Forensic Analysis of Fitbit Versa 2 Data on Android

Yung Han Yoon and Umit Karabiyik *

Abstract: The increase in the adoption of wearable fitness trackers has led to their inclusion as valuable evidence used by law enforcement during investigations. The information available in these fitness trackers can be used by law enforcement to prosecute or exonerate an individual. Wearable fitness devices are constantly being released by companies, with new firmware created for each iteration. As technology developers, research and law enforcement must keep pace to take advantage of data that can be used in investigations. The Fitbit line of devices is a popular brand of wearable trackers. This study will investigate what artifacts are generated by the new Fitbit Versa 2 by investigating what data are generated and stored on the smartphone app component of the new device. The artifacts discovered will be related to areas of forensic interest that are relevant to a law enforcement officer or digital forensics practitioner. Previous research and their methodologies used for application and mobile forensics will be used to conduct this research. This study finds the Fitbit Versa 2, and by extension, the Fitbit smartphone application does not store social media message notifications pushed to the tracker by the user’s mobile device. Some credit card information, health-related data, such as heart rate, GPS locations, and other potentially identifying data were found in plaintext. While the exposed data is not enough on its own to pose an immediate serious issue, it can be used as leverage to phish a user for further details.

Keywords: data privacy; digital forensics; internet of things; mobile forensics; security; wearable

1. Introduction

Wearable fitness trackers, such as those produced by Fitbit, Garmin, Samsung, and XiaoMi, are becoming more and more prevalent in society. As the popularity of wearable devices increases, their role in society has expanded and developed from being simple fitness trackers to health monitoring devices. This data includes medical information like heart rate and location information from GPS. This type of information, like heart rate, could be indicative of a person’s physical exertion or stress levels during a time frame relevant to a criminal investigation. For example, during a domestic violence case, a person may claim to be at home relaxed, but an elevated heart rate could show that they were physically active during that time frame, which could indicate that they made a false statement. The evidence contained in these devices have been used to incriminate and subsequently charge people for murder and other crimes in a substantial number of cases [1–3]. As such, these devices have a large potential to change the course of an investigation as new facts are discovered. The academic research needs to keep up with new technologies being developed for these devices, as well as newer models entering the market.
Wearable devices are also gaining more importance in technological developments beyond personal wellness trackers as they become key components in newly proposed systems. One such proposed system uses wearable medical devices to relay medical emergencies of a vehicle driver to their autonomous vehicle in order to trigger an emergency response that would save the driver’s life by bringing them to the nearest emergency center [4]. Other researchers note how wearable devices and their ability to sense and track events related to health parameters, such as body movement or vital signs, is an important feature being used in the medical observation of patients [5].

The forensics and academic communities have taken keen interest in investigating possible opportunities for research in these devices as their potential impact grows. Forensic artifacts and data stored by these wearable devices on their companion smartphone apps have been examined [6] in an attempt to determine what privacy concerns there may be, as well as what potential evidence exists that could be used in law enforcement. The security of these devices has also received significant attention from researchers as stored medical health information on these small devices represent a severe privacy risk.

There is an obvious need for forensic investigators to keep up to date on techniques and best practices used to acquire generated data, as well as research what pieces of evidence can be gathered from the newest devices being used by the consumer due to the increasing importance of wearable fitness trackers for both law enforcement and their increasing prevalence in various other important industries.

The Fitbit Versa 2 is a new device released by Fitbit Inc. In 2018, Fitbit sold over 13.9 million units worldwide, serving 27.6 million users [7]. A new device, Fitbit Versa 2, was released in September of 2019, and it boasts a few new features that have potential privacy and security implications. As Fitbit is a well-known brand, there is a high likelihood that these devices will see a moderate level of adoption and it may become a source of evidence during an investigation. This paper will examine the features and artifacts generated by the Fitbit Versa 2 and then stored by the Fitbit mobile smartphone application onto mobile device storage.

The contributions of this paper are as follows:

- Providing a detailed understanding of the artifacts generated by the new Fitbit Versa 2 line of trackers and its newly developed features.
- Improving the current literature regarding what forensically relevant artifacts are produced and where they are located.
- Evaluating the user data privacy concerns in a product that is likely to see a significant number of adopters.

2. Background and Related Work

Digital forensics is generally used when evidence of an event needs to be found, and the medium on which the evidence is available is digital in nature. These events could be related to law and crime, such as determining the location of a suspect at a specific time of day, or civilly related, such as determining whether a spouse had committed adultery. In both regards, the outcome of the investigation is critical, as it may significantly impact people’s lives. As such, digital forensics is a growing academic area, with increasing standards and organizations being established to improve upon the subject’s reliability, accuracy, and integrity. The core aims of digital forensics are to collect digital evidence, preserve its integrity, and analyze the data in order to answer questions pertinent to the case.

We can obtain a quick overview of how digital forensics is conducted by looking at one of the more established standards on digital forensics published by the Scientific Working Group on Digital Evidence (SWGDE). The SWGDE Best Practices for Computer Forensic Acquisitions generally outlines the digital forensics acquisition process as follows [8]:

...
1. Prepare the examiner’s tools and software prior to the acquisition or arriving on site.
2. After reaching the site, consider environmental factors, usage of encryption, and boot loader restrictions.
3. Triage all of the devices by previewing the data being acquired to ensure that only the right and relevant data is being copied.
4. Perform the acquisition using a variety of software and techniques after isolating the device and ensuring data will not be changed, depending on the state of the computer or requirements of the subsequent examination and analysis.
5. Verify the integrity, accuracy, and relevancy of the acquired image.
6. Document steps taken.
7. Preserve the acquired data by making a duplicate, repeating the verification steps when needed.

Subsequently, the acquired data must be analyzed, which is also mentioned in SWGDE’s Best Practices for Computer Forensic Examination. However, with regard to the actual analysis of data, the standards are not strictly defined, and the only suggestions are to be prepared and conduct the examination in a controlled, isolated, known environment. Tools and software being used should be tested and validated prior to the examination [9]. Analysis of an image can vary and would differ based on the preferences of the examiner, and the nature of the case being worked on. From these two documents, we can establish how digital forensics is conducted.

Data in traditional computer forensics are acquired in order of most to least volatile. Volatile data would be considered data that could be lost when the device loses power; for example, data that are stored in Random Access Memory (RAM). While data stored on disk is less likely to be corrupted or lost, and as such, it is acquired later on. Digital forensics also uses tools, such as write blockers, with physically prevent modifications being made to a connected computer hard drive.

Other research in digital forensics has attempted to improve upon the way digital evidence is stored. Current forensics software, such as AccessData’s FTK Imager or Encase, are generally able to store forensic copies of the devices being acquired as evidence in a few different formats. However, the way these formats are structured has costs and benefits in terms of the speed in which data analysis software can process them, as well as the information they can contain in a compact form. Moreover, in digital forensics, new disk image formats are being proposed, such as the Advanced Forensic Format (AFF) [10].

Research in digital forensics also concerns the development of new models and procedures to address new challenges or gaps in previously proposed models. New models, such as the Analytical Crime Scene Procedure Model (ACSPM), emphasizes preserving the integrity of acquired devices and give a clear workflow for investigators and law enforcement to follow in order to conduct digital forensics investigations while minimizing the possibility of errors [11]. ACSPM defines nine major steps to processing a scene, which includes steps that manage and control the area, identify, and gather devices of interest, acquire forensic copies of the devices, analyze and process evidence, and finally restore the scene to a functional state. According to the authors, this newly proposed model aims at addressing judicial and legal goals that were not addressed by other digital forensics models.

Mobile devices are commonly used in conjunction with wearable devices. These mobile devices generally use an application that manages and reports data collected by the wearable device. As such, we will need to look at mobile device forensics, as that will be the main focus of this research. Within the field of mobile forensics, some basic statistics show that it is a growing field with increasing relevance. As of 2019, 96% of Americans own a cellphone, while 81% of Americans own a smartphone [12]. However, mobile device forensics is different in significant ways from computer forensics. SWGDE has its own separate set of standards and best practices documented for mobile device acquisitions and analysis.

Some key differences between mobile forensics and computer forensics are the fact that there is no way to use write blockers on mobile devices [13]. Mobile device manufacturers also have
inconsistent standards used for both storing data, as well as the physical interfaces between device components \[13,14\]. Some mobile devices also lose data or have security features that can hinder access if powered off \[13\]. All of these additional challenges mean that mobile forensics is generally considered to be less robust when compared to computer forensics, as devices are acquired using industry-standard software by powering them up and running programs and custom operating systems on the device directly. The argument for forensic soundness is made by claiming that while the data on the device is being modified during the acquisition process, the user data remains intact. Additionally, sufficient documentation and testing of the tools’ effects on data can be used to identify what data is changed. Despite knowingly modifying data on the phone, we know which data has not been modified and can focus our investigation on that data only, thus maintaining the forensic soundness. Additionally, sufficient documentation and testing of the tools’ effects on data can be used to identify what data is changed. Despite knowingly modifying data on the phone, we know which data has not been modified and can focus our investigation on that data only, thus maintaining the forensic soundness. Mobile phone forensics does require the examiner to be careful with each phone, as differences in device manufacturers mean that data could be lost if the same methodology is followed for two different phone models. Otherwise, the digital forensics process for acquiring and examining mobile devices is similar to that of computers. The phone is still generally secured, isolated, connected to software and tools that acquire data, verified, documented, and then preserved \[13\].

Academic research has also been conducted focusing on specific smartphone applications and even application stores. Previous research in mobile application security has shown that applications available on the application store for their respective devices contain security vulnerabilities, despite what the manufacturers claim \[15,16\]. Forensics focused research of applications has also been conducted. Various articles look at how data are stored by these applications in order to establish methodologies to be used by practitioners to extract usable data \[17\]. One example is how social media applications, such as Facebook, use SQLite databases to store user data, which in turn requires the forensic examiner to extract the data accurately, posing an additional challenge to the forensic examiner \[15\]. Apple devices, given their prevalence, have also been investigated for forensic merit. Previous research has discovered where and how key pieces of information are stored on Apple mobile devices, such as which WiFi networks were connected to, camera pictures and videos, and third-party application data \[18\]. Desktop applications are also included in academic research. Windows Desktop instant messaging (IM) applications, such as Facebook and Skype, have also been examined to identify where important information is stored \[19\]. Researchers were able to find records of IM contacts, login events, and copies of transferred or deleted files \[19\]. The information found through their analysis is vital for the forensics field, as this information would be pertinent during investigations where communication between suspects is of key importance, or to establish a list of other parties who may be involved in the case.

The forensic merit of application-specific research is that it adds to current literature and can be used by forensic practitioners during their own investigations, saving valuable time and allowing the examiner to focus their energy on discovering other pertinent data. Previous research has been conducted on both mobile devices and traditional computer applications and found positive, useful results that help investigators find crucial information.

The system architecture used by Fitbit will have a high impact on what data is stored by the device, smartphone, and cloud. There are two forms of fitness tracker system architectures: dumb phone client and smart phone client. Both architectures use a cloud server either as a data syncing and storage service in the case of thick clients, or for actual data processing, interpretation, and visualization for thin clients \[20\].

Even though cloud services are out of scope for this paper, the possible existence of dumb and smart clients means that there may be a marked difference in terms of what data is stored locally, and how it is stored. This will have forensics implications while searching for malicious attacks against different client application types. In Fitbit devices, the wearable device sends data to the user’s smartphone, with the intent of pushing the data up to Fitbit’s cloud server. Important information is sent in one of two types of data transfers, which contain information, such as step count and distance
traveled [21]. These data transfers are end-end encrypted. With this information, we can gain a better understanding of how data is transferred between devices and what possible data may be available.

As the Fitbit Versa 2 fitness tracker does not have any GPS capability, it is safe to assume that GPS locations being recorded and displayed are recorded by the user’s smartphone. As such, we can expect there to be “small” data, such as step counts and distance traveled being recorded and potentially stored by the Fitbit tracker, while potentially more sensitive data, like location information, is recorded and stored solely on the mobile device.

Various previous studies into wearable tracking devices also provide us with the framework for an acceptable methodology to use while populating data, as well as acquiring and analyzing the smartphone app to see what potential new data is being stored. Recognized methods of extracting data from mobile devices, some of which will be used in this paper, include manual, logical, and physical extraction methods [22]. As this paper only concerns the data present on the smartphone device, the data acquisition method used must be recognized by the wider forensic community. Recognized tools that have been used for the of mobile data in previous work include Magnet AXIOM and MSAB XRY and have been tested by the National Institute of Standards and Technology (NIST) [23,24] to look for possible issues with the acquisition process.

The latest test of both MSAB XRY and Magnet AXIOM Process showed that MSAB XRY and Magnet AXIOM both might have issues obtaining all data from social media applications; however, they overall capture a large amount of data available on a device [23,24]. Data that had been missed are mainly certain messages and data from social media applications. While these benchmarks do not definitely prove that all Fitbit Versa 2 data will be acquired properly, it is impractical to expect benchmarks to test a tool’s ability to perfectly acquire everything from every application available to users.

Nevertheless, these tools are still overall quite robust and have been validated and approved for use by authorities, such as NIST. Therefore, these tools will be used in this study to investigate the data generated by the Fitbit Versa 2 and stored by the Fitbit Mobile smartphone application. The data stored on memory within the Fitbit Versa 2 is out of scope as the researchers do not have the skills and equipment necessary to extract that data using chip-off extraction techniques.

3. Methodology

We will have two primary perspectives to take for this research. The first perspective is that of law enforcement. If a case involving a wearable tracker has started, what information could be useful? Some examples of information that would be of interest to this perspective would be (1) data that establishes a person’s location at a specific time, (2) level of physical exertion in terms of heart rate, (3) personally identifiable information (PII), (4) contacts for the individual’s friends and associates, and (5) other data that could be used for attribution. This information could be used by law enforcement to corroborate a suspect’s statements, or even place them at the scene of the crime at the right time. If only a device were found at the crime scene, PII could also be used to establish that the property of an individual was found at the crime scene, leading to further questioning and investigation. Looking through the lens of law enforcement is important, as it allows for us to contribute to the literature that could aid in these important investigations.

The second lens we will use when evaluating our findings is that of a consumer. From the consumers’ perspective, privacy and security are highly valued. As such, any information that a consumer would want to remain private would be identified. This could include contacts, credit card details, their home address, contact information, and medical information. We take this lens as we feel that consumer data privacy and security is an important aspect, especially as wearable devices become medically related, which also needs to be addressed.
In order to fully test the Versa 2 and any new features implemented using a forensically sound method, the features list for the device was found from its store website. A testing methodology was then created for each feature that could have security implications if it was compromised. The main features that are listed in Table 1 below were taken from the Fitbit Versa 2’s online store page [25].

The mobile phone used in the study was a Samsung Galaxy S6 with Android 7 (Nougat), and the wearable device was a Fitbit Versa 2. The Samsung Galaxy S6 was used because the device was available to researchers at the time and was convenient. However, despite being used out of convenience, the S6 is still a popular device model. Data from the Device Atlas website show that the Samsung Galaxy S6 is still used quite regularly [26]. Web traffic data from 2019 shows that the S6 is still among the top 10 Android devices that were used to access their website in 8 countries: Canada, Germany, Norway, Netherlands, Ireland, Sweden, Portugal, and the United Kingdom [26]. While the United States had other Android devices that were responsible for more traffic share, it is safe to say that the S6 still has a significant market presence and it is a device that can be used for research without fear of it being irrelevant or obsolete. Besides, forensics experts may not have the luxury to pick and choose which devices they investigate. Relatively older models of phones, such as Samsung Galaxy S6, may appear in investigations, and this research can aid investigators in those situations.

| Feature to Test                       | Potential Concerns | Testing Method                                      |
|--------------------------------------|--------------------|-----------------------------------------------------|
| Alexa                                | Personal information leak | Using voice commands: queried weather, set alarm and calendar events |
| Exercise and Health Data (e.g., Heart Rate) | Health data privacy | Normal fitness tracker use |
| GPS Location Data                    | Privacy            | Normal fitness tracker use |
| Fitbit Pay                           | Financial privacy  | Linked credit card and made a purchase |
| Smartphone Notifications and Voice Reply | Privacy           | Used Skype and Discord messaging to create notifications |
| Alarms, Calendar events              | Privacy            | Set alarms and events using native applications |
| None                                 | Miscellaneous      | Root checker for acquisition verification stage |

In a similar vein, Android 7 is an older version of the operating system that is still being used. Statistics from 2020 show that Android 7 currently accounts for 6% of Android devices used between May 2019 and May 2020. However, other limitations exist as well due to the device being used. The Samsung S6 is no longer supported by the manufacturer as of 2018 [27]. Currently, the phone only officially supports Android 7 as its highest operating system version [28]. However, it is important to note that a cursory online search reveals that Android 8 has been installed on Samsung S6 devices, but these procedures are not official or released by the manufacturer and may involve loading third-party software. Android 7 can be used as a platform for research despite it being relatively old. In addition, these findings can still be relevant as third-party application data, in this paper the Fitbit application, may carry over across many Android versions as third-party applications are installed from the Google Play store on many different devices running different versions of the Android operating system. This would indicate that the user data needed for the app to operate should be present, regardless of the operating system version, on the device.

The mobile device must be wiped in order to study and analyze the data collection practices and security of the Fitbit app and a newly released device. First, the data storage encryption feature of the Android phone was activated. This ensures that data is encrypted while resting on disk. Taking a forensic image now would result in only viewing encrypted data. Next, the Android functionality of wiping a phone after a set number of sign-on fails was activated then purposefully tripped to trigger its wiping procedure. The phone was then factory reset after the Android security wipe had taken
place. The combination of disk encryption, triggering a device security wipe, followed by Factory Resetting the device should provide a clean device to work with.

After we set the phone to factory conditions, we installed a SIM card in the phone and then turned it on. We set up the phone as a new device while using a preexisting Google account for any basic requirements. A phone security pattern lock was enabled, and one of the authors was added as a biometric security option. These features are required in order to set up and enable the Fitbit Pay functionality that will be used later on. The data storage encryption feature was disabled to acquired data collected would be accessible. Data sharing features, such as sending usage data, were restricted as much as possible, but features that improved location accuracy were enabled to facilitate better results from the Fitbit application.

Next, the applications needed in order to test the device were installed from the Google Play Store. The applications installed are as follows:

- **Fitbit Application**—Required for pairing and collecting Fitbit data.
- **Discord**—Used to test notification system and message response system.
- **Skype**—Used to test notification system and message response system.
- **Root Checker**—Used to verify phone rooting process.

These applications were chosen to facilitate testing on as many features that were listed for the Fitbit Versa 2 device. Discord and Skype apps were used to send and receive messages so that they could appear on the Fitbit Versa 2’s screen. The pop-up notifications caused by these messages were then used to send a reply through the Fitbit Versa 2. The integrated Alexa feature allows the user to hold a button on the smartwatch to issue Alexa voice commands directly through the smartwatch. Alexa was then issued commands, such as reporting the time and local weather, to generate data that could be stored by the Fitbit app. Other features that will be tested also include Music Experience, Smartphone notifications, on-screen exercise and fitness related reporting, and Fitbit Pay. To clarify, these applications, Alexa, Discord, and Skype, are not in scope for the forensic analysis being performed. We will not be examining their data directories for artifacts. They are only being installed and run in order to create data that could then be retained by the Fitbit application during the smartwatch’s operation.

After installing the applications mentioned above, the Google account was removed from the device to avoid complications during imaging due to Factory Reset Protection. Subsequently, we created the image of the phone using MSAB XRY’s full logical image acquisition option. This image will be treated as the base, non-populated image.

The Google account was then re-added to the device, and the applications were set up appropriately with the new accounts. The Fitbit Versa 2 was then paired with the phone and updated. Notifications were enabled along with other features such as the use of Amazon Alexa. Exercise and location data was populated by walking around and starting the “Exercise” activity on the Fitbit Versa 2. The accurate recording of these exercises was verified by checking Fitbit’s website, which shows the duration of the activity as well as a geographic map that tracked the paths taken. This will populate the Fitbit’s step trackers, heart rate tracker, and GPS location data for the travel. The communication applications were then used to send various messages/files of different types, including text messages, pictures, mp3, mp4, docx, and pdf.

Moreover, we tested the Fitbit Pay application by linking a credit card through the Fitbit application and then making a purchase at a restaurant by scanning the Versa 2 against the credit card reader. An alarm was also set in Android’s native clock application as well as an event reminder in the calendar to push notifications out to the Versa 2 device. Finally, the integrated Alexa feature was tested using the Versa 2’s integrated Alexa support to set the alarm, report the local weather, and report local time.

We also created the second forensic image of the populated smartphone while using MSAB XRY’s full logical image method. This is the first populated image that is used to compare and contrast
findings between the forensic acquisition of the Fitbit application in rooted and unrooted smartphones. A third rooted device image was then taken using Magnet AXIOMS’ Full Physical acquisition method.

The populated device images, acquired with unrooted and then rooted privileges, were then opened in MSAB XACT and Magnet AXIOM Examine, respectively. Fitbit’s package directory and databases were analyzed to learn what artifacts generated were stored and able to be retrieved. The artifacts found were then compared and their security implications assessed.

As mentioned earlier, we rooted some phones in order to compare our results to unrooted phones. The rooting process was done using the custom recovery operating system, called TWRP [29], developed by the Team Win Recovery Project. The rooting software Magisk [30] and its corresponding interface application Magisk Manager was used in conjunction with TWRP to fully root the device. By rooting the device after populating data, we can use the Versa 2 device in a capacity similar to that of a normal end-user, then examine what artifacts are generated by both old and new features to see if any security or privacy issues exist in terms of data retained by the Fitbit Versa 2 and mobile application.

As the scope of this research is only concerned with the data stored by the smartphone device, we did not consider acquiring data in order of most to least volatile as only one data source was of interest to us, the smartphone. However, in a real investigation, law enforcement should aim to acquire data of the Fitbit Versa 2 first. Mobile forensics is a relatively established field; the storage of mobile devices are also relatively reliable and are likely less subject to be altered or modified than the storage of a small wearable device. Considering the amount of available storage and memory on a small wearable device such as the Versa 2, and the possibility that with each passing data could be overwritten, it would be prudent to assume that the data on the wearable device are more volatile and should be made a priority for acquisition.

During the entire investigative process, we followed nearly a complete digital forensics process. Initial wiping of the device is not part of the normal process but was done to ensure no residual data was acquired and could potentially interfere in the analysis process. After the mobile device was populated, the device was isolated from all networks using Airplane mode and treated as if it was a powered-on device discovered on a crime/incident scene. The device was then plugged into a forensic workstation, and instructions provided by the acquisition software MSAB XRY and Magnet AXIOM were followed as prompted to go through the acquisition process properly. After the image was created, the acquired file was duplicated, and the hash valued checked in order to ensure the duplicate working copies were identical.

A full list of the hardware and software used for this research is listed in Appendix A.

4. Investigation Results

In this section, we present the results we had after our thorough investigative processes. First of all, we found various database files and we examined them using Magnet AXIOM, MSAB XACT, and by exporting the files and viewing them through DB Browser for SQLite. The files and folders listed in Table 2 are all relative to the path: /data/com.fitbit.FitbitMobile/ directory were all manually searched while using the aforementioned tools, and the keywords used during the data population were searched for in the files.

Table 2 contains the artifacts of interest that were discovered and the corresponding locations that were found in. The root directory for the locations listed in the table is the com.fitbit.fitbit-Mobile package in the /data directory of the mobile phone.

No other artifacts that have any pertinence to the features being tested or have potential user security and privacy implication were present in the application. However, we were able to find GPS locations that were stored in plaintext, as depicted in Figure 1. Searching up the latitude and longitude data would allow us to track the user as they moved, while the correlated timestamp was in Unix Epoch time. Unix Epoch time is the number of seconds elapsed since 00:00 1 January 1970. As shown in Figure 2, we were also able to recover other logged data, such as average heart rate, calories burned, distance traveled, duration of exercise, and speed.
A database was discovered that had table columns that referred to details that would be found on a credit card, such as cardholder name and expiration date. However, despite the fact that the database was capable of storing credit card information, it contained no records, even though we had added a credit card to the Fitbit Versa 2 for testing (see Figure 3). It is possible that the credit card related data is kept in the cloud and only saved to this local database under certain conditions that were not reached during the data population. Due to the forensic significance of important data potentially being stored in this location, it was an important discovery, but more research is needed to determine what would trigger information to be stored here.

Table 2. Artifacts found at respective locations in Fitbit application under /data directory.

| Artifact               | Data Type          | Relative Path                      |
|------------------------|--------------------|------------------------------------|
| GPS Location           | Latitude, Longitude, Epoch timestamp | databases/exercise_db: EXERCISE_EVENT |
| Heartrate, Calories    | Numerical          | databases/activity_db: ACTIVITY_LOG_ENTRY |
| App ID                 | Alphabetical       | databases/device_notification.db: app_icon_color |
| Web Cookies Database   | Alphanumerical     | app_webview/Default/Cookies: cookies |
| Empty Credit Card Database | SQLite Database   | app_webview/Web Data: credit_cards |
| Image of credit card   | PNG                | cache/asset-cache/0dd0de4e92974ce7b15bd5ef68c5189.png |
| Alexa serial number    | Alphanumeric       | shared_prefs/alexa_device_preferences.xml |
| Credit card info       | Name, Date, Numerical | shared_prefs/ckData.xml |

Figure 1. GPS location records found in database shown in DB Browser for SQLite. These corroborate with the routes that were used to populate exercise events. Only 16 out of 4238 rows are shown in this figure.
Figure 2. Heart rate data collected during exercise and activities shown in DB Browser for SQLite.

Figure 3. Unused data table seemingly meant to hold credit card data shown in DB Browser for SQLite. No information within the entire database file is particularly significant, and, as such, the purpose of this database is unknown.

Furthermore, we were also able to locate some user data, including oauth refresh tokens (see Figure 4). As discussed in [31], the confidentiality of an access token must be preserved during the token’s transmission and storage. No other parties should be able to access the token other than the application itself, the authorization server, and the resource server [31]. As our research reveals, the availability of oauth token in plaintext raises significant security concerns for the investigated application.

Figure 4. OAuth token data found in plain text using DB Browser for SQLite.
There are references to other applications that exist on the mobile device (see Figure 5). One of these applications had been used to populate data, and as such, this information could be used by investigators to discover other apps which may contain user data. However, it must be noted that some of the app ID that found were not interacted with at all, such as com.spotify.music, as such it is not possible to determine exactly which of these apps have user data.

Finally, our research also revealed that important parts of the linked credit card could be found in an XML document, including a full billing address, and all parts of the credit card except for a cardholder name, the full credit card number, and the Card Verification Number (CVN) number, as shown in Figures 6 and 7.

![Figure 5. App ID data found in device_notification.db file using DB Browser for SQLite.](image)

![Figure 6. Full billing address stored as XML data was found in a file. The relevant XML data was extracted from the original file to omit irrelevant data.](image)

![Figure 7. Partial credit card information found as XML data in the same file as billing address information. The data was extracted from the original file to omit irrelevant data surrounding it.](image)

4.1. Unrooted Image Analysis

As we discussed in Section 3, we also acquired the unrooted version of the device. The unrooted image of the device was also analyzed to compare and contrast the findings. However, the analysis of the unrooted image revealed that the forensic tool was not able to recover any app data from the Fitbit application. As seen in Figure 8, the com.fitbit.FitbitMobile package, as well as many other apps, are missing.
5. Discussion on Findings

Overall, the artifacts discovered with pertinent security and user privacy issues can be summarized into the following categories: user data privacy, financial information security, and health data privacy. In this section, we will discuss each category of artifacts discovered during the course of this research and the implications of those artifacts. One particular data, the unique app ID, which we discovered during our analysis might be used by investigators to identify the folder where fitbit app data is located. It is more related to the app development domain; however, it can be used forensically to make sure that the investigator is analyzing a targeted app and timestamp of its last use.

Note that data creation and modification times were not checked for validity. No artifacts or any evidence suggested data was deleted by the device or application itself. No user action was committed which could result in deletion of user data.

5.1. Privacy Concerns

Artifacts discovered that are potential privacy concerns can be considered to be the following: GPS location, and Web cookies. Notifications produced by messaging applications Skype and Discord were not found in the Fitbit application package, which is a reassuring security feature. There were also no artifacts found that were generated using the integrated Alexa feature.

These artifacts related to privacy can be used by law enforcement to tie a user to a specific location at a specific time. It could also be used to connect users to various other social media applications, as links to the applications can be found in the Fitbit application, even if data from those applications do not seem to be stored by the Fitbit application itself. Moreover, if the device belongs to a suspect, investigators can have a good idea of suspect daily patterns with respect to location data.
phone is hacked, the information we found could be used by the hacker to harass further or even threaten the victim. For example, one could use the GPS information to determine where a person lives by examining what routes they commonly take and which buildings they return to often or are centered around. The attacker would be able to approximate where the victim lives and could ask them for money in return for not publishing the data online or use that information to create more convincing phishing attacks against the victim.

The negatives aside, however, the fact that social media message notifications and voice queries using Alexa are not stored in Fitbit is a good finding. Fitbit does not need to store a local copy of private and potentially sensitive data in plaintext, as it would serve the customer no additional benefit and only act as a potential data store that can be leaked or attacked by criminals.

5.2. Financial Information Security

A database was found that had tables that could be used to store credit cards linked to Fitbit Pay. However, examining these data tables did not yield any records of the credit card linked to the device. Even though the database table had columns for fields, such as a credit card’s expiration date, credit card holder’s name, etc., there were no records found even though a card was confirmed to be added to the Versa 2 and was used in a real transaction. Instead, a file containing XML data was discovered that contained the full billing address, expiration month and year, last four numbers of the credit card, and the name of the card itself but not the cardholder name.

It is clear that this information cannot be used to make fraudulent transactions by itself, because the cardholder name and CVN number are unknown. However, this information could still be used by a malicious attacker to conduct further attacks such as phishing attacks against the victim. Leveraging the information found in the Fitbit application, it is highly possible that a victim may tend to interact with the attacker if the attacker can provide these pieces of information as a way to build up trust, rapport, or authority. We can confidently argue that information of such nature should not be stored in plaintext in order to avoid or mitigate definite privacy risks the users might face.

5.3. Health Data Privacy

As discussed earlier, we were able to find records about the calories burned as well as heart rate in the Fitbit application. When combined with information on the duration of the run, the speed at which the user was going, there is a real concern that these data could be used to determine aspects of their medical health and well being. This is clearly a privacy concern as the data was not encrypted. If this information is leaked, there could be potential negative consequences for the victim. For example, an insurance company could use the heart rate and calorie data, combined with the timestamped GPS entries to determine whether a person was in physically fit condition, and in turn, raise their insurance premiums if they are found to be unfit as categorized by having very high heart rate during a relatively short time period performing minimal physical activity. It can also be argued that any user data that can be used to determine an individual’s overall health should not be so readily available and should be kept in an encrypted form.

5.4. Magnet Forensics and Rooting Challenges

During the course of our research, we have dealt with some challenges. One of the most significant problems occurred during the data acquisition stage. The Samsung Galaxy S6 device was not rooted before any data acquisition using MSAB XRY and Magnet AXIOM Process. However, during the attempt to acquire data via rooting, the Magnet Forensic’s acquisition tool offered an option to gain a physical image of the Galaxy S6, which normally requires root access. Through customer support communications and review of the Magnet Forensics User Manual, it seems reasonable to assume that the device had been rooted temporarily during the acquisition using the Magnet AXIOM Process. The root checker application was used after the third image acquisition, and it reported that the device was unrooted, which indicated that the device was temporarily rooted. However, examining this
image led to very little discoveries, and there were concerns on whether the claimed rooted image was accurate and complete. Messages and notifications artifacts were not found at all. As such, the phone was then rooted properly while using Magisk, and a second rooted image was taken using MSAB XRY. The device root status was confirmed through the use of the root checker application as well.

Although we were not able to discover new evidence of interest on the new image, it is important to note that this new image of the device did contain notable differences from the claimed rooted acquisition from Magnet Forensics. A few folders were missing from the Magnet Forensics image, which contained a few small files that were ultimately irrelevant.

5.5. Write Ahead Logging

Write Ahead Logging (WAL) files were discovered in conjunction with the database files. These files contain recently generated information that has yet to be added to the original database file [32]. As such, they may contain data that are pertinent to an investigation as newly logged data may be stored here but not yet included in the original database. The WAL files themselves are not valid database files and, as such, opening them in an SQLite database browser does not produce legible results. However, it is possible to merge the contents of the WAL files back into the original database file using checkpoints. Checkpoints are how transactions stored in WAL files are merged back into the original database file [32]. The database files were opened using the command line tool sqlite3 and the SQL command PRAGMA wal_checkpoint [33] was used on each database with a WAL file in order to create a checkpoint to merge them together. The databases were then examined as normal.

6. Conclusions

The privacy and security of data have always been a concern for the users of wearable devices, yet they are relatively secure. In this paper, we evaluated the user data privacy concerns in a new Fitbit Versa 2 wearable device, which is likely to see a significant number of adopters. Furthermore, we also presented what artifacts can be found in certain applications in an Android smartphone.

In short, data from social messaging applications, like Skype and Discord, do not get stored by Fitbit, even though the messages are pushed to the Fitbit Versa 2 to alert the user when a new message is received. However, there is still room for improvement in terms of Fitbit’s mobile application security. GPS data, health-related data, and credit card information are easily accessible and stored in plaintext. While these artifacts independently are not severe enough to result in a compromise of, for instance, a user’s bank account, it is still important information that should be kept more securely.

The credit card information is especially concerning, as our findings also testify. While the full credit card number is not available, enough information including the expiration date, the last four digits of the credit card number, and even a full billing address is available. This information, if obtained by a malicious actor, can be used by that actor as leverage to scam, phish, or defraud the victim further.

This work has identified where information pertinent to law enforcement is stored on mobile devices in regards to the Fitbit Versa 2 device. With this contribution to literature, we now know that certain credit card information is stored in files that may, otherwise, have been overlooked during analysis. The lack of encryption for user data, including physical addresses, credit card details, geolocation data, also poses a concern about consumer data privacy. As for future work, we would like to attempt to acquire data directly from Fitbit Versa 2 to see if social media message data is retained.

Author Contributions: The author contributions for this work are as follows: Conceptualization, Y.H.Y., U.K.; Methodology, Y.H.Y., U.K.; Software, Not applicable; Validation, Y.H.Y.; Formal analysis, Y.H.Y.; Investigation, Y.H.Y.; Resources, U.K.; Data curation, Y.H.Y.; Writing—Original draft, Y.H.Y.; Writing—Review and Editing, Y.H.Y., U.K.; Visualization, Y.H.Y.; Supervision, U.K.; Project administration, Y.H.Y., U.K.; Funding acquisition, Not applicable. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.
Abbreviations

The following abbreviations are used in this manuscript:

- GPS: Global Positioning System
- SWGDE: Scientific Working Group on Digital Evidence
- RAM: Random Access Memory
- FTK: Forensic Toolkit
- AFF: Advanced Forensic Format
- ACSPM: Analytical Crime Scene Procedure model
- SQL: Structured Query Language
- SQLite: Structured Query Language Light (Lite)
- IM: Instant Messaging
- NIST: National Institute of Standards and Technology
- PII: Personally Identifiable Information
- SIM: Subscriber Identity Module
- TWRP: Team Win Recovery Project
- DB: Database
- App: Application
- ID: Identification/Identify
- CVN: Card Verification Number
- XML: Extensible Markup Language
- WAL: Write Ahead Logging

Appendix A

Appendix A.1. Hardware Used

- Samsung Galaxy S6, Sprint Carrier (SM-G920P), Android 7
- Fitbit Versa 2
- Windows 10 PC for data acquisition and analysis

Appendix A.2. Software Used

- Root Checker by joeykrim v6.4.7
- Fitbit by Fitbit, Inc v3.9.1 (20243443)
- Magnet Axiom Process v3.0.0.13714
- Magnet Axiom Examine v3.0.0.13714
- XRY v7.12.0
- XACT v6.18.105
- Discord v9.8.8-HOTFIX(988)
- Skype v8.54.0.91
- TWRP v3.3.1.0-zerooflte
- Magisk v20.1(20100)
- Magisk Manager v7.4.0 (253)
- DB Browser for SQLite v3.11.2

References

1. Watts, A. Cops use murdered woman’s Fitbit to charge her husband. Australas. Polic. 2018, 10, 14.
2. Moriarty, E. 21st Century Technology Used To Help Solve Wisconsin Mom’s Murder. Available online: https://www.cbsnews.com/news/the-fitbit-alibi-21st-century-technology-used-to-help-solve-wisconsin-moms-murder/ (accessed on 22 August 2020).
3. Hauser, C. Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter’s Killing. Available online: https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html#:~:text=the%20main%20story-,Police%20Use%20Fitbit%20Data%20to%20Charge%2090%2DYear,Old%20Man%20in%20Stepdaughter%20Killing&text=The%20last%20time%20Anthony%20Aiello,Mr (accessed on 22 August 2020).

4. Rabieh, K.; Akkaya, K.; Karabiyik, U.; Qamruddin, J. A secure and cloud-based medical records access scheme for on-road emergencies. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018, pp. 1–8.

5. Haghi, M.; Thurow, K.; Stoll, R. Wearable Devices In Medical Internet of Things: Scientific Research and Commercially Available Devices. Healthc. Inf. Res. 2017, 23, 4–15. [CrossRef] [PubMed]

6. Kang, S.; Kim, S.; Kim, J. Forensic analysis for IoT fitness trackers and its application. Peer-to-Peer Netw. Appl. 2020, 13, 564–573.

7. Fitbit Reports $571 Million Q4’18 Revenue and $1.51 Billion FY’18 Revenue. Available online: https://investor.fitbit.com/press/press-releases/press-release-details/2019/Fitbit-Reports-571-Million-Q418-Revenue-and-151-Billion-FY18-Revenue/ (accessed on 22 August 2020).

8. SWGDE Best Practices for Computer Forensic Acquisitions. Available online: https://www.swgde.org/documents/published (accessed on 22 August 2020).

9. SWGDE Best Practices for Computer Forensic Examination. Available online: https://www.swgde.org/documents/published (accessed on 22 August 2020).

10. Garfinkel, S.; Malan, D.; Dubec, K.A.; Stevens, C.; Pham, C. Advanced forensic format: An open extensible format for disk imaging. In IFIP International Conference on Digital Forensics; Springer: Berlin/Heidelberg, Germany, 2006; pp. 13–27.

11. Bulbul, H.I.; Yavuzcan, H.G.; Ozel, M. Digital forensics: An analytical crime scene procedure model (ACSPM). Forensic Sci. Int. 2013, 233, 244–256. [CrossRef] [PubMed]

12. Demographics of Mobile Device Ownership and Adoption in the United States. Available online: https://www.pewresearch.org/internet/fact-sheet/mobile/ (accessed on 22 August 2020).

13. SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition. Available online: https://www.swgde.org/documents/published (accessed on 22 August 2020).

14. Reiber, L. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation; McGraw-Hill Education Group: New York, NY, USA, 2016.

15. Brunty, J. Mobile device forensics: threats, challenges, and future trends. In Digital Forensics; Elsevier: Amsterdam, The Netherlands, 2016; pp. 69–84.

16. Bays, J.; Karabiyik, U. Forensic Analysis of Third Party Location Applications in Android and iOS. In Proceedings of the IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29–30 April 2019, pp. 1–6.

17. Rathi, K.; Karabiyik, U.; Aderibigbe, T.; Chi, H. Forensic analysis of encrypted instant messaging applications on Android. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018, pp. 1–6.

18. Levinson, A.; Stackpole, B.; Johnson, D. Third party application forensics on apple mobile devices. In Proceedings of the 2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 4–7 January 2011; pp. 1–9.

19. Yang, T.Y.; Dehgchantanha, A.; Choo, K.K.R.; Muda, Z. Windows instant messaging app forensics: Facebook and Skype as case studies. PLoS ONE 2016, 11, e0150300. [CrossRef] [PubMed]

20. Rieck, J. Attacks on fitness trackers revisited: A case-study of unfit firmware security. arXiv 2016, arXiv:1604.03313.

21. Classen, J.; Wegemer, D.; Patras, P.; Spink, T.; Hollick, M. Anatomy of a vulnerable fitness tracking system: Dissecting the fitbit cloud, app, and firmware. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2018, 2, 5. [CrossRef]

22. MacDermott, Á.; Lea, S.; Iqbal, F.; Idowu, I.; Shah, B. Forensic Analysis of Wearable Devices: Fitbit, Garmin and HETP watches. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019, pp. 1–6.

23. NIST. Test Results for Mobile Device Acquisition Tool: Magnet AXIOM v1.2.1.6994; Technical Report; Department of Homeland Security: Washington, DC, USA, 2018.
24. NIST. Test Results for Mobile Device Acquisition Tool: XRY v7.8.0; Technical Report; Department of Homeland Security: Washington, DC, USA, 2018.
25. Fitbit Versa 2 Smartwatch. Available online: https://www.fitbit.com/eu/shop/versa (accessed on 22 August 2020).
26. The Most Popular Android Smartphones-2019. Available online: https://deviceatlas.com/blog/most-popular-android-smartphones#us (accessed on 22 August 2020).
27. Whitwam, R. Samsung Ends Update Support for Galaxy S6, S6 Edge, S6 Edge, and S6 Active. Available online: https://www.androidpolice.com/2018/04/02/samsung-ends-update-support-galaxy-s6-s6-edge-s6-edge-s6-active/ (accessed on 22 August 2020).
28. Farooqui, A. Don’t Hold Your Breath for the Galaxy S6 Android 8.0 Oreo Update. Available online: https://www.sammobile.com/news/dont-hold-your-breath-for-the-galaxy-s6-android-8-0-oreo-update/ (accessed on 22 August 2020).
29. TeamWin. TWRP for Samsung Galaxy S6. Available online: https://twrp.me/samsung/samsunggalaxys6.html (accessed on 22 August 2020).
30. XDA Developers. Magisk v20.3-Root & Universal Systemless Interface [Android 4.2]. Available online: https://forum.xda-developers.com/apps/magisk/official-magisk-v7-universal-systemless-t3473445 (accessed on 22 August 2020).
31. OAuth. Access Tokens. Available online: https://www.oauth.com/oauth2-servers/access-tokens/ (accessed on 22 August 2020).
32. Write Ahead Logging. Available online: https://www.sqlite.org/wal.html (accessed on 22 August 2020).
33. Caithness, A. The Forensic Implications of SQLite’s Write Ahead Log. Available online: https://digitalinvestigation.wordpress.com/2012/05/04/the-forensic-implications-of-sqlites-write-ahead-log/ (accessed on 31 August 2020).

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).