TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Kehinde Omotola Adebayo (174449IVSB)

DIGITAL FORENSIC ANALYSIS OF SMART WATCHES

Bachelor's Thesis

Supervisor: Hayretdin Bahsi
Research Professor

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kehinde Omotola Adebayo (174449IVSB)

NUTIKELLADE DIGITAALKRIMINALISTIKA

Bachelor’s Thesis

Juhendaja: Hayretdin Bahsi
Research Professor

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kehinde Omotola Adebayo

30.04.2020

Abstract

As wearable technology is becoming increasingly popular amongst consumers and projected to continue to increase in popularity they become probable significant source of digital evidence. One category of wearable technology is smart watches and they provide capabilities to receive instant messaging, SMS, email notifications, answering of calls, internet browsing, fitness tracking etc. which can be a great source of digital artefacts. The aim of this thesis is to analyze Samsung Gear S3 Frontier and Fitbit Versa Smartwatches, after which we present findings alongside the limitations encountered.

Our result shows that we can recover significant artefacts from the Samsung Gear S3 Frontier, also more data can be recovered from Samsung Gear S3 Frontier than the accompanying mobile phone. We recovered significant data that can serve as digital evidence, we also provided a mapping that would enable investigators and forensic examiners work faster as they are shown where to look for information in the course of an investigation. We also presented the result of investigating Fitbit Versa significant artefacts like Heart rate, sleep, exercise and personal data like age, weight and height of the user of the device, this shows this device contains artefacts that might prove useful for forensic investigators and examiners.

This thesis is written in English and is 42 pages long, including 6 chapters, 7 figures and 4 tables

Annotatsioon

Nutikellade digitaalkriminalistika

Kantav tehnoloogia on saamas tarbijate hulgas üha aina populaarsemaks ning eeldatakse, et populaarsuse kasv jätkub, millega muutuvad nad tõenäoliselt oluliseks digitaalsete tõendite allikaks. Üheks kantava tehnoloogia kategooriaks on nutikellad ja nad võimaldavad võtta vastu sõnumeid, SMS-e, e-posti teateid, kõnedele vastamist, Interneti sirvimist, treeningute jälgimist ning paljut muud, mis võivad olla suurepärased digitaalsete andmete allikad. Antud lõputöö eesmärk on analüüsida Samsung Gear S3 Frontier ja Fitbit Versa nutikellasid, mille järel tutvustame tulemusi koos ilmnenud piirangutega.

Meie tulemus näitab, et suudame Samsung Gear S3 Frontierilt olulisi andmeid taastada, samuti saab Samsung Gear S3 Frontierilt taastada rohkem andmeid kui sellega kaasasolevalt mobiiltelefonilt. Saime taastada olulisi andmeid, mida saab kasutada digitaalse tõestusmaterjalina. Esitasime ka kaardistuse, mis võimaldaks uurijatel ja kohtuekspertidel kiiremini töötada, kuna neile näidatakse, kust uurimise käigus teavet otsida. Tutvustasime ka Fitbit Versa uurimistulemusi.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 42 leheküljel, 6 peatükki, 7 joonist, 4 tabelit.

List of abbreviations and terms

ADB	Android Debug Bridge
AMOLED	Active Matrix Organic Light Emitting Diode
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
IoT	Internet of Things
LCD	Liquid Crystal Display
NFC	Near Field Communication
OS	Operating System
PC	Personal Computer
PIN	Personal Information Number
ROM	Read Only Memory
SDB	Smart Development Bridge
SDK	Software Development Kit
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
VR	Virtual Reality
Wi-Fi	Wireless Fidelity

Table of contents

List of figures

List of tables

1 Introduction

The Wearable Technology is probably going to become increasingly popular when we take a look at the future of our daily lives. People are using different types of wearable technology products like Health and Fitness Trackers, Smartwatches, Smart Glasses, VR Headsets, Wireless Headphones and Earbuds, Smart Running Shoes, and much more. Most of all, wearable technology is growing, and it'll likely become a part of our lives very soon like as our Android or IOS device, and other Smartphone accessories [1].The number of connected wearable devices worldwide has more than doubled in the space of three years, increasing from 325 million in 2016 to 722 million in 2019. The number of devices is forecast to reach more than one billion by 2022 [2].

Growth within the wearable devices market is primarily being powered by sales of smartwatches – shipments of smartwatches worldwide are forecast to surpass 100 million in 2020. Apple, who unveiled their first smartwatch in 2015, currently dominate the smartwatch market and have held a share of around 45 percent since 2018. Another reason for the growth of the wearables market is the rise in popularity of hearable devices. Also referred to as ear wear or ear-worn devices, this category is expected to soar over the next few years with shipments of devices forecast to increase by 45 percent to 105 million units by 2023 [2]. Digital forensics has proven to be crucial to breaking into evidence in the course of an investigation of a 19-year-old medical student Maria Ladenburger murdered in October 2016, the health data app on the iPhone of the suspect was used to correlate evidence, the phone suggested periods of more strenuous activity, including two peaks, which the app put down to him climbing stairs [3].

The data from the Fitbit of a woman was used to prove that she lied about her claims in a case, the woman who reported she was raped by an intruder was criminally charged after police claim her fitness watch proved the story was made up. It proved that she was walking around during the time she had said she was asleep and dragged from her bed [4]. Also, a man was facing multiple charges of reckless driving after he fled police in a road race. The man was wearing a GoPro camera which recorded the entire event, and he later posted the recorded video on YouTube [5]. We can go on to cite more instances where digital forensics of wearable devices has proven to be useful to forensic investigators.

Although this increased use of smartwatch wearable devices may lead to more convenience and efficiency for end-users, it also presents many new obstacles for forensic digital examiners to overcome as wearable use also become more prevalent in civil and criminal cases. Police departments are now finding that victims tend to own up to three smart devices, as do suspects and witnesses, leading to greater amounts of personally sensitive data being created, modified and accessed leading to potentially more evidence sources to be analyzed [6].

1.1 Problem Statement

As wearable devices are becoming popular and projected to continue to increase in popularity they become of interest to law enforcement bodies when carrying out investigations and for incidence handling in organizations. Digital forensics isn't a straightforward process it is usually a very tedious process as it is time consuming and can lead to delay in solving a case without the right tools. Both investigators and incidence handlers usually need tools that would enable them work faster and differentiate between artefacts found on devices.

There is not one-size-fits-all tool that is used for data extraction and analysis in forensics. New types of devices constitute problems and tools do not deal with all of them, especially new IoT devices like wearable devices. Smart watches contain sensors like barometer, gyroscope, heart rate monitor and pedometer all of which record data about users activity. This study aims at investigating how much user's sensitive or personal data that can be retrieved through a digital forensics of the smart watch.

1.2 Goals of the thesis

The goals of this thesis are to

1. Determine the artefacts that can be found on Samsung Gear Frontier S3, the companion Samsung Galaxy S9 plus mobile phone in rooted and unrooted scenarios and also artefacts that can be found on Fitbit Versa.

2. Provide a guideline for forensic examiners by providing mapping of where to look when working on these devices in order to save them both cost and time.

1.3 Outline of the thesis

The thesis is organised into chapters. Chapter one provides introduction to topic, problem statement and defines the goal of the thesis. Chapter two gives technical background into the internals of mobile phones and wearable devices. Chapter three describes the materials and methodology used during the research process as well as describes the different scenarios of extraction attempted in the course of the research.

In chapter four, the artefacts recovered from Samsung Gear S3 frontier, Galaxy S9 and Fitbit Versa are analysed and results presented. Chapter five concludes the thesis while Chapter six discusses possible further improvement on the work.

2 Background Information

2.1 Literature Review

Multiple studies have endeavoured to perform digital forensic on different smartwatches in order to determine what artefacts can be obtained from these devices. Smart watches, fitness bands and wearable device forensics is becoming of great interest to digital forensic investigators examiners as they are becoming popular and have become a major store of digital information that produce digital evidence. In 2011, research investigating third-party mobile applications on the iPhone was conducted [7]. The work focused on analysing built-in application data stored in files in formats like databases, JSON and XML

Researchers have also carried out studies which examined the extent that data is stored on phones connected to cloud services and to determine if users should be concerned about their data being left and accessible on their smart phones even after it has been synced to the cloud [8]. Other works identified areas where digital mobile forensics guidelines and standard could be refined [9].

Previous studies have shown that data such as e-mails, contacts, events, health and fitness information can be extracted from the artefacts acquired from paired wearable devices, this makes the forensic value of these devices worthy of investigation [10]. Additional studies focused attention to specific mobile operating systems, primarily the two most popular ones; iOS and Android. There has also been work that examined the logical backup of the iPhone 3GS and its forensic value [11].

Similar studies have been performed on the acquisition of smartwatch device data while some are not so detailed others employed manual acquisition process which limits the examiners to only what he can see on the screen [12]. Considering these limitations, we therefore need a much more detailed study and mapping for the acquisition of data directly from smartwatch wearable devices and paired devices, this is valuable to forensics investigators as it would save them cost and time in the course of their investigations as this study provides an insight into the potential evidence that can be discovered on smartwatch wearable devices and where to look for them.

2.2 Smartwatch definition

A smartwatch is like a mini computer and mini smartphone because it has both the features of computer and smartphone within a single watch. It can perform the smart task just like a computer. It has a touchscreen display for the interface. We can install applications, games, and videos via internet access in it [13]

A smartwatch has many features on top of time keeping, the digital watch allows you to monitor components such as heart rate, activity tracker, and reminder. A smartwatch has a touch screen that allows its user to perform actions through tapping or swiping on the screen. The watch consists of multiple apps similar to the applications available to smartphones. These applications extends to watches functionality such as stock prices and map displays, weather information.

Majority of smartwatches also have the capability of receiving text messages and making calls. The smartwatch requires a smartphone to function even though these applications run directly on the smartwatch. The phone is the first to receive the data then it is sent to the watch, because most smartwatches do not contain a SIM card or have Wi-Fi for cellular data the applications must rely on a smartphone which is compatible to provide the necessary data over Bluetooth connection [14]. They may contain sensors, LCD or AMOLED displays, volatile and non-volatile memory and the OS range from Google Android Wear, Huawei wearable platform, Tizen and WatchOS.

2.3 Technical background and definitions

2.3.1 ROM

ROM is abbreviation for Read Only Memory. A "ROM" is the operating system software that runs your smartwatch or smartphone. It is stored in the “Read Only Memory” portion of the hardware on both devices. This ROM comes in two forms: Stock ROM and Custom ROM.

2.3.1.1 Stock ROMs

Stock ROMs are the ones which come by default in smartwatches or smartphones. These are customized versions of ROM developed by manufacturers and carriers to let users stick to their devices with unique looks and features. The "out-of-the-box" smartphones and smartwatches are all shipped with stock ROM e.g. Samsung devices.

2.3.1.2 Custom ROMs

Custom ROMs are the ones which are customized or developed from the original source code of Android. Custom ROMs are not provided by Google or other mobile vendors but are developed and maintained by community and its contributors. [15]

2.3.2 Sensors

Sensors are at the core of smartwatches, and are the primary means by which watches input data. Mei Weixin of Mifree Technology said that smartwatches are sensors [16]. Sensors for smartwatches differ from those for other mobile electronic products as they offer unique features such as pedometer, heart rate monitoring, humidity test, UV test and temperature test.

Typically, sensors can be divided into three categories:

- **Biosensors:** These include glucose, blood pressure, ECG, EMG, temperature and brain wave sensors
- **Motion sensors:** Examples include acceleration, gyroscope, geomagnetic, and atmospheric pressure sensors
- **Environmental sensors:** For example, temperature and humidity, gas, PH, ultraviolet, ambient light, dust particles, and pressure sensors, as well as microphones

A sensor gathers and transmits data to the display processor or CPU [16].

2.3.3 Difference between Rooted and Unrooted Devices?

Rooting is a process allowing users of Smartphone’s, Smartwatches, tablets, and other devices running an operating system to attain privileged control (known as “root access”) within such OS. Basically rooting is performed to overcome the limitation that **wireless service providers** and **hardware manufacture** of android phone put on some devices. If a smartwatch is rooted that means it gives super users access and you have ability to customize or replace system application and settings the way you want to do. This little word rooting provide you power to run specialized apps that require administrator-level permissions and perform another operation which are inaccessible to unrooted device. Basically “root” term comes from the Unix/Linux world which is used to describe a user who has “super users” rights or permission to all the files and programs in the Android OS [17]. Meanwhile in an unrooted device such super user access is not possible as the device is locked by the manufacturer

2.4 Volatile vs Non-Volatile Memory

From the storage perspective, memory can be categorized as non-volatile and volatile. Non-volatile memory (NVM) is capable of retaining data even after power is removed and generally has a lower speed than volatile memory. Volatile memory, on the other hand, does not retain data after power is removed and has higher per-bit storage costs. Therefore, volatile memory is usually used for primary storage when the memory interacts with a system-on-chip (SoC) frequently, while NVM is used for secondary/mass storage. However, this rule of thumb may be changing because NVM is now becoming faster and cost per byte is going down, leading to its usage for primary storage as well. With the advent of new IoT applications, designers need to continue to review the available options and decide on their memory type based on the application requirement [18].

3 Methodology

We decided to work on these device as Gear S3 and Fitbit Versa have a considerable market share and thereby constitute a significant portion of forensic investigation landscape, we have employed a post-mortem approach to our investigation.

According to National Institute of Standards and Technology Guidelines on Mobile Device Forensics [19], understanding the various types of mobile acquisition tools and the data they are capable of recovering is important for a mobile forensic examiner. It also provides a framework for forensic examiners to compare the extraction methods used by different tools to acquire data. The tool classification system is displayed in **Figure 1**. As the pyramid is traversed from the bottom, Level 1, to the top, Level 5, the methodologies involved in acquisition become more technical, invasive, time consuming and expensive.

Level 1, Manual Extraction methods involve recording information brought up on a mobile or smart device screen when employing the user interface. This was important in identifying the type of evidence that can potentially be stored on a device, since there are no general knowledge of what information is stored on different smart watches. Although this was not sufficient in our case as we need to preserve the information extracted as well it was a necessary pointer to the kind of data that can be obtained. Level 2, Logical Extraction methods are used most frequently at this time and are mildly technical, requiring beginner-level training this was employed in this research.

Methods for levels 3 to 5 entail extracting and recording a copy or image of a physical store (e.g., a memory chip), compared to the logical acquisitions used at level 2 involve capturing a copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition). Level 3, Hex Dumping/JTAG Extraction methods, entail performing a "physical acquisition" of mobile device memory in situ and require advanced training. Level 4

Chip-Off methods involve the physical removal of memory from a mobile or smart device to extract data, requiring extensive training in electronic engineering and file system forensics. Level 5, Micro Read methods involve the use of a high-powered microscope to view the physical state of gates. Level 5 methods are the most invasive, sophisticated, technical, expensive, and time consuming of all the methodologies. [19]

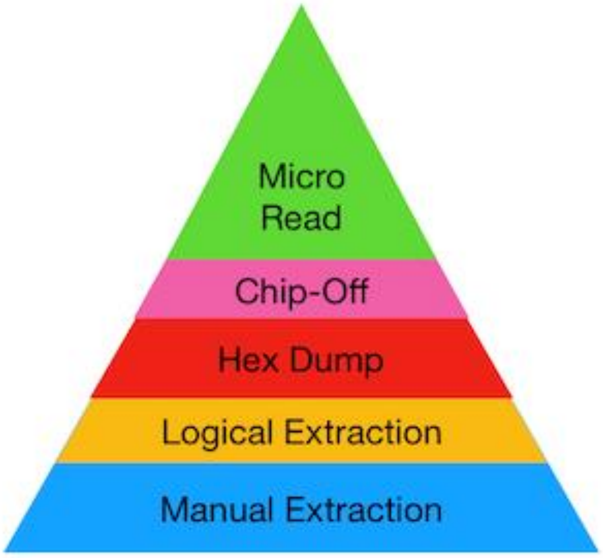


Figure 1 Mobile Device Tool Classification System (Source: https://study.com/academy/lesson/mobile-device-forensics-tool-classification-system-definition-levels.html)

3.1 Devices and Tools

In this section, we provide the description of the devices and tools listed in **Table 1** and **Table 2** used in this experiment. The detailed description of all the devices are not relevant thus we have chosen to explain the relevant ones.

Smart Development Bridge (SDB) is a command line tools that communicated with a connected target wearable device, it is responsible for managing connections with the target device.

- The SDB manages multiple connections with the target devices. You can list connected devices and send a command to a specific device with a serial number that is created by the SDB.
- The SDB supplies basic commands for application development, such as file transfer, remote shell command, port forwarding for a debugger, viewing, filtering, and controlling target log output.

The SDB is a client-server program that consists of a client, daemon, and server:

- Client sends commands to the server. The client runs on your computer. You can invoke the client from a shell by issuing the *sdb* command at the prompt.
- Daemon runs commands on the device. The daemon runs as a background process on each target device.
- Server manages communication between the client and the daemon. The server runs as a background process on your computer.

You can find the SDB tools in the $<TIZEN_STUDIO>/tools/ folder in the installation directory of Tizen Studio. [20]

NetOdin: It is a tool to flash Samsung Firmware Files onto Samsung Devices over a wireless connection. Mainly used for smartwatches, which don't have a wired connection available (e.g.: USB). This is different from Odin, which only works with wired connections, NetOdin uses a wireless connection to transfer the firmware to the device [21].

List of devices and tools:

Brand	Model	Version	Specifications
TP Link	450M Wireless N Router	TL-WR940N	3.19.1 Build 180119 Rel.59618n
Samsung	SM-R760	Gear S3	OS: Tizen Chipset: Exynos 7 Dual 7270 (14 nm) CPU: Dual-core 1.0 GHz Cortex-A53 4GB 768MB RAM
Samsung	SM-G965F	Galaxy S9	Snapdragon 845 / Exynos 9810. RAM: 6GB. Storage: 64GB
Lenovo	T480		Windows OS: Windows 10 Pro 64-bit (10.0, Build 18363)
Fitbit	Versa	Versa	Internal Memory: 2.5GB

Table 1 List of Devices

Author	Tool Name	Version	OS Used	Usage
Google/Android	Android Debug Bridge (ADB)	1.0.41	Windows	Used to interact with the mobile phone to back it up
Nikolay Elenkov	Android Backup Extractor	v20180521	Windows	Used to convert Android backup to a tar archive
René Peinthor Martin Kleusberg Mauricio Piacentini Justin Clift	DB Browser for SQLite	3.32.0	Windows	Used to analyse databases retrieved from the wearable device
Samsung	NetOdin 3	3.1.0	Windows	Used for installing a custom ROM on the wearable device
Samsung	SDB tools	v 3.6	Windows	Used for establishing a connection with Gear S3

Table 2 List of Tools

3.2 Data Extraction Setup

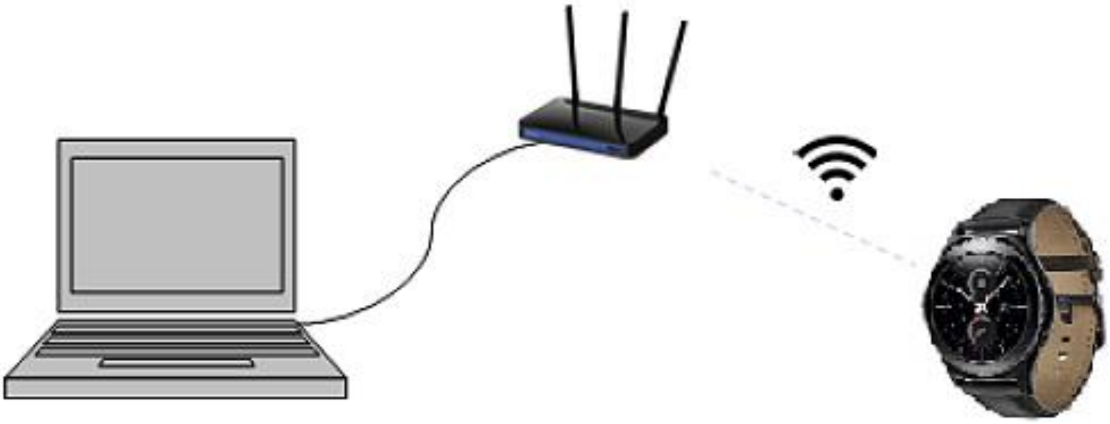


Figure 2 Connecting to Samsung Gear S3 (Source: https://developer.samsung.com/galaxy-watch-develop/testing-your-app-on-galaxy-watch.html)

We have made some assumptions about the Gear S3 and the companion Galaxy S9 it is paired with in this investigation such as;

- It has not been password protected with a PIN or the investigator may learn it from the owner.
- The wearable is used in connected mode which means it’s paired with a mobile phone.
- Data from the wearable device are synchronized with the accompanying Samsung S9 plus.
- The connection between the wearable device and the phone is established using the account of the owner of the mobile phone

3.2.1 Data Acquisition of non-rooted Gear S3

Just after we had the wearable device in our possession proper forensic procedure were observed in other to protect the integrity of data, we ensured flight mode was turned on which would turn off Bluetooth, NFC and Wi-Fi.

Samsung Gear S3 Frontier: This device provides no physical connection ports, it uses wireless connection for charging purposes; thereby extracting any sensitive user data and forensically applicable artefacts was made more difficult by this.

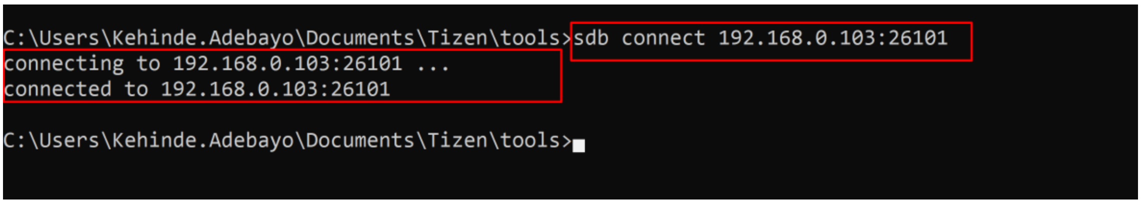
The methodology used in this research for data extraction is outlined below:

The Gear S3 device runs on Tizen OS which is a Linux based mobile operating system by Samsung, there is a Tizen Studio developed for it which can be used for developing apps for the device and also provides tool that serves as a connection bridge to the device. Through the Tizen Studio (v 3.6 Build Time 22.11.2019 11:41) (SDK), it is possible to connect Gear S3 Frontier to a workstation by using the Smart Development Bridge (SDB) device management tool. This approach requires connecting both the Gear 3 and the forensic workstation to the same local network using a Wireless Access Point (WAP), this acts as a USB connection between both devices as shown in **Figure 2**. This WAP was protected and not connected to the Internet in order to prevent data alteration and interference of any form.

Before connecting to the Gear S3 via the development bridge Bluetooth connectivity on the Gear S3 frontier was disabled. Debugging mode (Settings > About Watch > Debugging) and Wi-Fi of the Gear S3 were enabled through the Connection and Gear Info menu under settings and the device was powered off and restarted for it to initialize. At this point both the host PC and Gear S3 Frontier were connected to the WAP and have IPs assigned to them via Dynamic Host Configuration Protocol (DHCP) the IPs assigned were also noted. A terminal on the workstation was utilized to connect the Gear S3 Frontier via the assigned IP and Port 26101 through the SDB commands as shown in **Figure 3**, Port 26101 is standard for connecting to this device.
We used the command *sdb devices* to verify that a connection was established, a message is also displayed on the terminal for a listing connected devices **Figure 4**. The <sdb shell> command was issued to activate an interactive remote shell, since this is a Linux based system most Linux commands work on the device to copy files from Gear S3 Frontier
We used the command sdb -s IpAddress:26101 pull /opt \<OutputFolder>

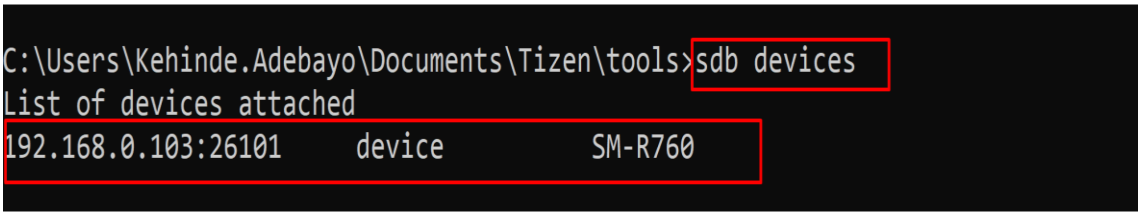
We use logical acquisition on this device as a physical acquisition was not possible because we couldn’t gain root access to the device thereby so many of the folders and files with root privilege could not be accessed. We couldn’t also make a forensic image of the device as this would also requires having root access.

We attempted to develop a Tizen Watch face application to be installed on this device but this won't be a forensically sound approach as it would lead to altering of the file system which would lead to evidence tampering. We also couldn't use the *dd* utility which is a Linux based command line tool for bit by bit copy of files from the device, this operation also requires us having root access.



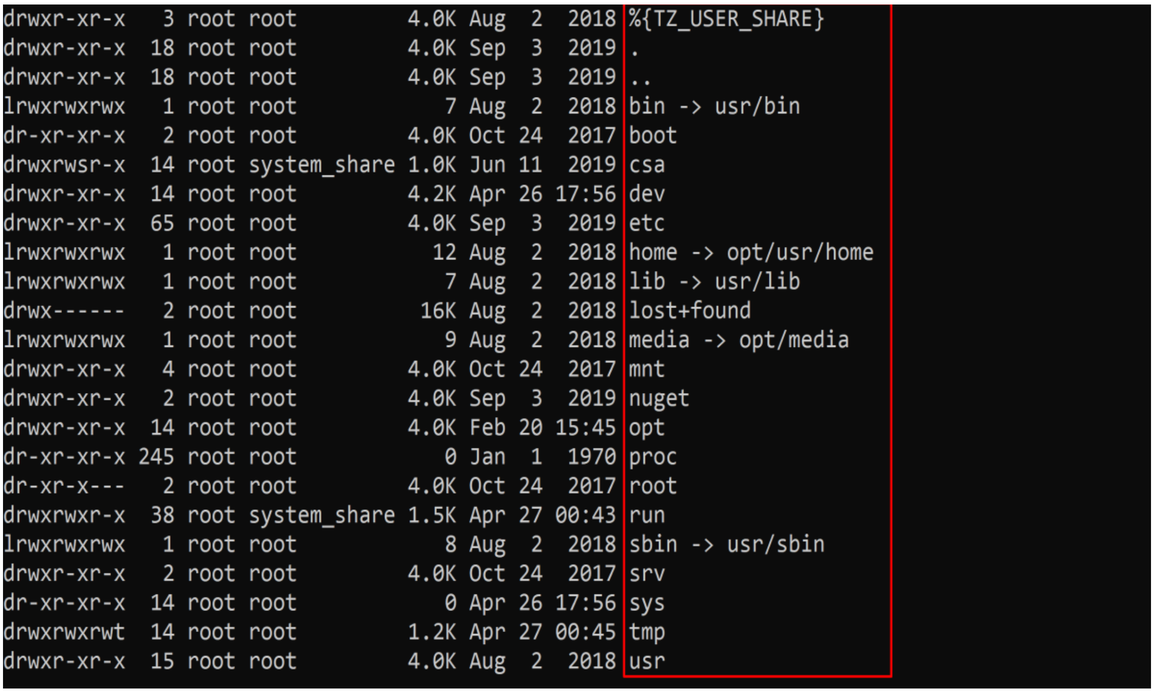
```
C:\Users\Kehinde.Adebayo\Documents\Tizen\tools>sdb connect 192.168.0.103:26101
connecting to 192.168.0.103:26101 ...
connected to 192.168.0.103:26101

C:\Users\Kehinde.Adebayo\Documents\Tizen\tools>
```

Figure 3 Connecting to Gear S3 via *sdb* command



```
C:\Users\Kehinde.Adebayo\Documents\Tizen\tools>sdb devices
List of devices attached
192.168.0.103:26101     device          SM-R760
```

Figure 4 Verifying connection by using sdb devices command



```
drwxr-xr-x   3 root root         4.0K Aug  2  2018 %{TZ_USER_SHARE}
drwxr-xr-x  18 root root         4.0K Sep  3  2019 .
drwxr-xr-x  18 root root         4.0K Sep  3  2019 ..
lrwxrwxrwx   1 root root            7 Aug  2  2018 bin -> usr/bin
dr-xr-xr-x   2 root root         4.0K Oct 24  2017 boot
drwxrwsr-x  14 root system_share 1.0K Jun 11  2019 csa
drwxr-xr-x  14 root root         4.2K Apr 26 17:56 dev
drwxr-xr-x  65 root root         4.0K Sep  3  2019 etc
lrwxrwxrwx   1 root root           12 Aug  2  2018 home -> opt/usr/home
lrwxrwxrwx   1 root root            7 Aug  2  2018 lib -> usr/lib
drwx------   2 root root          16K Aug  2  2018 lost+found
lrwxrwxrwx   1 root root            9 Aug  2  2018 media -> opt/media
drwxr-xr-x   4 root root         4.0K Oct 24  2017 mnt
drwxr-xr-x   2 root root         4.0K Sep  3  2019 nuget
drwxr-xr-x  14 root root         4.0K Feb 20 15:45 opt
dr-xr-xr-x 245 root root            0 Jan  1  1970 proc
dr-xr-x---   2 root root         4.0K Oct 24  2017 root
drwxrwxr-x  38 root system_share 1.5K Apr 27 00:43 run
lrwxrwxrwx   1 root root            8 Aug  2  2018 sbin -> usr/sbin
drwxr-xr-x   2 root root         4.0K Oct 24  2017 srv
dr-xr-xr-x  14 root root            0 Apr 26 17:56 sys
drwxrwxrwt  14 root root         1.2K Apr 27 00:45 tmp
drwxr-xr-x  15 root root         4.0K Aug  2  2018 usr
```

Figure 5 Listing directory structure with *ls -lah* command

3.2.2 Data Acquisition of rooted Gear S3

The Gear S3 watch uses Tizen Operating System which is based on Linux Kernel. Gear S3 has Wi-Fi connection which also serves as USB Bridge to it which can be used to connect the watch to a workstation for copying files from and to the Gear S3, when device is in recovery mode its Wi-Fi connection can also be used to install apps on the device.

The first step in our attempt to gain root access to the device was to first install all the necessary software and tools on our workstation, like sdb tool for communicating with the wearable device via the terminal, for root access the ROM of the device needs to be flashed and there is a tool by Samsung called NetOdin which is used for installing custom ROM on Samsung devices over a wireless connection be it mobile phones or wearable devices, NetOdin was installed on our workstation a connection with NetOdin was established through a wireless AP created when the wearable device was put in [AP Mode]. NetOdin can be obtained from android file host link [22].

Please note there is difference between Odin and NetOdin. NetOdin is a tool to flash Samsung Firmware Files onto Samsung Devices over a wireless connection. Unlike Odin, which only works with wired connections, NetOdin uses a wireless connection to transfer the firmware to the device [21].

Steps for installing a custom ROM

1) On the Samsung Gear Frontier S3 device press then hold the Home/Power button until you see the S3 screen shows up "Rebooting..."

2) Release the Home/Power button then quick Press it again three times.

Next step, you need to be a bit quicker to prevent the device from rebooting.

3) Use the Home/Power button to navigate to "Download (wireless)" option, then Press & Hold the Home/Power button to select. This has to be done quickly otherwise device will reboot.

4) Press the Home/Power button twice, you will see the "[WPS Mode]" change to "[AP Mode]"

5) From the workstation where NetOdin has been installed as described above, in the list of wireless connection choose the Access point with the same name that appears on the S3.

6) S3 will show that it's been connected to the IP of the computer as shown in **Figure 6**.

7) Open NetOdin, the S3 device will show up as shown in **Figure 8**.

8) Choose the right file for each Option from the files that was extracted after downloading the ROM as shown in **Figure 7.** Then press Start and wait for about (15-20 minutes) for the process to complete [23]

Steps 1 – 8 was used to download a new ROM to the device **Figure 6** shows ROM download in progress and after it was done we attempted to connect to the device via sdb, *sdb root on* command was issued but we were still unable to get root access picture in **Figure 7**, we tried several ROMs obtained from online sources [24] and [25] but none was able to give us root access to the device, this is because the downloaded ROMs has not been rooted and we were not able to obtain a rooted custom ROM at the point of this investigation. A similar approach was used to gain root access in Samsung Gear 2 Neo which is an older device also by Samsung with the same operating system as explained in [10].

This is a much recent device and it doesn't have a public custom ROM with root access that can be used to flash the device at least to the best of my knowledge during this research, installing a custom ROM does not seem to impact or tamper with data in the user space as things like emails saved on devices, messages and Wi-Fi passwords were still remembered by the device as we were able to connect to previously connected Wi-Fi connection without needing to enter the passphrase again comparing the hashes of these files can be helpful in establishing this.

After downloading a new ROM the user files appeared to still be intact and not wiped, this is a valuable information for investigators as the procedure above can be used in the future to gain root access when rooted custom ROM is made available.

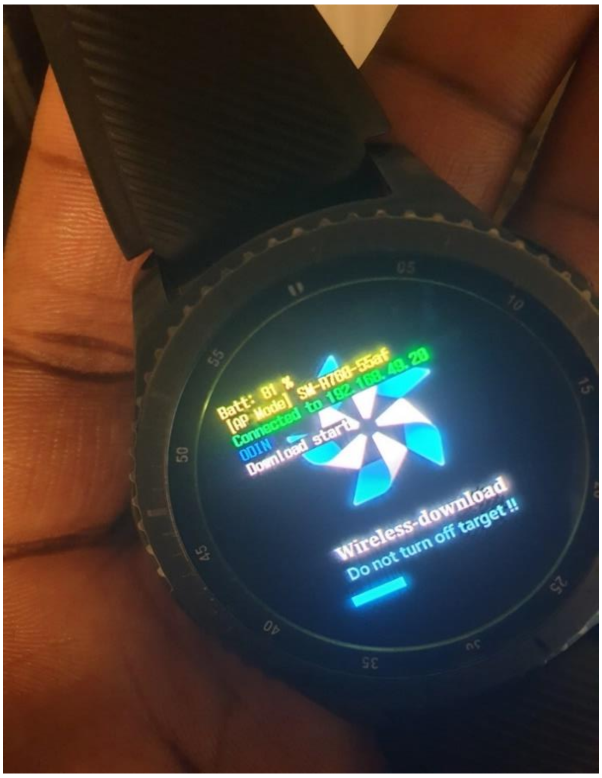
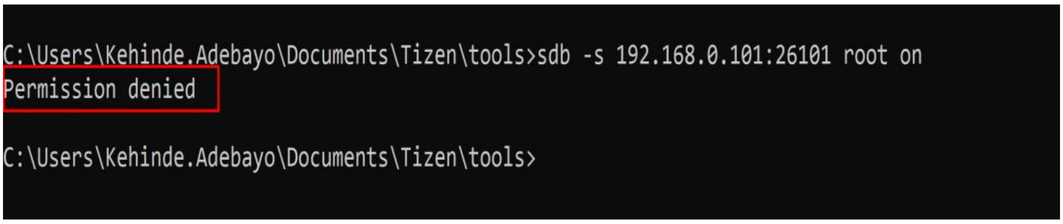
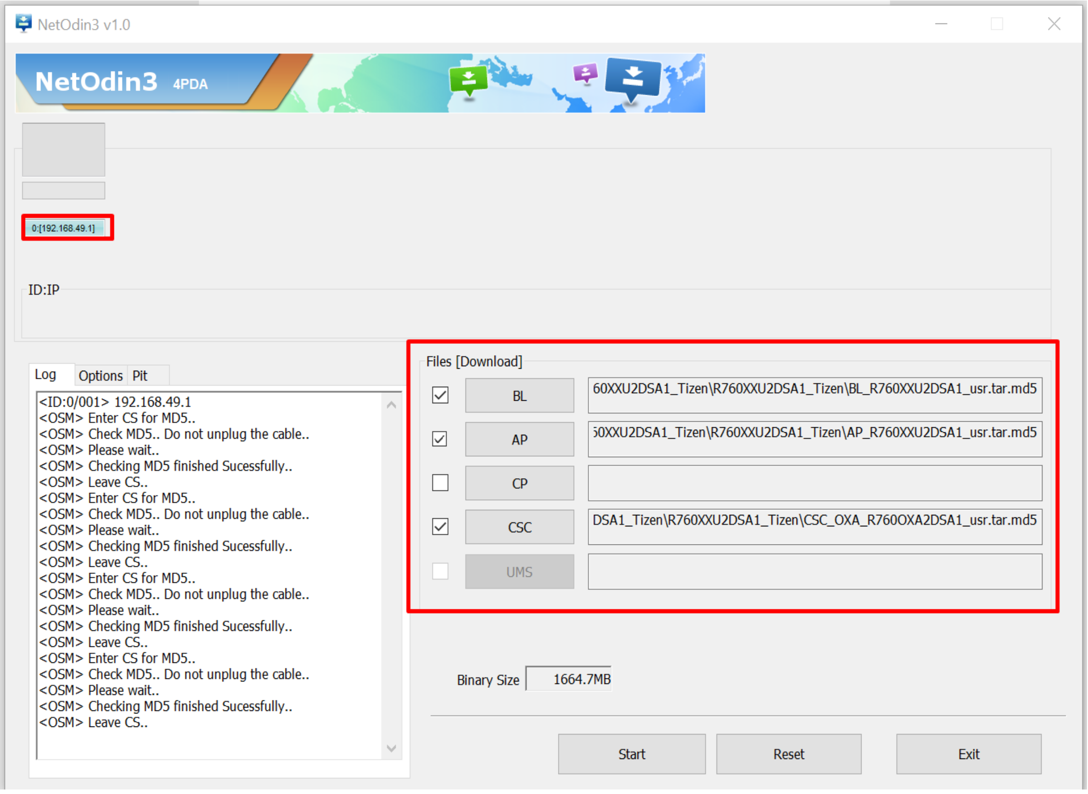


Figure 6 Device connected to computer and downloading a custom ROM



```
C:\Users\Kehinde.Adebayo\Documents\Tizen\tools>sdb -s 192.168.0.101:26101 root on
Permission denied

C:\Users\Kehinde.Adebayo\Documents\Tizen\tools>
```

Figure 7 Failed attempted to get root access on device



```
<ID:0/001> 192.168.49.1
<OSM> Enter CS for MD5..
<OSM> Check MD5.. Do not unplug the cable..
<OSM> Please wait..
<OSM> Checking MD5 finished Sucessfully..
<OSM> Leave CS..
<OSM> Enter CS for MD5..
<OSM> Check MD5.. Do not unplug the cable..
<OSM> Please wait..
<OSM> Checking MD5 finished Sucessfully..
<OSM> Leave CS..
<OSM> Enter CS for MD5..
<OSM> Check MD5.. Do not unplug the cable..
<OSM> Please wait..
<OSM> Checking MD5 finished Sucessfully..
<OSM> Leave CS..
<OSM> Enter CS for MD5..
<OSM> Check MD5.. Do not unplug the cable..
<OSM> Please wait..
<OSM> Checking MD5 finished Sucessfully..
<OSM> Leave CS..
```

Files [Download]

☑ BL 60XXU2DSA1_Tizen\R760XXU2DSA1_Tizen\BL_R760XXU2DSA1_usr.tar.md5

☑ AP 50XXU2DSA1_Tizen\R760XXU2DSA1_Tizen\AP_R760XXU2DSA1_usr.tar.md5

☐ CP

☑ CSC DSA1_Tizen\R760XXU2DSA1_Tizen\CSC_OXA_R760OXA2DSA1_usr.tar.md5

☐ UMS

Binary Size 1664.7MB

Figure 8 Selected files to be downloaded to the device

3.3 Android Forensics

3.3.1 Logical acquisition of non-rooted mobile phone

It is assumed the smartphone is unencrypted and not rooted which means the data recoverable are those ones at a user’s privilege level hence not all of user’s data. Nonetheless using Android Debug Bridge logical acquisition we were still able to recover some data from the device.

In order to establish connection using ADB, we enable USB Debugging on the phone under Settings, this option is available under Developer options of the phone.
If Developer options isn’t visible locate the *Build Number* menu and tap it several time until Developer options is enabled.
With adb tool installed on our workstation we connected it to the mobile phone by changing our working directory using the *cd* command to the folder where the adb tool is installed. If the present working directory is not the adb tool directory you will get the

message ‘adb’ *is not recognized as an internal or external command, operable program or batch file.* Please ensure you are in the right directory.

To do the ADB backup extraction open a command line program like windows command line and type in the terminal *adb backup -shared –apk -all -system -f backup.ab.*
It was necessary to unlock the phone after typing the command, in order to confirm the backup of the data. When the ADB backup is completed, a file called *backup.ab* was created on the workstation, in the format the files are not visible, and the next step is to convert it into an extractable format such at tar. To achieve this we used a tool called Android Backup Extractor by issuing the following command on our windows workstation *java -jar abe.jar unpack <backuppath> <path>backup.tar password*
Note that for this step also we changed our working directory into the directory on the workstation where the tool in installed, *password* part of the command is necessary if the backup has password or else it can be omitted. This command converted the backup file into an extractable tarball, when extracted, we were able to access the following data.

3.4 Data Acquisition of Fitbit Versa

The Gear S3 analysis was done with the device being connected to a Samsung S9 which was also analysed alongside. However, the paired devices are not always available and the devices still need to be analyzed. A second wearable device we analyzed is the Fitbit Versa and the study is done with the assumption that it is not paired with a mobile device. The manual extraction phase is always crucial in identifying the type of evidence that could possibly be stored in the device in the user accounts, NIST framework for mobile forensic specifies that manual extraction should first be done on the device as this is less invasive before moving to the more invasive forms of extraction should that not be sufficient [19].
The Fitbit displays very little information on the device about activities stored on it, the data stored in the user account would therefore be of value to a forensic examiner, this requires the owner granting access their Fitbit account and consenting to it being analyzed. For this analysis we have installed the Fitbit desktop application obtained from the Fitbit website [26], which was instrumental in accessing the database of activities on the device which is located in the path

InstallationDrive\Users\UserName\AppData\Local\Packages\Fitbit.Fitbit_6mqt6hf9g46tw\LocalState\fitbit.8HSV83.db. The database was copied for data extraction and analysis to be carried out on it. The database contained 126 tables, the format of the naming of the database is fitbit.UserID, UserID here is 8HSV83, and this database file is a trove of evidence as it contains several tables that logs user activities.

Some of the interesting tables include: *HeartRateDailySummaryDbEntity, PersonFriendsDbEntity, PersonShortDbEntity, RankedUserDbEntity, SleepLogEntryDbEntity* and *PersonFriendsDbEntity*.

4 Analysis of the results

4.1 Analysis of Gear S3 artefacts

The purpose of the analysis was to see if we can find data that could be supportive in an investigation. We performed a file system extraction on the Gear Frontier S3. After we have copied files, analysis was performed. All files and folders that are of forensics value as well as the data that can be found in them are provided in Table 3.

When we typed the command *cd /* to the terminal after issuing *sdb shell* command we were taken to the root directory and we issued *ls -lah* command these directories were listed %{TZ_USER_SHARE}, bin -> usr/bin, boot, csa, dev, etc, home -> opt/usr/home,

lib -> usr/lib, lost+found, media -> opt/media, mnt, nuget, opt, proc, root, run, sbin -> usr/sbin, srv, sys, tmp, usr. Majority of these directories could not be extracted due to lack of root access, it either skips the files/folder or give permission denied error. It is notable that the directory structure is similar to that of Linux as this watch utilizes. Tizen OS which is based on Linux Kernel. Most of the relevant user and device files can be found in */opt* folder of Gear Frontier S3.

Below is a list of files that are of forensic values:

Account.db: This is a SQLite database that contains six tables (*Account*, *Account_custom, Account_type, Capability, Label* and *Provider_feature*). Only the table named *Account* was found to contain info about the connected mobile phone android user account; email of owner of the paired mobile phone can be found there. This table that have significant forensic value especially in a scenario where the accompanying mobile phone cannot be found. The other tables were empty in this database file.

Bookmark.db: Also a SQLite database that contains data about URL bookmarked by user on the wearable device. It contains two tables *Bookmark* and *Current_bookmark*. Bookmark is the table where the (id, title, url, favicon and snap_path or the url is stored). Whereas table called *Current_bookmark* seems to contain the count of the bookmark saved on the wearable device.

Calendar_consumer.db: Another SQLite database that contains a very detailed information about user's upcoming events. It contains two tables *Event_table* and *Reminder_table*. *Event_table* contains summary, description, time zone, location and organizer information. This can be of forensic value for tracking a suspect, information about the attendants of the event can be requested or subpoenaed and can be used to narrow down the search for suspects in solving a case.

CompanionInfo.db: This contains detailed information about the mobile phone the wearable device is paired with. It contains only one SQLite table called *Companion_info*. This table contains information such as device_id, device_model_name, device_platform_type, device_platform_version, device_binary_version, device_manufacturer, sales_code, country_code, sim_mcc, sim_mnc and sim_subscriber_number which is the user phone number.

Contacts-svc.db: It contains data such as contacts, call logs, address books, favorites and groups. There are thirty-two tables in the database most of which are reference tables joining information from other tables. This can be of forensic important in a case where the companion phone is not found at crime scene, it contains all the contacts that can be found on the paired mobile phone.

Certs-meta.db: This database contains information about, SSL, VPN and Wi-Fi. There are six tables in the database. Relevant tables include ***ssl*** which contains certificate information. When the Wi-Fi table was opened it was empty.

Context-app-history.db: this contains data about application usage. It contains 6 tables in total but *Log_AppLaunch* and *Log_BatteryUsagePerApp* contain data like time when the application was first started, the Application ID and duration.

Context-sensor-recorder.db: SQLite database contains sensor data like Heart Rate, Pedometer, Pressure and Sleep Monitor. Data is located in five tables.

Shealth.db: This is the database that contains user's health data. We couldn't get to open the database because it is an encrypted database.

Wemail.db: this contains email data. There are 8 tables in the database, relevant tables includes *email_attachment_tbl* and *email_noti_tbl. Email_noti_tbl* contains information that are of great forensic importance, about 911 emails were discovered in this table containing detailed information about email notifications such as *sender_email, to_list, mail_preview, mail_body, mail_title, mail_time* and *sender_display_name* while *email_attachment_tbl* contains attachment_name and *attachment_local_path* on device of downloaded emails checked on the device.

/opt/usr/home/owner/apps_rw/com.samsung.wemail/data is a path found in the *attachment_local_path* table and it contains mail attachment that have been downloaded by the owner of the device. This can carry forensic value as the attachment can be opened and examined.

Wnoti-service.db: This table contains notification data. It contains eight tables relevant tables include application, *asset* and *data* tables. For previous notifications date, time and path to notification icons are saved. For notifications with icons they can be found in *opt/usr/data/wnoti.*

There are log files located in */var/log* in the device but every attempt to read files from the location via the sdb shell gives *permission denied* error. All the log files are protected from being copied.

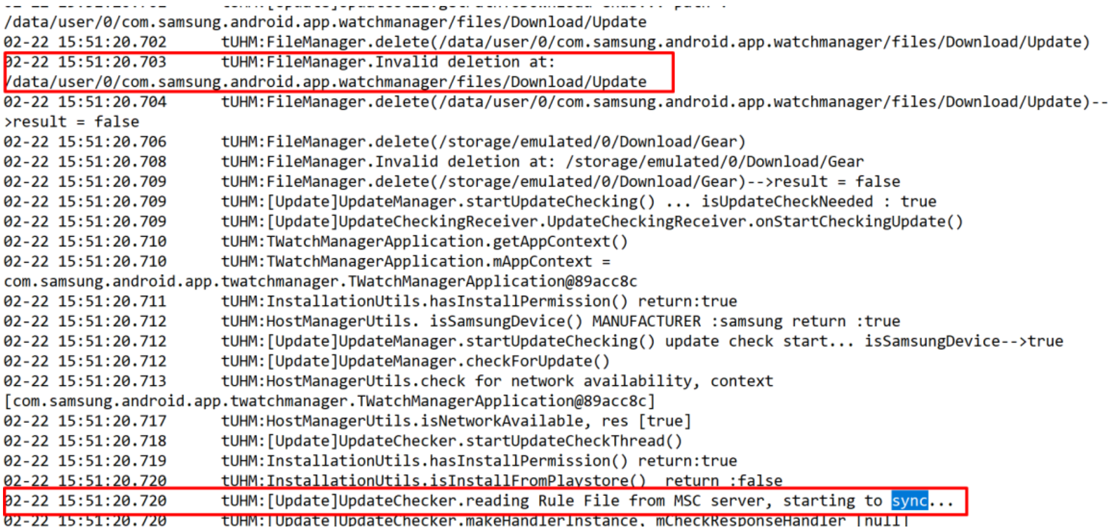
Folders that contains data of forensic value:
home/owner/data/contacts-svc/img/contacts-svc/img/contact: It contains thumbnails of the picture of contacts synced with the wearable device.
home/owner/share/media/.thumb/phone: The wearable device also allows user to take screenshots and which are located in location. Screenshot sometimes can contain messages or notifications that are important to the owner of the device. *opt/usr/data/wnoti*: This folder contains assets about the image of notification on the device.

File Path	File Content	Data
opt/dbspace/5001	.account.db	Connected mobile phone android user account data
opt/usr/home/owner/apps_rw/ *com.samsung.wbrowser/data*	.bookmark.db	URL bookmark by device user
opt/usr/apps/com.samsung.w-calendar2/data	.calendar_consumer.db	User’s upcoming event
opt/usr/dbspace	.companionInfo.db	Database for paired device data
home/owner/.applications/dbspace/ *privacy*	.contacts-svc.db	Database for contacts, call logs, address books, favorites and groups
opt/share/cert-svc/dbspace	.certs-meta.db	Database for ssl, vpn and wifi
opt/usr/home/owner/applications/dbspace	.context-app-history.db	Application use data
opt/usr/apps/com.samsung.wemail/ *data/dbspace*	.wemail.db	Contains email data
opt/dbspace	**.**context-sensor-recorder.db	Contains Heart Rate, Pedometer, Pressure, Sleep Monitor.
home/owner/apps_rw/ *com.samsung.shealth_gear/data*	.shealth.db	Samsung Health Database; this is encrypted
home/owner/data/contacts-svc/img/contact		Saved contact photos
home/owner/share/media/.thumb/phone		Screenshots taken with the device
opt/usr/dbspace	.wnoti-service.db	Notifications data

Table 3 : Mapping of forensic artefacts on Gear S3 and their location (Source: Author created)

4.2 Analysis of Galaxy S9 plus artefacts

Upon examining the file system of Galaxy S9 to see if there are forensic artifacts left by the smart watch, we discovered a log file, *Shared/0/log/GearLog/dumpState-UHM* which contains pairing information between the watch and the mobile device, synchronization events, watch event like deletion and mention of make and model of the wearable device. We were also able to see last connection date and synchronization between the two devices, also event that checks periodically if there are updates to be pulled from the device as shown in **Figure 9**.



```
/data/user/0/com.samsung.android.app.watchmanager/files/Download/Update
02-22 15:51:20.702      tUHM:FileManager.delete(/data/user/0/com.samsung.android.app.watchmanager/files/Download/Update)
02-22 15:51:20.703      tUHM:FileManager.Invalid deletion at:
/data/user/0/com.samsung.android.app.watchmanager/files/Download/Update
02-22 15:51:20.704      tUHM:FileManager.delete(/data/user/0/com.samsung.android.app.watchmanager/files/Download/Update)--
>result = false
02-22 15:51:20.706      tUHM:FileManager.delete(/storage/emulated/0/Download/Gear)
02-22 15:51:20.708      tUHM:FileManager.Invalid deletion at: /storage/emulated/0/Download/Gear
02-22 15:51:20.709      tUHM:FileManager.delete(/storage/emulated/0/Download/Gear)-->result = false
02-22 15:51:20.709      tUHM:[Update]UpdateManager.startUpdateChecking() ... isUpdateCheckNeeded : true
02-22 15:51:20.709      tUHM:[Update]UpdateCheckingReceiver.UpdateCheckingReceiver.onStartCheckingUpdate()
02-22 15:51:20.710      tUHM:TWatchManagerApplication.getAppContext()
02-22 15:51:20.710      tUHM:TWatchManagerApplication.mAppContext =
com.samsung.android.app.twatchmanager.TWatchManagerApplication@89acc8c
02-22 15:51:20.711      tUHM:InstallationUtils.hasInstallPermission() return:true
02-22 15:51:20.712      tUHM:HostManagerUtils. isSamsungDevice() MANUFACTURER :samsung return :true
02-22 15:51:20.712      tUHM:[Update]UpdateManager.startUpdateChecking() update check start... isSamsungDevice-->true
02-22 15:51:20.712      tUHM:[Update]UpdateManager.checkForUpdate()
02-22 15:51:20.713      tUHM:HostManagerUtils.check for network availability, context
[com.samsung.android.app.twatchmanager.TWatchManagerApplication@89acc8c]
02-22 15:51:20.717      tUHM:HostManagerUtils.isNetworkAvailable, res [true]
02-22 15:51:20.718      tUHM:[Update]UpdateChecker.startUpdateCheckThread()
02-22 15:51:20.719      tUHM:InstallationUtils.hasInstallPermission() return:true
02-22 15:51:20.720      tUHM:InstallationUtils.isInstallFromPlaystore()  return :false
02-22 15:51:20.720      tUHM:[Update]UpdateChecker.reading Rule File from MSC server, starting to sync...
02-22 15:51:20.720      tUHM:[Update]UpdateChecker.makeHandlerInstance, mCheckResponseHandler [null]
```

Figure 9 Sample of log file obtained from the Samsung S9

Furthermore we found plugin folder showing the two devices have been paired in the location *apps/com.samsung.android.app.watchmanagerstub.*

In general, more information were found on the Gear S3 device than on the Galaxy S9 plus as we were able to retrieve information like email account of the user of the device, contacts, received emails, upcoming events and other artefacts as show in **Table 3**

Folder / Path File	Type of file	Data recovered
Shared/0/log/GearLog/dumpState-UHM	Log File	It contains logs of device activity and different states of the device
apps/com.android.providers.calendar/db	SQLite Database (.db)	Information about Google Calendar, Upcoming Zoom events with attendees email, reminders, metadata etc
apps/com.android.settings.intelligence/db/ search_index.db	SQLite Database(.db)	Contains saved information queries by the device
apps/com.samsung.android.app .watchmanagerstub	Folder	

Table 4 mapping of forensic artefacts on Samsung S9 and their location (Source: Author created)

4.3 Analysis of Fitbit Versa artefacts

HeartRateDailySummaryDbEntity table, it stores Heartrate data such data have proven to be useful in judging cases in the past like the data obtained from the Fitbit fitness tracker Karen Navarra was wearing when she was murdered showed that her rate had spiked significantly around 3:20p.m on Sept 8 2018, when Mr. Aiello who was the suspect was there, then it recorded the heart rate slowing rapidly, and stopping at 3:28p.m., about five minutes before Mr. Aiello left the house as against the story given by the suspect that she walked him to the door when he was leaving [27].

PersonFriendsDbEntity stores information about ID of the owner of the device with foreign key relations to connected friends, *PersonShortDbEntity* contains personal information like Email, Encode ID, Name, and Steps Summary. *RankedUserDbEntity* contains information about Age, height, Full Name, Average Daily Steps of the user.

SleepLogEntryDbEntity, sleep related data has been useful in the past to disprove allegations like in the case of the woman who claimed to have been dragged of her bed while sleeping and raped, her Fitbit data showed that she was walking around [4].

ExerciseLogEntryDbEntity shows work out history of the user of the device. Other tables that contain interesting data include *WaterLogDbEntity*, *FoodLogDbEntity*.

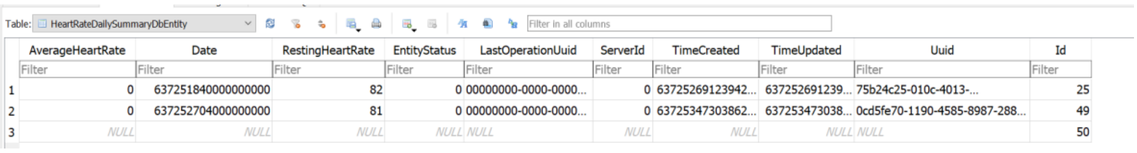


Table: HeartRateDailySummaryDbEntity

Filter in all columns

	AverageHeartRate	Date	RestingHeartRate	EntityStatus	LastOperationUuid	ServerId	TimeCreated	TimeUpdated	Uuid	Id
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	0	637251840000000000	82	0	00000000-0000-0000...	0	63725269123942...	637252691239...	75b24c25-010c-4013-...	25
2	0	637252704000000000	81	0	00000000-0000-0000...	0	63725347303862...	637253473038...	0cd5fe70-1190-4585-8987-288...	49
3	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	50

Figure 10 HeartRateDailySummary log database table

Database table	Information contained
ExerciseLogEntryDbEntity	It contains log of daily exercise
HeartRateDailySummaryDbEntity	Contains a summary of heart rate data
PersonFriendsDbEntity	This is a junction table that contains a mapping between the id of the user of the device and connected friends
PersonShortDbEntity	It contains personal information like Email, EncodeId, Name, StepSummary
RankedUserDbEntity	Contains information about Age, height, FullName, AverageDailySteps of the user.
SleepLogEntryDbEntity	Contains sleep data

Table 5 Fitbit Versa database tables of interest with information contained

5 Conclusion and Contributions

Wearables are becoming a standard as watch for many and also for fitness tracking, with this in mind the need to perform digital forensic research on the devices become necessary. The goal of this work was to provide a forensic analysis of Gear S3 and the paired Samsung S9, we also analysed Fitbit Versa to see if there are information that may be of interest to forensic examiners, based on our results, we were able to retrieve from Gear S3 the email address of the owner of the smartwatch, email messages, notifications, contacts saved on the paired mobile phone synced to Gear S3, pictures of saved contacts, upcoming events, reminders, bookmarks of visited sites. Even though from Samsung S9 less data was acquired but we were still able to obtain Calendar Events, detailed log containing synchronization events, installation and every interaction between the mobile phone and the wearable device.

Furthermore from the Fitbit Versa we were able to extract Heart rate, sleep, exercise and personal data like age, weight and height of the user of the device, this shows this device contains artefacts that might prove useful for forensic investigators and examiners. In this work we could not manage to do a physical acquisition of Gear S3 as it requires having root access to the watch which we weren’t able to achieve in this research, based on our analysis it is clear that wearable devices can be a rich source of evidence in the course of an investigation and we have been able to provide a mapping that would point investigators and forensic examiners to where to look when looking for evidence in the examined devices.

6 Future Work

This thesis has been focused on logical acquisition of smartwatches to see what forensic artefacts can be extracted from the device. We could not proceed to do a physical acquisition on Gear S3 because we didn’t get a rooted custom ROM or any tool that can enable physical acquisition. Physical acquisition can prove to be very valuable to future work as it will give access to those protected files and folders like the log files located in */var/log* which were giving permission denied error when we attempted to extract them.

Also since Samsung allows development of applications for the Gear S3 by using their Tizen Studio, future work can consider developing a watch face application for the Gear S3 device that can be used to access the file system.

References

[1] 10 Notable Facts about Wearable Technology
Available: https://medium.com/@TechTalker/10-notable-facts-about-wearable-technology-c01c21070324 [Accessed: 19-Feb-2020]

[2] Number of connected wearable devices worldwide from 2016 to 2022 Available: https://www.statista.com/statistics/487291/global-connected-wearable-devices/ [Accessed: 03-March-2020]

[3] Apple health data used in murder trial
Available: https://www.bbc.com/news/technology-42663297 [Accessed: 30-April-2020]

[4] Police claim woman lied about being raped after her Fitbit fitness watch showed she had not been dragged from her bed
Available: https://www.dailymail.co.uk/news/article-3134701/Police-claim-woman-lied-raped-Fitbit-fitness-watch-showed-not-dragged-bed.html [Accessed: 30-April-2020]

[5] Watch The GoPro Chase Video That Got This Motorcycle Rider Arrested
Available: https://jalopnik.com/watch-the-gopro-chase-video-that-got-this-motorcycle-ri-1584732768 [Accessed:17-May-2020]

[6] The Changing Nature of Crime and Criminal Investigations Available: https://www.policeforum.org/assets/ChangingNatureofCrime.pdf [Accessed: 15-Jan-2020]

[7] Alex Levinson, Bill Stackpole, and Daryl Johnson. Third party application forensics on apple mobile devices. In 2011 44th Hawaii International Conference on System Sciences, pages 1–9. IEEE, 2011

[8] G. Grispos, W. B. Glisson, and T. Storer, “Using smartphones as a proxy for forensic evidence contained in cloud storage services,” in System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE, 2013, pp. 4910–4919.

[9] P. Thomas, P. Owen, and D. McPhee, “An analysis of the digital forensic examination of mobile phones” in Next Generation Mobile Applications, Services and Technologies (NGMAST), 2010 Fourth International Conference on. IEEE, 2010, pp. 25–29

[10] Baggili I, Oduro J, Anthony K, Breitinger F, McGee G. Watch what you wear: preliminary forensic analysis of smart watches. In: L O'Conner, editor. *ARES 2015*: Proceedings of the 2015 10th International Conference on Availability, Reliability and Security; 2015 Aug 24-27; Toulouse, France. Piscataway, NJ: IEEE, 2015; 303– 11

[11] M. Bader and I. Baggili, “iphone 3gs forensics: logical analysis using apple iTunes backup utility,” Small scale digital device forensics journal, vol. 4, no. 1, pp. 1–15, 2010.

[12] Manual IoT forensics of a Samsung Gear S3 Frontier SmartWatch Available: https://ieeexplore.ieee.org/abstract/document/8903845 [Accessed: 13-Mar-2020]

[13] Smartwatch, do you know secret features of Smartwatch? How it works? What are the components inside it? Available: https://engineeringinsider.org/smartwatchdo-you-know-secret-features-of-smartwatch-how-it-works-what-are-the-components-inside-it/ [Accessed: 16-May-2020]

[14] Forensics Analysis of Smart Watches Available: https://pats.cs.cf.ac.uk/@archive_file?p=1169&n=final&SIG=c7b911655ae722324a055630538a6a6ca7f7aa96d668d8afb7f6a80c5417cf3c [Accessed: 12-April-2020]

[15] What is Stock ROM and Custom ROM for Android? Available: https://www.kingoapp.com/knowledge-base/android-stock-rom-and-custom-rom.htm [Accessed: 30-April-2020]

[16] What's inside a smart watch? Available: https://www.globalsources.com/gsol/I/Activity-tracking/a/9000000132594.htm [Accessed: 17-May-2020]

[17] What is rooting and Un-rooting in an Android Mobile? Available: https://nerdsmagazine.com/what-is-rooting-and-unrooting-in-android/ [Accessed: 19-April-2020]

[18] Memory options for the IoT Available: https://www.synopsys.com/designware-ip/technical-bulletin/memory-options.html [Accessed: 11-Mar-2020]

[19] Guideline on Mobile Device Forensics Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf [Accessed: 10-May-2020]

[20] Connecting Devices over Smart Development Bridge Available: https://developer.tizen.org/development/tizen-studio/web-tools/running-and-testing-your-app/sdb [Accessed: 05-May-2020]

[21] NetOdin vs Odin Available: https://appdb.winehq.org/objectManager.php?sClass=application&iId=19112 [Accessed: 25-April-2020]

[22] NetOdin download link Available: https://androidfilehost.com/?fid=11410963190603905901 [Accessed: 5-May-2020]

[23] Tizen 4 ROM, NetOdin SM-R765A/R765F/R765T/R765V/R775A/R775S/R775R/R775V/R770/R760 Available: https://forum.xda-developers.com/smartwatch/gear-s3/rom-tizen-4-odin-files-sm-r765t-sm-t3892404 [Accessed: 16-Mar-2020]

[24] Tizen 4 ROM Available: https://drive.google.com/file/d/0B2qh5ebkwJa6cU82UXBhOWVPOFk/view [Accessed: 27-April-2020]

[25] Download link for Samsung Gear S3 Frontier(SM-R760) Available: https://androidfilehost.com/?fid=11410963190603905836 [Accessed: 27-April-2020]

[26] Fitbit Desktop application download Available: https://www.fitbit.com/eu/setup [Accessed: 16-May-2020]

[27] Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter’s Killing Available: https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html [Accessed: 18-May-2020]