, events details, and gate passes

B. Backup Analysis

We analyzed the iOS backup of the iPhone to examine the synced data between the watch and mobile. We found the acquisition via the iOS backup in the following location on MAC:

```
/Library/ApplicationSupport/MobileSync/Backup
```

The `Manifest.plist` file contains the metadata about the backup files. The actual files that contain the data are hashed. In order to read such files, there are many popular available tools to review the backup data. We used iExplorer to read and export all the files in iOS backup. After syncing the iOS backup with iExplorer, we viewed the backup files in depth. We found the general information about the watch such as: watch name, model, serial number …etc. in the following location:

HomeDomain/Library/DeviceRegistry.state/history.plist

In order to view the `.plist` file in MAC, we used XCode to read the data in the file. Fig. 1 shows part of the data found in `history.plist` file which contains general information about the watch. On the other hand, the path of the file below allowed us to view all the secure information of Apple Watch such as: serial number, Wi-Fi MAC address, Bluetooth MAC address, device identifier …etc. as shown in Fig. 2.

HomeDomain/Library/DeviceRegistry.state/historySecureProperities.plist

While exploring the backup files, we noticed that Apple organizes all the watch's synced folders inside sub-directories and identifies those folders with the word Nano in the beginning of the name of the folder to distinguish them from the iPhone folders. All the installed watch applications are organized under the following application directory:

HomeDomain/Library/DeviceRegistry/<userID>/NanoAppRegistry/Applications

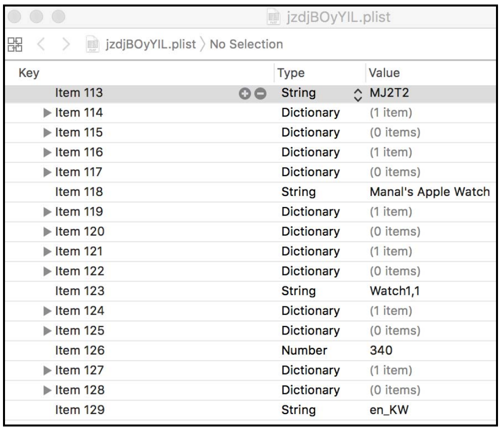
Inside this file location, each application has its own folder and the information of the application is stored inside this folder. For example, inside the NanoMail folder, we found a SQL database file named `registry.sqlite.` It turns that the file stores all the emails accounts inside the watch along with a unique ID. In addition to the emails account information, all the favorite contacts along with number are stored in the AddressBook folder in a file called `Favorite.previous` as shown in Fig. 3.

The user's preferences are all stored in different folders depending on the nature of the settings. For example, all the synchronization preferences are stored in the `PairedSyncServiceRestrictions` folder. It defines whether the end user likes to pair and sync his data with other applications or not. The folder contains many files holding only Boolean values of true/false to indicate if the access of pairing and syncing is granted.

Another file of interest is finding where the Apple's Wallet data is stored since this application stores boarding passes, credit cards, event tickets …etc. This folder contains sub-folder of the payment cards where the information of the credit cards is stored. In addition, the folder holds a SQL file which is `nanopasses.sqlite3` where the event tickets are stored. We were able to extract the information of a stored event ticket including the event ID, type, and name. Fig. 4 shows part of the file. The data is found in the following path:

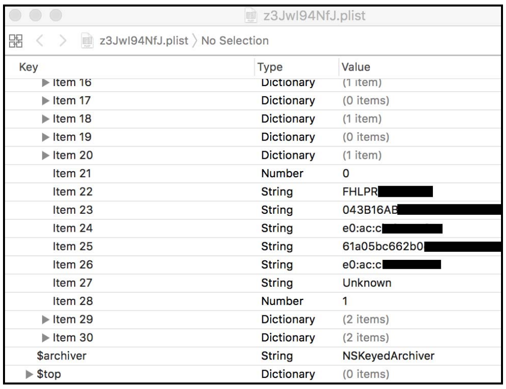
```
HomeDomain/Library/DeviceRegistry/<userID>/NanoPasses
```

Investigating the backup file proved to us that the watch keeps a lot of sensitive user data information. However, not all data are directly stored or even synced in the backup. For example, we were expecting to see the health data, such as heart rate, saved in the watch but this was not the case. Apple's Health application requires direct syncing with the paired iPhone to retrieve data. We found that most of the third party applications require such connection. Hence, we assume that the data on the watch is only mirroring the actual stored data on the iPhone. One way to validate such assumptions is to study and analyze the network Bluetooth/Wi-Fi traffic to see what type of the data is exchanged. This step must be explored in the Wireless Communication Analysis stage.



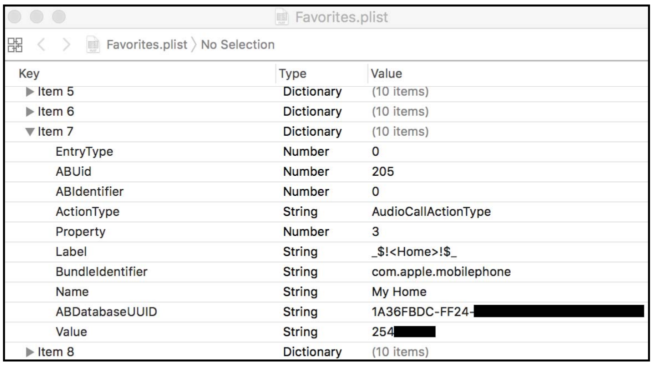
Key	Type	Value
Item 113	String	MJ2T2
▶ Item 114	Dictionary	(1 item)
▶ Item 115	Dictionary	(0 items)
▶ Item 116	Dictionary	(1 item)
▶ Item 117	Dictionary	(0 items)
Item 118	String	Manal's Apple Watch
▶ Item 119	Dictionary	(1 item)
▶ Item 120	Dictionary	(0 items)
▶ Item 121	Dictionary	(1 item)
▶ Item 122	Dictionary	(0 items)
Item 123	String	Watch1,1
▶ Item 124	Dictionary	(1 item)
▶ Item 125	Dictionary	(0 items)
Item 126	Number	340
▶ Item 127	Dictionary	(1 item)
▶ Item 128	Dictionary	(0 items)
Item 129	String	en_KW

Fig. 1. General Information in History Backup File.



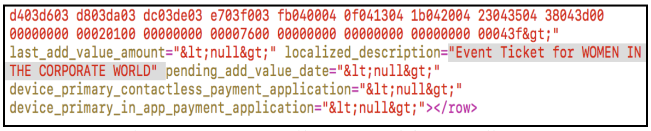
Key	Type	Value
▶ Item 16	Dictionary	(1 item)
▶ Item 17	Dictionary	(0 items)
▶ Item 18	Dictionary	(1 item)
▶ Item 19	Dictionary	(0 items)
▶ Item 20	Dictionary	(1 item)
Item 21	Number	0
Item 22	String	FHLPR[redacted]
Item 23	String	043B16AB[redacted]
Item 24	String	e0:ac:c[redacted]
Item 25	String	61a05bc662b0[redacted]
Item 26	String	e0:ac:c[redacted]
Item 27	String	Unknown
Item 28	Number	1
▶ Item 29	Dictionary	(2 items)
▶ Item 30	Dictionary	(2 items)
$archiver	String	NSKeyedArchiver
▶ $top	Dictionary	(0 items)

Fig. 2. Secure Communication Data.



Key	Type	Value
▶ Item 5	Dictionary	(10 items)
▶ Item 6	Dictionary	(10 items)
▼ Item 7	Dictionary	(10 items)
EntryType	Number	0
ABUid	Number	205
ABIdentifier	Number	0
ActionType	String	AudioCallActionType
Property	Number	3
Label	String	_$!<Home>!$_
BundleIdentifier	String	com.apple.mobilephone
Name	String	My Home
ABDatabaseUUID	String	1A36FBDC-FF24-[redacted]
Value	String	254[redacted]
▶ Item 8	Dictionary	(10 items)

Fig. 3. Favorite Contacts Details



```
d403d603 d803da03 dc03de03 e703f003 fb040004 0f041304 1b042004 23043504 38043d00
00000000 00020100 00000000 00007600 00000000 00000000 00000000 00043f&gt;"
last_add_value_amount="&lt;null&gt;" localized_description="Event Ticket for WOMEN IN
THE CORPORATE WORLD" pending_add_value_date="&lt;null&gt;"
device_primary_contactless_payment_application="&lt;null&gt;"
device_primary_in_app_payment_application="&lt;null&gt;"></row>
```

Fig. 4. Events Details Extracted from Wallet Data

VI. Conclusion

This paper suggests a framework to do forensics for smartwatches according to three different stages. Our experiment with Apple Watch revealed that a lot of information is stored internally in the watch regardless of its paired iPhone such as: text messages, phone book information, and pictures. We were also able to locate a deleted message. Investigating the backup files assured to us that a lot of sensitive data can be found within the backup files such as wallet data, Wi-Fi, Bluetooth, and MAC addresses. Since the backup files keep track and store a lot of sensitive data, we recommend that the backup data must be encrypted to keep personal data secured. As for future work, the wireless communication stage must be explored to see what packets the watch transfers and receives to and from the paired iPhone. Since Apple doesn't allow a direct pairing between Apple Watch and any other device than the iPhone, we suggest that this stage must be carried out using hardware sniffing tools. This stage concludes our proposed methodology to do forensics for smartwatches but we still believe that a more advanced framework must be developed in this area.

VII. References

[1] M. E. Berglund, J. Duvall, and L. E. Dunne, “A survey of the historical scope and current trends of wearable technology applications,” in *Proceedings of the 2016 ACM International Symposium on Wearable Computers*. ACM, 2016, pp. 40–43.

[2] M. E. Cecchinato, A. L. Cox, and J. Bird, “Smartwatches: the good, the bad and the ugly?” in *Proceedings of the 33rd Annual ACM Conference extended abstracts on human factors in computing systems*. ACM, 2015, pp. 2133–2138.

[3] S. H.-W. Chuah, P. A. Rauschnabel, N. Krey, B. Nguyen, T. Ramayah, and S. Lade, “Wearable technologies: The role of usefulness and visibility in smartwatch adoption,” *Computers in Human Behavior*, vol. 65, pp. 276–284, 2016.

[4] S. Pizza, B. Brown, D. McMillan, and A. Lampinen, “Smartwatch in vivo,” in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 5456–5469.

[5] G. Reyes, D. Zhang, S. Ghosh, P. Shah, J. Wu, A. Parnami, B. Bercik, T. Starner, G. D. Abowd, and W. K. Edwards, “Whoosh: non-voice acoustics for low-cost, hands-free, and rapid input on smartwatches,” in *Proceedings of the 2016 ACM International Symposium on Wearable Computers*. ACM, 2016, pp. 120–127.

[6] M. Nebeling, A. Guo, A. To, S. Dow, J. Teevan, and J. Bigham, “Wearwrite: Orchestrating the crowd to complete complex tasks from wearables,” in *Adjunct Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*. ACM, 2015, pp. 39–40.

[7] A. M. Hickey and P. S. Freedson, “Utility of consumer physical activity trackers as an intervention tool in cardiovascular disease prevention and treatment,” *Progress in cardiovascular diseases*, vol. 58, no. 6, pp. 613– 619, 2016.

[8] A. Holmes, S. Desai, and A. Nahapetian, “Luxleak: capturing computing activity using smart device ambient light sensors,” in *Proceedings of the 2nd Workshop on Experiences in the Design and Implementation of Smart Objects*. ACM, 2016, pp. 47–52.

[9] P. Alto. Hp study smartwatches vulnerable to attack. [Online]. Available:http://www8.hp.com/rs/sr/m/news/details.do?id=2037386& articletype=news release

[10] A. Bianchi and I. Oakley, “Wearable authentication: Trends and opportunities,” *it-Information Technology*, vol. 58, no. 5, pp. 255–262, 2016.

[11] M. G. Noblett, M. M. Pollitt, and L. A. Presley, “Recovering and examining computer forensic evidence,” *Forensic Science Communications*, vol. 2, no. 4, pp. 1–13, 2000.

[12] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press, 2011.

[13] I. Baggili, J. Oduro, K. Anthony, F. Breitinger, and G. McGee, “Watch what you wear: preliminary forensic analysis of smart watches,” in *Availability, Reliability and Security (ARES), 2015 10th International Conference on*. IEEE, 2015, pp. 303–311.

[14] S. L. Erin Poremski. Galaxy gear smartwatch forensics. [Online]. Available: http://selil.com/wp-content/uploads/2013/10/581-midterm.pdf

[15] P. H. Rughani and M. Dahiya, “Analysis of android smart watch artifacts,” *International Journal of Scientific & Engineering Research*, vol. 6, no. 8, 2015.

[16] G. Danny. Apple watch - investigative and forensic implications. [Online]. Available: http://cell4n6.com/1/post/2015/06/ apple-watch-investigative-and-forensic-implications.html

[17] Apple. Apple watch series 1 technical specifications. [Online]. Available: https://support.apple.com/kb/SP745?locale=en US

[18] Wikipedia. Apple s1. [Online]. Available: https://en.wikipedia.org/wiki/ Apple S1e