Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study

Liam Dawson
School of Computer Science and Mathematics
Liverpool John Moores University,
3 Byrom St, Liverpool L3 3AF Liverpool, United Kingdom
Email: L.M.Dawson@2016.ljmu.ac.uk

Alex Akinbi (Corresponding Author)
School of Computer Science and Mathematics
Liverpool John Moores University,
3 Byrom St, Liverpool L3 3AF Liverpool, United Kingdom
Email: o.a.akinbi@ljmu.ac.uk
ORCID: https://orcid.org/0000-0001-6980-307X

Abstract

Wearable IoT devices like fitness trackers and smartwatches continue to create opportunities and challenges for forensic investigators in the acquisition and analysis of evidential artefacts in scenarios where such devices are a witness to a crime. However, current commercial and traditional forensic tools available to forensic investigators fall short of conducting device extraction and analysis of forensic artefacts from many IoT devices due to their heterogeneous nature. In this paper, we conduct a comprehensive forensic analysis and show artefacts of forensic value from the physical TomTom Spark 3 GPS fitness smartwatch, its companion app installed on an Android smartphone, and Bluetooth event logs located in the app's metadata. Our forensic methodology and analysis involved the combination and use of a non-forensic tool, a commercial forensic tool, and a non-forensic manufacturer-independent analysis platform tool specifically designed for endurance athletes to identify, extract, analyse, and reconstruct user activity data in an investigative scenario.

We show forensic metadata associated with the device information, past user activities, and audio files from the physical smartwatch. We recovered data associated with past user activities stored in proprietary activity files and databases maintained by the app on an Android smartphone. From the event logs, we show when user activity was synced with the app and uploaded to the device cloud storage. The results from our work provide vital references for forensic investigators to aid criminal investigations, highlight limitations of current forensic tools, and for developers of forensic tools an incentive into developing forensic software applications and tools that can decode all relevant data generated by wearable IoT devices.

Keywords: IoT forensics; mobile forensics; Android forensics, TomTom; TomTom Spark 3; fitness tracker

1. Introduction

Wearable Internet of Things (IoT) devices which are mostly fitness trackers and activity tracking smartwatches are gadgets that can be worn by individuals throughout the day to keep track of various body parameters. These devices continuously sense the movements of the body on a 3-axis accelerometer. The data is recorded all the time it is worn and powered up, which enables the tracker to trace if the individual is walking, running, climbing, or standing still [1]. They can also include sensors that track biometric data (heart rate, sleep time, fitness progression, etc.), elevation, temperature, and location using Global Positioning System (GPS) depending on the features and brand. Forecasts suggest that an estimated 368.2 million wearable devices will be shipped globally by the end of 2020. This figure is projected to grow to more than 500 million by 2024 [2]. Most smartwatches and fitness bands have similar functionalities, complement smartphones, and interact with several of the applications on them by providing notifications and alerts. In the smartwatch market, Apple held the largest share of the global shipment (55.5%) in the first quarter of 2020, followed by Samsung (13.9%), Garmin (13.9%), and other brands (22.6%) respectively [3].

This astronomical growth in demand and the potential of these devices to generate data that are stored on the devices and smartphones they are synced with has created significant interest amongst many digital forensic researchers and an increased shift towards wearable IoT device forensics [4–9]. Law enforcement agents, legal experts, and forensic investigators have also taken a significant interest in IoT devices as sources of forensic artefacts, especially in scenarios where an IoT device has been a witness to a crime [10]. Wearable devices have been used for evidence in court cases, either to convict a criminal or to provide an alibi to someone being accused of a crime. In 2017, forensic evidence from a Fitbit was crucial in the conviction of a man suspected of killing his wife in Connecticut, USA [11]. In the U.K, data retrieved from a Garmin smartwatch was used to convict a British runner for the murder of two gangsters [12].

However, with a variety of wearable devices introduced into the market and growing advancements in software and hardware components, forensic acquisition and analysis of these devices has become a huge challenge for forensic investigators. This is due to the quantity of data they generate, the vendor-specific protocols and file types used, and the security improvements on smartphones they are synced with. Even in cases where evidence has been identified, investigators still face challenges of evidence analysis and correlation [9,13,14]. Moreover, current forensic tools geared towards conventional computer file systems and mobile devices may not be suitable for wearable IoT forensics, cumulative dataset may exist in multiple locations and data acquired may not be accessible with existing forensic tools [9,15,16]. Recovery of deleted data is also a major challenge in scenarios where a suspect deletes data from the device, making it difficult for crucial evidential data to be recovered, for example, GPS locations and time stamps. Similarly, there are still challenges associated with recovering forensic artefacts from wearable devices that hold a duplicate source of evidence if the

paired smartphone is inaccessible or unavailable. The heterogeneous nature of IoT devices and lack of IoT forensics standards make adopting traditional digital forensic investigation models difficult to achieve in the IoT context [9,17].

Currently, commercial and traditional forensic tools can perform the acquisition and forensic analysis of a very small number of smartwatches, focusing on those high-end devices with a large market share ("Samsung", "LG", "Apple Watch" etc.) [16]. However, there are numerous low-cost smartwatch brands available on the market which store user information differently and require an alternative forensic analysis methodology. Therefore, there is the need to adopt a different approach which includes the use of non-forensic tools, when dealing with these smartwatches to overcome the limitations of traditional and commercial forensic tools. In this paper, we focus on the extraction and analysis of forensic artefacts of interest from the physical TomTom Spark 3 GPS fitness smartwatch and the TomTom Sports app installed and running on an Android smartphone synced with the smartwatch. The main contributions in this paper are summarised as follows.

- We interact with the internal memory of the physical TomTom Spark 3 GPS fitness smartwatch to identify and extract forensic artefacts of interest and metadata.
- We identify, reconstruct, and interpret forensic artefacts of interest from the main databases maintained by the TomTom Sports app installed on an Android device and synced with the smartwatch.
- We show how to deal with deleted data by analysing the databases, interpret event logs, and decode proprietary activity files stored on the Android file system to reconstruct chronology and sequence of past activities carried out by the user of the smartwatch.

The goal of this paper is to present the data acquisition and forensic analysis carried out on the TomTom Spark 3 GPS smartwatch to demonstrate the limitations of commercial and traditional forensic tools and also show the results obtained from the study of the forensic artefacts acquired and analysed using non-forensic tools. This paper is organised as follows. In Section 2, we discuss related works. In Section 3, we discuss our experiments, analysis methodology, investigative scenario, and tools used in this study. In Section 4, we discuss forensic analysis of the TomTom Spark 3 GPS smartwatch. Forensic analysis and findings of the TomTom Sports app including artefacts recovered are presented in Section 5. In Section 6, we present our findings from the Bluetooth event logs. Finally, in section 7 we conclude the paper.

2. Related works

Many recent works of literature have acknowledged the importance of wearable forensics and focused on the forensic analysis of wearable IoT devices. MacDermott et al. [18] studied Fitbit, Garmin, and HETP devices using FTK Imager and Autopsy to analyse the accuracy of potential evidential data

generated and stored on the internal memory of each fitness tracker. Baggili et al. analysed the Samsung Gear 2 and LG G watches synced to an Android smartphone and showed database and XML files maintained by apps running on the smartphone[19]. They also analysed the devices by rooting the operating system and recovered very few data remnants of forensic value. Data acquisition and forensic analysis were done on different non-android smartwatches equipped with a low-cost MTK chip running Nucleus RTOS by Gregorio et al. [16]. They used a non-forensic tool named FlashTool to acquire the data and search for forensic files of interests on the internal memory chip of each smartwatch. Kang et al. analysed apps synced with the Xiaomi Mi Band 2 and Fitbit Alta HR fitness trackers on Android devices and recovered SQLite databases that contain evidential data [20]. In the study, they highlighted evidence of deleted and modified data in the databases and discussed their application in a possible scenario. Odom et al. [21] conducted a preliminary forensic analysis of the Samsung Gear 3 smartwatch, Apple Watch Series 3 smartwatch, and their companion smartphones to identify locations where sensitive user data and forensic artefacts are stored. They identified significant forensic files of interest from the Samsung smartwatch compared with the Samsung Galaxy S8 smartphone and likewise extracted more files of interest from the iPhone 6 compared with the Apple smartwatch. However, there was no detailed correlation of how these forensic artifacts could be used in a forensic investigation or related scenarios.

Previous forensic analyses of TomTom devices have focused solely on their satellite navigation devices as demonstrated in studies by [22–24]. None of these papers, however, covers the forensic analysis of TomTom smartwatches and identified up to date forensic artefacts on all sources of evidential data (IoT device, mobile app, and event logs) to aid forensic investigations. The selection of the TomTom Spark 3 GPS fitness smartwatch is also based on the popularity of the TomTom brand as one of the largest portable GPS navigation solutions providers involved in the development of wearable IoT devices. Hence, forensic investigators are more than likely to come across TomTom smartwatches during digital forensic investigations.

3. Experiments, methodology, and tools

In this study, we adopted the IoT forensic model described by Li et al. [6] (see Fig. 1) in a scenario where the wearable IoT device is a witness to a crime (e.g., data stored in the IoT device can directly implicate an individual accused of a crime). In our investigative scenario described in this paper, we performed a set of controlled experiments that involves several activities, each one referring to a specific usage scenario (running, walking, gym activities, etc.) during which a typical record of user activities have taken place. These activities enabled us to generate data to forensically examine the IoT device (examine TomTom Spark 3 GPS fitness smartwatch in a scenario where the smartphone paired to the smartwatch is not accessible or available), examine the companion app (examine smartphone paired to the smartwatch is available and the TomTom Sports app is installed) and finally,

companion network examination (examine event logs where the smartphone paired to the smartwatch is available and the TomTom Sports app is installed). Details of the investigative scenario are described as follows.

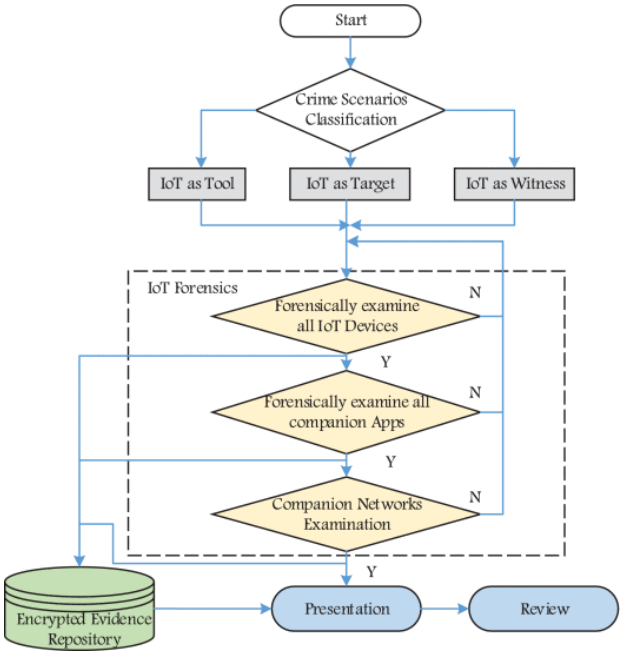

Fig 1. IoT forensic model [6]

3.1. Investigative scenario

A suspect of theft has been accused of stealing from a local shop in Hale. Eyewitness statements claim the suspect was in the area on the 19th of January 2020 at around 2:00 p.m. UTC. The suspect provides an alibi stating he was at home sleeping and was not in the vicinity on the day. The suspect's Android smartphone and TomTom Spark 3 GPS fitness smartwatch has been seized and investigators are keen to answer the following set of questions based on our forensic analysis:

1. Does the TomTom smartwatch store data on its internal memory chips? If so, can it be recovered and analysed?
2. Can user activity data be recovered from the TomTom Sports app installed on the Android smartphone? If so, can the data be reconstructed to show past user activities?
3. Can deleted user activity data be recovered from the TomTom Sports app installed on the Android smartphone?

3.2. Forensic analysis methodology and tools

In this study, we performed two phases of experiments before and after synchronizing the TomTom Spark 3 GPS fitness smartwatch with the Google Pixel 2 XL smartphone running Android 10. The TomTom Spark 3 smartwatch uses separate embedded memory chips which include an Atmel smart

RISC MCU with eFlash memory (128KB capacity non-accessible to the user) to store the device firmware [25], a Micron Serial Flash Memory (EEPROM 4MB capacity non-accessible to the user) to store user activity data and device information, and an internal media NAND storage (3GB capacity accessible to the user) to store music files. In the first phase of our experiment, we restored the TomTom smartwatch to factory default settings and generated new user data without pairing or synchronizing the device with the Android smartphone. There are no specific forensic tools to conduct the acquisition of the information stored inside of TomTom smartwatches. Therefore, we used a non-forensic open-source Linux command-line tool named *ttwatch* developed by Ryan Binns [26] to communicate with the TomTom Spark 3 GPS fitness smartwatch's internal Micron Serial Flash Memory (EEPROM 4MB storage capacity) and extracted device information and proprietary activity files *(.ttbin)* which store information associated with past user activities.

In the second phase after pairing and synchronization, we used *Cellebrite UFED 4PC v. 7.28* [27] commercial forensic software to extract the internal storage memory chips of the TomTom Spark 3 GPS fitness smartwatch and Google Pixel 2 XL smartphone running Android 10 in a forensically sound manner. We selected and used the TomTom generic profile (developed for TomTom Satnavs) to extract a physical bit-for-bit image *(.bin)* file of the device memory including unallocated space. *Cellebrite UFED 4PC v. 7.28* was only able to access and dump the internal storage media (3GB capacity for storing music files) normally accessible to the user.

To verify the acquisition of the smartwatch's internal memory for both phases of our experiments, we repeated the acquisition using *Access Data FTK Imager* [28] *v. 4.2.0.13*. Access Data FTK Imager, like Cellebrite, was only able to access the internal storage media (3GB capacity for storing music files) normally accessible to the user.

The data generated by the TomTom Spark 3 GPS fitness smartwatch and synced with its companion app are stored in databases and file locations on the Android smartphone which are inaccessible to the user. Therefore, a file system extraction of the smartphone was performed which allowed a logical extraction of the internal memory of the smartphone, in addition to hidden system files, databases, and other files that are not normally visible within a logical extraction. Once both extractions were completed, we used *Cellebrite Physical Analyzer v. 7.25* [27] to analyse the images. DB Browser for SQLite v. 3.11.2 (an open-source tool) [29] was used to analyse the database files and *Runanlyze* web application [30] was used to decode and analyse the proprietary TomTom activity *(.ttbin)* files recovered from the external SD card storage location of the Android smartphone. A summary of the tools and their usage is shown in Table 1.

Table 1: Summary of tools and usage

Tools	Usage
Cellebrite UFED 4PC v. 7.28	▪ A commercial forensic tool used to create a physical image of the internal media NAND storage (3GB capacity accessible to the user) ▪ Used to create a logical image of the Android smartphone.
ttwatch (Linux TomTom GPS Watch Utilities)	▪ Open-source, non-forensic Linux command-line tool used to interact with the physical TomTom GPS smartwatch and extract forensic artefacts stored on the Micron Serial Flash Memory (EEPROM 4MB storage capacity inaccessible to the user).
Cellebrite Physical Analyzer v. 7.25	▪ A commercial forensic tool used to analyse images created with Cellebrite UFED 4 PC.
DB Browser for SQLite v. 3.11.2	▪ Open-source tool used to analyse database files maintained by the TomTom Sports app.
Runanlyze web application	▪ A non-forensic tool used to analyse proprietary TTBIN files recovered from the TomTom smartwatch and TomTom Sports app.
Access Data FTK Imager v. 4.2.0.13	▪ A traditional forensic tool used to extract forensic artefacts from the physical TomTom Spark 3 GPS fitness smartwatch's internal Micron Serial Flash Memory (EEPROM 4MB storage capacity inaccessible to the user)

4. Forensic analysis of TomTom Spark 3 smartwatch

The TomTom Spark 3 GPS fitness smartwatch is an activity monitoring (steps, sleep, calories, active time, distance, heart rate, etc.) and GPS tracking device. Features include internal storage up to 3GB to store music files, supports incoming calls and text notifications, wireless synchronization to the TomTom Sports app installed and running on a smartphone via Bluetooth to monitor activity data. Manual navigation of the smartwatch shows a record of the last 10 user activities for each type of activity (swimming, running, freestyle, gym, etc.) on the device. The oldest activity in the list is deleted when the user completes a new activity. However, a user cannot delete an activity in the history list manually. In this section, we present the forensic analysis of the internal memory chips of the TomTom Spark 3 GPS fitness smartwatch to recover relevant data remnants, files, and forensic artefacts stored on the physical device.

4.1. Acquisition of artefacts from the physical TomTom Spark 3 smartwatch

During its use, the TomTom Spark 3 GPS smartwatch processes and store data remnants and files on the physical smartwatch. As mentioned previously, the TomTom smartwatch uses separate embedded memory chips which include an Atmel smart RISC MCU with eFlash memory (128KB capacity non-accessible to the user) to store the device firmware[25], a Micron Serial Flash Memory (EEPROM 4MB capacity non-accessible to the user) to store user activity data and device information, and an

internal media NAND storage (3GB capacity accessible to the user) to store music files. In this study, we used the *ttwatch* Linux command-line tool [26], to communicate with the device by plugging the device USB cable into our Linux forensic workstation and running the tool. We issued commands *(ttwatch -v = 'shows watch version' and ttwatch --list= 'lists user activity history')* to extract device information and list past user activities including dates and type of activity (freestyle) as shown in Fig. 2.

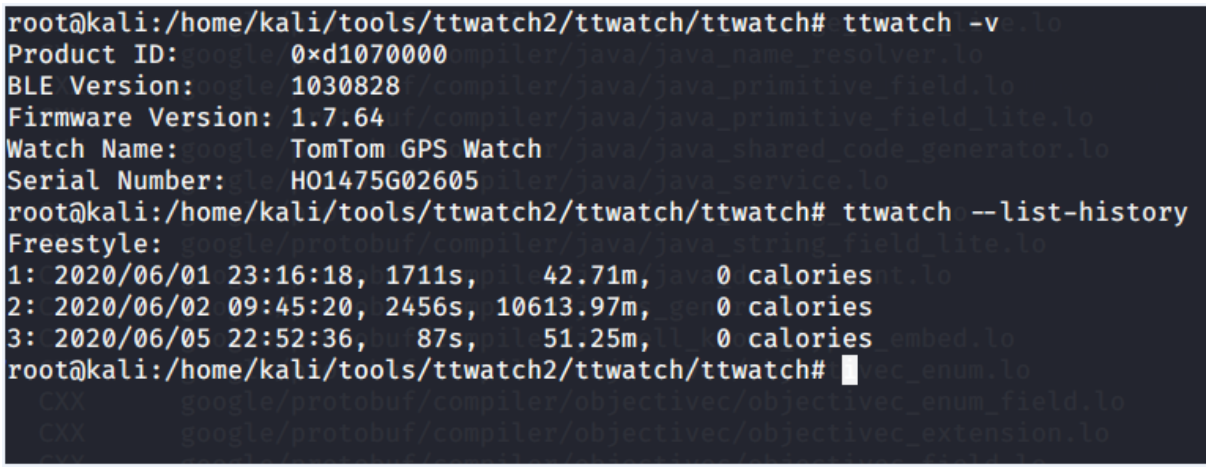

Fig. 2. Device information and user activity history via command line

Using the "*ttwatch --get-activities"* command, we extracted proprietary activity files (*.ttbin)* which store past user activities that are yet to be synchronized with the smartphone (see Fig. 3). In this figure, we see two files named "*Unknown_22-29-25_5491.ttbin"* and *"Unknown_21-55-1_5004.ttbin"*. Once the data is synced with the smartphone, the smartwatch deletes the activity files but keeps a record of the last 10 activities as discussed previously. In Section 5.4, we show how these proprietary '.ttbin' activity files can be decoded and analysed to reconstruct past user activities using a non-forensic web application tool.

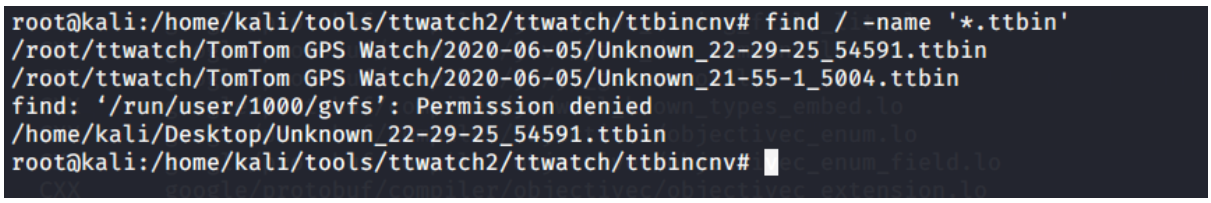

Fig. 3. Proprietary .ttbin files

4.2. Storage locations and format of data remnants on TomTom Spark 3 smartwatch

The TomTom GPS fitness smartwatch allows users to store music files in mp3 format on its internal memory chip (3GB capacity accessible to the user), by plugging the device into a desktop computer. From the analysis of the forensic image, the two most important locations on the internal memory file system are "*TOMTOM/MySportsConnect/"* and *"TOMTOM/System Volume Information/"* directories that store music audio files and information related to data entries respectively (see Fig. 4). The

TOMTOM/MySportsConnect/ directory has a subdirectory named "*Music"* where all mp3 audio files stored by the user on the device are located and can be recovered from. Each mp3 file found also includes embedded images (album covers) associated with each file.

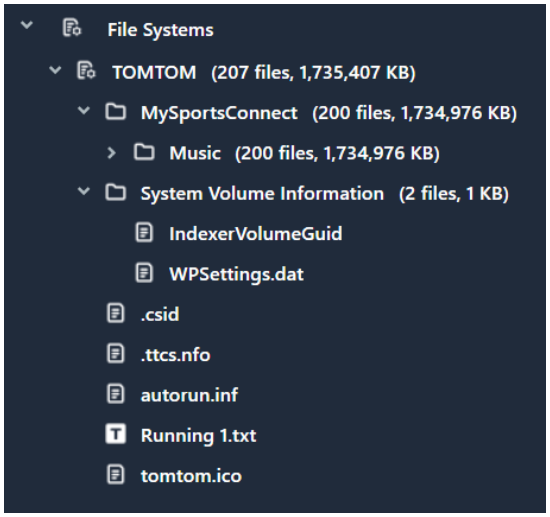

Fig. 4. File system structure of the TomTom Spark 3 smartwatch

The *TOMTOM/System Volume Information/* directory contains 2 files named *IndexerVolumeGuid and WPSettings.dat.* This directory and files are automatically created by the Windows operating system once the smartwatch is connected via a USB cable. *IndexerVolumeGuid* is a file used by the Windows Search service and contains the GUID (Globally Unique Identifier) for the smart device once plugged in. The *WPSettings.dat* is used by the Windows operating system to allow drives connected to the device to search for data entries faster. *The .csid, .ttcs.nfo, autorun.info, and tomtom.ico* files are used by the smartwatch for initial setup, syncing media files, and to restore the smartwatch to factory default settings using the *TomTom Sports Connect* desktop application. *Running 1.txt* is a text file that contains the list of all mp3 media files and the date each file was added to the smartwatch.

5. Forensic analysis of TomTom Sports app

The TomTom Sports app is a mobile application that converts all tracked activity and GPS data from the TomTom Spark 3 smartwatch and presents the analysed data to the user on a GUI on the smartphone. In our scenario, we downloaded, installed, and configured the *TomTom Sports app v. 10.0.16* (current version at the time of writing) on the Google Pixel 2 XL smartphone running Android 10. The app was then populated with user information and used to pair the smartwatch to the smartphone using a Bluetooth connection. Once the smartwatch had been paired, the activity and GPS data from the smartwatch are synced and stored on the app. The user can hold and drag down the app's GUI, which will refresh and synchronize recent activity data from the smartwatch to the smartphone.

5.1. Location and format of TomTom Sports app artefacts

During synchronization of activity data from the smartwatch to the smartphone, the TomTom Sports app stores several artefacts of forensic interest into various files and databases located in the "*/data/data/com.tomtom.Sports" and "/storage/emulated/0/TomTom_MySports"* directories of the Android file system, that contains several subfolders as described in Table 2.

Table 2. File paths of critical evidence sources of the TomTom Sports app

Directory Path	Details
/data/data/com.tomtom.Sports	• Contains information associated with the user account and activity data stored in the main databases. • Contains information associated with Bluetooth synchronization and event logs.
/storage/emulated/0/TomTom_MySports	• Contains several user activity data stored in *.ttbin* file format. • Contains information associated with Bluetooth synchronization and event logs.

5.2. Reconstructing user information and activities

To answer the question of whether activity data can be recovered from the TomTom Sports app from our investigative scenario, we identified two SQLite databases named *RKStorage* and *sport.db* located in the */data/data/com.tomtom.Sports/db* subdirectory. The *RKStorage* database store information associated with the user account configured during installation and setup of the app. The database has two tables but only one of the tables named *catalystLocalStorage* contains information of forensic interest. The user profile ID (email address) is stored in the "*com.tomtom.sportsapp.user.profile.id"* field, user profile information (age, country code, and date of birth) is stored in the "*com.tomtom.sportsapp.user.profileinfo"* field, the smartwatch's unique MAC address is stored in the *"com.tomtom.sportsapp.device.colors*" field and the last time and date (Unix timestamp) when user account information was last updated is stored in the *"com.tomtom.sportsapp.db.lastCompress"* field. The *sport.db* is the main database that stores and maintains information associated with all user activity and GPS tracking data and has 7 tables. From our findings, only 3 out of these 7 tables contain information of forensic interest namely tables *activities, activityDetails,* and *weight_measurements.* We discuss the contents of these tables in relation to our investigative scenario questions.

The *activities* table contains a record of all activity data (activity type, GPS coordinates, time and date of activity, step count, average heart rate, and activity duration) stored in JSON format in the "*blob"* field. Each activity is assigned a unique identifier stored in the *key* field. The start time and date, activity type, and web API endpoint (where the data is stored in the TomTom Sports cloud) are stored

in the "*start_datetine_user"*, "*activity_type_id_tt"* and "*link.self"* fields respectively (see Fig. 5). Details of parameters used to store data in the *blob* field and the interpretation is presented in Table 3.

Table: activities

	key	blob	activity_type_id_tt	start_datetime_user	link.self
	Filter	Filter	Filter	Filter	Filter
1	406775970	{"id":406775970,"activity_typ...	9	2020-01-10T11:06:41+00:00	/service/webapi/v2/activity/406775970?dv...
2	406775969	{"id":406775969,"activity_typ...	9	2020-01-06T07:45:41+00:00	/service/webapi/v2/activity/406775969?dv...
3	407343737	{"id":407343737,"activity_typ...	9	2020-01-13T07:49:23+00:00	/service/webapi/v2/activity/407343737?dv...
4	406775967	{"id":406775967,"activity_typ...	100	2020-01-06T00:00:00+00:00	/service/webapi/v2/activity/406775967?dv...
5	407748178	{"id":407748178,"activity_typ...	8	2020-01-15T11:52:24+00:00	/service/webapi/v2/activity/407748178?dv...
6	408002770	{"id":408002770,"activity_typ...	0	2020-01-16T20:24:20+00:00	/service/webapi/v2/activity/408002770?dv...
7	408161171	{"id":408161171,"activity_typ...	8	2020-01-17T19:23:29+00:00	/service/webapi/v2/activity/408161171?dv...
8	407343736	{"id":407343736,"activity_typ...	100	2020-01-13T00:00:00+00:00	/service/webapi/v2/activity/407343736?dv...
9	408505926	{"id":408505926,"activity_typ...	8	2020-01-19T14:14:01+00:00	/service/webapi/v2/activity/408505926?dv...

Fig. 5. *activities* table

Table 3. parameters in the *blob* field of the activity table (some parameters have been omitted because of their lack of forensic value)

Parameter	**Meaning**
id	unique identifier of the specific activity.
start_datetime; start_datetime_user	date and time (UTC) of activity
activity_type_id	specifies type of activity (gym =12, run=16, walk=21)
Active Daily time (7 days) Format(day1,day2,day3,day4,day5,day6,day7)	active time of the activities selected throughout the week (recorded in seconds. 6069 seconds = 101.15 minutes)
Daily Step count (7 days) Format(day1,day2,day3,day4,day5,day6,day7)	step count daily throughout the week. Day 1 is Monday; Day 2 is Tuesday and so on. (the starting day is determined when the app is first used, the app's starting day is Monday.
heartrate_avg (HR) Daily/ HR Zones Daily Minimum HR Daily/Maximum HR Daily Resting HR Weekly/Daily Format(day1,day2,day3,day4,day5,day6,day7)	heart rate values for an activity and each day of the week and the average heart rates throughout the week measures in BPM.
activity_score_daily Format(day1,day2,day3,day4,day5,day6,day7)	achievement score for daily activity milestones
elapsed_time_total; moving_time_total	duration of an activity measured in seconds
bounding_box	GPS coordinates of activity start/end locations
active_time_total	total time measured in seconds for when the user is active
metabolic_energy_total	calories burnt per activity
sleep_asleep_daily	daily sleep tracking data measured in seconds
formats	supported file formats user activity can be stored as.
hrz_dist	the horizontal distance covered by user daily
climb_total	number of steps on elevated ground
speed_avg	the average speed of user during an activity

From Fig. 5, we identified the 9th record from this table which relates to our investigative scenario and exported the JSON data from the *blob* field as shown in Table 4.

Table 4. User activity data (9th record) stored in *blob* field of the *activities* table

{"id":408505926,"activity_type_id":21,"start_datetime":"2020-01-19T14:14:01+00:00","start_datetime_user":"2020-01-19T14:14:01+00:00","activity_type_id_tt":8,"display_offset_seconds":0,"links":{"image":"/service/webapi/v2/activity/408505926/thumbnail.png?dv=3.3","webview":"/app/activity/408505926?dv=1.3","raceme":"/service/webapi/v2/training/race/408505926","convert_to_trail":"/service/webapi/v2/training/trail/from/408505926?dv=1.3","self":"/service/webapi/v2/activity/408505926?dv=1.3","share":"/service/webapi/v2/activity/408505926/permalink/{PARTNER}?dv=1.3"},"formats":["fit","pwx","csv","tcx","kml","gpx"],"zones":[97,116,135,155,174,194],"bounding_box":{"north_east":{"lat":53.334754,"lng":-2.79236},"south_west":{"lat":53.322295,"lng":-2.798301}},"aggregates":{"active_time_total":2524,"distance_total":2309.3,"elapsed_time_total":2525,"metabolic_energy_total":1009018.8,"speed_avg":0.91,"climb_total":20,"descent_total":21.1,"heartrate_avg":98.39,"hrz_dist":[1649,41,0,0,0],"hrz_none":834,"moving_time_total":2525,"moving_speed_avg":0.91,"activity_score":23}}

From Table 4, we see the unique identifier for this activity *("id":408505926)*, activity type shows the user is walking *("activity_type_id" : 21)*, the date and time for this activity was recorded as 19th of January 2020 at 2:14 pm UTC *("start_datetime": 2020-01-19T14:14:01+00:00)*, total elapsed time of the activity was 2525 seconds *("elapsed_time_total":2525)*, distance covered by the user is 2309.3 metres *("distance_total": 2309.3)* and GPS location is latitude 53.334754, longitude -2.79236 and latitude 53.322295, longitude -2.798301 *(bounding_box":{"north_east":{"lat":53.334754,"lng":-2.79236},"south_west":{"lat":53.322295,"lng":-2.798301})*. Other information shown are the users average speed while walking in km/hr *("speed_avg":0.91)* and average heart rate in BPM *("heartrate_avg":98.39)*.

The GPS coordinates were displayed on the map to visually confirm the user's route which placed the suspect at the location described in the scenario as shown in Fig. 6. The *weight_measurements* table stores information associated with the user's weight and time this record was last updated. This record is stored in the *blob* field of this table and assigned a unique identifier (date and time last updated) in the *key* field.

Fig. 6. GPS coordinates shown on Google Earth

5.3. Dealing with deleted user activity data

To answer the question of whether deleted activity data can be recovered from our investigative scenario, activity data associated with the 19th of January 2020 *("id": 408505926)* was deleted from the TomTom Sports app on the 26th of February 2020. We then acquired an extraction of the Android smartphone and analysed the *sport.db* database. Consequently, the record was not present in the *activities* table of the *sport.db* database. It is well known that remnants of deleted data from SQLite databases are kept in unallocated cells in the file corresponding to the database, from which they can be recovered [31,32]. However, our attempts to recover deleted data from the database using *Undark v 0.6* [33] and *Cellebrite Physical Analyzer* SQLite recovery tools were unsuccessful as the cells containing deleted data had been overwritten with null bytes upon deletion. We identified records of all past user activities including deleted ones stored in the *activityDetails* table (see Fig. 7). From the figure, we see the 14th and 15th records *("id": 408505926)* which contains activity data in the *blob* field and can be exported in JSON format. Each record in the table is assigned a unique identifier stored in the *key* table and shows the web API endpoint (*/service/webapi/v2/activity/408505926?dv=1.7*) used to upload the activity data to the TomTom Sports cloud. The timestamp indicating when the data was last updated is stored in the *accessCounter* field which is the 25th of February 2020 at 8:00:54 pm UTC *(Unix timestamp = '1582660854925').* The exported data stored in JSON format contains information associated with the user's GPS locations and speed per step count, tracking each step taken by the suspect on the 19th of January.

These coordinates can be plotted on a map to provide investigators with details of the route taken by the suspect.

	key	blob	accessCounter
11	/service/webapi/v2/activity/407343736?dv=1.48	{"id":407343736,...	1579263388212
12	/service/webapi/v2/activity/408161171?dv=1.3	{"id":408161171,...	1579441686707
13	/service/webapi/v2/activity/408161171?dv=1.5	{"id":408161171,...	1582725705144
14	/service/webapi/v2/activity/408505926?dv=1.3	{"id":408505926,...	1582660847707
15	/service/webapi/v2/activity/408505926?dv=1.7	{"id":408505926,...	1582660854925

Fig. 7. *activityDetails* table

5.4. Reconstructing user activity from proprietary .ttbin activity files

A chronology of events can also be reconstructed from the *.ttbin* files stored on the physical TomTom Spark 3 GPS fitness smartwatch as shown earlier in section 4.1 (before synchronization with the smartphone) and on its companion, mobile app installed on the Android smartphone (after synchronization with the smartphone). These proprietary activity workout (*.ttbin*) files are stored on the external memory (SD Card) of the Android device in the */storage/emulated/0/TomTom_MySports/<Watch Serial Number>/workouts/uploaded/* and the */storage/emulated/0/TomTom_MySports/<Watch Serial Number>/step_buckets/uploaded/* subdirectories. The files are named according to the date and time an activity was synced from the smartwatch to the app on the smartphone. From our investigative scenario, we identified the file "*00910000_20200119_161610.ttbin"* (19th January 2020 at 4:16:10 pm UTC), which was the only activity data consistent with the date from the scenario. We were able to analyse and reconstruct the suspect's activities on this day by uploading the file to the *Runalyze* web application, a manufacturer-independent analysis platform tool designed for endurance athletes [30].

In Fig. 8, detailed graphical analysis and statistics of the suspect's activity are shown. From the figure, we see details consistent with the *sport.db* database analysis which includes the total elapsed time *("42 mins 05 secs = 2525 seconds"),* distance *("2.31 km = 2309.3 meters"),* and heart rate *(99 bpm ~ 98.39 bpm). Runalyze* can plot the GPS coordinates from the *.ttbin* file on a map as shown in Fig. 9 which can also be downloaded as a KML (Keyhole Markup Language) file for expressing geographic annotation and visualization in maps such as Google Earth. Miscellaneous results from *Runalyze* also showed the date and time (19th January 2020 at 2:14 pm), weather conditions, wind speed, and temperature. It is worth noting that *.ttbin* files are not deleted from the smartphone when the user deletes past activity data from the app.

Fig. 8. User activity data in *Runalyze* web application *(source: runalyze.com)*

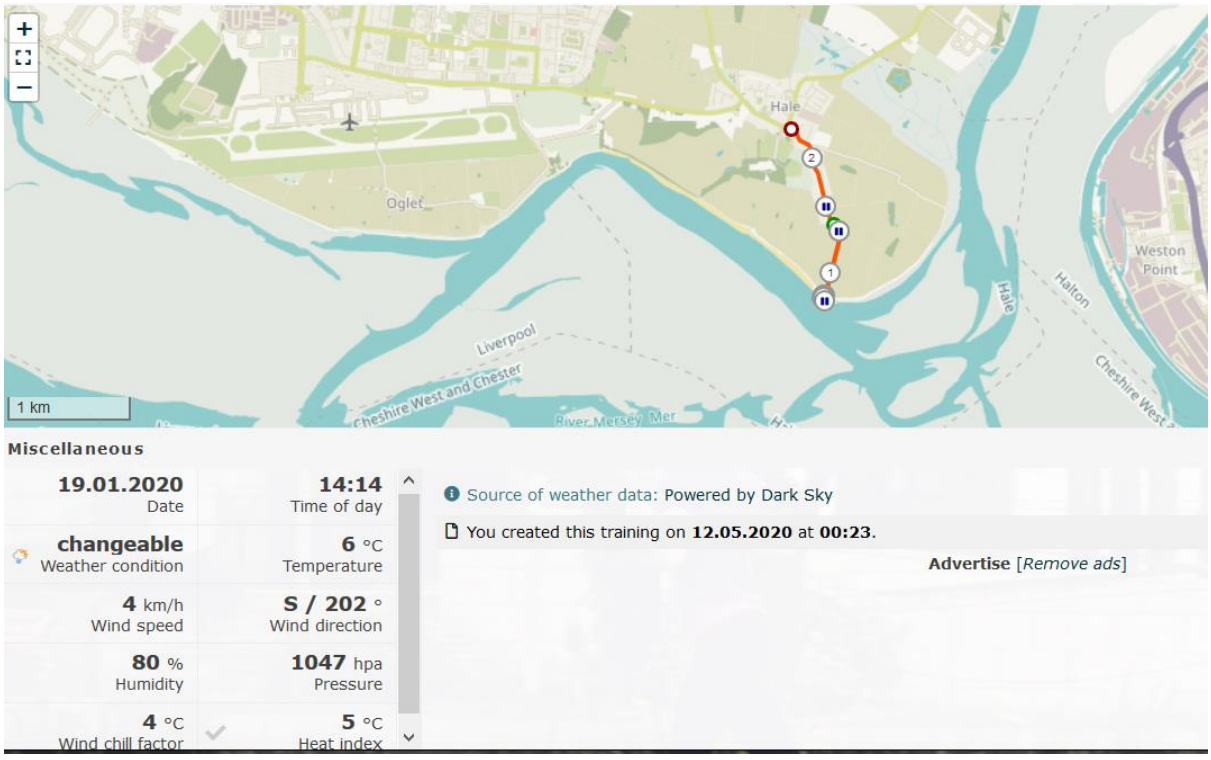

Fig. 9. User GPS tracking location in *Runanlyze* web application *(source: runalyze.com)*

6. Examining Bluetooth event logs

During each synchronization of recent activities between the smartwatch and the TomTom Sports app on the smartphone using Bluetooth, event logs are generated and stored as text files in the */data/data/com.tomtom.Sports/f/* (internal memory) *and /storage/emulated/0/TomTom_MySports /FullLogFile.txt* (SD card) directories of the Android file system. We identified two such files named "*Logfile_0.txt" and "FullLogFile.txt"* that both contain identical records and chronology of all past synchronization events that occurred in the application. The log files show the timestamp of the initial pairing of the smartwatch with the smartphone, a timestamp indicating when each activity file *(.ttbin)* was created and written to disk, timestamp, and web API endpoint used to upload each *.ttbin* file to the TomTom Sports cloud. For instance, the logs show the smartwatch was first paired with the smartphone on the 10th of January 2020 at 12:30:18 p.m UTC using Bluetooth. Event logs associated with our investigative scenario is shown in Fig. 10. From the figure, we see the *.ttbin* file (*00910000_20200119_161610.ttbin)* and activity id *(408505926)*associated with the suspect's activity successfully uploaded to the TomTom cloud on the 19th of January at 4:18 p.m UTC. This information could be utilized by an investigator to obtain data stored on TomTom's cloud systems.

Fig. 10. Bluetooth event logs

7. Conclusion

In this paper, we conducted IoT device forensics, mobile device forensics, and event log analysis for the TomTom Spark 3 GPS fitness watch. We explored storage locations, identified and extracted forensic artefacts of interest stored on the physical smartwatch using ***ttwatch***, a non-forensic Linux command-line tool. We also identified and reconstructed evidential data associated with user information, past activities, and GPS locations generated by the smartwatch and stored on databases maintained by the TomTom Sports mobile app installed on an Android smartphone using ***Cellebrite*** commercial forensic tools. We identified proprietary activity *(.ttbin)* files that contain evidential data associated with user activities stored on the Android file system and physical smartwatch. Using the ***Runalyze*** web platform non-forensic tool designed for analysing athletes' performance, we were able

to decode the activity files and reconstruct past user activities including GPS locations from our investigative scenario. Several other athlete performance web applications *(Strava, Endomondo, MapMyFitness, RunKeeper, and TrainingPeaks)* support and can analyse activity files with *.gpx*, *.tcx*, and *.fit* extensions used by other brands of fitness trackers. However, in our study, only *Runalyze* supports the analysis of TomTom's *.ttbin* files.

We studied the event logs of the TomTom Sports app extensively and drew significant results of activity data uploaded to the TomTom cloud which could help facilitate cloud forensic investigations. The methodology we followed in this study is demonstrated by using TomTom Spark 3 as a case study where the device is a witness to a crime. It is important to note that this methodology is not specific for the TomTom Spark 3 GPS fitness smartwatch only but can be extended to other fitness trackers and smartwatches provided a variety of tools are sourced to analyse forensic files of interest. Also, this study highlights the current limitations of a commercial forensic tool (Cellebrite) and traditional tool (FTK Imager) in its inability to access all storage locations, recover and decode forensic artefacts from the TomTom Spark 3 GPS fitness smartwatch, and had to be compensated with the use of non-forensic tools. The acquisition and forensic analysis of this type of device can be critical, when, for example, the smartphone is missing or damaged and the information can be only extracted from its linked smartwatch. This study helps forensic investigators interpret artefacts from smartwatches and fitness trackers and provides a vital reference for developers of forensic tools in developing software applications that can decode all relevant data generated by wearable IoT devices.

Acknowledgments

This work was supported by the School of Computer Science and Mathematics, Liverpool John Moores University, U.K.

Conflict of Interest

All authors have no conflict of interest to report.

References

[1] L. Cashmere, How do wearable fitness trackers measure steps?, News-Medical.Net. (2020). https://www.news-medical.net/health/How-do-wearable-fitness-trackers-measure-steps.aspx (accessed May 12, 2020).

[2] Statista, Wearable technology - Statistics & Facts | Statista, Wearable Technol. - Stat. Facts | Stat. (2019). https://www.statista.com/topics/1556/wearable-technology/ (accessed February 26, 2021).

[3] businesswire.com, Strategy Analytics: Global Smartwatch Shipments Grow 20 Percent to 14 Million in Q1 2020, Businesswire.Com. (2020). https://www.businesswire.com/news/home/20200506006138/en/Strategy-Analytics-Global-Smartwatch-Shipments-Grow-20 (accessed May 12, 2020).

[4] E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, Internet of Things Forensics: Challenges and Approaches, in: Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (ICST), 2013. doi:10.4108/icst.collaboratecom.2013.254159.

[5] A. Goudbeek, K.-K.R. Choo, N.-A. Le-Khac, A Forensic Investigation Framework for Smart Home Environment, in: 2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng., IEEE, 2018: pp. 1446–1451. doi:10.1109/TrustCom/BigDataSE.2018.00201.

[6] S. Li, S. Li, K.-K.R. Choo, Q. Sun, W.J. Buchanan, J. Cao, IoT Forensics: Amazon Echo as a Use Case, IEEE Internet Things J. (2019) 1–1. doi:10.1109/JIOT.2019.2906946.

[7] S. Parikh, D. Chavda, S. Chakraborty, D.P.H. Rughani, D.M.S. Dahiya, Analysis of Android Smart Watch Artifacts, Int. J. Sci. Eng. Res. (2015). doi:10.14299/ijser.2015.08.011.

[8] Q. Do, B. Martini, K.K.R. Choo, Is the data on your wearable device secure? An Android Wear smartwatch case study, in: Softw. - Pract. Exp., 2017. doi:10.1002/spe.2414.

[9] H.F. Atlam, E. El-Din Hemdan, A. Alenezi, M.O. Alassafi, G.B. Wills, Internet of Things Forensics: A Review, Internet of Things. (2020) 100220. doi:10.1016/j.iot.2020.100220.

[10] U. Salama, Investigating IoT Crime in the Age of Connected Devices, (2017). https://securityintelligence.com/investigating-iot-crime-in-the-age-of-connected-devices/ (accessed July 11, 2019).

[11] C. Hauser, In Connecticut Murder Case, a Fitbit Is a Silent Witness, New York Times. (2017). https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html (accessed May 4, 2020).

[12] Makena Kelly, Garmin data used to convict British runner for the murder of two gangsters, Verge.Com. (2019). https://www.theverge.com/2019/1/18/18188205/garmin-data-iceman-murder-mr-big-amazon-alexa (accessed February 26, 2021).

[13] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things security and forensics: Challenges and opportunities, Futur. Gener. Comput. Syst. 78 (2018) 544–546. doi:10.1016/j.future.2017.07.060.

[14] T. Zia, P. Liu, W. Han, Application-specific digital forensics investigative model in internet of things (IoT), in: ACM Int. Conf. Proceeding Ser., 2017. doi:10.1145/3098954.3104052.

[15] S. Watson, A. Dehghantanha, Digital forensics: the missing piece of the Internet of Things promise, Comput. Fraud Secur. (2016). doi:10.1016/S1361-3723(15)30045-2.

[16] J. Gregorio, B. Alarcos, A. Gardel, Forensic analysis of Nucleus RTOS on MTK smartwatches, Digit. Investig. (2019). doi:10.1016/j.diin.2019.03.007.

[17] A. Alenezi, N.H.N. Zulkipli, H.F. Atlam, R.J. Walters, G.B. Wills, The impact of cloud forensic readiness on security, in: CLOSER 2017 - Proc. 7th Int. Conf. Cloud Comput. Serv. Sci., 2017. doi:10.5220/0006332705390545.

[18] A. MacDermott, S. Lea, F. Iqbal, I. Idowu, B. Shah, Forensic Analysis of Wearable Devices: Fitbit, Garmin and HETP Watches, in: 2019 10th IFIP Int. Conf. New Technol. Mobil. Secur., IEEE, 2019: pp. 1–6. doi:10.1109/NTMS.2019.8763834.

[19] I. Baggili, J. Oduro, K. Anthony, F. Breitinger, G. McGee, Watch what you wear: Preliminary forensic analysis of smart watches, in: Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015, IEEE, 2015: pp. 303–311. doi:10.1109/ARES.2015.39.

[20] S. Kang, S. Kim, J. Kim, Forensic analysis for IoT fitness trackers and its application, Peer-to-Peer Netw. Appl. (2018). doi:10.1007/s12083-018-0708-3.

[21] N.R. Odom, J.M. Lindmar, J. Hirt, J. Brunty, Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices, J. Forensic Sci. (2019) 1556-4029.14109. doi:10.1111/1556-4029.14109.

[22] J. Elstner, M. Roeloffs, Forensic analysis of newer TomTom devices, Digit. Investig. (2016). doi:10.1016/j.diin.2016.01.016.

[23] B. Nutter, Pinpointing TomTom location records: A forensic analysis, Digit. Investig. (2008). doi:10.1016/j.diin.2008.06.003.

[24] O. van Eijk, M. Roeloffs, Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems, Digit. Investig. (2010). doi:10.1016/j.diin.2010.02.005.

[25] B. Prince, D. Prince, Memories for the Intelligent Internet of Things, Wiley, Hoboken, 2018. doi:10.1002/9781119298922.

[26] R. Binns, Rundat, ttwatch, (2016). https://github.com/rundat/ttwatch.

[27] Cellebrite, Cellebrite UFED 4PC and Physical Analyzer, (2020). https://www.cellebrite.com/en/home/.

[28] AccessData, FTK Imager, AccessData. (2016). https://accessdata.com/ (accessed February 26, 2021).

[29] Sqlitebrowser, DB Browser for SQLite, Sqlitebrowser.Org. (2016). https://sqlitebrowser.org/ (accessed February 26, 2021).

[30] Runalyze, Runalyze, Runalyze.Com. (2020). https://runalyze.com/ (accessed May 14, 2020).

[31] S. Jeon, J. Bang, K. Byun, S. Lee, A recovery method of deleted record for SQLite database, Pers. Ubiquitous Comput. 16 (2012) 707–715. doi:10.1007/s00779-011-0428-7.

[32] C. Anglano, M. Canonico, M. Guazzone, Forensic analysis of the ChatSecure instant messaging application on android smartphones, Digit. Investig. 19 (2016) 44–59. doi:10.1016/j.diin.2016.10.001.

[33] P. Daniels, Undark - a SQLite deleted and corrupted data recovery tool, (2015). https://github.com/inflex/undark.