D1.1

State of the Art in Mobile Forensics

Project number:	883156
Project acronym:	EXFILES
Project title:	Extract Forensic Information for LEAs from Encrypted SmartPhones
Start date of the project:	1st July, 2020
Duration:	36 months
Programme / Topic:	H2020-SU-SEC-2019 / SU-FCT02-2018-2019-2020 Technologies to enhance the fight against crime and terrorism

Deliverable type:	Report
Deliverable reference number:	SU-FCT02-883156 / D1.1/ V1.0
Work package contributing to the deliverable:	WP1
Due date:	September 2020 – M03
Actual submission date:	30th September 2020

Responsible organisation:	NFI
Editor:	NFI
Dissemination level:	PU
Revision:	V1.0

Abstract:	In the current smartphone market, Android and iOS are the dominant operating systems where Samsung, Huawei and Apple are the major smartphone developers, all using state-of-the-art ARM based chip technology. Traditional data acquisition methods are less effective against modern smartphones, without proper user authentication, due to strong cryptographic security mechanisms at the operating system level. Future forensic techniques need to focus on the exploitation of hardware and software vulnerabilities to escalate privileges to the level where an examiner can directly acquire decrypted user data from a running device, or extract key material that can be used to decrypt extracted user data afterwards. This results in new business models for forensic tools vendors but also raises legal issues related to network based data acquisition and responsible disclosure.
Keywords:	Mobile Forensics, Smartphone Security Features, Forensic Techniques, Smartphone encryption

The project EXFILES has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883156.

Editor

NFI

Contributors (ordered according to beneficiary numbers)

RHUL

CEA

CSIC

Cyber Intel

TEXPLAINED

ULille

IRCGN

NFI

BKA

RISCURE

SYNACKTIV

Reviewers (ordered according to beneficiary numbers)

BKA

Security Screening Board

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the authors’ views – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

In modern criminal investigations, smartphones are seized at every type of crime scene, and are often the most important items in the case. As a result, data from smartphones and attached cloud storage is widely used in criminal investigations and as evidence in court. Extensive research has been performed in the mobile forensic community to extract data from smartphones via scientific techniques, and various mobile forensic techniques have been researched and established over the last decade. However, many of those traditional data acquisition methods are less effective against modern smartphones, without proper user authentication, due to strong cryptographic security mechanisms at the operating system level. These mechanisms prevent execution of unauthorized software, and encrypt all user related data with keys derived from both a securely stored master key and a user chosen password.

Given the state of security features, current mobile forensic research is focused on identifying more invasive techniques to access data. These methods - which are mainly based on the exploitation of hardware and software vulnerabilities - can escalate privileges to the level where an examiner can directly acquire decrypted user data from a running device, or extract the key material that can be used to decrypt extracted user data afterwards. The growing need for vulnerability exploits is also creating new challenges. First, mobile forensic tool vendors are changing their business models. Instead of simply offering a tool, commercial forensic tool vendors are starting to offer exclusive in-house forensic analysis services, which they operate as proprietary solutions. Second, complex and ambiguous legal issues need to be taken into account when law enforcement agencies (LEAs) perform exploit-based forensic acquisition. The regulations regarding responsible disclosure of vulnerabilities in some jurisdictions may also have negative impacts on collaborative work among international law enforcement agencies.

In the current smartphone market, Android is significantly dominating the operating system market for mobile devices, followed by iOS. The dominant smartphone developers are Samsung (20%), Huawei (20%) and Apple (14%). While most popular devices are supported by existing, or yet to be developed, commercial forensic tools, LEAs will need to focus on developing their own acquisition methods for less common smartphones that are harder to forensically examine, which in turn are being attractive to criminal groups.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Introduction and Background

Mobile forensics is a branch of forensic science dedicated to the extraction and analysis of evidence found on digital devices via forensically sound conditions using accepted methods. Mobile forensic study has evolved significantly as mobile phones (and related devices such as mobile tablets) have become an essential part of our daily lives. Mobile devices, especially smartphones, frequently contain data relevant to criminal investigations, and forensic analysis of those devices has become an increasingly critical investigative capability for law enforcement agencies (LEAs). Mobile forensics is inherently challenging, due to the fact that compared to traditional personal computers, smartphones have limited processing and memory resources, different System-on-Chip (SoC) architectures, and well-secured operating systems. In addition, forensic examiners must deal with the general lack of hardware, software and interface standardization within the mobile industry, along with the rapid rate at which mobile device technology changes.

A key feature of modern smartphones - related to both hardware and operating systems - is the implementation of data encryption by default. The encryption feature creates challenges for LEAs seeking to extract data from modern smartphones. Those challenges are clearly illustrated by real world incidents, such as the December 2015 terrorist attack in San Bernardino, California, that resulted in many deaths and injuries [61]. During the FBI's investigation of the attack, their forensic examiners had to deal with an Apple iPhone 5C that was locked with a four-digit pin code and set to eliminate all its data after ten failed unlock attempts. On that basis, the FBI obtained a court order directing Apple to provide support to the FBI and use Apple's existing capabilities to extract evidence from the iPhone belonging to one of the attackers. In response, Apple CEO Tim Cook replied: "We oppose this order, which has implications far beyond the legal case at hand [64]." The dispute between the FBI and Apple led to a public debate about the implications of adding back-doors for government access to encrypted data on mobile devices. The debate has not been solved to this day, as commentators point out the security and privacy risks in purposely weakening encryption methods with backdoors.

In order to tackle the current technical challenges and extract data in clear-text from encrypted smartphones, digital forensic examiners at LEAs have been researching possible solutions. While some of the traditional forensic methods still work, often times, modern forensic techniques require exploiting system vulnerabilities. In this report, current trends of smartphones and the forensic techniques will be studied.

1.2 Report Organization

This report is organized as follows:

In **Chapter 2**, we discuss how the mobile forensic technique focuses have changed over the years due to the security features on smartphones. **Chapter 3** introduces current trends in smartphone markets and mobile forensic tools, including current and future market prediction for the purpose of identifying the future challenges in mobile forensics at the LEAs. Then, the state-of-the-art forensic techniques used in the LEAs will be introduced in **Chapter 4**, expanding the discussions found in Chapter 2. Lastly, forensic soundness of the current forensic techniques, as well as legal concerns will be introduced in **Chapter 5** as the introduction to the future Work Package 2. The overall conclusion will be provided in **Chapter 6**.

Chapter 2 The Paradigm Shift in Mobile Forensics

In this chapter, we provide an overview of traditional mobile forensics techniques, discuss the widespread adoption of encryption and other security features in mobile devices, and then assess the impacts of encryption on traditional mobile forensics techniques.

2.1 Traditional Mobile Forensic Techniques

With an ever-growing need for user data acquisition from mobile devices, the digital forensic community has conducted extensive research and development regarding the challenges. As defined by National Institute of Standards and Technology [1], mobile data acquisition techniques can be categorized into the following five levels:

- Level 1: Manual Extraction
- Level 2: Logical Extraction
- Level 3: Hex Dumping / JTAG
- Level 4: Chip-off
- Level 5: Micro Read

In **Manual Extraction (Level 1)**, an examiner directly manipulates the target smartphone using the device's input interface (i.e., keypads and buttons), and records the content shown on the display of the device. **Logical Extraction (Level 2)** which is the most common method in mobile forensics, extracts the smartphone data (files and folders) by communicating with the target phone through its wired/wireless connection interfaces. The **Hex Dumping and JTAG** approaches **(Level 3)** let an examiner acquire partial raw data stored on the phone's memory storage media. Acquisition can be done through debug interfaces on the target device or by uploading modified boot loaders or other custom software. By performing **chip-off (Level 4)**, an examiner can obtain an identical copy of the entire raw data on the target smartphone by directly accessing the non-volatile memory chip of the target device. **Micro read (Level 5)** is a highly-specialized technique, where the stored data in a non-volatile memory is extracted in electrical property form through the direct observation of the memory die *inside* the non-volatile memory chip. Data acquired through Level 1 and 2 techniques is usually called Logical Data, while data acquired via Level 3 to 5 techniques is called Physical Data and has the advantage to include remnants of deleted data.

The common understanding in traditional mobile forensic models has been that the higher the acquisition level, the higher the chance of forensic data recovery. Generally, as examiners use a higher acquisition level, the accessible range of data becomes wider. Furthermore, physical acquisition can bypass the user authentication mechanisms on smartphones such as pin-codes, passwords, and biometrics. Therefore, LEAs have widely utilized chip-off data acquisition as a generic technique to extract data from smartphones when the target device is in a locked state.

2.2 Encryption and Other Security Features in Smartphones

In order to protect user privacy and provide confidentiality of data, encryption techniques are currently widely implemented in modern smartphones. Traditionally, encryption techniques were applied at the application level in order to protect individual user data such as emails and photos. With the growing concerns over security and privacy, however, encryption techniques are now implemented at the Operating System (OS) or firmware level with a hardware "security anchor" deep within the silicon. In modern smartphones, user data is encrypted prior to being stored on the non-volatile memory. This means that the physical data, or data at rest, is stored in an encrypted manner.

In addition to encryption techniques, other "security by design" features, such as secure boot chain and OS level access control are implemented by default in modern smartphones. During the boot process, each hardware and software component is validated to ensure that only authorized code can be executed on the system. This mechanism is also known as Root of Trust (RoT).

By implementing those techniques, smartphone manufacturers protect not only user data, but also their corporate proprietary data and technology. As a result, users have little freedom to control their own mobile devices, and they are limited to using it within the device or OS maker's closed ecosystem.

2.3 Traditional Mobile Forensic Techniques Applied to Encryption

The natural question that may arise here is how the encryption and other modern security features impact the traditional mobile forensic techniques. The effectiveness of the five-level model of mobile forensics (described in Section 2.1), in the presence of encryption, can be evaluated as follows:

- Level 1: Manual Extraction

  If an examiner knows and possesses the legitimate user secret decryption technique (i.e., pin-codes, passwords, or fingerprints), and can properly unlock the target smartphone in a fully operating state, Manual Extraction is still effective on modern smartphones. A proper control will display the user data on the target smartphone screen, and the examiner can record its contents using an appropriate recording device. The remaining problems are application security mechanisms for which access codes might be needed and temporal local storage of decryption keys for which online connections are needed.

- Level 2: Logical Extraction

  Similar to Manual Extraction. If an examiner can take control of the target smartphone, and can communicate with it, Logical Extraction is still an effective data extraction method for modern smartphones. In order to perform Logical Extraction, an examiner sometimes needs to unlock or bypass the screen lock, or make the target device authorize a debugging operation. If the access codes are unknown, software vulnerabilities on the system can be exploited to escalate privileges and get access to acquire (unencrypted) user data. Depending on how the phone is configured, the access code still needs to be applied to acquire decrypted user data. Depending on the acquired privileges and extracted cryptographic material, unlimited access codes attempts can be done with software running on the phone itself (on-line) or on a faster computer cluster (off-line).

- Level 3: Hex Dumping / JTAG

  While JTAG and other debugging interfaces are used on modern smartphones, in many instances those interfaces are disabled or locked before a smartphone is shipped from the factory. Therefore, examiners may first need to find a way to utilize those debugging interfaces for Hex Dumping on the target device. Once enabled, Hex Dumping is still an effective data acquisition method. However, as the acquired physical data is in an encrypted state on modern smartphones, decryption procedures are required after data acquisition. The encryption keys are often derived from both the user defined access code and a cryptographic key stored in the phone which is protected in such a way that it can only be used by authorized software on the phone. Some smartphone vendors even claim that the encryption keys cannot be accessed from software [34].

- Level 4: Chip-off

  As long as the forensic lab possess a capability to read the memory chip of the target smartphone, Chip-off is still available for data acquisition. However, like Hex Dumping, data in the non-volatile memory is encrypted. Hence, the acquired data is unreadable until it is decrypted.

- Level 5: Micro Read

  The miniaturization of the modern semiconductor fabrication process creates a physical challenge to micro reading techniques. Even if an examiner can successfully extract the

contents of the non-volatile memory from the target smartphone, the data is encrypted, therefore the decryption procedure is once again required. Nevertheless, Micro Read may allow examiners to extract key material and hidden security mechanisms, although it remains as an arduous task.

2.4 The Need for New Techniques

As we saw in the previous section, contrary to the traditional beliefs, going higher in the traditional five-level model is not necessarily more effective in forensic data recovery for modern smartphones. While all those techniques are still technically available on modern smartphones, the acquired data itself is not always readable or meaningful due to encryption. Even though an examiner can access a wider range of data when performing physical data acquisition (using the techniques described in Levels 3-5), compared to logical acquisition, the data remains unreadable if not decrypted. Given this situation, currently, either extracting the data in a decrypted state, or extracting the encryption key is the major objective in forensic data extraction. Without the right user authentication, this can only be achieved either by exploiting software vulnerabilities on the target device, or by identifying and accessing the storage where cryptographic keys are stored. Details to perform those techniques, along with their role in data extraction work flow are introduced in Chapter 4.

Chapter 3 Trends in Smartphones and Mobile Forensic Tools

In this chapter, we study the current status of the smartphone market along with the trends in mobile forensic tools. Mobile forensic tools are constantly trying to keep up with the smartphone market trends. Studying those two trends side-by-side helps LEAs get a full picture of current publicly available solutions, and identify current and future targets in their mobile forensic research.

3.1 Smartphone Manufacturers

3.1.1 Sales Volumes

Table 1 lists recent smartphone models (sold within the last 3 years), and their number of units sold. Please refer to Table 3 in the Appendix for the complete top 30 most popular smartphone models worldwide based on sales volume between 2010 and 2020 [6-14].

Table 1: Most recent mobile devices (as of August 6, 2020) between 2017 and 2020.

Manufacturer	Model	Year	Million units sold	Overall Ranking by sales volume from 2010 to 2020 (taken from Table 3)
Apple	iPhone 8 and iPhone 8 Plus	2017	86.3	2
Apple	iPhone XR	2018	69.4	6
Apple	iPhone X	2017	63	7
Apple	iPhone Xs and iPhone Xs Max	2018	48	13
Samsung	Galaxy S8 and Galaxy S8+	2017	41	14
Apple	iPhone 11	2019	37.3	16
Samsung	Galaxy S9 and Galaxy S9+	2018	35.4	17
Apple	iPhone 11 Pro and iPhone 11 Pro Max	2019	33.1	18
Samsung	Galaxy A10	2019	30.3	19
Samsung	Galaxy A50	2019	24.2	22
Samsung	Galaxy A20	2019	23.1	23
Xiaomi	Redmi Note 7 and Redmi Note 7 Pro	2019	20	24
Huawei	P30 and P30 Pro	2019	20	25
Huawei	Mate 20 and Mate 20 Pro	2018	17	26
Samsung	Galaxy S10, Galaxy S10+, Galaxy S10e	2019	16	29
Huawei	P20 Lite	2018	16	28
Samsung	Galaxy J2 Core	2018	15.2	30

3.1.2 Market Trend

The worldwide market share of the smartphone vendors is shown in Figure 1. Samsung has been holding about 20% of the market share, followed by Huawei, Apple, Xiaomi and Oppo. The smartphone market has been dominated by those vendors, and all the rest has been shared by other vendors like Sony, Nokia, Honor, Razer, LG, OnePlus, Doro, Motorola, ZTE, BlackBerry, and Alcatel, to name a few.

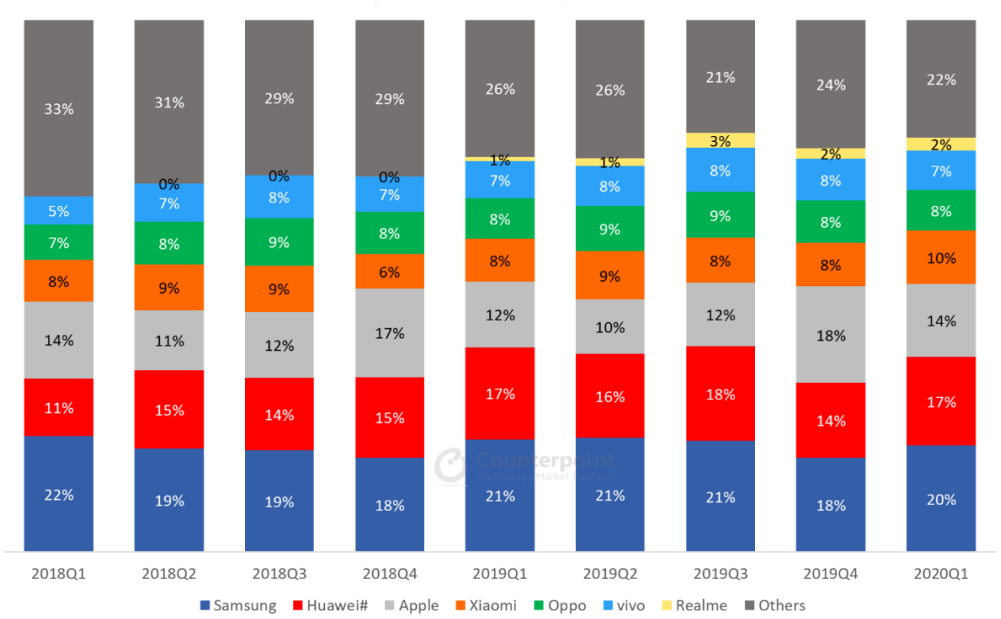

Figure 1: Mobile device vendor market share from 2018 to 2020 (retrieved from [15]).

3.2 Smartphone Operating Systems

3.2.1 Market Trend and Forecast

There are currently two Operating Systems (OSs) that dominate the smartphone market: Apple iOS and Android. The Apple iOS, a closed operating system based on the XNU kernel with limited open-source components, was first released in 2007. The Android, marketed by Google and developed by the Open Handset Alliance consortium which currently includes 84 companies, was first released in 2008. It is an open-source operating system based on a modified Linux kernel. Figure 2 shows the smartphone OS market share from 2012 to 2020. Android has been mostly dominating today's market [3]. Recent studies [4], [5] state that Android dominates around 74.6% of the market share, while iOS holds about 24.8%. The remaining 0.6% is shared by Windows and other OSs. It is forecasted that the Android will keep dominating the market for the next few years [2]. The latest stable version of each OS at the time of this writing is iOS 14 (released in September 2020), and Android 11 (released in September 2020), respectively.

There are also a few operating systems derived from Android, usually designed in order to enhance the end-user's privacy. The full list of smartphone OSs including the discontinued ones can be found in the Appendix.

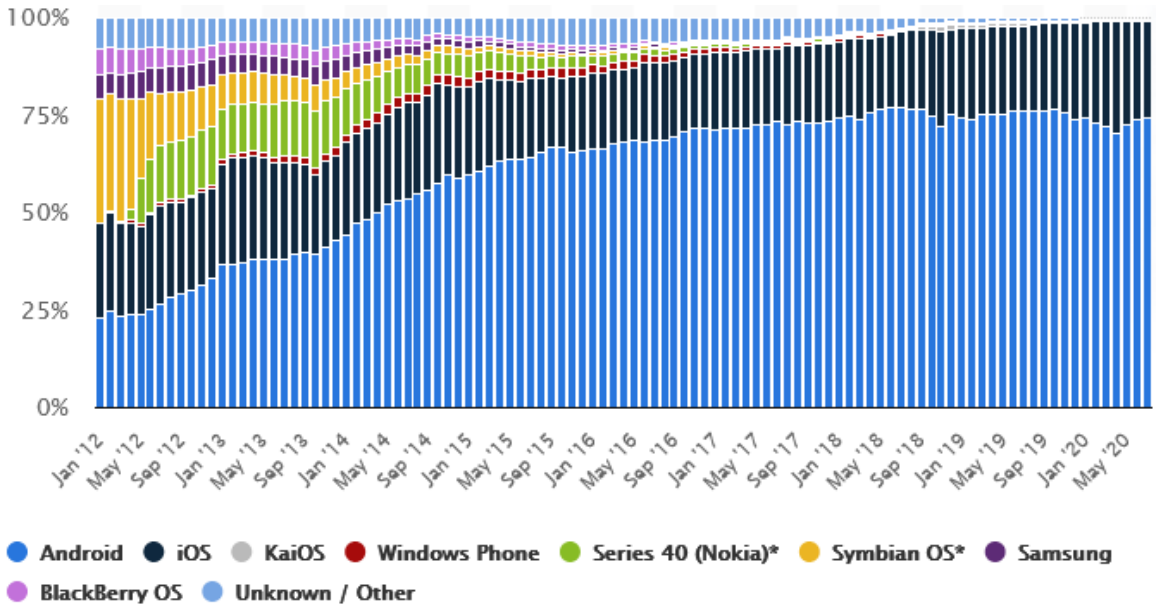

Figure 2: OS market share from July 2012 to July 2020 [5].

3.2.2 Security Features

Modern smartphone OSs encrypt user data by default. Apple introduced file-system encryption starting iOS 3. iOS versions higher than iOS 8 encrypt user data per file using user passcode. In Android, two types of encryption schemes have been employed. One is Full Disk Encryption (FDE) and the other is File Based Encryption (FBE). FDE is a technique where the whole user data partition is encrypted with a single encryption key, while FBE encrypts different files with different keys, allowing files being decrypted independently. FDE was introduced in Android 4.4, and has been supported up until Android 9. Starting Android 7.0, FBE has been used as the standard encryption technique. An historical breakdown of the various Android OS versions in use is provided in Figure 3. Today, most of the Android devices have a higher version than Android 6. This means that user data in the android devices that LEAs seize at crime scenes is now mostly encrypted.

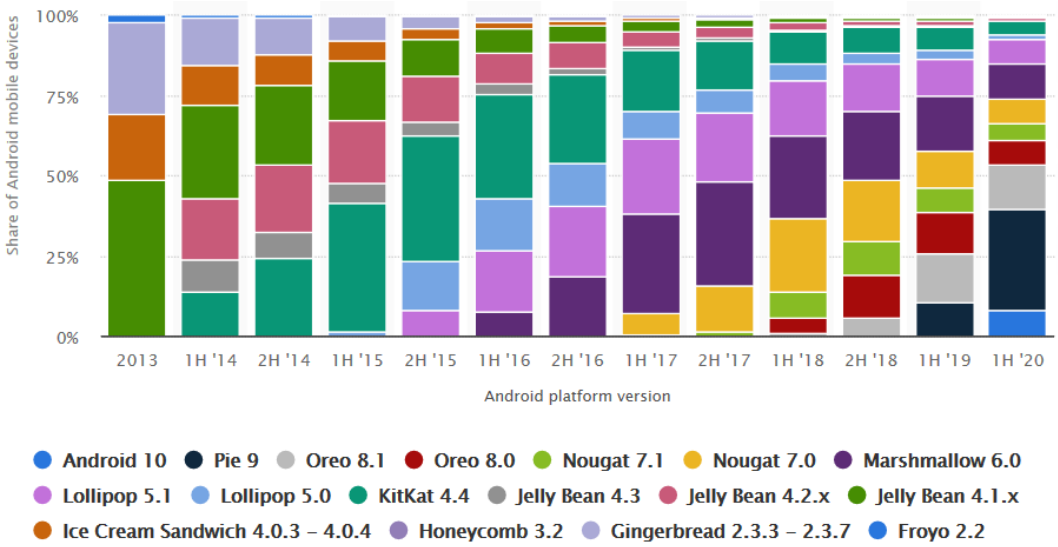

Figure 3: Breakdown of Android versions from 2013 to 2020 [2].

3.3 SoCs

A system on a chip (SoC) is the main integrated circuit (IC) of a smartphone printed circuit board (PCB) that integrates most components found on the motherboard of current desktop computers. Current smartphone SoCs contain multiple application processor cores, graphical engines, baseband processors and a lot of other building blocks for interfacing with external components. As the application processor core is the one which control the basic operation of the modern smartphone, we focus on application processors in this section. Since almost all the smartphones on the market use ARM architecture, we focus on ARM-based application processors in this section. ARM is a semiconductor designer which licenses its architectures to other SoC manufacturers such as Apple, Samsung, Qualcomm, MediaTek, Broadcom, LG, and Huawei. These manufacturers receive the core architecture and are licensed to implement it themselves, hence there exist wide range of ARM-based processors on the market.

3.3.1 ARM Architectures

ARM architectures use reduced instruction set computing (RISC), making ARM's micro-architectures more power-efficient than its x86 counterpart (i.e., Intel), and thus preferred for embedded devices. The ARM architecture comes in three different profiles, namely: A for application, R for real-time, and M for micro-controllers. The application profile (Cortex-A processor family) is the one used in mobile devices. It comes in either 32-bit or 64-bit mode (ARMv8-A only). Figure 4 shows the ARM instruction set architectures (ISAs) used in the modern SoCs. All the modern smartphone SoCs use 64-bit ISA. The integration trends to 64-bit can be seen starting in 2014. 32-bit ARM ISA is no longer used in the modern smartphone SoCs.

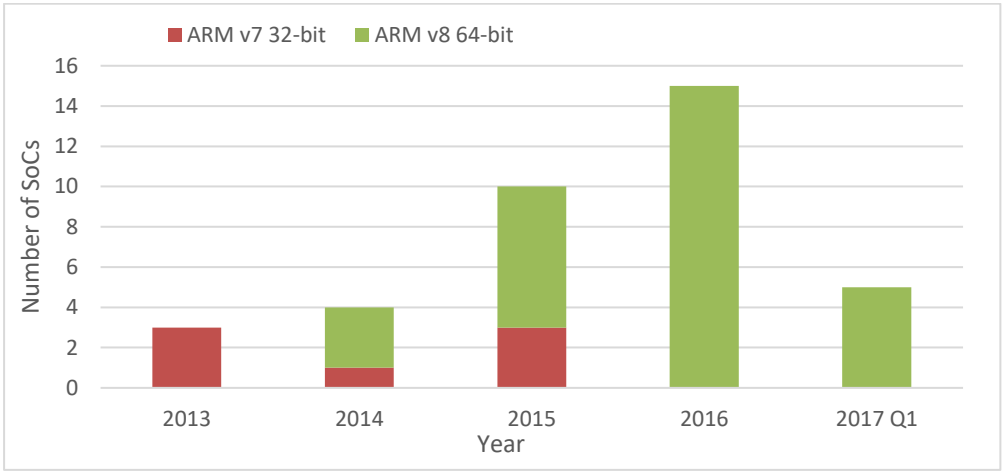

Figure 4: Instruction set used in smartphone SoCs since 2013 (sampled 37 popularly-used SoCs).

In addition to the shift of instruction set from 32-bit to 64-bit, new heterogeneous computing architecture developed by ARM, called big.LITTLE is popularly employed in today's SoC development. With big.LITTE architecture, multi-processor environment can be realized in one SoC. Figure 5 shows the implementation of big.LITTLE architecture in modern SoCs.

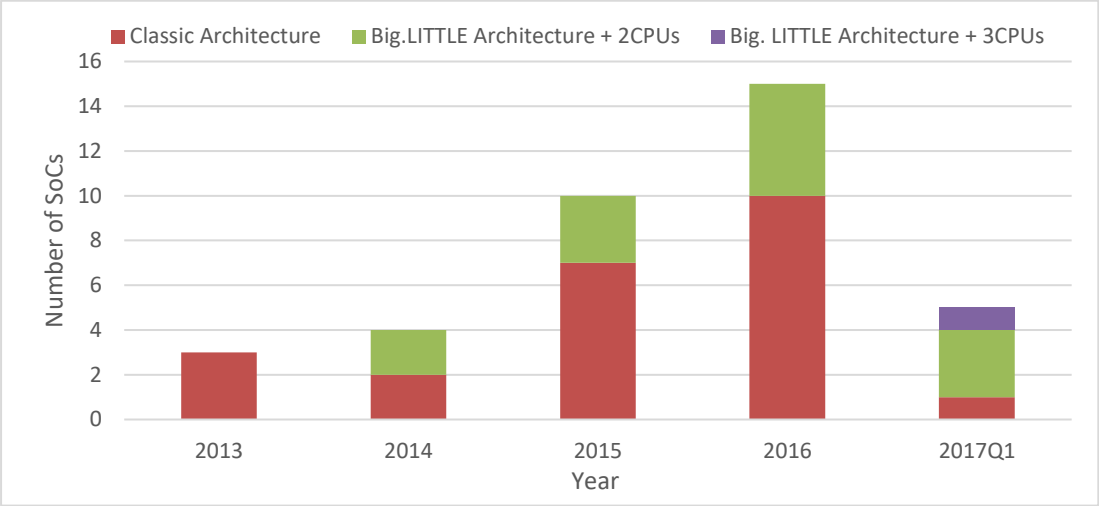

Figure 5: ARM Big.LITTLE implementation in modern smartphone SoCs

3.3.2 Market Trend

Application processor market share is shown in Figure 6. Qualcomm has been dominating the market, holding around 40% of the current application processor market. HiSilicon started sharing large amount of share starting in 2019. HiSillicon application processors are mainly used in smartphones produced by Huawei, its parent company. Other dominating smartphone vendors such as Samsung and Xiaomi are using Quacomm application processors. For more detailed specifications in smartphones application processors, please refer to Table 9.

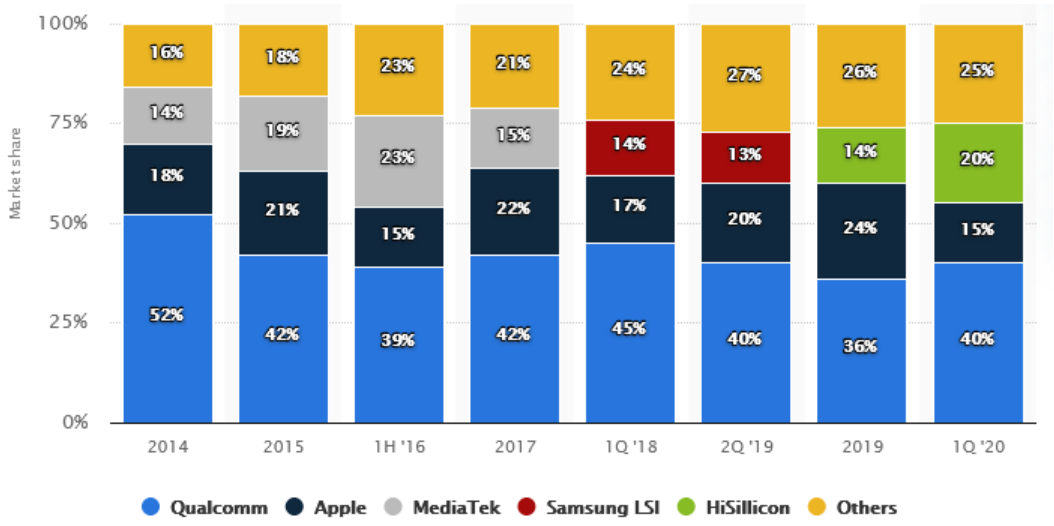

Figure 6: Smartphone SoC market share from 2014 to 2020 [33].

Application processors found in today's most recent smartphone models with the highest sales volumes (see Table 1) are:

- Apple:
  - Apple A13 Bionic (ARMv8.4-A ISA): Used in iPhone 11, iPhone 11 Pro and iPhone 11 Pro Max [16].
  - Apple A12 Bionic (ARMv8.3-A ISA): iPhone XR, iPhone Xs and iPhone Xs Max [17], [18] and [19].
  - Apple A11 Bionic (ARMv8-A ISA): iPhone 8, iPhone 8 Plus and iPhone X [20].

- Huawei:
  - HiSilicon Kirin 980 processor (ARMv8.2-A ISA): P30, P30 Pro, Mate 20 and Mate 20 Pro [21], [22].
  - HiSilicon Kirin 710 processor: P20 Lite [23].
- Samsung:
  - Exynos 7884 (ARMv8-A ISA): Galaxy A10, Galaxy A20 [24], [25].
  - Exynos 9610 (ARMv8-A ISA): Galaxy A50 [26].
  - Exynos 9820 (ARMv8.2-A ISA) and Qualcomm SM8150 Snapdragon 855 - Kryo 485 (ARMv8 ISA): Galaxy S10, Galaxy S10+ and Galaxy S10e [27].
  - Exynos 9810 (ARMv8.2-A ISA) and Qualcomm SDM845 Snapdragon 845 - Kryo 385 (ARMv8 ISA): Galaxy S9 and Galaxy S9+ [28].
  - Exynos 7570 (ARMv8-A ISA): Galaxy J2 Core [29].
  - Exynos 8895 (ARMv8-A ISA) and Qualcomm MSM8998 Snapdragon 835 – Kryo 280 (ARMv8 ISA): Galaxy S8 and Galaxy S8+ [30].
- Xiaomi:
  - Qualcomm SDM660 Snapdragon 660 - Kryo 260 (ARMv8 ISA): Redmi Note 7 [31].
  - Qualcomm SDM675 Snapdragon 675 - Kryo 460 (ARMv8 ISA): Redmi Note 7 Pro [32].

3.3.3 SoC Clock Frequency and Fabrication Process

Modern Smartphone SoCs can work on a very high speed. Figure 7 maps the clock speed of application processors used in modern smartphones. SoCs in the high-end smartphone models can operate more than 2.5 GHz range. Even the low-priced smartphones use SoCs that can operate faster than 1GHz.

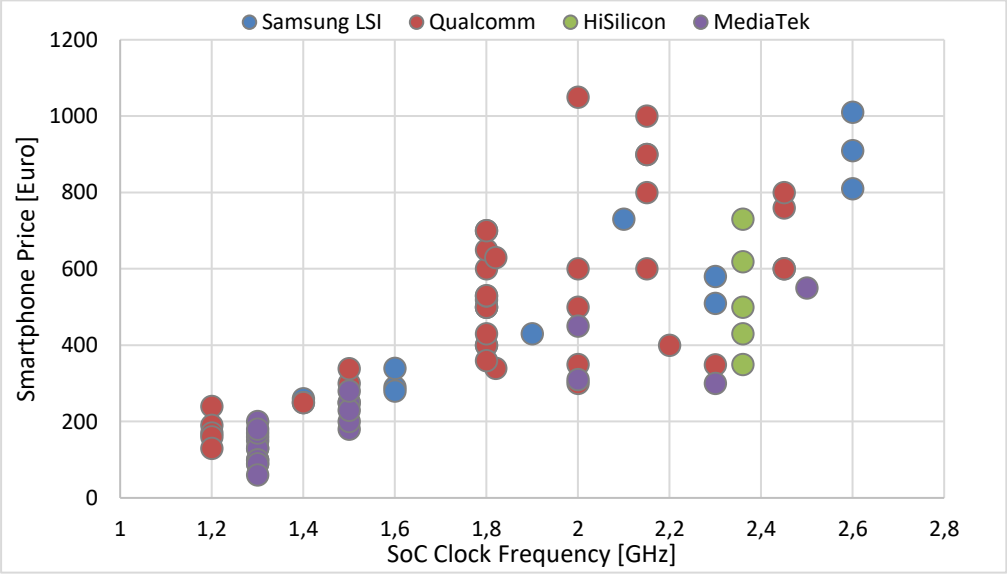

Figure 7: SoC clock frequency against smartphone price and its manufacture

In order to respond to the demanding needs for smaller size of SoCs, SoC fabrication process keeps shrinking accordingly. For example, Apple A13 is manufactured with 7nm+ technology, and Exynos 9820 with 8nm technology.

3.3.4 Security Trends

For the implementation of security mechanisms, modern smartphones heavily use ARM TrustZone technology integrated in almost all current processors. TrustZone is based on the

GlobalPlatform's Trusted Execution Environment (TEE) open standard and its implementation is openly available. Thus, different versions of TrustZone are found depending on the hardware manufacturer. Basically, TrustZone provides an isolated environment for security critical components in a system, by separating a normal operating system from a much smaller secure operating system, both running on the same hardware device. Hence a secure world and a normal world can co-exist on a system. Similar techniques are used on Apple devices to isolate the processing of cryptographic keys and other sensitive information.This system is called Secure Enclave Processor (SEP).

Because TrustZone and SEP are not designed to resist physical attacks, phone manufacturers are increasingly using hardware security modules (HSM) to raise security. The biggest driver for this trend is the high security demands for payment related functionality. Apple started to use a HSM with their iPhone 6 and uses the term Secure Element (SE) for a tamper resistant chip from NXP [34]. Google is introducing similar technology with its Titan M chip first introduced in the Pixel 3 [35].

3.4 Trends in Mobile Forensic Tools

3.4.1 New Business Model

Various mobile forensic tools are available on the market that allow forensic examiners to extract digital evidence from modern smartphones. Traditionally, software vendors used to provide software suites, where customers can purchase a set of software tools depending on their needs. Today however, since the software vendors focus on finding and exploiting device vulnerabilities in order to extract data from encrypted devices, they have a growing need to keep their findings secret. Therefore, forensic software vendors nowadays tend to follow a new business model, which is relevant for research at LEAs in order to get a full picture of current publicly available solutions. Instead of simply providing software suites, vendors sometimes provide services only to trusted parties, take many measures (including physical) to keep their findings secret, and follow a confidential contract. The typical business model is tiered as follows:

- Entry model: Universally available generic mobile forensic tool

  Using widely available phone controlling protocols or known security vulnerabilities, vendors develop a universal mobile forensic software tool. Tools are widely available commercially, as open source, or as free-ware.

- Intermediate model: Model-targeted prestigious forensic tool available for trusted parties

  Vendors develop software tools using zero-day or sensitive/trade secret related vulnerabilities on specific smartphone models. To protect company secrets, forensic software vendors develop a tool in a protected black box, and make it available as a prestigious product only to reliable customers.

- Advanced model: In-house forensic service at the vendor's premises

  In order to protect highly sensitive company secrets, or as highly technical knowledge is required during data acquisition, vendors perform analysis only at their premises. Vendors accept target devices at their premises, and acquisition is performed by the company's experts. Customers receive the results once the acquisition is completed. The tools are kept in the company, and never provided to a third-party.

Categorization of the existing tools regarding the business model can be found in Table 2. While the smartphone vendors harden their products and protect the proprietary software on their devices with high level security, mobile forensic tool vendors have been focusing on identifying the vulnerabilities on those products, and developing exploitation code which allows data acquisition. Since a technique becomes obsolete as soon as the security hole is patched by the

smartphone vendors, mobile forensic software vendors tend to not make their findings public. This seems to make the above mentioned three-tier model more common.

A service that surprisingly seems not to be offered by commercial forensic companies is the distributed search capability for user secrets (off-line search). For some modern smartphones, hashes or secret keys can be extracted with available exploits. However, in order to decrypt the user data, a user secret needs to be found before the data decryption key can be derived. Current "Advanced model" services only seem to offer on-line searching of user secrets and no off-line searching on distributed computers.

3.4.2 Cloud Data Extraction Capability

Modern smartphones store data not only on the physical devices, but also on cloud servers provided by manufacturers or OS vendors. Indeed, since the physical device has limited storage capacity, some apps upload old data to the cloud server, and delete them from the physical device. Taking this behaviour, some mobile forensic vendors offer a cloud-based evidence collection function in their software tools. After acquiring required information from the target devices (user credentials), the software accesses the cloud server, and collects information belonging to the target device. Forensic tools that handle cloud data extraction can be found in Table 2. Legal issues regarding this procedure are discussed in Section 5.2.1.

3.5 Mobile Forensic Software Tools

Table 2 shows a list of widely used mobile forensic software tools in alphabetical order, that can extract logical or physical data from modern smartphones. Note that Table 2 does not include flasher box tools used for repair and hacking of smartphones. While flasher box tools can be useful for both forensic research and case examinations, extensive testing on a reference phone is required before each use [54].

Table 2: Existing Mobile Forensic Tools

Company name	Tool name	Extraction level L=Logical F=File system P=physical	Business model E=Entry M=Intermediate S=In-House Service	Software model C=Commercial F=Freeware O=Open Source	Generic/ Specific	Cloud extraction
Bjoern Kerler	Mobile Revelator	F, P	E	F	G	
Belkasoft	Acquisition Tool	L	E	C	Android/ iOS	Y
Blackbag	Mobilyze	L	E	C	Android/ iOS	
Cellebrite	UFED	L, F	E	C	G	Y
Cellebrite	UFED Premium	F, P	M	C	Android/ iOS	
Cellebrite	CAS	F, P	S	C	G	
Compelson Labs	MOBILedit	L	E	C	G	
Denis Sazonov	Andriller CE	L	E	O	Android	
Elcomsoft	Cloud Explorer	L	E	C	Google	Y
Elcomsoft	Phone Breaker	L	E	C	Apple	Y
Elcomsoft	iOS Forensic Toolkit	L, F, P	E	C	iOS devices	
Grayshift	GrayKey	F	M	C	iOS devices	
Hancom Forensics	MD	L, P	E	C	G	Y
Magnet Forensics	AXIOM		E	C	G	Y
MSAB	XRY	L, F, P	E	C	G	Y
MSAB	Access Services	F, P	S	C	G	
NowSecure	AFLogical OSE	L	E	O	Android	
NowSecure	Santoku	L, F	E	O	G	
Oxygen	Forensic Detective	L, F, P	E	C	G	Y
Paraben	E3:DS	L	E	C	G	Y
Susteen	Secureview		E	C	G	

Chapter 4 State-of-the-art Mobile Forensic Techniques

As discussed in Chapter 2, the widespread implementation of encryption and other modern security features have undermined the effectiveness of traditional mobile forensic techniques, and it is requiring LEAs to develop new or refined approaches for extracting data from mobile devices. In this chapter, we introduce the state-of-the-art mobile forensic techniques that LEAs are using against encrypted smartphones. As introduced in Chapter 2, we categorize the techniques following the traditional five-level classification system. Required data decryption techniques or cryptographic key acquisition techniques are explained along with each data extraction technique.

4.1 Manual Extraction

In cases where an examiner can obtain the user secret required to unlock the device, the examiner can manually manipulate the target device, and perform the Manual Extraction by recording its contents. Existing commercial tools can support the manual extraction procedures with functions like semi-automated camera kits, emulation of user input combined with automatic screen capturing, and report generation [36], [37]. A user secret required for unlocking the device could be a password, a passcode, pattern-drawing, or a biometric characteristic (fingerprint, voice, face). If a fingerprint is used for user authentication, LEA examiners are sometimes able to spoof the authentication by copying the fingerprint of the device owner, then use it on the fingerprint scanner to unlock the device. Note that fingerprint authentication, along with other biometric authentication, only works if the target device is in After First Unlock (AFU) state, and not equipped with other advanced security features such as inactivity-time detection measures (secure smartphones can be set up to automatically reboot after a set period of inactivity time). AFU means that the target device is in a state where it has been turned on, and unlocked at least once after booting, and never turned off since then. When the smartphone is in Before First Unlock (BFU) state (it has never been unlocked since last booting, or it is turned off), a password, a passcode, or a pattern is required to unlock the device and enable the biometric authentication. Additionally, most biometric authentication methods have a limited timespan (e.g. 48 hours for current iOS devices) in which biometric characteristics can be used before the BFU code would be required again.

When performing Manual Extraction, examiners should note that there is a “panic” password option available in some modern smartphones. When set up, the panic password can execute a hidden rule, such as wiping data, or disabling some functions of a phone. If the panic password was used instead of the legitimate unlocking password prior to data extraction, manual extraction would fail, and there is a great chance that the data is unrecoverable.

Modern smartphones are also equipped with anti-brute-forcing techniques. After a set number of failed authentication attempts with incorrect passcodes/passwords/patterns, the device becomes unavailable for a set amount of time. In the worst case, data on the target device can be erased and become unrecoverable.

4.2 Logical Extraction

4.2.1 Logical Data Extraction through User Communication Interfaces

If the target smartphone operates properly, and if an appropriate software tool is available, Logical Extraction is the quickest way to extract data from the target device in criminal investigations. Logical extraction can be done through user level communication interfaces on the device, such as USB, external storage, Wi-Fi, and Bluetooth. A wide range of mobile forensic software tools

are available that allow examiners to perform logical extraction. The basic protocol used for logical extraction is the data backup function [38], which can either be standard or vendor-specific. Data access management on modern smartphones is controlled at the application level, and forensic software can use this function to copy selected app-relevant data to a connected storage media or to a connected computer. When required, forensic agent software may be uploaded onto the target device to utilize APIs in a forensically sound way, to efficiently acquire required app-related data.

In order to perform logical data extraction, most modern smartphones must be unlocked by entering the user secret. One should note that unlocking the target phone with user secrets raises the same challenges as manual extraction. Once unlocked successfully, the target phone needs to be configured to accept commands from the connected computer for data extraction. For modern smartphones, rooting the device (escalating the administrator privilege) is often required to perform logical data extraction. Furthermore, on current versions of Android, applications may choose not to be part of the backup operations supported by the operating system. If the user data from an opted-out app is required for extraction, downgrading the app version on the target smartphone may allow examiners to extract the user data. This operation is supported by some forensic software tools [65]. However, since this operation directly modifies the target smartphone, it should be regarded as the last option.

4.2.2 File System Extraction

When strict Logical Extraction is used for data acquisition, an examiner can only collect files and folders related to selected apps or communication protocols, and deleted data cannot be recovered. Traditionally, this is where mobile forensic examiners decide whether they proceed to physical acquisition or not. However, since most modern smartphones use known file systems (i.e. APFS for Apple iOS devices, and ext4 for Android devices), and the data is stored on non-volatile memory in a file system structured format, an examiner can try to extract partial or full file system data. Some forensic tools are available for performing file system extractions (example tools can be found in Table 2.)

Compared to traditional logical extraction, file system extraction allows examiners to acquire more data, potentially including deleted data remnants. All data related to the apps is collected, and a forensic tool does not have to communicate and acquire individual data through an app-level API. An examiner can therefore access app-related databases, system files and logs. As long as the deleted data remnants remain in the database, an examiner can perform data recovery after file system extraction. Moreover, when FBE is used, file system extraction is preferred instead of physical extraction (techniques introduced in section 4.3 and section 4.4) because of the way the encryption is implemented.

In order to conduct effective file system extraction, rooting the device is required. Without rooting, examiners can only acquire partial data, and data recovery may be limited. Please note that the methods used for file system extraction are various and can be categorized in either logical, Hex Dumping / JTAG, or Chip-off.

4.2.3 User Secret Acquisition

As discussed in section 4.1 and 4.2.1, prior to perform Manual Extraction or Logical Extraction, correct user secret needs to be obtained. While modern smartphones prevent examiners from performing brute-forcing user secrets, exploiting vulnerabilities can bypass this restriction [62]. Several forensic acquisition tools can automate this process. Through exploitation, an examiner can search for user secrets on the device itself (on-line) or extract intermediate information from the device which can be used on faster (distributed) systems to search for user secrets (off-line). Some tools acquire key information from the RAM of the target device, but this approach is only effective if the target device is in AFU state [62].

4.3 Hex Dumping / JTAG

Hex Dumping / JTAG along with Chip-off (section 4.4) try to establish a direct access to the raw information stored in the non-volatile memory in the target smartphone. If FDE is used in the target device, and if an examiner can acquire the disk encryption key, then the examiner can acquire the physical data, and manually decrypt the acquired data. To acquire the disk encryption key, often a combination of software exploits and password attacks is required [39]. Most Android devices with FDE can be configured by the user to use secure startup or not. If a device is not configured with secure startup, it uses an encryption key derived from a default password [63] which is available in several forensic extraction tools. In that case, acquisition of decrypted data is possible with a method that gives access to the device at the data partition level. In most other cases, however, vendor specific FBE and Key Derivation functions (KDF) need to be reverse engineered.

4.3.1 Hex Dumping

A popular option for Hex Dumping for modern smartphones is to utilize a modified boot loader, or other custom software. Combination of several techniques described in this section can be used to perform Hex Dumping.

4.3.1.1 Exploiting Boot Sequence Vulnerabilities with a Custom Boot loader

If an examiner can load a custom boot loader into the target device during the boot process and run it, there is a great chance that the device can be manipulated by running arbitrary code, making physical data acquisition possible. Traditionally, loading a custom boot loader was enabled by the device manufacturer. Special modes (i.e., download mode or rescue mode) allowed users to run a custom boot loader into the RAM during boot-up. In modern devices, however, in order to maintain system integrity, manufacturers enable boot loaders to run only after they are properly verified.

The boot loaders are responsible for initializing hardware components and loading the operating system which then starts device operation including encryption. Figure 8 shows an example of Android booting process. When a smartphone is powered on, multiple boot loaders are executed in chain. The first boot loader which is hard-coded in the ROM of a SoC is called the primary boot loader (PBL), and the one that is loaded by this PBL (normally after verification of a signature that can only be produced with a private key of the phone manufacturer or OEM) is called the secondary boot loader (SBL). The SBL normally loads another boot loader that finally loads the operating system [45]. Only when the verifications are passed, the boot loader is loaded into the system memory, allowing the system to start the normal booting procedures.

The verifications are usually done by checking if the boot loader is properly signed. For some smartphone models, signed boot loaders are publicly available [46]. By flashing those boot loaders with known vulnerabilities into the target smartphone, an examiner may gain the highest privilege of the target phone, successfully acquiring the memory data. The flashing of the boot loaders can be done by utilizing some special modes such as Emergency Download (EDL) mode in Qualcomm SoCs and Device Firmware Update (DFU) mode in Apple devices. EDL mode allows the phone manufacturers to flash software on their devices even if all existing data in the non-volatile memories is corrupt. Therefore the proper handling lets an examiner flash boot loaders into the target smartphone without modifying the user data. Unless any additional authorization mechanism is implemented, modern smartphones with Qualcomm SoCs can be entered into EDL with a command, or a special cable, or hardware modifications.

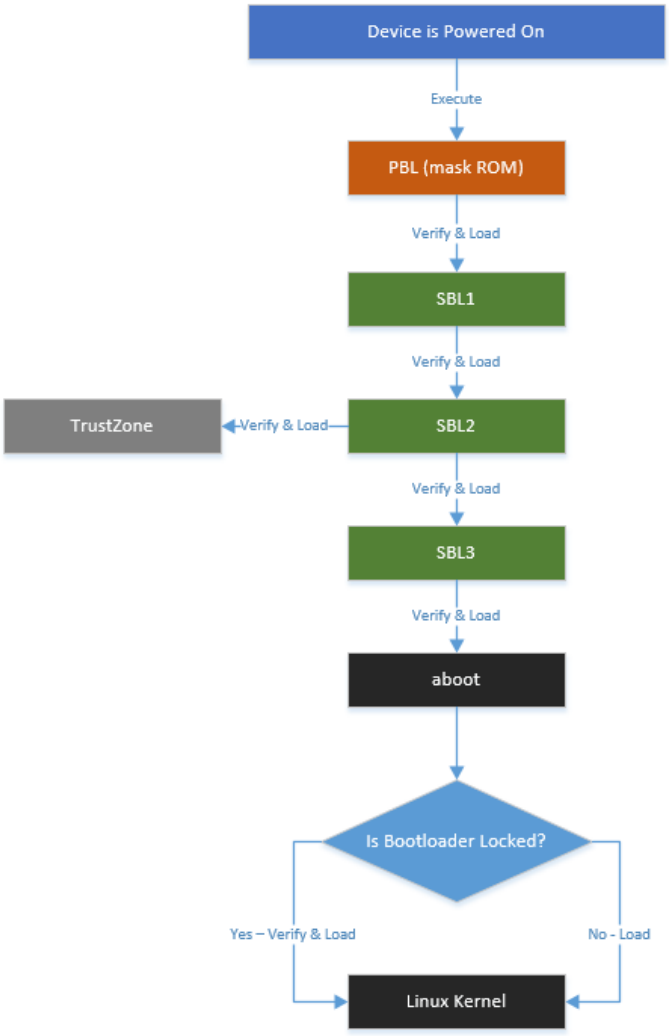

Figure 8: Android booting image (taken from [66])

Moreover, research has revealed that there are critical vulnerabilities in the EDL mode [46]. When exploited, an examiner can bypass the lock and potentially acquire the user data or cryptographic secrets from the target by running arbitrary code. In Apple devices, a well-known exploitation suite called checkm8 [47] can be utilized to control the boot-chain and bypass the security features, then acquire the file system.

4.3.1.2 Downgrading

If allowed by the device manufacturer, one can try to downgrade parts of the boot chain of the target device to a lower version. By downgrading one can exploit known vulnerabilities that are fixed with security updates in the actual version of the boot chain. However, recent smartphones have anti-rollback mechanisms, which are often implemented, with counters that use one-time programmable fuses, preventing users from downgrading the system to older versions [48].

4.3.2 Joint Test Action Group (JTAG)

JTAG is a standard testing and debugging interface implemented in modern processors. Forensic examiners can leverage the JTAG on the target device to manipulate it. Using JTAG, one may communicate with the memory chip through one of the available processors, and acquire the dump image from it [40]. There are a wide-range of software/hardware tools available to leverage

JTAG for data acquisition from modern smartphones. Once an examiner can detect standard JTAG pins, data extraction might be possible using those tools.

In order to get memory access through JTAG, an examiner needs to access the internal circuit board of the target device. Also, the circuit board needs to be working properly for JTAG acquisition to succeed. Modern smartphones can have JTAG authorization mechanisms or one-time programmable fuses that permanently disable JTAG access for non-developer versions of a specific phone model. Therefore, examiners may need to tweak the device in order to utilize those debugging interfaces for hex dumping.

4.4 Chip-off

Similar to Hex Dumping / JTAG, if an examiner can acquire the disk encryption key (for FDE) or can decrypt the files on the system (for FBE), then the physical data acquisition through the techniques described in this section can be effective.

4.4.1 Physical Chip-off

If a forensic lab is properly equipped, examiners can perform physical Chip-off analysis [41]. In physical Chip-off analysis, an examiner needs to physically access the circuit board in the target device. Although the circuit board does not need to be in a working state for an examiner to perform physical chip-off, the target memory chip needs to be undamaged and operative. In order to remove a memory chip from a PCB, either a soldering/rework station or a grinder/polisher machine is required. A soldering/rework station melts the solder that is fixing the memory chip on the PCB. A grinder can grind off the PCB underneath the memory chip and expose its electrodes. Once the memory chip is detached from the PCB, the memory chip can be connected to a memory reader (i.e., NFI Memory Tool Kit [42], UP-2008 [43], etc.) for byte-to-byte copying.

Since physical Chip-off is a destructive procedure, it is important for an examiner to know if the data stored in the memory chip on the target device is encrypted or not prior to performing the procedure. If the data is encrypted, other components on the target device may be required to decrypt the data. This is especially important if chip transplant procedures [44] need to be performed for severely damaged phones.

4.4.2 In-System-Programming (ISP)

While chip-off requires a destructive operation to the target device, if the required device pins for reading the chip are accessible on the PCB without detaching the chip itself, one can try In-System-Programming (ISP) for data extraction. The idea behind ISP is basically the same as chip-off. By connecting a memory reader to electrical traces connected to the memory chip on the PCB, one can access the memory chip and create a byte-for-byte copy. In order to successfully acquire data through ISP, the related part of the circuit board of the target device needs to be non-defective. In addition, an examiner needs to have a proper understanding of signal integrity and other electrical details. By performing ISP, examiners can acquire the same physical data as the data acquired by chip-off *without* damaging the operative state of the target smartphone.

ISP can be performed as long as a memory reader is compatible with the target memory chip technology. Traditionally, eMMCs (embedded Multi-Media Cards) and eMCPs (embedded Multi-Chip Packages) have been widely used in embedded devices. Those memory chips use single-ended signals, therefore simply connecting the traces may let examiners read the memory data. However, new memory technologies like UFS use high speed differential signals. Performing ISP is therefore becoming challenging as making external connection on a PCB can greatly disturb the signal integrity.

In some cases, where no trace is available on the surface of the PCB, partial chip decapsulation with laser ablation may be required to perform ISP. The proper handling can keep the device still operative even after partial decapsulation of the memory chip.

Because ISP and physical Chip-Off/On can directly access non-volatile memory, it can be used for exploitation purposes targeted towards data access and data decryption. Partial data read can contribute to encryption key data extraction, and partial data writing may let the examiner bypass the phone unlocking using user authentication.

4.5 Micro Read

To the best of the authors knowledge, there are no publicly available forensic methods related to Micro Read that can be used to acquire data from modern encrypted smartphones.

4.6 Emerging Techniques

In addition to the forensic techniques described above, research has shown that the following methods can be used to manipulate a wide range of modern devices. While not all the techniques have yet been used by LEAs for forensic data extraction from smartphones, they might be applicable to modern smartphone forensics. Note that some techniques need to be performed in combination with existing forensic methods in order to get access to decrypted user data.

4.6.1 Side-Channel Analysis

Research has shown that when Integrated Circuits (IC) operate on a PCB, these circuits may leak information related to their internal processing. This information can sometimes be used to extract internal secrets like cryptographic keys [49],[50]. Typical sources (side channels) are the direct current flow of a specific processor or the electromagnetic (EM) emanations caused by these current flows. This type of analysis is called side-channel-analysis (SCA), and is widely researched for smart cards and other security demanding hardware. In modern smartphones, SCA could possibly be utilized to retrieve secret keys from SoCs. For properly designed systems these secret keys are needed to find user secrets on distributed systems which can then be used to directly enter the device or derive user data decryption keys for decryption of extracted data.

While SCA is considered as a promising technique for retrieving secret keys from smartphone SoCs, advanced technologies used in modern SoCs are already posing challenges to SCA in mobile forensic analysis. As shown in Section 3.3.3, modern SoCs are operating on a very high clock frequency. Also, the size of modern SoC keeps shrinking. In order to keep up with the advancing SoC technologies, highly sophisticated measuring equipment, along with highly specialized triggering systems, may be required at a digital forensic lab. In addition, other modern technologies, such as shrinking technology size, heterogeneous operation, and voltage frequency optimization, will pose additional challenges against effective use of SCA in mobile forensics. SCA, together with Fault Injection (Section 4.6.2) in smartphone forensics will be explored in Work Package 5.

4.6.2 Fault Injection

Fault Injection (FI) is a technique where inputs of the device are manipulated for the purpose of manipulating the control flow of running software [51]. An example of FI is the fluctuation of the power of a device controller for the purpose of making the controller miss legitimate instructions. By utilizing this ‘glitching', one could make the system skip certain software verification instructions (i.e., secure boot chain), and gain control of the target device. Another application is bypassing JTAG password verification. Technical advance in SoCs, such as implementation of 64-bit architecture (Section 3.3.1), may pose a challenge to the utilization of FI in mobile forensics against modern smartphones.

4.6.3 Firmware Extraction

In modern smartphones, firmware is stored in a protected and/or encrypted state. Extraction of firmware might be possible with micro read techniques for primary boot loader code stored in ROM, or with side channel analysis and fault injection. After acquisition of the device firmware,

examiners can reverse engineer the code and look for possible vulnerabilities that let them run arbitrary code on the target device.

4.6.4 SoC Reverse Engineering

SoC die-level reverse engineering has not been explored much to date in digital forensic community. SoC reverse engineering requires highly specialized lab equipment, together with highly skilled technical examiners with semiconductor knowledge. Through SoC reverse engineering, one can learn how the system is structured by checking internal circuit connections. A semiconductor die consists of multiple layers interconnected with each other. By delayering each layer, and translating the connection into a circuit, one can retrieve the overall design and try by this way to learn and understand how the system works.

The brief procedure of the SoC reverse engineering is as follows. First, the target SoC needs to be carefully prepared for monitoring. The preparation can be done by fine mechanical polishing, and dry and wet etching techniques. Mechanical polishing can be done with milling machines like Allied X-Prep [52] or Ultratec ASAP1-IPS [53]. After milling, the sample can be etched with Reactive Ion Etching (RIE) or with wet chemicals. Once the preparation is done, a highly detailed die-level observation is performed. A Scanning Electron Microscope (SEM) is the widely used system for this purpose. SEM imaging with proper adjustment can give examiners the structural image of the target system.

Using SoC reverse engineering procedures, an examiner may also be able to acquire hardware-bound key information which is stored in one-time-programmable memory area.

The main concern in SoC reverse engineering is the ever-shrinking size of the SoC's manufacturing process technology. The size of process technology used in recent SoC fabrication is less than 10nm, which makes SoC reverse engineering harder than before, requiring highly specialized equipment at a digital forensic lab.

4.6.5 System Vulnerability Exploitation

Multiple vulnerabilities on smartphone components (i.e., Wi-Fi modem, bluetooth SoC, and other software applications) have been reported through security research. Critical vulnerabilities on an unpatched smartphone can allow an attacker to execute arbitrary code on the device, which lets the attacker manipulate the device and access the stored content. Examiners at LEAs may utilize this scenario to access the "live" data on a target smartphone.

4.7 Additional Resources and Future Research

In order to extract meaningful data from secured and encrypted modern smartphones, an examiner needs to either

- Unlock the target device using correct user secrets, or
- Extract the encrypted physical data and decrypt it with the correct encryption key, or
- Bypass the security features and extract the decrypted user data.

Given that LEAs can rarely acquire user secrets, those requirements can only be achieved by

- Brute-forcing the user secret, or
- Extracting the encryption key, or
- Exploiting system vulnerabilities\ to disable or trick the security features.

Since modern smartphones are equipped with mechanisms which prevent attackers from performing those activities, the only way an examiner can access required information is to look for an entry point (system vulnerability), and exploit it to bypass or trick the security mechanisms. While many forensic software vendors develop available tools for modern smartphones, there will always be smartphone models that are not supported because of one of the following reasons:

- The model does not have enough market share to be beneficial for a company to work.
- A recent security patch fixed a vulnerability that was exploited by the forensic extraction method.
- The model is only sold with high subscription fees to a selected group of (criminal) people. (Hence no access available for vendors)

For these reasons, LEAs need to come up with a better plan, and try to identify techniques that work on smartphones which are not expected to be supported by existing forensic tool developers. Future research needs to focus on vulnerabilities at the SoC level, as the SoC may be the only component an examiner can access in a locked smartphone. As we studied in Section 3.3, the smartphone SoC market is dominated by 4 manufacturers. By investigating those SoCs and identifying their vulnerabilities, entry points might be identified that can enable forensic acquisition of data. The research by [46] is a good example that shows the effectiveness of SoC level research. Some example devices that are available for forensic technique evaluation can be found in Table 9 in the Appendix.

Chapter 5 Forensic Soundness and Legal Concerns

Forensic soundness is a term used in the digital forensics community to qualify and justify the use of a particular forensic technology or methodology. Mobile forensics has always been a discipline where maintaining forensic soundness is complicated by complex and constantly evolving technology trends. Key challenges include: (1) mobile phones are switched on permanently and connected to external communication networks; (2) methods for making a passive byte-by-byte copy of all data on a device are virtually non-existent (which is a significant difference from traditional hard-disk forensics); and (3) current mobile forensic methods mostly focus on finding system vulnerabilities by reverse engineering software, SoC, and other hardware levels. In this chapter, we introduce forensic soundness and legal concerns related to current extraction techniques. Extensive coverage of these topics is included in Work Package 2 (WP2) on Legal, Ethical and Societal Issues.

5.1 Forensic Soundness

Traditional digital forensic methods need to comply with forensic soundness as defined in quality documents of ACPO [55], ENFSI [56], and SWGDE [57]. Requirements from these documents that are particularly challenging for current and future mobile forensic techniques are:

- “examiners need to have deep understandings of technologies used when performing forensic extraction.”

  Forensic examiners operating forensic products do not necessarily know what technologies are used for the extraction. Even the tool vendors might not fully understand possible side effects of exploits they use.

- “No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.”

  This is especially challenging when manual or logical extraction is performed on a working mobile device, since its data is continuously changing on the file system level. An example of an action taken to minimize the data change is re-mounting the user data partition in read-only mode as the first step of the extraction procedure.

- “In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. “

  Recent techniques working on devices in AFU or using semi-live methods to extract data with methods that exploit security vulnerabilities raise the demands for examiners to be competent to explain the inner workings and forensic implications.

5.2 Legal Issues

The international legal framework for law enforcement has little focus on evidence. The rules regarding criminal proceedings vary considerably from State to State, "*even amongst countries with similar legal traditions* [58]" as stated by the United Nations Office on Drugs and Crime in its 2013 *Comprehensive Study on Cybercrime.* Moreover, while some states apply traditional laws on electronic evidence, others adapted their legislation regarding evidence to integrate specific rules for digital forensics investigations. Although the situation has evolved considerably since 2013, there is still no overall international legal framework regarding electronic evidence. However, certain international conventions apply to this field, reinforced and clarified by guidelines and technical standards, and cooperation mechanisms have been developed, in particular by the Council of Europe. Extensive coverage of these topics is part of Work Package 2 on Legal, Ethical and Societal Issues. The main sources of concern as seen by forensic examiners working on mobile forensic area are briefly introduced below.

5.2.1 Network Based Data Acquisition

Current smartphones store data not only on the physical device, but also on cloud servers provided by manufacturers or OS vendors. Examples are iOS based devices which store user and application data bound to iCloud accounts on Apple servers, and Android devices for which user related data is bound to a Google account and stored on their servers. Besides these OS based storage solutions, individual app providers can also store app related data (even cryptographic keys) on servers of their own in such a way that access to data stored on a device is only possible after connection with a server. Another application where data from a secondary source can be useful is mobile device management (MDM) software. MDM is used by companies, and also in the smartphones used by criminal groups in order to limit and control user access. Most MDM services, however, have a kind of escrow facility that could be used to get access to device data.

The data stored on the cloud server or the required credentials can sometimes be obtained from the network or application providers using the appropriate legal process (i.e., subpoenas or court orders). Some digital forensic tools provide data acquisition functionality from cloud servers over the Internet [59], [60]. These tools also offer functionality to get the data directly from the data providers by using credential data acquired from the physical device. While this procedure allows examiners to perform effective data acquisition, it may raise legal issues, which are different in each country.

From a legal point of view, cross-border acquisition raises its own issues. EU legislation partially provides a framework for the lawful processing of such data. Relevant legal instruments such as the Budapest Convention, the NIS Directive, the LED Directive (and others) will be discussed in more details in WP2, in order to find the most relevant approach for cross-border cases. However, some legal issues are related to differences in data retention periods, certifications and unlawful processing of personal data. All these issues may also apply to back-ups of smartphone information stored in cloud services.

5.2.2 Responsible Disclosure and Government Zero-day Policies

A zero-day vulnerability is a software vulnerability that is either unknown to the developer, or un-addressed by those who should have an interest in mitigating the vulnerability (including the vendor of the target software). Some countries are implementing responsible disclosure policies where manufacturers are notified of discovered flaws in order to fix them. LEA's would like to use these zero-days as long as possible, but this might conflict with general safety.

Additional issues related to responsible disclosure and forensics include:

- If responsible disclosure policies are different in each country, it will have a negative impact on collaborative work and sharing of methods. This is also the case for specific responsible disclosure policies of companies.

- Forensic tool manufacturers will try to protect their zero-days as much as possible, which increases costs and makes it harder for forensic examiners to comply with forensic soundness criteria.

5.2.3 Scope of Data Analysis

The scope of a mandate may vary, since it may be difficult for authorities to know in precise terms what is adequate in accordance with the principle of data minimisation and environmental difficulties. The Law Enforcement Directive establishes clear principles for the processing of personal data in line with the General Data Protection Regulation (GDPR). Nevertheless, the extraction of information from encrypted devices is useless as long as the encryption issue is not bypassed. Irrelevant personal data and third party data must be treated differently. WP2 will focus in part on the harmonisation of procedures to address these issues in greater depth.

5.3 Cooperation with Smartphone Vendors

LEAs often struggle to get assistance from smartphone manufacturers when it comes to forensic data extraction. In the FBI-Apple encryption dispute [61], the FBI asked Apple “to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation.” Apple rejected this with the arguments that “In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone’s physical possession”. Technically, it ought to be possible for a phone manufacturer to make a specific software version that only works on a specific phone in a given criminal case, and only after approval by a court of law. In addition to requests for individual software changes, LEAs would greatly benefit from easy access to smartphone-related product documentation (i.e., SoCs, memory chips, PCB layout, schematics), which allow lawful forensic acquisition in criminal investigations.

Chapter 6 Summary and Conclusion

The growing importance of data on seized smartphones in criminal investigations is accelerating the need for advanced mobile forensics research by LEAs. As smartphones become essential tools in peoples' daily lives, and security and privacy concerns are growing, modern smartphone vendors are implementing multiple types of security protection measures - like encryption - to guard against unauthorized access to the data on their products. Data encryption on modern smartphones, together with complicated secure booting sequences, is negatively impacting the ability of mobile forensic analysis at LEAs, thereby degrading the effectiveness of criminal investigations. Through this report, we have discussed how the dynamics of mobile forensics have changed over the last decade due to new security features on modern smartphones. Traditionally developed mobile forensic techniques are no longer effective to the same degree. Without proper user authentication, traditional forensic acquisition almost always fails on modern smartphones.

Today, mobile forensic research focuses on identifying more invasive techniques, such as bypassing the security features, and extracting the key material through privilege escalation by exploiting vulnerabilities. While many smartphone forensic tools use software exploits in their product, those exploits are rarely publicly available. As a result, forensic tools are becoming black boxes, or exclusive services provided at the vendor's premises. On the other hand, forensic tool vendors are trying to keep up with smartphone market trends, and tools are, or will be, eventually available for those devices dominating the smartphones market.

A problem for LEAs is that criminal groups are also taking advantage of smartphone security features and are using secured phones for their communications. Unfortunately, the market share of those criminal-used smartphones is not large enough to attract smartphone forensic tool vendors. Therefore, LEAs themselves need to identify effective forensic solutions against those smartphone models being used by criminals. Throughout this report, we have shown that the mobile forensics study needs to focus on vulnerabilities at SoC level. When pursuing SoC level vulnerability research, however, LEAs need to be aware of legal regulations. Proper understanding of the legal and regulatory landscape, including rules on responsible disclosure of zero-days and network data acquisition, together with critical research, will lead to effective forensic data extraction from modern smartphones and help LEAs fight crimes.

Chapter 7 List of Abbreviations

Abbreviation	Translation
AFU	After First Unlock
AOSP	Android Open Source Project
API	Application Programming Interfaces
BFU	Before First Unlock
DFU	Device Firmware Update
EDL	Emergency Download Mode
FI	Fault Injection
FIB	Focused Ion Beam
FBE	File Based Encryption
FDE	Full Disk Encryption
IC	Integrated Circuit
ISP	In System Programming
HSM	Hardware Secure Module
JTAG	Joint Test Action Group
LEA	Law Enforcement Agency
OS	Operating System
PCB	Printed Circuit Board
PBL	Primary Boot Loader
RISC	Reduces Instruction Set Computing
RoT	Root of Trust
SBL	Secondary Boot Loader
SCA	Side Channel Analysis
SE	Secure Element
SEM	Scanning Electron Microscope

Abbreviation	Translation
SEP	Secure Enclave Processor
SoC	System on a Chip
TEE	Trusted Execution Environment

Chapter 8 Bibliography

[1] U.S. Commerce Department, National Institute of Standards and Technology (NIST) Special Publication 800-101 Revision 1, “Guidelines on Mobile Forensics” (May 2014)

[2] "Android operating system share worldwide by OS version from 2013 to 2020," Statista, April 2020. [Online]. Available: https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/. [Accessed 7 August 2020].

[3] Tam, Kimberly, et al. "The evolution of android malware and android analysis techniques". ACM Computing Surveys (CSUR) 49.4 (2017): 1-41.

[4] “Mobile Operating System Market Share Worldwide” GlobalStats, [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide. [Accessed 27 August 2020].

[5] “Mobile operating systems' market share worldwide from January 2012 to July 2020”. Statista, [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/. [Accessed 27 August 2020].

[6] "Apple has the world’s two top-selling phones, but how well is iPhone 8 selling?," Digital trends, 10 November 2017. [Online]. Available: https://www.digitaltrends.com/mobile/iphone-8-iphone-7-sales-apple/. [Accessed 3 August 2020].

[7] J. Callaham, "Samsung Galaxy S3: Years later, its iPhone-bashing commercial still works," Android Authority, 29 May 2019. [Online]. Available: https://www.androidauthority.com/samsung-galaxy-s3-anniversary-991555/. [Accessed 3 August 2020].

[8] S. Chris, "Galaxy S9 sales are better than the Galaxy S8, but that’s not saying much," BGR, 25 August 2018. [Online]. Available: https://bgr.com/2018/04/25/galaxy-s9-sales-are-better-than-the-galaxy-s8-but-thats-not-saying-much/. [Accessed 3 Augus 2020].

[9] "Galaxy S10 outsells predecessor but analysts don’t consider it a success," Sammobile, [Online]. Available: https://www.sammobile.com/news/galaxy-s10-outsells-predecessor-analysts-dont-consider-success/. [Accessed 3 August 2020].

[10] C. Miller, "iPhone XR was the world’s best-selling smartphone in 2019, new data suggests," 9 to 5 mac, 25 February 2020. [Online]. Available: https://9to5mac.com/2020/02/25/iphone-xr-2019-best-seller/. [Accessed 4 August 2020].

[11] T. Segal, "What's the Best-Selling iPhone Model of All Time?," Investopedia, 26 June 2019. [Online]. Available: https://www.investopedia.com/ask/answers/021315/whats-bestselling-iphone-model-all-time.asp. [Accessed 3 August 2020].

[12] "The 20 bestselling mobile phones of all time," The Telegraph, 6 August 2017. [Online]. Available: https://www.telegraph.co.uk/technology/2016/01/26/the-20-bestselling-mobile-phones-of-all-time/. [Accessed 3 August 2020].

[13] L. Tyler, "63 Million iPhone X Handsets Have Been Sold To Date," Ubergizmo, 9 December 2018. [Online]. Available: https://www.ubergizmo.com/2018/09/63-million-iphone-x-handsets-sold-to-date/. [Accessed 5 August 2020].

[14] "iPhone sales decline for a third consecutive quarter, XR is the best-seller," GSM arena, 10 September 2019. [Online]. Available: https://www.gsmarena.com/iphone_sales_decline_for_a_third_consecutive_quarter_xr_is_the_bestseller-news-39114.php. [Accessed 3 August 2020].

[15] “Global Smartphone Market Share: By Quarter” Counterpoint, [Online]. Available: https://www.counterpointresearch.com/global-smartphone-share/. [Accessed 27 August 2020].

[16] "Apple iPhone 11 specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/apple_iphone_11-9848.php. [Accessed 7 August 2020].

[17] "Apple iPhone XR specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/apple_iphone_xr-9320.php. [Accessed 7 August 2020].

[18] "Apple iPhone XS specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/apple_iphone_xs-9318.php. [Accessed 6 August 2020].

[19] "Apple iPhone XS Max specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/apple_iphone_xs_max-9319.php. [Accessed 5 August 2020].

[20] "Inside iPhone 8: Apple's A11 Bionic introduces 5 new custom silicon engines," Apple insider, 2018. [Online]. Available: https://appleinsider.com/articles/17/09/23/inside-iphone-8-apples-a11-bionic-introduces-5-new-custom-silicon-engines. [Accessed 31 July 2020].

[21] "Kirin 980," Huawei, [Online]. Available: https://consumer.huawei.com/en/campaign/kirin980/. [Accessed 7 August 2020].

[22] "HUAWEI Mate 20 Pro," Huawei, [Online]. Available: https://consumer.huawei.com/en/phones/mate20-pro/. [Accessed 31 July 2020].

[23] "HUAWEI Mate 20 lite," Huawei, [Online]. Available: https://consumer.huawei.com/en/phones/mate20-lite/specs/. [Accessed 30 July 2020].

[24] "Samsung Galaxy A10 specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/samsung_galaxy_a10-9580.php. [Accessed 30 July 2020].

[25] "Galaxy A20 specifications," Samsung, [Online]. Available: https://www.samsung.com/levant/smartphones/galaxy-a-series/a20/. [Accessed 3 August 2020].

[26] "Exynos 9610 processor specifications," Samsung, [Online]. Available: https://www.samsung.com/semiconductor/minisite/exynos/products/mobileprocessor/exynos-7-series-9610/. [Accessed 29 July 2020].

[27] "Samsung Galaxy S10 specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/samsung_galaxy_s10-9536.php. [Accessed 30 July 2020].

[28] "Samsung Galaxy S9 specifications," GSM arena, [Online]. Available: https://www.gsmarena.com/samsung_galaxy_s9-8966.php. [Accessed 4 August 2020].

[29] "Samsung Galaxy J2 Core specifications," [Online]. Available: https://www.gsmarena.com/samsung_galaxy_j2_core-9255.php. [Accessed 5 August 2020].

[30] "Samsung Galaxy S8," GSM arena, [Online]. Available: https://www.gsmarena.com/samsung_galaxy_s8-8161.php. [Accessed 7 August 2020].

[31] "Encryption," Google, [Online]. Available: https://source.android.com/security/encryption. [Accessed 7 August 2020].

[32] Apple, "iOS Security (iOS 12.3)," May 2019. [Online]. Available: https://www.apple.com/tr/business/docs/site/iOS_Security_Guide.pdf. [Accessed 31 July 2020].

[33] “Global market revenue share of leading smartphone application processor (AP) vendors from 2014 to 2019”. Statista, [Online]. Available: https://www.statista.com/statistics/233415/global-market-share-of-applications-processor-suppliers/. [Accessed 10 August 2020].

[34] “Apple Platform Security”. Apple Inc, [Online]. Available: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf [Accessed 10 August 2020].

[35] “Building a Titan: Better security through a tiny chip”, N. Modadugu and B. Richardson, [Online]. Available: https://android-developers.googleblog.com/2018/10/building-titan-better-security-through.html.[Accessed 08 september 2020]

[36] “XRY Photon”, MSAB, [Online]. Available: https://www.msab.com/products/xry/xry-photon/. [Accessed 08 september 2020]

[37] “Cellebrite SEEKER”, Cellebrite [Online]. Available: https://www.cellebrite.com/en/seeker/. [Accessed 08 September 2020]

[38] N. Scrivens and X. Lin, “Android digital forensics: data, extraction and analysis,” Proc. of the ACM Turing 50th Celebration Conference - China

[39] “Extracting Qualcomm's KeyMaster Keys - Breaking Android Full Disk Encryption,” [Online]. Available: https://bits-please.blogspot.com/2016/06/extracting-qualcomms-keymaster-keys.html

[40] Ing.M.F. Breeuwsma “Forensic Imaging of Embedded Systems Using JTAG (Boundary-Scan),” Digital Investigation, vol 3, Issue 1, pp.32-42, 2006

[41] M. Breeuwsma et al., “Forensic Data Recovery from Flash Memory,” Small Scale Digital Device Forensics Journal (2007)

[42] “NFI Memory Toolkit,” Netherlands Forensic Institute, [Online]. Available: https://www.forensicinstitute.nl/products-and-services/forensic-products/nfi-memory-toolkit [Accessed 01 September 2020]

[43] “UP-828P Programmer,” Teel Technologies, [Online]. Available: https://teeltech.com/mobile-device-forensic-hardware/up-828-programmer/. [Accessed 01 September 2020]

[44] T. Heckmann et al., “Forensic smartphone analysis using adhesives: Transplantation of Package on Package components,” Digital Investigation, 26 (2018), pp. 29-39,

[45] “Reverse Engineering Android’s Aboot”, J. Levin, [Online]. Available: http://newandroidbook.com/Articles/aboot.html [Accessed 08 September 2020]

[46] “Exploiting Qualcomm EDL Programmers (1): Gaining Access & PBL Internals,” R. Hay and N. Hadad, Jan. 2018. [Online]. Available: https://alephsecurity.com/2018/01/22/qualcomm-edl-1/ [Accessed 7 September 2020]

[47] “A Practical Guide to Checkm8”, R. Arato, Jan. 2020. [Online]. Available: https://www.cellebrite.com/en/topics/investigative-techniques/a-practical-guide-to-checkm8/

[48] “Secure Boot and Image Authentication”, A.W. Dent, Aug. 2019, [Online]. Available: https://www.qualcomm.com/media/documents/files/secure-boot-and-image-authentication-technical-overview-v2-0.pdf

[49] Kocher P., Jaffe J., Jun B. (1999) “Differential Power Analysis.” In: Wiener M. (eds) Advances in Cryptology — CRYPTO’ 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48405-1_25

[50] A. Vasselle et al., “Breaking Mobile Firmware Encryption through Near-Field Side-Channel Analysis” Proc. of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop (2019) doi.org/10.1145/338508.3359571

[51] “Master the art of Fault Injection,” Riscure, [Online]. Available: https://www.riscure.com/fi/

[52] “X-Prep® Precision Milling/Polishing System,” Allied High tech products. Inc., [Online]. Available: https://www.alliedhightech.com/Equipment/x-prep-mechanical-mill

[53] “ASAP-1® IPS,” Ultra Tec Manufacturing, inc., [Online]. Available: https://www.ultratecusa.com/product/asap-1-ips/

[54] K. Jonkers, The forensic use of mobile phone flasher boxes, Digital Investigation, Volume 6, Issues 3–4,2010, Pages 168-178, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2010.01.006.

[55] ACPO Good Practice Guide for Digital Evidence, https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[56] “Best Practice Manual for the Forensic Examination of Digital Technology,” ENFSI, [Online]. Available: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

[57] “SWGDE Best Practices for Mobile Phone Forensics,” Scientific Working Group on Digital Evidence, [Online] Available: https://www.irisinvestigations.com/wp-content/uploads/2019/05/SWGDE-Best-Practices-for-Mobile-Phone-Forensics-021113.pdf

[58] “Comprehensive Study on Cybercrime,” United Nations Office on Drugs and Crime, Feb 2013, p. 158

[59] Cellebrite UFED CLOUD, Unlock cloud-based evidence to solve the case sooner, https://www.cellebrite.com/en/ufed-cloud/

[60] MSAB XRY Cloud, Recovery of data beyond the mobile device, https://www.msab.com/products/xry/xry-cloud/

[61] “Inside Apple CEO Tim Cook’s Fight With the FBI,” Time, [Online]. Available: https://time.com/4262480/tim-cook-apple-fbi-2/ [Accessed 17 September 2020]

[62] “Apple Confirms iOS Security Feature to Block Devices Like GrayKey,” The Mac Observer, [Online] https://www.macobserver.com/news/apple-confirms-ios-feature/

[63] “Demystifying Android Physical Acquisition,” Elcomsoft, [Online]. Available: https://blog.elcomsoft.com/2018/05/demystifying-android-physical-acquisition/

[64] “A Message to Our Customers,” Apple, [Online]. Available: https://www.apple.com/customer-letter/ [Accessed 18 September 2020]

[65] ”UFED 4PC, UFED Touch 2 & UFED Infield Version 7.16,” cellebrite, [Online]. Available: https://cf-media.cellebrite.com/wp-content/uploads/2019/03/ReleaseNotes_UFED_7.16-web.pdf

[66] “Unlocking the Motorola Bootloader,” [Online]. Available: https://bits-please.blogspot.com/2016/02/unlocking-motorola-bootloader.html [Accessed 1 September 2020]

Appendix

Most Sold Mobile Devices

Table 3: 30 most sold devices within the last 10 years (as of August 6, 2020)

Ranking by sales volume	Manufacturer	Model	Year	Million units sold
1	Apple	iPhone 6 and iPhone 6 Plus	2014	222.4
2	Apple	iPhone 8 and iPhone 8 Plus	2017	86.3
3	Samsung	Galaxy S4	2013	80
4	Apple	iPhone 7 and iPhone 7 Plus	2016	78.3
5	Apple	iPhone 5	2012	70
6	Apple	iPhone XR	2018	69.4
7	Apple	iPhone X	2017	63
8	Apple	iPhone 4s	2011	60
9	Samsung	Galaxy S III	2012	60
10	Samsung	Galaxy S7 and Galaxy S7 edge	2016	55
11	Apple	iPhone 5s	2013	52
12	Apple	iPhone 4	2010	50
13	Apple	iPhone Xs and iPhone Xs Max	2018	48
14	Samsung	Galaxy S8 and Galaxy S8+	2017	41
15	Samsung	Galaxy S II	2011	40
16	Apple	iPhone 11	2019	37.3
17	Samsung	Galaxy S9 and Galaxy S9+	2018	35.4
18	Apple	iPhone 11 Pro and iPhone 11 Pro Max	2019	33.1
19	Samsung	Galaxy A10	2019	30.3
20	Samsung	Galaxy Note II	2012	30
21	Samsung	Galaxy S	2010	25
22	Samsung	Galaxy A50	2019	24.2
23	Samsung	Galaxy A20	2019	23.1
24	Xiaomi	Redmi Note 7 and Redmi Note 7 Pro	2019	20
25	Huawei	P30 and P30 Pro	2019	20
26	Huawei	Mate 20 and Mate 20 Pro	2018	17
27	HTC	Thunderbolt	2011	16
28	Huawei	P20 Lite	2018	16
29	Samsung	Galaxy S10, Galaxy S10+ and Galaxy S10e	2019	16
30	Samsung	Galaxy J2 Core	2018	15.2

Most Recent Mobile Devices by Vendor

Table 4: Most sold devices from Apple within the last 3 years

Model	Year	Million units sold
iPhone 11	2019	37.3
iPhone 11 Pro and iPhone 11 Pro Max	2019	33.1
iPhone XR	2018	69.4
iPhone Xs and iPhone Xs Max	2018	48
iPhone 8 and iPhone 8 Plus	2017	86.3
iPhone X	2017	63

Table 5: Most devices from Huawei within the last 3 years

Model	Year	Million units sold
P30 and P30 Pro	2019	20
Mate 20 and Mate 20 Pro	2018	17
P20 Lite	2018	16

Table 6: Most devices from Samsung within the last 3 years

Model	Year	Million units sold
Galaxy A10	2019	30.3
Galaxy A50	2019	24.2
Galaxy A20	2019	23.1
Galaxy S10, Galaxy S10+ and Galaxy S10e	2019	16
Galaxy S9 and Galaxy S9+	2018	35.4
Galaxy J2 Core	2018	15.2
Galaxy S8 and Galaxy S8+	2017	41

Table 7: Most devices from Xiaomi within the last 3 years

Model	Year	Million units sold
Redmi Note 7 and Redmi Note 7 Pro	2019	20

List of Smartphone Operating Systems

Table 8: Mobile Phone Operating Systems

OS Name	Developer	Based on	Miscellaneous
Sirin OS	Sirin Labs	Android	
AliOS	Alibaba	Android	
CopperheadOS	Coppperhead Limited	Android	
GrapheneOS	independents	Android	
Funtouch OS	Vivo	Android	
Replicant OS	independents	Android	
KATIM OS	DarkMatter Group	Android	
Silent OS	Silent Circle	Android	
BlackBerry Secure	BlackBerry	AOSP	
LineageOS	the LineageOS open-source community	AOSP	
Indus OS	independents	AOSP	
ColorOS	Oppo	AOSP	
EMUI	Huawei	AOSP	
FLYme	Meizu	AOSP	
MIUMI	Xiaomi	AOSP	
OxygenOS	OnePlus	AOSP	
Sailfish OS	Jolla	Linux	
PureOS	Purism	Linux	
Ubuntu Touch	Canonical	Linux	
postmarketOS	the postmarketOS open-source community	Linux	
CyanogenMod	the CyanogenMod community		Discontinued
Cyanogen OS	Cyanogen		Discontinued
Firefox OS	Mozilla		Discontinued
MeeGoo	The Linux Foundation		Discontinued
webOS	Palm		Discontinued
BlackBerry OS	Research In Motion		Discontinued
Symbian OS	Nokia		Discontinued
Bada	Samsung Electronics		Discontinued
Windows Mobile	Microsoft		Discontinued
Windows Phone	Microsoft		Discontinued
Windows 10 Mobile	Microsoft		Discontinued

Specification of Recent Mobile Devices

Table 9: Specification of recent mobile devices

Smartphone	Manufacturer	Release date	OS (at release time)	Processor	Processor manufacturer
Pixel 2	Google	Oct'17	Android 8	Snapdragon 835	Qualcomm
Pixel 2 XL	Google	Oct'17	Android 8	Snapdragon 835	Qualcomm
Pixel 3	Google	Oct'18	Android 9	Snapdragon 845	Qualcomm
Pixel 3 XL	Google	Oct'18	Android 9	Snapdragon 845	Qualcomm
Pixel 3a	Google	Oct'19	Android 9	Snapdragon 670	Qualcomm
Pixel 3a XL	Google	Oct'19	Android 9	Snapdragon 670	Qualcomm
Pixel 4	Google	Oct'19	Android 10	Snapdragon 855	Qualcomm
Pixel 4 XL	Google	Oct'19	Android 10	Snapdragon 855	Qualcomm
Nexus 5X	LG	Oct'15	Android 6	Snapdragon 808	Qualcomm
P30	Huawei	Mar'19	Android 9	Kirin 980	HiSillicon
P30 Pro	Huawei	Mar'19	Android 9	Kirin 980	HiSillicon
Nexus 6P	Huawei	Sep'15	Android 8	Snapdragon 810	Qualcomm
Nexus 6	Motorola	Nov'14	Android 5	Snapdragon 805	Qualcomm
Nexus 9	Google	Nov'14	Android 5	Denver	Nvidia
Galaxy S20	Samsung	Mar'20	Android 10	Exynos 990 (global)	Samsung
				Snapdragon 865 (USA)	Qualcomm
Galaxy S20 +	Samsung	Mar'20	Android 10	Exynos 990 (global)	Samsung
				Snapdragon 865 (USA)	Qualcomm
Galaxy S20 Ultra	Samsung	Mar'20	Android 10	Exynos 990 (global)	Samsung
				Snapdragon 865 (USA)	Qualcomm
Galaxy A10	Samsung	Mar'19	Android 9	Exynos 7884	Samsung
Galaxy A50	Samsung	Mar'18	Android 9	Exynos 9610	Samsung
Galaxy A20	Samsung	Apr'19	Android 9	Exynos 7884	Samsung
Galaxy S10	Samsung	Mar'19	Android 9	Exynos 9820 (EMEA/LATAM)	Samsung
				Snapdragon 855 (USA/China)	Qualcomm
Galaxy S10+	Samsung	Mar'19	Android 9	Exynos 9820 (EMEA/LATAM)	Samsung
				Snapdragon 855 (USA/China)	Qualcomm
Galaxy S10e	Samsung	Mar'19	Android 9	Exynos 9820 (EMEA/LATAM)	Samsung
				Snapdragon 855 (USA/China)	Qualcomm
Galaxy S9	Samsung	Mar'18	Android 8	Exynos 9810 (EMEA)	Samsung
				Snapdragon 845 (USA/LATAM/China)	Qualcomm

Smartphone	Manufacturer	Release date	OS (at release time)	Processor	Processor manufacturer
Galaxy S9+	Samsung	Mar'18	Android 8	Exynos 9810 (EMEA)	Samsung
				Snapdragon 845 (USA/LATAM/China)	Qualcomm
Galaxy S8	Samsung	Apr'17	Android 7	Exynos 8895 (EMEA)	Samsung
				Snapdragon 835 (USA/China)	Qualcomm
Galaxy S8+	Samsung	Apr'17	Android 7	Exynos 8895 (EMEA)	Samsung
				Snapdragon 835 (USA/China)	Qualcomm
Galaxy J2 Core	Samsung	Aug'18	Android 8.1	Exynos 7570	Samsung
iPhone 11	Apple	Sep'19	iOS 13	A13 Bionic	Apple
iPhone 11 Pro	Apple	Sep'19	iOS 13	A13 Bionic	Apple
iPhone 11 Pro Max	Apple	Sep'19	iOS 13	A13 Bionic	Apple
iPhone SE	Apple	Mar'16	iOS 9	A9	Apple
iPhone XR	Apple	Oct'18	iOS 12	A12 Bionic	Apple
iPhone XS	Apple	Sep'18	iOS 12	A12 Bionic	Apple
iPhone XS Max	Apple	Sep'18	iOS 12	A12 Bionic	Apple
iPhone 8	Apple	Sep'17	iOS 11	A11 Bionic	Apple
iPhone 8 Plus	Apple	Sep'17	iOS 11	A11 Bionic	Apple
iPhone X	Apple	Nov'17	iOS 11	A11 Bionic	Apple
Mate 20	Huawei	Nov'18	Android 9	Kirin 980	HiSillicon
Mate 20 Pro	Huawei	Oct'18	Android 9	Kirin 980	HiSillicon
P20 Lite	Huawei	Mar'18	Android 8	Kirin 659	HiSillicon
Redmi Note 7	Xiaomi	Feb'19	Android 9	Snapdragon 660	Qualcomm
Finney	Sirin	May'18	Sirin OS	Snapdragon 845	Qualcomm
Exodus 1	HTC	Oct'18	Andoid 8	Snapdragon 845	Qualcomm
Exodus 1 Binance	HTC	Dec'19	Andoid 8	Snapdragon 845	Qualcomm
Exodus 1s	HTC	Oct'19	Andoid 8	Snapdragon 435	Qualcomm
Tough Mobile 2	Bittium		Android 9	Snapdragon 670	Qualcomm
Tough Mobile 2C	Bittium		Android 9		Qualcomm
KATIM R01	DarkMatter Group	2019	KATIM OS	Snapdragon 845	Qualcomm
Blackphone 2	Silent Circle	Mar'15	Silent OS	Snapdragon 615	Qualcomm
Boeing Black	Boeing & BlackBerry	Feb'17	Android	ARM Cortex-A9	
Turing Phone	Turing Space Industries	Apr'16	Sailfish OS	Snapdragon 801	Qualcomm

Smartphone	Manufacturer	Release date	OS (at release time)	Processor	Processor manufacturer
UnaPhone Zenith	Una Inc Ltd	Apr'16	UnaOS		

List of Devices Available for Forensic Technique Evaluation

Devices listed in Table 10 can be used for validating forensic techniques, since their vulnerabilities and/or system details are publicly available.

Table 10: Devices available for forensic technique evaluation

Device Name	SoC Name (Equivalent)	Type	Manufacturer
Nexus 6	Snapdragon 805	Smartphone	Motorola/Google
Open-Q 660	Snapdragon 660	Development board	Intrinsyc
Open-Q 835	Snapdragon 835	Development board	Intrinsyc
Snapdragon 660 Mobile Hardware Development Kit	Snapdragon 660	Development board	Qualcomm
Snapdragon 835 Mobile Hardware Development Kit	Snapdragon 835	Development board	Qualcomm
Snapdragon 845 Mobile Hardware Development Kit	Snapdragon 845	Development board	Qualcomm
Snapdragon 855 Mobile Hardware Development Kit	Snapdragon 855	Development board	Qualcomm
Snapdragon 865 Mobile Hardware Development Kit	Snapdragon 865	Development board	Qualcomm
DragonBoard 410c Development Board	Snapdragon 410E	Development board	Qualcomm
BQ-X2	Qualcomm sdm660	Mobile phone	BQ
MediaTek X20	Helio X20	Development board	
DragonBoard™ 810	Snapdragon 810	Development board	Intrinsyc
Howchip ExSOM-8895	Exynos 8895	Development board	Howchip
Developer Transition Kit (2020)	Apple A12Z	Development board	Apple
Security Research Device		Mobile phone	Apple

Device Name	SoC Name (Equivalent)	Type	Manufacturer
MCIMX8M-EVK	i.MX 8M	Development board	NXP
HiKey 960	Kirin 620	Development board	96Boards