# A Digital Evidence Taxonomy of M-Health Apps in IoT Environment

**Muhammad Thariq Abdul Razak, Nurul Hidayah Ab Rahman, Nurul Azma Abdullah**

***Abstract:*** ***The adoption of IoT in enabling mobile health (m-health) apps created threats platform to the black hat hackers to compromise sensitive information (e.g. User personal detail, medicine data and outdoor activities) available from the apps. The heterogeneous nature of IoT infrastructure, however, would complicate activities of digital forensics. Therefore, we proposed a model of digital evidence taxonomy of m-health apps in IoT environment. The model includes evidence acquisitions and analysis at three layers of IoT such as mobile, application, and network layer. 34 top rating Android m-health apps were applied in a controlled experiment to examine the usability of the proposed model. Our results present fully, partially and none recovered evidence artifacts from the three layers as well as the analysis of forensic interest. This suggests that applying the model would facilitate forensic investigation activities and enable a forensically ready environment.***

***Index Terms: Digital Forensics; Forensic by Design: Forensic Readiness; Forensic Taxonomy; Internet of Things (IoT); IoT Forensics.***

## I. INTRODUCTION

Internet of Things (IoT) is one of the emerging technologies that enable the "things" (i.e. physical electronic devices) to be connected to the internet and capable to collect IoT related data from the physical environment [1]. The collected data will be transmitted to the specific application via wired and wireless internet connection (e.g. 3G, Wi-Fi, and 4G). Smart phone is an example of the physical devices that provide mobile applications (apps) and becoming the center of the IoT with related services such as social media, healthcare and surfing internet apps [2].

Mobile health (m-health) is an example of current technology that enables IoT environment by using a smartphone as a platform to record and analyze real time data of human biological changes [3]. It is about 325,000 m-health apps are available in the digital market with the highest number, about 160 000 are in Google Play Store while iOS Apps Store comprises around 140,000 apps [4].

The increasing adoption of both m-health apps and IoT infrastructure, however, has also enabled platform exploitation by cybercriminals to launch malicious actions.

**Revised Manuscript Received on April 07 ,2019.**

**Muhammad Thariq Abdul Razak,** Information Security Interest Group (ISIG), Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia

**Nurul Hidayah Ab Rahman,** Information Security Interest Group (ISIG), Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia

**Nurul Azma Abdullah,** Information Security Interest Group (ISIG), Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia

For instance, a recent data breach of a healthcare app incident in Singapore has compromised about 1.5 million data including Prime Minister privacy data such as name, birth identification number (IC) and race [5].

Dealing with vast amount of IoT related data, may complicate the activities of acquiring and analyzing significant digital evidence. Hence, digital evidence taxonomy would facilitate the activities and enhance forensics readiness (i.e. what type evidence is required prior to incident occurrence, time taken and total cost) [6]. Furthermore, it will help forensic expertise to become proactive and well prepared in terms of forensic tools, standard forensic procedures and experiences.

In this study, taxonomy of digital evidence is proposed by using m-health apps as a case study in Android platform. Significant of our study is to enable a forensically ready for m-health apps in IoT environment.

## II. RELATED WORKS

IoT forensics is one the digital forensics branch that specifically for the cybercrime related to the IoT environment. However, the evolvement of IoT technology and the number of connected devices gives a new challenge to the forensic expertise to preserve, collect, acquire and analyze digital evidence due to the lack of standards forensic readiness and established forensics tools [7]. Since digital forensics are generally reactive, then most of IoT systems or infrastructures are not designed as digital forensics ready. Forensics readiness refers to the capability of an organization to maximize the potential use of digital evidence while minimizing the cost of an investigation [9]. Previous study by Ab Rahman et al. [8] proposed a forensic by design framework specifically for cyber physical cloud system that consists of six development phases such as forensics readiness principle and practices, and laws and regulations to facilitate forensic investigation. The study pointed out that forensic readiness enables forensic by design framework in ensuring the digital evidence are pre-collected, preserved, acquired and analyzed by well standard forensic procedure to protect the integrity of the data.

Previous study by Azfar et al. [10] developed a forensic taxonomy for social apps in Android platform and validated the forensic taxonomy using 30 social apps. Cahyani et al. [11] proposed an evidence based forensic taxonomy on Windows platform. The authors investigated 30 apps to identify which artefacts can be recovered and how the artefacts being organized. Furthermore Azfar et al. [6] proposed a forensic taxonomy for m-health apps in Android platform.

The author outlined 40 m-health apps downloaded from Google Play store to demonstrate the proposed forensic taxonomy. It can be suggested that existing studies in forensic taxonomy are focused on m-health apps in smartphone, however, no existing forensic taxonomy related to the m-health apps that linked to the IoT environment. This is the gap that this paper seeks to address.

## III. THE PROPOSED DIGITAL EVIDENCE TAXONOMY MODEL

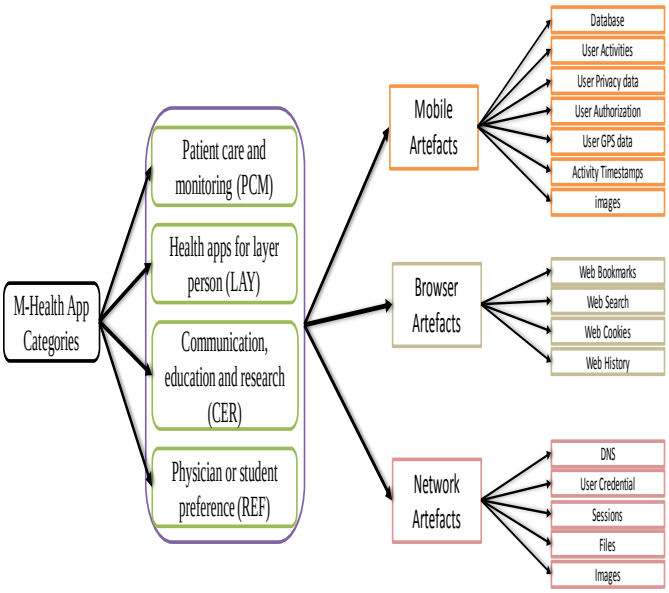


**Fig. 1 Digital evidence taxonomy model for m-health application in IoT environment**

We adopt a m-health classifications from previous study by Ozdalga et al. [12], which categorized into 4 categories, namely: (1) patient care and monitoring (PCM), (2) health apps for layer person (LAY), (3) Communication, education and research (CER) and (4) physician or student preference (REF). We classified the m-health apps artefacts into 3 categories for forensic acquisition activities, namely: (1) mobile artefacts, (2) browser artefacts and (3) network artefacts, as consistent with the three IoT layers—device layer, network layer and application layer—from An et al. [13]. The acquired evidence artefacts are then classified into a number of evidence categories for forensic analysis purpose (see Figure 1).

In order to validate the proposed taxonomy, we investigated the top 34 rating and free Android m-health apps available which reached more than or equal to 50 000 downloads on Google Play Store. This is consistent with previous study by Azfar et al. [6] that investigated 40 apps, and Cahyani et al. [11] investigated 30 apps. A controlled experiment procedure is described in the next sub section.

### A. Experimental Setup in IoT Environment

A controlled experiment approach in Ab. Rahman et al. [14] was adopted as a guide of our experimental design. Six stages of the experiment were designed as follows: (1) Prepare the smartphone device by doing hard reset and install m-health apps; (2) Register m-health apps by adding required details to enable simulation activities; (3) Set up a hotspot to capture network packets; (4) Perform simulation activities such as running, cycling and jogging; (5) Undertake forensic acquisition from the three layers – mobile, browser, and network; and (6) Examine and analyze the acquired artefacts based on the defined artefact types.

We installed the apps on an HTC Butterfly Build (Android version 4.4.2). Magnet Acquire was used to acquire a logical and physical image of the mobile phone. An analysis tool, Autopsy (version 4.7.0) was used to perform the analysis on the acquired images to extract any useful information. Personal laptop (PC) with operating system (OS) Windows 10 Pro will be used to perform the simulation to the specific health website using a specific browser such as Google Chrome and Firefox. After the simulation finished, FTK Imager software (version 3.2.0) was used to acquire a logical image. Network packets were captured using Wireshark software (version 2.6.2) while Network Miner software (version 2.3.2) was used to perform the analysis of network packets.

## IV. RESULTS AND DISCUSSION: FORENSIC ANALYSIS OF 34 M-HEALTH APPS

In this section, we discuss the experiments result of two apps only (due to page limitation). The overall results of the 34 m-health apps evidence taxonomy are presented in Appendix A. Each recovered artefact is represented by three types which are full (F), partial (P) and none (N).

### A. Experiment Results: Runtastic Running App & Mile Tracker

Runtastic Running App & Mile Tracker (version 8.8) allows users to track their physical activities such as running, walking, jogging and cycling. Furthermore, users can set their goals with a specific period of time, share their sports activities and photo with another application such as Facebook, Twitter, and Instagram.

#### 1) Mobile Artefacts

Main database and key tables were found that presents correspondence metadata with the simulated activities.

**Database**

Forensic analysis pointed out that the files and database created by Runtastic Running App & Mile Tracker are stored on the internal smartphone memory from the path /data/com.runtastic.android/database. It should be noted that the path is inaccessible to end users. The acquired artefacts from the app are listed in Table 1.

**Table. 1 Artefacts of Runtastic Running App & Mile Tracker**

| Content | Directory | Files |
|---|---|---|
| Main Database | /data/com.runtastic.android/database | db.db (SQLite, 39 tables) |

The db.db database is the app's main database containing 39 tables in which, only 8 tables present significant evidence of interest (see Table 2).

**Table. 2 Artefacts of Runtastic Running App & Mile Tracker**

| Table name | Content |
|---|---|
| Users | Users detail such as first name, last name, country code and city name |
| Workout<br>Speed<br>Gps<br>Session<br>Training plan<br>Goal | User record of type of workout, User speed record each workout, location and planning and goal |
| geotaggedPhoto | User photo uploaded time, location (longitude, latitude and altitude), time taken and link URL of the photo |

In table Session, for example, the attributes of startTime, endTime, firstLatitude, firstLongtitude, lastLongtitude, lastLatitude and locationName fields present key evidence of forensic interest (see Table 3). For example, startTime and endTime stored user starting and ending timestamp for each activity. It should be noted that the timestamp is stored in UNIX Epoch format. Furthermore, firstLatitude, firstLongtitude, lastLongtitude, and lastLatitude stored location point of user for each activity performed. Time and location are the common key points in determining what, where, and when, in addition to who, why, and how a crime occurred.

**Table. 3 Metadata of sessions table in Runtastic Running App & Mile Tracker**

| Id | userID | startTime | month | Year | End Time | Server Update | Location Name | First Altitude | First Longtitude | Last Altitude | Last Longtitude |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 135422373 | 1536565526000 | 9 | 2018 | 1536565838000 | 1536565924000 | Parit Raja | 1.86008405685425 | 103.084365844727 | 1.85996174812317 | 103.084335327148 |
| 2 | 135422373 | 1536628842000 | 9 | 2018 | 1536629466000 | 1536629578000 | Parit Raja | 1.86010456085205 | 103.084098815918 | 1.86015605926514 | 103.084480285645 |
| 3 | 135422373 | 1536657440000 | 9 | 2018 | 1536657812000 | 1536657933000 | Parit Raja | 1.86008954048157 | 103.084403991699 | 1.86008954048157 | 103.084403991699 |

### 2) Browser Artefacts

Our analysis on the PC forensic images pointed out several evidences found in browser internet history such as bookmarks, and search engine that useful for forensic investigation.

**Table. 5 Web search results metadata**

| Text | Domain | Date Accessed | Program |
|---|---|---|---|
| runtastic | www.google.com | 2018-09-10 16:10:34 SGT | Chrome |
| runtastic | www.google.com | 2018-09-11 12:12:58 SGT | Chrome |
| runtastic | www.google.com | 2018-09-11 17:27:13 SGT | Chrome |
| Runtastic login | www.google.com | 2018-09-11 16:36:57 SGT | Chrome |

Based on Table 5 all the text of search engine in browser internet history has been successfully acquired. The date accessed, text and domain can be classified as important evidences as it recorded the time, date and the typed from the search engine. Besides that, domain field denoted domain used by the user to search a specific keyword for specific purposes.

**Table. 6 Web bookmarks metadata**

| URL | Title | Date Created | Program | Domain |
|---|---|---|---|---|
| https://www.runtastic.com/ | Runtastic: Running, Cycling & Fitness GPS Tracker | 2018-09-10 15:55:59 SGT | Chrome | www.runtastic.com |

Table 6 illustrates the acquired web bookmarks which presents the Uniform Resource Locator (URL), date created and domain. For example, web bookmarks will store the URL of the specific website when the user adds specific URL to bookmark, the browser will store the date created and domain of URL.

### 3) Network Artefacts

Our examination of hosts information, network sessions, DNS queries and answer, and the timestamp is presented in Table 7. It has been observed that the app using Secure Socket Layer (SSL) protocol to encrypt the communication between the client and the host at the network application layer.

**Table. 7 Network Metadata**

| Client Host | Server host | Protocol | DNS Queries | DNS Answers | Timestamp |
|---|---|---|---|---|---|
| 192….22 [android-6f50fc21bb17521b](Linux) | 83…..133 [prd-ssl-appws.runtastic.com][appws.runtastic.com] | SSL | appws.runtastic.com | www.runtastic.com | 2018-09-11 01:31:09 UTC |
| 192….22 [android-6f50fc21bb17521b](Linux) | 83…..133 [prd-ssl-appws.runtastic.com][appws.runtastic.com] | SSL | runtastic.pushwoosh.com | r1-front-06.pushwosh.com | 2018-09-11 01:33:53 UTC |

DNS queries, for example 'appws.runtastic.com' is the example of the query used to request information to the specific server. In forensic perspective, this query can represent clues about the app activity in the network layer. It can thus be suggested that timestamp can be utilized for timeline analysis technique to correlate with correspondence information from mobile, browser, as well as from the site of apps' servers.

### B. Experiment Results: MyPlate Calorie Tracker

MyPlate Calorie Tracker (version 3.4) provides services calories tracker and stay fit within user Android phone. User can share their recipe, photo, tips and advice in active community filled with thousands of members. This app also allows users to add specific foods (that are not available in the database) because each region country has different type of food and meals.

#### 1) Mobile Artefacts

Main database and key tables were found presents correspondence metadata with the simulated activities.

**Database**

Forensic analysis indicated that the files and database created by the MyPlate Calorie Tracker are stored on the internal smartphone memory from the path /data/com.livestrong.tracker. The acquired artefacts from the app are presented in Table 8.

**Table. 8 Artefacts of MyPlate Calorie Tracker**

| Content | Directory | Files |
|---|---|---|
| Main Database | /data/ com.livestrong.tracker/ database | Calorietracker. db (SQLite, 10 tables) |

The Calorietracker.db database is the app's main database containing 10 tables. However, only 6 tables present significant evidence of interest (see Table 9).

**Table. 9 Artefacts of Runtastic Running App & Mile Tracker**

| Table name | Content |
|---|---|
| DIARY_ENTRY | Record user activity such as carbs consumed, fat consumed, protein consumed and time period |
| FOOD MEAL GOALS | User record of type food, meal and goals |
| EXERCISE | User record exercise |
| PROFILE | Users detail such as username, date of birthday, age and gender. |

Based on Table 9, for example table profile, the attribute of USERNAME, AVATAR_LARGE, AVATAR_SMALL, DOB, HEIGHT, WEIGHT, WEIGHT_GOAL, AGE and GENDER represent as key evidence for forensic interests (see Table 10). For example, AVATAR_LARGE and AVATAR_SMALL stored the user profile picture in term of link URL. Furthermore, table MEAL consists attributes such as DATE_CREATED, DATE_DELETED, DATE_MODIFIED and NAME that are useful for forensic investigation. For example, DATE_CREATED, DATE_DELETED, DATE_MODIFIED store the user creation and deletion time of specific meal. Moreover, attribute NAME will store the name of the specific meal created by the user. Furthermore, attribute WEIGHT and WEIGHT_GOAL store the actual weight and weight goal in format pound (lbs.). For the attribute gender, 2 flags have been used to represent user gender, which is 0 - male and 1 - female.

**Table. 10 Metadata of profile table in MyPlate Calorie Tracker**

| USERNAME | AVATAR_SMALL | AVATAR_LARGHE | DOB | HEIGHT | WEIGHT | WEIGHT_GOAL | AGE | GENDER |
|---|---|---|---|---|---|---|---|---|
| Thariq9694 | https://img.aws.livestrongcdn.com/ls-96x96/livestrong/ls_images/tdp-images/avatars/0/1/14269160.png?v=1540267850 | www.livestrong.com/ls_images/tdp-images/avatars/0/1/14269160.png?v=1540267850 | 2018-09-10 | 0 | 151.02 | 110.231124 | 24 | 0 |

### 2) Browser Artefacts

Our analysis on the PC forensic images indicated several evidences found in browser internet history such as bookmarks, and search engine that useful for forensic investigation.

**Table. 11 Web search results metadata**

| Text | Domain | Date Accessed | Program |
|---|---|---|---|
| myplate login | www.google.com | 2018-10-23 12:14:05 SGT | Chrome |
| myplate login | www.google.com | 2018-10-24 15:15:48 SGT | Chrome |
| myplate login | www.google.com | 2018-10-26 11:16:13 SGT | Chrome |

Based on Table 11 all the text of search engine in browser internet history has been successfully acquired. The Date Accessed, Text and Domain can be classified as important evidences as it recorded the time, date and the typed from the search engine. In addition, domain field denoted domain used by the user to search a specific keyword for specific purposes.

### 3) Network Artefacts

Based on our observation on host, network sessions, DNS queries and DNS answers and the timestamp, we can conclude that MyPlate Calorie Tracker app using Secure Socket Layer (SSL) to encrypt the communication between the client host and server host (see table 12).

**Table. 12 Network metadata**

| Client Host | Server Host | Protocol | DNS Queries | DNS Answers | Timestamp |
|---|---|---|---|---|---|
| 192….110 [android-6f50fc21bb17521b](Linux) | 23…..252 [e3087.g.akamaiedge.net][san.www.demandmedia.com.edgekey.net][www.livestrong.com][www.demandmedia.com] | SSL | www.livestrong.com | cdn-www.livestrong.com.edgesuit.net | 2018-10-23 03:59:30 UTC |

Based on Table 12, DNS query ‘www.livestrong.com’ is the example of the query used by the app to request specific information to the server. In the forensic viewpoint, this query can stand for clues about the app activity in the network layer. Furthermore, attribute Client Host and Server Host store the IP address of the specific server and client, hence can be as an evidence to identify which device being used to request information to the targeted server. Attribute Timestamp will store the time taken when the client and server perform specific operations to transfer and receive data through the internet. It should be noted that the timestamp is in format Coordinated Universal Time (UTC).

## V. SUMMARY

Digital evidence taxonomy would facilitate forensic expertise to identify any possible artefacts of data remnant in each layer of the IoT model in forensic investigation. In this study, we presented digital evidence taxonomy in IoT environment and focus on m-health apps, hence contributing to the gap in the existing related works. 34 top rating m-health apps is used is this study to validate the purposed digital evidence taxonomy in IoT environment. All the acquired data from each layer in IoT environment can be categorized based on the purposed digital evidence taxonomy. Our results identified important metadata of m-health apps in each IoT layer such as type of activity, location (altitude, longitude and altitude), web bookmarks, DNS query and timestamps which able to facilitate evidence correlation. This indicates the usability of the proposed taxonomy model. Future research will focus on developing a knowledge based expert system repository to automate the identification of potential artefacts in each IoT layer as well as enable a forensically-ready environment.

## ACKNOWLEDGMENT

The authors express appreciation to the Ministry of Higher Education (MOHE) and Universiti Tun Hussein Onn Malaysia (UTHM). This research is supported by the Fundamental Research Grant Scheme (FRGS) grant (Vot 1640) and grant TIER 1 grant (Vot H196). The authors thanks to the anonymous reviewers for the feedback and UTHM for supporting this research.

## REFERENCES

1. M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, “A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT),” in 2015 Internet Technologies and Applications (ITA), 2015, pp. 219–224.
2. R. Fitzgerald and V. Karanassios, “The Internet of Things (IoT) for a smartphone-enabled optical spectrometer and its use on-site and (potentially) for Industry 4.0,” 2018, vol. 10657, pp. 1065705–1065711.
3. P. Macharia et al., “Enhancing data security in open data kit as an mHealth application,” in 2015 International Conference on Computing, Communication and Security (ICCCS), 2015, pp. 1–4.
4. Markus Pohl, “325,000 mobile health apps available in 2017 – Android now the leading mHealth platform,” 2017. [Online]. Available: https://research2guidance.com/325000-mobile-health-apps-available-in-2017/.
5. Irene Tham, “Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore’s worst cyber attack,” 2018. [Online]. Available:

https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

6. A. Azfar, K. K. R. Choo, and L. Liu, "Forensic Taxonomy of Popular Android mHealth Apps," Proc. Am. Conf. Inf. Syst. 2015, no. August, pp. 13–15, 2015.
7. O. Adjei, N. Babu C, and O. Yakubu, "a Review of Digital Forensic Challenges in the Internet of Things (Iot)," Int. J. Mech. Eng. Technol., vol. 9, no. 1, pp. 915–923, 2018.
8. N. H. A. Rahman, W. B. Glisson, Y. Yang, and K. K. R . Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," IEEE Cloud Comput., vol. 3, no. 1, pp. 50–59, 2016.
9. R. Rowlingson, "A Ten Step Process for Forensic Readiness International Journal of Digital Evidence," Int. J. Digit. Evid., vol. 2, no. 3, pp. 1–28, 2004.
10. A. Azfar, K. K. R. Choo, and L. Liu, "Forensic Taxonomy of Android Social Apps," J. Forensic Sci., vol. 62, no. 2, pp. 435–456, 2017.
11. N. D. W. Cahyani, B. Martini, K. K. R. Choo, N. H. Ab Rahman, and H. Ashman, "An Evidence-Based Forensic Taxonomy of Windows Phone Communication Apps," J. Forensic Sci., vol. 63, no. 3, pp. 868–881, 2018.
12. E. Ozdalga, A. Ozdalga, and N. Ahuja, "The smartphone in medicine: A review of current and potential use among physicians and students," J. Med. Internet Res., vol. 14, no. 5, 2012.
13. J. An, J. Hwang, and J. Song, "Interworking technique and architecture for connecting LAN IoT devices towards standardized IoT service layer platform," 2016 IEEE 5th Glob. Conf. Consum. Electron. GCCE 2016, pp. 1–2, 2016.
14. N. H. Ab Rahman, N. D. W. Cahyani, and K. K. R. Choo, "Cloud incident handling and forensic-by-design: cloud storage as a case study," Concurr. Comput. , vol. 29, no. 14, pp. 1–16, 2017.
15. S.V. Manikanthan, T.Padmapriya, "United Approach in Authorized and Unauthorized Groups in LTE-A Pro", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue, 2018, pp. (1137-1145).

## APPENDIX A- DIGITAL EVIDENCE TAXONOMY OF THE 34 M-HEALTH APPS

| App ID | App Name | Version | App Category | | | | | Mobile Artefacts | | | | | | | Network Artefacts | | | | | | | Browser Artefacts | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Patient care and monitoring | Health apps for the layperson | Communication, education and research | Physician or student preference | Database | User Authorization | User Privacy Data | user activities | User GPS data | Activity Timestamps | Images | Parameter | DNS | Session | User Credential | Files | Images | Web Bookmarks | Web Cookies | Web Search | Web History |
| 1 | Google Fit: Health and Activity Tracking | 1.82.40 | | / | | | P | N | N | P | P | F | N | F | F | P | N | F | N | F | P | F | F | P |
| 2 | Fitness Buddy: Gym Workout, Weight Lifting Tracker | 3.1 | | / | | | F | N | N | F | F | F | N | P | F | P | P | P | N | F | P | F | F | P |
| 3 | TrainingPeaks | 6.6 | | / | | | P | P | P | N | N | F | N | P | P | P | N | P | N | F | P | F | F | P |
| 4 | Runtastic Running App & Mile Tracker | 8.8 | | / | | | F | N | F | F | F | F | N | F | P | P | N | P | N | F | P | F | F | P |
| 5 | WebMD | 6.3.4 | / | / | / | | P | P | P | F | F | P | N | P | F | F | P | F | N | F | P | F | F | F |
| 6 | Caledos Runner - GPS Running Cycling Walking | 4.1.0.510 | | / | | | N | P | N | N | N | N | N | F | F | P | N | F | N | F | P | N | F | F |
| 7 | Lose It! - Calorie Counter | 9.6.4 | | / | | | F | N | N | F | F | F | N | P | P | P | N | P | N | F | P | P | F | F |
| 8 | Relive - Your Outdoor 3D Videos | 2.4.6 | | / | | | F | N | F | F | F | F | P | F | P | F | N | P | N | F | P | P | F | F |
| 9 | Pacifica - Stress & Anxiety | 7.0.2 | | / | | | N | N | N | N | N | N | P | P | F | F | N | F | N | F | P | P | P | F |
| 10 | Runtastic Road Bike Trails & GPS Bike | 3.6.2 | | / | | | F | N | F | F | F | F | F | F | P | P | N | P | N | F | P | P | F | P |
| 11 | SuperBetter | 1.1.8 | | / | | | N | N | N | N | N | N | N | F | P | P | N | F | N | F | P | P | P | F |
| 12 | Sports Tracker Running Cycling | 3.43.2 | | / | | | P | P | N | F | F | F | P | P | F | F | N | P | N | F | P | P | P | P |
| 13 | Instant Heart Rate: HR Monitor & Pulse Checker | 5.36.4730 | / | / | | | F | P | F | N | F | F | N | F | F | P | N | F | N | F | P | P | F | F |
| 14 | Running tracker - Run-log.com | 1.25.2 | | / | | | F | F | N | F | F | F | N | P | F | F | F | F | N | F | P | P | F | F |
| 15 | u4fit: GPS Track Run Walk | 7.9.1 | | / | | | F | P | P | F | F | F | N | P | F | F | N | P | P | P | P | P | F | F |
| 16 | Lifesum Diet Plan, Macro Calculator & Food Diary | 6.3.6 | / | / | | | F | F | P | F | N | F | N | P | F | F | N | P | N | F | P | P | F | F |
| 17 | Happify-Science-based activities and games to overcome stres | 1.34.0 | | / | / | | N | F | N | N | N | P | N | F | P | P | N | F | N | F | P | P | F | F |
| 18 | Decathlon Coach - Running, Walking, Pilates, GPS | 1.20.1 | | / | | | F | P | N | F | F | F | N | P | P | P | N | F | N | F | P | P | F | F |
| 19 | Endomondo: Running & Walking | 18.8.1 | | / | | | F | N | N | F | F | F | N | P | P | P | N | F | N | F | P | P | F | F |
| 20 | Smiling Mind | 3.3.7 | | / | | | F | P | P | P | N | P | N | P | F | F | N | F | N | F | P | P | F | P |
| 21 | IFIT Workout Tracker, Weight Lifting, Gym Log App | 10.11 | | / | / | | F | F | P | F | N | F | N | F | F | P | N | P | N | F | P | P | P | F |
| 22 | Workout Tracker, Weight Lifting, Gym Log App | 1.13 | | / | / | | N | P | F | N | N | N | N | F | P | P | P | P | F | F | P | P | F | P |
| 23 | Glucose Buddy Diabetes Tracker | 5.36.3775 | / | / | | | P | P | F | F | N | F | N | P | P | F | N | F | P | F | P | P | F | F |
| 24 | Strava Training - Track Running, Cycling & Swimming | 64.0.0 | | / | | | F | P | P | F | F | F | F | F | F | F | N | P | P | F | P | P | F | F |
| 25 | Workout Trainer fitness coach | 8.9 | | / | / | | N | N | P | N | N | N | N | F | P | F | P | F | F | F | P | P | F | F |
| 26 | Calm Meditate, Sleep, Relax | 4 | | / | | | F | P | N | F | N | F | N | F | P | P | P | N | F | N | P | P | F | F |
| 27 | CareZone | 7.6.0.2 | / | | / | | F | N | P | F | N | F | F | P | P | F | N | F | N | F | P | P | P | F |
| 28 | Alo Moves: Yoga Classes | 4 | | / | / | | N | N | N | P | N | P | P | P | F | F | P | P | N | F | P | P | F | F |
| 29 | Calorie Counter & Diet Tracker | 4.71 | / | / | / | | P | F | N | P | N | F | N | F | F | P | P | P | F | F | P | P | F | F |
| 30 | AllTrails: Hiking, Running & Mountain Bike Trails | 8.9.3 | | / | | | F | P | N | F | F | F | N | F | F | P | F | N | F | N | P | P | F | F |
| 31 | Skimble: GPS Sports Tracker | 1.0.4 | | / | | | F | N | P | F | F | F | N | F | F | F | P | P | F | N | P | P | F | F |
| 32 | Runtastic Mountain Bike GPS Tracker | 3.6.2 | | / | | | F | N | F | F | F | F | F | P | F | P | N | P | N | N | P | P | F | F |
| 33 | MyPlate: Calorie Tracker | 3.4.0(0) | / | / | / | | F | N | F | F | N | F | P | F | F | P | N | F | P | F | P | P | F | F |
| 34 | Calorie Counter by FatSecret | 7.9.36 | / | / | / | | F | P | N | F | N | F | F | F | F | P | F | N | F | N | F | F | F | F |

Notes
"F" - detailed information recovered successfully;
"P" - only partial data was recovered,
"N" - None data was recovered