Data Extraction and Forensic Analysis for Smartphone Paired Wearables and IoT Devices

Gokila Dorai
Florida State University
dorai@cs.fsu.edu

Shiva Houshmand
Santa Clara University
shoushmandyazdi@scu.edu

Sudhir Aggarwal
Florida State University
sudhir@cs.fsu.edu

Abstract

Wearable devices and Internet of Things (IoT) devices have marked the beginning of a new era in forensic science. Data from smart home gadgets and wearable devices can serve as an important "witness" in civil as well as criminal cases. Thus data extracted from these devices has started to impact and transform litigation. Data collected from wearable devices can help determine truths in witness testimony since these devices document several types of activities of an individual at all times. Increased use of smart home devices also opens a new window for investigators. The collective data extracted from wearables and smart home devices can help investigators view the detailed events that have happened in an environment in a larger context, and give them better perspectives in the case under investigation. Our work aims to provide a solution to the challenges faced by the investigators in both extracting and analyzing the sheer volume of extracted data, and illustrates techniques to automatically highlight anomalies and correlations in the time series data collected from these devices.

1. Introduction

Wearable devices have become increasingly popular. The number of wearable devices is expected to surge and reach 150 billion by 2027 [1]. The number of IoT devices, particularly in the home is expected to increase at a similar pace. By 2020, it is expected that 20 billion IoT devices will be connected to the internet [2]. This marks the beginning of a new era for digital forensics: Digital Forensics meets Big Data. In the next few years, the digital forensics community will face the key challenge of dealing with huge amounts of data needed to be obtained from many devices even used just by one person. A second challenge is how to analyze this large amount of data for investigative purposes. In this paper we describe a Device Data Extraction and Forensic Analysis Model (DEFA) for digital forensic investigations that uses automatic data extraction and a suite of integrated analysis tools to support the needs of large data forensic investigations. The majority of wearable devices currently are health and fitness related and augment what a smartphone can do. These devices can be worn without having the need to carry a smartphone although they need to sync the data collected at a later time by being close to the paired smartphone. Increased usage of wearables increases the amount of data being collected. The number of smart home IoT devices is also increasing as new sensors and capabilities for monitoring are added. Each new device produces a substantial amount of data.

A mitigating aspect of the large amounts of data generated by wearables and smart home devices is that these devices are generally categorized into only a few apps on the smartphones. For example, most of the health wearables are synced with a health app on the smartphone. Similarly, many smart home devices are again synced with a single app (for example Nest app used to control HVAC system, indoor/outdoor security cameras, smoke detector, etc). Thus the data extraction and analysis problem becomes manageable for our environment.

In this paper, we first explore the issue of data extraction and analysis from fitness wearables, smartwatches and smart home IoT devices. For the iPhone we have automated the data extraction from all of these devices. We believe that our approach can be extended to automated extraction from other sets of IoT devices and wearables. With respect to data analysis, information overload for a digital investigator often happens when there is too much data available for analysis. Current analysis tools such as data carving and command line tools for information retrieval may no longer be adequate. In our prototype DEFA system we implement a set of analysis and interactive / visual tools including exploratory data analysis tools useful for queries related to multi-dimensional crime mapping / crime scene analysis. In the future, we expect other tools that incorporate high level techniques used in

behavioral profiling and psychological profiling will also be integrated into DEFA. In this paper we describe some of the core tools in our system.

In order to show the efficacy of our approach, we evaluate real-world criminal cases where data from such devices has helped investigators solve these cases and provide insights into how DEFA analysis tools can expedite the process of evidence discovery. Our primary contributions are:

- Design of a data extraction and analysis (DEFA) system for forensic investigations related to smartphones, wearables and smart home devices that are paired and synced with the smartphone.
- Implementation and integration of an inference engine including statistical analysis and visualization tools into DEFA.
- Demonstration of how DEFA could be used for analyzing various criminal cases.

The paper is organized as follows. In the next section we discuss some related work and in section 3 we further discuss the DEFA model. In section 4 we discuss our work on automated data extraction from iPhone synced apps. In section 5 we discuss analysis tools and usage in example situations with a set of real cases where extracted digital information was important. Finally in section 6 we conclude the paper.

2. Related work

We discuss related work divided into three sections: Data Extraction, Data Analysis and Legal Expectations. Each is relevant to the DEFA system.

Data Extraction: Data extraction is increasingly becoming more complete across a broad range of devices and more automatic. Furthermore, capability to do selective extraction of only the desired data is also improving. We discuss a few examples of such extraction work. In [3] the authors developed a system to automatically extract selected data such as photos, messages, etc. from Android and iOS mobile devices, based on investigator defined filtering using aspects such as dates, location and type of content. In [4] the authors showed how to automatically extract Nest device data from an iTunes backup and generate a report. In early work, Baggili et al. [5] identified evidence of potential forensic value that can be obtained from Android based smartwatches such as Samsung Gear 2 Neo and LG. The authors described a methodology to help examiners extract relevant artifacts.

Data Analysis: Statistical data analysis is a very broad field and has been applied to many domains, so we don't discuss the statistical work specifically. Note that event correlation need not be statistical and can be based on logical sequencing or other techniques. Luo et al. [6] evaluated the correlation between events and time-series data for the purpose of service incident diagnosis of online services. Han et al. [7] discuss data analysis and related algorithms in the context of data mining. Motahari et al. [8] explore event correlation for business processes related to web services. Correlating events using dependency graphs is explored in [9]. Lin et al. [10] used temporal and spatial analysis to detect duplicated video clips in digital (video) forensics. A tool by Jin Yu [11] is used to create a timeline analysis for android-based systems. Kasiaras et al. [12] have proposed a tool called Android Forensic Data Analyzer which uses timeline and location information stored in Android apps. Their work uses data obtained only from an Android device and does not take into account any devices that could be paired and syncing data to the smartphone device. A forensic tool called Internet Evidence Finder (IEF) [13] produced by Magnet Forensics is capable of providing a geo-spatial view of chat history. Autopsy [14] is a free forensic tool which can perform timeline analysis by pulling timestamp information from files, EXIF data in pictures, etc. As far as we are aware, there are no tools which weave all the synced data together for visualizing big data for digital forensics purposes. A widely used forensic tool by Cellebrite has incorporated AI and pattern recognition into Cellebrite Analytics [15] for applications such as facial recognition in photos and videos. In the commercial domain, tools purporting to doing data analytics are generally focused on extracting and categorizing rather than addressing the issue of correlating multiple events and data from various smart devices. In our work on the analysis part of DEFA, we explore the type of integrated analyses that can be done for forensic purposes on the data that can be extracted from wearable devices and relevant IOT devices. We explore the kinds of questions that can be asked and how to develop a system that can, at minimum, visualize correlated and related events. This system should be integrated with the data extraction process. We believe that requirements for selective data extraction can easily be incorporated into such a system following the work in [3].

Legal Expectations: Federal Rules of Evidence have not yet changed to reflect advances in the digital age although some states have done so through state legislation. Legal expectations of what can be gained by extracting data from wearables & IoT devices, and what is admissible, is a complex subject and rapidly evolving. Privacy issues due to the large volumes of data stored

on these devices are also influencing the determination of admissibility of this type of data as evidence. Fundamentally, data in the form of electronically stored information (ESI) has been admissible as evidence if it can be shown to be relevant, reliable and probative.

Vinez [16] discusses the growing demand of wearable technology (focusing on Fitbit fitness trackers), its use as evidence in court and problems of admissibility. The author discusses how the large amount of data stored on wearable devices has great potential to augment and corroborate evidence from witnesses, but recommends that the legal community use it in a "strictly limited capacity until the technology industry can improve the reliability and functionality of the devices." Paranjpe [17] and Chauriye [18] discuss concerns of using such data from smart devices for litigation given the lack of clear legal standards. NFSTC [19] and NIJ [20] provide guidelines for the discoverability and admissibility of digital evidence that are applicable to mobile devices. Although there have been some arguments against the admissibility of evidence extracted from devices such as Fitbit, we believe the guidelines will also soon apply to current wearable devices and IoT devices.

3. Proposed investigative approach

As discussed, for forensic investigations current research and commercial tools do not sufficiently integrate extraction and analysis capabilities for multiple devices now owned by many users. This results in a very high cognitive workload for investigators. A conceptual model that was developed for IoT forensics is Forensic-aware IoT [21] in which the authors proposed a centralized trusted repository to support evidence collection and analysis. Kebande et al. [22] proposed a framework for IoT forensics that added proactive and reactive processes to the the work in FAIoT [21]. Our investigative framework envisioned as the DEFA system proposes to address the problem of high workload differently. The questions we believe that need to be addressed include how should the extracted data be stored and viewed, what are the analysis tools that can help forensic investigators and how can the investigators actually use various analysis techniques to get further insights into the culpability or not of suspects.

Figure 1 shows an overview of the DEFA system. The first step is to have all the data extracted from all devices of the target(s) of the investigation. Our scope of devices is the group of devices synced to smartphones such as wearables and smart home IoT devices that would be relevant to forensic investigations. Because each of the devices has a linked app on the smartphone, the data extraction is only necessary from the smartphone itself. For any such device, we consider the data extracted and stored in DEFA to be the set of feature values of that device defined on a spatiotemporal timeline. For simplicity we use the term timeline where we mean the spatiotemporal aspects.

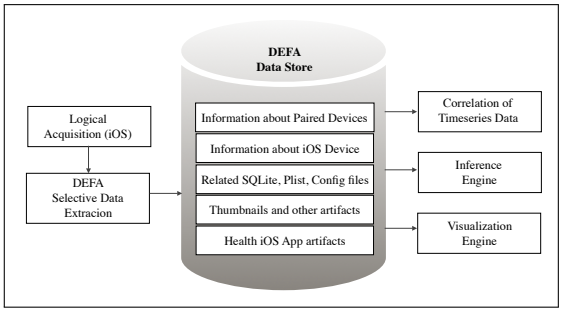

Figure 1. DEFA system

Consider as an example the Apple smartwatch and determining its spatiotemporal timeline. We consider heart rate as the feature and would expect to have a complete description of the this heart rate over any time and related location. Note that restrictions on the spatiotemporal timeline based on irrelevancy to the case could further reduce the data that needs to be extracted. Even this might not be possible at all relevant times since if the smartwatch is not equipped with a WiFi/cellular connection, then there will be unknown values on parts of the timeline when the smartphone is not nearby. UNKNOWN is assumed to be a valid value. Although the Apple smartwatch is equipped with GPS, the location information from the watch is not synced to the health app on the Apple smartphone. Additionally, if the cellular connection exists, then parts of the timeline could be populated by data from the cloud. In our approach, we assume that cloud data is typically not available. As a second example, consider a Nike wearable device synced to an Android phone. These devices typically have location information in addition to time information. In this case both the Android smartphone (using Google Fit app) and the wearable device would have independent location information on their timelines.

The DEFA analysis assumes that all timeline data is available as just described. In the analysis section we focus on timelines from the Apple native Health app (Activity, Mindfulness, Nutrition, Sleep) and from the Nest IoT devices (Thermostat and Camera). We assume that timeline data from other relevant devices related to the forensic investigation have also been obtained.

We divide up the analysis capabilities of DEFA into the following classes: (1) Basic Timeline Analysis; (2)

Statistical Analysis; (3) Event Correlation Analysis and (4) High-level Analysis. The DEFA system goal is to support a forensic investigator by being able to answer various types of queries. In Basic Timeline Analysis, an example query that should be answerable is "at a specific time what was the heart rate of the target." Or, during a particular time period "what was the location of the target's phone." The assumption is that information across multiple individual times can be accessed and displayed. In Statistical Analysis we support queries using a variety of statistical techniques such as means or standard deviations of values of specific timelines or statistical correlations across multiple timelines. Queries such as "are the timelines of heart rate and step count statistically correlated during a particular period of time" and "what is the average heart rate when the step count is 0" are supported by tools in this class. In Event Correlation Analysis we consider tools that can evaluate queries such as what was the temperature in the home of the "victim" when the suspect was downtown. Or "was the suspect running when the victim's smartphone was connected to a home WiFi network." Finally, tools in the class High-level Analysis support queries that can only be answered with more complex analyses of the data. For example, a query such as "was the suspect depressed that morning when the victim visited" may need development of a complex tool that incorporates AI and machine learning approaches. It has been shown in recent work [23] that a voice sample can identify whether or not an individual is agitated based on some prior training of voice samples. Possible tools in this class are only recently emerging.

Table 1. Devices/Apps used

Item	Description
Smart Devices	(1) Smart Thermostat by Nest (Model Number: T3007ES)
	(2) Outdoor Security Camera by Nest (Model Number: NC2100ES)
Other Devices	(1) iPhone 8 (iOS 12.1.4)
	(2) Mac OS X (v10.12.6)
	(3) Apple Watch Series-4 (16S535)
Apps	(1) Nest iOS app (v5.32.0.10)
	(2) Health iOS app
Testing period	03-01-19 to 03-05-19 (mm-dd-yy)

4. Data extraction

In this section we consider data generated by various wearable and IoT devices that are synced to an Apple iPhone. We discuss the extraction methodology and the artifacts located as evidence of pairing and syncing. In our automated extraction the smartphone only needs to be connected to the DEFA system and the relevant data is automatically extracted to the DEFA storage. Extracting data from smartwatch and smart home devices has been made easier because the data for a range of IoT devices for a single manufacturer is in a single app. Also, the data for most fitness tracking wearable devices and smartwatches is contained within an app container/app group. We explain the extraction process for each device and wearable that is synced to the iPhone in the following sections. In our experiments we used an Apple Watch with GPS and cellular; the full list of devices and apps used is shown in Table 1.

4.1. Extracting data synced from wearable

An Apple Watch always needs to be paired with a companion iPhone. The companion device is needed to install apps, change settings, and sync information on the Apple Watch. Apple Watch content is constantly being backed up to the paired iPhone. The synced data from the Apple Watch can be found in the iTunes backup.

Users can interact with many apps on the Apple Watch such as Calendar, Apple Pay, Maps, Smart home controlling IoT apps, Photos, etc. There are two types of apps [24] that are accessed through the Apple Watch: iPhone-based apps and stand-alone apps. iPhone-based apps require the companion device to be nearby since the app on the Watch only contains the user interface. When the Watch is first paired with the iPhone, data from the iPhone (types such as photos, calendar events, etc.) is pre-loaded into the application on the Watch. The Watch cache size depends on the data type. The cache size for live updates and notifications is very small. Thus these may be lost if the companion device (iPhone) is not nearby for any length of time. Stand-alone apps are based on Watch OS and have access to cellular data and WiFi hotspots even if the iPhone is not close by. The stand-alone watch apps are fully functional at all times. Apple Watch does not have physical connections for charging or syncing since it uses wireless charging. Therefore, for data extraction from Apple Watch we have to rely on the iPhone to which it is paired. If an Apple Watch is unpaired from an iPhone, a complete backup of the watch is automatically stored on the iPhone.

4.2. Extracting data from iPhone

A logical acquisition is performed using *libimobiledevice* and *idevicebackup2* [25]. The artifacts shown in Table 2 are then *selectively* extracted from the IoT devices and wearables. Note that DEFA will only extract data and artifacts related to paired devices, whereas, the trivial logical acquisition will

Table 2. Location of artifacts

	Artifact Location in iOS-Backup Folder	Name of the file	Details
1	Main folder	Info.plist, Status.plist	Device details, Status of backup
2	/c5/c5ad63c1c7304bbc53dcd4ac9b7a35060450f8e7	Nest.sqlite	(Nest) Thermostat settings
3	/e1/e1da0e82d74bf22b60dc11a27bedda82f6525590	com.nestlabs.jasper.release.plist	(Nest) Device configuration
4	/48/4846b419d656bd151b3843b83e54174ac4ad338a	historySecureProperties.plist	Paired Apple Watch specifics
5	/5c/5c8e9c1b467c560ecae4f5c64374bc67fbd5819b	activeStateMachine.plist	Watch GUID and Pairing Date
6	/b8/b89530717d32fb55a5fc608a1d56027f1b5d1128	Application.dat	(Nest) IoT Watch App specifics
7	/ad/ade0340f576ee14793c607073bd7e8e409af07a8	com.apple.wifi.plist	Wifi Connections showing timestamp and BSSID
8	/f7/f7493f633a76ff3541317ab846b17b5df0dfae12	AttachmentsList.plist	The date/time of the last notification received from the Nest IoT Device

obtain all data and artifacts. The selective extraction is possible since we know the location of artifacts synced from paired devices beforehand. In the second column of Table 2 the SHA-1 hashes corresponding to the file names in column three are shown. Note that, sensitive data such as health app data does not appear in the iOS backup due to Apple's security policy. However, we leveraged the iOS Share Feature [26] to export the Health App data and then extract relevant data from the exported files. This limitation exists only for the native Health iOS App. For third-party fitness tracking apps, this limitation does not exist and we can perform data extraction using logical acquisition and DEFA's selective extraction.

4.3. Artifacts

Artifacts about Paired Devices: The specifications of the paired Apple Watch and the date it was last paired are shown in rows 4 and 5 of Table 2. The information in *historySecureProperties.plist* is organized by the UDID of the paired devices. We found the watch-specific pairing information in *activeStateMachine.plist*, represented by the GUID (Globally Unique Identifier Number) of the Apple Watch along with the initial date of pairing. This file also includes information about the pairing status and the build number of the device. In the same hierarchy of folders, the folder named *DeviceRegistry* contains all artifacts synced from the watch inside a sub-folder named after the GUID of the watch. The pairing of the watch with the IoT device is evident from the details shown in *Application.dat* file of the Nest application as shown in row 6 of Table 2.

Table 3. Thermostat settings on 03/03/19

Time	Source	Adjustment	Status
10:58AM	Apple Watch	$72°(H) to 75°(H)$	User adjustment
11:05AM	Apple Watch	$75°(H) to 72°(H)$	Set by Nest App
11:23AM	Apple Watch	$72°(H) to 68°(H)$	Set by Nest App
11:31AM	iPhone	$68°(H) to 72°(C)$	Set by Nest App
11:36AM	iPhone	$72°(C) to 77°(C)$	Set by Nest App
11:42AM	iPhone	$77°(C) to 68°(H)$	Set by Nest App

Artifacts Synced from Smart Home Devices: We used Nest IoT devices such as the thermostat and camera as examples of smart home devices. We are able to extract a timeline of the thermostat temperature changes made by the user (either from the iPhone or Apple Watch). Database tables such as ZCDENERGYEVENT, ZTOUCHEDBY and ZTOUCHEDWHEN were parsed from the Nest sqlite database (see row 2 of Table 2) in order to obtain manual settings and location information. Our parser was used to parse these database table and list the date/time, cooling temperature (C), heating temperature (H) and source of change as shown in Table 3. We found that the source value of '2' indicates temperature adjustments performed from the Apple Watch and the source value of '6' indicates adjustments by the iPhone App. The data retrieved was independently verified in our set of experiments. If there are multiple devices from different manufacturers used in a smart home setting, we can narrow down the search for relevant artifacts by searching for the "App Group Name" of specific applications used to control those devices.

Artifacts about User Location: When a smartphone connects to a wireless access point or a hotspot, this information can be retrieved from the extracted files. The *com.apple.wifi.plist* file contains information about the BSSID number, data and time at which the device connected to an access point, whether the WPA was set for a personal or an enterprise network, network usage, and whether the user manually connected to the access point or the device was automatically connected. The BSSID is a unique MAC address of a wireless access point, but it does not directly show the physical location of the device. We used Google Geo-location API [27], to lookup the BSSID number and find the latitude and longitude information of the access point location.

Artifacts about Events/Notifications: Some smart home devices are event driven, meaning that when an event happens the user will receive a notification on their phone, or smartwatch. In our experiment, the Nest camera sends alert/notifications to the iphone or Apple watch when the camera senses a movement or a person.

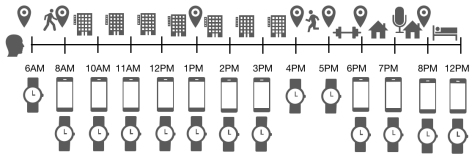

Figure 2. User activity abstracted from several timelines (step count, walking/running, sleep)

We were able to retrieve jpeg images that were received as user alerts/notifications of the Apple watch. The *BulletinDistributor* directory contains attachments which are primarily thumbnails of notifications received from IoT cameras on the Apple Watch. We also noticed that this data gets overwritten occasionally and could not be recovered if the backup is obtained several days after a camera notification was received on the watch. Notification artifacts can be viewed in the *AttachmentsList.plist* file (see row 8 in Table 2). The only useful information we were able to retrieve is the last modification date of the *AttachmentsList.plist* file which implies the last date/time at which the user received a notification from the Nest camera. Note however that the images are retrievable in a jailbroken iPhone.

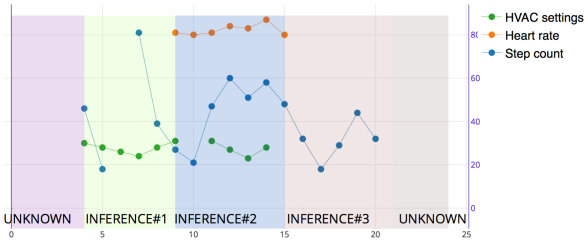

Figure 3. A scatter plot of step count, heart rate and HVAC settings

5. Forensic analysis with DEFA

Using geospatial data for forensic analysis has a long history. Elmes et al. [28] describe in depth how geospatial applications have been used for investigating civil and criminal cases. In a survey paper Quick et al. [29] discuss the need for new techniques to handle the challenge of big data in forensic analysis and conclude more research needs to be done for practical solutions. Fowle et al. [30] discuss a variety of computer modeling of data for visualization. None of these discuss building a forensic system to support forensic analysis.

The forensic analysis goals of DEFA are (1) to store the data in an efficient manner so as to be able to access the data needed for analysis and (2) to have a set of integrated analysis tools as part of the system that can essentially answer any question about the data that a forensic investigator might pose, with useful visualization capabilities. In this section, we describe *some* of the analysis tools and visualization capabilities that we have developed and implemented in our prototype to illustrate what is possible.

We have not yet explored efficient management of the data store of DEFA and have only implemented a basic interface. Our purpose in this section is to also provide some directions and ideas for the type of complete analysis system that should be developed. We describe the analysis tools organized into the four categories that we have previously presented: basic timeline analysis, statistical analysis, event correlation analysis and high-level analysis. Our DEFA analysis system is written in Python. The analysis tools all use the *feature spatiotemporal timeline* as the basic logical data (See Figure 2). The raw data extracted from the iPhone related to any specific feature is actually a complex record that provides data elements such as creation date, start date, end date and value. From this data, we create the basic spatiotemporal timelines. We support values indexed by time & location such as heart rate. We also support values indexed by a time interval [time1, time2] & location such as step count.

5.1. Basic timeline analysis

For basic timeline analysis we support the ability to show a graph plot of timeline data for any set of features in the database. The key aspect of support tools in this class is that they primarily consider individual timelines and related data as well as displaying sets of timelines with capabilities to zoom in/out of the timelines. Consider the following question: was the suspect using a smartwatch on March 3rd from 1 AM to 11 PM? Assume we know that data exists from the suspect's smart home thermostat that indicates heating/cooling values set by the suspect's smartwatch and suspect's smartphone. We also have timeline data of the suspect's heart rate. We can plot these features as time series data on the same graph for the period of time (see Figure 3). Note that in Figure 3 HVAC Setting represents the Nest Thermostat heating/cooling values extracted from the Nest iPhone App. INFERENCE#1. Watch was not worn but phone was with the user. User was active and walking. INFERENCE#2. Watch was worn. INFERENCE#3. Watch was not worn but phone was with user.

5.2. Statistical timeline analysis

Tools in this class use statistical processing on time series data defined by the timelines to answer queries.

First consider statistics on a single timeline. Continuing with the suspect example we might next choose to compare if the mean heart rate on March 3rd is the same as on several other days for which a quick view shows no special obvious variation of the heart rate. This could confirm that it was not someone else that made the temperature changes while using the suspect's watch. Our tools for statistical analysis of the time series data can do auto-correlation, lag plot, trend analysis and seasonal pattern analysis. In addition we support tools that can find statistical correlations across timelines. Suppose we are interested in checking if the number of steps walked by the user (recorded by phone/watch), the heart rate (recorded only by the watch) and the number of calls made are correlated on Sundays. We might find that the heart rate and number of steps are correlated but the number of calls made seems uncorrelated.

5.3. Event analysis

Event analysis tools use multiple timelines to "correlate" events but not in the sense of statistical correlation. For example the query "was the heart rate of the victim unusual (out of a given range) when the suspect was at a particular location."

On a random sample data set of user's location over time during a day, we arrived at a geo-plot based on spatio-temporal analysis which can provide insights about user's location pattern over time (see Figure 4). For experimental purposes, this data was coupled with heart rate and step count data, for a person that is doing his regular daily activities and then suddenly starts running. In this example, by overlaying the activity data plot on the spatio-temporal plot, the investigator will be able to infer that between 9 pm (when the user was at the pool) and 10 pm (where the location of the person is UNKNOWN), something unusual had happened which triggered the person to start running at a high speed. The sub-plot in Figure 4 shows the heart rate/step count that has been plotted at 5 minutes intervals, and shows both hear rate value and step count have suddenly increased.

5.4. High-level analysis

This is a catch-class for tools that do complex analyses with the data. Tools in this class could be derived from machine learning or AI approaches. There is significant work currently going on related to psychological and emotional states of persons, derivable from information such as health data, environmental data, voice trace data etc. For example, Salekin et al. ([31], [23]) explore deriving social anxiety level and agitation level based on voice data together with health data derived from IoT devices and wearables. Lundholm et al. [32] show that alcohol and drug use can trigger violence. Researchers from Harvard University suggest that the heart rate variability measurement can be used to understand how one's behavior can affect the nervous system. According to their article [33], a high HRV indicates that the person is in a relaxed state, and a low HRV indicates that the person is in some kind of stress. The effects of stress and heart rate variability (HRV) has been studied by several researchers ([34], [35], [36]). As tools become sophisticated enough to be useful in digital forensics cases, we would propose adding them to this class to make the data more understandable to investigators. An investigator might not easily notice the high HRV value by looking at the raw data, but if the tool marks the high HRV values on the plot as 'stressed', it might help the investigator to pay closer attention to those points in time to see what had affected the victim/suspect at that time.

5.5. Use of DEFA in criminal cases

In this section, we discuss seven different real-world and recent criminal cases to showcase how our data extraction approach can be helpful in solving cases. Fitness tracker data from smart wearable devices has been previously used in court to challenge individual's self-reports of actions [37] and prove physical impact in personal injury lawsuits. From the cases mentioned here, it is evident that data recovered from wearable and smartphone devices can shed light on various activities performed by an individual before and after a crime.

Case-1. Wearable device data from Fitbit was used as an evidence in the court of law for the first time by a law firm in Canada to show their client's activity level was less than usual as a result of an injury [38]. In this case the lawyers were able to show that the activity level of their client, who was a personal trainer was in fact even less than that of an average person. Using DEFA, the Fitbit activity timeline would show a low level of activity. Furthermore, mean activity level could also be determined and compared with either previous activity if such data existed or compared with general population activity. Additionally, Fitbit heart rate data could also be correlated with activity data to confirm low levels of activity.

Case-2. In March 2015, Risley reported that she was pulled out of bed and attacked [37]. Her Fitbit record showed that she had been awake and walking around the entire night. She was charged with filing a false police report and false alarms for public safety. Using DEFA, Fitbit timelines for features such as walking and sleep would have been used. If the home had smart home devices equipped with motion sensors, smart bulbs,

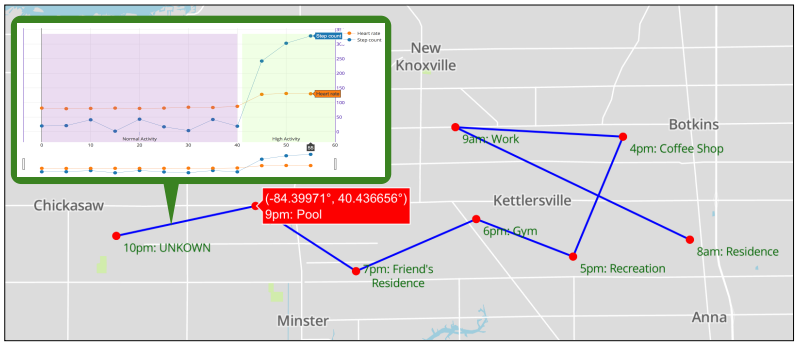

Figure 4. Geo-plot with activity data

cameras, etc., these feature timelines could correlate with the walking activity. Additionally the Fitbit heart rate timeline could be used to confirm likelihood of no attack.

Case-3. In an investigation [39] in Germany during January 2018, data from the Health app was used as evidence in a rape and murder case. In the trial, investigators alleged that the suspect had disposed of the victim's body in a river. Excerpt from the case report [40]: "The app records how many steps he took and what kind of activity he was doing throughout that day. The app recorded a portion of his activity as 'climbing stairs,' which authorities were able to correlate with the time he would have dragged his victim down the river embankment, and then climbed back up. Freiburg police sent an investigator to the scene to replicate his movements, and sure enough, his Health app activity correlated with what was recorded on the defendant's phone." The suspect's smartphone was connected to a single reception tower during this linking him to the crime scene. Using DEFA, statistical correlation of suspect's timeline and investigator's replicated timeline for several features would be done. Location information would indicate the path taken. Previous suspect data on normal climbing and descending times could be compared with those in the case.

Case-4. In 2018 forensic investigators used the heart rate data from Apple watch of the victim - who was murdered in Australia in 2016 - and were able to narrow down the exact moment Myrna was attacked and murdered [41]. The article reports that the heart rate data showed a high burst of heavy activity (consistent with being attacked), and a period of slow activity (when the victim lost consciousness), and then the watch stopped recording heart rate. This led to the arrest of Caroline (the victim's daughter-in-law), since the timeline obtained from the watch contradicted her story that her mother-in-law was arguing with a group of men after a road rage accident. Using DEFA, timelines from the victim's watch would indicate the attack event and location of watch as being consistent with the events described. iPhone data could verify independently location of the smartphone and any syncing activity.

Case-5. Fitbit data was used in a murder of a woman to contradict her husband's story in 2015 [42]. Richard claimed that an intruder broke into their home, tied him to a chair and shot his wife when she returned home. Investigators used the wife's Fitbit data along with the alarm system logs to determine the timelines of events that day. The wife's movement timeline along with her cellphone connection data to their home WiFi contradicted the husband's story, as it indicated that she was at home all the time. Investigators charged Richard with murder and false statements. Using DEFA, the victim's Fitbit timelines would clearly indicate the victim's activity of not leaving home and time of murder. Timelines from smart home devices and Richard's smartphone could confirm that Richard was in fact not tied up during the period claimed.

Case-6. In September 2018, a 90-year old man was charged for the murder of his stepdaughter using the data from the Fitbit the victim was wearing [43]. Anthony told police that he went to his stepdaughter's house on September 8 to drop off pizza. Karen was found dead 5 days later in her home. The Fitbit fitness tracker showed her heart rate spiked on September 8 around the same time Anthony was visiting her. Then the data showed a slow down in the heart rate and stopping 5 minutes before Anthony left her house. Using DEFA, timelines from the victim's Fitbit would indicate when the attack happened exactly. The suspect's watch would also be correlated with this data to see if the spike of heart rate is consistent in both.

Case-7. In September 2016, an Ohio man told authorities he awoke to find his home burning [33]. He was later charged with arson and insurance fraud since investigators used the data from his pacemaker to show

that his heart rate and cardiac rhythms indicated he was awake at the time he claimed he was sleeping. Using DEFA, timelines from smart home devices and heart rate and step counts would indicate activities of the victim consistent with the victim not sleeping.

5.6. From analysis to inference

The real-world criminal cases discussed in the previous section showed mainly how data from wearables and the smartphone was used to aid the criminal investigation. From the DEFA analysis perspective the analysis tools were primarily basic timeline analysis to help the investigator make appropriate inferences about the state of a user at a specific time, or whether a user was wearing a wearable device during a certain time period. In figure 3, we had shown how such inferences can be automatically shown on a graph. We used the presence of heart rate data to infer whether the watch was worn by the user or not. We also plotted some features that can be relevant such as step count, heart rate and HVAC settings performed using the Nest app. The presence of step count data can infer whether or not the user was carrying the phone, and whether or not the user was active and walking at that time. Inferring whether the user changed the home HVAC settings manually is also possible since source device information is part of the data extracted. More complex inferences may also be possible in a more sophisticated inference engine.

5.7. Implications for research

Although the ability to do appropriate extraction of data from wearables and IoT devices for forensic investigations is becoming well understood, the situation for analysis is not so clear. Types of analyses that can be useful are not clearly defined, questions that can be asked and answered by automated analysis systems are not obvious and even the types of queries that forensic investigators should be able to ask are not known. Each of these are important areas for further research.

5.8. Implications for practice

Digital forensics investigators are facing increasing workloads because of the large and varied digital forensic data that is becoming available. Investigators are already struggling to keep their forensic data recovery tools extensive enough to include information stored on wearable/IoT/handheld devices. Thus it is important that developers of forensic tools work with researchers to develop ideas and procedures as to how automated systems might support their investigative procedures and more specifically aid in the inference process to support determining the culpability or not of suspects.

6. Conclusion

Our own future research agenda is the more sophisticated DEFA system that we have outlined. We believe that a more comprehensive version of our system with a friendly user interface can be a very useful addition to the digital forensics investigator's toolkit.

References

[1] S. Crucius, "Wearable tech is here to stay with a robust presence in the future healthcare industry." `https://www.wearable-technologies.com`, 2018.

[2] Egham, "8.4 billion connected things." `www.gartner.com/newsroom/id/3598917`, 2017.

[3] S. Aggarwal, G. Dorai, U. Karabiyik, T. Mukherjee, N. Guerra, M. Hernndez, J. Parsons, K. Rathi, H. Chi, T. Aderibigbe, and R. Wilson, "Design and implementation of a targeted data extraction system for mobile devices," in *Advances in Digital Forensics XV. (Proceedings 15th IFIP WG 11.9 Int.Conf., Jan 2019)*, Springer, 2019.

[4] G. Dorai, S. Houshmand, and I. Baggili, "I know what you did last summer: your smart home internet of things and your iphone forensically ratting you out," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, p. 49, ACM, 2018.

[5] 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*, pp. 303–311, IEEE, 2015.

[6] C. Luo, J.-G. Lou, Q. Lin, Q. Fu, R. Ding, D. Zhang, and Z. Wang, "Correlating events with time series for incident diagnosis," in *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1583–1592, ACM, 2014.

[7] J. Han, J. Pei, and M. Kamber, *Data mining: concepts and techniques*. Elsevier, 2011.

[8] H. R. Motahari-Nezhad, R. Saint-Paul, F. Casati, and B. Benatallah, "Event correlation for process discovery from web service interaction logs," *The VLDB JournalThe International Journal on Very Large Data Bases*, vol. 20, no. 3, pp. 417–444, 2011.

[9] J.-G. Lou, Q. Fu, S. Yang, J. Li, and B. Wu, "Mining program workflow from interleaved traces," in *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 613–622, ACM, 2010.

[10] G.-S. Lin and J.-F. Chang, "Detection of frame duplication forgery in videos based on spatial and temporal analysis," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 26, no. 07, p. 1250017, 2012.

[11] Y. Jin, "Timeline analysis for android-based systems," *Kongens Lyngby*, 2013.

[12] D. Kasiaras, T. Zafeiropoulos, N. Clarke, and G. Kambourakis, "Android forensics: Correlation analysis," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pp. 157–162, IEEE, 2014.

[13] Magnet-Forensics. www.magnetforensics.com/, 2019.

[14] B. Carrier, "Timeline analysis." https://www.sleuthkit.org/autopsy/timeline.php, 2019.

[15] Cellebrite, "Cellebrite-analytics." https://www.cellebrite.com/en/analytics/, 2019.

[16] K. E. Vinez, "The admissibility of data collected from wearable devices." https://www2.stetson.edu/advocacy-journal/wp-content/uploads/2017/06/Vinez_-_Wearables.pdf, 2017.

[17] T. R. Paranjpe, "Social media, smart devices, and their use for trial strategies." http://www.texasbarcle.com/cle/OLViewArticle.asp?a=190461&t=PDF&e=15479&p=1, 2017.

[18] N. Chauriye, "Wearable devices as admissible evidence: Technology is killing our opportunity to lie," *Catholic University Journal of Law and Technology*, vol. 24, no. 2, p. 9, 2016.

[19] NFSTC, "A simplified guide to digital evidence." http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf, 2009.

[20] NIJ, "Electronic crime scene investigation: A guide for first responders, second edition." https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, 2008.

[21] S. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things," in *Services Computing (SCC), 2015 IEEE International Conference on*, pp. 279–284, IEEE, 2015.

[22] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)," in *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*, pp. 356–362, IEEE, 2016.

[23] A. Salekin, H. Wang, K. Williams, and J. Stankovic, "Dave: detecting agitated vocal events," in *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, pp. 157–166, IEEE Press, 2017.

[24] S. Caldwell, "Everything the apple watch can do without an iphone." www.imore.com/heres-what-apple-watch-can-do-without-iphone, 2017.

[25] M. Szulecki, "libimobiledevice." http://www.libimobiledevice.org, 2018.

[26] Apple, "A bold way to look at your health." https://www.apple.com/ios/health/, 2019.

[27] Google, "Developer guide geolocation api." https://developers.google.com/maps/documentation/geolocation/intro, 2018.

[28] G. A. Elmes, G. Roedl, and J. Conley, *Forensic GIS: the role of geospatial technologies for investigating crime and providing evidence*, vol. 11. Springer, 2014.

[29] D. Quick and K.-K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digital Investigation*, vol. 11, no. 4, pp. 273–294, 2014.

[30] K. Fowle and D. Schofield, "Visualising forensic data: Investigation to court," 2011.

[31] A. Salekin, J. W. Eberle, J. J. Glenn, B. A. Teachman, and J. A. Stankovic, "A weakly supervised learning framework for detecting social anxiety and depression," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 2, p. 81, 2018.

[32] L. Lundholm, U. Haggård, J. Möller, J. Hallqvist, and I. Thiblin, "The triggering effect of alcohol and illicit drugs on violent crime in a remand prison population: a case crossover study," *Drug and alcohol dependence*, vol. 129, no. 1-2, pp. 110–115, 2013.

[33] J. Jouvenal, "Commit a crime? your fitbit, key fob or pacemaker could snitch on you." https://www.health.harvard.edu/blog/heart-rate-variability-new-way-track-well-2017112212789, 2017.

[34] J. Delaney and D. Brodie, "Effects of short-term psychological stress on the time and frequency domains of heart-rate variability," *Perceptual and motor skills*, vol. 91, no. 2, pp. 515–524, 2000.

[35] N. Hjortskov, D. Rissén, A. K. Blangsted, N. Fallentin, U. Lundberg, and K. Søgaard, "The effect of mental stress on heart rate variability and blood pressure during computer work," *European journal of applied physiology*, vol. 92, no. 1-2, pp. 84–89, 2004.

[36] H.-G. Kim, E.-J. Cheon, D.-S. Bai, Y. H. Lee, and B.-H. Koo, "Stress and heart rate variability: A meta-analysis and review of the literature," *Psychiatry investigation*, vol. 15, no. 3, p. 235, 2018.

[37] M. Snyder, "Police: Woman's fitness watch disproved rape report." https://www.abc27.com/news/police-womans-fitness-watch-disproved-rape-report/1107961245, 2015.

[38] P. Olson, "Fitbit data now being used in the courtroom." https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#26c1d88b7379, 2016.

[39] S. Cole, "Apple health data is being used as evidence in a rape and murder investigation." https://motherboard.vice.com/en_us/article/43q7qq/apple-health-data-is-being-used-as-evidence-in-a-rape-and-murder-investigation-germany, 2018.

[40] P. Kuhn, "The version of acting in the affect is obsolete with the today." https://www.welt.de/vermischtes/article172287105/, 2018.

[41] N. Y. Post, "Victims apple watch data used as evidence in murder trial." https://nypost.com/2018/04/02/authorities-used-apple-watch-data-to-identify-a-murder-suspect/, 2018.

[42] A. Watts, "Cops use murdered woman's fitbit to charge her husband." https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html, 2017.

[43] C. Hauser, "Police use fitbit data to charge 90-year-old man in stepdaughter's killing." https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html, 2018.