Forensic analysis of smartwatches: Is forensic analysis of smartwatches worth further research and development for forensic analysts, if so wat type of relevant and useful information can be retrieved?

Patricia Booth
C1535545
CM2303 One Semester Individual Project

Supervisor: Helen R Philips
Moderator: Bailin Deng

Cardiff University school of Computer Science & Informatics
10th May 2019

Table of Contents

Forensic analysis of smartwatches: Is forensic analysis of smartwatches worth further research and development, if so what type of relevant and useful information can be retrieved?

1. Introduction

1.1. Problem and Background

Statistically Google's Android operating system holds the largest market share of smart phones. Google has introduced Android Wear in March 2014 with the aim of integrating all digital platforms with smart OS. The purpose of these smartwatches are to access and operate

smart phones through a more convenient interface device. With the use expected to increase throughout the upcoming years, the number of crimes relating to smartwatches world-wide will also likely increase. It has been stated that “By 2022 Wear OS and Android are expected to be installed in 37 million smartwatches worldwide while another 34.5 million smartwatches are expected to run Apples watch OS” (Topic: Smartwatches, n.d.)

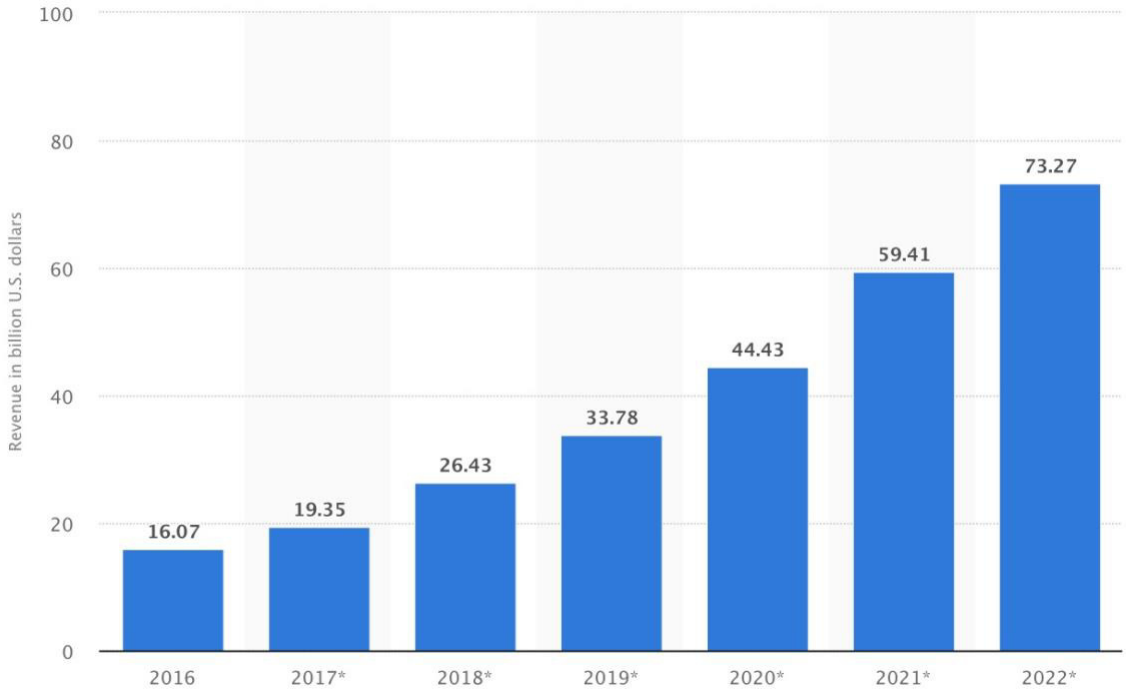


Figure1. Wearable device sales revenue worldwide from 2016 to 2022 (in billion U.S. Dollars) (Wearable device revenue worldwide 2016-2022, n.d.)

A strong piece of evidence found in a crime scene such as a smartwatch can be a significant factor in solving a crime. The investigation of this project is attempting to prove the value of this digital evidence. The predicted increase in users imply that if the answer to the main question is yes, it is worth further research and development then the next phases would suggest that an increase in smartwatches security must also be developed.

This projects focus is on extracting and investigating potential sensitive data from smartwatches to assess if these devices are worth the further research and development then the next phases would suggest that an increase in smartwatches security must also be developed or if they are just another “fad” within the technology field that is not worth the

time and resources. One of the main objectives is to explore which file location within their file systems hold the most valuable information. Furthermore, the main interest is looking into the data relating to the two devices connection via Bluetooth, the watch can be found at a crime scene without its paired phone. Would the information stored on the smartwatch differ depending on this connection with the phone and if so, would the value of the evidence stored within the smartwatch still be of value. There will be a number of investigations, looking into a smartwatch along with its paired phone, investigating both devices performing forensic analysis.

If the technology were to increase in market share and more users increased as predicted, there would be a growth in the number of crimes relating to these devices. It is beneficial to have a more preventative solution than a reactive one. As more and more criminals are exploiting smartwatch vulnerabilities having a well-developed methodology in acquiring and performing forensic analysis on these devices will provide authorities and forensic analysts with a great advantage allowing them to be steps ahead of the criminals who hope to take advantage of this somewhat new technology. This project takes the initial steps to developing methods of how to examine and how to deal with smartwatches when found in crime scenes. Although they have similarities with mobile phones which already have a standardised methodology for forensic analysts in how to handle the device throughout the investigation; Smartwatches is still a different device meaning that the methodology implemented would have nuances to phones even though they are similar. Having the knowledge of these nuances allows analysts to examine the device in the most effective and efficient manner.

Smartwatch similar to mobile phones will begin to present a challenge to law enforcement due to the fast changes in technology with the number varied models of smartwatches already in use. Phones utilise closed operation systems and proprietary interfaces which leads to difficulties when extracting forensically extracting digital evidence. However, for smartwatches the lack of research and development on the security area the problem is not with the forensic analysis but the vulnerability of the devices themselves. Vulnerabilities that are already being exploited by criminals. On the other hand, smartwatches can also be beneficial to authorities. For example, there are a number of articles (John Scheerhout, 2019) which state that a hitman named Mark Fellows was convicted of two murders as his

smartwatch places him at the scene of the crime. It is stated that it took three years to convict him however after raiding his home where the watch was located the watch exhibited provided proof that he was at the scene of the pre-assassination meeting that incriminated him. A picture of the Fellows wearing the watch as he takes part in the Great Manchester Run was spotted by the authorities, this correlated with the GPS as it showed his speed of travel, this allowed the police to put together a more educated guess of how they believe the events unfolded providing them with a more accurate timeline. The GPS data was cross-referenced with CCTV footage where he was spotted with another suspect who eventually admitted that he was a party to the murder. Fellows used technologies like GPS and night vision hunting scope to allow him to track his targets. Not only did the information on the watch help solve the overall investigation but also provided the authorities with detailed information that allowed the investigation to be thoroughly completed so that all charges against the criminal lead to justice. Valuable telling data is what is anticipated to be found during the analysis for both devices.

1.2. Smart Watch: Android Wear

A smartwatch has many features on top of time keeping, the digital watch allows to you to monitor components such as heart rate, activity tracker, 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 the watches functionality such as stock prices and map displays, weather information. Majority of smartwatches also have the capability of receiving text messages and making phone 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 smart watches 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. This means that some functionality of the watch is limited when the phone is not connected. For example, if a messaging application on the watch allows you to send a message, the actual message is sent by the phone connected to the watch. If the connection is lost, then the message will not be sent.

Functionality such as activity tracking is possible without the need of a connection to a smart phone. Generally, smartphones are considered as a smartphone accessory rather than a standalone device. However, because it still have some functionality without phone connection. Analysing the watches data should allow us to realise if the limitation of no connection secures the users data or if the data within the watch is still valuable for forensic analysis. Furthermore, one of the two watches being analysed can technically be a stand-alone device as it has phone like capabilities, it has the capabilities of containing a sim within the device itself and not needing the phone for messages or calls to have those types of features. You could argue that the watch is then a stand-alone device.

Googles Android Wear introduced a new operating system for Wearable Devices which uses Bluetooth communications to connect hand-held devices. To synchronize a phones data with a smartwatch the operating systems prerequisite is that the hand-held device is running on Android 4.3 or higher and one companion application, in this case WearOS which was formerly known as Android Wear. The connection allows the data such as updates from the paired devices to be transferred onto the watch. Updates such as phone notifications, incoming calls, text messages.

The investigation focuses two Android devices a smartwatch and its paired phone, analysing both devices, examining their contents to see if there are valuable digital evidence in existence, especially on the smartwatch. Android OS structure has similarities to the basic structure of Android Wear along with the Kernel which is also the same as Android OS. To handle multiple complex data in an efficient manner in real time by interacting with a smartphone the wearable data layer is used. There are three APIs that consists of the basic structure of Android Wear Data API, Message API and Node API.

Data API(the wearable data layer API) provides a communication channel for the smartwatch and its paired phone where the system can synchronize and send through its wireless communications and listeners that notify the applications of important occurrences within the data layer. Message API manages API calls between devices. Node API is what informs a

smartphone when a node is connected. Node events are distributed to every application on devices.

2. Methodology/Approach

As previously mentioned, the two main devices used for investigation are both Android devices a smartwatch and a phone in which the two devices are paired through a Bluetooth connection. The smartwatch being the primary device as it is the device in question whether it's worth further research and development if valuable digital evidence is found. There will be a focus on three main partitions which are /cache, /system and data. Although looking at the device as a whole would be ideal for an investigation as valuable digital evidence can be found in any location, the three mentioned memory blocks are the areas that would likely have the most interesting and telling data. Therefore it is appropriate to prioritise them, focusing on the most relevant data first.

The bellows is a list of tools/software used for implementation which is also further discussed in later chapters in more detail.

- ADB 1.0.40
    - Android Debug Bridge a command line tool which allows communication with a device.
- Fastboot 28.0.1
    - An engineering protocol which boots Android device. Fastboot mode allows the modification of file system images from a machine via USB connection.
- Autopsy 4.11.0
    - The graphical interface for The Sleuth Kit, a digital forensic tool.
- Odin3
    - Internally used by Samsung as a utility software, used to flash custom recovery firmware image. Also used to unbrick Android devices .
- SuperSU
    - An access management tool providing access right to all apps on the device that needs root.

2.1. Design: prerequisites/setup

For the investigation there were technically two computers involved a MacBook and a Windows 10 virtual machine(VM). ADB and fastboot were primarily setup on the Mac however Autopsy lead to a number of inconveniences like the available download version for Mac is an older one which means less capabilities; For this project it is ideal to have the most suitable and latest tools therefore, the installation of the latest version of Autopsy on the Windows machine is reasonable. Having both machines also allowed a number of work arounds for both the smartwatch and the phone. However, note that the Windows virtual machines command line interface had limited capabilities in terms of commands already configured on the command line. Therefore, ADB and fastboot could only be downloaded on the MacBook.

In terms of general setup for the Sony Smartwatch 3 an application is required to be installed on its relative phone, the application is named Wear OS. Wear OS enables the synchronisation between the smartwatch and the phone. Syncing the necessary applications and data that is needed by the watch as it cannot be a stand-alone device. As previously mentioned, the device sometimes only creates a copy the application or the applications data and not the application itself as it does not have as much capacity in comparison to a mobile device. If the user where to have a high volume of application the small device would not be able to handle the load. The Wear OS application allows the flow of data between the phone and the smartwatch to be efficient and easily updatable as the user continuously reconnects the two devices together.

There are a number of prerequisites necessary so that the watch can be investigated. These steps are needed as they allow the device to be accessible with more capabilities, dealing with permissions enabling any features that is needed so that the device can connect or be recognised by the Computer.

During the pairing of the phone and smartwatch, all features asked to be accessed by the application to be enabled were allowed. A basic generic setup for both devices provides a good starting point when analysing the data. This means that majority of the data analysed is what will be commonly found in most similar devices. This makes the findings of this project

more reliable as the devices used are that of the real world. Once the pairing is completed the watch and phone both need to be rooted. Below are the steps taken to root the paired phone:

On the computer(Windows 10 VM): Download compatible Samsung USB driver
On the phone: Go to Setting > About Device > Model Number Take note of the stated model number : SM-G920F
On the computer(Windows 10 VM): Download Auto-Root.zip file compatible to noted model number SM-G920F which consists of: o CF-Auto-Root-zeroflte- zerofltexx-smg920f.tar.md5 o Odin3 (Configuration Settings file type) o zlib.dll (Application Extension) o tmax.dll zlib.dll (Application Extension) o Odin3-v3.10.6 (Application)
On the phone: Go to Setting > About Device > Software Info > Build Number Select Build number until interface states that you are Developer, this enabled Developer mode which allows you to access Developer Options Go to Setting > Developer Options > USB debugging Enable USB debugging, puts the phone on debug mode when USB is connected which is needed when using ADB
Plug the phone to the computer via USB, this will allow the drivers to properly install, then unplug
Turn off phone, then turn on holding down power button, volume down button and home button. Hold until a Blue screen appears
Push the volume up button to continue
Plug the phone back to the computer via USB
On the computer(Windows 10 VM):

Go to the Odin application and select “AP” and choose the CF-Auto-Root-zeroflte-zerofltexx-smg920f.tar.md5” Select “start” Once the phone is rebooted the SuperSU application should now be installed on the phone On the computer (MacBook): Check if devices is rooted *>adb devices* - on the phones notification centre there will be an option which currently states, “Transferring media files via USB – Tap for other USB options”. For the phone to be recognised by adb tap the option which states “Connect a MIDI device – Use the connected device as a MIDI player or input source.” >*adb shell* >*su*
On the phone: The SuperSU application will show a prompt asking to allow or deny su access to the computer Select “Allow”

The steps above roots the phone allowing the majority of the commands to be performed that is needed for the next stages of the investigation. The Windows computer is the machine used to execute the steps mentioned above. The rooting of the phone is on the Windows machine as the tools/software used were all compatible to Windows. (attempted rooting on mac lead to incompatible files downloaded as they are more suited to Windows).

Wear OS is set to connect with the computer via ADB (Android Debug Bridge). ADB allows the control of a device over USB from a computer along with features such as copying files to and from either the device or the connected computer, installations or uninstallations of applications, running shell commands etc. It is a command-line service incorporated with Googles Android SDK. ADB will prepare the device for forensic analysis meeting all its conditional requirements. Below are the steps taken to root Smartwatch 1:

On the computer(MacBook):

Open terminal

>brew install homebrew/cask/android-platformtools

Android SDK must be downloaded and installed on the machine as it is required by the investigation when using ADB. *"/android-platformtools"* consists of both adb and fastboot

On the watch:

Go to Settings > About > Build Number : tap on Build Number 7 times, this enables Developer Options

Go to Setting > Developer Options: tap on USB Debugging and Debug over Bluetooth and enable these features

Ensure that the watch is connected to the computer via USB cable, the watches interface will then ask if the connected device is to be allowed debugging, select the option 'Yes'

On the Computer(MacBook):

Open terminal

>adb devices

- this provides a list of devices that are connected to the computer.

if the smartwatch is listed but it is stated that it is unauthorized

>adb kill-server

>adb start-server

>adb devices

the device should now be listed as authorized

>adb reboot bootloader

When adb help is typed in terminal this is what it stated for adb reboot bootloader – *reboot [bootloader|recovery|sideload|sideload-auto-reboot] reboot the device; defaults to booting system image but supports bootloader and recovery too. sideload reboots into recovery and automatically starts sideload mode, sideload-auto-reboot is the same but reboots after sideloading.*

>fastboot OEM unlock

type in twice if asked by interface, the device must be rooted to allow implementation to occur this command unlocks the devices bootloader.

>fastboot boot /Users/patriciabooth/Downloads/SM3root/new_boot.img

When fastboot help is type in terminal this is what is stated for fastboot boot image.img - *boot image: boot KERNEL [RAMDISK [SECOND]] Download and boot kernel from RAM.*

- This downloads TWRP(Team Win Recovery Project) on the device. TWRP is an open-source software custom recovery image for Android-based devices, providing its user a touchscreen interface allowing the capability of installing third-party applications onto the device along with the back-up of the current system.

The steps above roots the smartwatch allowing the majority of the commands to be performed that is needed for the next stages of the investigation.

3.Acquisition/ Implementation

3.1Consideration of Best Practices

For the acquisition and implementation of the analysis it is ideal to perform best practices. However, putting into consideration that this technology is still in its initial stages there are no standard best practices that is commonly known by the market. On the other hand, the most similar device that does have well developed best practices are mobile phones. In this project the best practices for a mobile phone forensic analysis are also loosely applied to smartwatches. This allows the investigation to be more accurate to a real-world scenario. If a smartwatch were to be found in crime scene the environment setup for this project is formatted to be as close to a real-life environment similar to what forensic analysts would have setup, this environment improves the relevance of the results of this project. The more accurate the investigation and environment the more reliable the proof provided. In addition, in this project the implementation of the analysis there is a key factor that was not implemented but should be noted. When creating a copy of the devices it is important that before attempting this that a write blocker is in place to prevent any altering of data on the original data. The key feature of the blocker is that it allows read commands which is what is needed for analysis, but “blocks” write commands. This ensures the data’s integrity is maintained especially in the earlier stage like acquisition, if the data is not guaranteed to secured from being corrupted the analysis of these devices and their value as digital evidence may become redundant to the investigation.

The Association of Chief Police Officers also known as ACPO has provided a "ACPO Good Practice Guide for Digital Evidence" guide (QPM, 2012). This document is written for the guidance of UK law enforcement personnel who may handle digital evidence. The list of best practices below are mostly relevant for mobile phones but could be applied to smartwatches and are also selected dependent on its relevance to this project. The chosen guidelines are the ones most followed during the investigation:

- *"Ensure that details of where the item was found are recorded, which could assist in prioritising items for examination at a later stage"*
    - It is vital to take note whether the smartwatch was found with or without its paired phone. For the investigation, it is obvious that the smartwatch was found with its coupled phone as those are the two main devices being investigated within this scenario. Knowing that there is a paired device, the investigation can then look more into both of the devices data relating to their Bluetooth connection. This connection leads to a number of interesting areas within the memory blocks that were investigated as stated within the finding of this report. Taking note of the paired device allowed the investigations direction to go the right way the first time around allowing the process to be more efficient.
- *"Differentiate between mobile phone found on a suspect (likely to be in current use) and phones found in a drawer (may not be in current use), as different levels of examination may be possible for these*"
    - It is important to realise that the device being investigated is one that is currently being used by the suspect being investigated or if it is an older device that may not hold as much evidence as it may not have been used during the time of the crime being committed which likely means that the data found on it would not be as relevant even though it may still be knowledgeable. Investigating a device with the mentality that it has recently been used direct the analyst in the right direction in terms of which areas to focus on within the memory blocks being looked into. There are log files that clearly imply when a device was last used as the files have timestamps. Both devices being examined are assumed to be in current use therefore the level of examination is detailed and thorough .

- *"When submitting evidence to Digital Forensic Units, investigators must supply specific requirements. It is not practically passible to examine every item of digital data and clear tasking is needed to ensure that the digital forensic practitioner has the best chance of finding any evidence which is relevant to the investigation"*
    - It has been clearly stated within the investigation that the three main areas being analysed for both devices are /cache, /system and /data, it can be assumed that within this scenario the investigator specified these areas to priorities for the analyst. These areas are the most relevant and interesting in the context of this investigation as the evidence being attempted to be found is likely to be within these three main areas. Mainly focussing on these three allows the investigation process to be more efficient and less time consuming as looking throughout each devices filesystem would take a lot of time but instead that saved time is being used to investigate the main areas in a detailed manner to ensure that what is found is relevant and is useful for this examination.
- *"Interpretation of digital data 5.10.1. As with other forensic evidence, interpretation is often required to ensure the evidential weight of recovered digital evidence is clear. Practitioners who undertake the interpretation of digital data must be competent to do so and have had sufficient training to undertake the task assigned to them."*
    - There is an awareness that the analyst for this investigation that their "training" undertaken is not official and therefore the interpretation of data is only limited to what was informed and learned by the analyst. The interpretations are not from an officially trained perspective however the analyst still has enough knowledge in which educated decisions can be made when attempting to understand the evidence. The awareness of the lack of official training justifies if some of the digital evidence interpreted is not exactly how they should be interpreted in a standardised official approach.
- *"Interpretation of digital data 5.10.5. It must also be borne in mind that the development of digital technology is dynamic, and the practitioners may well face significant challenges to their knowledge. It is not possible to be an expert in all aspects of digital forensic examination, but a practitioner should be aware of the limits of their knowledge and where further research or additional specialist knowledge is required."*

- In the results of the investigation it is ideal to make note of any uncertainty in the findings and if there is a need for further research or a requirement for additional specialist knowledge. The awareness of the limitations of one individual's knowledge is beneficial as the interpretation of the evidence needs to be as accurate as possible so that it can hold the most value it has the capability to. If the analyst choses to ignore the resource of other specialist, then the analysis of the evidence being interpreted may be in accurate. Therefore, leading the investigation to being unfair and lead to an injustice if someone was wrongfully incriminated by misinterpreted evidence.

3.2 Image Acquisition

The key part of the investigation is creating an image of the evidence which in this case is the smartwatch itself. One of the basic concepts of forensic investigation is that the original evidence should not be altered. Therefore, creating a bit by bit image of the evidence will allow the analysis of evidence without tampering the original data. To ensure integrity a hash is of the memory block and the created image are compared to ensure that the copy created is identical to its original.

Within the investigation process the analysis of original data is never performed. Imaging is most commonly performed on three main memory blocks /cache, /data and /system which are three of the most vital and interesting locations when looking at the filesystem from an investigation perspective.

On the computer(MacBook): Open terminal *>adb shell* - accesses the watches shell, any commands ran from this point forward are executed on the smartwatch
/cache memory block:
>md5sum /dev/block/mmcblk0p30 > /sdcard/cache.md5 - hash the memory block before imaging
>dd if=/dev/block/mmcblk0p30 of=/sdcard/cache.img bs=512

- imaging the memory block
    - dd extracts small areas of the disk for analysis
    - dd if=IFILE of=OFILE [OPTIONS]
    - if=/MountingPoint: input filename –where memory block is located that needs imaging
    - of =/Destination/partitionType: Output Filename – destination path of where you want the image to be saved, partition type is the type of partition being imaged in the process
    - bs= Block Size : Sets the block size
    - if/of can be a file, disk device, partition or tape

>md5sum /sdcard/cache.img > /sdcard/cacheimg.md5 (hashing the newly created image of the memory block

>cat /sdcard/cache.md5

>cat /sdcard/cacheimg.md5

```
/dev/block/platform/sdhci.1/by-name # cat /sdcard/cacheimg.md5
44d67a8348fd2f8cc27265e21d8412cf  /sdcard/cache.img
/dev/block/platform/sdhci.1/by-name # cat /sdcard/cache.md5
44d67a8348fd2f8cc27265e21d8412cf  /dev/block/mmcblk0p30
```

output of the two cat commands should be the same which validates that both the original data and the image created are identical

>adb pull /sdcard/cache.img /Users/patriciabooth/Documents/watch1/cache.img

adb pull copies files/directories to the device, from the smartwatch to the computer. This means the image is not acquired and is on the machine and is now ready to be analysed

Note : The same few steps are now repeated with /system and /data memory blocks

/system memory block:

>md5sum /dev/block/mmcblk0p31 > /sdcard/system.md5

>dd if=/dev/block/mmcblk0p31 of=/sdcard/system.img bs=512

>md5sum /sdcard/system.img > /sdcard/systemimg.md5

>cat /sdcard/system.md5

>cat /sdcard/systemimg.md5

>adb pull /sdcard/system.img /Users/patriciabooth/Documents/watch1/system.img

/data memory block:

>md5sum /dev/block/mmcblk0p32 > /sdcard/data.md5
>dd if=/dev/block/mmcblk0p32 of=/sdcard/data.img bs=512
>md5sum /sdcard/data.img > /sdcard/dataimg.md5
>cat /sdcard/data.md5 *>cat /sdcard/dataimg.md5*
>adb pull /sdcard/data.img /Users/patriciabooth/Documents/watch1/data.img

A similar imaging process implemented on the paired device the phone, ensuring that all perquisites are met, and that the phone is connected to the computer:

On the computer(MacBook): Open terminal *>adb shell*
/userdata memory block:
>md5sum /dev/block/sda18 > /sdcard/phoneUserdata.md5
>dd if=/dev/block/sda18 of=/sdcard/phoneUserdata.img
>md5sum /sdcard/phoneUserData.img > /sdcard/phoneUserDataImg.md5
>cat /phoneUserdata.md5 *>cat /phoneUserDataImg.md5* `126|zeroflte:/ # cat /sdcard/phoneUserDataImg.md5` `a8b0afa06f3411fca636757dfa7ddbda /sdcard/phoneUserData.img` `zeroflte:/ # cat /sdcard/phoneUserDataImg.md5` `a8b0afa06f3411fca636757dfa7ddbda /sdcard/phoneUserData.img`
>adb pull /sdcard/phoneUserdata.img /Users/patriciabooth/Documents/watch1/phoneUserdata.img
/cache memory block:
>md5sum /dev/block/sda16 > /sdcard/phoneCache.md5
>dd if=/dev/block/sda16 of=/sdcard/phoneCache.img
>md5sum /sdcard/phoneCache.img > /sdcard/ phoneCacheimg.md5
>cat / phoneCache.md5
>cat / phoneCacheimg.md5
>adb pull /sdcard/phoneCache.img /Users/patriciabooth/Documents/watch1/ phoneCache.img
/system memory block:

>md5sum /dev/block/sda15 > /sdcard/phoneSystem.md5
>dd if=/dev/block/sda16 of=/sdcard/phoneSystem.img
>md5sum /sdcard/ phoneSystem.img > /sdcard/ phoneSystemImg.md5
>cat / phoneSystem.md5
>cat / phoneSystemImg.md5
>adb pull /sdcard/phoneSystem.img /Users/patriciabooth/Documents/watch1/phoneSystem.img

4. Results and evaluation: Image analysis/investigation

As previously stated, Wear OS does not have the capability or capacity to store any application individually on its system. The application must first be downloaded on the paired smartphone which then synced by downloading through a download of a copy of the application on to the device. Furthermore, in terms of basic health-based applications that are available to be install on the Wear it is limited to a small number due to its storage capabilities. The more commonly used applications that are likely the most useful to the Wear user such as messenger, email, gaming and other major application can only be accessed on the smartwatch through synchronisation with its paired device. This indicates that only a small part of the complete data can be captured from the devices as it actually stored within the paired smartphone. When the device is synced with the phone all possible application notification alerts that are compatible with the device will be on the smartwatch. Even though, the amount of data stored within the device is only a small part of the overall data that can be retrieved the data that is stored on the device is likely the most relevant as it is the most important information that its users' value. Thus the investigation is focussing on /cache /system and /data memory blocks as they are the likely to be the area of device which holds the most valuable information.

Forensic analysis software such as Autopsy, Scalpel, and FTK imager can be utilised to parse the newly acquired images. Although Autopsy was used to analyse the images there was an attempt on using both Scalpel and FTK imager for the investigation. Scalpel is primarily a program for recovering deleted data and is currently being integrated with Sleuthkit which the front end of Autopsy. Scalpel on its own did not have the correct capabilities for the investigation. Forensic Tool Kit (FTK) imager has the most similarities to Autopsy in terms of

capabilities however Autopsy is the tool most familiar and user friendly therefore it was not chosen as the main tool for analysis.

The smartwatch being the primary device of this overall project means that the main focus was analysing the data in the watch's filesystem more so than its paired phone. The phones investigation was to inspect to see if there was any fascinating data flowing through from the phone to the watch apart from the expected information that would be included. When the two devices are connected the expected information is found both on the smartwatch and phone. The phone however did not showcase any significant information therefore there was no need to mention the findings in the investigation as the data found during the analysis was expected in comparison to the smartwatches findings where they were of more value thus this is what the main focus of the next few topics.

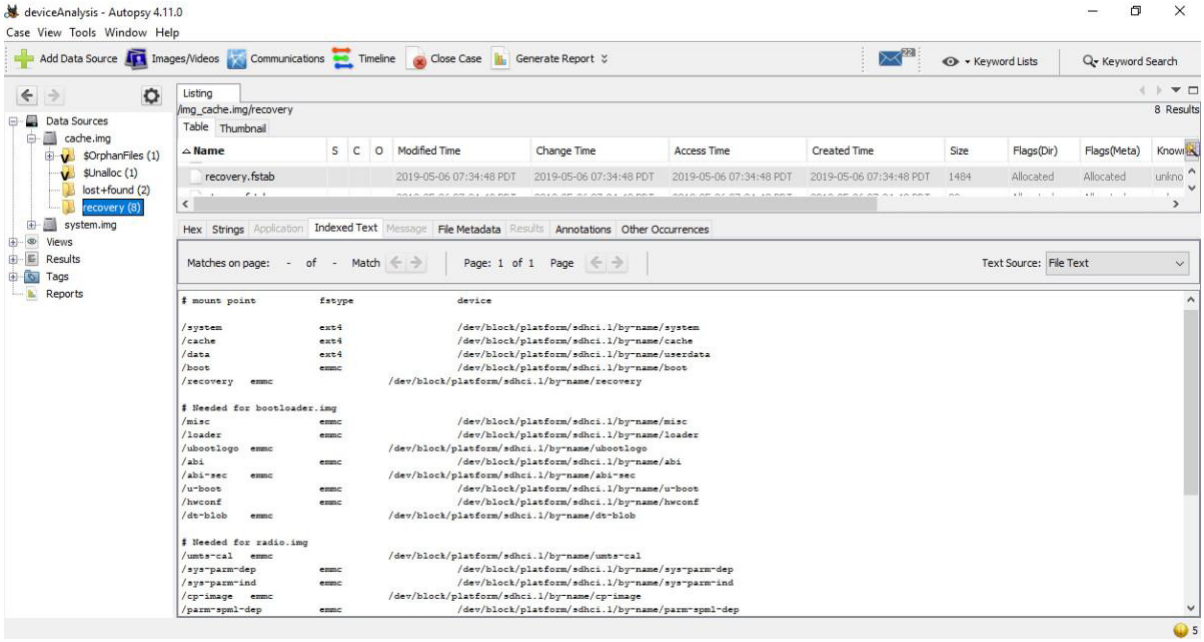
4.1. /cache

Cache is data that is already known and stored by the system and is accompanied by its relevant application allowing efficiency for future requests so that they may be handled faster. Usually the data is a duplication of existing data or result of a computation that was performed in the past.

4.1.1. /cache: Smartwatch

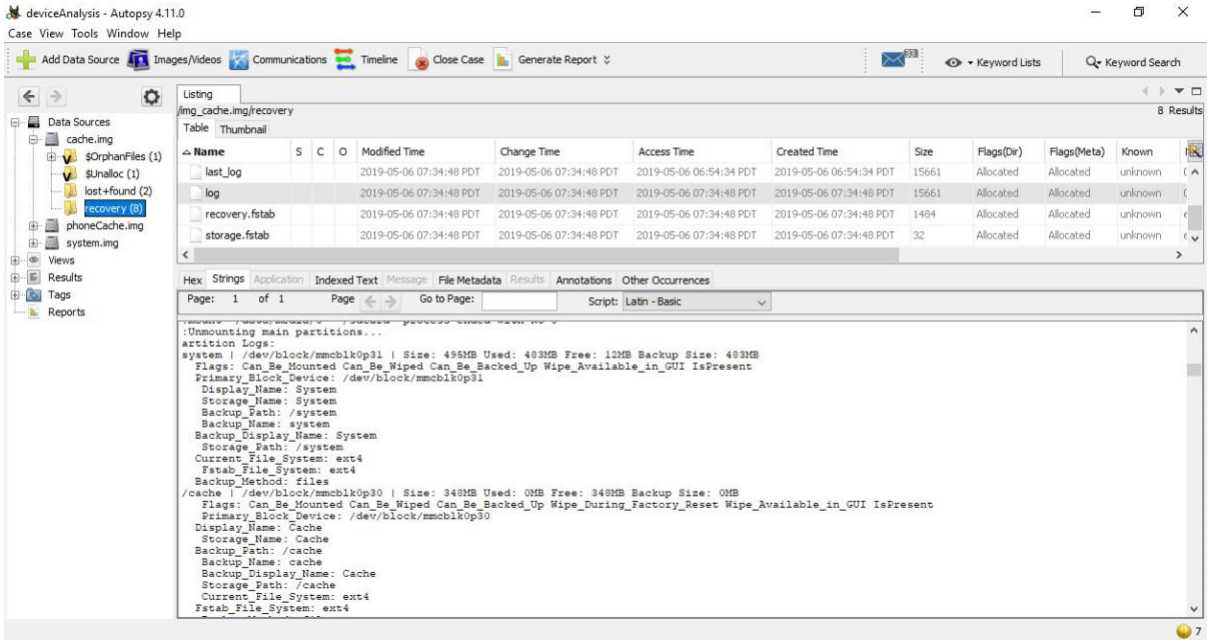
Within the cache memory block image it revealed that an fstab entry which is used for specifying partitions and devices or how and where to use said partitions on a device and information about the filesystem in use. This is vital information storing file which is a necessity for the device. During further investigations it was also discovered that general recovery information, partition logs and their recovery information was also stored within this memory block. /cache contains files which is populated at the first boot of the Android device and information about the already installed apps. To optimise its launch Android uncompressed each app and saves it into /cache. /recovery consists of the files required for the device to boot into recovery mode which provide a number of capabilities such as wipe

/data, /cache, and install an update package.



The screenshots above illustrates that within /cache/recovery there is a file named “recovery.fstab” which shows the mount point, fstype(filesystem type) and device with its file path. Recovery.fstab file is used by package-building tools and the recovery binary, in the file you can specify the name of the partition map in “TARGET_RECOVERYFSTAB”. All mount points must be defined to correctly configure, there’s is also the option of adding extra partitions to devices. The two main file system types specified on this specific recovery.fstab are emmc which is used for bootable partitions like recovery and boot, emmc is raw a block device but is never actually mounted. To locate the device in the table a mounting point string is configured. Ext4 is another filesystem type which sits on top of emmc flash device and “device” must be the path of the block device, it is the file system for internal flash memory on Android devices.

This digital evidence has the potential of being valuable to a case and or be of interest to an analyst because it shows the analysts all the file path locations of all partitions along with their filesystem types. Although there is a general standard structure for the more common filesystems like Android this is still beneficial to the analyst.



The screenshot above shows in /cache/recovery is a log file, within said file the main partitions are provided with an overview. The key areas of information are highlighted on the screenshot where the partition name, location path of the memory block, overall size, used size, free space, back up size, and flags such as Can_be_Mounted, Can_be_Wiped, Can_be_backed_up, Wipe_available_in_GUI, IsPresent are all stated. There is also another file called “last_log” which shows the last boot of the device along with the mentioned overview of the highlighted information.

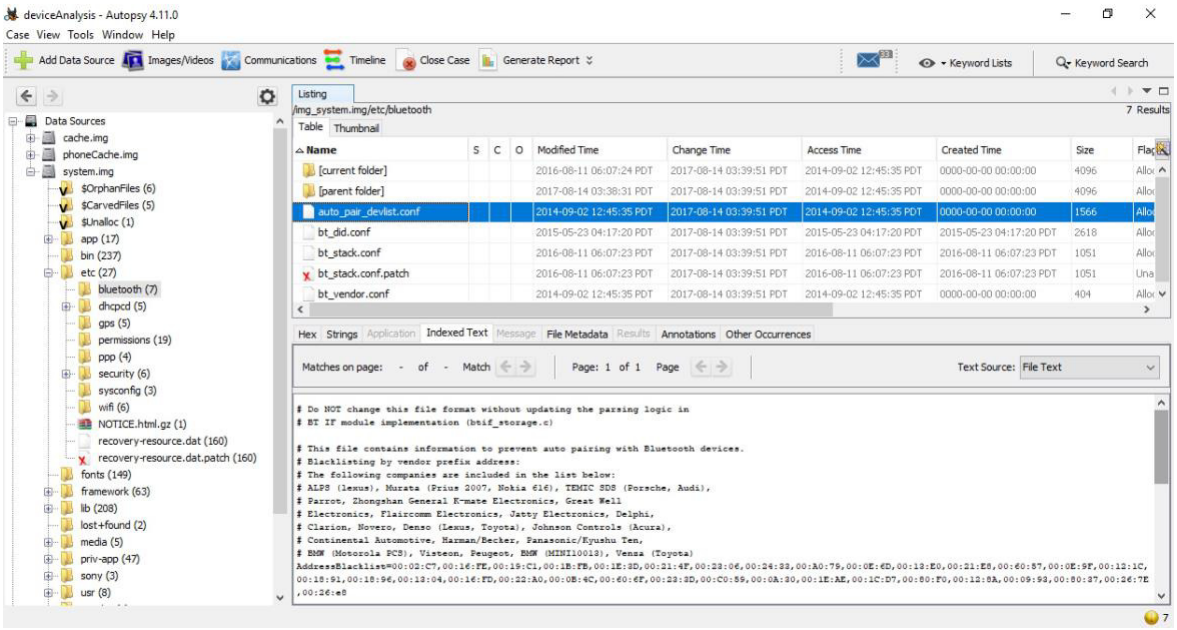
This digital evidence has the potential of being valuable to a case and or be of interest to an analyst because it provides an overview of all of the partitions current state. There could be a significant increase in one of the partitions storage size which is included within the overview of each partition. An analyst would have a general idea of the range of the partition’s storage sizes. If there was a partition with a much larger size than normal, then this implies that there may be some file or folders stored that contains a lot of data. If the investigation implied that the investigation involved a hacker, or the criminal has hidden information somewhere then this would be a convenient file to use as a tool. Although there are commands available to provide an overview of the partitions and their storage size, the file itself is still informative.

4.2. /system

System contains data about the core system which consist of the devices installed applications, framework, applications from the manufacturer, configurations set by default like fonts and font sizes, media files. Command ls -al can be used to list all the directories where you can find details about the system like the file system, directories such as block (contains files related to all memory blocks), device (contains directories related to the devices platform, software, system etc), module (contains directories of package modules used by the system.

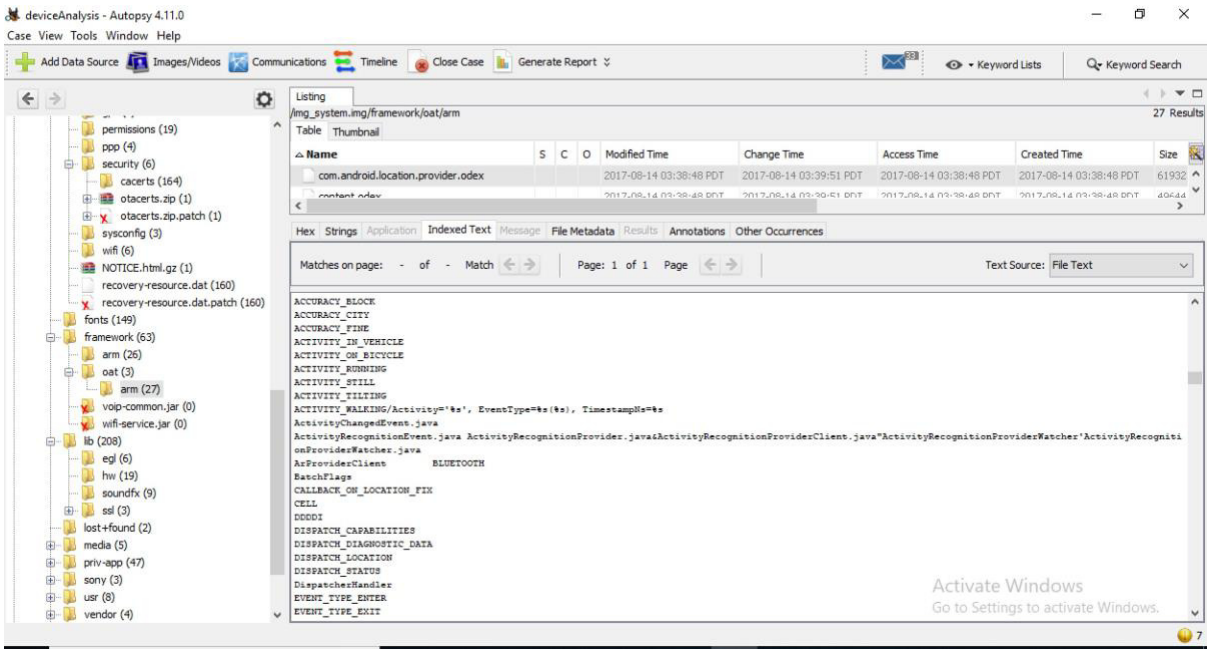
4.2.1. /system: Smartwatch

The /system directory consists of the directories that is normally seen under the root directory of a standard Linux distribution. The partition contains the entire Android OS including its GUI and preinstalled system applications



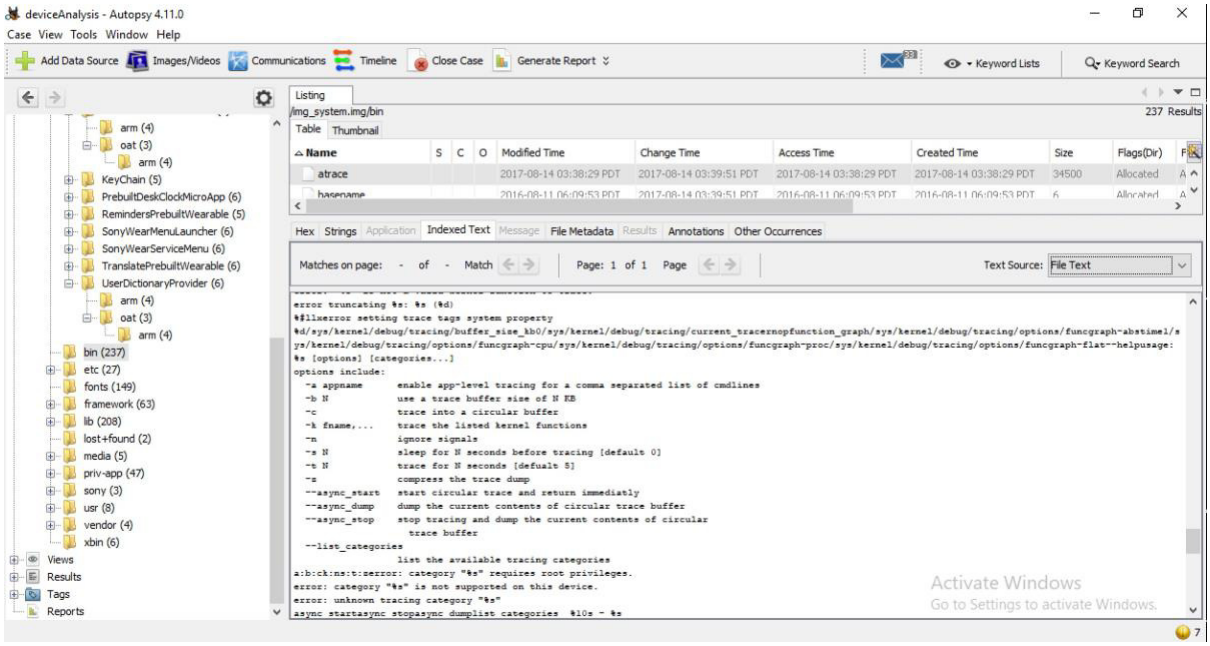
The screenshot above displays that within /system/etc/Bluetooth contains a file named “auto_pair _devlist.conf” the file consists of a list of different company devices which are blacklisted so that they are prevented to auto pair through a Bluetooth connection. This digital evidence has the potential of being valuable to a case and or be of interest to an analyst in the context that the investigation state that an individual was not at the place of crime as their device did not pair with another device that would if they were present at that location. If this was the case, a list of devices that are prevented from automatically pairing to this

device would disprove that point. Although, no device was paired automatically the blacklist would state otherwise assuming that the relative device is within the list blacklisted.



The screenshot above shows that within /system/framework/oat/arm consist of a file called “com.android.location.provider.odex” in which the file implies that there are a number of variables that is recorded such as ACCURACY_BLOCK, ACCURACY_CITY, ACCURACY_FINE, ACCURACY_IN_VEHICLE, ACCURACY_ON_BICYCLE, ACCURACY_RUNNING, ACCURACY_STILL, ACCURACY_TILTING, ACCURACY_WALKING etc. An Android application contains executable code in dex files, odex files are optimised version of these files. Dex files are standardised to have the compatibility to run on all Android devices, odex is more devices specific.Odex files for applications are created by Android before they are run. They contain the same filename prefix as their applications related APK file. The data used in the dex file stored inside the APK file is replaced by the data in the odex file .

This digital evidence has the potential of being valuable to a case and or be of interest to an analyst because it provides a number of different variables that may indicate the different scenarios of what the user was doing at a certain point in time. If an investigation was looking at creating a timeline of when a crime occurred and attempting to correlate CCTV and GPS data that has already been previously discovered. Further investigation on the relative files may show if the user was walking, running, driving etc.



The screenshot above displays that inside /system/bin contains a file named “atrace”, in this file there is variety of information implying that some sort of trace command is being used and that with that command there are a number of options included.

This digital evidence has the potential of being valuable to a case and or be of interest to an analyst with further help from another analyst there is a possibility that what is being traced could be of value. Dependent on the thing actually being traced and if it is of any relevance to something of worth, it may just be tracing some piece of data for one of the applications running. Further specialist knowledge is needed to confirm or reject if this is of value.

4.3. /data

Storage location of the user’s data such as user settings, installed applications, messages, contacts, calendar, downloads etc. This partition contains the majority of the user’s data therefore its value in terms of the investigation is significant. There are a number of subdirectories that are of interest, some of the most noteworthy subdirectories under the data folder are app, dalvik-cache, data,misc, property and system

4.3.1. /data: Smartwatch

Even though a smartwatch is not designed to store large amounts of data it is still one of the most significant areas to look in to. Some of the data stored is in database format which are sqlite3 DB files this also implies that is also contains a shared preferences folder which

consists of a config file that belongs to all applications including folders such as calendar, contacts, media and settings. These folders each contain information that is gathered from the same application on the paired devices. For example, the calendar folder would store event, alarms, important calendar dates and so on, events on the calendar of the paired phone that is synced to the smartwatch to notify the user

In /data/data/com.google.android.apps.fitness/shared_prefs it consists of the files

- /_account_store.xml : data variables used such as time of data, speed, walking and steps
- / com.google.android.apps.fitness_preferences.xml : data variables used such as notification_last_time_checked, notification_last_glocal_percent and fitness_application_checked_system_sensors
- /global_store.xml : data variables used such as global_store_is_ios with its value stated as false and global supported metrics such as time of day, distance, duration, speed, energy, expending, steps

All three files have valuable data, in context of an investigation which needs to have an idea of what an individual was doing at a certain time of day, these files if further analysed by another specialist may indicate information that implies what that individuals' activities were. If there was a change in speed you could assume that its use it running and dependent on the length of time the analyst can use it to accurately help create a timeline of the event when the crime was committed

4.4. Chosen Devices

There are a number of watches considered for this project, the main factors deliberated when deciding are suitability for investigation, accessibility, price, capabilities of the watch. With these factors considered one of the main phones that was primarily considered along with the Sony Smartwatch 3 was the Apple watch series 3. This was not chosen as the watch for the project, although it is easily available to the project in comparison to other watches and it is one of the most commonly used smartwatches on the market, Apples security capabilities seemed too time consuming in terms of attempting an investigation on an Apple device. During research it was implied that investigating Apple products lead to more complex methods with a lot of work arounds. In addition, there were only a handful of paper discussing

the investigation of an Apple watch majority of the papers read used Android devices when investigating watches. Furthermore, as mentioned previously the definition of what categorises as a Smartwatch has no exact answer, what has been stated is what is used when choosing the watched ensuring that the watches investigated are smartwatches and not activity monitor devices or other health and fitness devices.

In addition, both chosen devices being android devices allowed some of the procedures executed on these devices to have some similarities. This meant that once one device was rooted it was a lot simpler to root the other as the devices have very similar formatting. There were only a number of nuances in their methods that was faced. This convenience allows the process to be more efficient.

Even though having the difficulty of navigating between two machines throughout the investigation, having the access to both machines with differing Oss lead to a number of work arounds that helps the investigation to progress. The benefits of having two machines outweighed its complications.

4.4.1. Chosen Paired phone: Samsung Galaxy S6

The Samsung Galaxy S6 was chosen to be the paired phone, Samsung holds a large share of the market therefore this is an appropriate choice as it is a popular device to the public. It is ideal to have an android device as it prevents further incompatibility issues between the watch and the phone. In addition, the method of imaging and investigating android devices is much simpler in comparison to let's say an IOS device which is likely the other commonly used device. Utilising the same method for both devices also provides a control variable within the investigation. If the devices were investigated using different methods and tools that may imply that the results would not be as valid as different methods were used.

4.4.2. Chosen computer: MacBook

Similar to the phone the chosen computer to connect to the watch was also chosen as it was the most accessible machine at the time. When attempting to root the smartwatches there were a lot of small problems which were time consuming and seemed to have no solutions. To find a compromise a Linux Ubuntu virtual machine was created where the implementation

was attempted. This work around was to allow more compatibilities in terms of the android device and the machine as number of the solutions found online during research showed solutions to non-MacOSx machines. However new errors occurred such as the usb cable connection to smartwatch and virtual machine lead along with to new problems when running commands. This just led to more problems and was not worth the work around therefore the project went back to its original machine being MacOSx where the implementation continued, and the problems were eventually solved.

4.4.3. Chosen Computer: Windows 10 (Virtual Machine(VirtualBox))

A Windows 10 virtual machine was also used during the examination. There are a number of incompatibilities and inconveniences with setting up the tool Autopsy on the MacBook. To avoid these problems the virtual machine was created. This allowed the investigation access to the tool in its latest version. The MacBook also had autopsy configured however it was an older version with less capabilities which is not ideal for the investigation. In addition, Windows was also used when rooting the paired phone devices as the tools used for the process was also more suited to Windows. The files and software available was easiest to configure on the Windows machine rather than a Mac. It provided convenience being able to switch between the two. The virtual machines command line had very limited capabilities therefore doing the whole investigation on just that one machine was not possible. The creation of the machine was also not done until later on in the investigation, so the setup of other tools used such as ADB and fastboot were already installed on the Mac.

4.4.4. Chosen Smartwatch: Sony Smartwatch 3 SWR50

The Sony Smartwatch 3 is the primary watch chosen for this project as it one of the most commonly investigated watches mentioned when reading research papers. The articles and papers (Wilson, 2017) (Baggili, 2015) utilised as reference guides for this project's investigation used the same model therefore it provided a guideline for the investigation to be loosely followed. It also provides this investigation with previous data/results that can be built up on.

5. Future work

This project can progress in a number of different ways. The forensic analysis of multiple smartwatches with varying manufacturers such as Apple, Microsoft, Blackberry etc would lead to a more realistic scope in terms of gathered data from all different types of smartwatch operating systems. The comparison between all the available watches currently in the market may also be very revealing in a sense that you can see which manufacturers hold the most valuable data within their devices. In addition, different manufacturer use varied operating systems, investigating all the different OSs available will allow the guide/list of the most useful areas within the filesystem to be more specific to each OS.

In terms of data retrieval it can be experimented with different methods attempting to gather the vital information from the device without going through the standard processes. This allows the investigation to gain a hacker's perspective and would allow the development of a preventative measure in terms of future hackings. If the authorities are aware of the vulnerabilities, then technology can be developed to solve these weaknesses.

5.1. Notable Artefacts Discovered

There are a number of significant artefacts found during the investigation that worth making a note of. Paired device data is located in the folder /data/misc/Bluetooth which contains five subdirectories. One of the five subdirectories files is called .bt.mac.info which contained information about the connected Bluetooth device along with its device id and mac address.

Application notifications are broadcasted to the device through Googles gms services. During the investigation it was revealed that the directory shows a database with its application name and notification.

6. Conclusions

Looking back to the main question of this project, is forensic analysis of smartwatches worth further research and development for forensic analysts, if so what type of relevant and useful information can be retrieved? Yes, there is usefulness in furthering the research and development for forensic analysts. The project implementation illustrates that the

information found although distributed in varied memory blocks is of significant data found. The project explored which file locations within each device's filesystem has the most useful information. The three main memory blocks chosen to be focused on being /cache , /system and /data which exhibited a number of notable information that had the potential of being valuable digital evidence as demonstrated and emphasised by the screenshots. As the number of users increase which will have knock on effect on the number of crime. With these increases it is beneficial to further research and develop the current technology especially its security features. In addition, methods of finding specific information within smartwatches should be established and standardised to allow forensic analysts and authorities to use these devices to their advantage.

7. Reflection on Learning

During the attempt of rooting both device I came across a number of problems. Rooting the watch first was very time consuming as it was something I have not done previously. In hindsight if I did more research about the rooting of a device before attempting to do so in the first place, the understanding gained from that research could have helped progress the process. There were a lot of problems in terms of incompatibilities with files being uploaded. Once the first device was rooted the second only had a few nuances meaning that the process was a lot less time consuming. Both devices being Android devices meant that both methods of rooting were very similar, and some steps were even identical. With this in mind it may have been more ideal to have attempted the rooting of the mobile device then the smartwatch. Rooting a smartphone has a lot more guidelines in comparison to a smartwatch, when coming across a problem and looking for a solution online the volume of results for the phone was significantly higher in comparison. In addition the mobile phone as a device has more users than a smartwatch meaning that in general there would be more material online about the attempts of rooting that type of device. I faced a lot more problems when trying to root the watch than I did the phone. There was also more resources available in terms of the required files that was needed to be installed. Although it should be considered that maybe what I learnt from rooting the watch first is what made rooting the phone easier. It was logical to attempt to root the smartwatch first as it was the primary device to investigate as it held the most potential for finding the most interesting and valuable evidence that could have possibly been found.

As mentioned previously the creation of the Windows 10 virtual machine was later on in the examination as it was a work around for incompatibilities. If I only realised this sooner by looking at the problem at a higher level, then it may have saved a lot more time. A decent amount of time was spent attempting to use the older version of Autopsy and attempting to root the phone on the MacBook. If I stopped trying to solve each small problem for such long periods of time before moving on and finding a different solution to the problem and looking at the problem at a bigger scale, the realisation of creating a virtual machine with a different OS may have come sooner.

There was an attempt to examine a second watch for the project. However, there were a few issues that occurred during this attempt. The main problem was that the watch did not have the OS that it advertised when it was purchased for the project. The product stated that it was Android Wear which is Wear OS' predecessor however the smartwatches actual OS was completely different. This meant the methods used to investigate the two android devices that are involved in the investigation can no longer be implemented on this device. The product was then researched into to see if there was any material online relating to the forensic analysis of this specific device or even the rooting of this device, there were very minimal to no results. I tried to find a "Developer Options" within the device to see if it may have somewhat similar features to the android devices. However, the closest I got to a developer mode was typing a secret code in its keypad, the secret code being "*#3646633#" which lead to an engineering more. The options within the device was very limited which implies that its capabilities were also limited in comparison to an android device. In hindsight, there should have been a double check to ensure that the devices chosen where the correct one. Although an effort was made to ensure this the unwanted outcome still occurred and the watch was not used for the investigation. It was more time consuming and a dead end.

Furthermore, in terms of project management at a higher level there are a number of things I have learnt through the process of doing this project. Within the initial stages of the project and an initial plan written up, it provided a brief overview of how I wanted or how I expected the project to occur throughout the weeks. Meeting with my supervisor it was stated that the initial plans are loosely followed as there are a number of uncontrollable factors which leads

to a delay in the overall progress of the project. I had weekly hour meetings with my supervisor in which we discuss my current progress and what I plan on doing the next week, along with her feedback on the work I was producing. It was ideal to have these meetings weekly as it allowed be to have guidance throughout the project and allowed me to overcome a number of problems and issues with the project with great help and good advice from my supervisor.

The progression of the project especially in its initial stages was very slow, during the implementation attempting to root one of the devices, the smartwatch lead to a number of problems which was very time consuming. This caused a big delay on the overall progress of the project. I would seek advice from my supervisor in how to move forward in other areas of the project whilst I was stuck on this one so that there would be at least some progress elsewhere and I was producing some sort of work. In which she suggested the start of writing this report, there were only a certain number of areas of the report I could write about as this was still in the initial stages of the project therefore, she provided me with some pointers of what can be discussed at that time. This continued and as the implementation of the investigation of the project slowly progressed the more content I could produce in the report.

In addition, there were parts of the project where I could have asked for help and guidance from someone who had the technical knowledge of what I have having issues with at the time at an earlier stage. I discussed my project with a peer to help talk through the problem however the problem was so specific that general knowledge could have helped but only to a certain extent. Only when I started to look at the problem from a higher level, where I created a virtual machine to provide multiple work arounds to a number of issues I was facing was when great progress was occurring.

References

Baggili, I. &. (2015, August). Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. Retrieved from https://www.researchgate.net/publication/283734724_Watch_What_You_Wear_Preliminary_Forensic_Analysis_of_Smart_Watches

John Scheerhout, C. O. (2019, Jan 10). Retrieved from Manchester Evening News: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/murder-paul-massey-how-mr-15641732

QPM, D. J. (2012). Retrieved from Digital-detective.net: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Smartwatch Definition. (n.d.). Retrieved from Techterms.com: https://techterms.com/definition/smartwatch

Topic: Smartwatches. (n.d.). Retrieved from statista: https://www.statista.com/topics/4762/smartwatches/

Wearable device revenue worldwide 2016-2022. (n.d.). Retrieved from Statista: https://www.statista.com/statistics/610447/wearable-device-revenue-worldwide/

Wilson, C. (2017, October 29). Smartwatch Forensics – Discovering what the Watch Watched. Retrieved from Data Forensics Simplified — Software Tools for Digital Forensic Analysis: https://www.dataforensics.org/smartwatch-forensics/