Forensic Science International: Digital Investigation 45 (2023) 301555

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Post-mortem digital forensics analysis of the Zepp Life android application

Patrício Domingues [a, b, c], José Francisco [a], Miguel Frade [a, c, *]

[a] School of Technology and Management - Polytechnic Institute of Leiria, Leiria, Portugal
[b] Instituto de Telecomunicações, Portugal
[c] Computer Science and Communication Research Centre, Portugal

ARTICLE INFO

Article history:
Received 27 December 2022
Received in revised form
19 April 2023
Accepted 20 April 2023
Available online xxx

Keywords:
Digital forensics
Mi band
Fitness trackers
Android
Wearable

ABSTRACT

This paper studies the post-mortem digital forensic artifacts left by the Android *Zepp Life* (formerly *Mi Fit*) mobile application when used in conjunction with a Xiaomi *Mi Band* 6. The *Mi Band* 6 is a low-cost smart band device with several sensors that allow for health and activity monitoring, collecting metrics such as heart rate, blood oxygen saturation level, and step count. The device communicates via Bluetooth Low Energy with the *Zepp Life* application, which displays its data, provides some controls, and acts as a bridge to the Internet.

We study, from a digital forensics perspective, the Android version of the mobile application in a rooted smartphone. For this purpose, we analyze the data repositories, namely its databases and XML files, and correlate the data on the smartphone with the corresponding usage of the Mi Band device. The paper also presents two open-source scripts we have developed to ease the task of forensic practitioners dealing with *Zepp Life*/*Mi Band* 6: ZL_std and ZL_autopsy. The former refers to a Python 3 script that extracts high-level views of *Zepp Life* data through the command-line, whereas the latter is a module that integrates ZL_std functionalities within the popular open-source Autopsy digital forensic software. Data stored on the Android companion device of a *Mi Band* 6 might include GPS coordinates, events and alarms, and biometric data such as heart rate, sleep time, and fitness activity, which can be valuable digital forensic artifacts.

© 2023 Elsevier Ltd. All rights reserved.

1. Introduction

Since the inception of the first Apple's iWatch in 2015, smartwatches — that is, digital devices worn at the wrist — have been gaining popularity, merging commodity features such as phone calls and message notifications, with activity tracking, acting as an appendix of the ubiquitous smartphone. This popularity trend has increased with the emergence of low-cost and feature-charged wrist-worn devices, also known as *smart bands* (Canalys Newsroom, 2021). Examples include Samsung Gear Fit, Huawei's Band, Huami's Amazfit Band, and Xiaomi's Mi Band, to name just a few. Smart band devices can perform basic functions such as timekeeping, alarm clock, displaying received SMS, and notifying of incoming phone calls or messages. They can also perform more advanced functions such as triggering the paired smartphone to ring to facilitate its localization, or displaying the weather prediction for the next few days. In addition, they can also collect health metrics, such as heart rate, level of blood oxygen saturation, perform sleep analysis, and track calorie consumption, as well as gather activity-related metrics, such as steps taken, running, biking, or pool swimming.

A significant portion of a smart band's usefulness comes from its *companion mobile application*, which is usually a vendor-specific app that runs on a smartphone and communicates with the smart band via Bluetooth Low Energy (BLE). The companion app is an essential part of the smart band/smartphone pair, as it receives and processes data collected by the band and provides internet connectivity for tasks such as uploading data to the band vendor's cloud, downloading firmware updates for the band, or simply accessing weather forecast data.

Smart bands companion apps also serve as a rich source of digital forensic evidence, as they gather a vast amount of sensitive personal information and usage patterns, which can be used to reconstruct

[*] Corresponding author. School of Technology and Management - Polytechnic Institute of Leiria, Leiria, Portugal.
E-mail address: miguel.frade@ipleiria.pt (M. Frade).

https://doi.org/10.1016/j.fsidi.2023.301555
2666-2817/© 2023 Elsevier Ltd. All rights reserved.

the user's activities and provide valuable insights into criminal investigation (Kim and Lee, 2020; Reedy and Houck, 2023). For instance, heart rate may provide evidence on the time of death of a victim, as it was the case in a murder in the USA in 2015, where data from the Fitbit device worn by the victim was used to establish a precise time of death and refute the alibi of a suspect (BBC News; Dorai et al., 2018). The murder in the USA of Karen Navarra in 2018 is another case where data from a Fitbit device worn by the victim assisted investigators in contradicting the alibi of the suspect, as the victim's heart rate soared then slowed and stopped in a period coincident with the suspect's presence at the victim's house (BBC News, 2018). In the Crouch case, heart data rate from a biometric watch worn by the victim along with the paired smartphone was used to disprove the alibi of the main suspect (BBC News, 2021). UK's Mitesh Patel case is another example where data from the suspect's Fitbit showed intense physical activity following the female victim's death, contradicting his testimony (Franqueira and Horsman, 2020). Recognizing the growing importance of adequately assessing mobile and wearable devices, Scotland Yard has announced plans to strengthen its resources for collecting data from wearables and IoT devices, namely FitBit, doorbells, and others (France, 2021).

This paper analyzes the digital forensic artifacts left by the *Zepp Life* Android application (formerly *Mi Fit*) coupled with the *Mi Band* 6. The Mi Band is a lineage of low-cost wrist-worn wearable activity monitors. Version 6 is identified as *Mi Band* 6 and packs a vast set of activity-related features for a cost of around 35 euros. Its long list of features, low price, and several-week-long battery life have made the Mi Band a commercial success, with each model selling several million units and establishing itself as a market leader in the realm of smart bands (Canalys Newsroom, 2021). For instance, in Q2 2021, Xiaomi sold around eight million Mi Band 6, leading the market with a share close to 20% (Canalys Newsroom, 2021). This market leadership is also visible for the Mi Band default companion application – *Zepp Life* – whose Android version has more than 100 000 000 downloads, and over nearly 2 500 000 reviews in Google Play,[1] with an average score, at the time of this writing, of 4 out of 5. Note that Xiaomi's *Mi Fit* was renamed in 2022 as *Zepp Life*. As observed by Gadgets & Wearables (Xiaomi re, 2022), *Zepp* is the name of Huami's Amazfit bands software,[2] with Huami being the manufacturer of the Xiaomi Mi Bands. The two applications share many similarities. In this paper, we present a case study of the *Zepp Life* mobile application in an Android rooted smartphone paired with the Xiaomi *Mi Band* 6.

The main contributions of this paper are: *i*) identification and analysis of the digital forensic artifacts available in a post-mortem examination of a rooted Android smartphone with *Zepp Life* installed; *ii*) Development of an open source digital forensic software consisting of a Python 3.6+ script called ZL_std and a module called ZL_autopsy for the open-source Autopsy software.

The remainder of this paper is organized as follows. Section 2 reviews related work, while Section 3 describes the materials and methods of this study. Section 4 analyzes the *Zepp Life* application, highlighting its primary forensic artifacts. Section 5 presents our open-source software tools ZL_std and ZL_autopsy. Finally, Section 6 concludes the paper.

2. Related work

We now analyze related work, focusing primarily on the forensics of wrist-wearable health trackers.

Baggili et al. presented a pioneer work focusing on wrist-worn digital devices (Baggili et al., 2015). The paper analyzes the digital forensic traces left by two smartwatches – *i*) Samsung Gear 2 Neo and *ii*) LG G – by directly accessing the smartwatches. For this purpose, the authors needed to root the smartwatches. Other works focus on Fitbit, which is a more capable but also more expensive fitness tracker. Examples of Fitbit's studies from a digital forensic perspective include (MacDermott et al., 2019; Williams et al., 2021; Yoon and Karabiyik, 2020). Other works focus on specific smartwatches. Odom et al. (2019) analyze the digital forensic artifacts left by the interaction of the Samsung Gear S3 Frontier smartwatch with a Samsung Galaxy S8 smartphone running Android. Note that the Gear S3 Frontier is a mid-range priced smartwatch that can work without a paired smartphone, although with limited functionalities. The paper studies both devices and reports the difficulties of extracting data in a forensic sound manner. The authors provide a software tool to extract data from Gear S3 Frontier devices. Another study regarding smartwatches is provided by Dawson and Akinbi (2021). They analyze the TomTom Spark 3 GPS fitness smartwatch ecosystem, which includes the smartwatch and the companion mobile application TomTom Sports. They study data extraction for relevant forensic artifacts and analyze the recovery of deleted data. Contrary to Mi Band, TomTom Spark 3 is much less popular as it is geared toward fitness-focused individuals.

Gregorio et al. analyzed three low-cost smartwatches built around MediaTek (MTK) chips which run the proprietary Nucleus real-time operating system (RTOS) (Gregorio et al., 2019). They resort to the smartwatch manufacturer supplied FlashTool software to perform the memory acquisition of the device. The authors reported that they could recover contacts, call logs, text messages, notifications, and Bluetooth connection logs.

Closer to our work are studies involving Mi Band devices. Kang et al. study the forensic artifacts left on an Android 7 smartphone by the *Mi Fit* paired with Mi Band 2 application, and the *Fitbit* application coupled to a Fitbit fitness device (Kang et al., 2020). Interestingly, several of the databases in *Zepp Life* already existed in the *Mi Fit* application. Examples include SQLite 3 databases such as origin_DB, FemaleHealth_ID.db and stress_ID.db. We examine these databases and their tables later on. This confirms that *Zepp Life* is the successor of *Mi Fit* and that the mobile application maintains the central data structures across versions regardless of the application name. Both applications resort to the same private directory to store their files, that is,/data/data/com.xiaomi.hm.health. Our work goes deeper and involved two versions of Android – 8.1 and 10. Additionally, we provide open-source software to assist in the analysis of the most forensically relevant artifacts.

Hassenfeldt et al. studies 13 Android mobile health and fitness applications. They remark that a significant amount of personally identifiable information (PII) is demanded at the account creation for all mobile applications. For instance, the profile of one of the applications required the user's ethnicity, blood type, pregnancy status (y/n), and body measurements such as waist and hip circumferences (Hassenfeldt et al., 2019). The authors developed a generic software tool that searches keywords on XML, database, and image files that report identified matches. Contrary to our approach, Hassenfeldt et al. work does not focus in-depth on the digital artifacts of mobile health/fitness applications but instead performs a broad review of the artifacts and PII of the applications, in Android versions 6 and 7.

Hantke and Dewald analyze the Xiaomi Mi Band 2, Fitbit Charge 2, and Huawei Band 2, collecting data with a paired Samsung Galaxy S4 (Hantke and Dewald, 2020). They report that in a Mi Band 2, by authenticating via Bluetooth, it is possible to access the last 15

[1] https://play.google.com/store/apps/details?id=com.xiaomi.hm.health.

[2] https://play.google.com/store/apps/details?id=com.huami.watch.hmwatchmanager.

days of data, as these data are kept at the band. The paper also lists the tables holding the most crucial digital forensics data without referring to the hosting databases or giving details. Although the authors tried to explore the Huami API, which is used by *Zepp Life*, they were unsuccessful. Our study is more detail-oriented, as we aim to provide information for quick reference and software tools to ease forensic data analysis.

Casagrande et al. study the security of Xiaomi fitness tracking ecosystem from Mi Band 2 to Mi Band 6, reporting several insecurities, namely that Bluetooth communications between the band and the companion application are insecure and can be eavesdropped due to the adopted logical protocol of the bands (Casagrande et al., 2022). They identify insecurities such as keys exchanged in clear text, unilateral and replayable authentication, and the lack of Bluetooth Low Energy traffic encryption. The authors present four man-in-the-middle (MITM) attacks and two vulnerabilities that leverage a malicious Android application to snoop on Mi Band data. Such vulnerabilities or similar can be of great interest for digital forensics, as they could be used to collect data from a Mi Band, even without physical access to its paired smartphone.

Accuracy is an essential factor in digital forensics. Paradiso et al. assess the precision of step and heart rate measurement of the Mi Band 2 in a controlled 6-min walk test, reporting good accuracy for step counting but less reliability for heart rate measurement, namely underestimating heart rate during exercise (Paradiso et al., 2020). Another study from de la Casa Pérez et al. evaluates the Mi Band 4 in so-called free-living conditions (de la Casa Pérez et al., 2022), reporting good accuracy at low and high walking speeds for both walked steps and heart rate. Vink et al. proposes a different approach based on the likelihood ratio (LR), which presents the degree of support for one hypothesis versus another to assist the expert in assessing their certainty about the step count data (Vink et al., 2022).

3. Materials and methods

We present materials — hardware and software — and the main research methods used to study the *Mi Band* 6/*Zepp Life* pair. First, we describe the hardware and software ecosystem and then the main methods used in this study.

3.1. Hardware

To analyze the *Mi Band* 6/*Zepp Life* pair, we resorted to a non-NFC *Mi Band* 6 and two rooted smartphones: a Xiaomi Mi A2/Android 10 (API 29) and a BQ Aquaris X Pro/Android 8.1 (API 27). The *Mi Band* 6 hardware version was 0.82.17.3, while the firmware version was 1.0.6.16. Note that while one can consult the firmware version of the *Mi Band* 6 in both the band and the *Zepp Life* application, neither the band nor the application displays the hardware version. As we shall see later, the hardware version is available through the HARDWARE_VERSION attribute of the DEVICE table of the origin_db_<id> SQLite 3 database, where id is the result of applying the MD5 hash algorithm to userID. Besides the two physical smartphones, we also resorted to the Genymotion emulator configured with a Google Pixel Android 6 (API 23). The hardware employed in this study is listed in Table 1.

Table 1
List of devices used in this study and their respective OS versions.

Device	OS version
Mi Band 6	V0.82.17.3
Xiaomi Mi A2 (rooted)	Android 10 (API 29)
BQ Aquaris (rooted)	Android 8.1 (API 26)
Genymotion emulator	Android 6.0 (API 23)

3.1.1. Xiaomi Mi Band 6

The Xiaomi *Mi Band* 6 has many hardware sensors explored by the *Zepp Life* application. The *Mi Band* 6 is a small — 47.4 × 18.6 × 12.7 mm — and lightweight — 12.8 g — wrist-wearable device with a 360 × 152 pixels display. It features several sensors: a 3-axis accelerometer, a 3-axis gyroscope, heart rate, blood oxygen saturation (SpO$_2$), and proximity sensors. It has 512 MiB of RAM and 16 GiB of persistent storage, is powered by a 125 mAh battery, and is presented as having a water resistance up to 5 ATM (Band 6 Review, 2021). As reported earlier, the Mi Band set, namely Mi Band 4 onward, is reported to have good accuracy for step count and heart rate measurements in laboratory tests (de la Casa Pérez et al., 2022). The *Mi Band* 6 uses Bluetooth Low Energy 5.0 (BLE 5.0) to connect with its paired smartphone. Another model — the *Mi Band* 6 NFC — adds Near-Field Communication (NFC) support. The NFC model was initially only available in the Chinese edition of the band but was later made available in the so-called global edition. This paper studies the non-NFC global edition of the *Mi Band* 6.

3.2. Software

The About screen of the *Zepp Life* app that was studied listed version 6.0.1 for the application and version 2.8.12 for the algorithm. Although we could not find the exact meaning of what is considered “algorithm” by *Zepp Life*, we hypothesize that it is how data are processed to produce several computed metrics, such as walked steps, distance, and Personal Activity Intelligence (PAI) (Zisko et al., 2017).

To collect data and execute commands on the smartphone, we enabled Android *debug mode* and resorted to Android Debug Bridge (ADB) command lines. We collected data through ADB,[3] focusing on analyzing SQLite3 databases and XML files, as we shall see later. To analyze and query *Zepp Life*'s SQLite3 databases, we used DBBrowserforSQLite[4] and litecli[5] software tools. Other tools include the HxD[6] hexadecimal editor, Python's JSON. tool module to make JSON data human readable, and the ent[7] command line application to measure the entropy of files and hence detect compressed and encrypted files. The software tools employed in our research are listed in Table 2.

3.3. Method

To populate *Zepp Life* with data, we put the *Mi Band* 6, coupled with the rooted smartphone, through several testing scenarios, which can be summarized as follows: *i*) *regular usage*; *ii*) *workout usage*; *iii*) *phone notification*. Regular usage is the simple act of wearing the Mi Band 24 h/day, with the fitness tracker monitoring basic biometric parameters, such as heart rate, sleeping times, and steps. Workout usage is activated by the user, who can select one of the 30 available workout modes. In this study, we only analyzed walking and cycling. Finally, phone notifications are the events triggered at the band to signalize phone events like phone calls and reception of messages such as SMS and social media applications (WhatsApp, Messenger, *etc*) notifications. To determine the timezone setting of the timestamps, we conducted tests using two different timezones. Our tests revealed that the Mi Band 6

[3] https://developer.android.com/studio/command-line/adb.

[4] https://sqlitebrowser.org/.

[5] https://litecli.com/.

[6] https://mh-nexus.de/en/hxd/.

[7] https://www.fourmilab.ch/random.

Table 2
Software tools.

Tool name	Version	Usage
Mi Band	V0.1.0.49	Firmware
Zepp Life application	6.0.1	Connected to Mi Band
Zepp Life algorithm	2.8.12	Connected to Mi Band
ADB	1.0.41/33.0.1	Data access
DB Browser for SQLite	3.12.2	Database analysis and queries
litecli	1.7.0 (Linux)	SQLite analysis and queries
Autopsy	4.19.3	Digital forensics analysis
CyberChef	9.37.3	Miscellaneous (timestamp decoder, *etc*)
Visual Studio Code	1.7	Software development
Python	3.10	Module and script development
Python's json.tool	3.10	JSON beautifier
HxD	2.5.0.0	Hex Editor
ent	2008 (Linux)	Entropy calculator

ecosystem records timestamps in UTC.

For each scenario, the pair *Mi Band* 6/*Zepp Life* was used accordingly for a given period, which varies according to the monitored activity. The band was worn 24/7 as it is supposed to be used, allowing the collection of metrics such as daily steps, sleep duration, and modes. We activated the corresponding workout activity through the paired *Zepp Life* application and worked out for at least 30 min for activities such as walking and cycling. To ensure complete access to the data of the Android devices, all devices used in the data collection process were rooted. The data was then collected using ADB commands and subsequently analyzed using the software tools listed in Table 2. It is worth noting that none of the databases extracted were encrypted, simplifying the analysis process.

The need for root access to the companion smartphone might not always be possible nor appropriate in a digital forensic scenario. Acquiring data from non-rooted devices is challenging due to the security protections put in place by manufacturers, which restrict access to data. As a result, forensic tools and investigators often need to use exploits or other techniques to access the data stored on non-rooted devices (Fukami et al., 2021). This is a time-consuming process and may not always be successful, leading to potential limitations in the amount or type of data that can be acquired or, in the worst case, data loss. Due to the complexity and device-specific nature of this process, acquiring data from non-rooted devices falls outside the scope of this work.

4. The Zepp life application

The main screen of the *Zepp Life* Android application comprises several panels, as shown in Fig. 1. If the panel does not fit on a single screen, the interface can be scrolled up, revealing more panels. By default, *Zepp Life* displays the live count of steps taken so far in the current day on its main screen. This provides an indication of the user's progress towards their daily step goal. For example, Fig. 2 shows detailed information when the *Steps* panel is pressed on the main screen.

When the screen content is scrolled up, there is a timeline depicting each stage of the user's last night of sleep, deep sleep, light sleep, REM (Rapid Eye Movement), and awakening. Further down is the heart panel, which displays the current and average heart rates for the previous 24-h day. Further below, the application displays the so-called Personal Activity Intelligence — PAI (Zisko et al., 2017), which is a metric to track and measure a person's physical activity. The PAI requires continuous heart rate monitoring, substantially depleting the battery, and thus it is not enabled by default. In the next panel, the application presents a summary of the last workouts performed by the user. Female health is next, and it deals with menstruation, with the user's data needing to be manually inputted. Further down, the *weight* panel shows the user's weight. This panel can be filled manually or automatically if the user has a compatible weighing scale. Note that the user can configure the main screen, adding or removing panels. More importantly, by clicking into a panel, the user accesses a more detailed view of the data. For instance, the walked steps panel will break down step activity by hours, besides giving statistics, such as steps per week, month, and years, amid other data.

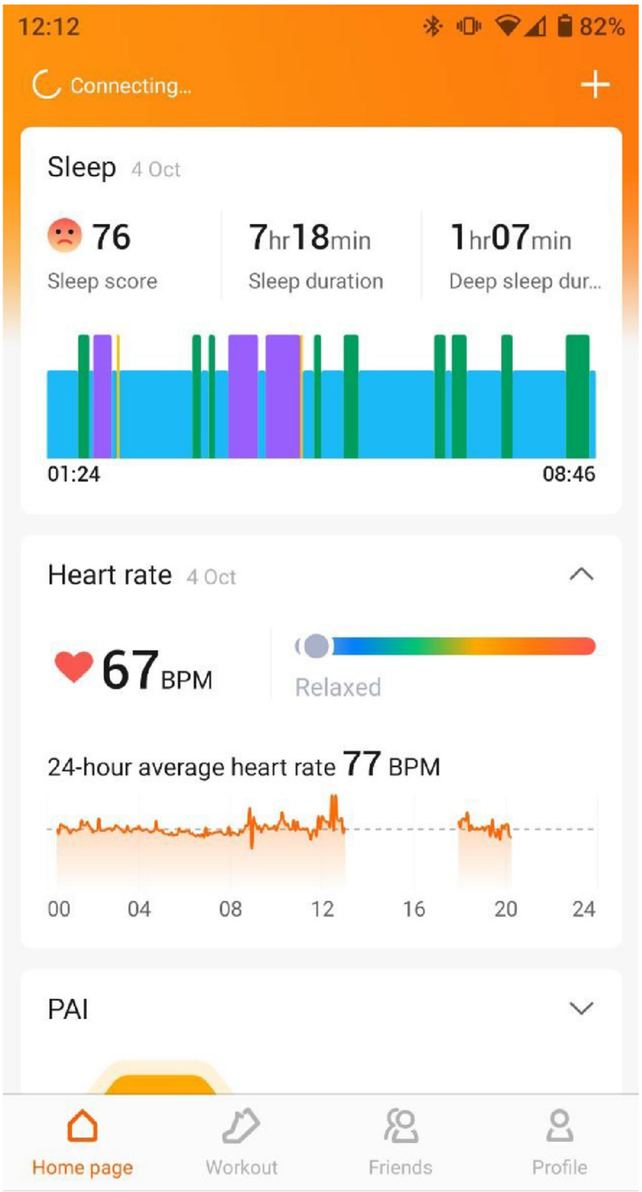


Fig. 1. Main screen of *Zepp Life*

The *Zepp Life* application also has a “friends” section. Users can add other *Zepp Life* users within this section, sharing their physical activity and sleep data. For this purpose, one has to scan a QR code that holds the other user's identification or use the userID of the remote user. Both can be displayed in *Zepp Life* through the option *My QR Code* of the *Friends* activity. The QR code holds a simple JSON-formatted string with the *Zepp Life*'s userID, his/her username, and in the latest version, a field named ftoken, which is a 114-character long invitation token. The userID is represented as a

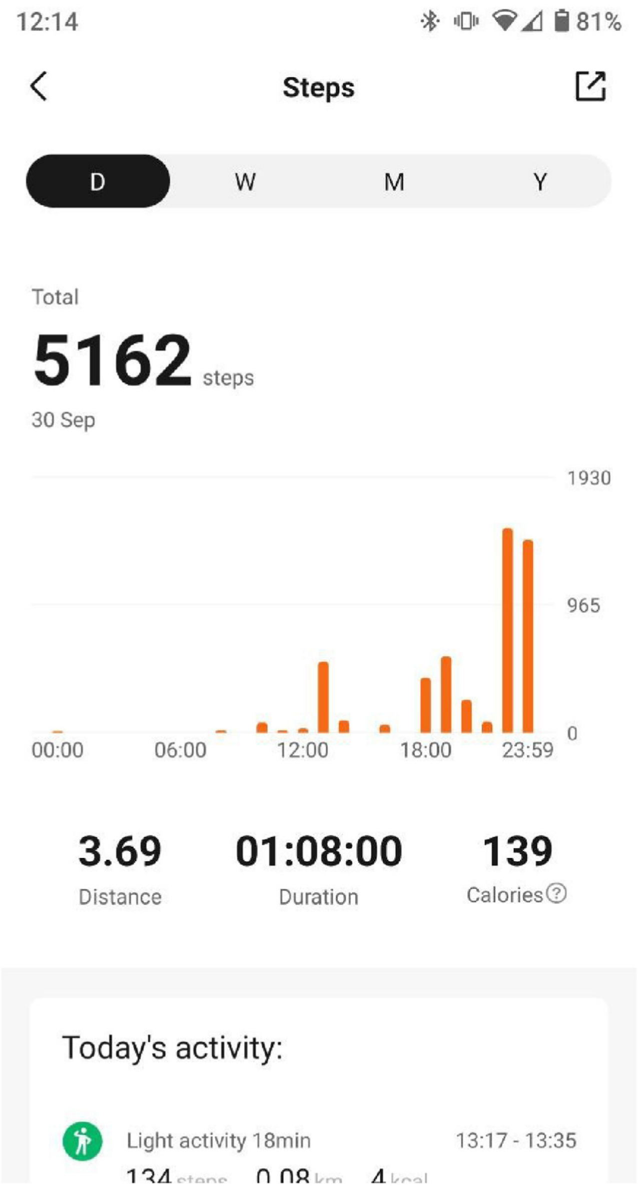


Fig. 2. *Zepp Life* detail of the *Steps* count.

10-digit integer. Listing 1 shows a generic JSON string for a Friend QR code invitation. If the friendship invitation is approved by the other user, both users start sharing metrics regarding daily walking and sleeping activities. Walking metrics include walked steps, distance, and burned calories, while sleep data encompass asleep time, wake-up time, and sleep duration. Besides this data sharing, one can “nudge” a friend through the *Zepp Life* application. A nudge materializes by a notification at the friend, which makes the band vibrate and display the message “FRIEND has nudged”, with the mobile application keeping a record of the nudge.

Table 3
Most relevant functionalities of the Mi Band 6.

Feature	Description
Heart rate	Measure the heart rate.
Oximeter	Measure the level of oxygen in the blood, also known as SpO_2.
Steps	Count the number of steps.
Sleep	Analyze sleep along four main components: deep sleep, light sleep, rapid eye movement (REM), and awaken time.
Workout	Allow selecting one of 30 workouts (walking, running, swimming, etc.). Some workouts require active GPS on the smartphone.
Notification	Mi Band vibrates and displays a message for some smartphone notifications (e.g., calls, SMS, WhatsApp, *etc.*).
Time	Time-related functions such as chronometer, countdown timer, and the so-called Pomodoro technique.
Weather	Display weather prediction for the user's location (given by the smartphone's GPS or inferred from the IP address).

Table 4
Android permissions requested by the *Zepp Life* application.

Permission	Usage
Call log	Access and modify the call log
Camera	Take photos and videos
Address book	Access the phone address book
Location	Access geolocation
Microphone	Record audio
Body sensors	Access to wearable sensors
Messages	Access to the phone messages
Storage	Access to the phone storage
Call	Place phone calls

Table 3 lists the most relevant features of a paired *Mi Band* 6/*Zepp Life*. There are other features such as “Find my Device”, which triggers the phone to ring so that it can be more easily located, which are not considered in this work, as they do not yield relevant forensic artifacts.

4.1. Android permissions

The *Zepp Life* application requires a set of Android permissions that must be enabled when the application is installed or the first time a feature of the application is used. The Android permissions for the *Zepp Life* application are listed in Table 4.

4.2. Databases

Under the databases directory, the application holds seven SQLite3 database files. The names of the databases, the number of tables, and a brief description are given in Table 5. We also provide, for each database, the number of tables that hold records, as we observed that many tables were empty. Note that _ID seen in Table 5 in the name of the database corresponds to the 32-characters of the MD5-hashed identifier of the account's ID of the data, as we explain later.

Listing 1
JSON string of a *Zepp Life* Friend QR code invitation

```
{
   "uid":704.......,
   "username":"REDACTED",
   "ftoken":"AHROigzOdCamFUmcp... (base64 114 character token)"
}
```

Table 5
Brief description of *Zepp Life*'s databases. The column "# tables" displays the total of tables of the database and, within parenthesis, the number of tables with data.

Database	# tables		Description
FemaleHealth_ID.db	4	(0)	Records female health data (data need to be manually inserted.)
FitTime_ID.db	45	(1)	Deal with the network of friends.
origin_d_ID	61	(14)	Misc. data (alarm, weight info, *etc*)
ppg_db	4	(0)	Photoplethysmography (PPG) optical technique.
spo2	8	(1)	Data regarding SpO_2 oxygen measurements.
stress__ID.db	3	(3)	Data to assess stress level.

4.2.1. Female health

The FemaleHealth_ID.db database holds four tables related to the female reproductive cycle. As the data has to be manually inserted by the user, it is not certain that data will exist. It is worth noting that the Electronic Frontier Foundation (EFF) has warned about the possible privacy danger if these personal data fall into the wrong hands (McCallum, 2022).

4.2.2. Origin

The origin_db_ID database holds the most meaningful digital forensic data. It has 61 tables, although, in our setup, only a minor number of tables had data. These tables are listed in Table 6 and classified regarding the digital forensics value. Next, we analyze the most relevant, forensically speaking, of these tables.

4.2.2.1. origin_db_ID/DATE_DATA.

This table holds one record per day. The day of the record is identified by the date kept in ISO format (YYYY-MM-DD) in the DATE field. The main fields of the DATE_DATA table are shown in Table 7. The column DATA contains a JSON string that encodes one-day worth of data, as the two JSON fields start $= 0$ and end $= 1439$ corresponds to the number of minutes of a day, while the did field corresponds to the device ID. The primary data of this JSON string is data, which holds base64-encoded data that we could not interpret. The field DATA_HR of table DATE_DATA is a BLOB with 1 440 bytes, holding the heart rate for each minute of the 1 440 min of the day. From a forensic point of view, the most relevant data field of DATE_DATA table is SUMMARY, a JSON string which, as the name implies, summarizes the daily activity, which comprises two main elements: walking and sleep.

Table 6
Non-empty tables of the origin_db_ID database.

Table	Forensic	Description
	value	
ALARM	low	User configured alarms
CONFIG	low	Configuration of the band
DATE_DATA	high	Logs several metrics per day (steps, heart rate, etc.)
DEVICE	fair	Data about the band
FRIENDS	high	Data about *Zepp Life*'s friends
HEART_RATE	fair	Logs heart rate values
HM_PROPERTY	low	Generic flag repository
MANUAL_DATA	fair	Data manually inserted by the user
REMINDER	fair	Reminders set by the user within the application
RUNCONFIG	low	Configuration for workouts
TRACKDATA	high	Data about workout activities
TRACKRECORD	high	Details regarding TRACKDATA
USER_INFOS	high	Personal data of users (name, birthdate, weight, …)
WEIGHT_INFOS	low	Weight data

Table 7
Main fields of the table DATE_DATA

Name	Type	Description
SOURCE	Integer	ID of the device
DATE	Text	Date in ISO format (YYYY-MM-DD)
SUMMARY	Text	JSON string that summarizes activities performed in day DATE
DATA	Text	JSON string holding one-day data
DATA_HR	BLOB	Holds heart rate for each of the 1 440 min of the day (one byte per minute)

Table 8
Main attributes of a slp entry in JSON summary object.

Name	Type	Description
st (start)	UNIX timestamp	start sleep datetime (UTC)
ed (end)	UNIX timestamp	end sleep datetime (UTC)
dp (deep)	integer	total time spent in "deep" sleep
lt (light)	integer	total time spent in "light" sleep
wk (awaken)	integer	total time spent "awaken"
stage	array	list of intervals of each stage (start, stop, mode)

For this purpose, besides some global statistics of the day, the SUMMARY field details several elements with the JSON object summary, namely: the step activity within the stp property and the sleep cycle with the slp property. Next, we describe each of these properties.

slp. The slp property has six main attributes, which are summarily described in Table 8. The slp attribute tracks sleep cycles. A sleep cycle comprises a mix of four modes — deep sleep, light sleep, awake, and Rapid Eye Movement (REM) — with the last one being the dream stage. A sleep mode is recorded in the JSON object through the integer mode attribute. Table 9 lists mode values and corresponding sleep stages.

Table 11
Attributes of the stp property of the SUMMARY object.

Attribute	Datatype	Summary
Ttl	integer	Total number of steps
Dis	integer	Total distance (meters)
Cal	integer	Total burned calories
Wk	integer	Total walking time (minutes)
Rn	integer	Total running time (minutes)
runDist	integer	Total running distance (meters)
runCal	integer	Total calories burned while running
stage	array	Keep records of each activity (walking/running)

Listing 2
Partial listing of a slp attribute

```
{ "..."
   "slp":{
      "st":1663282200,
      "ed":1663307760,
      "dp":91,
      "lt":275,
      "wk":3,
      "usrSt":-1440,
      "usrEd":-1440,
      "wc":1,
      "is":44,
      "lb":59,
      "to":0,
      "dt":57,
      "rhr":60,
      "ss":86,
      "stage":[
         "..."{
            "start":1490,
            "stop":1516,
            "mode":4
         },
         "..."
      ]
   },
   "..."
}
```

An example of the slp JSON construct is given in Listing 2. It has the following meaning: the monitored user started his/her sleep activity in 2022.09.15/23h50:00 (1663282200) and ended it in 2022.09.16/06h56:00 (1663307760). We can observe that during the sleep period, the user was assessed as being 91 min in “deep sleep” (dp), 275 min in light sleep (lt) and 3 min awaken (wk). The stage construct is a JSON array that keeps records of the sleep stages. Indeed, each stage corresponds to the sleep phase and is classified with three attributes: start, stop, and mode. Start and stop keep, respectively, the start and the end of the sleep stage, resorting to relative time in seconds, that is, the number of seconds since the start of the sleep record. Therefore, to find the time of day that corresponds to start, one needs to sum the value of start with the value of st. For example, in Listing 2, start = 1490 means that this stage started 1490 s (slightly less than 25 min) after the start of the sleep record, that is around 2022.09.16/00h15:00. Table 10 describes the three fields of the stage attribute.

Table 9
Mode attribute values and corresponding sleep stages.

Mode	Type of sleep
4	light sleep
5	deep sleep
7	time awake
8	Rapid Eye Movement (REM)

Table 10
Attributes of the JSON array stage of a sleep record.

Attribute	Datatype	Summary
start	integer	When this mode started (number of seconds since st)
stop	integer	When this mode stopped (number of seconds since st)
mode	integer	Type of activity

stp. The stp property of the SUMMARY object has eight main attributes to record daily step activities. These attributes are briefly described in Table 11. An example of a SUMMARY JSON record is shown in Listing 3.

Listing 3
Partial listing of a stp attribute

```
{
   "...",
   "stp":{
      "ttl":7119,
      "dis":5235,
      "cal":219,
      "wk":97,
      "rn":0,
      "runDist":204,
      "runCal":32,
      "stage":[
         "..." {
            "start":518,
            "stop":589,
            "mode":7,
            "dis":460,
            "cal":17,
            "step":590
         },
         "..."
      ]
   }"..."
}
```

An important attribute of the SUMMARY object is the JSON array stage. This array records all the individual activities – one array element per activity – that contribute to the total of steps which is accounted for in the ttl field. The content of an individual array element is described in Table 12, while Table 13 interprets the values of the mode field within a stp element.

Contrary to the slp object, there are no start and end fields in stp, as it is not needed since the daily step/activity account starts each day at midnight and ends at 23h59m59s. Note that the SUMMARY object and its property stp exist as part of a record in the table DATE_DATA, which also holds the field DATE that points out the date/time of the record.

Listing 3 gives a partial view of the JSON field. Interestingly, since 2022.03.01, another two fields – DATA and DATA_HR– are being filled by the application. DATA is a binary blob we could not interpret. The other one is DATA_HR, also a binary blob, which contains 1 440 bytes, one byte per heart measurement, corresponding to one measurement per minute for one day. The hexadecimal FF marks minutes that do not have a heart measurement.

4.2.2.2. origin_db_id/FRIENDS. Table FRIENDS keeps the so-called *friends* of the *Zepp Life* account user. As stated earlier, a *Zepp Life friend* is another account with whom the user shares daily walking and sleep metrics and can interact by sending a *nudge*. For each *Zepp Life* friendship, table FRIENDS has one record holding the UID, USERNAME, WEIGHT, and BIRTH_DAY of the friend. This data record also has three Unix EPOCH millisecond-precision timestamp fields, all in UTC: LAST_UPDATE_TIME, CREATE_TIME, and LAST_DETAIL_UPDATE_TIME. The former keeps the date/time of the last time data were received from the friend, while CREATE_TIME is the date/time of the friendship creation, and LAST_DETAIL_UPDATE_TIME holds the date/time of the last synchronization between the two accounts. Other fields of the FRIENDS table are the self-describing STEP, DISTANCE, and CALORIE. The main fields of the FRIENDS table are shown in Table 14.

Table 12
Attributes of the JSON array stage of a step record (Table DATE_DATA).

Attribute	Datatype	Summary
start	integer	When the activity started
stop	integer	When the activity ended
mode	integer	Type of activity
dis	integer	Distance (meters)
cal	integer	Burned calories
step	integer	Number of steps of the activity

Table 13
Mode values of stp element (Table DATE_DATA).

Mode	Summary
1	slow walk
3	fast walk
4	run
7	light activity

4.2.2.3. origin_db_id/MANUAL_DATA. The MANUAL_DATA table holds information regarding data manually edited by the user through *Zepp Life* interface. The table is organized per date, that is, there is a record per date whenever a record of that date was manually edited. The information held by the table can be important in digital forensic analysis, as it reveals that a manual edition of data has occurred. Thus it might be an attempt for the user to forge evidence, for example, by setting back the time of sleep. Note that this manual tampering can be easily spotted, as the original device-created record is kept untouched in the DATE_DATA table, and a record with the manual edition is created in the MANUAL_DATA table. Additionally, to the best of our knowledge, sleep-related data is the only one captured by the device that can be manually edited.

4.2.2.4. origin_db_id/REMINDER. The REMINDER table records reminders explicitly set by the user through the *Zepp Life* application. Reminders are very short text messages – 16 characters maximum – appearing in the Mi Band display at the date/time set by the user. To signalize the reminder, the band vibrates, and the message is displayed on the band screen. The user can acknowledge the reminder, end it, or snooze it for another 10 min. The most relevant fields of the REMINDER table are listed in Table 15.

4.2.2.5. origin_db_id/DEVICE. The measuring devices that provide data to the *Zepp Life* application are described in the table DEVICE.

Table 14
Main fields of Origin_DB_ID/FRIENDS table.

Name	Type	Description
UID	text	Friend's 10-digit User ID
USERNAME	text	Friend's username
WEIGHT	integer	Friend's weight
CREATE_TIME	integer	Date/time of friendship creation
LAST_UPDATE_TIME	integer	Date/time of friend's last received metrics (UTC Unix Epoch in milliseconds)
LAST_DETAIL_UPDATE_TIME	integer	Date/time of friend's last synchronization (UTC Unix Epoch in milliseconds)

Table 15
Main fields of the reminder table.

Name	Type	Description
_id	integer	Date/time when the reminder was set (UTC UNIX millisecond timestamp)
START_DATE	text	Date/time of the reminder (*e.g.*, 2022-08-22 10:54)
STOP_DATE	text	Date/time of termination
BODY	text	Message of the reminder

Each device is identified by a device ID (DEVICE_ID), which in the case of a Mi Band corresponds to the concatenation of the Bluetooth MAC address with the pair of bytes FFFE, while the table also includes the MAC address of the device in the field DEVICE_ADDRESS. The table provides several date/time fields, such as the bind date/time (field DEVICE_BIND_TIME), the date/time of the last synchronization of the band with the application (DEVICE_SYNC_DATA_TIME). Device data also includes its serial number (SN) and several version numbers, such as the firmware version (FIRMWARE_VERSION), the hardware version (HARDWARE_VERSION), and the product version (PRODUCT_VERSION). Furthermore, the table also holds the USER_ID, a 128-bit authentication key (AUTHKEY), and several synchronization timestamps, such as AF_RESULT_SYNC_TIME, with AF standing for atrial fibrillation, and P_SPO2_SYNC_TIME, to name just a few. Table 16 lists the main fields of DEVICE table.

4.2.2.6. origin_db_id/HEART_RATE. The HEART_RATE table collects Mi Band's heart rate measurements. It holds the heart rate and the UTC timestamp, which is kept in the TIME field, a UNIX EPOCH 32-bit timestamp. Another field is DEVICE_ID, a 64-bit that identifies the measuring device, that is, the Mi Band. The heart rate can play an important role in an investigation, as evidence of the band bearer being alive and high heart rates, as a possible indicator of high-intensity physical activity or emotional stress. A summary of the HEART_RATE table is given in Table 17.

Table 17
Main fields of the HEART_RATE table.

Field	Datatype	Description
TIME	integer	UTC Unix timestamp (seconds)
HR	integer	Heart rate
DEVICE_ID	text	Device identifier (hexadecimal text)

4.2.2.7. origin_db_id/TRACKRECORD and origin_db_id/TRACKDATA. The TRACKRECORD table keeps workout activities that are manually activated by the user. Activities include hiking, running, and cycling (see Fig. 3), to name just a few. Table TRACKRECORD has 61 fields, with many fields being very specific to given activities (*e.g.*, swim_style, altitude_ascent). We selected eight fields and briefly described each one in Table 18. The geohash format (Moussalli et al., 2015) encodes a location's latitude and longitude information into a variable-length string, which is stored in the LOCATION field. This string is known as a *tile*. An example is ez4y97zvdvbq, which corresponds to the following GPS coordinates: 40.5391535,-7.3171192. The tile's dimensions are determined by its string length, which in turn impacts the accuracy of the geolocation. Longer strings correspond to smaller tiles and therefore provide higher precision. In the case of *Zepp Life*, 12-character strings are used to achieve maximum accuracy, resulting in tiles with centimetre-level dimensions.

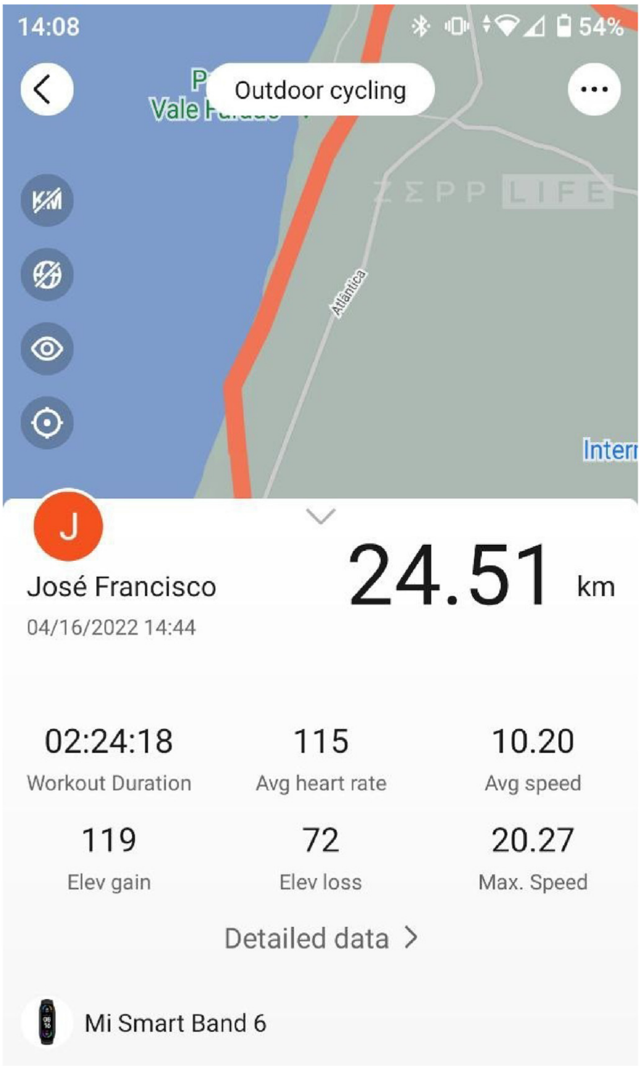
The TRACKDATA table is connected to TRACKRECORD, as it provides detailed data about activities logged in TRACKRECORD. A TRACKDATA record is linked to the corresponding record in TRACKRECORD through the TRACKID field, which represents the UTC timestamp in UNIX Epoch format. The TRACKDATA has 34 fields, although, from a digital forensic perspective, the most relevant, besides TRACKID is BULKLL. This field keeps the GPS coordinates of the activity as shown in Listing 4. The GPS coordinates are kept in text format, in differential mode, as follows: after the first pair, which records the absolute GPS coordinates of the starting point with 7-digit precision, the following GPS points are relative to the previous one. For instance, in Listing 4, the starting point is kept as 416174929, −75734916, which corresponds to 41.6174929 North and 7.5734916 West, while the second point can be obtained by adding −799 and −967, respectively to the latitude and the longitude of the previous point. To obtain the coordinates of the third GPS point, one has to add −1534 and 267 to the second point, and so on. The character "; " is the separator. Note, however, that GPS coordinates for a given workout are only available in the database if the path workout has been visualized on the device.

Table 16
Main fields of the DEVICE table.

Field	Datatype	Description
DEVICE_ID	text	ID of the device (hexadecimal text)
DEVICE_ADDRESS	text	Bluetooth MAC address (hexadecimal text)
DEVICE_BIND_TIME	integer	Date/time of device binding with the application, UTC UNIX timestamp in milliseconds
SN	text	Serial number
USER_ID	integer	10-digit identifier of the user account
AUTHKEY	text	128-bit authentication key (hexadecimal text)

Listing 4
Partial content of BULKLL field

```
416174929,75734916;-799,-967;-1534,267;-2299,-2900;-1165,-1166;-1634,-632;
732,-400;-1432,-799;-1667,-166;-1533,-233;-1366,33;-1;-1132,333;-1067,400;
033,365;-1067,400;
```



José Francisco
04/16/2022 14:44
24.51 km
02:24:18 Workout Duration
115 Avg heart rate
10.20 Avg speed
119 Elev gain
72 Elev loss
20.27 Max. Speed
Mi Smart Band 6

Fig. 3. *Zepp Life* detail view of a *outdoor cycling* workout.

Table 18
Main fields of the table TRACKRECORD

Name	Type	Description
DATE	text	Date in ISO format (YYYY-MM-DD)
TYPE	integer	Type of activity (walking, pilates, etc.)
TRACKID	integer	Start of activity (UTC UNIX timestamp)
ENDTIME	integer	End of activity (UTC UNIX timestamp)
DISTANCE	integer	Travelled distance
CAL	integer	Burned calories
AVGHR	integer	Average heart rate
LOCATION	text	Location expressed in geohash format

4.2.2.8. origin_db_id/USER_INFOS. The USER_INFOS table holds the user's personal information. This includes user-supplied data such as name, birthday, gender, and height. Other relevant fields are the USER_ID and the self-explaining field AVATAR_URL. The field CREAT_TIME records, in UTC Unix Epoch timestamp format, the date/time of the account creation, while LAST_LOGIN_TIME keeps the date/time of the last login, also in the same timestamp format. Finally, the field LOCATION keeps the name of the location (*e.g.*, name of the town), and it is filled automatically by the application. The main fields of the USER_INFOS are listed in Table 19.

4.2.3. origin_db_id/SPO2_ID

The SPO2_<ID> database, where <ID> is, as reported earlier, the MD5 hash of the user numerical identification, holds six tables related to oxygen saturation levels. Table 20 summarily describes the tables of the SPO2_<ID> database. Most tables seem to be linked to oxygen related metrics pointing out sleeping-linked respiratory problems such as obstructive sleep apnea (OSA). This is the case of the four tables — origin_osa_event, origin_osa_process, osa_event and osa_process — whose name includes OSA, and also of the table ODI, with ODI corresponding to Oxygen Desaturation Index, a metric used to assess obstructive sleep apnea (Rashid et al., 2021). All these features are linked to the monitoring of sleep-breathing quality.

In our study, solely the table click_measured_spo2 had records. Each record corresponds to an oxygen saturation measurement triggered by the user. The main fields of the table are shown in Table 21. The forensic value of the data of the click_measured_spo2 table is limited, as measurements need to be explicitly triggered by the user.

Table 19
Main fields of USER_INFOS table (origin_db_ID database).

Name	Type	Description
USER_ID	text	ID of user
NAME	text	Registered name of the user
BIRTHDAY	text	Birthday of user
GENDER	integer	1 = male; 2 = female
HEIGHT	integer	Height in centimeters
WEIGHT	real	Weight in kilograms
CREAT_TIME	text	Date/time when the *Zepp Life* account was created (UTC Unix timestamp seconds)
LAST_LOGIN_TIME	text	Date/time of last login (UTC Unix timestamp seconds)
LOCATION	text	Name of town (filled automatically)

Table 20
Tables of the SPO2 database.

Name	Description
click_measured_spo2	Keeps user-triggered O_2 measurements
Odi	Oxygen Desaturation Index
origin_osa_event	Related to Obstructive Sleep Apnea
origin_osa_process	Related to Obstructive Sleep Apnea
osa_event	Related to Obstructive Sleep Apnea
osa_process	Related to Obstructive Sleep Apnea

Table 21
Fields of the click_measured_spo2 table.

Name	Type	Description
userId	text	User ID
utcTimestamp	integer	timestamp of measurement (UNIX Epoch milliseconds)
spo2	integer	SpO_2 value (80–100)
deviceSource	integer	device identification within the DB
deviceId	text	Bluetooth MAC address of device
Sn	text	Serial number
spo2History	text	60-value array (*e.g.*, [96,0,0,50,0,34,-49,*etc*])
timeZoneId	text	Time zone in text (*e.g.*, Europe/Paris)
Date	text	Date (ISO format)
uploaded	integer	1 if data have been uploaded, 0 otherwise

4.3. Shared preferences

The Shared Preferences directory contains several relevant files, most of which are in XML format, although some of these files also include significant parts in JSON format. One of the most important files is hm_id_sdk_android.xml as it holds several tokens that can be used to access the user account through *Zepp Life* backend service. Specifically, the JSON record Token_info, shown in Listing 5 holds the app_token and the login_token. Note that although the app_token can be used to access the user's data kept at *Zepp Life* backend, the time to live (henceforth TTL) of the token, expressed by the field app_ttl is 43 200 s, that is, 12 h. The login_token has a TTL of 31 536 000 s, that is, 365 days.

loc_weather.xml

The *Mi Band* 6 can display a 5-day weather prediction for the current localization of the band. This feature is provided by the *Zepp Life* application and requires an active BLE connection linking the band to the internet connected smartphone. Forensically, this is an interesting feature as it provides data regarding the last recorded localization of the pair band/smartphone. The weather data is persisted in the XML file loc_weather.xml. Additionally, if GPS is enabled on the smartphone, the persisted data in the file includes the GPS coordinates, the town, and, when available, even the street name. A partial and redacted version of a loc_weather.xml file is shown in Listing 6.

4.4. Cloud access

Like many mobile applications, *Zepp Life* communicates and keeps data with a cloud backend system. This cloud system can be accessed through a web interface allowing for several operations to be performed, namely *i*) Clear Data, *ii*) Delete Data, *iii*) Revoke Authorization, and *iv*) Export Data, as shown in Fig. 4. Specifically, these functionalities are accessed through https://mifit.huami.com/t/account_mifit or https://user.huami.com/privacy2/index.html, requiring the email address and password linked to the Mi Band account. The most important functionality for a digital forensic investigation is the Export Data which, as the name suggests, allows to export data. For this purpose, the user has to define the data's range dates (start and end). Afterwards, a ZIP archive is sent by email to the user. The ZIP archive name comprises the user ID and, separated by an underscore, the UTC UNIX Epoch timestamp in milliseconds (*e.g.*, ID_Timestamp). The ZIP archive is protected by an 8-character password, which is shown in the web interface, but not sent in the mail that has the ZIP archive. As documented in Table 22, the ZIP archive holds nine directories, each holding a CSV file with the user's data.

Although the web accessibility of the *Zepp Life* cloud backend offers a means for the forensic team to export valuable data, as long as the account-linked email and the corresponding password are known, it also poses a risk to the data. Indeed, someone knowledgeable of the pair email/password can access the backend through the web interface and activate either the Clear Data or the Delete Data operation. This can seriously hinder the data collection from the *Zepp Life* application and the investigation.

5. Zepp life forensic data analyzer

To ease and speed up the analysis of Android *Zepp Life* data in a digital forensic post-mortem environment, we developed two programs: ZL_std and ZL_autopsy. The former is a Python 3.6+ standalone script that analyses the SQLite 3 databases of a *Zepp Life* to produce a set of reports. The ZL_autopsy is a Jython-based module

Listing 5
Partial listing of hm_id_sdk_android.xml file (redacted)

```
  "token_info":{
     "app_token":"<APP_TOKEN>",
     "app_ttl":43200,
     "lu_app_ttl":1636302856376,
     "lu_ttl":1636302856376,
     "login_token":"<LOGIN_TOKEN>",
     "ttl":31536000,
     "mutime_long":0,
     "user_id":"<USERID>"
  }
```

Listing 6
Partial and redacted content of loc_weather.xml file

```
<map>
    <long name="lastTimerStamp" value="1661292256300" />
    (...)
    <string name="LastLocationDetail">40.5391535,-7.3171192,Portugal</string>
    <string name="LastLocation">Guarda</string>
    <string name="KEY_LAST_LOCATION">   {"longitude":-7.3171192,"latitude":40.53⌋
↪    91535,"altitude":0,"has_altitude":false,"address":{"countryCode":"PT","adm⌋
↪    in":"Guarda","locality":"Guarda","thoroughfare":"Chãos"}}</string>
</map>
```

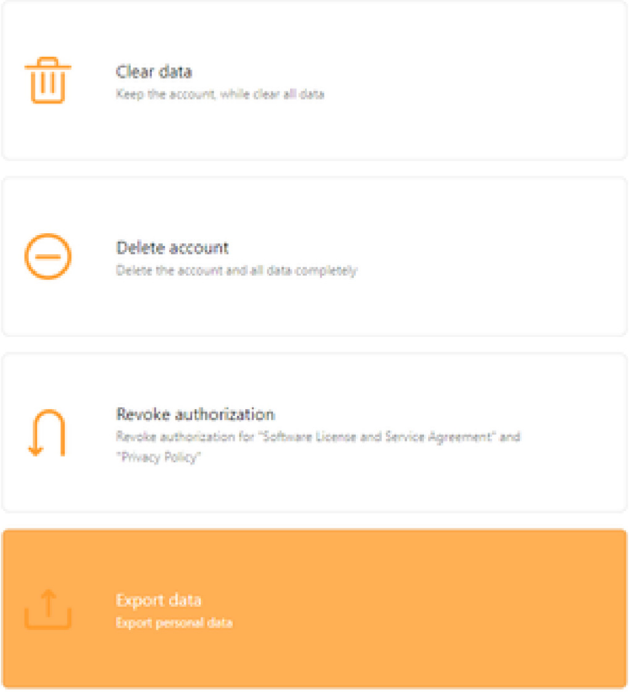

Clear data
Keep the account, while clear all data
Delete account
Delete the account and all data completely
Revoke authorization
Revoke authorization for "Software License and Service Agreement" and "Privacy Policy"
Export data
Export personal data

Fig. 4. Main operations available through the web interface of a *Zepp Life* account.

which runs within the well-known digital forensic software Autopsy and is able to provide the interaction between Autopsy and ZL_std. First, we present ZL_std and then ZL_autopsy. The developed software is open source, and it is available at https://github.com/labcif/MifitAnalyzer under a GNU General Public License v3.0.

5.1. *ZL_std*

The ZL_std software is a Python 3 script run on the command line (see Table 23). It requires a path to a data dump of a *Zepp Life* instance. A data dump is the directory tree of *Zepp Life* collected from the rooted Android device, which was paired with the *Mi Band* 6 and contains the SQLite3 database files and the XML files.

Table 23
Command line parameters of ZL_std

Short	Long	Description
-p	–path	Path of directory holding the data dump
-o	–output	Path for the output report
-h	–help	Standard help
-s	–start	Starting date (optional)
-e	–end	Ending date (optional)
-g	–gps	Create KML file with GPS coordinates (optional)

The behaviour of the ZL_std application can be tailored through command line options. A mandatory option is a -p/–path <DataDump>, which specifies the path to the directory that holds the *Zepp Life* data dump. With the -o/–output option, users can specify the name of the output JSON file. The -s/–start and -e/–end options allow for the specification of a starting and ending date, respectively, so only data that fall within the range of these two dates are processed by ZL_std. When none of these options are specified, the whole data dump is processed. Finally, a Keyhole Markup Language (KML) file can be created from the data dump using the -g/–gps option. This option is only relevant when the data dump contains GPS coordinates, which occur when workouts are performed with the paired smartphone's GPS enabled. A simple working command line of ZL_std is shown in Listing 7, where <path/to/dump> needs to be replaced with the path that holds the dump top-level directory, and -o is followed by the name of the JSON file to be outputted by the application. Additionally, ZL_std also recognizes five non-mandatory environment variables that carry information regarding the forensic case and forensic practitioner(s). The names of the environment variables and a brief description are listed in Table 24.

The ZL_std software runs a set of SQL queries to the SQLite 3 databases and performs analysis of the most relevant XML files. It

Table 24
Environment variables of ZL_std

Name	description
CASE_NUMBER	ID of the forensic case
EXAMINER_NAME	Name of the forensic practitioner
EXAMINER_PHONE	Phone number of the forensic practitioner
EXAMINER_EMAIL	Email of the forensic practitioner
EXAMINER_NOTES	Observations by the forensic practitioner

Table 22
Data provided by *Zepp Life* web export function.

Name	Description
ACTIVITY	Total of steps per day
ACTIVITY_MINUTE	Total of steps per minute (only minutes with steps are recorded)
ACTIVITY_STAGE	Steps, calories, distance organized by time ranges (*e.g.*, from 14h17 to 14h39)
BODY	Several body metrics (weight, height, BMI, bodyWaste, *etc*)
HEARTRATE	Heart rate measured on user demand
HEARTRATE_AUTO	Periodic measurement of heart rate (by default, one measurement per minute)
SLEEP	Sleep data
SPORT	Sport activities explicitly recorded by the user
USER	Several user-related data (userID, gender, height, weight, nickname, birthday)

Listing 7
Partial listing of a ZL_std-produced JSON file

```
python start.py -p <path/to/dump> -o out.json
```

yields two main outputs: *i*) a JSON file with the extracted information from the *Zepp Life*'s dump, and *ii*) a report directory that holds a set of HTML files that summarizes *Zepp Life*'s data. Next, we describe each of these outputs.

5.1.1. *JSON output*

The main purpose of the JSON file is to provide processed data to the ZL_autopsy module for the Autopsy software. Note that the universality and easiness of processing JSON files mean that other software can themselves make use of the JSON file produced by ZL_std. For instance, a program can provide a convenient graphical interface to the forensic data collected from a *Zepp Life* instance. A much-trimmed view of a ZL_std-produced JSON file is shown in Listing 8 showing two heart rate values.

Listing 8
Partial listing of a ZL_std-produced JSON file

```
{
   "...",
   "report":{
      "origin":{
         "hr":[
            {
               "time":1658591348,
               "value":"75",
               "device":"**REDACTED**"
            },
            {
               "time":1658601225,
               "value":"71",
               "device":"**REDACTED**"
            },
            "..."
         ]
      }
   }
}
```

5.1.2. *Report output*

To allow the digital forensic practitioner to analyze relevant artifacts from the data dump, the ZL_std application produces a set of HTML files (Fig. 5) yielding a dynamic site. This way, by resorting to a browser and through the entry point index. html, forensic practitioners can visualize relevant data. For this purpose, there is a left menu bar, shown in Fig. 6, where users can select the data to visualize. For instance, when the Steps entry is selected, the interface will display a plot with steps data, as shown in Fig. 7. A further functionality of the HTML report is date filtering: users can restrict the data visualization to a range of dates through the interface. The date filters are located in the top part of the interface, as shown in Fig. 7.

For the workouts activities, the ZL_std-generated report also displays a map as shown in Fig. 8. For this purpose, ZL_std resorts to OpenStreetMap[8] functionalities. As reported earlier, the GPS coordinates of a given workout are only available on the device database if the path workout has been visualized on the device.

5.2. *ZL_Autopsy*

Autopsy is a well-known open-source software for digital forensics (Javed et al., 2022; Barr-Smith et al., 2021). Built around a graphical user interface, Autopsy provides a set of functionalities for the forensic analysis of digital material. It runs within a Java Virtual Machine (JVM) and encompasses many applications and libraries. Examples of these applications and libraries include the Sleuth Kit to access unmounted filesystems, Tesseract[9] for optical character recognition, PhotoRec[10] for file carving, and Apache Solr[11] to index keyword text for searches, to name a few. Many Autopsy functionalities are available through modules, which can be either *Ingest* or Report modules. An ingest module aims to extract meaningful data and knowledge from the source it is processing to integrate the data/knowledge into the analysis, while a report module is geared toward presenting data/knowledge to benefit the analysis of the digital forensic team. For instance, while an ingest module might process GPS coordinates for a given track, a report module might produce a dynamic HTML file with an embedded map displaying the track.

Autopsy functionalities can be further extended by user-developed modules. Many open source modules are available.[12] Modules can be developed either in Java or in Jython. Jython is a

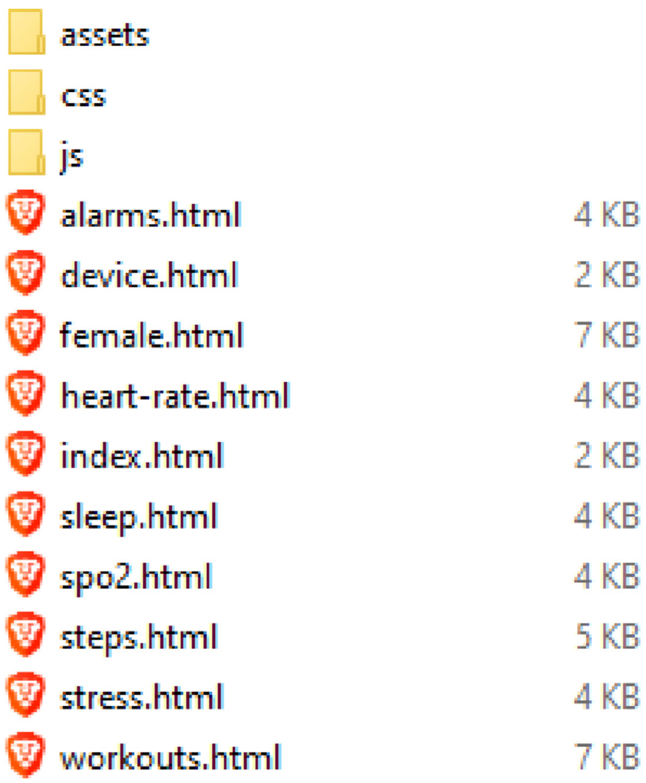
[8] https://www.openstreetmap.org/.

[9] https://github.com/tesseract-ocr/tesseract.

[10] https://www.cgsecurity.org/wiki/PhotoRec.

[11] https://solr.apache.org/.

[12] https://github.com/sleuthkit/autopsy_addon_modules/.



assets	
css	
js	
alarms.html	4 KB
device.html	2 KB
female.html	7 KB
heart-rate.html	4 KB
index.html	2 KB
sleep.html	4 KB
spo2.html	4 KB
steps.html	5 KB
stress.html	4 KB
workouts.html	7 KB

Fig. 5. List of files of an ZL_std report.

Python interpreter that runs within a JVM. We developed the ZL_autopsy module in Jython. ZL_autopsy relies on the autonomous script ZL_std for collecting the needed data from a *Zepp Life* data dump. For this purpose, ZL_autopsy spawns a process to run ZL_std, setting the execution through the command line parameters supported by ZL_std, which, in turn, delivers its results through the JSON output file. When it receives the notification that ZL_std has completed its processing, ZL_autopsy processes the ZL_std's produced JSON file, importing the data within Autopsy so they can be displayed in the Autopsy interface.

Fig. 9 displays the extracted content by the ZL_autopsy script from a *Mi Band* 6 dump. The Bluetooth Adapter corresponds to the *Mi Band* 6 and gathers several data related to the device. A detailed view of the data is provided in Fig. 10a. The Extracted Content encompasses, besides the Bluetooth Adapter, items such as GPS Trackpoints, Alarms, Heart Rate Records, Sleep, SPO2, Steps, and Stress.

As suggested by the graphic symbol assigned by Autopsy, the GPS Trackpoints can also be displayed by Autopsy's internal GPS Geolocation viewer as seen in Fig. 10b. However, Autopsy GPS viewer does not allow for the visualization of individual workout

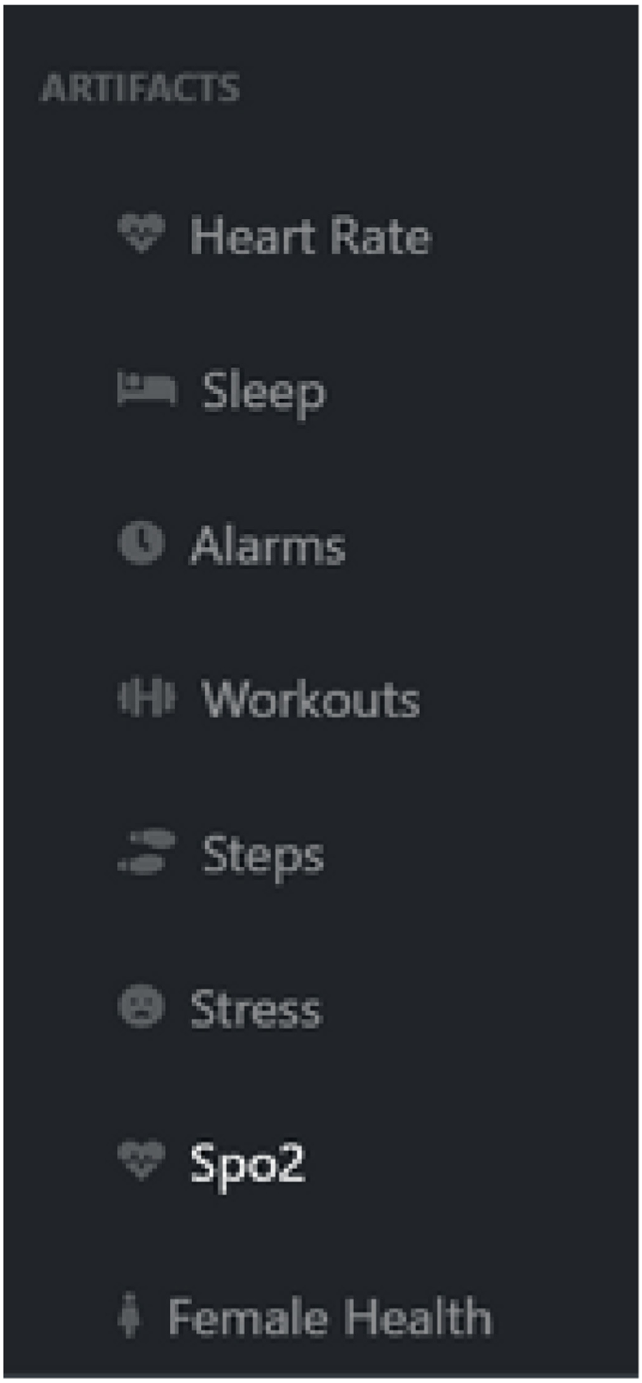
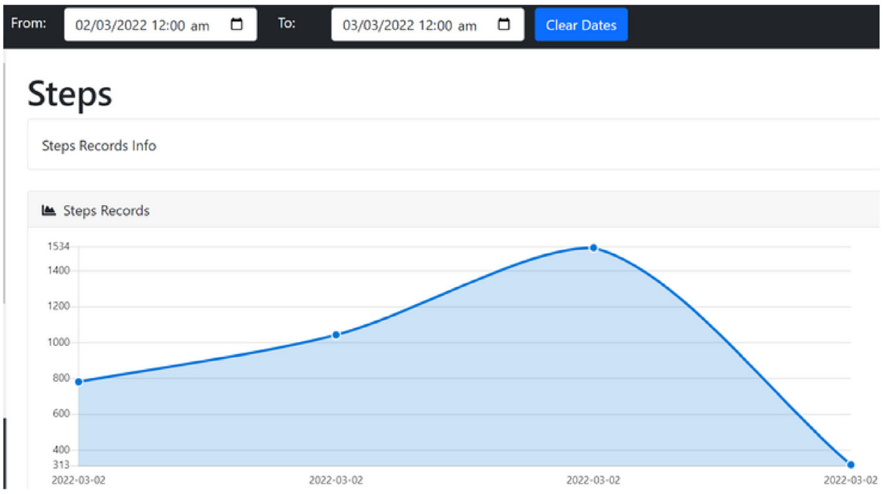


Fig. 6. Left menu bar of ZL_std report interface.



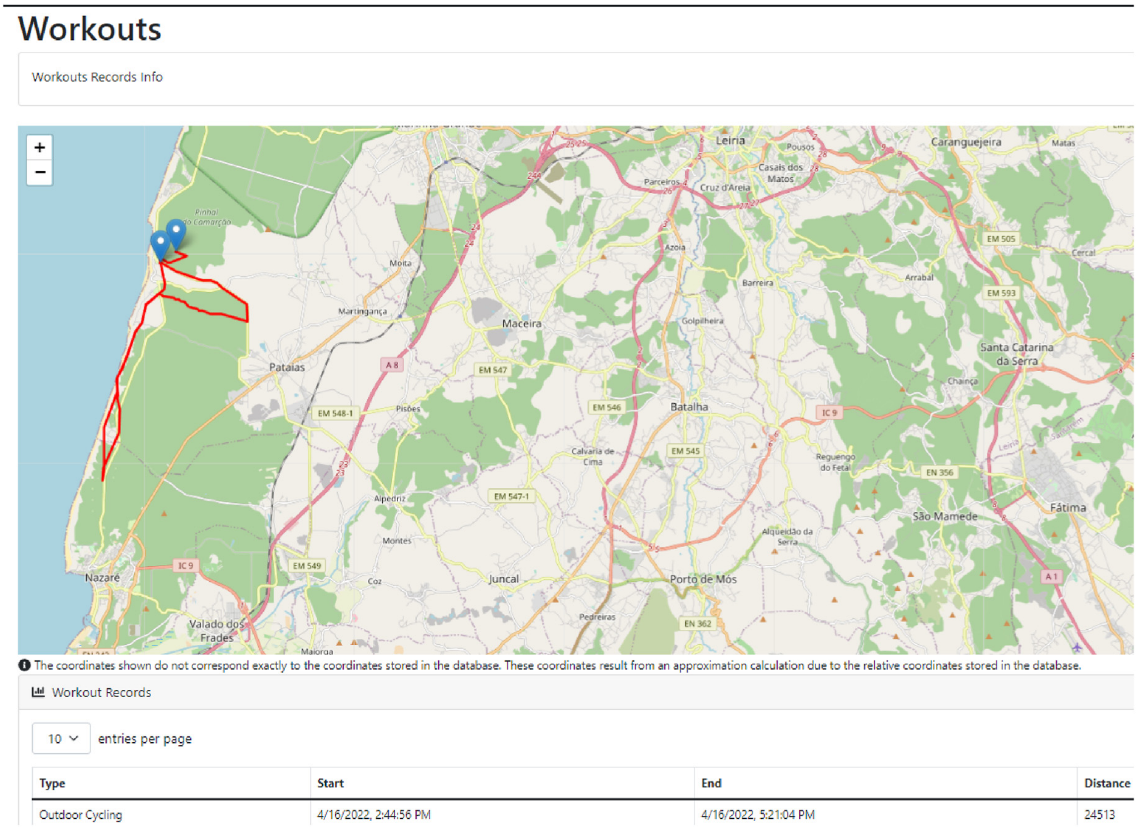
From: 02/03/2022 12:00 am To: 03/03/2022 12:00 am Clear Dates

Steps

Steps Records Info

Steps Records

Fig. 7. Steps data as shown in ZL_std HTML report.



Workouts

Workouts Records Info

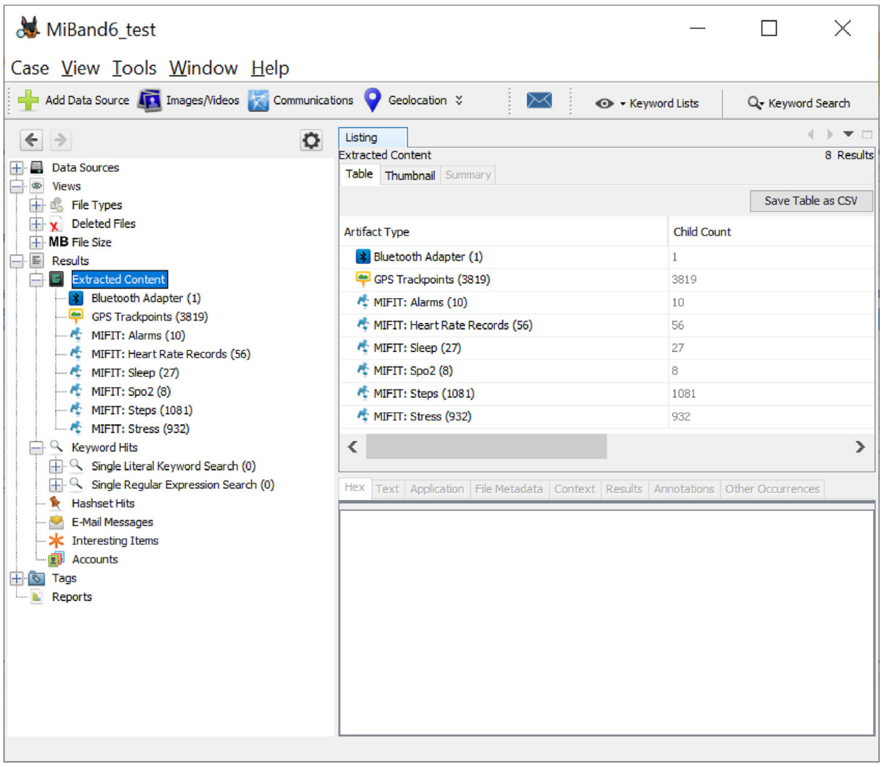
The coordinates shown do not correspond exactly to the coordinates stored in the database. These coordinates result from an approximation calculation due to the relative coordinates stored in the database.

Workout Records

10 entries per page

Type	Start	End	Distance
Outdoor Cycling	4/16/2022, 2:44:56 PM	4/16/2022, 5:21:04 PM	24513

Fig. 8. Map displaying a cycling workout.



Artifact Type	Child Count
Bluetooth Adapter (1)	1
GPS Trackpoints (3819)	3819
MIFIT: Alarms (10)	10
MIFIT: Heart Rate Records (56)	56
MIFIT: Sleep (27)	27
MIFIT: Spo2 (8)	8
MIFIT: Steps (1081)	1081
MIFIT: Stress (932)	932

Fig. 9. Extracted content from a *Mi Band* 6 dump as shown in Autopsy.

paths, as it processes GPS data from several workouts as a whole, as shown in Fig. 10b.

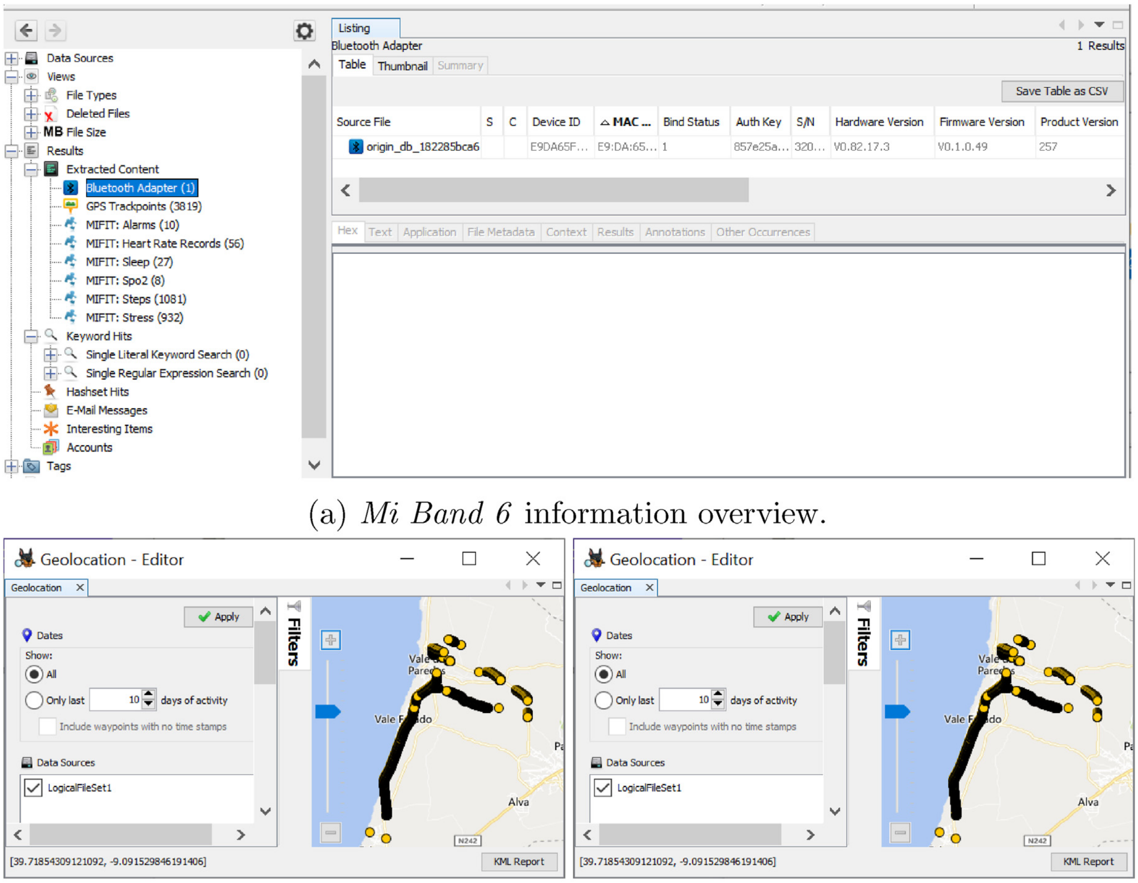
The ZL_autopsy also provides a report module. The report module can be triggered through the Autopsy Report selector, as shown in Fig. 10c. As the module resorts to the reporting functionality of ZL_std, the format and the output of a report are identical to the one provided directly through ZL_std command line script.

6. Conclusion

We analyzed, from a digital forensic point of view, the forensic artifacts left by the *Zepp Life* application ran on a mobile Android device and coupled to a Xiaomi Band 6. Due to its plethora of sensors, the Mi Band 6 collects a meaningful amount of data – heart rate, SpO_2, sleep periods, step counting, and workouts, to mention a few. Some of these data are sent over the cloud and can be collected from there, as long as the access credentials – email and password – are known. Additionally, a large set of data are persisted in XML files and SQLite 3 databases by the *Zepp Life* application and can be accessed for post-mortem analysis to extract digital forensic artifacts. Valuable artifacts include activity/rest/sleep periods, walking steps, oxygen saturation levels, alarms, reminders, and for specific workouts, GPS coordinates, and timestamps in UTC. Past cases demonstrate the high value of accessing and analyzing data from wrist-wearable health trackers. The increased popularity of the *Zepp Life* application – more than 100 million downloads in the Google Play store at the time of this writing – reinforces the potential and value for a digital forensic usage of the data.

To facilitate the use of *Mi Band* 6/*Zepp Life* in forensic analysis, we developed the applications ZL_std and ZL_autopsy. While ZL_std only requires Python 3.6+ to run, ZL_autopsy is a module that extends Autopsy with the ability to extract and analyze data from a *Zepp Life* Android application which has been coupled with a Mi Band.

As future work, we aim to adapt ZL_std and ZL_autopsy to other Mi Band, namely the newly commercialized Mi Band 7 (Xiaomi Mi Smart Band 7, 2022), and to study the iOS version of *Zepp Life*.



Bluetooth Adapter 1 Results

Source File	S	C	Device ID	MAC ...	Bind Status	Auth Key	S/N	Hardware Version	Firmware Version	Product Version
origin_db_182285bca6			E9DA65F...	E9:DA:65...	1	857e25a...	320...	V0.82.17.3	V0.1.0.49	257

Show:
● All
○ Only last 10 days of activity
□ Include waypoints with no time stamps

Data Sources
☑ LogicalFileSet1

[39.71854309121092, -9.091529846191406]

(a) *Mi Band 6* information overview.

(b) GPS data from *Mi Band 6*.

(c) Autopsy report selector

Fig. 10. Autopsy displaying *Mi Band* 6 information.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgment

CIIC partially supported this research under the project UIDB 04524/2020 by FCT/MCTES and EU funds under the project UIDB/EEA 50008/2020.

References

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, pp. 303–311. Reliability and Security, IEEE.

Band 6 Review, Mi, 2021. Yet Another Great-Value Fitness Tracker from Xiaomi. URL: https://www.xda-developers.com/xiaomi-mi-band-6-review. (Accessed 31 March 2023) [Online.

Barr-Smith, F., Farrant, T., Leonard-Lagarde, B., Rigby, D., Rigby, S., Sibley-Calder, F., 2021. Dead man's switch: forensic autopsy of the nintendo switch. Forensic Sci. Int.: Digit. Invest. 36, 301110.

BBC News, 2017. Fitbit Contradicts Husband's Story of Wife's Murder - Police. BBC News. URL: https://www.bbc.com/news/world-us-canada-39710528. (Accessed 31 March 2023) [Online.

BBC News, 2018. Fitbit Data Used to Charge US Man with Murder. URL:. BBC News https://www.bbc.com/news/technology-45745366. (Accessed 31 March 2023).

BBC News, 2021. Greece Killing: Husband Confesses to Caroline Crouch Death. BBC News. URL: https://www.bbc.com/news/world-europe-57523469. (Accessed 31 March 2023).

Canalys Newsroom - Global Wearable Band Shipments up 6% as the Market Shifts to Wristwatches, 2021. URL: https://www.canalys.com/newsroom/global-wearable-band-shipments-up-6percent-as-the-market-shifts-to-wristwatches. (Accessed 31 March 2023).

Casagrande, M., Losiouk, E., Conti, M., Payer, M., Antonioli, D., 2022. BreakMi: reversing, exploiting and fixing xiaomi fitness tracking ecosystem. IACR Transactions on Cryptographic Hardware and Embedded Systems 330–366.

Dawson, L., Akinbi, A., 2021. Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study. Forensic Sci. Int.: Report 3, 100198.

de la Casa Pérez, A., Latorre Román, P.Á., Muñoz Jiménez, M., Lucena Zurita, M., Laredo Aguilera, J.A., Párraga Montilla, J.A., Cabrera Linares, J.C., 2022. Is the xiaomi mi band 4 an accuracy tool for measuring health-related parameters in adults and older people? An original validation study. Int. J. Environ. Res. Publ. Health 19, 1593.

Dorai, G., Houshmand, S., Baggili, I., 2018. I know what you did last summer: your smart home internet of things and your IPhone forensically ratting you out. URL. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3230833.3232814, 10.1145/3230833.3232814.

France, A., 2021. In: Your Fitbit Is Watching You, Scotland Yard Warns Criminals, Evening Standard. URL: https://www.standard.co.uk/news/crime/fitbit-coffee-maker-scotland-yard-b966937.html. (Accessed 31 March 2023).

Franqueira, V.N., Horsman, G., 2020. Towards sound forensic arguments: structured argumentation applied to digital forensics practice. Forensic Sci. Int.: Digit. Invest. 32, 300923. https://doi.org/10.1016/j.fsidi.2020.300923. URL: https://www.sciencedirect.com/science/article/pii/S2666281720300184.

Fukami, A., Stoykova, R., Geradts, Z., 2021. A new model for forensic data extraction from encrypted mobile devices. Forensic Sci. Int.: Digit. Invest. 38, 301169. https://doi.org/10.1016/j.fsidi.2021.301169. URL: https://www.sciencedirect.com/science/article/pii/S2666281721000779.

Gregorio, J., Alarcos, B., Gardel, A., 2019. Forensic analysis of Nucleus RTOS on MTK smartwatches. Digit. Invest. 29, 55–66. https://doi.org/10.1016/j.diin.2019.03.007. URL: https://www.sciencedirect.com/science/article/pii/S1742287618304286.

Hantke, F., Dewald, A., 2020. How can data from fitness trackers be obtained and analyzed with a forensic approach?. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, pp. 500–508.

Hassenfeldt, C., Baig, S., Baggili, I., Zhang, X., 2019. Map My Murder: a digital forensic study of mobile health and fitness applications. In: Proceedings of the 14th International Conference on Availability. Reliability and Security, pp. 1–12.

Javed, A.R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., Gadekallu, T.R., 2022. A comprehensive survey on computer forensics: state-of-the-art, tools, techniques, challenges, and future directions. IEEE Access 10, 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508.

Kang, S., Kim, S., Kim, J., 2020. Forensic analysis for IoT fitness trackers and its application. Peer-to-Peer Networking and Applications 13, 564–573.

Kim, D., Lee, S., 2020. Study of identifying and managing the potential evidence for effective android forensics. Forensic Sci. Int.: Digit. Invest. 33, 200897. https://doi.org/10.1016/j.fsidi.2019.200897. URL: https://www.sciencedirect.com/science/article/pii/S1742287619301367.

MacDermott, Á., Lea, S., Iqbal, F., Idowu, I., Shah, B., 2019. Forensic analysis of wearable devices: Fitbit, Garmin and HETP watches. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, pp. 1–6.

McCallum, B.S., 2022. Period Tracking Apps Warning over Roe V Wade Case in US. BBC News. URL: https://www.bbc.com/news/technology-61347934. (Accessed 31 March 2023) [Online.

Moussalli, R., Srivatsa, M., Asaad, S., 2015. Fast and flexible conversion of geohash codes to and from latitude/longitude coordinates. In: 2015 IEEE 23rd Annual International Symposium on Field-Programmable Custom Computing Machines, pp. 179–186. IEEE.

Odom, N.R., Lindmar, J.M., Hirt, J., Brunty, J., 2019. Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices. J. Forensic Sci. 64, 1673–1686.

Paradiso, C., Colino, F., Liu, S., 2020. The validity and reliability of the mi band wearable device for measuring steps and heart rate. International journal of exercise science 13, 689.

Rashid, N.H., Zaghi, S., Scapuccin, M., Camacho, M., Certal, V., Capasso, R., 2021. The value of oxygen desaturation index for diagnosing obstructive sleep apnea: a systematic review. Laryngoscope 131, 440–447.

Reedy, P., 2023. Mobile device forensics. third edition ed.. In: Houck, M.M. (Ed.), Encyclopedia of Forensic Sciences, third ed. (third ed. Elsevier, Oxford, pp. 613–623. https://doi.org/10.1016/B978-0-12-823677-2.00240-3. URL: https://www.sciencedirect.com/science/article/pii/B9780128236772002403.

Vink, M.M., Sjerps, M.M., Boztas, A.A., van Zandwijk, J.J.P., 2022. Likelihood ratio method for the interpretation of iphone health app data in digital forensics. Forensic Sci. Int.: Digit. Invest. 41, 301389. https://doi.org/10.1016/j.fsidi.2022.301389. URL: https://www.sciencedirect.com/science/article/pii/S2666281722000701.

Williams, J., MacDermott, Á., Stamp, K., Iqbal, F., 2021. Forensic analysis of Fitbit versa: android vs iOS. In: 2021 IEEE Security and Privacy Workshops (SPW). IEEE, pp. 318–326.

Xiaomi mi smart band 7 review. URL: https://www.wareable.com/xiaomi/xiaomi-mi-band-7-review-8838–. (Accessed 31 March 2023).

Xiaomi Re-brands Mi Fit to Zepp Life, Xiaomi Wear App to Mi Fitness, 2022. URL: https://gadgetsandwearables.com/2022/03/18/xiaomi-rename-mi-fit-zepp-life. (Accessed 31 March 2023).

Yoon, Y.H., Karabiyik, U., 2020. Forensic analysis of Fitbit versa 2 data on android. Electronics 9, 1431.

Zisko, N., Skjerve, K.N., Tari, A.R., Sandbakk, S.B., Wisløff, U., Nes, B.M., Nauman, J., 2017. Personal activity intelligence (pai), sedentary behavior and cardiovascular risk factor clustering–the hunt study. Prog. Cardiovasc. Dis. 60, 89–95.