Digital Investigation 29 (2019) 55–66

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Forensic analysis of Nucleus RTOS on MTK smartwatches

J. Gregorio*, B. Alarcos, A. Gardel

Instituto Universitario Investigación en Ciencias Policiales, Universidad de Alcalá, 28871, Alcalá de Henares, Madrid, Spain

ARTICLE INFO

Article history:
Received 21 November 2018
Received in revised form
15 March 2019
Accepted 17 March 2019
Available online 19 March 2019

Keywords:
Forensic analysis
Notifications
Instant messaging
Smartwatch
Wearable

ABSTRACT

Embedded personal devices as smartwatches can be a valuable source of information for the investigation of criminal acts, as they can store contact data, call records, instant messages, multimedia files and so, without requiring access to the connected smartphone. This paper presents the acquisition and forensic analysis done on different non-android smartwatches equipped with a low-cost MTK chip. In this article, we will present the results of a complete study about the information contained in these smartwatch models, showing those artifacts that could be stored inside and might be critical in the investigation of a criminal act.

Introduction

Smartwatch devices are diverse in functionalities befitting from counting on not only the typical functions of a watch (time, date, alarm, etc.) but also features related to the smartphone connected to (calls, SMS, email notifications, instant messaging applications, etc.). Additional functionalities are provided using the information given by on-board sensors (positioning, heart rate, steps, motion, sleep, etc.) and embedded hardware such as bluetooth music player and camera. Therefore, the smartwatch devices are very attractive for both personal and professional use, with a large number of different applications managed from the connected smartwatch.

There are situations in which the forensic specialist must acquire and analyze the information on the smartwatch device, for example, seeking information about the latest instant messenger (IM) notification or positioning of the device. The smartwatches, as a general rule and depending on the type, are not used as a primary means in the execution of a criminal act, although they can store relevant information. These information and functionalities make these devices very promising in police investigations.

Fig. 1 shows an ordered list with the main companies of wearables (Global Wearables Market, 2017). There are companies such as Apple, Fitbit, Xiaomi, Garmin or Huawei, which have the most important share in the business of smartwatch devices.

Within the "Others" category we find devices that do not belong to well-known companies like low-cost smartwatches. In fact, these devices are currently the best option for those people looking for a smartwatch at an affordable price but with mid-level capabilities. Besides, there is a continuous growth in the sale of these low-cost smartwatches (Smartwatch unit sales wo, 2014).

High-end smartwatch devices are able to make calls, send text messages, use instant messaging applications by means of their own data connection through a dedicated SIM card operating as a mid-level smartphone. The forensic analysis of top smartwatches devices such as "Apple Watch" or "Samsung Gear" does not differ from the analysis performed on smartphones based on "watchOS" or "Android" with operating systems respectively. Commonly, low cost smartwatches are not based on these operating systems but execute a real-time operating system (RTOS) (Stankovic and Rajkumar, 2004) (Walls, 2012), (List of open source real-, 2018) e.g. "Nucleus RTOS" which manages and stores the information in a different way. This kind of devices, in general, requires a different forensic analysis methodology. In the study (orecasts Worldwide S, 2019), it is estimated that RTOS smartwatches market will have a growth by 2020 only exceeded by "watchOS" and "Android Wear", over others like "Tizen" or "Pebble".

The goal of this paper is to present the data acquisition and forensic analysis carried out on different models of low-cost smartwatches running "Nucleus RTOS", showing the results obtained from the study of the information acquired.

* Corresponding author.
E-mail addresses: jesus.gregorio@edu.uah.es (J. Gregorio), bernardo.alarcos@uah.es (B. Alarcos), alfredo.gardel@uah.es (A. Gardel).

https://doi.org/10.1016/j.diin.2019.03.007
1742-2876/

Top 5 Wearable Companies by Shipment Volume, Market Share, and Year-Over-Year Growth, Q4 2017 (shipments in millions)

Company	4Q17 Shipment Volumes	4Q17 Market Share	4Q16 Shipment Volumes	4Q16 Market Share	Year Over Year Change
Apple	8.0	21.0%	5.1	14.4%	57.5%
Fitbit	5.4	14.2%	6.5	18.5%	-17.3%
Xiaomi	4.9	13.0%	5.2	14.7%	-4.5%
Garmin	2.5	6.5%	2.3	6.6%	4.7%
Huawei	1.6	4.3%	0.8	2.4%	93.2%
Others	15.6	41.0%	15.3	43.5%	1.7%
Total	**37.9**	**100.0%**	**35.2**	**100.0%**	**7.7%**

Source: IDC Worldwide Quarterly Wearables Tracker, March 1, 2018

Fig. 1. Top 5 wearable companies, Q4 2017.

The article is organized as follows. The state of the art on forensic analysis and digital security research on smartwatches is discussed in the next section. Then, the proposed methodology to conduct the analysis on low-cost smartwatches is described in section 3. The Forensic analysis of data extracted from smartwatches is described in depth in section 4. Finally, several conclusions are summarized in section 5.

Related work

Concerning the forensic analysis of smartwatches, many of the research papers currently published are focused on the study of the high-end smartwatches as the “Apple Watch” or “Samsung Gear” and the analysis of artifacts that can be found in their operating systems “watchOS” or “Android”. Likewise, many of these studies perform a brief analysis of the artifacts that are stored in the smartwatch.

In the work “Analysis of Android Smart Watch Artifacts” (Parikh et al., 2015), the authors conduct a study on extraction and search of different artifacts (paired device information, voice commands, Bluetooth packet analysis, logs, notifications, recent tasks, etc.) stored in an Android-based smartwatch. Likewise, in (Baggili et al., 2015) the authors perform an analysis of the artifacts generated by two Android smartwatch devices (Samsung Gear 2 Neo and LG G watch), focusing the study in the data acquisition techniques. In (Alabdulsalam et al., 1801) the logical and physical acquisition of data located in the connected iPhone smartphone is done via the analysis of the information shown on the screen of the smartwatch. In the study “Live acquisition of main memory data from Android Smartphone and smartwatches” (Yang et al., 2017), the authors make a detailed analysis of the limitations in the available methods for the acquisition of data stored on the internal NAND flash (rooted, secure boot, custom kernel, recovery). Additionally, they extract data information through the hacking of firmware update protocols on several Android devices. Finally, it is worth mentioning the article (RongenGeradts, 2017) about the extraction and forensic analysis of the artifacts located in the wearable “Google Glass”, also based on Android.

As it has been shown, previous works are focused on the study on the different forms of acquisition and analysis of the information in Android/Apple smartwatches, not very different from the forensic analysis of a smartphone with the same operating system. For this reason and due to the lack of references, our paper conducts a study on the acquisition and forensic analysis of low-cost smartwatches with RTOS.

Methodology

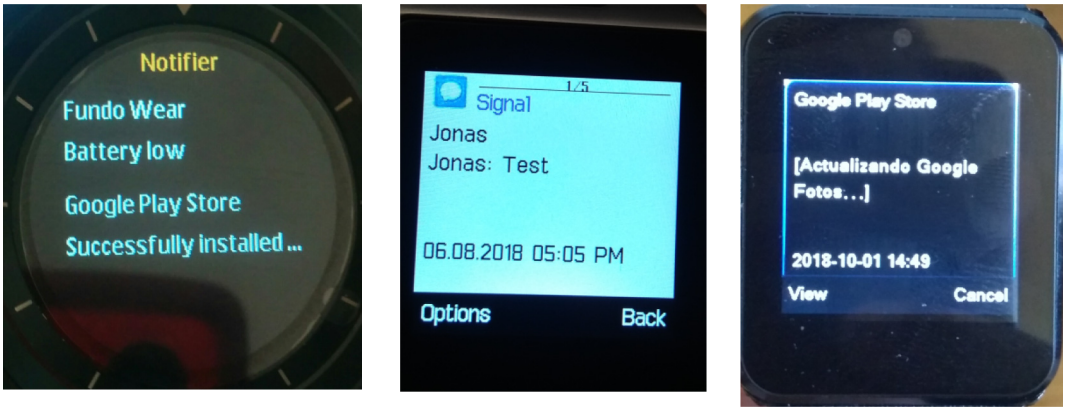
This section presents our working for the study of the information stored in low-cost RTOS smartwatches. Multiple data acquisitions of the devices under study have been performed to validate the relevant information location for different states of use considering a comparative analysis of the retrieved information.

For this study, we have selected three low-cost smartwatches corresponding to the models “NO. 1 G6”, “CAWONO DZ09”and “KINGWEAR GT08”. These devices have been selected because of their low cost (less than $30), similarity of capabilities, proprietary operating system and MTK chip processor (MTK2502DA, MTK6261D). These smartwatches have been linked through a Bluetooth connection to the same smartphone “LG Nexus 5” with an Android OS 6.0.1. The management of the notifications received in the smartwatches is done using the applications recommended by the manufacturers, enabling the communication of different types of notifications between the smartphone and the smartwatch (text messages, IM applications, system notifications, etc.). In order to carry out this study, the notification applications “FundoWear” and “BTNotification” will be installed and configured on the smartphone linking all type of notifications received in it, both user and system notifications. Fig. 2 (a, b, c) shows different examples of system and IM application notifications, corresponding respectively to the smartwatches under analysis.

Currently, commercial forensic tools are able to perform the acquisition and forensic analysis of a very small number of smartwatches, focusing on those high-end devices with a large market share (“Samsung”, “LG”, etc.). No specific forensic tools conduct the acquisition of the information contained inside these RTOS smartwatches. Beyond a manual acquisition or recording of the content of the screen, the forensic specialist must make use of other tools that allow the extraction and subsequent analysis of the information of the smartwatches with “Nucleus RTOS”. In particular, we will use the application “FlashTool” to acquire the memory contents out of the analyzed smartwatches. This application is developed “MediaTek Inc” and provided by each smartwatch manufacturer (Flashtool, 2019). It is used to update the firmware, flash recovery and information from any MTK chip model.

We will use the commercial forensics software “Cellebrite Physical Analyzer” Version 7.9 and Data Recovery application “R-Studio” Version 7.8.160829 to perform the forensic analysis of the above device memory acquisitions.

Next section describes the main results obtained from the study of the artifacts located in the different low-cost smartwatches, as



(a) Smartwatch "NO.1 G6" (b) Smartwatch "CAWONO DZ09" (c) Smartwatch "KINGWEAR GT08"

Fig. 2. Notifications example for the different smartwatches.

well as the different questions that may arise from the analysis performed.

Forensic analysis

Low-cost smartwatches as the three smartwatch models analyzed are based on a RTOS that provides the basic capabilities necessary for the management of the device itself. Such systems, also known as "Real-Time Embedded Systems" (Fan, 2015), have been developed to manage, in real time, the information with minimal hardware resources and reduced storage data (Shukla et al., 2018).

Specifically, the OS executed on the three smartwatches under study is "Nucleus RTOS", being a proprietary operating system with closed source code, deployed in about 3 trillion of devices (Nucleus RTOS, 2018) (Nucleus RTOSIOT, 2018). "Nucleus RTOS" supports different types of file-systems, including "File Access Table" (FAT) or "Nucleus SAFE" (Nucleus RTOSStorage, 2018). Similarly, it supports the use of relational databases as "Sqlite", however, there is no trace of this type of file in the devices studied.

Because "Nucleus RTOS" is a proprietary and closed-source customized version done by the manufacturer, we need to study the information stored on it by reverse engineering comparing the acquisitions retrieved from the three different smartwatch models. Specifically, the study of the information analyzed tries to answer different questions related to the data stored inside the smartwatch and that may be useful in the investigation of criminal acts. The list of objectives of this study can be as broad as the diversity of information that can be stored by the smartwatch. Let us summarize different specific issues that our paper will answer:

1. Acquisition of information: Define the methodology to acquire the data from this type of devices without forensic tools.
2. Information Analysis: What kind of information stores the linked smartwatch.
   - Get from the smartwatch the contact list stored on the device.
   - Get traces of call logs and/or text messages.
   - Get traces of notifications received on the linked device.
   - Get records of data related to the linked smartphone.

Fig. 3 shows the procedure followed corresponding to the different processes of acquisition, analysis and presentation of results, which will be described later in this paper.

The forensic specialist must identify the smartwatch in order to check the model of MTK chip included, because depending on the model, it is possible to know the type of operating system installed. If it is a smartwatch with supported operating system ("Android", "Android Wear", "watchOS", etc.) it will be possible to make use of the different forensic tools both for the acquisition and for the data analysis. In our case, the smartwatches use a "Nucleus RTOS", so a new procedure has been set up. The forensic methodology followed is based on the comparative analysis of the artifacts obtained from each of the tested smartwatches at a certain time. Each item studied in our forensic analysis has been evaluated through 3 phases (followed sequentially for each smartwatch).

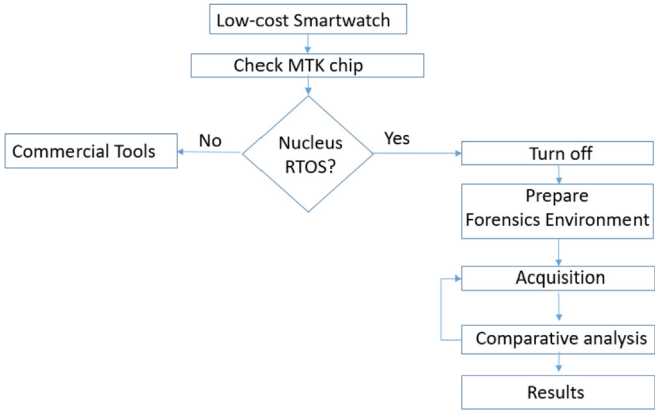


Fig. 3. Flowchart with the analysis procedure.

In a first phase, the data is generated on the smartphone with the desired operations to be analyzed, for example, sending a WhatsApp message, SMS or call record. In a second phase, the smartphone is linked to each one of the smartwatches, synchronizing all the smartwatches, storing the same information and reaching the same state. In this new state, the acquisition of the flash memory of each smartwatch is performed. In the third phase, the analysis of the information extracted from the different smartwatches is carried out, checking both the location and content of the files that the artifacts store. In this analysis we compare the information among the smartwatches to obtain similarities and differences.

These 3 phases must be repeated for all those actions or events that we wish to analyze, extracting a series of conclusions regarding the way in which the information of Nucleus RTOS smartwatches is structured.

Acquisition

There are several aspects that the specialist must know before performing the acquisition of the information contained in a smartwatch with an MTK chip. On one hand, depending on the MTK chip model, as in the case of the models studied, these devices, will have a reduced storage capacity, being in many occasions, less than 4 MB. In this small size is stored the firmware of the device, which is divided, as a general rule, in a bootloader (process to start the operating system), the operating system and a data partition (which stores the user information). On the other hand, the memories are usually NOR flash memories, which have "wear leveling policies" and "garbage collection services" running in the Flash Translation Layer (FTL) (Kumar Panigrahi et al., 2014) (Boukhobza et al., 1209). The "wear leveling policies" distribute the information through the whole memory space, reallocating logical sectors to different physical sectors. The "garbage collection services" will then re-structure the information indicating which of those sectors are marked as occupied or free. Although these processes improve the efficiency and useful life of flash memories, from a forensic point of view it can result in a loss of information when a restructuring of the memory occurs, overwriting parts. Therefore, the information obtained in the acquisition of this type of smartwatches depends on the available storage memory size as well as the execution of both the "wear leveling policies" together with the "garbage collection services". We have used the UFED Physical Analyzer plugin to process data retrieved from current FTL used pages and flash memory sectors marked as free has not been processed in this work.

The acquisition of the information requires the connection to the different pinouts of the JTAG port located on the PCB (Printed Circuit Board) shown in Fig. 4 (a, b). Due to the size and location of these pinouts, this operation can be quite laborious and should be done by a HW specialist, because, any bad practice can corrupt or destroy the evidence. Commonly, the MTK specific model included in the smartwatch can be read printed on top of the chip.

The smartwatch data can be downloaded by making use of different applications available for flashing or updating the device. This communication is done using a USB-type connection integrated into the smartwatch and through the installation and correct configuration of the drivers corresponding to the MTK chip in the host computer.

In our case, for the acquisition of the information contained in the smartwatches, the "FlashTool" application has been used. Although "FlashTool" is not a forensic tool, as it is developed by "Mediatek Inc" to do updates and backups from their MTK chips, it can be assumed that the acquisition process with the Read Back option makes a valid read operation, without writing the device memory. Our tests have confirmed the correct operation of FlashTool on all the smartwatches analyzed.

The procedure requires to turn off the smartwatch device and then connect to the forensic computer. Then the "FlashTool" application will gain access to the internal memory of the device. Fig. 5 shows the recognition of the smartwatch as "MediaTek USB port (COM7)" within the device type "port (COM and LPT)" in the "Desktop manager" tab.

Additionally, if the device is switched on, the forensic specialist can introduce a series of codes to access different configuration menus which provide more detailed information about the current smartwatch (How to Hack Chinese (Wat, 2018). In particular, "Engineer mode" menu provides information regarding the device's specific chip model. The engineer mode codes could be obtained from different ways: i) analyzing the flash memory of other identical device, ii) extracting the information from the manufacturer technical manuals or iii) downloading it from specialized technical online sites.

In the case of the devices analyzed to grant access to "Engineer mode" the technician must type in the call option of the smartwatch, the code "*#993646633#" in the case of the model "NO. 1 G6" and "*#3646633#" in the case of models "DAWONO DZ09″ and "KINGSTART GT08".

On the other hand, if the smartwatch is switched off, the most reliable way to know the specific chip model, would be to open the

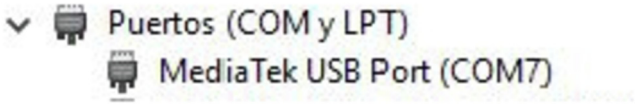
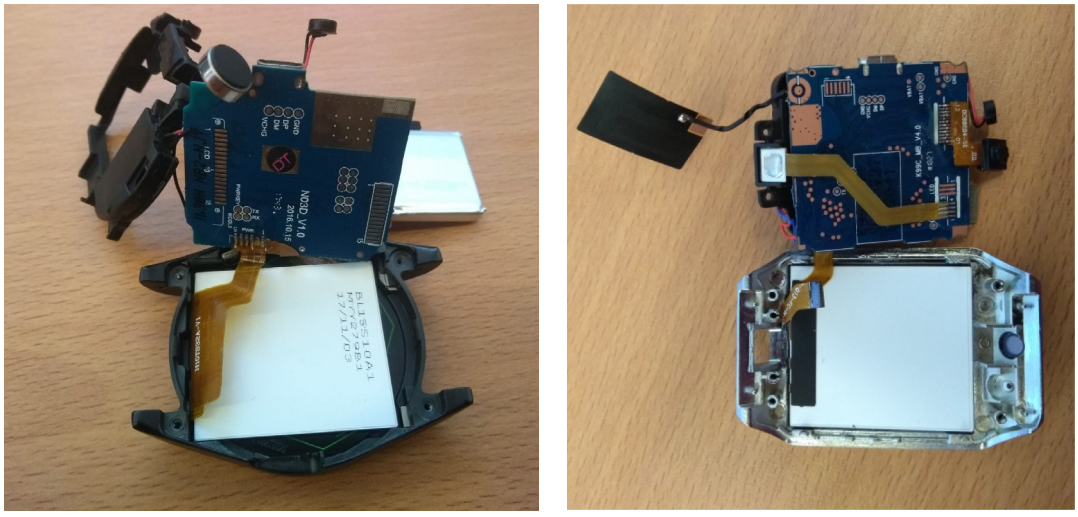


Fig. 5. Smartwatch MTK Chip recognized in Windows operating system. MediaTek USB Port. port COM.



(a). Smartwatch "NO.1 G6". (MTK2502DA)

(b) Smartwatch "CAWONO DZ09". (MTK6261D)

Fig. 4. PCB smartwatches.

device case finding the version printed on the corresponding chip, because, there is the possibility that the same smartwatch model has different versions of MTK chip.

Once the MTK chip model of the smartwatch is known, the specialist must retrieve the memory data structure. This information can be obtained from the different files that compose the firmware of the device. In order to make the correct acquisition of the information contained inside the internal memory of the smartwatch, the application "FlashTool", requires two files. The file "Download Agent" is used by the tool to correctly read and write on the device memory and the "Scatter file" or configuration file that contains the structure of the information in the Flash memory. Agent file and scatter file can be downloaded from the manufacturer web site, for example, the firmware for the NO.1 G6 model can be downloaded from "http://en.001phone.cn/download-55.html".

In Fig. 6, it is shown the selection for the "Download Agent" and "Scatter File" of the "FlashTool" application with the corresponding files "MTK_AllInOne_DA.bin" and "config_mtk.cfg", related to the smartwatch "CAWONO DZ09″ with the chip model "MTK6261D". The labelled address ranges (begin-end) correspond to the length of each firmware file required to update the device flash memory. The region addresses are related to the current smartwatch device. They are used for the firmware update process not for the "Read Back" operation.

In Fig. 6, the file named "config_mtk.cfg" included in section "Scatter File" corresponds to the "Configuration file" that contains the structure of the information in the flash memory of the device "DZ09" with "MTK6261" chip. The configuration file depends on the MTK chip model, existing differences in the structure of information between the smartwatch "DZ09" with "MTK6260" and the same smartwatch with "MTK6261" chip.

Fig. 7 shows some of the information contained in the configuration file "config_mtk.cfg" with the structure of the smartwatch "DZ09" on a "MTK6261" chip.

Once you have defined the data corresponding to the "Download Agent" And "Scatter File" the information is accessible from the "Read Back" tab. The forensic specialist must provide the start address value and internal memory size to be acquired (length) which is specific for each MTK chip model (shown in the scatter file).

Therefore, in Fig. 8, the acquisition is configured with a start address equal to "0x00000000" and length value "0x00400000", corresponding to the maximum size of the storage capacity (4 MB) for the "MTK6261D" chip of the smartwatch "CAWONO DZ09". As a result of this operation, the application creates a file named "ROM_0″ which stores the acquisition of the device flash memory.

File system mapping

In order to automate the analysis of the different acquisitions done for the different low-cost smartwatches ("NO. 1 G6″, "CAWONO DZ09" and "KINGSTART GT08"), the commercial forensic tool "UFED Physical Analyzer" will be used. Although this tool does not perform the specific analysis of the information contained in smartwatches, it already has a series of "chains" or processes that help the forensic specialist to quickly process the data information available.

Hence, the forensic specialist will be able to carry out each acquisition on the different smartwatches (see Fig. 9), by means of the "Open (Advanced)" option from the "File" menu of the "UFED Physical Analyzer" application. In this option the string specified in the section "Switch Chain" will be selected together with the acquisition file in the section "Binary dumps" (file "ROM_0" shown in Fig. 8).

Next, the specialist will select the chain "Non-Android MTK" within the "Switch Chain" option. As shown in Fig. 10, this chain executes a series of scripts to perform the decoding of the information, among which is "MTK NOR", corresponding to the type of memory of the devices analyzed.

After the selection of the chain, the forensic specialist will select the file with the acquisition by means of the option "NOR Select file" of the section "Binary dumps". The forensic application "UFED Physical Analyzer", perform a decoding of the information contained in each acquisition, cataloging in "Data files" section the different artifacts that are identified in the analysis performed. As shown in Fig. 11 (a, b, c), in the case of our analysis carried out on low cost smartwatches, the tool only identifies three types of files, corresponding with image files, text files or "uncategorized", not providing more information on the artifacts generated in the devices under study, as it does in other analyses. The specialist can navigate through the "FAT" file system recognized by the tool.

The "R-Studio" tool has been used to validate the information obtained from "UFED Physical Analyzer" in the forensic analysis of different device acquisitions. This tool is commonly used by forensic analysts to acquire the device file system and file structure, to verify the validity of a forensic image obtained from another acquisition tool, for example "UFED Physical Analyzer". Fig. 12 shows the file structure retrieved by "R-Studio" for the "KINGSTART GT08" smartwatch.

The result of the analysis of the information on the structure of the file system, as well as the information contained in its files, will be presented in the next section, describing those artifacts that have been found in the "NO NAME" system files of the different acquisitions made on the smartwatches devices under study.

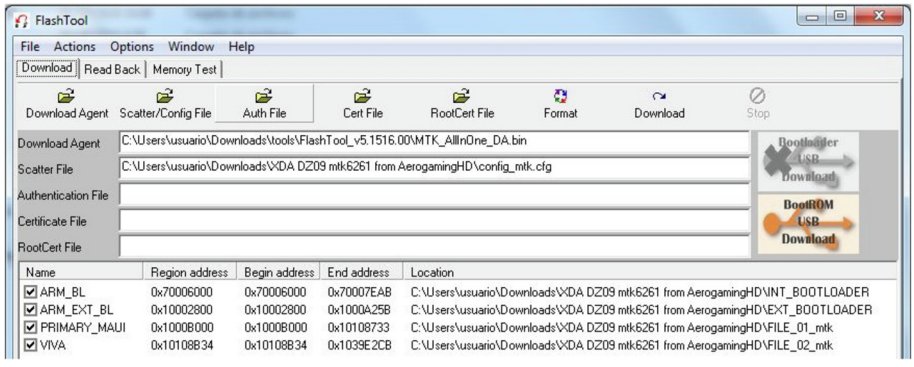


Fig. 6. FlashTool application. Download configuration.

```
general:
    config_version : alpha # config file version (alpha, beta is used before SQC done.)
                           # After SQC done, the version should be 1 for the first release version.
    platform:              # It is used for tool to identify the right setting for specific target

boot_region:
  alignment: block         # block[default], page(NAND:2K/512B, NOR: 1KB, eMMC: 512B, SF: 256B)
  rom:
    - file: INT_BOOTLOADER
    - file: EXT_BOOTLOADER

control_block_region:
  rom:

main_region:
  alignment: block         # block[default], page(NAND:2K/512B, NOR: 1KB, eMMC: 512B, SF: 256B)
  rom:
    - file: FILE_01_mtk
    - file: FILE_02_mtk

file_system_region:
  rom:
```

Fig. 7. Example of configuration file - “Scatter File” for the MTK 6261 chip.

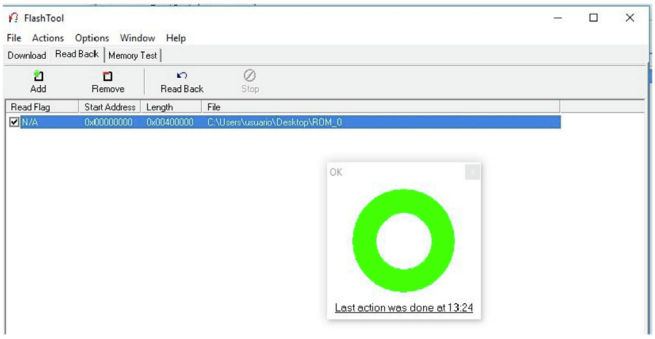


Fig. 8. Application “FlashTool”. Read Back operation.

Data analysis

This section presents the study carried out on the different artifacts contained in the data partition of the different smartwatches under analysis. In each of the acquisitions the three smartwatches analyzed will contain the same data, related to the contact list, text messages, notifications and so on. Finally, different analyses of the information stored in each of the three devices will be conducted, exposing the comparison results obtained.

Information regarding contacts

Analyses showed several common files with the names “LIST.TMP” and “ENTRY.TMP” located inside of the folder “NO NAME/@PBAPC” and containing the records related to the contact list of the linked smartphone device. “LIST.TMP” contains only the contact names whereas “ENTRY.TMP” contains the list of names and associated telephone numbers. Figs. 13 and 14 depicts part of these files. From Fig. 13 we identify the name “Jonas”, a contact name located in the phonebook of the linked smartphone, and in Fig. 14 the contact “Jonas” and his phone number are also distinguished.

Therefore, it has been concluded that from the analysis on the file system of the different smartwatches, inside the directory “NO NAME/@BTDIALER” an identical copy of these files exist.

Calls log

Located inside of the folder “NO NAME/@BTDIALER” is the file “FOLDER. TMP”, which contains among other, the information related to the calls log. The calls log located in this file are structured using the “BEGIN:vcard” and “END:vcard” tags, which can be found in the information related to the name, phone number, date and type of call registration (dialed, missed, etc.). Fig. 15 shows several call logs contained in the file “FOLDER. TMP”.

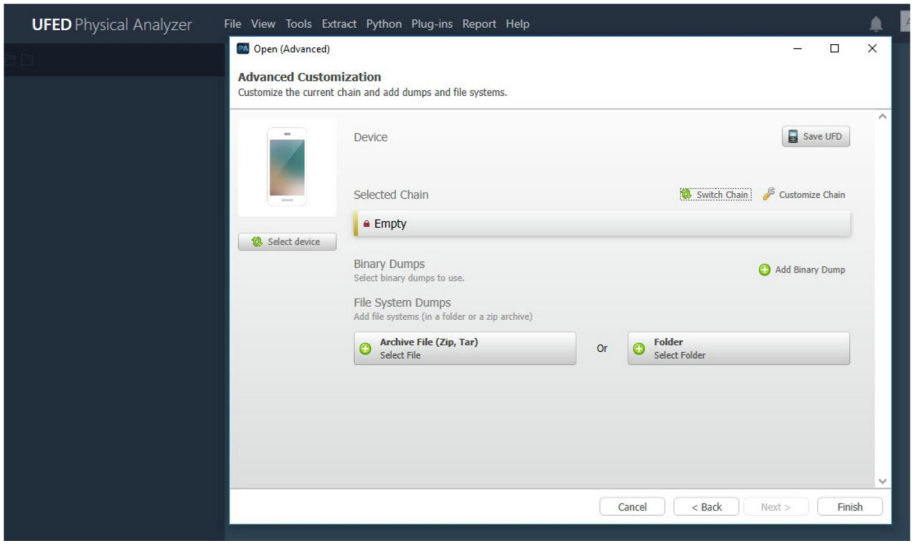


Fig. 9. Open (Advance). UFED physical Analyzer.

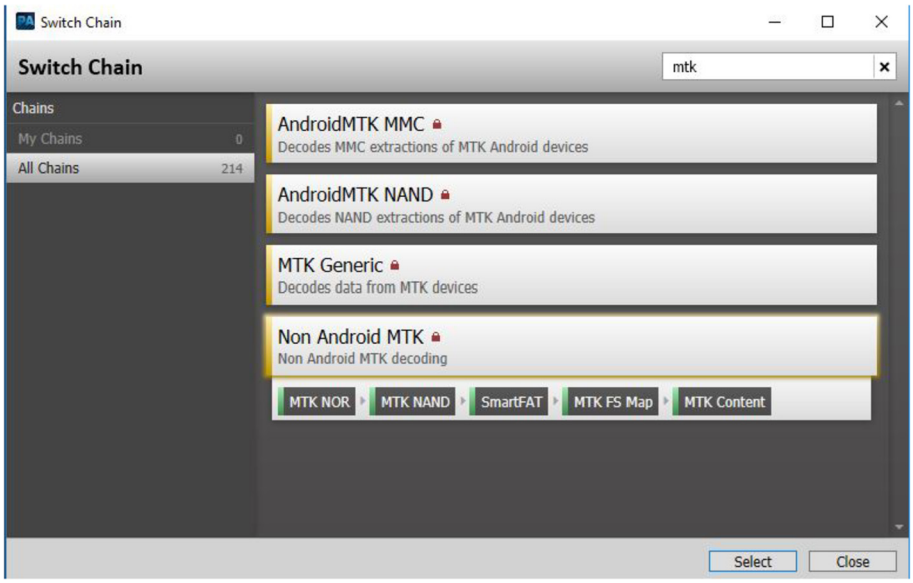
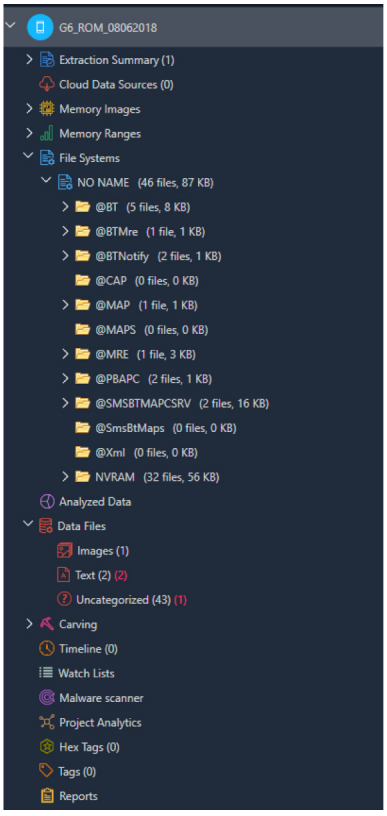
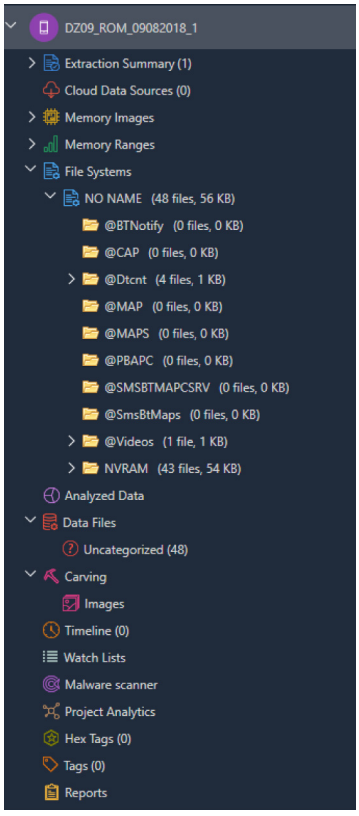


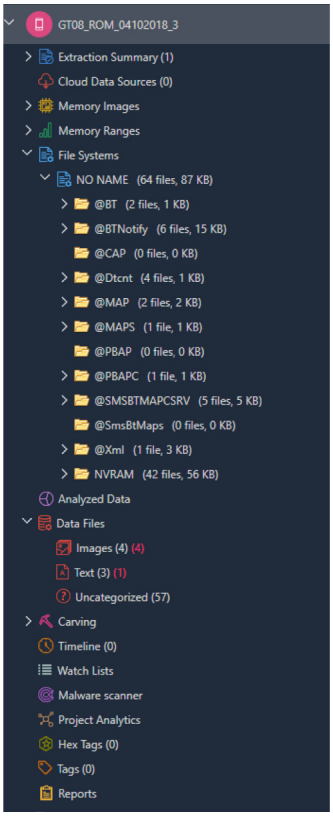
Fig. 10. Switch chain. UFED physical Analyzer.



(a) Smartwatch "NO.1 G6"



(b) Smartwatch "CAWONO DZ09"



(c)Smartwatch "KINGSTART GT08"

Fig. 11. UFED Physical Analyzer Filesystem example.

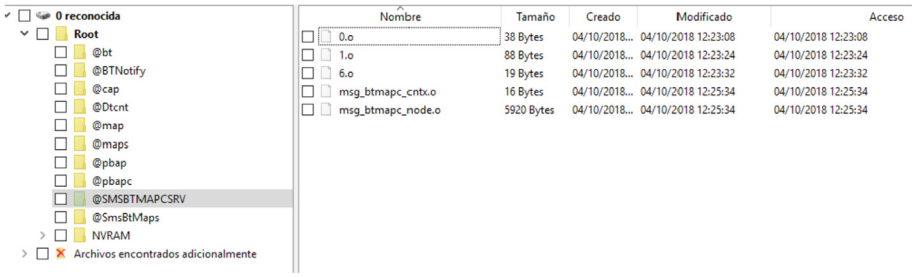


Fig. 12. R – Studio. Filesystem example smartwatch "KINGSTART GT08".

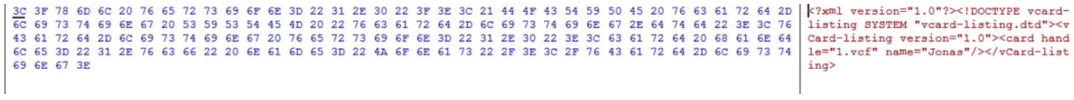


Fig. 13. Content sample of "LIST.TMP" file located in the folder "NO NAME/@PBAPC"

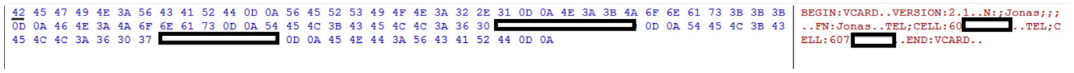


Fig. 14. Content sample of "ENTRY.TMP" file located in the folder "NO NAME/@PBAPC". Some data have been hidden to ensure the privacy of the user.

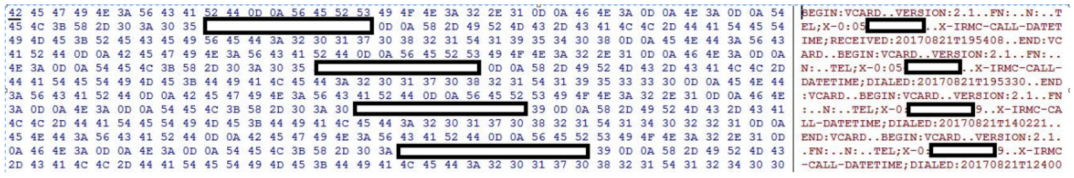


Fig. 15. Content sample of FOLDER. TMP file located in the folder "NO NAME/@BTDIALER". Some data have been hidden to ensure the privacy of the user.

Fig. 16 shows an example, of a registered call made, where the different fields appear between the tags "BEGIN:vcard" and "END:vcard"

Fig. 16. Call log example for a registered call made. File FOLDER. TMP located in the folder "NO NAME/@BTDIALER". Some data have been hidden to ensure the privacy of the user.

It has been concluded that from the analysis on the system of files of the different smartwatches under study, inside the directory "NO NAME/@PBAPC/" an identical copy of these files exists.

Text messages

Text messages are stored independently in different files with nomenclature {number}".O" which are stored inside the folder "NO NAME/@SMSBTMAPCSRV". Fig. 17 shows an example content, a text message which is in the "1. O" file.

Additionally, all text messages can be stored in a single file, "msg_btmapc_node.O" located in the same folder "NO NAME/@SMSBTMAPCSRV" as shown in Fig. 18.

Furthermore, inside the directory "NO NAME/@MAP/" exists the file "bt_notify_map.vcf" which contains records related to SMS-type notifications, with a data structure defined between "BEGIN" and "END" tags, with the following relevant data: name, phone

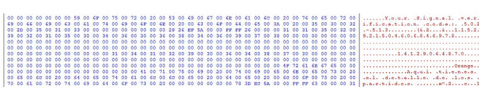


Fig. 18. Example content of the file "msg_btmapc_node.O" located in the folder "NO NAME/@SMSBTMAPCSRV".

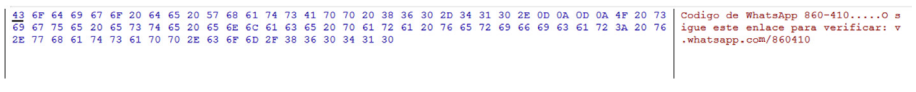


Fig. 17. Example content of the file "1. O" located in the "NO NAME/@SMSBTMAPCSRV" folder.

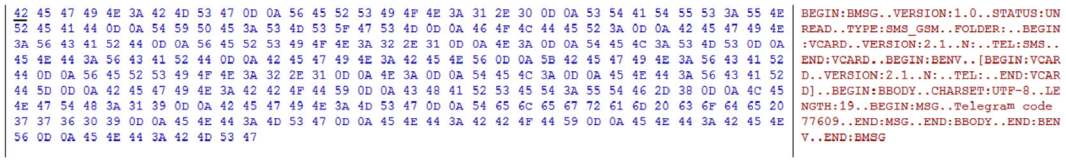


Fig. 19. Example content of the file "bt_notify_map.vcf" located in the folder "NO NAME/@MAP"

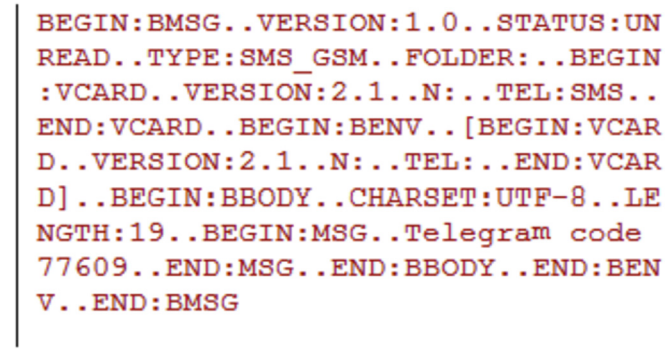


Fig. 20. Example of content message for a registered call in file "bt_notify_map.vcf" located in the folder "NO NAME/@MAP"

number, date, status, length of the text or text of the message. Fig. 19 shows an example content of a text message contained in the file "bt_notify_map.vcf".

Besides, also in the same file "bt_notify_map.vcf", in Fig. 20, it is shown the record of a registered call, where the different fields appear between the tags "BEGIN:BMSG" and "END:BMSG". Among these tags, there is a nested data structure with more "BEGIN" and "END" tags (VCARD, BENV, BBODY, and MSG). It is straightforward for the forensic specialist to extract the data from this structure.

Notifications

After a comparative analysis of the information retrieved from the 3 smartwatches following the same steps in the application of the linked smartphone we have found that the file "bt_notify_0000. xml" located inside the folder "NO NAME/@BTNofity" is an XML file that stores the data about the last received notification on the smartwatch device. Among the different fields contained in this file are the following: the message identifier (msgId), the application that makes the notification (sender) the application identifier (appId), the notification content (ticker_text) and the date of the notification (timestamp).

Fig. 21 shows the contents of the file "bt_notify_0000. xml", in which is observed, among others, the field "category" with the literal "notification", the field "sender" with the name of the application "BTNotification", the field "ticker_text" that contains the text of the notification "WOO Partner connected remote device" and field "timestamp" contains the message date in epoch-unix format "1538648733" (Thursday, October 4, 2018 12:25:33 PM - GMT + 2).

Additionally, located inside the folder "NO NAME/@MAP "exists the file named "bt_notify_map.xml", an XML file which contains an index of the notifications linked in the smartwatch. This file, among other fields, contains a numeric identifier (handle), the date of dispatch (datetime), name of the application or number that sends the notification (sender_name), the type of notification (type), size or if it has been read (read). Fig. 22 shows an example content of the data structure stored in the file "bt_notify_map.xml" related to a notification.

Fig. 21. Example of the file "bt_notify_0000. xml" located in The "NO NAME/@BTNotify" folder.

Bluetooth connections log

The files "COD" and "DEVDB" located in the directory "NO NAME/@BT" contain, among other information, the Bluetooth address of the linked device or smartphone devices, although this data is stored in the reverse direction. Fig. 23 (a, b), show the content of file "COD", with the value "0 × 70B9AAD0A9F8″ corresponding to BT address "F8:A9:D0:AA:B9:70".

The stored value "0 × 70B9AAD0A9F8″ corresponds to the Bluetooth address "F8:A9:D0:AA:B9:70" of the linked smartphone, as it can be seen in Fig. 24.

Similarly, the files "MP26_001 and MP80_000″ located in the directories "NO NAME/NVRAM/NVD_DATA" and "NO NAME/NVRAM/NVD_DATA/PACKALID" contains information about the device name of linked smartphone and Bluetooth address. Fig. 25 shows, as an example, the contents of the file "MP26_0001" which identifies the name of two linked smartphone devices and their respective Bluetooth addresses.

Additionally, the specialist can use the Bluetooth address of the device to obtain more information related to the linked smartphone. For example, Fig. 26 shows the identification of the device brand using the retrieved Bluetooth address.

Fig. 27 shows as an example, the contents of the file "MP80_000", with the name of the linked smartphone device.

Smartwatch device information

In file "MP25_001" located in the directory "NO NAME/NVRAM/NVD_DATA/PACKALID/", you can find information related to the name of the identifier and the Bluetooth address of the smartwatch. Fig. 28, shows as an example, the contents of the file "MP25_001", with the Unicode value "GT08″ corresponding to the name of the smartwatch device and the hexadecimal value "0 × 6162F7005A007F3A" (deleting 0x00) corresponding to its Bluetooth address "3A:7F:5A:F7:62:61".

```
MAP-msg-listing = [
  msg =
    Annotations : = [
      handle : attribute = 1152921504606846993
      subject : attribute =
      datetime : attribute = 20181001T145643
      sender_name : attribute = +17026604496
      sender_addressing : attribute = +17026604496
      recipient_name : attribute =
      recipient_addressing : attribute =
      type : attribute = SMS_GSM
      size : attribute = 38
      text : attribute = true
      reception_status : attribute = 0
      attachment_size : attribute = 0
      priority : attribute = false
      read : attribute = 0
      sent : attribute = true
      protected : attribute = false
  msg =
    Annotations : = [
```

Fig. 22. Example of the file "bt_notify_map.xml" located in the "NO NAME/@MAP" folder.

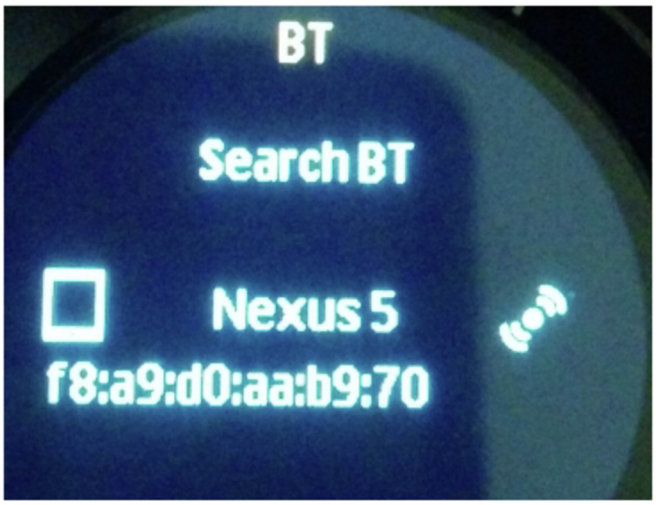


Fig. 24. BT address link notification shown in the smartwatch.

Conclusions

The amount of information stored inside the smartwatches implies that they should be subject to study by forensic specialists. The diverse capacities and multiple functionalities of this type of devices cause them to be one of the main data sources in the investigation of criminal acts. Such is the case of low-cost smartwatches, which, even with limited storage capacity, can store relevant information for an on going investigation. The acquisition and forensic analysis of this type of device can be critical, when, for example, a Smartphone is blocked or damaged and the information can be extracted from its linked smartwatch. Embedded personal devices as smartwatches can be a valuable source of information for the investigation of criminal acts, as they can store contact data, call records, instant messages, multimedia files and so, without requiring access to the connected smartphone. The forensic analysis of this type of devices is sometimes of vital importance (Smartwatch data proves A, 2019).

The paper has shown a systematic data acquisition and forensic analysis of low-cost smartwatches. It moves away from what would be a typical forensic analysis performed on high-end smartwatches with standard operating systems such as "Android" or "watchOS". It has been shown that current forensic tools provide a very limited support for this type of devices. These commercial forensic tools leave the low-cost smartwatch devices in the background, but as our analysis has proved, they can store relevant information related to the linked smartphone.

This paper presents the data acquisition and forensic analysis done on different non-android smartwatches equipped with a low-cost MTK chip. For the data acquisition, we have used the non-forensic tool "FlashTool". To quickly search for information in the whole unknown structured data of "Nucleus RTOS" based smartwatches, different forensic commercial tools have been applied, validating the digital evidence.

The analysis section has presented multiple results from a complete study about the information contained in the smartwatch models, showing those artifacts that could be stored inside and might be of interest in the investigation of a criminal act, for example, data related to contacts agenda, calls log, text messages, notifications, Bluetooth connections and linked smartwatch device

```
02 00 00 00 06 BB 05 3E 5A 1C 00 00 3C 04 08 00 70 B9 AA D0 A9 F8 0B F0 0C 02 5A 00 00 00 00 00 00 00 00 00 00 | .......>Z...<...p.....Z.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
```

(a) File "COD" located in the folder "NO NAME/@BT/".

```
01 00 70 B9 AA D0 A9 F8 00 84 FC E0 92 47 1B C9 56 CB 14 BA B5 03 CB F8 BA 00 00 05 04 00 00 00 00 00 00 00 00 00 00 | ..p.....G..V.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................................
```

(b) File "DEVDB" located in the folder "NO NAME/@BT/"

Fig. 23. Example of Bluetooth addresses of the linked devices.

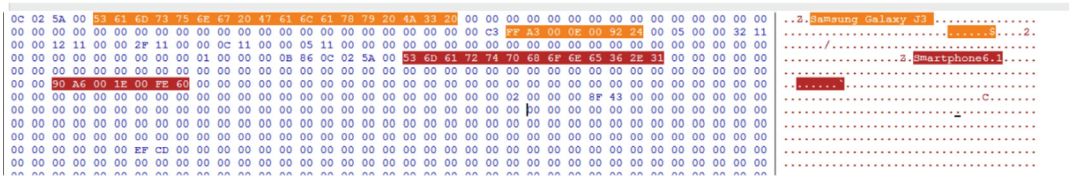


Fig. 25. Example file "MP26_001" located in "NO NAME/NVRAM/NVD_DATA/".

Fig. 26. Identification of device brand using Bluetooth address.

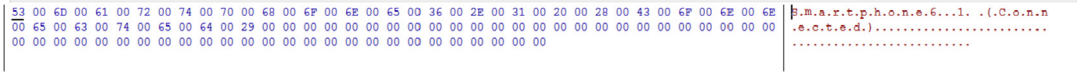


Fig. 27. Example of the file "MP80_000" contained in the folder "NO NAME/NVRAM/NVD_DATA/PACKALID/"

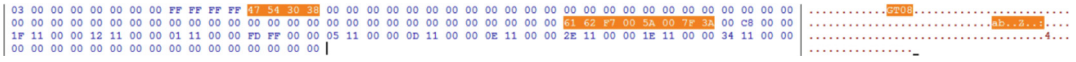


Fig. 28. Example of the file "MP25_001" located in the directory "NO NAME/NVRAM/NVD_DATA/PACKALID/"

information. The retrieved information from smartwatches can be priceless in certain police investigations.

References

Alabdulsalam, Saad, Schaefer, Kevin, Kechadi, Tahar, Le- Khac, Nhien-An. Internet of things forensics: challenges and case study. https://arxiv.org/abs/1801.10391.

Ibrahim Baggili, Jeff Oduru, Kyle Anthony, Frank Breitinger, Glenn McGee. "Watch what you wear: preliminary forensic analysis of smart watches". 2015 10th International Conference on Availability, Reliability and Security.

Boukhobza, Jalil, Olivier, Pierre, Rubini, Stéphane. A cache management strategy to replace wear leveling techniques for embedded flash memory. https://arxiv.org/pdf/1209.3099.pdf.

Fan, Xiaocong, 2015. Real-Time Embedded Systems, first ed. Design Principles and Engineering Practices.

Flashtool, M.T.K.. https://www.dtone.cc/smart-watch/g6.html?tab=down. Accessed Mar 2019.

Global Wearables Market Grows 7.7% in 4Q17 and 10.3% in 2017 as Apple Seizes the Leader Position, Says IDC. https://www.idc.com/getdoc.jsp?containerId=prUS43598218. Accessed Jun 2018.

How to Hack Chinese (watch) phone firmware. https://www.dr-lex.be/hardware/china_phone_flashing.html. Accessed Jun 2018.

Kumar Panigrahi, Sanjat, Maity, Chandan, Gupta, Ashutosh, March 2014. A simple wear leveling algorithm for NOR type solid storage device. CSI Transactions on ICT 2 (1), 65–76.

List of Open Source Real-Time Operating Systems. https://www.osrtos.com. Accessed Jun 2018.

Nucleus RTOS. https://www.mentor.com/embedded-software/nucleus/. Accessed Aug 2018.

Nucleus RTOS, IOT. https://www.mentor.com/company/news/mentor-nucleus-rtos-wearable-devices. Accessed Aug 2018.

Nucleus RTOS, Storage. https://www.mentor.com/embedded-software/nucleus/storage#. Accessed Aug 2018.

IDC forecasts Worldwide shipments of wearables to surpass 200 million in 2019, driven by strong smartwatch growth and the emergence of smarter watches. https://www.businesswire.com/news/home/20160317005136/en/IDC-Forecasts-Worldwide-Shipments-Wearables-Surpass-200. Accessed Jun 2018.

Parikh, Shreyas, Chavda, Dhaval, Chakraborty, Shourjo, Rughani, Parag H., Dahiya, M.S., August-2015. Analysis of android smart watch artifacts. Int. J. Sci. Eng. Res. 6 (8). ISSN 2229-5518.

Rongen, J., Geradts, Zeno, 2017. Extraction and forensic analysis of artifacts on wearables. Int. J. Forensic Sci. Pathol. 312–318. https://doi.org/10.19070/2332-287X-1700070.

Shukla, Amit K., Sharma, Rachit, Muhuri, Pranab K., 2018. A review of the scopes and challenges of the modern real-time operating systems. Source Title: Int. J. Embed. Real-Time Commun. Syst. (IJERTCS) 9 (1). https://doi.org/10.4018/IJERTCS.2018010104. https://www.igi-global.com/article/a-review-of-the-scopes-and-challenges-of-the-modern-real-time-operating-systems/193622.

Smartwatch data proves Australian woman killed mother-in-law, prosecutors say. https://www.foxnews.com/world/smartwatch-data-proves-australian-woman-killed-mother-in-law-prosecutors-say. Accessed Jan 2019.

Smartwatch Unit Sales Worldwide from 2014 to 2018. https://www.statista.com/statistics/538237/global-smartwatch-unit-sales/. Accessed Jun 2018.

Stankovic, J.A., Rajkumar, R., 2004. Real-Time Systems, vol 28, p. 237. https://doi.org/10.1023/B:TIME.0000045319.20260.73.
Walls, Colin, 2012. Chapter 7 - Real-Time Operating Systems, Embedded Software, second ed., pp. 243–286 https://doi.org/10.1016/B978-0-12-415822-1.00007-6.
Yang, Seung Jei, Choi, Jung Ho, Kim, Ki Bom, Bhatia, Rohit, Saltaformaggio, Brendan, Xu, Dongyan, 2017. Live acquisition of main memory data from Android smartphones and smartwatches. Digit. Invest. 23.