Forensic Analysis of Fitbit Versa: Android vs iOS

Joseph Williams[1], Áine MacDermott[2], Kellyann Stamp[2], Farkhund Iqbal[3]
[1]*Merseyside Police's Digital Forensics Unit,*
[2]*School of Computer Science and Mathematics, Liverpool John Moores University,*
Liverpool, UK
[3]*College of Technological Innovation, Zayed University, United Arab Emirates*
joewilliams96@outlook.com {a.m.macdermott; k.a.stamp}@ljmu.ac.uk; farkhund.iqbal@zu.ac.ae

***Abstract*—Fitbit Versa is the most popular of its predecessors and successors in the Fitbit faction. Increasingly data stored on these smart fitness devices, their linked applications and cloud datacenters are being used for criminal convictions. There is limited research for investigators on wearable devices and specifically exploring evidence identification and methods of extraction. In this paper we present our analysis of Fitbit Versa using Cellebrite UFED and MSAB XRY. We present a clear scope for investigation and data significance based on the findings from our experiments. The data recovery will include logical and physical extractions using devices running Android 9 and iOS 12, comparing between Cellebrite and XRY capabilities. This paper discusses databases and datatypes that can be recovered using different extraction and analysis techniques, providing a robust outlook of data availability. We also discuss the accuracy of recorded data compared to planned test instances, verifying the accuracy of individual data types. The verifiable accuracy of some datatypes could prove useful if such data was required during the evidentiary processes of a forensic investigation.**

Keywords—Cellebrite, Cloud forensics, Digital forensics, Fitbit, Fitbit forensics, Forensic analysis.

I. Introduction

Digital forensics is becoming more challenging due to the tremendous increase in computing devices and computer-enabled paradigm, providing new challenges to the distributed processing of digital data and adding to the investigative complexity. With the new types of devices that are part of the Internet of Things (IoT) paradigm, we must determine the best approach for ensuring they are examined in the same forensically sound manner. Wearable devices and technology fall under this IoT category. Wearable technology is usually marketed towards its health and exercise benefits; however, if criminal activities have taken place while wearing these devices, the data stored within them could prove crucial to investigations. Data stored on wearable devices provides a general overview of where an individual has been, the speed they were travelling at and their heart rate at the time.

Data on smart watches has been considered by the court of law in the past, and this is proving to be more and more common in recent years. There have been several cases in the court of law where data retrieved from a Fitbit device has been used as evidence in criminal investigations. Fitbit data has been used by US police investigating whether a 90-year-old murdered his stepdaughter [2]. The victim was suspected of taking her own life and the accused denied being present when her death happened. A significant spike in heart rate, GPS data and CCTV tied the suspect to the crime. In a separate case, a murder victim's Fitbit data was used to prove that her husband had committed the crime. The Fitbit timeline proved movement within the house and distance travelled, placing him at the crime scene [3]. There has been an immense increase in the number of wearable devices submitted to Digital Forensic Units for analysis. These devices are increasingly collecting a wealth of personal data and have the potential to contain vital, incriminating evidence. With the rapid increase in use of these devices and the lack of standardization, there needs to be further scrutiny and analysis of the capabilities of these devices and the reliability of the data within.

Our main contributions can be summarized as follows:

- Recover the data Fitbit stores about their users, as well as data which is created by users; this will occur via performing several extraction techniques, which will aim to analyse the parent application linked to the Fitbit Versa smart watch in extensive detail.
- Compare the findings between XRY and Cellebrite extractions. Present comparisons between the data that is retrieved from Fitbit using different methods of extraction.
- Improving the current literature regarding what forensically relevant artefacts are produced and where they are located on iOS and Android.

To the best of the authors' knowledge, forensic analysis of Fitbit Versa has not been investigated, nor has there been detailed analysis and explanation of the Cellebrite UFED features in comparison to MSAB XRY for investigations. This paper is structured as follows: In Section II we present related work in this field to convey the current views. In Section III we detail our methodology and present findings from our experiments. In Section IV we conclude.

II. Related Work

In [4], the authors analyse artefacts from the Fitbit desktop application in a Windows 10 environment and discuss the implications investigators may face when analysing Fitbits. Interestingly, the 'community' section of Fitbit's application interface provided the majority of data. Recoverable data included the users profile picture, public posts, sleep data and some data related to the users 'friends' on Fitbit. Account information varied depending on the progress posted and the security settings, e.g. if the account was set to public or private. Any exercises performed on the test account were also logged which showed the activity name e.g. 'run', the number of calories burned and the speed the user was tracked at whilst performing the activity. The duration of the exercise is logged as well as the distance covered. Another artefact of importance is the date and time of exercise, as this can aid criminal cases when putting the culprit in a specific location at a specific time.

In [5], a Fitbit account has been populated with a simulated 'mock murder scenario' in order to display how data could provide timeline evidence to a real-world investigation. The extractions taken are analysed and presented in a way in which a forensic investigator could gain an understanding of what has happened. For example, a sudden increase or decrease in the number of steps taken, when combined with heart rate data

stored on the device could indicate an attack taking place and provide investigators with a dataset which could be used to produce timeline evidence. it is interesting to see what data can be recovered from this form of extraction and how the data can provide investigators with a timeline of events which may correlate with the timeline of the suspected crime that has taken place. This research project is still feasible to investigators dealing with a case in which they need to provide evidence that a certain person was in a certain place, at a certain time, suspected of doing a certain thing. The step count, heart rate monitor and sleep data can help investigators solve an investigation from the perspective of both the victim and the offender.

The work of [6] presents a comparison of artefacts recovered from a Fitbit Charge HR, Garmin Forerunner 110 and a HETP Fitness Tracker. The experiments taken place in this project occur in a forensically sound manner, which is useful when relating to a real-world scenario. Regardless of frequent or infrequent use, these fitness bands may store vital data for forensic investigators. Also discussed is whether the data acquired could be useful and admissible, how accurate the evidence generated is and the potential of data contamination in the form of anti-forensic techniques. The 'ExerciseLogEntryDbEntity' and 'SourceName' tables of these databases identified activities have been captured, which enables the user to see what physical Fitbit device was used and what linked device was used alongside it. The same database included a table showing any GPS tracked activities. These activities showed second by second coordinates of an activity taking place which would help greatly in real-world investigations, corroborating witness and CCTV evidence with Fitbit data. With newer Fitbit devices, manual extractions are not possible. Therefore, we will attempt to retrieve data using several extraction methods. We will compare the data acquired from both iOS and Android devices using logical and physical extraction methods across many forensic tools and use proprietary tools Cellebrite and XRY on both Android and iOS devices.

III. Methodology

This study aims to provide investigators with timely information to utilize in future investigations where health data is recovered across a range of devices and forensic techniques. Apple devices in general are the most popular devices in the UK, and the iPhone 7 series is the most sought-after iOS device on the market. The Google Pixel range are deemed "*the best Android phone and the most affordable*" in 2021 [7].

TABLE II. Device Details

Device	Operating System	Fitbit Application
iPhone 7Plus	iOS 13.3	Version 3.8 (882)
Google Pixel 2XL	Android 10	Version 3.17 (20243485)

We will be analyzing the Fitbit Versa looking for private messages, feed posts, profile information, GPS data, sleep data and heart rate data – the type of data that is collected by the Fitbit Versa. For the experiments, a Fitbit test account called 'FitbitForensics' was created and worn by the participating user over a period of three months: from 13/12/19 to 21/03/20. The test account was populated with data we believe may be of interest to investigators in real-world scenarios to see if these artefacts could be recovered using forensic tools. Personal information such as height, weight, profile picture and food plans were added. Apps were downloaded onto the device and posts made on the public dashboard. Messages were exchanged within the app and the profile adjusted from public to private to see if certain posts were visible. Also, whilst this test account was used, various exercises were automatically tracked by the physical Fitbit Versa device.

A. Logical extraction of an iOS device using Cellebrite

The first extraction was completed using UFED by Cellebrite. Figure 1 shows this extraction and reveals one of the main areas of interest to forensic investigators when analysing Fitbit data. With Cellebrite, this data is taken from its raw format and put into a Fitbit folder, within the activities tab. However, as would be suspected, this folder only contains the user's activity data and no other information that has been used as test data such as private messages, community groups, sleep data etc.

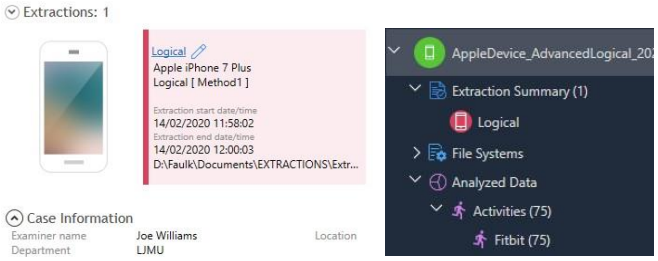


Fig. 1. Extraction information and directory of interest

The Fitbit activities directory shows both data that originates from the device itself, and the synced device (i.e. mobile phone). Although this Fitbit information is in a different folder than other Fitbit data on Cellebrite, it derives from the same database location. All the Fitbit data analyzed from this extraction derives from the same *'fitbit.sqlite'* database which contains 193 tables.

The file path for the Fitbit SQLite file located on the iPhone 7 Plus is:

iPhone/mobile/Containers/Data/Application/com.fitbit.FitbitMobile/Documents/fitbit.sqlite

To analyze these results, we exported the fitbit.sqlite file from Cellebrite and analyzed the contents using DB Browser. The 'ZCONVERSATION' table in the fitbit.sqlite database shows messages that have been sent and later deleted by the user. Several columns of interest can be seen in Figure 2. In 'ZUNREADMESSAGES' a number 0 will be displayed if the message has been opened.

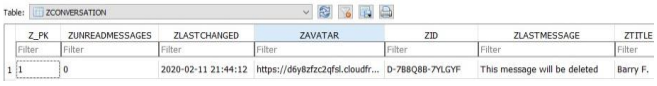


Fig. 2. Deleted messages

In instances where the message has not been opened by the user, 1 will be displayed here. 'ZLASTCHANGED' provides date and time information relating to when the message was deleted. In this instance, the date and time information are 11/02/20 at 21:44:12, which corroborates with the actual time the message was deleted, which was recorded for testing purposes at 11/02/20 at 21:44 as can be evidenced in the experimental data. Column 'ZAVATAR' shows a link that

redirects users to a cloud content delivery network, which provides a globally-distributed network of proxy servers which cache content – in Fitbit's case, account display pictures. 'ZID' displays the Fitbit account ID of the recipient and 'ZLASTMESSAGE' shows the message that was sent to the receiver. A further table of interest is 'ZCONVERSATIONMESSAGE' shown in Figure 3. 'ZTIME' displays the time and date a message was sent. 'ZCONTENT', shows the content in the message sent or received.

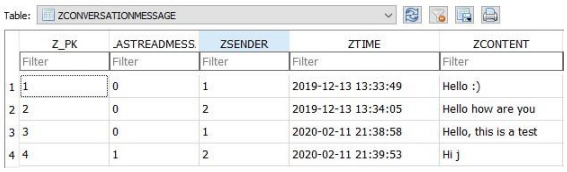


Table: ZCONVERSATIONMESSAGE

	Z_PK	ZASTREADMESS	ZSENDER	ZTIME	ZCONTENT
	Filter	Filter	Filter	Filter	Filter
1	1	0	1	2019-12-13 13:33:49	Hello :)
2	2	0	2	2019-12-13 13:34:05	Hello how are you
3	3	0	1	2020-02-11 21:38:58	Hello, this is a test
4	4	1	2	2020-02-11 21:39:53	Hi j

Fig. 3. Direct messages

With the 'ZCONVERSATION' table forensic investigators can see whether a message has been opened and who the sender of the message was by following the 'ZLASTREADMESSAGE' and 'ZSENDER' columns retrospectively. In table 'ZCOVERPHOTO' the user's cover picture from their profile can be recovered. As well as identifying potential evidential images stored on a user's profile, this table helps locate the user's unique identifier. In the 'ZENCODEDUSERID' column, the text *'7YLGYF'* is displayed. This is also shown in the 'ZID' column of the 'ZCONVERSATION' discussed previously; this helps verify that the owner of the account holds the unique identifier *'7YLGYF'* (shown previously in Figure 2).

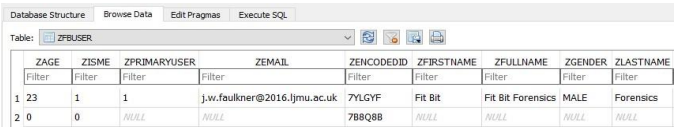
Significant data regarding the user of the Fitbit account being analyzed can be retrieved from the 'ZFBUSER' table within the fitbit.sqlite database. This table contains personal information about both the user and anyone they have added as a friend on their Fitbit account.

Table: ZFBUSER

	ZAVGSTEPS	ZHEIGHT	ZWEIGHT	ZABOUTME	ZAVATAR	ZCOUNTRY	ZDISPLAYNAME
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	4023.0	175.199996948242	63.503	This is a test	https://d6y8zf...	GB	Fit Bit F.
2	-1.0	0.0	0.0	NULL	https://d6y8zf...	NULL	Barry F.

Fig. 4. ZFBUSER table displaying personal details of test user and friends

'ZAVGSTEPS' displays the number of steps the user takes on average from their recorded data. However, this data is not entirely reliable as most users do not wear their watch consistently enough for this number to be an average of their daily steps taken. 'ZHEIGHT' displays the height the user has manually entered into the Fitbit application, in centimeters. The 'ZWEIGHT' column shows the weight the user has entered, in kilograms. In instances where a profile is not set to public, these will show '0' as can be evidenced by profile 2. The first profile shows the data recovered from a public profile, where user 2 has privacy restrictions enabled. The 'ZABOUTME' column shows the text a user has entered into their 'About Me' section on the Fitbit application. The 'ZAVATAR' column, shows the user's display picture. Next follows the 'ZCOUNTRY' column, showing the country the user has entered when signing up to Fitbit. Similarly, the 'ZDISPLAYNAME' column displays the forename and the first letter of the surname the user has entered into Fitbit when signing up. In this case – Fit Bit F. (Fit Bit Forensics).



Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ZFBUSER

	ZAGE	ZISME	ZPRIMARYUSER	ZEMAIL	ZENCODEDID	ZFIRSTNAME	ZFULLNAME	ZGENDER	ZLASTNAME
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	23	1	1	j.w.faulkner@2016.ljmu.ac.uk	7YLGYF	Fit Bit	Fit Bit Forensics	MALE	Forensics
2	0	0	NULL	NULL	7B8Q8B	NULL	NULL	NULL	NULL

Fig. 5. ZFBUSER table containing personal data for the test account

Figure 5 shows continued columns of the 'ZFBUSER' table. Here, 'ZAGE' displays the age entered by the user upon sign up. 'ZISME' confirms which account listed is the primary, user account (FitbitForensics). The next column, 'ZEMAIL' displays the email address that the user utilizes to sign into the Fitbit application.

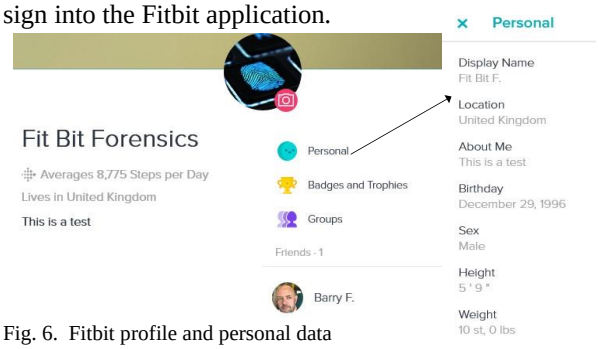


Fig. 6. Fitbit profile and personal data

The information presented in Figure 6 verify the data carried across to the Fitbit database file. The average steps do not match as this is continuously updated and should not be relied upon to outline abnormalities in the average numbers of steps taken by an individual.

The 'ZDEVICEINFORMATION' table (shown in Figure 7) provides an overview of the physical device that is signed into the Fitbit account. The 'ZDEVICEMANUFACTURER' column gives information regarding the manufacturer of the device. The device used for testing was an iPhone 7 Plus. The 'ZDEVICEMODEL' shows 'iPhone9,4' this is simply the device ID.

Table: ZDEVICEINFORMATION

	ZDEVICEMANUFACTU	ZDEVICEMODEL	ZDEVICENAME	ZOSNAME	ZOSVERSION
	Filter	Filter	Filter	Filter	Filter
1	Apple	iPhone9,4	iPhone	iOS	12.0
2	Apple	iPhone9,4	iPhone	iOS	13.3.1

Fig. 7. Device information

Having analyzed the messages, account details, device details and associated accounts; we will now continue to uncover the experimental test data by analysing the activities performed by the user. Some important data regarding user activities were in the 'ZFBACTIVITYLOG' table displayed in Figure 8. 'ZACTIVEMINUTES' shows the number of minutes the user has been active for during the activity taken place. This can then be brought together with the subsequent columns. 'ZAVERAGEHEARTRATE' displays what the users average heart rate was during this activity – this combined with the average minutes can help figure out what activity was taking place.

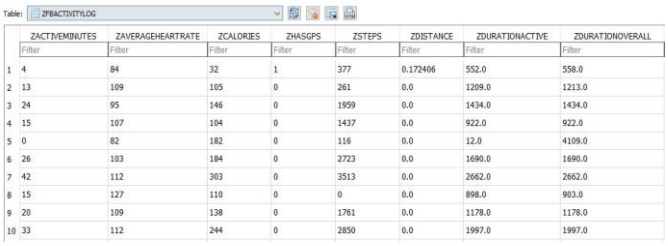


Table: ZFBACTIVITYLOG

	ZACTIVEMINUTES	ZAVERAGEHEARTRATE	ZCALORIES	ZHASGPS	ZSTEPS	ZDISTANCE	ZDURATIONACTIVE	ZDURATIONOVERALL
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	4	84	32	1	377	0.172406	552.0	558.0
2	13	109	105	0	261	0.0	1209.0	1213.0
3	24	95	146	0	1959	0.0	1434.0	1434.0
4	15	107	104	0	1437	0.0	922.0	922.0
5	0	82	182	0	116	0.0	12.0	4109.0
6	26	103	184	0	2723	0.0	1690.0	1690.0
7	42	112	303	0	3513	0.0	2662.0	2662.0
8	15	127	110	0	0	0.0	898.0	903.0
9	20	109	138	0	1761	0.0	1178.0	1178.0
10	33	112	244	0	2850	0.0	1997.0	1997.0

Fig. 8. Fitbit activity log

Although Fitbit attempts to predict what activity is taking place, this is not always accurate as numerous biking activities were recorded on this account, which had not taken place. 'ZCALORIES' provides an estimation of how many calories were burned during the activity. The 'ZHASGPS' column proves to be of great interest for forensic investigations. Where GPS has been utilized, a 1 will be displayed in this column and where GPS was not used, a 0 is displayed. The first column has GPS where the others do not. 'ZSTEPS' and 'ZDISTANCE' display the number of individual steps. Where GPS has been utilized, the distance covered will be displayed. 'ZDURATIONACTIVE' and 'ZDURATIONOVERALL' depict the overall duration of an activity and the amount of time an individual was active, measured in seconds. Figure 9 continues the ZFBACTIVITYLOG table. Here, the ZLASTMODIFIED column shows when the activity was uploaded to the Fitbit application, not when the activity took place. Again, where GPS is utilized the column 'ZSPEED' gains significance as the speed the user was travelling during the activity can be tracked by the Fitbit device.

Table: ZFBACTIVITYLOG

	ZLASTMODIFIED	ZSPEED	ZNAME	ZSOURCETYPE
	Filter	Filter	Filter	Filter
1	2019-12-20 10:35:22	1.1364586956...	Run	tracker
2	2019-12-28 09:33:00	0.0	Workout	tracker
3	2020-01-09 13:13:09	0.0	Walk	NULL
4	2020-01-02 14:58:03	0.0	Walk	NULL
5	2020-01-28 21:22:57	0.0	Fitstar: Personal Trainer	tracker
6	2020-01-28 17:12:55	0.0	Walk	NULL
7	2020-01-07 14:57:15	0.0	Walk	NULL
8	2020-02-10 07:42:35	0.0	Bike	tracker
9	2020-01-24 12:48:25	0.0	Walk	NULL
10	2019-12-20 15:40:43	0.0	Walk	NULL

Fig. 9. Fitbit activity log continued

The 'ZNAME' section displays the workout that either the user has manually started, or the device has automatically predicted, using the Fitbit Versa's smart tracking feature. All the activities listed here are accurate, apart from the bike activities, which the Fitbit Versa has automatically recorded but did not take place. 'ZSOURCETYPE' shows the source device that recorded the activity. This information derives from tables 'ZFBACTIVITYLOG' and 'ZFBLOCATION' – which evidence the activity taking place and the location of the activity.

Start Time	End time	From point	To point
20/12/2019 10:25:51(UTC+0)	20/12/2019 10:35:09(UTC+0)	(53.436104, -2.986155, 260.1...	(53.413335, -2.981382, 220.7...

Fig. 10. Fitbit activity details and GPS data

Name	Source	Account	Source file information
Run	Fitbit		fitbit.sqlite : 0x1D9ECC

Fig. 11. Fitbit tracked run activity

Figure 10 and Figure 11 taken from Cellebrite outline information regarding the tracked activity containing GPS data. The start time of this instance according to Cellebrite is 20/12/19 at 10:25:51 and ends at 20/12/19 at 10:35:09. This date and time pulled from the 'ZFBLOCATION' table in the fitbit.sqlite database matches the start time and end time listed in the experimental testing section, validating accuracy. Figure 12 contains data regarding the date and time of the activity, what activity had taken place, where evidence of this is stored on the iPhone and the longitude and latitude details.

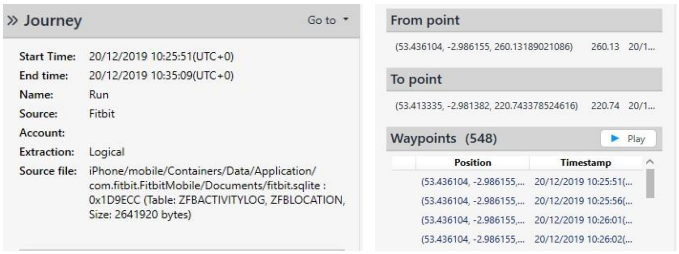


Fig. 12. Journey information and waypoints

There are 548 waypoints in this 10-minute journey – thus meaning that analysis of those waypoints using a DB browser, would take an extremely long time, analysing each waypoint individually. With Cellebrite, their forensic tool offers a mapping technique, which compiles these GPS results and produces a Google Map's like feature. Cellebrite's online maps is shown in Figure 13, which gives the user an easier overview of where the individual may have been, based on GPS data stored on the Fitbit Versa. This provides a home symbol indicating where the activity started and a finish line symbol to display where the activity ended.

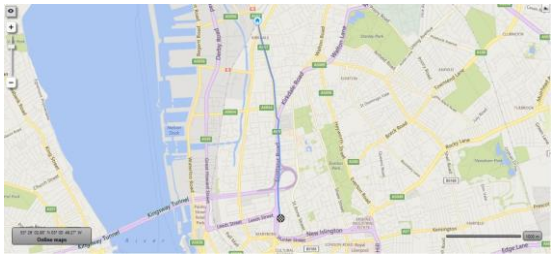


Fig. 13. Cellebrite maps

'ZBATTERYPERCENTAGE' displays the battery percentage on the watch at the time when the extraction of the mobile device was performed. Though, this percentage is based from when the physical Fitbit device was last synced with the mobile application.

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ZFBDEVICE

	ZBATTERYPERCENTAGE	ZISSLEEPENABLED	ZONDOMINANTHAND	ZBTMACADDRESS	ZDEVICEID
	Filter	Filter	Filter	Filter	Filter
1	98	1	0	F67784FE5DF0	1064838705

Fig. 14. ZFBDEVICE table displaying Device ID and MAC address

'ZISSLEEPENABLED' provides an indication as to whether the user has sleep recording enabled. If the user does track their sleep using the watch a number 1 will appear, if they have this feature disabled, 0 will appear. Another interesting column is the 'ZONDOMINANTHAND' – this tells us on what wrist the user is wearing the physical device. This information is likely to be determined by the smart track feature previously discussed, calculating and tracking user movements. Details on the MAC address of the Fitbit device and the device ID for the physical Fitbit Versa linked to the Fitbit application are available also.

Table: ZFBDEVICE

	ZFIRMWAREAPPCURRENT	ZFIRMWAREAPPLATEST	ZFIRMWAREBSLCURRENT	ZFIRMWAREBSLLATEST
	Filter	Filter	Filter	Filter
1	32.70.7.14	32.70.7.14	32.1.12	32.1.12

Fig. 15. ZFBDEVICE firmware details

In Figure 15, the 'ZFBDEVICE' table details the current version of firmware running for the Fitbit mobile application, the next column displays the latest firmware update – in this

case, the Fitbit application is running the latest firmware. In Figure 16, 'ZPRODUCTEDITION' shows which edition of the Fitbit Versa the user is using, in this case – it is the Fitbit Versa with NFC enabled. Although NFC is not utilized for the purpose of this paper, this could be interesting to investigators. 'ZPRODUCTNAME' simply provides detail of the Fitbit device linked to the mobile application where 'ZTYPE' displays what type of device this is. The 'ZWIREID' gives the identification number for the Fitbit charger.

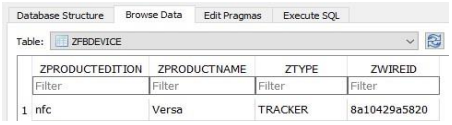

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ZFBDEVICE

	ZPRODUCTEDITION	ZPRODUCTNAME	ZTYPE	ZWIREID
	Filter	Filter	Filter	Filter
1	nfc	Versa	TRACKER	8a10429a5820

Fig. 16. ZFBDEVICE continued

Numerous details on food and water intakes and usage are available. In figure 18 we can see the types of data that can be tracked by the user. The 'ZLOCALCREATIONDATE' matches with the time this was entered for testing purposes, meaning the results from the database can be verified.


Table: ZFBFOOD

	ZFOODID	ZACCESSLEVEL	FAULTSERVINGU	ZNAME
	Filter	Filter	Filter	Filter
1	692076049	PUBLIC	toast	Toast
2	742319428	PUBLIC	slice	Chicago Thin Pepperoni Pizza, XL
3	69819	PUBLIC	serving	Snickers (full size bar)
4	82776	PUBLIC	oz	Potato Chips
5	80969	PUBLIC	serving	Ham & Cheese Sandwich
6	17222	PUBLIC	gram	Coffee
7	82932	PUBLIC	oz	Hash Browns

Fig. 17. Logged food information

The 'ZPOST' table evidences instances where the user has posted something to either the Fitbit dashboard or to a community group. The 'ZCHEERCOUNT' column shows the number of other users that have 'cheered' the post. Unfortunately, the Fitbit ID or username of the person 'cheering' the post is not displayed. 'ZCOMMENTCOUNT' shows how many comments there are on the post where 'ZGROUP' provides a '1' if the post was sent into a community group rather than the Fitbit dashboard. 'ZIMAGEURL' shows the image that the user posted to their feed. Figure 18 shows the images that were posted to the Fitbit feed via the mobile application. Post 1 was posted to the Fitbit dashboard when the helicopter badge was earned. Post 2 was posted in a community group, which was evidenced by the 'ZGROUP' column. The third post is slightly different, this post contains an image from the user's mobile device, uploaded to Fitbit.

Fig. 18. Post 1, Post 2, and Post 3

The details provided on user sleep and location are important to note. The 'ZSLEEPCONSISTENCY' table (figure 19) shows the consistency levels of the user's sleep data, and 'ZSLEEPLOG' shows sleep data. We can see the efficiency level of the sleep; this can help gain a further insight into what instance of sleep may be considered abnormal for the user.


Table: ZSLEEPCONSISTENCY

	ZRECOMMENDEDDURATION	ZTYPICALDURATION	ZAWAKERESTLESSPERCENTAGE	ZTYPICALWAKEUPTIME
	Filter	Filter	Filter	Filter
1	495	471	0.0526694942737962	2001-01-01 07:07:00

Fig. 19. Sleep consistency

The 'ZLEVELDATA' is much more detailed and provides an overview of the date and time the sleep occurred as well as every instance where the user had woken up and for how long. This section also displays how long the user was active in light, deep and REM sleeping instances. This column also includes the number of seconds the user was restless for and at what time waking occurred throughout.

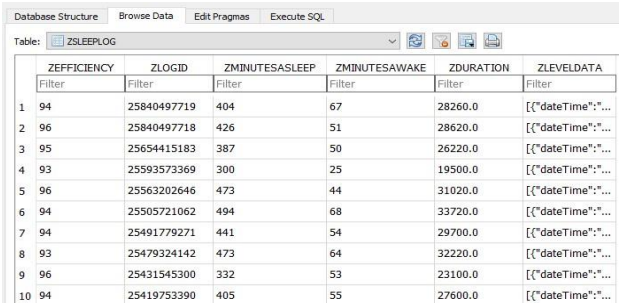
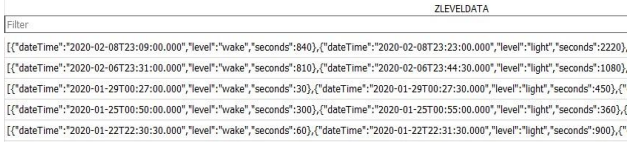

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ZSLEEPLOG

	ZEFFICIENCY	ZLOGID	ZMINUTESASLEEP	ZMINUTESAWAKE	ZDURATION	ZLEVELDATA
	Filter	Filter	Filter	Filter	Filter	Filter
1	94	25840497719	404	67	28260.0	[{"dateTime":"...
2	96	25840497718	426	51	28620.0	[{"dateTime":"...
3	95	25654415183	387	50	26220.0	[{"dateTime":"...
4	93	25593573369	300	25	19500.0	[{"dateTime":"...
5	96	25563202646	473	44	31020.0	[{"dateTime":"...
6	94	25505721062	494	68	33720.0	[{"dateTime":"...
7	94	25491779271	441	54	29700.0	[{"dateTime":"...
8	93	25479324142	473	64	32220.0	[{"dateTime":"...
9	96	25431545300	332	53	23100.0	[{"dateTime":"...
10	94	25419753390	405	55	27600.0	[{"dateTime":"...

Fig. 20. Sleep log


ZLEVELDATA

Filter

[{"dateTime":"2020-02-08T23:09:00.000","level":"wake","seconds":840},{"dateTime":"2020-02-08T23:23:00.000","level":"light","seconds":2220},
[{"dateTime":"2020-02-06T23:31:00.000","level":"wake","seconds":810},{"dateTime":"2020-02-06T23:44:30.000","level":"light","seconds":1080},
[{"dateTime":"2020-01-29T00:27:00.000","level":"wake","seconds":30},{"dateTime":"2020-01-29T00:27:30.000","level":"light","seconds":450},{"
[{"dateTime":"2020-01-25T00:50:00.000","level":"wake","seconds":300},{"dateTime":"2020-01-25T00:55:00.000","level":"light","seconds":360},{
[{"dateTime":"2020-01-22T22:30:30.000","level":"wake","seconds":60},{"dateTime":"2020-01-22T22:31:30.000","level":"light","seconds":900},{"

Fig. 21. Sleep data

Figure 21 shows a small section of what is contained within the 'ZLEVELDATA' column. This data can become extremely confusing to analysts if they are not aware of what the information means. We will provide further captures, detailing what each section of the 'ZLEVELDATA' column information entails.

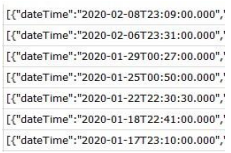

[{"dateTime":"2020-02-08T23:09:00.000","
[{"dateTime":"2020-02-06T23:31:00.000","
[{"dateTime":"2020-01-29T00:27:00.000","
[{"dateTime":"2020-01-25T00:50:00.000","
[{"dateTime":"2020-01-22T22:30:30.000","
[{"dateTime":"2020-01-18T22:41:00.000","
[{"dateTime":"2020-01-17T23:10:00.000","

Fig. 22. Fallen asleep


"level":"wake","seconds":840},{"dateTime":"2020-02-08T23:23:00.000","
"level":"wake","seconds":810},{"dateTime":"2020-02-06T23:44:30.000","
"level":"wake","seconds":30},{"dateTime":"2020-01-29T00:27:30.000","l
"level":"wake","seconds":300},{"dateTime":"2020-01-25T00:55:00.000","
"level":"wake","seconds":60},{"dateTime":"2020-01-22T22:31:30.000","l

Fig. 23. Awoken

Figure 22 shows the time the user fell asleep. The user was recorded by the Fitbit Versa to have fallen asleep on 08/02/2020 at 23:09:00. Figure 23, details when the first instance of broken sleep occurs. To follow the example of the first line, the user wakes up for 840 seconds and then falls back to sleep at 08/02/2020 at 23:23:00. If investigators have pinpointed a specific date and time they are interested in; this data then becomes extremely important in proving innocence or guilt of a suspect.

B. Logical extraction of an iOS device using XRY

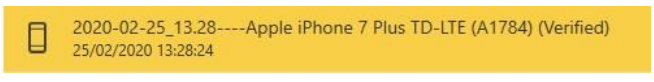

2020-02-25_13.28----Apple iPhone 7 Plus TD-LTE (A1784) (Verified)
25/02/2020 13:28:24

Fig. 24. Extraction information

A logical extraction performed on an iPhone 7 Plus on 25/02/2020 at 13:28:24 using MSAB XRY. When presented

with the results from analysis we used the keyword “Fitbit” to locate existing data stored on the device. This returned 51 artefacts (the majority of which is health data). Although this keyword search helped locate specific data related to Fitbit artefacts, the fitbit.sqlite database was not found here. As a result, this keyword was removed, and further analysis of the directory provided by XRY was completed. This is where all of the Fitbit data is stored.

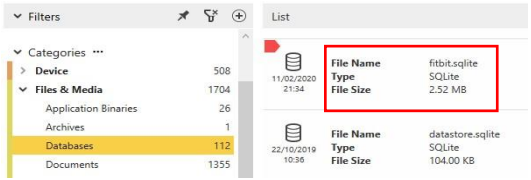


Fig. 25. Fitbit database

Before we move on to analysis of the fitbit.sqlite database we will provide some insight into how the Fitbit data is presented using XRY. The information is exported from the database and shown in a user-friendly format. Figure 26 displays the list of activity artefacts stored by XRY.

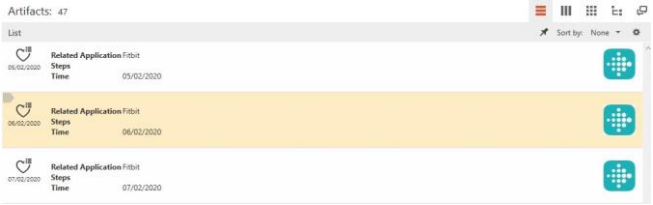


Fig. 26. XRY Fitbit artefacts

XRY provides a list of the daily steps taken by the user and analyses those steps further by producing a graph which shows how many steps were taken each hour. The capture displays the number of steps taken on 22/12/2019 and more specifically, how many of those steps were completed in each hour.

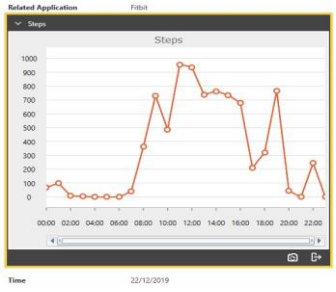


Fig. 27. XRY Fitbit artefacts

Fig. 28. Fitbit accounts

Figure 28 provides information regarding the accounts stored on the Fitbit application, these include the user account and any friends added. The Security/Accounts artefacts contain information such as email addresses, usernames, profile picture’s, date of birth, user identification numbers, country of residence, height, weight, age, and gender. Further Fitbit artefacts, relating to the physical Fitbit device linked to the smartphone.

Fig. 29. Device type

The unique ID of the device (shown in figure 29), as well as the device model are found. Figure 30 details further information about the fitbit.sqlite file. Here we can see the size of the file as well as its file path. Other data recovered include the created, modified and status changed time of the file as well as the SHA1 hash value of the file.

Fig. 30. Fitbit database

The Fitbit database file is located on the mobile device at the following path:

iPhone/mobile/Containers/Data/Application/com.fitbit.FitbitMobile/Documents/fitbit.sqlite

This fitbit.sqlite database file contains 193 tables and after analysis this file contains the exact same data as the fitbit.sqlite database file mentioned in the Fitbit analysis on the iPhone using Cellebrite. This can be evidenced by both MD5 and SHA1 hash values of the fitbit.sqlite file, which match those from Cellebrite. After analysing the Fitbit artefacts recovered by XRY we obtained the exact same results as those recovered from the Cellebrite analysis of the Fitbit artefacts, from the iOS device. Recovery of the Fitbit artefacts stored on the iPhone do not differ across forensic tools Cellebrite UFED and MSAB XRY and therefore, database analysis of the fitbit.sqlite file is not required for this section. These tools provide different formats in how they present the data, but the data itself all stems from the same location.

C. Logical extraction of an Android device using XRY and Cellebrite

- Device: Google Pixel
- Operating System: Android 10
- Account: FitbitForensics

The Google Pixel is supported by Cellebrite via an advanced logical extraction, file system extraction and a physical extraction when the device is rooted. The Pixel is also supported by XRY via a partial logical extraction. Unfortunately, the Fitbit application is not supported by logical extraction on Android devices on Cellebrite or XRY. The data required to access the Fitbit information on this device, is stored in a protected data folder and therefore, this data would only be retrievable using this device if a full physical extraction was performed. Therefore, Genymotion was used to emulate an Android device and gain a physical extraction rather than rooting the device.

D. Physical extraction of an Android device using Genymotion

The emulated device provided by Genymotion offers the same functions and features as the physical Google Pixel device and was used in order to retrieve the Fitbit data stored in the protected data folder. We signed into the *FitbitForensics* test account and made a copy of the physical image of the phone.

Fig. 31. Genymotion

Next we exported *com.fitbit.FitbitMobile* from the copy of the physical Android image.

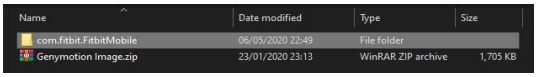


Fig. 32. com.fitbit.FitbitMobile

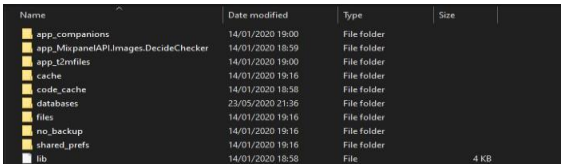


Fig. 33. Fitbit application data

Figure 33 displays the Fitbit application folder retrieved from the physical image of the emulated Android device. As was evidenced with the analysis of the iOS device, vast amounts of significant Fitbit artefacts are stored within database files. This extraction contains information from other areas such as the folder 'shared_prefs'. This folder, as well as the databases folder, contains interesting data. The /shared_prefs folder contains various XML documents that show permissions and preferences of tracker activity enabled by the user, on both the physical smart watch and its Fitbit application counterpart.

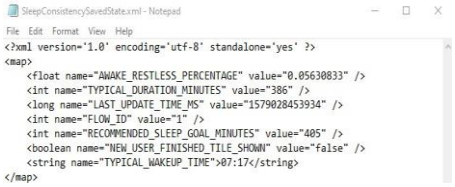


Fig. 34. Fitbit application data

Figure 34 shows the user's saved sleep consistency, on average, which is stored by the tracker. This information is stored in XML format and within the shared_prefs folder. It can be located at:

com.fitbit.FitbitMobile/shared_prefs/SleepConsistencySavedState.xml.

This provides details regarding the average 'awake and restless' percentage of the user, also showing the typical wake up time (which can help identify any abnormalities in typical patterns when analysing a suspect's sleep data). Within the shared_prefs folder, the file 'profile_lite.prefs.xml' displays information about the user, e.g., user's avatar, display name, and Fitbit ID. Figure 35 shows information regarding the Fitbit application installation. The email address used to create the Fitbit account and the authentication token are shown. Forensically, authentication tokens can be used to access accounts.

Fig. 35. Avatar link and application installation

Moving on to database analysis of Fitbit artefacts from an Android device, database files recovered from the physical extraction are stored differently than iOS. With the iPhone extractions, the Fitbit data was all stored within the *fitbit.sqlite* database, which contained 193 tables. In Android's case, there are many database files stored individually within the databases folder. Figure 35 shows the table 'WATER_LOG_ENTRY' within the database 'logging.db'. This displays when water intake has been logged by the user. When analysing the iOS extraction, only one instance of water intake was recorded on 11/02/2020 at 21:44 whereas Android analysis displays multiple water intake entries on 14/01/2020 between 19:03:43 and 19:03:52.

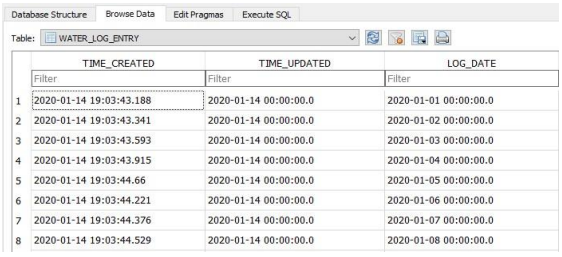


Fig. 36. Water logs

'AUTO_CUE_OPTION' is a table which displays specific exercises and whether GPS is enabled by default. Exercises including: Running, Cycling, Hiking, and Walking are all equipped with automatic GPS recording. There are several exercises which are not supported for GPS and two where GPS recording is disabled by default. Located in the same fitbit.db database file is a table named 'DEVICE'.

This table also featured in the iOS analysis and recovers data relating to the physical fitness tracker connected to the application installed on the mobile device. Details on the exact time and date the watch was last synced with the application are included, and even specifics on the identification number for the charging cable used to charge the device. We can also see the battery percentage when the device was last synced, 8%. Figure 36 continues, providing details regarding the MAC address of the device as well as the current firmware app version and the current boot strap loader. This table also contains several other columns of significance shown in Figure 38.

Fig. 37. Further device information

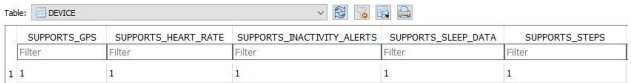


Fig. 38. Device support

From these columns, we can see that the device supports GPS, heart rate data, sleep data and records steps. As well as this, the device supports inactivity alerts, which means that when a user is not displaying their usual activity, based on a calculated average – the device will send inactivity alerts to the user through the Fitbit application.

Fig. 39. Further device information

Further device information is shown in Figure 39. The 'AVAILABLE_NOTIFICATION_TYPES' column shows the notifications that come through from the linked mobile device, to the linked physical fitness tracker. Notifications that come through to the Fitbit device include incoming calls, text messages, and any calendar entries. Application syncing is also supported as well as connected GPS. Connected GPS is where the location activity of the linked mobile device can be utilized when GPS connectivity is not available via the fitness tracker. Also contained within the same fitbit.db database is a table named 'PROFILE', where information regarding the user's profile is displayed. Some profile information was retrieved from the iOS analysis, however, more data relating to the user's profile is listed here. Firstly, we have the 'TIME_CREATED' column – this shows the date and time the profile was created, the Fitbit Forensics profile was recorded as being created on 13/12/2019 at 12:50 whereas the time recorded here is 00:00:00, although the date is correct.

Table: PROFILE

	TIME_CREATED	ENCODED_ID	FULL_NAME	FIRST_NAME	LAST_NAME	DISPLAY_NAME	ABOUT_ME	DATE_OF_BIRTH
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	2019-12-13 00:00:00.0	7YLGYF	Fit Bit Forensics	Fit Bit	Forensics	Fit Bit F.	This is a test	1996-12-29 00:00:00.0

Fig. 40. Profile information

This is something that was not recovered from the iPhone. As with the iPhone extraction, profile information such as the account ID, full name, display name, about me section and the date of birth entered by the user are retrieved. Figure 39 shows continued columns from the 'PROFILE' table. We can see height information entered by the user, as well as the users average stride length when running and walking. After these columns, we then have another instance where the user's profile photo is shown.

HEIGHT	STRIDE_LENGTH_RUNNING	STRIDE_LENGTH_WALKING	PROFILE_PHOTO_LINK	AVERAGE_STEPS	EMAIL
Filter	Filter	Filter	Filter	Filter	Filter
1752.0	125.5	72.7	https://d6y8zfzc2qfsl....	4089	j.w.faulkner@...

Fig. 41. Profile information continued

Column 'AVERAGE_STEPS' shows the average amount of daily steps taken by the user – this can be misleading however as the average is calculated daily. If the battery dies on the device, or the device is not worn for a period of time – this is still used to calculate the user's average step count. Another database of interest is the 'HEART_RATE_DB' database. This displays the resting heart rate of the user daily. This may pose interest to forensic investigators if the resting heart rate on a specific day is dramatically higher than it usually is. Where a lower resting heart rate is displayed such as 0 could mean that the watch has not been used on this day.

Located at the 'MESSAGES_DB' database, within the 'USERMESSAGE' table, interactions between the user and recipients are displayed - Figure 42. Messages '*Hello, this is a tes*t' and *'Hi j'* are not visible here as the physical extraction was completed before those messages were sent. The 'USERMESSAGE' table has recovered all messages stored within the user's inbox at the time of the extraction.

Table: UserMessage

	message	timestamp	read	senderDisplayName	senderAvatar	senderEncodedId
	Filter	Filter	Filter	Filter	Filter	Filter
1	Hello how are you	2019-12-13 13:34:05.764	1	Barry F.	https://d6y8zf...	7B8Q8B
2	Hello :)	2019-12-13 13:33:49.956	0	Fit Bit F.	https://d6y8zf...	7YLGYF

Fig. 42. Messages

These messages corroborate with the date and time the messages were sent. As has previously been recovered with the iOS extractions, we are able to recover the messages that were sent and received, the time and date that messages were either sent or received, information regarding the sender's display name and their profile picture and finally, the user's Fitbit ID.

Next, we analyzed the 'SLEEP' database which contains information about the users recorded sleep data. The 'SLEEP_LOG' table provides several columns of interest to investigators. The first column shows the overall duration of sleep in seconds. The next column displays sleep efficiency; this may not pose great interest to investigations, but dramatic increases or decreases in efficiency when analysing a large data set may indicate abnormalities. The 'MINUTES_ASLEEP' column shows the number of minutes the user spent in the sleep stage, then the 'MINUTES_AWAKE' section displays how long the user was awake for the duration of this sleep. 'START_TIME' displays the time that the user entered the first stage of sleep.

Table: SLEEP_LOG

	DURATION	EFFICIENCY	MINUTES_ASLEEP	MINUTES_AWAKE	START_TIME
	Filter	Filter	Filter	Filter	Filter
1	23100000	96	332	53	2020-01-13 23:19:00.0
2	27600000	94	405	55	2020-01-13 00:34:30.0
3	10560000	97	171	5	2020-01-09 13:52:00.0
4	21660000	97	317	44	2020-01-07 23:44:00.0
5	28440000	95	418	56	2020-01-05 23:36:00.0
6	22980000	94	339	44	2020-01-04 00:54:00.0
7	23160000	91	345	41	2020-01-01 23:12:00.0
8	25500000	89	379	46	2020-01-01 00:34:30.0
9	22860000	96	325	56	2019-12-31 01:08:30.0

Fig. 43. Sleep Database, Sleep_Log Table

E. Comparison

Table II depicts the generic data you would aim to uncover as an investigator and whether the data has been recovered or not during analysis. For these experiments, all account details were provided to easily access the account. However, there may be instances where credentials are unavailable, but investigators wish to access the account in an attempt to recover evidential user data. Something that was not recovered from Android analysis, that was during iOS analysis, is the users posts to their Fitbit feed or community groups. These social posts were uploaded before the Android extraction took place but were not visible in any of the database files from the physical extraction of the emulated Google Pixel 2XL.

These extractions contained varying amounts of data and some extractions contained data sets which weren't recovered from other methods of extraction. In order to obtain the maximum amount of data, we believe the username and password would be required, where an investigator could then prepare the preferred investigation method. With the Fitbit Versa, if the suspect's mobile device has been seized, the Fitbit application is installed on the linked device, but the Fitbit credentials have not been provided by the suspect the investigator should attempt to use the authorised access token

TABLE II. COMPARISON OF FINDINGS

Extraction Method	Private Messages	Feed Posts	GPS Data	Profile Information	Sleep Data	Heart Rate Data
Logical (Cellebrite)	✓	✓	✓	✓	✓	✓
Logical (XRY)	✓	✓	✓	✓	✓	✓
Logical (Cellebrite)	X	X	X	X	X	X
Logical (XRY)	X	X	X	X	X	X
Physical (Genymotion)	✓	✓	✓	✓	✓	✓

potentially stored on the device. This token is securely stored on the mobile device and is not easily accessible to device owners. The token, when retrieved, can then be paired with proprietary forensic software to gain access to the users account without having to manually enter the credentials, this would then result in full account access. Thus, a logical extraction or a file system extraction of the iOS mobile device would then uncover the Fitbit data.

A further point is the role the profile information table can play. Although generic profile information is likely to already be known to investigators working a case, this table contains other columns which may help in identifying an individual accused of committing a crime. For example, in column 'HEIGHT' the user's height is displayed, but further to this the columns 'STRIDE_LENGTH_RUNNING' and 'STRIDE_LENGTH_WALKING' show the user's average stride length when both walking and running. This may help in a real-world scenario where for example, a suspect may have been arrested on suspicion of committing a crime but both CCTV and witness cooperation may help identify grainy CCTV footage where the individuals face is not visible. Carefully analysing the CCTV footage may help recognise these characteristics of the suspect, although this is likely to be dismissed in court, when corroborated with other pieces of information e.g. clothing worn, this data may help convict an individual of a suspected offence.

IV. CONCLUSION

This paper has demonstrated several areas of data significance which are currently likely to be unknown to many digital forensic practitioners and researchers. Thus resulting in further development and knowledge within the field of digital forensics. In terms of the recovery of Fitbit artefacts, we have retrieved information which we have not seen evidenced elsewhere. The extraction and analysis methods utilized in this paper can aid future digital forensic investigations, potentially alleviating investigatory pressures and put suspects of crime before the courts, whilst subsequently safeguarding victims of crime.

To obtain the maximum amount of data, we believe the username and password would be required, where an investigator could then prepare the preferred investigation method. Though the term 'maximum amount of data' can be misleading, as specific circumstances of a case should be taken into consideration here. For example, for a suspect whose whereabouts are unknown, investigators may wish to uncover the maximum amount of GPS data to put together a robust case. In this case, we would recommend the use of the cloud extraction analysis if possible, as this form of extraction recovered the maximum amount of detailed GPS data in the results section. Each successful extraction offers its own unique use case, as analysis of these methods prove that the preferred extraction type could vary from case to case due to the vast amount of data stored in different ways across different methods of extraction.

In terms of further work which could be completed in the field of wearable forensics, the same extraction methods and analysis techniques could be used across a range of popular wearable devices. We believe that Fitbit forensics is the most prevalent sub-branch of wearable forensics at this moment in time and will continue to be over the coming years, with Google's purchase of the wearable's giant.

REFERENCES

[1] J. Gill, "Fitbit Data Provides Clues in Murder Case: eDiscovery & Criminal Investigation", JDSURPA Legal News, 2019, https://www.jdsupra.com/legalnews/fitbit-data-provides-clues-in-murder-92645/

[2] BBC News. "Fitbit data used to charge US man with murder", Technology, 2018. https://www.bbc.co.uk/news/technology-45745366

[3] A. Watts, "Cops use murdered womans fitbit to charge her husband", CNN, 2017. https://edition.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html

[4] C. Grimes. (2017) 'Application Analysis: Fitbit', Leahy Center for Digital Investigation (LCDI), pp. 1-29. doi: 10.1016/b978-1-59749-727-5.00008-8.

[5] N. Jones. (2018) 'Analysing If Data Extracted From Wearable Fitness Devices Can Add Value To Criminal Investigations' Supervised by Dean Northfield. Staffordshire University, UK.

[6] A. MacDermott. S. Lea, F. Iqbal, I. Idowu, B. Shah. (2019) 'Forensic analysis of wearable devices: Fitbit, Garmin and HETP Watches', in 2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop. doi: 10.1109/NTMS.2019.8763834.

[7] J. Palmer. (2021) "The Best Android Phones in 2021", Tom's Guide, https://www.tomsguide.com/uk/us/best-android-phones,review-6051.html

[8] Fitbit (2020) "Fitbit SmartTrackTM Auto Exercise Recognition". Available at: https://www.fitbit.com/uk/smarttrack