Peer-to-Peer Networking and Applications (2020) 13:564–573
https://doi.org/10.1007/s12083-018-0708-3

Forensic analysis for IoT fitness trackers and its application

Serim Kang[1] · Soram Kim[1] · Jongsung Kim[1,2]

Received: 27 May 2018 / Accepted: 4 December 2018 / Published online: 22 December 2018

Abstract

A fitness tracker monitors our daily activity by measuring distance walked (or run), calorie consumption, heartbeat and quality of sleep. Although originally designed to check the user's health, its data is important in verifying the veracity of interrogation responses of the suspect, or the activities of the victim near the time of the incident. Xiaomi Mi Band 2 and Fitbit Alta HR are representative fitness trackers which allow users to view measured data on connected mobile devices. We compare the functionality of the two wearable devices, select the data that must be acquired (based on the Android device used), and provide the analysis methods for each file from the perspective of digital forensics.

Keywords Fitness tracker · Xiaomi Mi Band 2 · Fitbit Alta HR · IoT forensic

1 Introduction

A fitness or activity tracker is an Internet of Things (IoT) wearable device that collects user's bio-metric information and monitors daily sleep-wake rhythms [1]. It measures distance walked (or run), calorie consumption, and heartbeat with built-in sensors. Certain devices also measure sleep status and body temperature. The user is warned when there is no movement for an extended period. The top 3 manufacturers in the global fitness tracker market are Xiaomi, Fitbit and Apple. In 2017, Xiaomi and Fitbit ranked first (13.7%) in the third quarter. Apple led the market with 21.0% in the fourth quarter [2, 3]. Fitness bands are connected to the mobile device via Bluetooth. The user data generated by the tracker is synchronized to the mobile device. Each manufacturer develops a mobile application to interpret and visualize health-related data from the tracker. Providing user-friendly data as well as accurate measurement of health status are important factors that determine the quality of experience (QoE)[1] for fitness trackers.

The large volume of data provided for the user's convenience can be utilized in digital forensic[2] investigations. The study of fitness band forensics has become more important as the use of wearable devices has increased. According to the International Data Corporation (IDC), global wearable device shipments amounted to 102 million in 2016, up from 82 million in the previous year [4]. Fitness band data can play an important role in refuting the false testimony of the suspect. However, few studies have been conducted on the fitness band in relation to its importance as a source of digital evidence. Forensic investigators should simplify and shorten the investigation process by increasing their awareness of how to select and interpret data from these devices.

In this paper, general aspects that a forensic investigator should know about fitness tracker analysis are discussed.

This article is part of the Topical Collection: *Special Issue on IoT System Technologies based on Quality of Experience*
Guest Editors: Cho Jaeik, Naveen Chilamkurti, and SJ Wang

✉ Jongsung Kim
jskim@kookmin.ac.kr

Serim Kang
ksl5442@kookmin.ac.kr

Soram Kim
kimsr2040@kookmin.ac.kr

[1] Department of Financial Information Security,
Kookmin University, 77 Jeongneung-Ro, Seongbuk-Gu,
Seoul, 02707, South Korea

[2] Department of Information Security, Cryptology
and Mathematics, 77 Jeongneung-Ro, Seongbuk-Gu,
Seoul, 02707, South Korea

[1] A measure of the delight or annoyance of a customer's experiences with a service.

[2] The process of collecting and analyzing data to submit electronic evidence to law enforcement.

The Xiaomi Mi Band 2 and Fitbit Alta HR are selected for study as they contain the standard functions of fitness trackers. The main features of each device are discussed in Section 3. The method to extract tracker data from Android devices is presented in Section 4. Section 5 proposes methods to analyze the user's body, sleep, and activity state from the extracted data. A method to recover deleted data is also given. Section 6 confirms the application method from the existing case and the possible scenario.

2 Related work

Most studies on wearable devices are focused on the forensic analysis of the smartwatch. De Arriba-Pérez et al. proposed several methods to collect and process data from wearable devices [5]. They state that smartwatch data collection requires a wearable device, smartphone, PC, and a server/cloud service. SDKs (Software Development Kits)[3] or APIs provided by the smartwatch vendor are used. Fitbit synchronizes the data to the mobile device and the server. The data stored on the server can be extracted through the provided Web API. However, this is only possible if the investigator knows the user's Fitbit account credentials.

Baggili et al. present the forensic analysis of the Samsung Gear 2 Neo and LG G [6]. They extracted the data of Samsung Galaxy S4 synchronized with smartwatches and confirmed which format (db, xml) the user data was stored as. In addition, they describes the rooting and imaging method of the Android-based Tizen OS (for Samsung Gear 2 Neo) and Wear OS (for LG G).

3 Features

The Xiaomi Mi Band 2 and Fitbit Alta HR, which represent the wearable fitness tracker. They share some basic features. Firstly, they both must be connected to the mobile device via Bluetooth to utilize most of the features. To manage long-term data, the fitness bands store them in the internal storage and then synchronizes them by transmission to the mobile device. Secondly, they both provide notifications of phone calls and messages, as well as displaying the time through an OLED (Organic Light-Emitting Diode) display. Finally, both support: 'Body' (the number of steps, calorie consumption, heart rate etc.), 'Sleep' (the start/end time of sleep, duration etc.), and 'Activity' (the start/end time of activity, location etc.) functions for user fitness. The Activity function includes the ability to calculate the distance, altitude, and speed of walking/running/hiking. Once the activity is completed, the user can view GPS maps and related data from the application. Additional features and differences between the two devices are described in Table 1.

Mi Band 2, released in 2016, is one of the Xiaomi wearable series. Despite its low price compared to other trackers, it supports many functions, most of which depend on the official Mi Band application called 'Mi Fit'. Figure 1 shows the three basic features of Mi Fit. Figure 1a is the main UI that represents the last records of sleep/activity and the number of steps per day. Figure 1b shows the sleep records, which is recorded by dividing the time into deep sleep, light sleep, and awake time.

Fitbit Alta HR, released in 2017, differs from Mi Band 2 in that it synchronizes data to a Fitbit server as well as the mobile application named 'Fitbit' (Fig. 2). Although device data is displayed in a similar manner to Mi Fit, the difference with Fitbit is that it supports 'MobileTrack'. It loads the user data (step count, distance, calories burned) that the mobile device recognizes to the Fitbit application. This means that some fitness data can be measured without a Fitbit device.

4 Data acquisition

Mi Band 2 and Fitbit Alta HR do not have an embedded OS and the applications cannot be installed inside the devices. However, as the data in the fitness tracker is synchronized to a mobile device or the server (in the case of Fitbit), it is necessary to extract relevant data from it. For the purposes of the study, we install the latest version of Mi Fit (v3.3.0) and Fitbit (v2.67) and then extracted the image of userdata partition (/userdata) using the mobile forensic software,

Table 1 Comparison of Mi Band 2 and Fitbit Alta HR

Functions	Xiaomi Mi Band 2	Fitbit Alta HR
Step counting	O	O
Heart rate measuring	O	O
Sleep monitoring	O	O
GPS tracking	O	O
Self-measuring system	X	O
Phone call/message alert	O	O
App vibrate alert	O	X
Calendar alert	X	O
Alarm	O	O
Unlock android	O	O
Battery life	20 days	7 days

[3] A set of software development tools that allows the creation of applications.

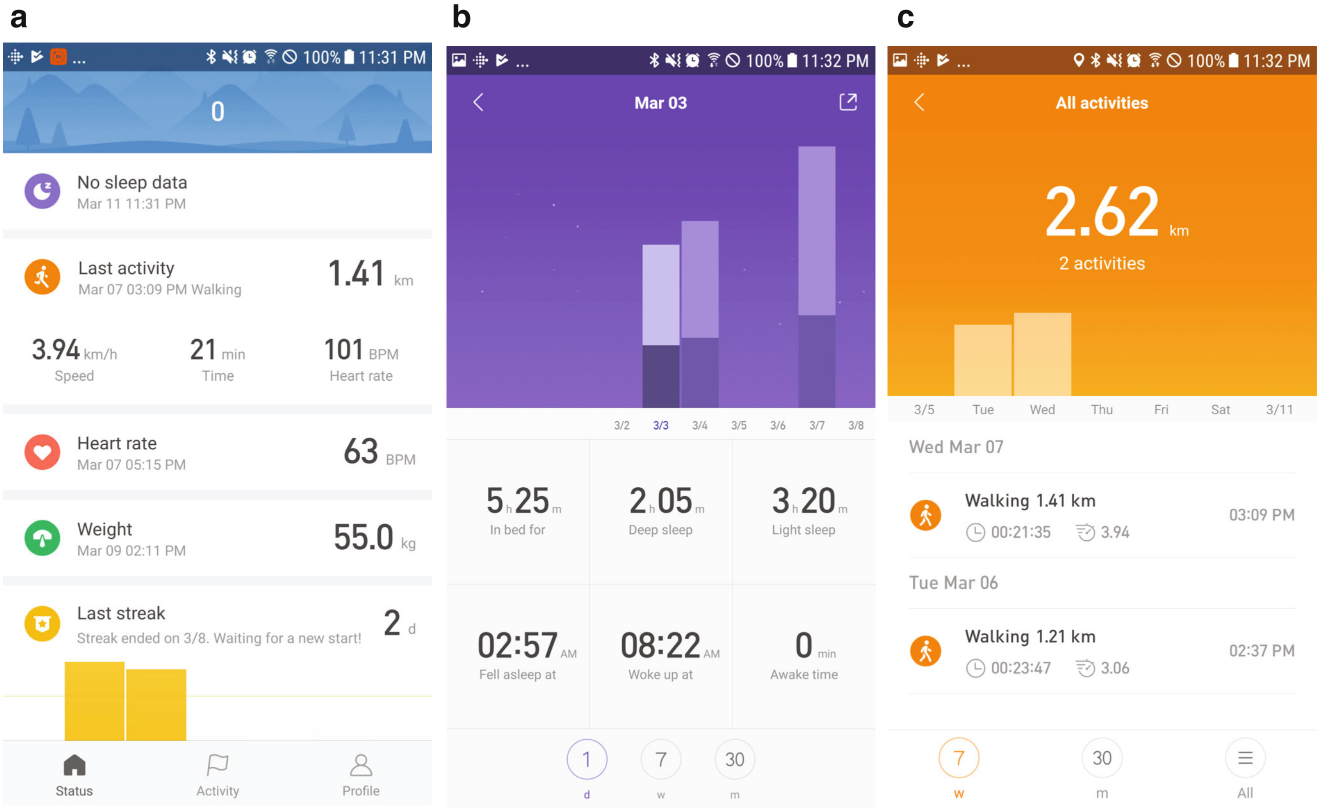


Fig. 1 The GUI of Mi Fit

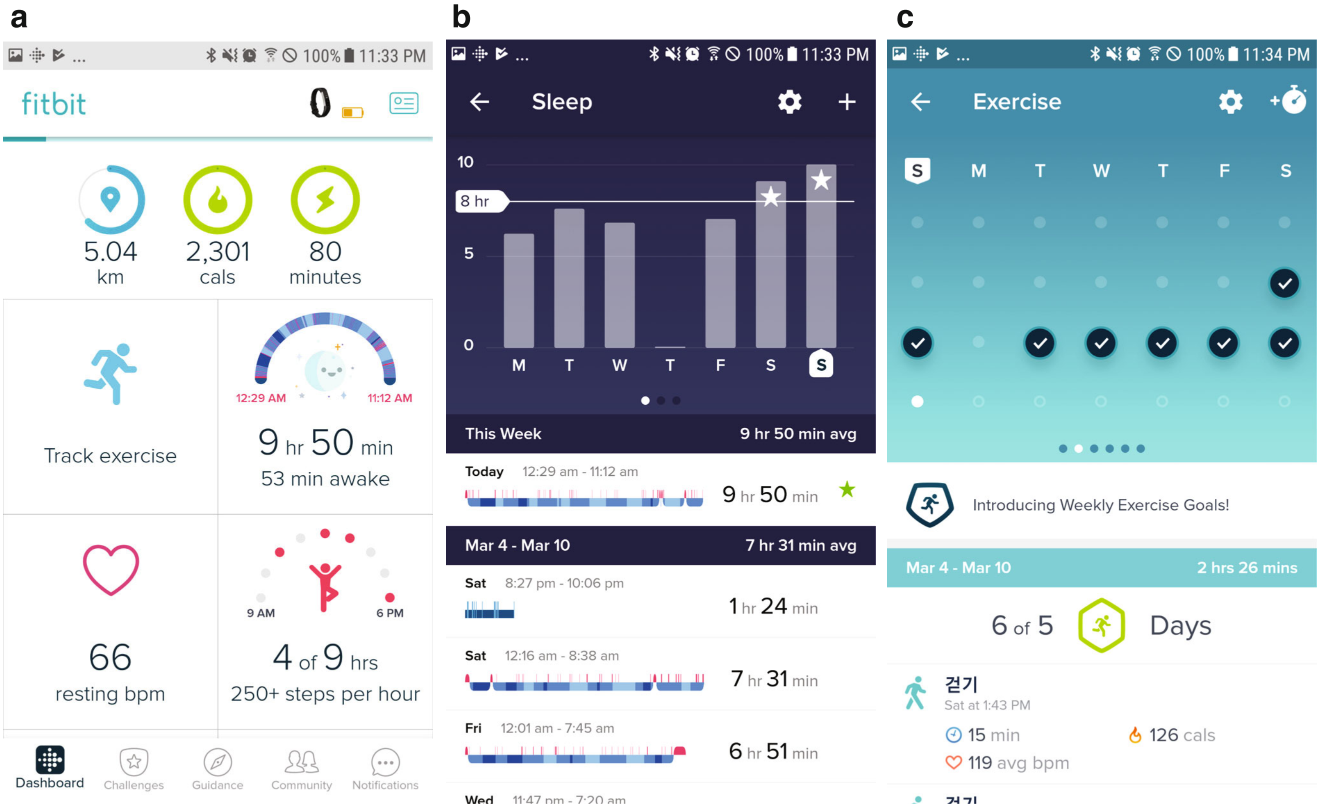


Fig. 2 The GUI of Fitbit

Table 2 Significant data to be acquired for each application

App Name	Paths	Contents
Mi Fit	< MiDir >/databases/origin-db_MD5(User ID)	- Device - Body - Sleep - Activity
	< FitDir >/databases/fitbit-db	- Device info - Body
Fitbit	< FitDir >/databases/sleep	- Sleep
	< FitDir >/databases/exercise_db	- Activity
	< FitDir >/cache/	- GPS maps

MD-NEXT.[4] The target mobile device is Samsung Galaxy S6 with Android Nougat (7.0) OS. The working directories for Mi Fit and Fitbit on Android devices are as follows.

- < MiDir > := /data/data/com.xiaomi.hm.health
- < FitDir > := /data/data/com.fitbit.FitbitMobile

Mi Fit stores thumbnails on another path (/data/media/0/.miband), but Fitbit manages them inside the working directory. All meaningful evidence is stored in SQLite3-formatted database files (paths are listed in Table 2).

Because Fitbit is synchronized with the web server, it is possible to log in with the same user credentials used for the application. The Fitbit web server provides the function to export data in CSV and XLS format. Body, activity and sleep data can be acquired for a period (up to 31 days) specified by the user.

5 Forensic analysis

This section describes the analysis method of databases mentioned in the previous section. For convenience, the table names are in italics (*table name*) and the column names in square brackets ([column name]).

5.1 Xiaomi Mi Band 2

Mi Band 2 manages user information, sleep, and activity records in a single SQLite3-formatted database named 'origin_db_MD5(User_ID)'. The number of databases is same as the number of accounts logged in to the Mi Fit app (a user identification (User_ID) is assigned to each account). The tables to be analyzed in each databases are shown in Table 3.

Table 3 Table names and contents to be analyzed

Table name	Contents
USER_INFOS	User information (User ID, Name, Birthday, Height, Weight, Last login time)
DEVICE	Connected device information (Device ID, Device MAC address, Bind status, Bind time, User ID)
DATE_DATA	Sleep and step records per day
TRACKRECORD	Activity information (Date, Track ID, Distance, Cost time, Consumed calorie, Activity finished time, total step)
TRACKDATA	Activity information (Track ID – Activity start time in UNIX timestamp, longitude, latitude)

USER_INFOS shows the account owner information. The name, birthday, height and weight are set by user. The last login time is recorded by the application. The wearable devices associated with the User_ID can be found in *DEVICE*. The type of the fitness band is set to 0, and the status of the most recently connected device is set to 1. Each device is identified by device ID or address. Daily sleep cycle and steps are located in *DATE_DATA* in summary form. Data on March 7th can be interpreted as shown in Table 4. All time information recorded in this table follows the UNIX timestamp.

Another major feature of the Mi Band 2 is the activity tracker, which is activated/deactivated by the user. The application visualizes the route, distance, time, and speed. The remaining tables are *TRACKRECORD* and *TRACKDATA*, which show data related to the activity tracker. *TRACKRECORD* shows time, distance, calorie and average heart rate for each track. Track ID represents the start time of the activity based on UNIX timestamp. An outline picture (contour) of the path of the user's movement is also stored.

The *TRACKDATA* table stores the GPS coordinates for each track. Because they are stored as a string, it is necessary to normalize it to a set $C = \{C_0, C_1, C_2, \ldots\}$ of elements like (latitude, longitude).

(1) Extract the [BULKLL] value for the specific track ID. We denote this extracted string as s.
(2) Split s by semicolons (;) and treat the split strings $T_i \quad (i = 0, 1, 2, \ldots)$ as coordinates.
(3) Denote each coordinate T_i created above and the final elements C_i as

$$T_i = (a_i, b_i), \quad C_i = (c_i, d_i), \quad i = 0, 1, 2, \ldots$$
$$(c_0 = a_0, d_0 = b_0)$$

[4] Mobile data acquisition tool developed by Hancom GMD.

Table 4 Interpretation result of [summary] on March 7th

		value
slp (sleep cycle)	st (start time)	1520347140 (2018-03-06 23:39:00 UTC+09:00)
	ed (end time)	1520380020 (2018-03-07 08:47:00 UTC+09:00)
	dp (deep sleep)	185 (3 hr. 5 min.)
	lt (light sleep)	336 (5 hr. 36 min.)
	wk (wake time)	27 (27 min.)
stp (step record)	ttl (total steps)	7075
	dis (distance)	4846 (m)
	cal (calorie)	121 (Cal.)

Then calculate each coordinate:

$$c_j = c_{j-1} + a_j, \quad d_j = d_{j-1} + b_j \quad (j = 1, 2, \ldots)$$

(4) A set C consists of the elements C_i and represents user's path.

These coordinates can be displayed on the map to visually confirm the route. Python code is implemented that normalizes the coordinates from the input database and outputs it to a KML file. KML is an XML-formatted file type used by Google Earth.[5] It contains coordinates and style information used to represent them. An example output file is shown in Figs. 3 and 4. shows this KML file opened in Google Earth.

5.2 Fitbit Alta HR

Fitbit Alta HR manages multiple SQLite3-formatted databases to store device information, steps, sleep and activity. 'fitbit-db' shows which devices are connected to the application (*DEVICE*) and the number of steps the user walks on specific times (*TIME_SERIES_OBJECT*). Figure 5 stores the number of steps taken in 15 minutes increments. If the [OBJECT_TYPE] is 11, the record indicates step-related data. Otherwise, the body weight and the calorie consumption are shown. [LEVEL] indicates walking strength. The higher the value, the higher the strength.

The sleep record is based on detecting movement of the wearing the band. A sleep state is recorded if there is no movement for an hour. If the user does not go to sleep and does not move for a long period of time, the band may misread the status. The sleep date, time and duration (millisecond) are recorded (*SLEEP_LOG*). The sleep phase is measured by combining the heart rate and the movement pattern (*SLEEP_LEVEL_DATA*).

The GPS data recorded if the user has activated the 'Mobile Run' function within the application. 'exercise_db' stores the latitude, longitude, altitude, and speed (with timestamp) in the *EXERCISE_EVENT* table. These data are then displayed on a map and saved as PNG file (which can also be found on the Fitbit server). When the mouse cursor is placed on the dashboard, the location for the specific time is shown immediately.

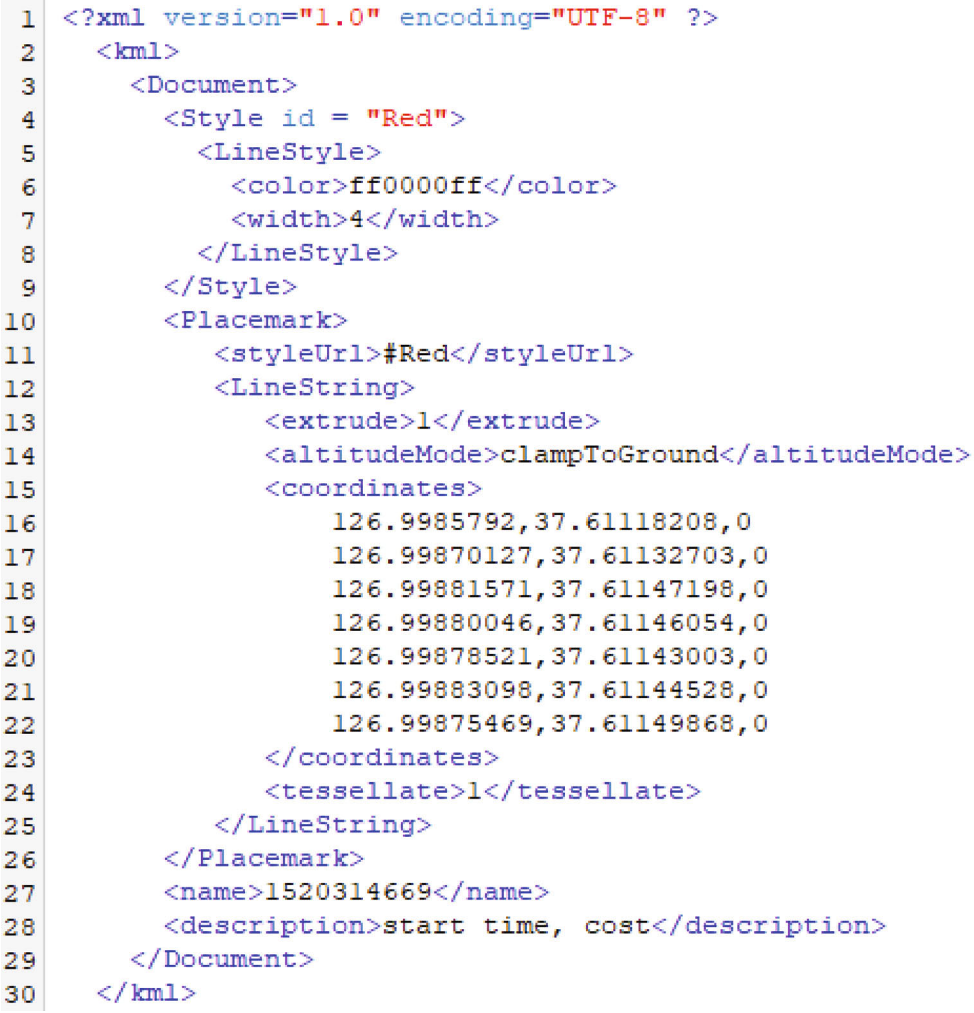
5.3 How to analyze intentionally deleted or modified data

Most of the data mentioned above is automatically recorded by the fitness band according to the user's motion. The Mi Fit and Fitbit applications provide users with the ability to add or delete data. For example, the user can delete unnecessary data or add data when it is not recorded due to device malfunction etc. The capability to modify data can be misused by someone who wants to conceal their actions. Table 5 shows whether the user can delete or modify sleep/activity data for each tracker.

The sleep data can be modified in both apps. A suspect may claim to have been sleeping at the time of an incident by changing his sleep start or end time. The activity data cannot be modified but can be deleted. A suspect is likely to delete the data so that he or she does not expose their movements over a particular period. The forensic investigator must find the context in which the user has modified or deleted the

[5] Google-provided services that covers local information around the world, including satellite imagery, maps, terrain and ED building information.

Fig. 3 The example of the KML file



```
<?xml version="1.0" encoding="UTF-8" ?>
  <kml>
    <Document>
      <Style id = "Red">
        <LineStyle>
          <color>ff0000ff</color>
          <width>4</width>
        </LineStyle>
      </Style>
      <Placemark>
         <styleUrl>#Red</styleUrl>
         <LineString>
            <extrude>1</extrude>
            <altitudeMode>clampToGround</altitudeMode>
            <coordinates>
                126.9985792,37.61118208,0
                126.99870127,37.61132703,0
                126.99881571,37.61147198,0
                126.99880046,37.61146054,0
                126.99878521,37.61143003,0
                126.99883098,37.61144528,0
                126.99875469,37.61149868,0
            </coordinates>
            <tessellate>1</tessellate>
         </LineString>
      </Placemark>
      <name>1520314669</name>
      <description>start time, cost</description>
    </Document>
  </kml>
```

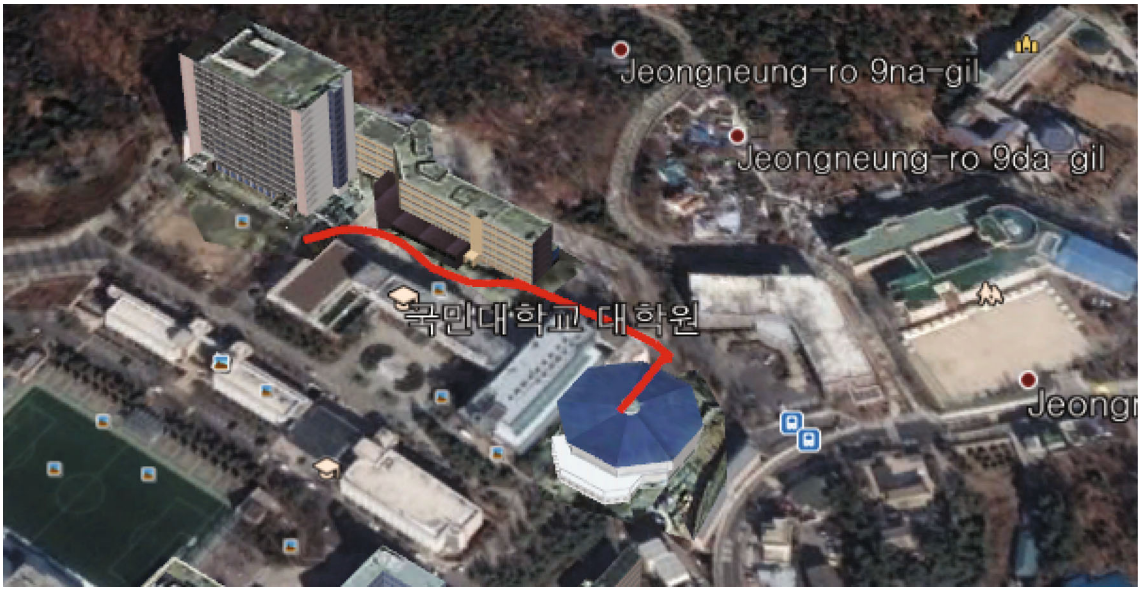
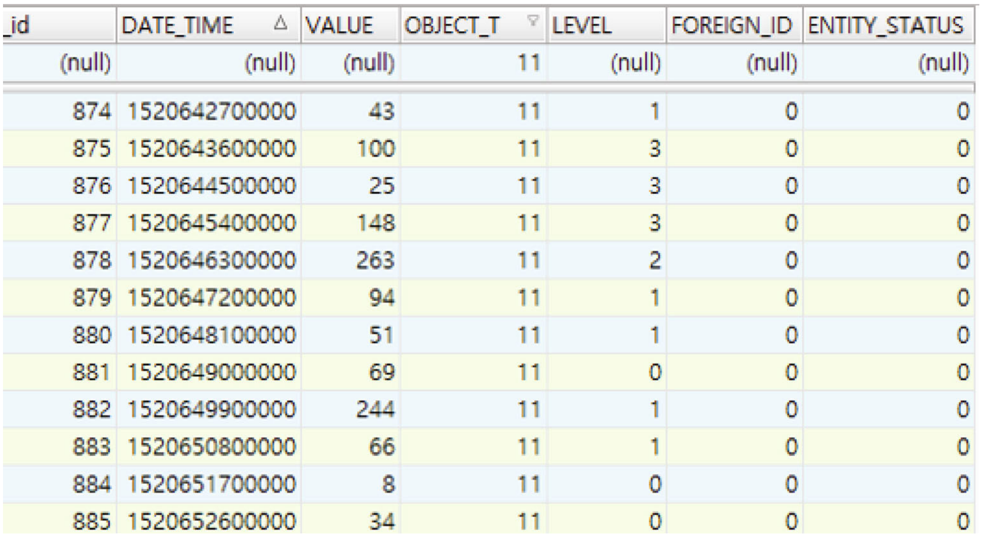


Fig. 4 KML file on google Earth



_id	DATE_TIME	VALUE	OBJECT_T	LEVEL	FOREIGN_ID	ENTITY_STATUS
(null)	(null)	(null)	11	(null)	(null)	(null)
874	1520642700000	43	11	1	0	0
875	1520643600000	100	11	3	0	0
876	1520644500000	25	11	3	0	0
877	1520645400000	148	11	3	0	0
878	1520646300000	263	11	2	0	0
879	1520647200000	94	11	1	0	0
880	1520648100000	51	11	1	0	0
881	1520649000000	69	11	0	0	0
882	1520649900000	244	11	1	0	0
883	1520650800000	66	11	1	0	0
884	1520651700000	8	11	0	0	0
885	1520652600000	34	11	0	0	0

Fig. 5 Contents of the *TIME_SERIES_OBJECT*

original (which must also be recovered). In this section, the consequences of deleting or modifying data in each app are described, including how and if data can be recovered.

5.3.1 Xiaomi Mi Band 2

The Mi Band 2 user cannot delete existing sleep data, but can modify it or add new entries by adjusting the sleep start and end time. Typically, *DATE_DATA* contains raw data which are recorded when the Mi Band and mobile application are synchronized. It also accumulates records by date, regardless of whether sleep data is recorded or not. If the user changes existing data or adds new data, the modified or added data is added to the new table, named *MANUAL_DATA*, instead of being updated in *DATE_DATA*. In summary, *DATE_DATA* contains the 'raw' data measured daily by the tracker. *MANUAL_DATA* contains the 'modified' or 'added' data. We divided the sleep record for Mi Band 2 into four types:

– *MANUAL_DATA*
  Type 1. Newly added data
  Type 2. Modified data

– *DATE_DATA*
  Type 3. No data
  Type 4. Raw data

Table 5 Data deletion/modification capabilities of tracking devices

		Deleted	Modified
Mi Fit	Sleep	X	O
(Xiaomi)	Activity	O	X
Fitbit	Sleep	O	O
	Activity	O	X

These types can be distinguished by comparing timestamps (*st*, *ed*, *dp*, *lt*, and *wk*) in [summary] of the corresponding table. First, the records in *MANUAL_DATA* belong to Type 1 or Type 2. If dp, lt, and wk are all set to 0, it is newly added data (Type 1) since the only values the user can change are st and ed. For Type 2, the original data can be recovered from the corresponding record in *DATE_DATA*. Setting the sleep time to be less than originally recorded will automatically change the dp, lt and wk values in the *DATE_DATA*. Records of dates not included in the *MANUAL_DATA* should be checked in *DATE_DATA*. If no sleep data was measured (Type 3), the values of st and ed are equal to the timestamp of the previous day at 00:00. Finally, for the raw data (Type 4), the following formula is established.

$$ed - st = (dp + lt + wk) * 60$$

The activity data written by Xiaomi Mi Band 2 can only be deleted and cannot be modified. When a specific activity is deleted, the corresponding record in *TRACKRECORD* cannot be seen through the SQLite viewer. The deleted data remain in the file and the original data can be obtained. Note, there is a recovery method for the deleted record from SQLite [9]. Another way to recover deleted activity data is by using the *TRACKDATA* table. The records in it can be checked through the viewer even if the activity is deleted (it contains coordinates representing the user's route). The recoverable data and recovery methods are as follows:

– Start time : Convert [TRACKID] from unix timestamp to UTC
– Cost time : Get [BULKTIME], split it by semicolon(;) and add all the values
– End time : Add cost time to start time

Table 6 Recovery and analysis results of deleted data

	Original	Recovered /Interpreted
TRACKRECORD		
[DATE]	–	2018-01-15
[TRACKID]	–	1515995640
[COSTTIME]	–	1372
[ENDTIME]	–	1515997020
TRACKDATA		
[TRACKID]	1515995640	Start time 2018-01-15 14:54 UTC+09:00

[BULKTIME][a]	46;11;4;4;13;12;11;112;2;2;2;16;
	8;4;4;4;2;2;2;2;4;4;10;6;4;4;4;4;3;
	6;2;6;4;4;9;4;6;4;2;6;4;4;4;6;4;4;4;
	4;2;4;5;6;6;4;6;4;4;4;8;6;6;2;3;4;4;
	4;4;4;4;5;7;6;8;4;4;4;4;4;9;8;40;16;
	9;16;20;2;8;14;6;8;6;5;8;4;4;4;4;3;
	4;4;4;6;9;6;2;2;2;4;6;4;4;4;6;4;6;4;
	6;6;6;6;4;6;4;4;4;4;4;6;4;4;4;8;8;4;
	209;2;3;3;13;5;2;4;9;5;4;8;2;4;2;6;
	4;4;6;6;59;79;2;2;4;10;7;4;4
		Cost time
		1372 sec. (22 min. 52 sec.)

[a] End time = Start time + Cost time

5.3.2 Fitbit Alta HR

Fitbit's sleep data is updated at the time of modification. Hence, simple analysis does not indicate if it has been modified by someone. Fortunately, it is possible to know whether data is deleted. The deleted record is not visible in the SQLite viewer, but remains in the file with the string 'pendingDelete'.[6] The Fitbit's activity records are also maintained in the database, even if they are deleted. However, there is a difference between the binary of the record before and after the deletion. One record contains created time and update time. If the record is deleted, 0x02 is added after the update time. Additionally, both timestamps are updated with the deleted time.

6 Applications in digital forensic

6.1 Real cases

In this section, the use of fitness data of the users as critical evidence in court is examined. In 2015, Fitbit data disproved a woman's claim that she was raped by an unknown intruder. She insisted that someone broke into the house while she was sleeping and threatened her with a knife. Police found furniture that had been turned over and a knife at the scene. She claimed her Fitbit had disappeared during the struggle. However, it was later found in the hallway. Police obtained her Fitbit account login and the device showed she was awake and walking around at the time she claimed she was sleeping [7]. In December of the same year, there was another false testimony by a man regarding the murder scene of his wife. He claimed that a man killed his wife as she returned through their garage after a workout. However, the facts revealed by the Fitbit worn by his wife are as follows [8].

- She was moving around for more than an hour after her husband said the murder took place.
- She had traveled more than 1,200ft after arriving home.

Both are cases where the claims of the suspect are refuted based on Fitbit data. In the first case, the sleep record should have been recorded even if the suspect was not wearing her tracker at the time of the incident. In the second case, the victim was wearing the Fitbit. There were records of movements after the time at which the victim was alleged

[6] If it is a normal record, 'synced' should be recorded.

to have died. Since the Fitbit records the number of steps at regular time intervals, it is possible to compare to the time claimed by the suspect.

The characteristics of fitness trackers mean they can serve as important evidence in criminal cases. Critically, it can be used to clarify a victim's behavior and/or body status before their death. The data may also be crucial in determining the suspect's geographic range of activity (based on GPS information).

6.2 A possible scenario

In this section, a hypothetical scenario.[7] On January 15, 2018, a woman was murdered in her house in Seoul, Korea. Her husband was identified as a suspect, and he made the following claims:

- He went to the department store with his wife and went back home at 15:30 on the day she was murdered.
- Afterwards, he was taking a nap in the bedroom and his wife was watching TV in the living room.
- When he woke up and went out into the living room, she was dead.

The police secured the Xiaomi Mi Band 2 worn by the woman (and a mobile phone connected to it) at the crime scene. The forensic investigator first extracted the database (origin_db_MD5(User ID)) managed by the Mi Fit app from the mobile phone. Considering the record on January 15 of *DATE_DATA*, the total number of steps (*ttl*) was 12430 and the sleep start (*st*)/end (*ed*) time were the same at 1515888000 (2018-01-14 00:00 UTC+09:00).[8] There was no data in *TRACKRECORD* where the Activity summary is stored, but there were 13 records in *TRACKDATA*. The path was recovered from [BULKLL] of each record using the method discussed in 5.1. Of the 13 records recovered (including the January 15th), 8 were showing the park in front of her house. The timestamps deleted from *TRACKDATA* were recovered using *TRACKRECORD*. Table 6 shows the recovery and interpretation of these results. The analysis proves that her husband made false testimony regarding her death. The data recovered proved that she was in the park when he insisted that he went back to the department store with her. The record showing this was deleted by someone. This example illustrates that it is possible for forensic investigators to logically disprove a suspect's false statements (made to hide his or her behavior/actions) with the tracker data.

7 Conclusions

In fitness tracker forensics, it is important to identify the general features of the tracker, select the data to be investigated, and understand how to analyze them. These steps were addressed using two fitness trackers: the Xiaomi Mi Band 2 and the Fitbit Alta HR. They are designed to monitor body, sleep, and activity. The records generated by these functions can be crucial to criminal investigations. Fitness bands interact with the mobile devices. Consequently, relevant data can be acquired from the connected device. The trackers manage the majority of the data in the form of SQLite3 databases for Android devices. In the case of the Fitbit Alta HR, it is possible to acquire the same data that transferred onto the connected mobile device on a Fitbit server (using the user's account). The number of steps, heart rate, the sleep cycle, and GPS data (with timestamp) are significant not only to verify the suspect's claim but also to deduce time of death of the victim. The applications for interacting with the fitness tracker are developed by each vendor. Hence, the way in which the applications manage the data (file format, name, etc.) is different. Therefore, it is necessary to analyze various devices so that data extraction techniques can be developed for applications in any cases.

Acknowledgements This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00344, Deciphering and forensic analysis of recent mobile devices).

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Zambotti Massimilianode, Claudatos S, Inkelis S, Colrain IM, Baker FC (2015) Evaluation of a consumer fitness-tracking device to assess sleep in adults. Chronobiology International: The Journal of Biological and Medical Rhythm Research 32:1024–1028
2. IDC: Worldwide Wearables Market Grows 7.3% in Q3 2017 as Smart Wearables Rise and Basic Wearables Decline https://www.idc.com/getdoc.jsp?containerid=prUS43260217 (2017) Accessed 30 November 2017
3. IDC: Global Wearables Market Grows 7.7% in 4Q17 and 10.3% in 2017 as Apple Seizes the Leader Position https://www.idc.com/getdoc.jsp?containerid=prUS43598218 (2018). Accessed 01 March 2018
4. Statista: Fitbit Leads Global Wearables Market https://www.statista.com/chart/8420/wearable-device-shipments/ (2017). Accessed 7 March 2017
5. de Arriba-Pérez F, Caeiro-Rodríguez M, Santos-Gago JM (2016) Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios, Sensors 2016. https://doi.org/10.3390/s16091538

[7] This scenario was adapted from that given in the DFRWS IoT Forensic Challenge (2017-2018).

[8] Korea Standard Time (KST)

6. Baggili I, Oduro J, Anthony K, Breitinger F, McGee G (2015) Watch what you wear: preliminary forensic analysis of smart watches. In: 2015 10th international conference on availability, reliability and security. https://doi.org/10.1109/ARES.2015.39
7. abc27: Woman's fitness watch disproved rape report http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/ (2015). Accessed 19 June 2015
8. The Guardian: Man suspected in wife's murder after her Fitbit data doesn't match his alibi https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate (2017). Accessed 25 April 2017
9. Jeon S, Band J, Byun K, Lee S (2012) A recovery method of deleted record for SQLite database. Pers Ubiquit Comput 16:707–715

Serim Kang received her Bachelor degree in Mathematics from Kookmin university, Korea in 2017. She is currently studying for a Master's degree in Dept. of Financial Information Security at Kookmin University, Korea, since March 2017. She is a researcher in the DF&C Laboratory. Her research interests include information security and digital forensics.

Soram Kim received her Bachelor degree in Mathematics and Master degrees in Financial Information Security from Kookmin university, Korea in 2016 and 2018, respectively. She is currently studying for Doctor's degree in Dept. of Financial Information Security at Kookmin University, Korea, since March 2018. She is a researcher in the DF&C (Digital Forensic & Cryptanalysis) Laboratory. Her research interests include information security and digital forensics.

Jongsung Kim received his Bachelor and Master degrees in Mathematics from Korea university, Korea in 2000 and 2002, respectively. He received double Doctoral degrees completed in November 2006 and February 2007 at the ESAT/COSIC group of Katholieke Universiteit Leuven and at Engineering in Information Security of Korea University, respectively. He had been a Research Professor of Center for Information Security Technologies (CIST) at Korea University, Korea, from March 2007 till August 2009, and an assistant professor of department of e-business at Kyungnam University, Korea, from September 2009 till February 2013. Dr. Kim has been an associate professor of Dept. of Information Security, Cryptology, and Mathematics / Dept. of Financial Information Security at Kookmin University, Korea, since March 2013. He is currently leading the laboratory named "DF&C" (its full name is Digital Forensic & Cryptanalysis: http://dfnc.kookmin.ac.kr). Dr. Kim has published more than 60 research papers in international journals, conferences and books. He has been serving as chairs, program committee, or organizing committee chair for many international conferences and workshops including FSE and Asiacrypt. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Inderscience. His research interests include security issues, cryptography, and digital forensics.