Forensic Analysis of Wearable Devices: Fitbit, Garmin and HETP watches

Áine MacDermott[1], Stephen Lea[1], Farkhund Iqbal[2], Ibrahim Idowu[1], Babar Shah[2]
[1]*Department of Computer Science, Liverpool John Moores University, Liverpool, UK*
[2]*College of Technological Innovation, Zayed University, United Arab Emirates*
{a.m.macdermott, s.p.lea, i.o.idowu}@ljmu.ac.uk;{farkhund.iqbal, babar.shah}@zu.ac.ue

***Abstract*—Wearable technology has been on an exponential rise and shows no signs of slowing down. One category of wearable technology is Fitness bands, which have the potential to show a user's activity levels and location data. Such information stored in fitness bands is just the beginning of a long trail of evidence fitness bands can store, which represents a huge opportunity to digital forensic practitioners. On the surface of recent work and research in this area, there does not appear to be any similar work that has already taken place on fitness bands and particularly, the devices in this study, a Garmin Forerunner 110, a Fitbit Charge HR and a Generic low-cost HETP fitness tracker. In this paper, we present our analysis of these devices for any possible digital evidence in a forensically sound manner, identifying files of interest and location data on the device. Data accuracy and validity of the evidence is shown, as a test run scenario wearing all of the devices allowed for data comparison analysis.**

Keywords—digital forensics, internet of things, wearable technology, forensic analysis, fitbit, garmin, fitness bands.

I. Introduction

Wearable technology and smart devices are increasingly utilised in our daily lives, with varying functionalities. Wearable technology is an umbrella term for many 'smart' devices, i.e. smartwatches, smart clothing, smart eyewear. This paper specifically explores smart fitness watches/bands /trackers which also fall under this category. Many popular brands are worn on a daily basis by users to track their activities, such as sleeping, walking, and running, etc. Recently, they are used by employers to track employees' performance/utilisation of resources etc. – an example of this is in Amazon warehouses. Regardless of frequent or infrequent use, these fitness bands may store vital data for forensic investigators. Current trends show how fitness tracking wearables have risen in popularity, with wrist worn devices the most used. A close connection from the user to a device that is monitoring what the user is doing, the amount of personal data that is being created, transmitted and stored is apparent, and the type of data that may possibly be extracted from wearable devices can play a vital role in the future of digital forensics.

As more people use such technology, device type and price can determine forensic feasibility, and level of device security. At the time of writing, no specific research has been conducted on the actual products that will be evaluated in this project. Comparable work has mainly focused on smartwatches and the paired devices, such as smartphones and the applications used in conjunction with the smartwatch or fitness band. This paper has a particular focus and motivation of evaluating the devices themselves and not any paired smartphone devices due to the lack of current research. Web applications that have a user account linked to a device and that can be synced will also be reviewed, and finally if any evidence is acquired, how valuable and accurate is the evidence. The increasing amount of digital devices that use various hardware and software increases the challenges and difficulties that face the digital forensics sector [1], current obstacles are indicated by [2] and include complexity, consistency, data volume, and unified time-lining of evidence due to multiple time zones. Digital forensics will be able to assist in a many more crimes and investigations if more is done to fill the research void and by conducting the related research, build a greater knowledge of fitness bands. An example of how else wearable technology can be used for other forensic assessments is presented [3], where a Fitbit smartband is used in a compensation case after a person was seriously injured. The main objectives of the project were as follows: 1) Run manual, physical and logical data extraction methods as required on the three devices if possible and their connected applications on a PC. Explore what data is stored or what data will be potentially stored on all devices. Record all data captured, any difficulties that may have been present during the extraction, and also any additional methods that may have to be used to extract the user data. 2) Based upon the literature review, define exactly what experiments are needed for the aforementioned devices in order to forensically examine Garmin, Fitbit and a generic low-cost HETP fitness tracker based upon the documented firmware systems. 3) Conduct experiments to establish what data is retrievable, where is that data stored on such devices, how does one conduct an investigation on the devices whilst maintaining integrity of the data. Document Manual extraction findings from the three devices paired applications. The structure of this paper is as follows: Section II provides background on the rise in wearable devices and digital forensics. Section III conveys related works in this area. In Section IV, we discuss the methodology and experiments on our fitness trackers. Section V details our findings and evidences found on the trackers, and we conclude our findings in Section VI.

II. Background

The Internet of Things (IoT) offers many challenges to digital forensics and most research to date concerning IoT devices has mainly focused on security and privacy issues, due to the data collection functionalities of such devices. Forensic data extraction techniques and analysis methodologies have to be considered an imminent need for IoT device analysis. The amount of devices currently in use will only grow and many IoT devices have the capabilities to store digital evidence, though: *how, where, and for how long* is often unclear. As stated, the focus of this project was on fitness bands and in particular the device only and no other connecting hardware. Some of these devices will work alone as an individual device and some will work with pairing device, such as smartphone or PC. This is mainly for visual representation of the users activities, based upon what the fitness band may be monitoring and its functionality, but the data that is passed across from the device instantly and what data is left behind on the device is a key question. The fitness bands will be

978-1-7281-1542-9/19/$31.00 ©2019 IEEE

forensically examined in order to evaluate what user data is stored on the device and what data can be extracted for use by a forensic examiner who may need that data as evidence in an investigation. Additionally, a further question was: *if the fitness band was lost or stolen, is the data easily accessible?* Once the experiments have been conducted, the results will be compared to any research of others, some of that research was carried out on smartphone applications or web server applications used in conjunction with similar devices.

A report by the International Data Corporation (IDC) [4] showed the growth in wearable device shipments. It stated that in the first quarter of 2018 there was a rise by 1.2%, two of the top five leading brands featured are used within this project - Fitbit and Garmin. Interestingly, out of the 21.5 million wearable devices shipped, 95% of these devices were watches and wrist bands. These figures show the continuing growth of wearable devices being sold, wrist bands and in particular, Garmin and Fitbit are right at the top of leading manufactures with 5.0% and 8.7% of the market share, but over 50% of the market share belongs to other brands, which was a motivating factor to compare well-known brands and a generic fitness band. In [5], a technical article discusses how evidence from wearable devices can and have been used in various criminal cases. In one case, Fitbit data proved that a woman was lying about being assaulted. It proved that she was walking around during the time she had said she was asleep and dragged from her bed [6]. A Fitbit was used to prove the lack of activity and movement due to an accident in a personal injury case, this is to determine the effects of the accident [7]. Finally, a man was facing multiple charges of reckless driving after he fled police in a road race. The man was wearing a GoPro camera which recorded the entire event, and he later posted the captured video on YouTube [8].

Obviously the majority of wearable devices are smaller in comparison to smartphones or tablets, thus memory types and storage sizes have to be a big consideration for manufacturers, designers and developers. The vast majority of fitness bands are embedded systems and use flash memory. Physical imaging of a hard drive can often find a plethora of data, whereas physical imaging of many wearable devices may be impossible or just not achievable with the knowledge and forensic tools available, proving the importance of this research. Other ways and means have to be explored in order keep pace with the development of wearables, additionally to the variety of brands, operating systems (OSs) and memory types of all wearables have to be considered when conducting research and developing new forensic software. Watson et al. [9] detail how there currently are no standards, methods or guidance on how a forensic practitioner would embark on an investigation regarding many wearable devices. They also question what data is being captured, is it being shared with other devices, is that data accessible and readable to an investigator? And finally, can it be retrieved at all?

With this in mind, our research questions for experiments are as follows:

- Do the fitness bands actually store data?
- What data (if any) is stored on the devices?
- Is it possible to acquire evidence in a forensically sound manner?
- Do different leading brands of fitness bands store data differently i.e. in a different format and offer different challenges in comparison to a generic cheaper brand?
- Could any possible data acquired be used as evidence, i.e. can the data be useful? And admissible in court?
- How accurate is any evidence generated by fitness bands?

III. Related Works

The amount of devices that process, share, and store data is rising. The digital forensic industry needs to work with companies that design and develop these devices in order to update methods and techniques for data extraction [4] - this is essential as digital evidence is being generated constantly and there is growing ignorance and confusion as to how to analyse and extract the data. Based upon the lack of related work to this point of the project, we expect to achieve a certain level of data extraction but, data type, quality and quantity is unknown. Retrieving data from flash memory IoT devices can be extremely challenging for digital forensic practitioners, as many of the tried and tested methodologies and software tools in use today are simply not designed in such way - tools are more matched with traditional digital forensics. The National Institute of Standards and Technology (NIST) published a report in 2014 [10] regarding guidance for mobile forensics, in the report a detailed model of levels of extraction for mobiles. The key forensic extraction methods are:

- Manual extraction: Viewing the evidence directly from the devices display
- Logical extraction: Connectivity to the device via either a wired or Bluetooth connection and creating a logical image of files and folder
- Hex Dumping/JTAG: Physical extraction level, deleted files and unallocated space can be analysed
- Chip-Off: Physical removal of the memory for analysis
- Micro Read: View the physical state of gates using microscopes

A data extraction model was proposed by [11]. Each branch represents stages of analysis, breaking the extraction methods into separate sections as shown in Figure 1.

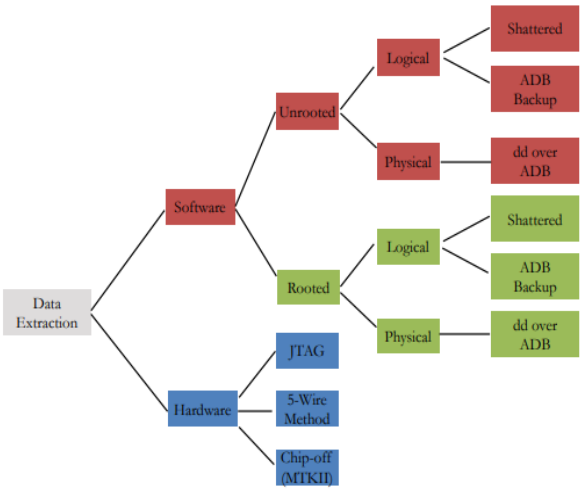


Fig. 1. Data extraction branch methods [11]

The majority of research on wearable technology has covered iOS and Android OS specifically for wearables such as smartwatches, and this may not be what is installed on all fitness bands – this can vary per brand and functionality. Analysis of two Samsung watches in [12] also highlights the lack digital forensic research of smartwatches (notably a common theme regarding wearable technology amongst researchers). In their work they were successful in extracting data from both smartwatches, one using a Linux based kernel and the other using an Android kernel. The Linux based smartwatch was reported to be analysed in a *"more forensically sound"* manner because the Android based smartwatch had to be reset and flashed to gain root access to the device.

Similarly, in [13], analysis of a Sony smartwatch 3, also running an Android OS, needed to be rooted in order to gain access. FTK was used to analyse the device. An Apple smartwatch series 2 was analysed by [14], as there is no connectivity in terms of a physical cable, logical and manual acquisition methods were used in the case study. The logical acquisition method did use the traditional method of many others, with a logical image being taken of the paired smartphone, on this case, an Apple iPhone. Evidence of the connected smartwatch was found in a database of paired Bluetooth devices, the database had multiple data entries regarding the smartwatch which could prove as vital evidence: UUID (Universal Unique Identifier), name, address, resolved address, last seen and last connection times were all observed. This evidence was all found inside the watch application on the Apple iPhone. Nike plus and GPS data were all retrieved and an abundance of data was found, which could all be potentially, used as evidence. In [15], forensic analysis of an Android Wear Sony Smartwatch 3 (SWR50) running Android OS is presented. The process begins with rooting the device, like [12, 13]. The evidence found on the device was scattered across memory blocks, but would hold a significant importance to an investigation. Activities from the paired Smartphone were present on the Smartwatch but in a partial form. As there are no defined principles for IoT device forensics, investigations will significantly rely on understanding and analysis of the mechanical and physical nature of the smart device [15].

IV. Methodology and Experiments

Much of the digital forensics research regarding wearable devices has been conducted on the paired devices, with the applications that connect to the device (e.g. mobile phone) being analysed or closely related devices in order to gain knowledge. However, if the paired device is not accessible or available, the devices themselves have to be analysed. Our experiments will be conducted on three fitness bands - a Garmin forerunner 110, a Fitbit Charge HR and a low cost generic band HETP fitness tracker – as illustrated in Figure 2.

Fig. 2. From left to right, Garmin, Fitbit and HETP devices

The devices will be connected to a forensic workstation for analysis, and a secondary workstation established to if the devices can be synced to another device using a different user account. A new user account will be set up using a different email to ensure it is completely independent from the initial user.

Scenario

All devices had historical data (specifically for testing purposes) on them before the four test runs were completed. Leaving the historical data on the devices will help identify evidence that may be available, and also to determine what evidence is expected to be present on the devices. The test runs were based on the subject wearing all devices at once, running one mile with a deliberate elevation change in a predetermined route, approximately at the half way point, which will allow for evidence accuracy and validity tests. Forensic Toolkit (FTK) and FTK Imager, plus Autopsy forensic tools will be used in examining the devices. In addition, open source suites that are deemed useful or have any extra features will be used.

Device recognition and forensic imaging

Manual extraction phase was crucial in identifying the type of evidence that could be possibly stored in user accounts of all three of the devices and the paired accounts that can accessed via the test machines. This was due to the lack of research and knowledge of what information is stored in various fitness brands. The *Garmin Forerunner 110* device did allow potential evidence to be seen on screen without any password or pin protection. Simply scrolling through the device options to view all activities stored on the device, the user profile and device setup. Both the *Fitbit* and *HETP* devices displayed very little information on the device and the step, floor counters etc. resetting to zero each night at 00:00. The amount of personal data that is stored in the paired user accounts in either the web browser or in the Smartphone application would have huge value to an investigator, this would be reliant on the user giving up their passwords and log in details and giving consent to analyse the accounts.

A. Garmin Forerunner

The Garmin Forerunner was imaged directly using FTK Imager and the Windows 10 virtual machine file was imaged (.vmdk) using FTK Imager. A snapshot of the image was also taken and analysed. Both images were fully verified correctly using FTK and with the hash values correct – see Figure 3.

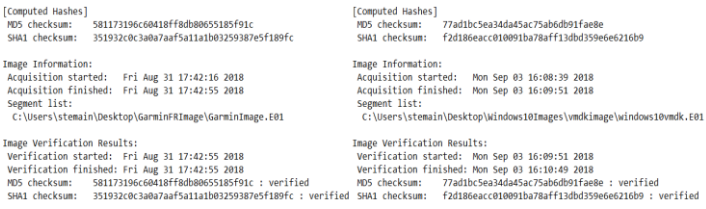


Fig. 3. Verified hash values of the acquired images

Files of interest were all located inside the Garmin folder stored directly on the device and all other files were stored inside the following folders. The activities folder contains all of the devices saved activities regardless of type (running, walking, cycling etc.). The four activities selected are the test runs that were completed during this project and therefore, have been highlighted. After examining the activities folder, a total of 278 activities were listed: 215 of the listed activities were accessible through the device and a windows folder once connected to a machine. Deleted activities were found in the unallocated space. The remaining 63 activities were either deleted by the user at some point in the device history or

deleted automatically by the device due to memory constraints. Once the device has reached its capacity, it begins to overwrite the previous activities from first written (oldest) onwards. These were successfully retrieved and viewed as shown in Figure 4.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
2016-04-19-09-07-59.fit	2016-04-19 10:01:14 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-19 10:01:14 BST	10856	Unallocated
2016-04-21-12-00-29.fit	2016-04-22 10:14:40 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-22 10:14:40 BST	19568	Unallocated
2016-04-19-09-07-59.fit	2016-04-23 14:26:46 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-23 14:26:46 BST	5148	Unallocated
2016-04-23-14-26-50.fit	2016-04-24 08:29:42 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-24 08:29:42 BST	17756	Unallocated
2016-04-24-08-29-54.fit	2016-04-25 14:02:18 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-25 14:02:18 BST	21508	Unallocated
2016-04-25-14-02-30.fit	2016-04-26 09:08:40 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-26 09:08:40 BST	30812	Unallocated
2016-04-26-09-08-53.fit	2016-04-29 09:18:18 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-04-29 09:18:18 BST	9360	Unallocated
2016-05-01-08-19-58.fit	2016-05-04 11:43:10 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-05-04 11:43:10 BST	36832	Unallocated
2016-05-04-11-43-49.fit	2016-05-06 15:37:20 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-05-06 15:37:20 BST	43344	Unallocated
2016-05-06-15-37-24.fit	2016-05-06 16:31:24 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	2016-05-06 16:31:24 BST	16460	Unallocated

Fig. 4. Deleted activities found in the unallocated space of the Garmin

At this stage though, the amount of deleted activities that may be retrievable, cannot be confirmed. How long they are stored in the unallocated space before they are overwritten? Is there a limit to how many would be stored on the device and still be accessible through forensic tools? Note in Figure 4, that the found files end in a *.fit* extension. Various file types from both the Garmin and Fitbit devices were found and were not all viewable in FTK Toolkit and Autopsy. A key file was the *.fit file*. The different file types did have to be extracted from the toolkits used and imported to open source software packages - GoldenCheetah and FitSDK. GoldenCheetah is analysis software for fitness devices, whereas FitSDK is a development package (creates and decodes the .fit file structure). Firstly, analysing the data inside an activity file - GoldenCheetah displays a summary of the activity, duration, time moving, distance and elevation gain in addition to many other activity details. FitSDK allows the conversion of the *.fit file* to a *.csv file*, which can then be viewed in Microsoft Excel. While the information is similar to what is available in GoldenCheetah, more device specific evidence is available using the FitSDK.

Type	Local Number	Message	Field 1	Value 1	Units 1	Field 2	Value 2	Units 2	Field 3	Value 3	Units 3
Definition	0	file_id	serial_number	1		time_created	1		manufacturer	1	
Data	0	file_id	serial_number	3861884384		time_created	904374761		manufacturer	1	
Definition	1	file_creator	software_version	1		hardware_version	1				
Data	1	file_creator	software_version	270							
Definition	2	event	timestamp	1		data	1		event	1	
Data	2	event	timestamp	904374761	s	timer_trigger	0		event	0	
Data	2	event	timestamp	904374761	s	battery_level	3.802	V	event	11	
Definition	3	unknown	unknown	1		unknown	1		unknown	1	
Data	3	unknown	unknown	904374761		unknown	12583		unknown	850	
Definition	4	device_info	timestamp	1		serial_number	1		cum_operating_time	1	
Data	4	device_info	timestamp	904374761	s	serial_number	3861884384		manufacturer	1	
Data	4	device_info	timestamp	904374761	s	manufacturer	1		garmin_product	1080	
Definition	5	unknown	unknown	1		unknown	1		unknown	1	
Data	5	unknown	unknown	904374761		unknown	1		unknown	1	
Data	5	unknown	unknown	904374772		unknown	1		unknown	1	
Data	5	unknown	unknown	904374773		unknown	1		unknown	1	
Definition	6	record	timestamp	1		position_lat	1		position_long	1	
Data	6	record	timestamp	904374775	s	position_lat	637749793	semicircles	position_long	-35499668	semicircles
Data	5	unknown	unknown	904374781		unknown	1		unknown	1	
Data	6	record	timestamp	904374781	s	distance	13.07	m	altitude	37.6	m
Data	5	unknown	unknown	904374782		unknown	1		unknown	1	
Data	6	record	timestamp	904374788	s	position_lat	637745809	semicircles	position_long	-35500976	semicircles
Data	6	record	timestamp	904374793	s	position_lat	637744053	semicircles	position_long	-35501438	semicircles
Data	6	record	timestamp	904374798	s	position_lat	637742345	semicircles	position_long	-35501843	semicircles
Data	6	record	timestamp	904374804	s	position_lat	637740261	semicircles	position_long	-35502362	semicircles

Fig. 5. A .fit file converted into a .csv for analysis in FitSDK

The serial number of the device, software version, and Garmin product number are embedded in the file which cannot be viewed in the other programs mentioned. Different formats of timestamps, longitude and latitude are used in the FitSDK. Further information such as software version and battery status are also captured. *Settings.fit* contained the user defined settings and personal user data. The serial number, product number, and software version is viewable as in the activity file. The file *running.fit* appears to have pre-set options in regards to the activity 'running' which can be defined in the Garmin Connect user dashboard. The *totals.fit* file contains the total time and distance of all the activities stored on the device and sport type. Crucially, as with the other *.fit files*, device specific evidence is linked and viewable in the file.

Type	Local Number	Message	Field 1	Value 1	Units 1	Field 2	Value 2	Units 2	Field 3	Value 3	Units 3	Field 4	Value 4	Units 4	Field 5
Definition	0	file_id	serial_number	1		time_created	1		manufacturer	1		product	1		number
Data	0	file_id	serial_number	3861884384		manufacturer	1		garmin_product	1124		type	10		
Definition	1	file_creator	software_version	1		hardware_version	1								
Data	1	file_creator	software_version	270											
Definition	2	totals	timer_time	1		distance	1		calories	1		message_index	1		sport
Data	2	totals	timer_time	1395550	s	distance	3158573	m	calories	0	kcal	message_index	0		sport

Fig. 6. totals.fit file

B. Fitbit

The Fitbit windows 10 application folder was crucial in identifying the files of interest on the Fitbit Charge HR. The main file of interest that contained all of the personal user data account activity was located in:

localDrive\Users\%UserName%\AppData\Local\Packages\Fitbit.Fitbit_6mqt6hf9g46tw\LocalState\fitbit.4TXYGG.db.

This requires hidden files/folders to be checked to show. The database file contained a total of 124 tables. In addition to the database file, the following contained more evidence:

Tag	File	Size (Bytes)	Hash
Notable Item (Notable)	Fitbit.Fitbit_6mqt6hf9g46tw/LocalState/fitbit.4TXYGG.db	1639424	711ed2555f7e1518554a54050b39d3f0
Notable Item (Notable)	Fitbit.Fitbit_6mqt6hf9g46tw/Settings/settings.dat	32768	d0cd76622fe0cd2c96be643cd269c32b
Notable Item (Notable)	Fitbit.Fitbit_6mqt6hf9g46tw/LocalState/imgs/906dc60720e6b3e0601daec84d4175c29d88d75e	10043	517a8e3d1aa1dfd2130d1e0063ae4b8f
Notable Item (Notable)	Fitbit.Fitbit_6mqt6hf9g46tw/LocalState/imgs/4c24fc8fb2315c33c059f80929a2ff664e06296e	9419	b52910d8766b63322ed6345d150d025a
Notable Item (Notable)	Fitbit.Fitbit_6mqt6hf9g46tw/LocalState/imgs/bff13b7ddcec2f99506d0d1367e2ded26d91596	102567	15fbbf3ad9cdfcc1b7c37b60d6a40239
Notable Item (Notable)	Fitbit.Fitbit_6mqt6hf9g46tw/LocalState/maptiles/16469131702-954x176.png	111947	d9db2028ae55162849374b0ade9626e

Fig. 7. Fitbit files of interest

The imgs folder did store stock images for Fitbit account and displays for headers etc. but it contained the user profile picture, friend profiles pictures and a number of pictures posted on the community group that user was a current member in. The files were extracted and examined for any Exif data or GPS data, but all images had no such information, this could be that when the user uploads an image, any personal information is stripped from the image. The *settings.dat* file contains numerous pieces of evidence that link to the user, the last user, in addition to the device and pairing connection type.

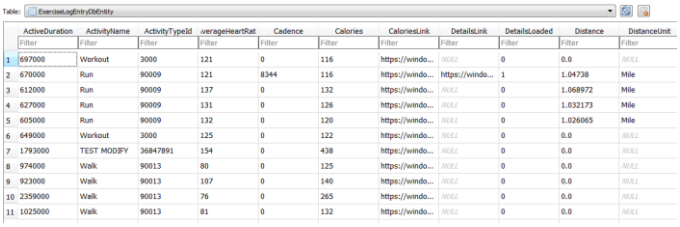
```
Fitbit.Statistics.Pairing.
ChargeHR
Dongle
```

Fig. 8. Device connection type to the account

User ID can be seen as *4TXYGG* and various types of evidence available in the settings.dat file can be associated with the user ID. The database file *fitbit.4TXYGG.db* was the main source of evidence and is extensive in its content. The database file is very much a live database, while the Fitbit application is running, any changes made instantly update in the file. Changes made elsewhere, either in the smartphone application or in the browser dashboard are not reflected in the file until the application is started in Windows 10.

fitbit.4TXYGG.db

Personal user data found in the database file has multiple table entries, they contain data such as achievements, and badges earned, device pairing, exercise logs of all activities synced to the account. In the *ExerciseLogEntryDbEntity* table, all activities are shown in the history of the user.



	ActiveDuration	ActivityName	ActivityTypeId	AverageHeartRat	Cadence	Calories	CaloriesLink	DetailsLink	DetailsLoaded	Distance	DistanceUnit
1	697000	Workout	3000	121	0	116	https://windo...	NULL	0	0.0	NULL
2	670000	Run	90009	121	8344	116	https://windo...	https://windo...	1	1.04738	Mile
3	612000	Run	90009	137	0	132	https://windo...	NULL	0	1.068972	Mile
4	627000	Run	90009	131	0	126	https://windo...	NULL	0	1.032173	Mile
5	605000	Run	90009	132	0	120	https://windo...	NULL	0	1.026065	Mile
6	649000	Workout	3000	125	0	122	https://windo...	NULL	0	0.0	NULL
7	1793000	TEST MODIFY	36847891	154	0	438	https://windo...	NULL	0	0.0	NULL
8	974000	Walk	90013	80	0	125	https://windo...	NULL	0	0.0	NULL
9	923000	Walk	90013	107	0	140	https://windo...	NULL	0	0.0	NULL
10	2359000	Walk	90013	76	0	265	https://windo...	NULL	0	0.0	NULL
11	1025000	Walk	90013	81	0	132	https://windo...	NULL	0	0.0	NULL

Fig. 9. Exercise log database table

Any GPS tracked activities show second by second coordinates of that activity. Other useful logs include: *ExerciseLogEntryDbEntity*, *FoodLogDbEntity*, *WaterLogDbEntity*, *HeartRateExerciseZoneDbEntity*, etc. All sleep details and activity patterns are present in the *SleepLogEntryDbEntity* and *SleepStatDetailDbEntity* tables and weight logs of the user is available in the *WeightLogEntryDbEntity* table. The *PostDbEntity* tables holds any information of users that have posted in a joined group. In this project a group regarding injuries was joined. A user, who posts a message, leaves a trail of information in the table such as, profile, the picture posted was located in the imgs folder contents, display name and if that person is a friend of the projects user. This comment that was made by a user and found in the database, which can be seen in the original post – shown in Figure 10.

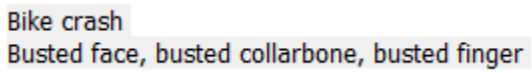


Fig. 10. Extracted user comment on the post

The post in the application shows the image posted, once again the URL can be taken from the database table "*PostMetaData*" column and copied and pasted in to internet browser for viewing without any restrictions. The retrieved evidence shows that comments, posts and images that are made into Fitbit groups can successfully extracted, thus, offering extensive insight into to the user, groups the user is a member of and any possible acquaintances.

C. HETP

The HETP only has the Smartphone application to view any activities and they cannot be viewed, modified or deleted from the device or the mobile application. The only way to delete any user data and activities is to reboot the device and deleted the application, removing the user account details simultaneously. Unlike the other two devices, the HETP seems to be more like a piece of middleware that interacts with the smartphone application, rather than a smart device.

V. Analysis of Results

An important factor in extracting data from the .fit files was using both GoldenCheetah and FitSDK together. FitSDK had device serial number, product number, software versions etc., which GoldenCheetah did not display, but in terms of visualising the data, GoldenCheetah offered a much clearer view of the activities and therefore could be an excellent tool used to describe a user's activity in a court.

The files of interest for both devices have been identified, whereas the HETP device would have evidence inside the smartphone application (which was not the focus of this experiment). Manual extraction confirmed what types of evidence could be potential available and how much fitness bands and there user accounts collect, store and transmit across various community groups inside the Garmin and Fitbit Connect platforms. During the analysis, the installation folder of Garmin and Fitbit connect were examined for any evidence, though nothing of value was found on either. Additionally, Google Chrome history and cache files were analysed – again, no significant evidence was traced. Even though there were differences found in each brand and test runs on the same device, any differences were minimal and would not affect the admissibility of the evidence. Through analysing all of the database tables and log files, our experiments proved that the Fitbit device did in fact store 31 days' worth of data. Using a combination of GoldenCheetah and the FitSDK packages was vital in viewing and interpreting the acquired evidence.

Timestamps

Timestamps can be crucial for an investigation. For the devices used in this project, timestamps can show when a device was last synced to an account or machine, and can give context to recent user activity. Timestamps were found for both the Garmin and Fitbit devices in the *totals.fit* and the *settings.dat* files. A last sync or connection time from a device to a machine could be vital in an investigation. A timestamp regarding the Fitbit was found of a last sync time in a settings file. For Garmin, a specific timestamp that had a last sync time was not found, however, a last written time was found in the totals.fit file. This was created once the last test run was completed as shown in Figure 11.

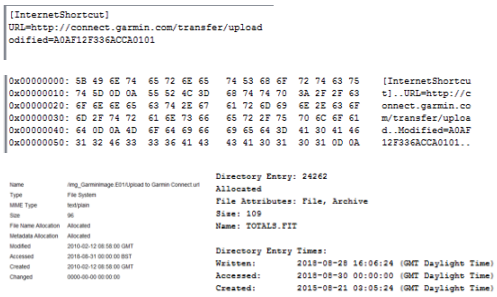


Fig. 11. Last written time of the Garmin

Third party login

As many devices now have the capability to connect to various machines, trying to sync the devices to an independent account was carried out in separate experiments. The Garmin Forerunner 110 was allowed to connect to an independent account with no security processes to stop all the user data stored on the device being transferred to another unlinked account. The Fitbit and the HETP did not transfer any device data to the new device with different log in details, with the new accounts an applications appearing blank. A forensic investigator could easily view all of the Garmin activity by connecting and synchronising the device to another account.

Accuracy comparison

The test runs were based on the subject wearing all devices at once, running one mile with a deliberate elevation change on a predetermined route. The test runs did show some inconsistencies when compared to each different brand and also when compared to each test run on the same device – as shown in tables I-III. The main observation was that the starting heart rates captured on the Fitbit and the HETP showed an 8bpm difference.

TABLE I. FITBIT TEST RUNS

Test Run	Distance	Steps	Cals	Heart rate	Pace
1	1.03 miles	1553	120	132 avg	10.05
2	1.03 miles	1572	126	131 avg	10.27
3	1.07 miles	1588	132	137 avg	10.12

TABLE II. HETP TEST RUNS

Test Run	Distance	Steps	Cals	Heart rate	Pace
1	1.05 miles	1845	84	128 avg	9.26
2	1.05 miles	1555	84	128 avg	9.43
3	1.06 miles	2005	67	87 avg	9.27

TABLE III. GARMIN TEST RUNS

Test Run	Distance	Cals	Latitude	Longitude	Pace
1	1.04 miles	152	53.455419863	-2.9756228174	9.41
2	1.06 miles	153	53.455570151	-2.9755477994	9.52
3	1.05 miles	153	53.455519692	-2.9755363162	9.37

Comparing the different brands each test run, slight differences do occur. These inaccuracies are well documented by the manufactures themselves, but these anomalies have not affected many court cases using fitness bands as evidence, and have still led to convictions.

VI. CONCLUSION AND FUTURE WORK

Fitness bands are becoming as standard as a traditional watch for many people. With this in mind, the need to address the digital forensic research on these devices was a difficult but rewarding challenge. Forensic analysis of a Garmin Forerunner 110, a Fitbit Charge HR and a Generic low-cost HETP fitness tracker was presented, and a comparison of the approaches and findings of each was conveyed. File formats that the data was stored in was challenging, as even though the files of interest were found, they were not viewable in either FTK Toolkit or Autopsy. Using a combination of GoldenCheetah and the FitSDK packages was vital in viewing and interpreting the acquired evidence. These software packages were useful when comparing the data accuracy and validly of the potential evidence.

Future work involves performing experiments on different versions of the brands used in this paper to establish if different versions of the same brand can be forensically examined by following the same process, or do they require different forensic tools and methods to achieve evidence acquisition. The development of forensic tools that can match new and emerging technology has to be a main area of concern. Many of the current tools are simply not designed to analyse new IoT devices and wearable technology due to different memory types and firmware. Digital forensic software and toolkits that can instantly recognise smart devices such as fitness trackers are key to the future of digital forensics. Imaging these devices will without doubt, offer significant evidence to forensic investigators as the complexity and functionality of the devices become greater. The more the devices can do, the percentage of evidence being generated grows at the same rate.

REFERENCES

[1] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead," IEEE Security & Privacy, vol. 15, no. 6, pp. 12-17, 2017.

[2] D. B. Lillis, Brett A.; O'Sullivan, Tadhg; Scanlon., "Current Challenges and Future Research Areas for Digital Forensic Investigation," presented at the 11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, Florida, USA, 24-26, May 24, 2016. Available: http://conference.adfsl.org/

[3] R. Ferreira. (2017). "Wearable Technology: What are you wearing and what is it saying about you?", One Source Discovery, Available: https://www.onesourcediscovery.com/wearable-technology-wearing-saying/

[4] M. Shirer. (2018). "Wearable Device Shipments Slow in Q1 2018 as Consumers Shift from Basic Wearables to Smarter Devices, According to IDC." IDC Available: https://www.idc.com/getdoc.jsp?containerId=prUS43900918

[5] W. Kruse, "Your Employee May Be Wearing Their Alibi - Or Your Evidence," Altep2015, Available: https://smarterforensics.com/wp-content/uploads/2014/06/ALT-Art-Wearables_Kruse.pdf, Accessed on: August 2 2018.

[6] K. Pickles. (2015). Police claim woman lied about being raped after her 'Fitbit' fitness watch showed she had not been dragged from her bed. Available: http://www.dailymail.co.uk/news/article-3134701/Police-claim-woman-lied-raped-Fitbit-fitness-watch-showed-not-dragged-bed.html

[7] P. Olson. (2014). Fitbit Data Now Being Used In The Courtroom. Available: https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#4376703e7379

[8] F. Carolina. (2014). Police: SC motorcyclist fled from officers, posted GoPro video on YouTube. Available: http://www.foxcarolina.com/story/25645528/police-man-fl

[9] S. Watson and A. Dehghantanha, "Digital forensics: the missing piece of the Internet of Things promise," Computer Fraud & Security, vol. 2016, no. 6, pp. 5-8, 2016/06/01/ 2016.

[10] S. B. Rick Ayers, Wayne Jansen "Guidelines on Mobile Device Forensics," in "NIST Special Publication 800-101 Revision 1," National Institute of Standards and Technology 2014, Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf,

[11] R. J and Z. Geradts, "Extraction and Forensic Analysis of Artifacts on Wearables," International Journal of Forensic Science & Pathology (IJFP), pp. 312-318, 2017.

[12] I. Baggili, J. Oduro, K. Anthony, F. Breitinger, and G. McGee, "Watch What You Wear: Preliminary Forensic Analysis of Smart Watches," in 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 303-311.

[13] D. C. Shreyas Parikh, Shourjo Chakraborty, Dr. Parag H. Rughani, Dr. M. S. Dahiya, "Analysis of Android Smart Watch Artifacts," International Journal of Scientific & Engineering Research, vol. 6, no. 8, 2015.

[14] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N.A. Le-Khac," Internet of things forensics: Challenges and Case Study." IFIP International Conference on Digital Forensics (pp. 35-48). Springer, Cham. 2018.

[15] A. MacDermott, T. Baker, and Q. Shi, "IoT forensics: Challenges for the IoA era." In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.