

ANALYSIS OF DATA REMANENCE AFTER FACTORY RESET, AND SOPHISTICATED ATTACKS ON MEMORY CHIPS

Mariia Khramova, Sergio Martinez

Blanco Technology Group

Abstract: Considering the amount of data stored on smartphones, it is critical that none of the user information is retrievable in case of device resell or disposition. Data security on disposed devices is one of the key enablers for device lifetime extension and, consequently, for making electronics more sustainable. Factory Reset, being default data wipe solution offered by Android, has already been challenged by researchers from University of Cambridge back in 2015. That has been the first comprehensive study and probably one of the most recognized works on evaluation of Android Factory Reset performance. The study proved that default erasure process is failing to securely sanitize the storage on Android versions from Gingerbread to Jelly Bean (v.2.3 – 4.3). However, despite frequent updates of Android OS, there was no further research conducted to reexamine Factory Reset reliability on newer devices and OSes. Our study has brought this line of research to the new level and investigated the changes of Factory Reset effectiveness over the past years. In addition, we have evaluated the robustness of in-built Android sanitization against attacks of different degree of sophistication including chip-level data read on one of the best-selling smartphones in history Samsung Galaxy S4 (80 Million units) [1]. The results show that Android Factory Reset logical sanitization has generally improved making user data more difficult to recover. However, default erasure process is still failing to irretrievably erase the data, which allowed us to retrieve the user data directly from the NAND flash bypassing the controller. Considering the share of smartphones running on Android Lollipop and below, over one third of Android devices (from Lollipop (5.0) and earlier) are vulnerable to improper storage sanitization. The magnitude of failing Factory Reset data sanitization is huge and despite the improvements the number of Android smartphones that may not properly sanitize the storage has grown by over 50% between 2015 and 2018. This means that over 770 million devices, that are currently circulating in the second-hand market, may still store previous owners' sensitive information, which represents serious security risk.

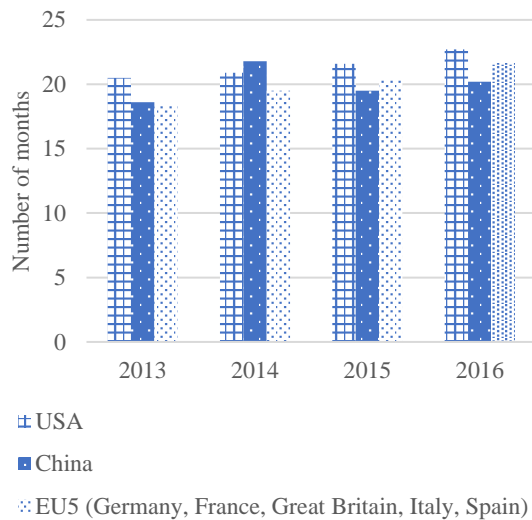
Keywords: Android, Factory Reset, data recovery, mobile forensics

1. BACKGROUND AND MOTIVATION FOR RESEARCH

Rapid technological development has quickly made smartphones an essential part of modern life, changed and redefined the concept of phone. High rates of smartphone adoption are being enabled by 1) technological improvements offered by modern devices, 2) growing diversity of offering in terms of models and manufacturers as well as 3) increasing affordability of smartphones ranging from low-cost entry-level models to the latest and greatest flagships. Since the introduction of the first iPhone and a year later Android phone smartphone industry has observed a steady growth [2] projected to reach 1.9 billion units shipped by 2018 [3]. Recent estimations

[2] show that by year 2021 40 percent of the global population will own a smartphone. These transformations have influenced not only smartphones' functionality and performance, but also affected the way people treat and dispose their devices. The main trend observed on smartphones' usage is short lifecycle and frequent upgrade rate. Even though average smartphone lifetime (Figure 1) observed in the US, China and five biggest European countries tends to increase, overall product lifetime is short. Smartphones are typically replaced within less than 2 years' time being disposed as frequently as general clothing or shoes [4].

Figure 1: Smartphone lifecycle [5]



There are various reasons behind smartphones life expectancy that are pushing users to upgrade their devices more frequently. These factors can be generally classified into the following groups:

1- Marketing

- a. Enhanced smartphone experience and new technologies [5]
- b. Compelling services and content [5] such as wearables, VR, AR, AI.

2- Product

- a. Design
Modern smartphones are featuring slick and slim design. This results in increasing popularity of glass as a key material for device casing explained by esthetic reasons and incorporation of wireless charging. Another trending feature is increasing screen size and bezel-less design.
- b. Durability
Smartphones are complex and fragile electronic devices which are prone to physical damage. Device drop, and water damage are the major factors influencing produce lifetime.
- c. Repairability
With few exceptions such as FairPhone (fully modular smartphone) and LG G5 (some parts are replaceable), modern smartphones have not been designed for repair. For instance, slim design has given preference of glue instead of screws, which makes it harder to access the internal components and hard or impossible to replace the parts. Extensive use of glass reduces the durability of the device.
- d. Obsolescence

Hardware (e.g. internal storage, RAM) and software wear (planned or occurring naturally) are making devices performance slower and affect user experience. For example, device may run out of storage.

3- Usage

Mainly related to the user's behavior and measures taken to care about device (protection cases, screen protectors).

Moreover, smartphones have firmly entered business environment, where on the top of already mentioned factors, there are additional drivers for fast smartphones' renewal. Among those are corporate policies determining certain period of time for work phone to be retired or security reasons. All these lead to constantly increasing number of smartphones that are not in use anymore. However, recycling rates are still very low. According to the EU project PROSUITE, only 11% of mobile phones are recycled, while over 60% of used phones are hibernating in homes or otherwise unaccounted for [4]. Sustainability and environmental issues related to the production and use of modern electronics are getting greater attention of the industry, academia and policy makers. Climate change, ecological problems and scarcity of natural resources are pushing towards taking actions to protect environment and more efficient resource usage. To support green initiative many companies are engaging into take-back and buy-back programs. The EU has launched a Framework Programme for Research and Innovation Horizon 2020 which goals also include resource efficiency and sustainability. Presented research has been undertaken within sustainablySMART project, which is part of the Horizon 2020 program. The main goal of the project is to enhance sustainable use of smartphone devices through redesigning the concept of smartphone, recycling and re-purposing of components and material recovery. Extremely high environmental footprint of smartphone production and end-of-life mobile assets disposal are the key challenges the project is aiming to combat. One fundamental aspect when considering the repurposing of technology is to ensure that data privacy and protection requirements are observed to prevent an unwanted data breach. The reuse of devices with storage components requires a sound process for data erasure. Moreover, the erasure process for flash-based memories can be hindered by the added complexity due to data management processes on a device. Blancco Technology Group (hereafter referred to as "Blancco"), being the leading provider of mobile device diagnostics and secure data erasure solutions, is managing the data security aspect of the sustainablySMART project with the primary aim of identifying the processes required to enable secure

disposal or repurposing of memory components. Since Android OS platform has a dominant position in smartphone market (Table 1) and is widely adopted across different phone manufacturers, it has been chosen as a targeted OS for research. Moreover, the closed nature of the second most popular platform, Apple's iOS, and restrictions on its analysis and modifications are representing serious problems when attempting to verify the quality of erasure.

Table 1: Smartphone OS market [6]

Period	Android	iOS	Windows	Others
2016 Q1	83.4%	15.4%	0.8%	0.4%
2016 Q2	87.6%	11.7%	0.4%	0.3%
2016 Q3	86.8%	12.5%	0.3%	0.4%
2016 Q4	81.4%	18.2%	0.2%	0.2%
2017 Q1	85.0%	14.7%	0.1%	0.1%

To erase the data prior to device disposal, users are offered a default solution, i.e. Factory Reset. Since secure data destruction has been identified as one of the major user concerns and a significant barrier for higher recycling rates, presented research aimed at evaluation of Android in-built sanitization function. The purpose of our study is to evaluate its effectiveness against various threats and tactics. These tactics have deployed according to the degree of their technical sophistication and time required going from less demanding to more challenging ones. Due to time and budget constraints, all the attacks except the most advanced known, have been performed in-house. The most sophisticated attack on mobile device storage has been performed by the independent 3rd party using bespoke custom-made tools. Analysis of smartphones recycling market has been performed to identify the most common phone manufacturers and smartphone models. Thus, test devices' sample consisted of 68 second-hand Android smartphones representing 9 vendors and Android OS versions varying from Ginger Bread (2.3.5) to Nougat (7.0). Our analysis of data remanence after Factory Resets shows that user data were still recoverable from 20% of the tested smartphones. Older Android versions still remain to be more vulnerable to improper device sanitization than newer ones. However, even on newer devices and OSes user data were still possible to recover. Though it required significantly more effort than before. Also, introduction of the out-of-the-box encryption has made it more difficult to verify the erasure quality.

The rest of the paper is structured as follows. Section 2 presents literature review on previous works done on evaluation of Factory Reset reliability and identified issues on solid-state drives sanitization. Section 3 explains potential threat actors, tools and techniques that can be deployed to perform the data recovery attacks on device internal storage. The conceived threat modelling served as base for the

undertaken testing, which has been defined in the Section 4. This section also describes the selection of the devices in the sample, test procedure and tools. Section 5 outlines the results of internal and external data erasure verification considering Android OS versions, phone models and manufacturers. Finally, Section 5 draws the conclusion of the research and gives the direction for future work.

2. RELATED WORKS

Being the most popular operating system for smartphones and tablets, Android's security in general and Factory Reset reliability in particular have been in the focus of researchers' attention for many years. Though, Factory Reset promises to permanently erase user data from the device storage, some researchers have proved it fails in its promise. The study performed by AVAST [7] showed that user data from 20 supposedly sanitized second-hand phones were still recoverable. Although the diversity of mobile forensic tools is wide, researchers at AVAST used only software analysis aimed at logical data extraction. For deeper investigation, test devices have been rooted and physical image, i.e. bit to bit copy of the memory image, was extracted.

Another forensic analysis of smartphone Factory Reset function was performed by ADISA [8]. A sample of 24 phones representing different manufacturers and OSes was analysed using commercial mobile forensic tool. Results showed that user data were improperly sanitized on 25% of tested devices. Noteworthy, failing devices were the ones running on the Android OS.

However, one of the most comprehensive and recognized works on Factory Reset reliability has been performed by Simon L. & Anderson R. [9], who confirmed that Android in-built sanitization is not erasing the data beyond the recovery up to Jelly Bean (v.4.1 – 4.3). In that study 21 Android devices of various versions from 5 vendors have been tested. Having preliminary rooted the devices, researchers successfully managed to recovered data from all the smartphones in the sample. Range of retrieved user data previously stored on the phones was also broad varying from multimedia files and documents to applications' login credentials. It has also been proposed by the authors that future research should investigate the level of security provided by Factory Reset function to analyse how the situation changes over time [9].

Our analysis of existing literature shows that the amount of research specifically focused on Android Factory Reset reliability is very limited, fragmented and inconsistent being characterised as the following:

- 1- no consistent approach on test sample selection: devices have been selected randomly or based on availability
- 2- very small sample of devices [10], [11]
- 3- old Android OS version and device model
- 4- data recovery after Factory Reset has been done using very few tools, all from the same type (commercial mobile forensic)

Moreover, secure sanitization is also related to the type of memory underpinning the device. Modern electronics devices are massively deploying flash-based memory storage that has already been known to be challenging to securely erase [12]. *Wei et. al* [13] empirically proved that hard-drive sanitization techniques are not effective on flash-based SSDs. *Skorobogatov S.* [12] in his research on flash memory devices outlined the problem of data remanence, which leads to residual data to still be recovered from the sanitized flash drives.

Therefore, to bridge the research gap our study aimed to 1) perform testing on larger number of devices, which would represent the recycling market situation and have wide coverage in terms of OS, model and vendor, 2) apply consistent methodology on device selection and test procedure as well as 3) deploy wider variety of data recovery techniques with escalating degree of sophistication, including invasive methods that implement low-level hardware to evaluate the degree of Factory Reset security. All these will help us to get a better understanding on Android Factory Reset efficiency and its reliability, observe if there have been any improvements over time.

3. THREAT MODELLING AND ATTACK VECTORS

The memory storage densities of the modern smartphone devices have a great potential for significant volumes of data to be recoverable thanks to different forensic techniques, especially if the device has not been erased properly. Moreover, the variety of equipment and methods used for smartphones' forensics is large which increases the likelihood of the data to be recovered even if the device has severe physical damage. In any case, the effectiveness of an attack is defined by the capability of the threat actor and the sophistication of attack methods. Therefore, in our research, the tools and techniques used for testing have been aligned in accordance with escalating sophistication of potential threat actors. Thus, we start from the easier and widely accessible data recovery methods moving to more demanding ones. Table 2 explains the different approaches of data recovery that have been implemented during our testing. Demonstrated techniques are covering all known

approaches expect for the most advanced currently known method i.e. micro-read (disassembling the eMMC chip package and reading directly from the NAND bypassing the controller). Included are the associated tools of accessing the data stored on a device, varying from the normal user interface (UI) (i.e. via the phone's Operating System) through to the most advance tactics. Table 2 highlights the degree of destruction required to perform the attack and gives a brief description of the attack vector.

Table 2: Data recovery tactics performed during testing

The level of sophistication	Tools	Method	Characteristics	Image extracted
Low	Manual inspection	Non-invasive	Manual navigation on the UI	None
Low - Medium	Forensic imaging (COTS tools)	Non-invasive	Connecting the phone to the PC or dedicated forensic HW via USB or special proprietary jigs.	Logical / physical
Medium - High	JTAG/eMMC ISP	Non-invasive but can be destructive (depends on the device)	Connection to the test access ports on device motherboard	Physical
	Chip-off	Invasive and destructive	De-soldering the memory chip from the PCB	Physical
High	Bespoke tools	Invasive and destructive	Using proprietary or custom-made tools to retrieve the data from the NAND flash directly by-passing the controller	Real physical

The easiest and least advanced way of how to check if the device stores any data is to navigate through the smartphone UI and manually check the folders that typically store user generated content (gallery, downloads, messages, phonebook etc.). However, the UI represents will not show the deleted or hidden files. A logical image can be extracted without rooting, relying on the available data obtained from the Android Application Programming Interface (API), which is in general terms, the Android version. Amount of data recoverable from logical image is always limited and does not provide comprehensive view on all the files stored on the flash memory. For example, you may not be able to recover location related data associated with a picture or message, or

metadata associated with contacts or phone numbers. With only logical image, the probability of recovering deleted files is low.

Commercial data extraction tools proliferate the market and there is an active hacking community that provides a knowledge base for those who wish to develop skills and gain experience. These tools are aiming to extract physical image which stores media files, databases, locations, social media interactions, call logs, messages, web browsing history, etc. For that matter, even if the process for obtaining a physical image is much more demanding than the one for a logical image, it is always the best choice to ensure qualitative results. The tools for both the extraction and analysis of binary image are available in the market. These tools operate on an OS level, some work through the Android exploits, others require device to be rooted to be able to extract the image. In our testing we have used several extraction and analytical tools. The need for multiple tools is explained by the fact that commercial mobile forensic tools can run only on the devices/models/vendors/OS versions that are supported. Also the capabilities of commercial-off-the-shelf (COTS) tools vary greatly and therefore the results they provide may be different (some tools are better at recovering the web-related activities and documents, others at multimedia content, the range of file formats also varies).

Advanced data recovery is commonly considered as a last resort in case previously discussed methods are not sufficient. These are highly technical hardware-based techniques that bypass OS level and are able to communicate with the eMMC chip either through the phone's micro-processor (e.g. in case of JTAG) or communicate directly (via eMMC ISP). These methods are only used for data extraction and require additional software tool for analysis. Utilizing these tools can potentially provide better results and recovery more data. One of the key advantages include ability to read the eMMC chip content even in the case of phone's severe physical damage but relatively minor deformation of the PCB. In addition, these tools are easier accessible or can be built cheaply if there is sufficient knowledge and experience. On the contrary, the extraction of data takes considerably longer time and requires the devices to be supported and PCB pinouts to be available.

Among all the advanced data recovery techniques, chip-off is considered to be even more challenging to perform due to technical complexity of the attack and knowledge and experience required to rework the memory chip. Reworking of the IC component requires de-soldering the memory chip from the PCB, cleaning, re-balling and reading the content through the chip reader. This method is very similar to In-system programming but is used when the chip pinout is not available, or PCB has been severely damaged.

There is a high-risk of permanently damaging the memory chip due to multiple thermal cycles applied during rework process as well as difficulty to remove the underfilling.

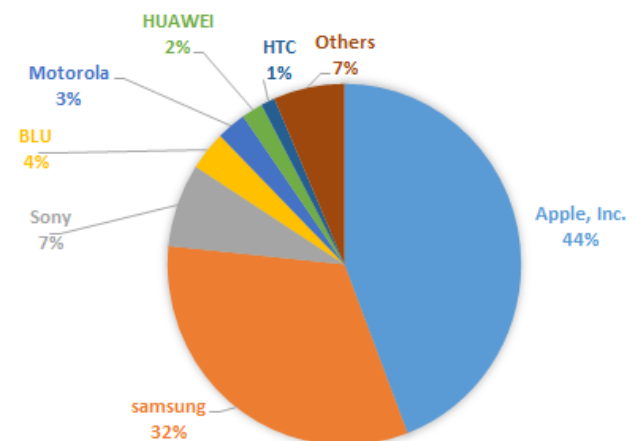
Finally, the attacks of high level of sophistication include building custom-made hardware, use of proprietary tools and techniques or any other non-trivial approaches aiming to recover the data from the memory chip. Typically, such tools are available to highly sophisticated and experienced threat actors with sufficient budget, such as e.g. state security agencies or state sponsored threat actors.

4. METHODOLOGY

4.1. Device sampling

Due to high fragmentation of Android platform in terms of smartphone models, differences in memory hardware and its version even between the devices in the same production batch, phone manufacturers and OS versions, testing all the existing devices is not feasible. Therefore, we have analysed European market of Android smartphones that undergo recycling using Blancco internal data which have been cross-checked with publicly available data on most popular devices in use [14]. Based on that, we have profiled the most popular smartphone manufacturers (Figure 2) and models that have been sold the most during the past years. From every vendor we have picked up the most commercially successful phone models to be tested ensuring diversity and variety of test devices. This sample is representative to the whole number of devices circulating in Europe which give us a base to draw the conclusions about the general state of the Factory Reset performance.

Figure 2: Top smartphone vendors



The market share of major smartphone manufacturers has been presented on the Figure 2. The leading vendors are Apple and Samsung together taking 76% of the whole market. The next major ones are Sony,

BLU (mainly present in the UK), Motorola, Huawei and HTC. Other players account for less than 1% of the market and are grouped into "Others" category. The dominance of Samsung devices is also clearly seen from the statistics on top recycled smartphones for the past 2 years.

Top 10 Android devices that have undergone recycling in Europe (2015-2017):

- 5- Samsung Galaxy S6 Edge
- 6- Samsung Galaxy S5
- 7- Samsung Galaxy S6
- 8- Samsung Galaxy S7 Edge
- 9- Sony Xperia Z3
- 10- Sony Xperia Z3 compact
- 11- Motorola Moto G (4 generation)
- 12- Samsung Galaxy S6 Edge +
- 13- Samsung Galaxy S7
- 14- Samsung Galaxy Tab 4 7.0

Presented analysis served as a base for the selection of the devices for the test sample, that consisted of the 68 Android phones purchased from the phone refurbishers. In our testing we are mainly focusing on such vendors as Samsung, Sony, Motorola, Huawei, HTC and LG. In addition, some other popular brands that have smaller market share, but are still present on the European market, have been tested based on the availability of the devices on suppliers' side (e.g. ZTE, CAT, Asus etc.). The full list of test devices is given in the Appendix 1.

4.2. Test procedure

Testing of reliability of Factory Reset performance involves the following steps presented in the Table 3. The main goal is to simulate the real-life experience of the device usage through generating different data types that are typically found on modern smartphones and then erasing through Factory Reset. After that device undergoes data recovery process that consists of the memory dump extraction and analysis which can be performed by using a single tool (e.g. COTS) or several tools together (advanced methods).

Table 3: Test protocol

Stages	Description
Device preparation	Ensuring that the device does not store any data prior the testing. This way it is easier for us to identify the origin of the data that can be potentially recovered after the Factory Reset.
Populating device with data	Simulating the real device usage and generating user data: installing the applications, writing multimedia files, saving documents, syncing the phonebook and other accounts, connecting to the Wi-Fi networks, generating web history, making calls and sending text/mms messages through different platforms etc.
Erasure	Performing Factory Reset

Data recovery	<i>Data extraction:</i> reading the content of the memory storage in the form of memory dump <i>Data analysis:</i> analysing the dump to identify any meaningful data
---------------	--

The main objective of the data extraction stage is to perform physical read of the content stored in the memory chip using JTAG interface or ISP. Accessing the eMMC with those methods grants the possibility to save a duplicate of the memory content and save it locally in a computer or external drive. The result is called a binary image, which is created as a bit-by-bit copy of the entire file system present on the memory chip [15], containing all current and deleted data from the partitions and unallocated space.

Once the binary image is obtained, the last step is to analyse it in order to check what kind of files can be carved and recovered, this includes media files such as audio, images and video, user accounts and potentially their passwords, locations, metadata from applications, etc. The analysis is done via dedicated software typically being the part of the commercial mobile forensic package.

4.3. Equipment and tools

4.3.1. COTS tools

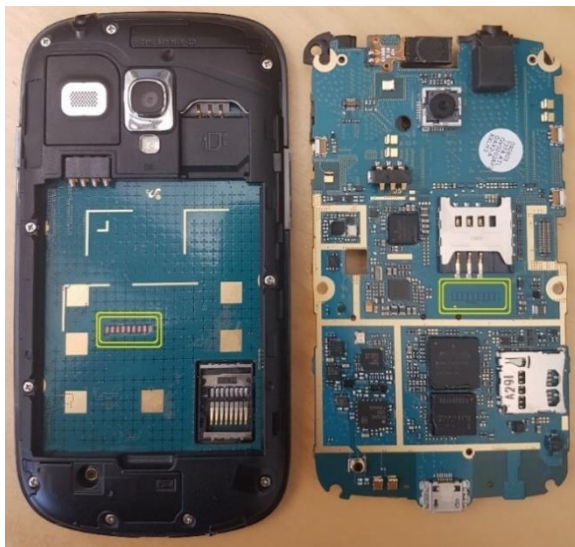
We have used several of the most renown commercial mobile forensic tools such as Magnet Axiom (demo), Oxygen Forensic Detective (full version) and Cellebrite: UFED Touch and Physical Analyser (demo). All these tools have different capabilities and strengths as well as the range of supported devices. Magnet Axiom requires the device to be rooted to run the physical image extraction. Oxygen Forensic Detective typically also requires rooting, however, there is a couple of special modes (for MTK and some Samsung and LG models) that do not need super user privilege. Cellebrite is the admitted leader in the mobile forensic market and supports a wide range of phones and vendors. It does not require the device to be rooted and operates through the Android OS exploits that give the tool a temporary root access for the period of extraction. One of the other distinguishable differences between the tools is the range of artefacts they are capable to recover. Magnet Axiom has a strong emphasis on web-activity and documents, Cellebrite can carve the images from the unallocated space and differentiate the system files from the user data. Due to all these peculiarities, it has been beneficial to have several tools that altogether can provide a greater device and feature coverage and allow cross-checking and verification of the results.

4.3.2. ISP and JTAG tools

These tools are *advanced data extraction methods* which involve connecting to the specific ports on the device and instructing the processor or eMMC controller to transfer the data stored on the memory [16]. Depending on the design of the device (glue or screw-based housing) these can be considered as invasive or non-invasive. These acquisition techniques are effective to verify the results of the COTS tools and to perform the tests on the devices that are not supported by any commercial mobile forensic tools. Advanced data extraction methods are low-level hardware-based techniques that leverage the advantage of PCB and IC (Internal Circuit) test interfaces used for programming and quality control of the electronic devices during production.

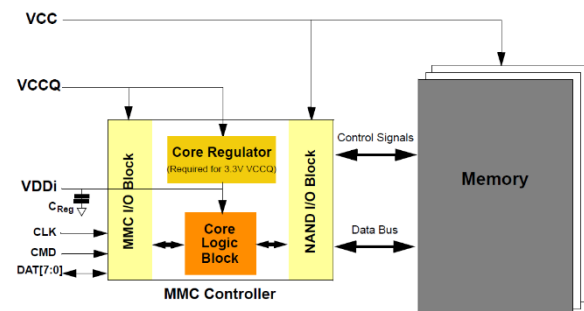
JTAG forensics is an acquisition procedure which involves connecting to the Standard Test Access Port on a device and instructing the processor to transfer the raw data stored on connected memory chips. Jtagging supported phones can be an extremely effective technique to extract a full physical image from devices that cannot be acquired by other means. Although device manufacturers document the JTAG schematics, this information is not available for the general public [16]. JTAG pins can be exposed on the phone's PCB, but they can also be hidden under a coating surface, in this case tools are needed to remove the coating and leave the pins exposed for connection and testing. Figure 3 shows the JTAG pins that have been hidden underneath the battery and covered by the product info label and protected by the coating. However, manufacturers also tend to limit the access of external parties to the JTAG ports and either by making them inaccessible after the end of production testing or breaking them on purpose.

Figure 3: JTAG pins (left exposed, right coated)



In System Programming (ISP) is a technique where current microcontrollers and memory chips can be programmed after been placed onto the PCB and then re-programmed without removing them from the board. This process reduces the risk of damaging the chip since it is not exposed to high temperatures unlike in case of chip-off process. In contrast to JTAG that is used for the boundary scan of all the components sitting on the PCB, ISP is designed to test only one particular component (in our case eMMC) bypassing the processor. Communication with eMMC device is performed by sending commands to the chip and receiving responses back. To be able to retrieve data, the chip firmware must be able to boot up and afterwards the content of the memory can be read [17]. Due to direct communication with the chip the memory acquisition through ISP is much faster to perform than through the JTAG. The biggest limitation for both these techniques is limited availability of the ISP/JTAG pinouts. This information is considered to be manufacturer proprietary and not intended to be used by the third parties. However, there is a community of enthusiast and hackers as well as commercial labs specialized in offering the service of finding the ISP/JTAG pinouts. Figure 4 explains the internal structure of the eMMC chip and the signals used to perform JTAG/ISP communication.

Figure 4: eMMC structure and interface [18]



The instructions/commands (in our case “read”) are sent through the CMD (command) signal to the MMC controller of the memory. The response (data output) is sent via data busses DAT0 to DAT7 synchronized with the clock signal (CLK).

Programmer tool: there are many programmer tools commercially available [19], all of them offer support for different chipsets and cores (required to communicate with the eMMC via JTAG). For our research, programmer tool is necessary to communicate with memory chip and perform read and write operations. We have selected one of the most commonly flasher boxes used by phone repair shops, the RIFF Box2.

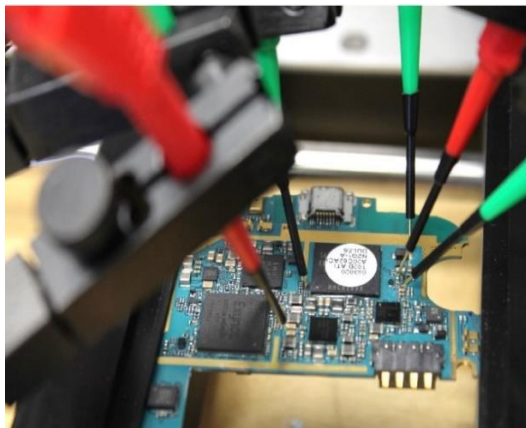
Figure 5: RIFF Box2 (Programmer Tool)



This programmer offers support for accessing the eMMC chip through both JTAG and ISP connection. It also has the capability of detecting the pinout of the actual JTAG port once it has been physically found. Some of the basic characteristics of this programmer tool are the reading speed that can reach up to 10 MB/s (via ISP), support for all eMMC revisions since v4.0, adjustable output voltage required for VCC and VCC_Q, 4-bit (DAT0 – DAT3) bus width and standard connectors for external accessories and adapters.

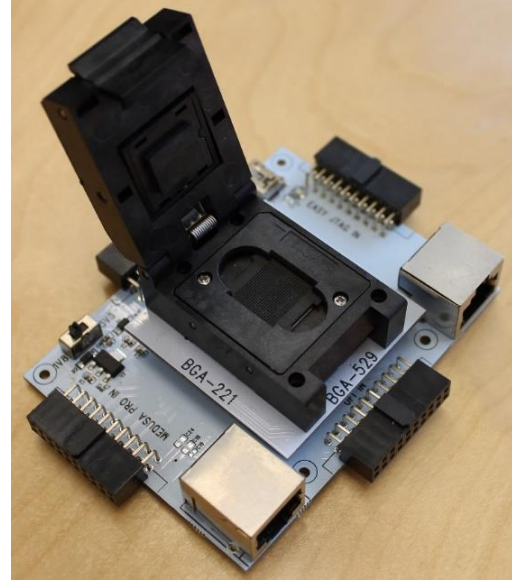
VR-Table: in order to be able to perform the memory read via JTAG/ISP interface, the solid connection to the Test Access Ports should be established. Traditionally, soldering has been applied to connect the wires to the pins. However, the pins are typically very tiny dots on the PCB and making a solid connection requires jewellery accuracy and experience in micro-soldering. Any mistake or improperly soldered wires would mean inability to establish the communication with the pins and result in re-soldering. To avoid all these complexities, we have used a VR-Table (Figure 6) that represents robotic arms holding the probes of 0.5mm and embedded power supply providing different voltages. The other end of the probe is connected to the corresponding input of the flasher box. The probes of the VR-Table are movable and adjustable which allows us to reconnect the pins without any problem. To enhance the precision of the connection a microscope camera (part of the additionally purchased accessory) that is placed on one of the arms has been used to facilitate the process.

Figure 6: VR-Table setup



Chip-off tools: as has been stated above, the chip-off technique was not in the main focus of our internal testing as it is basically the same as reading through the ISP but more invasive. For these tests, we used a universal socket from E-Mate Pro eMMC Moore Figure 7 supporting the eMMC chips of BGA 153 – 169, BGA 162-186, BGA 221 and BGA 529 of the size 11.5x13, 12x16, 14x18 and 15x15 mm.

Figure 7: eMMC chip adapter



The adapter corresponding to the eMMC size is attached to the socket with 2 screws and the chip is held into its position by a locator. This solution allows easy and safe interchange of the socket and perfect alignment of the chip on the pin matrix of the socket. After that the socket is connected to the reader via the adapter and then connected to the PC. During the read process, the raw data is acquired from the chip resulting in a binary file that is saved on a PC for further examination via Physical Analyser tools.

All the data recovery approaches explained above have been performed internally, however, the most advanced testing aiming at reading the data from the raw NAND by-passing the eMMC controller was outsourced to the independent third party due to high complexity of the testing and time required to complete the attack on chip. Also, since this type of extremely complex testing is time consuming and very costly, it was possible to test only one device. For this purpose, we selected one of the best-selling smartphones of all times [1], i.e. Samsung Galaxy S4.




5. RESULTS

We have performed multiple Factory Reset tests following the procedure described in the Table 3. Memory dumps extracted after these tests have been stored locally (in form of a binary image) and analysed



with the help of the COTS forensics tools. The amount of recovered data varies depending on many factors such as the memory type, phone model, Android OS version, manufacturer, etc. Figure 8 represents an example of summary of the obtained physical image analysis, where the numbers before the brackets indicate the total amount of files within the category, while numbers in brackets show the amount of recovered deleted files. It has been possible to recover lots of personally identifiable information, including the passwords from email accounts, Google services and applications, using multiple commercial tools. The amplitude of risk in particular for Google credentials to be obtained by unauthorized party may result in huge security breach, since many applications can be linked to the same credentials.

Figure 8: Summary of the analysis

Phone Data

 Call Log	17 (17)	 Chats	8 (8)
 Emails	121 (121)	 Installed Applications	177
 Passwords	16	 Powering Events	2
 User Accounts	2	 Wireless Networks	17

Data Files

 Applications	973 (64)	 Audio	125
 Databases	92 (36)	 Images	160 (11)
 Uncategorized	3397 (2531)		

It has been also possible to recover multimedia files, documents, emails, messages (phone native and application specific) (see Appendix 2), contacts (phonebook, email, WhatsApp etc.), call logs (including the ones done through the applications such as Skype / WhatsApp), browsers' history and more data depending on the forensic tool in use. Appendix 2 provides the example of how the documents appear after being recovered. Besides the content of the file itself, the last modification date and author were identified.

In some cases, only the content of the files has been recovered. In others, we were also able to extract the metadata of the file, which contained e.g. timestamp (messages, email, documents, etc.), file extension, status of the message (sent/received). In some instances, we were able to see the path to the recovered file, which provided us with better understanding on the origin of the file (downloads folder, camera, etc.). In case of Wi-Fi data recovery, it is further possible to track the SSID number and identify the location of the

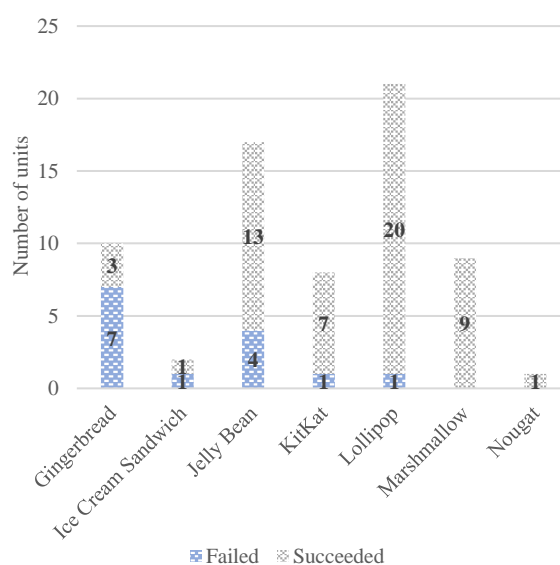
Wi-Fi hotspot. It is a similar situation in case of photo's metadata recovery: if the geo location has been enabled on the phone and the picture has been recovered, there is a high chance that the geo data may be recoverable too.

In addition, in case of superficial Factory Reset there is a potential to also recover cache images. These are typically browser cache images in a form of thumbnails used for faster browser/application operation (to avoid the re-download of the content of already visited pages). Same applies to browser history that is possible to recover if the device does not perform the Factory Reset properly. With a rise of connected devices and Internet-of-Things (IoT), we observed potentially recoverable data, for instance, related to the connection to Amazon Alexa. This information includes the timestamps of connection and Gmail address.

User data were possible to recover on 14 phones, clearly identified as the test data used for populating the phone prior to the Factory Reset process. These findings represent 20% of the devices failing to perform a proper erasure within our sample.

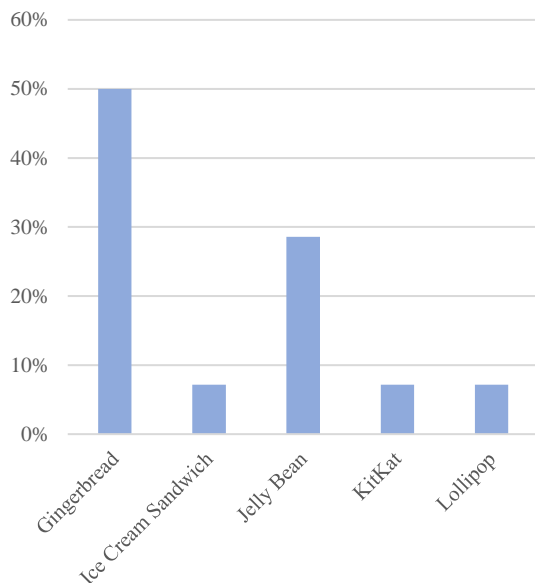
Further, it has been observed that Android OS version is an important factor in determining the quality of the Factory Reset process. Noteworthy, half of the test devices that failed to properly sanitize the device storage after Factory Reset are running on Gingerbread (2.3 – 2.3.7), followed by Jelly Bean (4.1 – 4.3.1) accounting for slightly less than 30% of devices (Figure 9). The rest of devices improperly sanitizing user data are running on Android Ice Cream Sandwich (4.0 – 4.0.4), KitKat (4.4 – 4.4.4) and Lollipop (5.0 – 5.1.1) representing 7% each.

Figure 9. Overall summary on devices' Factory Reset performance



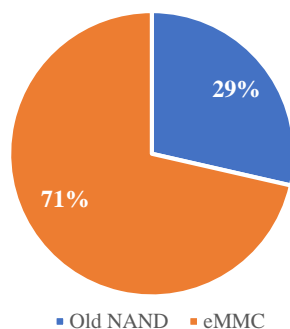
More detailed breakdown of the Android OS versions for devices that failed to properly erase data after Factory Reset is presented on the Figure 10.

Figure 10: Factory Reset failure rate by OS



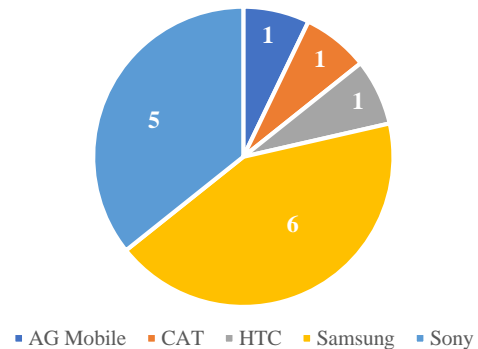
Related to the memory type, 10 out of 14 devices failing to erase data after Factory Reset use eMMC (Figure 11). This represents vast majority of the memory technologies. Unsurprisingly, older devices are not only running on outdated Android OS, but also feature older storage technology. This older memory storage is also NAND flash based (typically One NAND) with no separate controller. The absence of a controller simplifies verification of erasure quality since communication is done directly with the NAND flash.

Figure 11: Memory technology of failing devices



Regarding the phone manufacturers, most of the devices failing to properly erase user data are from Samsung with 6 devices. The second one is Sony accounting for 5 phones. AG Mobile, CAT and HTC have 1 device each failing at Factory Reset (Figure 12).

Figure 12. Devices (in units) failing Factory Reset by manufacturer



In terms of the actual data recovered from devices that failed the Factory Reset process, Appendix 3 illustrates the number and specific type of artefacts recovered deploying various data recovery approaches and tools. These data include multimedia files, conversations, emails, contacts, call logs, browser history, etc.

As stated before, independent data recovery company has been involved to verify the quality of data erasure after Factory Reset. The goal of this testing was to develop the procedure and build the tools allowing data extraction directly from the eMMC's raw NAND by-passing the controller. This is due to the nature of solid-state drives: the controller is doing all the data management operations internally, typically hiding deleted files and performing actual erasure later. Another source of deleted data is bad blocks, which are retired areas of the flash memory still readable but not any more programmable.

Due to proprietary nature of the performed work, technical complexity, high costs and long time required to achieve the verification on the very low level, it has been possible to test only one device, the Samsung Galaxy S4, which has successfully passed less sophisticated attacks. In other words, no data were found after Factory Reset via COTS or hardware-based tools. However, the results (Figure 13) indicate that user data were still recoverable after Factory Reset. Though, the range of recovered data was not large and limited to only SMS. Noteworthy, unlike with any other device tested, it was also possible to recover not only known data set used for testing, but also the data from the previous owner.

Figure 13: Results of external testing

Number	Deleted	Read	Type	Folder	Timestamp (UTC+0)	From	To
1	yes	no	SMS	Inbox	09.04.2018 6:36:07	+35840021	Message 2: received
2	yes	yes	SMS	Sent	09.04.2018 6:34:59		Monday message 2 to
3	yes	yes	SMS	Outbox	09.04.2018 6:34:57		Monday message 2 to
4	yes	yes	SMS	Sent	09.04.2018 6:31:22		Monday message to
5	yes	yes	SMS	Sent	09.04.2018 6:31:21		Monday message to
6	yes	yes	SMS	Sent	06.04.2018 7:15:38	+35841	To have the .db files with some info
7	yes	yes	SMS	Sent	06.04.2018 7:15:37	+35841	To have the .db files with some info
8	yes	yes	SMS	Sent	06.04.2018 7:15:12	+35841	Simply logs
9	yes	yes	SMS	Sent	06.04.2018 7:15:10	+35841	Simply logs
10	yes	yes	SMS	Drafts	06.04.2018 7:05:35		Drive Samsung Galaxy S4
11	yes	yes	SMS	Drafts	06.04.2018 7:05:08		Drive Galaxy S4
12	yes	yes	SMS	Drafts	06.04.2018 7:04:22		Drive S4
13	yes	yes	SMS	Drafts	06.04.2018 7:03:41		Drive

The analysis of Factory Reset effectiveness against different types of attacks is given in the Table 4. Non-sophisticated attacks such as browsing through the user interface of the phone will not give an access to any previously stored data. At this level devices look wiped with no visible traces of data. However, deployment of commercial data forensic tools allowed accessing user data on 12 out of 62 devices after Factory Reset. Furthermore, applying more invasive methods such as eMMC ISP made it possible to recover the data that were not visible otherwise. Finally, performing the attack of the highest known level of sophistication lead to retrieval of the data previously inaccessible with any other tools. These data were not limited to only test data, but also included the information of the previous owner of the device. This means that the highly sophisticated threat actors with advanced tools and sufficient amount of knowledge and experience are capable of recovering the data where other approaches do not provide any results.

Table 4: Factory Reset robustness against different attacks

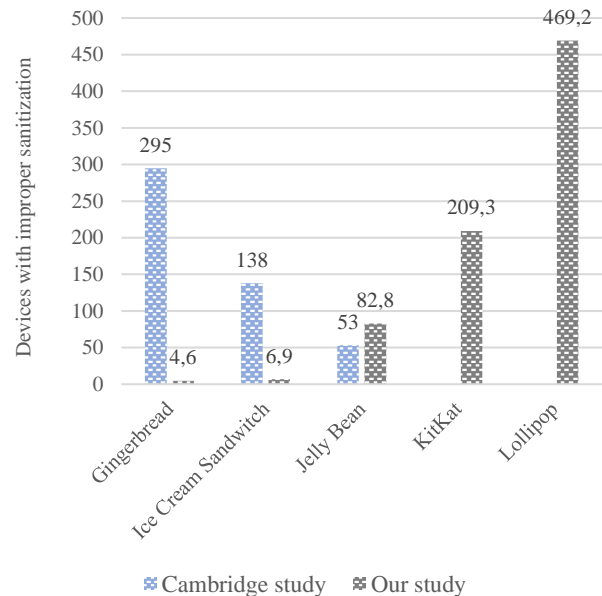
The level of sophistication	Techniques / Tools	Sample	Units failed
Low	Manual inspection	68	0
Low-Medium	Forensic imaging (COTS tools)	62	12
Medium-high	JTAG / eMMC ISP / Chip-off	12	1
High	Bespoke tools	1	1

Considering the distribution of the Android smartphones across versions (Table 5), it is clear that vast majority of the devices are not running on the latest OS version. One third of Android phones still has Lollipop or older OS. Many of these smartphones will not receive the upgrade or security fixes, since manufacturers discontinued the support of old devices. However, our results show that phones with these Android versions may not sanitize the storage beyond the recovery when performing Factory Reset.

Table 5: Android OS versions distribution [20]

Version	Codename	Distribution
2.3.3 – 2.3.7	Gingerbread	0.2%
4.0.3 – 4.0.4	Ice Cream Sandwich	0.3%
4.1 - 4.3	Jelly Bean	3.6%
4.4	KitKat	9.1%
5.0-5.1	Lollipop	20.4%
6.0	Marshmallow	23.5%
7.0 – 7.1	Nougat	30.8%
8.0 – 8.1	Oreo	12.1%

Back in 2015 when researchers at University of Cambridge analysed reliability of Factory Reset performance, estimated number of devices vulnerable to improperly sanitize the storage accounted for up to 500 million devices [9]. However, smartphone market has significantly evolved and grown over the past years and reached 2.3 billion devices by 2018 [21]. Considering Android distribution and results of our study, we can conclude that the number of devices that may not properly erase the user data after Factory Reset account for over 770 million units globally. This is over 50% growth for a three years period. Figure 14: Devices in the market failing to securely sanitize data



6. CONCLUSIONS

The results of our testing show that Factory Reset is still failing to permanently erase user data on the smartphones running on Android Gingerbread to Lollipop versions. Though, no data were visible on the phone user interface after performing in-built sanitization function, it has been possible to recover supposedly erased data using a range of tools varying from commercially available to custom-built ones. It has not been possible to identify any correlation between the Factory Reset performance and the phone models, manufacturers or OS version due to high degree of Android OS fragmentation. Even the same smartphone model typically has multiple model variants depending on the region where the device has been sold. Moreover, within the same variant there might be various hardware revisions, which will use different storage components. Furthermore, even in case of identically the same devices and hardware, the version of memory chips may also vary. The differences in memory chip versions will determine different set of supported commands, including the ones related to data sanitization. Another problem with Android OS is huge number of supported devices, which makes it close to impossible to maintain the updates for all versions and smartphones of different hardware. This means that as soon as a newer version is released support for older devices will be discontinued. And even in case of smartphone still being supported it takes significantly more time to push it across the devices, since there are different levels of parties involved in new OS version customization and modification starting from manufacturers to phone carriers. In comparison, 81% of iOS devices are running the latest OS version [22] since updates are done directly. Same applies to encryption, which significantly strengthens device security and makes it harder to extract the data from the device. 95% of iOS devices are encrypted vs less than 10% of Android [23].

A bright example is Android Gingerbread that was running on half of the devices that failed to perform data erasure after Factory Reset and allowed us successfully recover user data. That OS version was released back in 2010. On the hardware side, the first versions of the eMMC chips did not have as much features as the current ones, hence, the data can be accessed without much restrictions compared to new eMMC versions. Another interesting observation is that many devices where data have been recovered after Factory Reset erasure were using old NAND technology (e.g. OneNAND). The ease of data recovery from this type of storage is explained by the absence of the on-chip controller, therefore, it has been possible to get direct access to raw NAND flash. Deployment of newer storage technology such as

eMMC made it harder to retrieve the data since the controller and the raw NAND are placed on the same IC. Commercially available tools did not provide any evidence of data remanence. However, utilization of bespoke custom-built hardware made it possible to bypass the controller and read the content of the memory and recover both test data and previous user data. This represents a serious data security risk and danger for data privacy.

7. ACKNOWLEDGMENT

For more information on the sustainablySMART project, its partners and publications please refer to <https://portal.effra.eu/project/1544>

The project sustainablySMART has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no.680640.



8. REFERENCES

- [1] The Telegraph, "20 bestselling mobile phones of all time," 2017. [Online]. Available: <https://www.telegraph.co.uk/technology/2016/01/26/the-20-best-selling-mobile-phones-of-all-time/>.
- [2] Statista, "Smartphones industry: Statistics & Facts," 2018. [Online]. Available: <https://www.statista.com/topics/840/smartphones/>.
- [3] Statista, "Global smartphone shipments forecast from 2010 to 2022 (in million units)," 2018. [Online]. Available: <https://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/>.
- [4] European Parliament, "A Longer Lifetime for Products: Benefits for Consumers and Companies," April 2016. [Online]. Available: [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/579000/IPOL_STU\(2016\)579000_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/579000/IPOL_STU(2016)579000_EN.pdf).
- [5] Kantar Worldpanel ComTech, "An incredible decade for the smartphone: what's next? The Future of Mobile is in Combining, Devices, Content, and Services," February 2017. [Online]. Available: <https://www.kantarworldpanel.com/global/News/2017-smartphone-industry-insight-report>.
- [6] IDC, "Smartphone OS," 2017. [Online]. Available: <https://www.idc.com/promo/smartphone-market-share/os>.
- [7] Avast, "Tens of thousands of Americans sell themselves online every day," 2014. [Online].

Available: <https://blog.avast.com/2014/07/08/tens-of-thousands-of-americans-sell-themselves-online-every-day/>.

[8] ADISA, "Forensic Analysis of Smartphone Factory Reset Function," 20 05 2015. [Online]. Available:

<https://www.informationsecuritybuzz.com/articles/forensic-analysis-of-smartphone-factory-reset-function/>.

[9] L. Simon and R. Anderson, "Security Analysis of Android Factory Resets," 2015. [Online]. Available: https://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf.

[10] R. Schwamm, "Effects of the factory reset on mobile devices," *Journal of digital forensics, security and law*, vol. 9, no. 2, pp. 20-220, 2014.

[11] J. Kong, "Data Extraction on MTK-based Android Mobile Phone Forensics," *Journal of Digital Forensics, Security and Law*, vol. 10, no. 4, pp. 31-41, 2015.

[12] S. Skorobogatov, "Data Remanence in Flash Memory Devices," in *CHES'05 Proceedings of the 7th international conference on Cryptographic hardware and embedded systems*, Edinburgh, UK, 2005.

[13] M. Wei, L. Grupp, F. Spada and S. Swanson, "Reliably Erasing Data From Flash-Based Solid State Drives," in *Proceedings of the 9th USENIX Conference on File and Storage Technologies (FAST'11)*, 2011.

[14] DeviceAtlas, "The Mobile Web Intelligence Report Q4 2016," 2016. [Online]. Available: <http://discover.deviceatlas.com/mobile-web-intelligence-report-q4-2016/>.

[15] INFOSEC Institute, "Getting Started with Android Forensics," 20 August 2014. [Online]. Available:

<http://resources.infosecinstitute.com/getting-started-android-forensics/#gref>. [Accessed 15 August 2017].

[16] H. Mahalik, S. Bommisetty and R. Tamma, *Practical Mobile Forensics*, Second ed., Birmingham-Mumbai: Packt Publishing, 2016.

[17] I. Sestanj, "NAND Flash Data Recovery Cookbook," 2016. [Online]. Available:

www.adreca.net/NAND-Flash-Data-Recovery-Cookbook.pdf.

[18] JEDEC standard, "Embedded MultiMediaCard (eMMC) eMMC/Card Product Standard, High Capacity, including Reliable Write, Boot, and Sleep Modes (MMCA, 4.3)," 2007. [Online]. Available: <https://www.jedec.org/system/files/docs/JESD84-A43.pdf>.

[19] J. Swauger, "Chip-off Forensics: Extracting a full bit-stream image from devices containing embedded flash memory," *Digital Forensics Magazine*, pp. 52-56, 2012.

[20] Android Authority, "Android version distribution: Pie is missing from August's distribution numbers," 1 09 2018. [Online]. Available:

<https://www.androidauthority.com/android-version-distribution-748439/>.

[21] Newzoo, "Insights into the 2.3 Billion Android Smartphones in Use Around the World," 17 01 2018. [Online].

Available: <https://newzoo.com/insights/articles/insights-into-the-2-3-billion-android-smartphones-in-use-around-the-world/>.

[22] Digital Trends, "iOS 11 is now running on 81 percent of iPhones and iPads," 2018. [Online]. Available:

<https://www.digitaltrends.com/mobile/ios-distribution-news/>.

[23] Express, "Almost ALL iPhones are encrypted, almost ALL Android smartphones are NOT," 2016. [Online]. Available: <https://www.express.co.uk/life-style/science-technology/653099/iphone-ios-Encryption-Android-OS-Google-Smartphone>.

APPENDIX 1: FULL LIST OF TESTED DEVICES

Model	OS version	Model	OS version
1. AG Mobile Chrome Selfie	4.4.2	35. Samsung Galaxy S III I9300	4.3
2. AG Mobile Ghost	5.0.2	36. Samsung Galaxy S III I9300	4.1.2
3. Asus Memo Pad HD7 (ME173X) 16GB	4.2.2	37. Samsung Galaxy S III Mini i8190	4.1.2
4. Asus Zenpad	5.0.2	38. Samsung Galaxy S III Mini i8200N	4.2.2
5. CAT B15	4.1.2	39. Samsung Galaxy S Plus	2.3.6
6. FairPhone 2	6.0.1	40. Samsung Galaxy S2 I9100	4.1.2
7. HTC Desire 310	4.2.2	41. Samsung Galaxy S4 I9505	5.0.1
8. HTC Desire 620	4.4.4	42. Samsung Galaxy S4 Mini I9195 LTE	4.2.2
9. HTC Desire C	4.0.3	43. Samsung Galaxy S5 (SM-G900F)	5.0
10. HTC Desire S	4.0.3	44. Samsung Galaxy S5 Mini G800F	5.1.1
11. HTC Desire X	4.1.1	45. Samsung Galaxy S6 (SM-G920F)	6.0.1
12. HTC One M7	5.0.2	46. Samsung Galaxy Tab 3 7.0 (SM-T211)	4.4.2
13. HTC One M8	6.0	47. Samsung Galaxy Trend 2	4.4.2
14. HTC One Mini 2	4.4.2	48. Samsung Galaxy XCover	2.3.6
15. Huawei Ascend G620S	4.4.4	49. Samsung Galaxy Y Pro (GT-B5510)	2.3.6
16. Huawei Y6	5.1.1	50. Samsung i8160 Galaxy Ace 2	4.1.2
17. Lenovo IdeaTab 2	4.4.2	51. Samsung S5830 Galaxy Ace	2.3.6
18. LG G flex2 (LG-H955)	5.1.1	52. Samsung XCover II (S7710)	4.1.2
19. LG G2 (LG-D802)	4.2.2	53. Sony Xperia Go	4.1.2
20. LG G3 D855	5.0	54. Sony Xperia J	4.1.2
21. LG G4 H815	6.0	55. Sony Xperia M2	5.1.1
22. LG V10 32GB	6.0	56. Sony Xperia M2 Aqua	5.1.1
23. Motorola Moto G (XT-1039)	4.4.4.	57. Sony Xperia SL	4.1.2
24. Motorola Moto G 3rd	6.0.1	58. Sony Xperia SP	4.3
25. Motorola Moto G4	7.0	59. Sony Xperia Tipo	4.0.4
26. Motorola Moto X 2nd	5.0	60. Sony Xperia U	2.3.7
27. Nexus 1	2.3.6	61. Sony Xperia Z1	5.1.1
28. Nexus 4 (LG-E960)	5.1.1	62. Sony Xperia Z1 Compact	5.1.1
29. OnePlus One (A0001)	6.0.1	63. Sony Xperia Z2	5.1.1
30. Samsung A5 (SM-A500FU)	6.0.1	64. Sony Xperia Z3 Compact	5.0.2
31. Samsung Galaxy Note N7000	4.1.2	65. Xiaomi Redmi 3	5.1.1
32. Samsung Galaxy Note3 (SM-N9005)	5.0	66. ZTE Blade	2.3.5
33. Samsung Galaxy Note4 (SM-N910F)	6.0.1	67. ZTE Blade V6 Lite	5.1
34. Samsung Galaxy S	2.3.6	68. ZTE Skate	2.3.5

Title	Authors	Last Modified Dat...	File Sys...	File
		6/6/2013 12:44:02 PM		
Novel Anti-forensics Approaches for Smart Phones	S. Azadegan, W. Yu, H. Liu, M. Sistani, S. Acharya	11/16/2011 8:07:09 PM		
Microsoft Word - 150. Manuscript	Siddhu			
Guidelines on Mobile Device Forensics	Ayers, Richard P.;?Brothers, Sam;?Jansen, Wayne	2/3/2016 8:32:51 AM		
UFS Unified Memory Extension v0.5	JEDEC	9/18/2013 4:01:53 PM		
Theory and practice of flash memory mobile forensics	Salvatore Fiorillo	1/31/2010 7:06:04 AM		
		9/6/2012 4:15:36 AM		
Guidelines on Mobile Device Forensics	Ayers, Richard P.;?Brothers, Sam;?Jansen, Wayne	9/16/2015 2:36:01 PM		
		5/25/2015 1:36:15 AM		
Untitled	Sean Yang	6/9/2014 1:42:18 AM		
Draft Special Publication 800-101 Revision 1, Guideli...	NIST Computer Security Division, and Software and...			
		8/15/2013 3:32:36 AM		
ISO28000 Security Management System Project	Luke Simmons	3/5/2009 11:13:05 AM		
		7/25/2012 2:40:12 PM		
Mobile device forensics: A snapshot	Christopher Tassone, Ben Martini, Kim-Kwang Raym...	8/7/2013 10:59:54 PM		
MultipleCopies.pdf	Michael Wei <m3wei@cs.ucsd.edu>	12/17/2010 6:58:45 AM		
		10/21/2015 12:44:19 PM		
Flash Memory Summit Final - Aug 11	sglenn	8/15/2009 2:35:13 PM		



Table View				Thumbnail View			
	Image	Name	Path	Size (byte)	Metadata		
<input checked="" type="checkbox"/>		image276.jpg	Images/image276.jpg	12466			
<input checked="" type="checkbox"/>		image277.jpg	Images/image277.jpg	6828			
<input checked="" type="checkbox"/>		image278.jpg	Images/image278.jpg	6061			
<input checked="" type="checkbox"/>		image279.jpg	Images/image279.jpg	7059			
<input checked="" type="checkbox"/>		image28.jpg	Images/image28.jpg	230489			
<input checked="" type="checkbox"/>		image280.jpg	Images/image280.jpg	10405			
<input checked="" type="checkbox"/>		image281.jpg	Images/image281.jpg	7946			
<input checked="" type="checkbox"/>		image282.jpg	Images/image282.jpg	6306			

? < Images

Details Events (0)

Name: image279.jpg
Type: Images
Size (bytes): 7059
Path: Images/image279.jpg
Created:
Accessed:
Modified:
Deleted:
Extraction: Physical
MD5: db6a04c7315a87809824c4ce1f5a22b7
Source file: blk0_mmcblk0.bin : 0x78EADC0Q

Map

Position:
Address:
Map Address:

SMS Message
 Go to ▾

Source:

SMSC:

Folder: Sent

Timestamp: 8/11/2017 2:36:01 PM(UTC+0)

Delivered:

Read:

Status: Sent

Extraction: Physical

Source file: [blk0 mmcblk0.bin: 0x63260171](#)

All timestamps

Parties

To: 04002 █████

Body

I can't talk now. Please send me a message.

Email
 Go to ▾

Account:

Snippet: San Antonio police officer Miguel I. Moreno, who was hit by gunfire during a ...

Folder:

Subject: POLICE OFFICER DIES: San Antonio officer dead after shootout

Timestamp: 6/30/2017 5:09:41 PM(UTC+0)

Priority:

Source: Gmail

Status:

Extraction: Physical

Source file: [NAND\(00000000-21000000\).bin: 0x1DCC21A1](#)

From

From: foxnews@newsletters.foxnews.com FoxNews.com

To

To: baraguza.smart@gmail.com

CC

BCC

Attachments

Body

 HTML Text

San Antonio police officer Miguel I. Moreno, who was hit by gunfire during a Thursday shootout in downtown San Antonio, died of his injuries on Friday, the department announces.

More on this:

APPENDIX 3: TYPES OF DATA RECOVERED WITH DIFFERENT TOOLS

Device	WEB RELATED	CALL LOGS	CONTACTS	DOCUMENTS	EMAILS	IMAGES	MMS	AUDIO	SMS	VIDEO	WHATSAPP	Skype	Wi-Fi Passwords
AG Mobile Chrome Selfie				5		53		1					
CAT B15	2	4		70		7308		2588		28			
HTC Desire S	19	10	100	50	89	465	5	374	18	29	3		4
Samsung Galaxy Ace	21	6	1		205	15	4	73	11	3	3		
Samsung Galaxy S	47	7	3	276	239	392		96	1	304	252		7
Samsung Galaxy S Plus		4	16	344	311	7707			80	100	404		
Samsung Galaxy S4									55				
Samsung Galaxy XCover	57	6	8	22	137	746		77	12		2		16
Samsung Galaxy Y Pro	14		2		141	404		63		2			
Sony Xperia Go	205	6		94	1506	22410		243	8	74	90	18	
Sony Xperia J	12			69	1	2867		270		43	3		
Sony Xperia SL	139	1		99	2	1357		137	2	83	10		16
Sony Xperia Tipo	24			152		1599		260		94			
Sony Xperia U	39	17		91	121	2856	2	125	13	70	89		16