Wearable Device Forensics

Ms. Asmita Namjoshi
Research Scholar
Department Of Computer Science
Tilak Maharashtra Vidyapeeth, Pune

Mr. Rakesh Patil
Faculty
Department Of Computer Science
Tilak Maharashtra Vidyapeeth, Pune

Dr. Anup Girdhar
CEO, Founder,
Sedulity Solutions & Technologies, New Delhi

Abstract:
A Fitbit wellness tracker is a standout amongst the most well-known wearable gadgets utilized by numerous individuals today. Computerized Proof assumes a fundamental job in examinations and similarly, it is trying for the Examination and the Digital crime scene investigation group in India. The most effective method to deal with explicit computerized gadgets like fitbits and other brilliant gadgets and to make it admissible to the courts is the basic inquiries. The significant difficulties are gadget taking care of, information cutting, information protection, information investigation and reportage with its credibility. New advances and new gadgets are quickly being created, which makes new wellsprings of computerized proof. This shows a test to law implementation organizations and advanced examiners to remain known regarding the quick improvement in the computerized field. This paper talks about a generally new wellsprings of advanced proof. This shows a test to law implementation organizations and advanced examiners to remain known regarding the quick improvement in the computerized field. This paper talks about a generally new wellsprings of advanced proof which is the proof extricated from Wearable gadgets. Dealing with information gathering from logs, information purification and cutting used to recognize the important information, another stage is to safeguard the proof and assess its honesty checks lastly to create the report dependent on distinguished antiquities.

Keywords: Forensics, Digital Forensics, Wearable Devices, Fitbit, Cyber Law.

Introduction:
The use of wearable technology such as smart watches, activity trackers, GPS-connected devices, and other “personal” monitoring devices is on the rise and it is beginning to invade what is left of our privacy. Although wearable technology is marketed for its health and exercise benefits, the widespread use of this type of mobile technology is becoming a tool used by attorneys and considered by courts. In establishing case law on this matter, courts must strike a balance between the benefits of such technology and people’s expectation of privacy.

The past decade has seen rapid development in cases relating to digital forensics, with criminals utilizing new technology as a platform for their criminal activity. There has also been a large increase in the market concerning the number of wearable health and fitness trackers available; however, little research exists surrounding the data that can be recovered from the devices and the value this data can hold. The specific objective of this research was to analyze whether data extracted from Fitbit devices could add value to a criminal investigation. A sample data collected from the voluntary participants was used to collate specific heart rate and step count data over a period of 24 hours using their own personal Fitbit devices. The results have been extracted and analyzed to determine the value in relation to a criminal investigation. The results and retrieval
methods are critically reviewed to establish whether the potential value of the data outweighs the issues surrounding the intrusion of privacy and other ethical considerations. These results could provide further tools and questions to use in investigations where suspects or victims own a wearable fitness device to possibly corroborate with other evidence or statements.

In India, people are now more fitness freaks, started evaluating that up to what extent they are able to burn their calories, wearable devices which track an individual’s fitness are becoming increasingly popular. The devices promote the ability to track your daily steps, log what you eat and share progress with an online fitness community or even link devices with friends and family to compete in challenges. Wearable fitness trackers are a popular way to stay active and in control of personal fitness levels via a small device worn on the wrist, like a digital watch. A fitness tracker uses an accelerometer, a small instrument that measures acceleration forces, to calculate physical activity.

Large companies such as Fitbit, Samsung, and Apple encourage users to track their health and lifestyle using online platforms linked to the device itself usually via an app (Fitbit, 2018). The devices are still improving and most include basic functions such as step tracking and heart rate monitoring. However, newer versions of the devices also allow users to track sleep patterns, GPS locations and also log exact work outs. The devices also include the option for the user to log food and water intake to track their calories throughout the day. These devices collate specific data that can then be used to gain further insight into an individual

However, Law implementation organizations are being tested by the need to prepare their staff to remain exceptional because of the quickly developing nature of new innovations in the advanced field. [1]. There are a few attributes relating to the idea of advanced proof that recognizes it from the run of the mill proof. Computerized proof can be time delicate, dormant (covered up), and can be effectively changed, harmed or annihilated [2]. Furthermore, computerized proof crosses jurisdictional limits, which introduces significantly more noteworthy difficulties for advanced examiners and law authorization authorities. A measurable expert must ensure that the strategies utilized are completely agreeable with every single appropriate law and guidelines in that specific locale [3].

In this paper, distinctive wellsprings of computerized proof are talked about, with the attention being on Wearable gadgets as advanced proof. A contextual analysis identified with this specific computerized proof is exhibited.

The rest of this paper is organized as follows: the process of digital forensic investigation is presented in section 2. An overview of the different sources of digital evidence is presented in section 3. Purpose of the proposed Algorithms is to store the relevant values and further use for the analysis and investigation purpose. 4. A discussion of the challenges of using Wearable’s as digital evidence is presented in section 5, and a conclusion is presented in section 6.

Process of Digital Forensic Investigation

Gadget Forensic analysis might be required in a wide range of circumstances, for example, proof accumulation for legitimate procedures, and inside corporate examination of Security Arrangement infringement [4]. The strategies and devices utilized by scientific specialists may differ contingent upon the kind of occurrence and the sort of explored computerized proof, subsequently a characterized method is required to oversee the procedure of advanced examination and follow industry benchmarks and fitting laws [5]. There are different proposed models for Digital Forensics. In any case, the five stages utilized in research areas illustrated in Figure 1 Phases of Digital Forensics process.

Collection of Data  Data filtering  Data Acquisition  Data Identification & Analysis-> Reporting

Figure 1: Phases of Digital Investigation Process.

For the most part, an advanced criminological examination begins with the distinguishing proof of the episode and the recognizable proof of the wellsprings of computerized proof. At that point, a court order is issued by the appointed Law requirement office to gather and break down the advanced proof. The measurable specialist must know that the utilization of inappropriate system or unlawful pursuit and seizure can contrarily influence the tolerability of the proof [5]. When the court order received, the criminological examiner will set up the apparatuses and the procedures required for whatever
remains of the procedure. The five phases of the procedure are then pursued as portrayed underneath:

**An overview of the different sources of digital evidence**

**Collection of Data**
The Gathering stage alludes to the accumulation of advanced proof from the different sources identified with the episode being explored. When gathering the proof, it is important that no progressions are made to the first information. For instance, when gathering proof structure a PC hard plate, a criminological duplicate of the information put away on the hard circle is taken so as to play out the examination on that duplicate. An exceptional gadget called a compose blocker is utilized amid the duplicating procedure to keep any progressions to the information on the hard plate [6].

The gathering stage is of most extreme significance as whatever is left of the stages rely upon the present accumulation of proof. Two basic factors in this stage are the Realness of the proof information gathered, and the Safeguarding of the advanced proof. The realness of advanced proof alludes to the confirmation that the proof has not been modified and that it originates from a specific source. In Government Courts, legitimacy is administered by Standard 901(a), which expects that to build up that a thing is bonafide, a defender must deliver allowable proof "adequate to help a finding that the thing is the thing that the advocate claims it is." [7]

The conservation of computerized proof alludes to following generally accepted procedures and rules when dealing with the proof. The most critical rules are as per the following [6]:

- Guarantee that every advanced proof gathered is legitimately archived, named, checked, shot, video recorded or outlined, and stocked.
- Guarantee that extraordinary consideration is taken with the computerized confirmations material amid transportation to maintain a strategic distance from physical harm, vibration and the impacts of attractive fields, electrical static and substantial variety of temperature and mugginess.
- Guarantee that the advanced proof is put away in a safe, atmosphere controlled condition or an area that isn't liable to extraordinary temperature or dampness. Guarantee that the advanced proof isn't presented to attractive fields, dampness, residue, vibration, or whatever other components that may harm or pulverize it.

**Data Filtering**
Data Filtering is the way toward picking a little piece of your informational index and utilizing that subset for review or examination. Separating is for the most part (yet not constantly) transitory – the total informational index is kept, however just piece of it is utilized for the estimation. Separating might be utilized to:

- Look at results for a specific timeframe.
- Calculate results for specific gatherings of intrigue.
- Exclude wrong or "awful" perceptions from an examination.
- Train and approve factual models.

Sifting expects you to indicate a standard or rationale to recognize the cases you need to incorporate into your investigation. Sifting can likewise be alluded to as "sub-setting" information, or an information "drill-down". In this article, we show a sifted informational index and talk about how you may utilize separating.

**Data Acquisition**
The following stage after the information filtration is information securing. It is the way toward examining signals that measure true physical conditions and changing over the subsequent examples into computerized numeric qualities that can be controlled by a PC. Information procurement frameworks, condensed by the abbreviations DAS or DAQ, normally convert simple waveforms into computerized esteems for handling. The parts of information procurement frameworks include:

- Sensors, to change over physical parameters to electrical signs.
- Signal molding hardware, to change over sensor signals into a structure that can be changed over to computerized values.
- Analog-to-computerized converters, to change over molded sensor signs to advanced qualities.

For this situation, the most part alluding to the recovery of material from a gadget, when contrasted with the bit duplicate imaging utilized in PC legal sciences. The information gained from the logs/metadata is as parameters which should be preserved for the further examination and investigation. Wearable’s are restrictive in nature, in a couple of devices, it is hard to extricate and gain information which meets to an impasse. Anyway on the off chance that the information gets removed then it further arranged by a continuum, along which strategies turn out to be progressively specialized and "forensically stable," apparatuses turn out to be increasingly costly, examination takes longer, inspectors need all the more preparing, and a few techniques can even turn out to be progressively intrusive.
**The Identification and analysis phase**

The Identification and analysis phase alludes to dissecting the information coming about because of the examination stage to achieve suitable ends dependent on the proof found or verify that no end can yet be drawn. The examination ought to incorporate recognizing individuals, spots, things, and occasions, and deciding how these components are connected to an end can be come to. The specialized information and experience of the expert assume a noteworthy job in playing out a powerful examination. The investigation ought to be led utilizing legitimately reasonable strategies and procedures [4] & [8].

**The Reporting Phase**

The Reporting Phase alludes to the way toward getting ready and showing the data coming about because of the investigation stage. It accomplished by showing the proof and the examiner's decision to the individual or gathering asking for the digital forensics examination [6].

**Proposed Algorithms**

Many Controversial criminal cases now registered in India where the suspected pieces of evidence are attached along with more digital evidence as a part of reports.

Due to the latest trends of the usage of digital gadgets, especially Fitbit's the admissibility of the digital evidence in the court is another challenging phrase.

In this research, the proposed algorithm benefits for further research and development dedicated to the Investigations agencies and produce digital evidence.

The list of proposed algorithms is as follows:

1. **First method is to prepare the users profile**
   
   ```
   fitbit_profiles(uid, full_name, birthday, profile_image, height, gender, avg_walking_stride, avg_running_stride, timezone, country, location)
   {
     # log in all parameters
     log_file = uid + full_name + birthday + profile_image + height + gender + avg_walking_stride + avg_running_stride + timezone + country + location;
     return log_file;
   }
   ```

2. **Second method is to analyze the user steps**
   
   ```
   Fitbit_steps(uid, starting_timestamp, ending_timestamp, steps_count, location)
   {
     Calories_burned_log_file = function_to_calculate_burned_calories_for_specific_uid(uid, start_timestamp, ending_timestamp, step_count, location);
     return calories_burned_log_file;
   }
   ```

3. **Third Method is to analyze heart rates**
   
   ```
   Fitbit_heart_rate(uid, starting_timestamp, ending_timestamp, average_heart_beat, location)
   {
     Heart_rate_log_file = function_to_calculate_heart_rate_for_specific_uid(uid, start_timestamp, ending_timestamp, avg_heart_rate_in_BPM, location);
     return Heart_rate_log_file;
   }
   ```

Further, these proposed algorithms use to save the user data to day activities in the form of logs which is subject to analysis the behavior of the user. For example, the user is in sleep mode, walking mode, running mode, mental stress, correlated to the timestamps and the location as well. It is very much supportive for further investigation and easy to make it admissible in front of the court.

**Challenges on using Wearable’s Digital Evidence**

Although computerized proof removed from Wearable gadgets has been utilized in a few lawful cases as talked about above[9], [10] & [11]; there are a few difficulties with Wearable proof that may be utilized to discredit the legitimacy and unwavering quality of the proof. As we would like to think, these difficulties can be classified into legitimate difficulties, operational difficulties, and abuse difficulties as pursues:

1. **Legitimate difficulties:**
   - Computerized information proof social event is new and wrongdoing scene police may not be proficient in how to gather, secure, transport or store advanced information to guarantee information isn't undermined or lost.
   - Only one out of every odd law implementation office has research centers or confirmed scientific specialists to analyze and translate information from Wearable gadgets.
2. Operational Difficulties:
   - The time-stamp inside the Fitbit can be set to an incorrect time, consequently the season of the occasions won't be exact, and connection with other computerized proof won't be conceivable.
   - Fitbit relies upon GPS for information transmission and following. GPS requires an immediate way to the satellite it is utilizing for legitimate information transmission. On the off chance that the GPS flag is being hindered for reasons unknown - the client is underground, climate conditions – at that point the information gathered won't be exact.
   - Numerous models of Wearable gadgets are accessible available, each with its very own arrangement of highlights and capacities. Not all gadgets give similar usefulness and translation of development. For instance, a few models won't recognize arm development from real advances, and subsequently, their information records won't be solid.

3. Abuse Difficulties
   - More than one individual may wear a Fitbit.
   - The information records from the Fitbit are exact as long as the client is wearing the gadget and utilizing it legitimately. For instance, wearing the gadget on the lower leg will create conflicting information.

Conclusion
Computerized scientific examination has grown gigantically amid the ongoing years. The coming of new gadgets that store information has been trying to measurable examiners and law authorization offices. New measurable examination apparatuses and strategies were and as yet being created so as to almost certainly process and break down information from these gadgets. PCs and cell phones are the most well-known wellsprings of computerized proof; in any case, it has been demonstrated from numerous lawful cases that there are different wellsprings of significantly advanced proof.

Wearable gadgets store unlimited measures of information about the client's area, movement levels, rest designs, and moving propensities; in this manner making a nitty-gritty story of the client's regular daily existence. Proof removed from Wearable gadgets has not yet been utilized on a wide scale because of contentions in regards to the unwavering quality and exactness of these gadgets. Be that as it may, these gadgets are being improved persistently, their exactness and unwavering quality and along these lines, acceptability is improving extraordinarily when they are matched up to different gadgets like cell phones and PCs which are now utilized as allowable proof in court.

Gave that the proof meets the prerequisites of acceptability, Wearable gadgets ought to be considered as one of the wellsprings of advanced proof that can be useful in numerous legitimate cases.

References