International Journal of
Research in
Circuits, Devices and Systems

E-ISSN: 2708-454X
P-ISSN: 2708-4531
IJRCDS 2022; 3(1): 55-64
© 2022 IJRCDS
www.circuitsjournal.com
Received: 07-11-2021
Accepted: 18-12-2021

Brij Mohan Goel
Professor, Department of Computer Science and Application, Baba Mastnath University, Rohtak, Haryana, India

Shefali Saini
Research Scholar, Department of Computer Science and Application, Baba Mastnath University, Rohtak, Haryana, India

Corresponding Author:
Shefali Saini
Research Scholar, Department of Computer Science and Application, Baba Mastnath University, Rohtak, Haryana, India

Extract data from encrypted mobile devices

Brij Mohan Goel and Shefali Saini

Abstract
In modern criminal investigations, mobile devices are seized at all kinds of crime scenes, and data from these devices often become important evidence in a case. Several mobile forensic technologies have been created and evaluated through research to extract potential evidence data from devices for decades. However, as mobile devices have become essential tools for everyday life, security and privacy concerns have increased, and modern smartphone vendors have implemented various types of security protection measures, such as encryption, to guard against unauthorized access to your product data. This trend is making obtaining forensic evidence more difficult than ever, and extracting data from those devices for criminal investigation is becoming more and more difficult. Today, mobile forensics focus on identifying the most prevalent technologies, such as bypassing security features and hacking targeted smartphones by exploiting their weaknesses. In this paper, we explain the increased protection and security measures on modern mobile devices and their impact on traditional forensic data mining techniques for law enforcement purposes. To overcome challenges, new forensic methods rely on bypassing security features and exploiting system weaknesses. A new model for forensic acquisition has been proposed. The model is based on a legal framework that focuses on the usability of digital evidence obtained by exploiting vulnerabilities.

Keywords: Data, encrypted, devices, mobile, crime

1. Introduction

Mobile devices often contain data relevant to criminal investigations, and forensic analysis of these devices has become a critical investigative ability for law enforcement agencies. In recent decades, many forensic researchers have established methods and processes for extracting evidence data from mobile devices in a forensically sound manner (Barmpatsalou *et al.* 2013; Al-Dhaqm *et al.* 2020; Reedy, 2020) [5, 2, 40]. These methods have been widely used in real-world forensics and have addressed general challenges in mobile forensics, such as the lack of standardization within the mobile industry and the rapid rate at which mobile technology is changing. On the other hand, however, recently new challenges have emerged with the powerful security features of modern mobile devices (Chernyshev *et al.* 2017) [10]. Clearly, encryption, along with other security guard features, has created challenges for forensic investigators looking to extract data from mobile devices seized at crime scenes. These security features have disrupted many data acquisition methods that were historically in use, and new methods of getting data from modern mobile devices must be explored.

The challenges posed by encryption were publicly highlighted during the 2015 dispute between Apple and the FBI in the wake of the widely reported terrorist attack in San Bernardino, California. Not only has this case sparked an intense legal debate about cryptographic regulation and government access to encrypted devices, but it has also drawn public attention to issues related to the security and privacy of data stored on personal mobile devices. Not surprisingly, mobile device vendors are implementing higher levels of security features in their products to address personal data protection. In today's modern mobile devices, user data is highly protected from malicious access by unauthorized attackers, as long as the user settings are properly configured.

The impact of cryptography on forensic analysis, as well as efficient data acquisition processes in computational forensics (Casey *et al.* 2011; Hargreaves and Chivers, 2008; Kornblum, 2009) [9, 21, 31]. It has been suggested that temporary files, data in volatile memory, cryptographic scheme metadata, or access to a key management system may decrypt the target data, allowing examiners to extract the original data, which can then be used in criminal investigations. However, the challenges in getting data from encrypted mobile devices stem from the fact that this enumerated data is not accessible by default, which requires screen modification.

While some traditional forensic data acquisition methods are still effective, the target device must be opened and modified directly to obtain the data effectively, often requiring scans.

In this paper, we investigate modern mobile forensic techniques and compare them with traditional mobile forensic techniques. Given the paradigm shift in mobile forensic technologies, it is clear that following the traditional forensic data mining model is no longer effective. Therefore, a new model for forensic acquisition has been proposed and modern forensic data mining techniques are being evaluated in the context of controversial and backward regulation of cryptography and government access to encrypted devices.

2. Background: A paradigm shift in mobile forensics

The advanced technologies used in modern mobile devices have greatly affected the effectiveness of mobile forensic technologies. In this section, we provide an overview of traditional forensic data acquisition techniques for mobile devices, discuss the widespread adoption of encryption and other security features in mobile devices, and then evaluate the effects of these security features on traditional mobile forensic technologies.

2.1 Conventional mobile forensic techniques

Forensic data acquisition techniques for multiple mobile platforms were researched. The integrity of their forensic evidence is assessed prior to implementation, and is currently available through multiple commercial forensic tools (Barmpatsalou *et al.* 2013; Al-Dhaqm *et al.* 2020; Reedy, 2020) [5, 2, 40]. The acquisition techniques used in mobile forensics were graded using the classification system proposed by the National Institute of Standards and Technology (NIST). The classification system includes the following five levels (Ayers *et al.* 2014; Chernyshev *et al.* 2017) [4, 10]:

- **Level 1: Manual Extraction:** The examiner directly processes the target mobile device using the device's input interface (i.e., keyboards and buttons), and records the content displayed on the device's screen.
- **Level 2: Logical Extraction:** Data (i.e. files and folders) on the target mobile device is extracted by connecting to wired/wireless communication interfaces. The extracted data is human-readable because it is in a format that can be recognized by computer applications.
- **Level 3: Hexagon Dumping / JTAG:** in storage media on the target mobile device is obtained if technologies classified at this level are used. The debug interface on the target mobile device, such as JTAG (Join Test Action Group), is generally used to perform hex dumping. Technologies that can obtain raw data without destroying hardware are generally categorized at this level.
- **Level 4: Chip off:** Chip-off requires the physical removal of the non-volatile memory stick from the target mobile device. The examiner can get a mirror copy of the entire raw data of the target mobile device, which likely contains the remains of the deleted data.
- **Level 5: Micro Read:** Micro read is a highly specialized technology, in which the data stored in the non-volatile memory is extracted in the form of an electrical property by direct observation of the memory death within the non-volatile memory chip.

Data obtained through Level 1 and 2 technologies is usually called logical data, while data obtained through Level 3 through 5 technologies is called physical data and has the advantage of including omitted data leftovers. In general, data analysis is required to provide human-readable data after obtaining the physical data.

The common understanding in traditional mobile forensic models has been that the higher the level of acquisition, the greater the chance of forensic data recovery. As examiners use a higher acquisition level, the range of accessible data becomes wider. Moreover, physical acquisition can bypass smartphone user authentication mechanisms such as PIN codes and passwords while accessing stored data, and does not require the target device to be in normal operating condition. Therefore, law enforcement agencies have widely adopted discrete data acquisition as a high-level data mining technology from various mobile devices. Note that although accurate reading is categorized as the highest in the aforementioned classification system, and although previous research has demonstrated that reading data directly from deleted memory is feasible (Corbon *et al.* 2017) [13], in practice, it is not considered an extraction technique Practical mobile data in mobile forensics to the best of the authors' knowledge.

2.2 Encryption and other security features in modern mobile devices

In order to protect user privacy and provide data confidentiality, encryption technologies are currently implemented in modern mobile devices by default. Traditionally, in mobile devices, application-level encryption techniques have been implemented in order to protect individual user data such as emails and photos. With growing concerns about security and privacy, system-wide encryption techniques are now implemented using unique, statically encrypted passwords that cannot be accessed, even by device manufacturers. Therefore, inactive mobile device data is stored in an encrypted manner. Two types of encryption schemes are frequently used in mobile devices. One is full disk encryption (FDE) and the other is file-based encryption (FBE) (Loftus and Baumann, 2017) [34]. FDE is a technology in which the entire user data partition is encrypted with a single encryption key, while FBE encrypts the data for each file base with different keys, allowing files to be decrypted independently. In Apple devices, FDE was first introduced in the iPhone 3 GS with iOS 3.X (Teufl *et al.* 2013) [49]. Apple devices with iOS versions higher than 8 use FBE. In Android devices, FDE was introduced in Android 4.4, and was supported until Android 9. Beginning with Android 7.0, FBE was used as the standard encoding method. Today, more than 80 percent of Android devices in the market are reported to be running an Android version higher than 6 (Statista, 2013) [48]. This means that user data in Android devices that were seized during the criminal investigation is now mostly encrypted.

In addition to encryption techniques, other "security by design" features are implemented in modern mobile devices. One such example is Root of Trust (RoT). When a mobile device is started, every hardware and software component in the boot chain is validated to ensure that only authorized components are executed on the system. If validation fails due to unsigned software or other reasons, the target device does not boot, preventing malicious users from accessing the device. This makes traditional data acquisition techniques such as those suggested by Vidas *et al.* (2011) [53] impractical. The Trusted Execution Environment (TEE), which is also heavily used, provides an isolated environment for critical security components of a system, by separating the normal operating system from the much smaller secure operating system, both running on the same hardware. Hence, a safe world and a normal world can coexist on an order. ARM's Trust Zone technology is largely used in Android devices. While Apple uses a similar technology called Secure Enclave Processor (SEP) to isolate the encryption key and process other sensitive information. When implementing a TEE, even "rooting" or having the highest privilege in the system does not allow access to the master data. By including these security features, mobile device manufacturers protect not only user data but also company-owned data and technologies. As a result, users do not have the freedom to control their mobile devices, and are limited to using them in the closed ecosystem of the device vendor.

2.3 Impact of security features on traditional mobile forensic techniques

As discussed, the common use of encryption, combined with complex security measures on modern mobile devices, affects the ability of traditional technologies to obtain forensic data. The effectiveness of the five-level model for mobile forensic extraction techniques discussed in Section 2.1 can be evaluated as follows in the presence of security features. Note that we are assuming that the user configurations are set up in such a way that all security features can be enabled on the target device.

- **Manual extraction:** In order to perform manual extraction on a modern encrypted mobile device, the examiner needs to know and possess legitimate user authentication credentials (for example, identification codes, passwords or fingerprints), to properly unlock the target smartphone in a fully operational state. The appropriate 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 that require access tokens.
- **Boolean extraction:** The same requirements for manual extraction can be applied to logical extraction. Once the examiner can control the target data with the correct user authentication credentials, the examiner needs to proceed to modify the system settings such as debugging authorization, in order to extract the logical data through the communication interfaces.
- **Hex Dumping/JTAG:** While JTAG and other debugging interfaces are still used on modern mobile devices, in many cases, these interfaces are disabled or locked before the devices are shipped from the factory. Therefore, testers may first need to find a way to use those debug interfaces to flood the hex on the target machine. Once enabled, hex dumping is still an effective way to get data to bypass device lock. However, since the physical data obtained is in an encrypted state on modern smartphones, decryption procedures are required after data acquisition. Cryptographic keys are often derived from both a user-specified access token, and an encryption key stored in the protected phone in such a way that it can only be used by authorized software on the device (Apple, 2020).
- **Chip-off:** Similar to hex dump, chip detachment allows the examiner to obtain the physical data of the target device by bypassing the device lock. As discussed regarding hex dumping, the data acquired is not readable until it is decrypted.
- **Micro Read:** Previous research shows that reading memory data at the die level is feasible (Corbon *et al.* 2017) [13]. However, the miniaturization of the modern semiconductor manufacturing process along with its ever-increasing capabilities makes this procedure impossible. In addition, even if the examiner succeeds in extracting the non-volatile memory contents from the target mobile device, the data is encrypted. The techniques used for fine-reading may still allow examiners to extract essential materials and analyze hidden security mechanisms from components on the target device, but it remains a daunting task.

Contrary to traditional beliefs, moving up the five-level model is not necessarily more effective in recovering forensic data of modern smartphones. Unless decoding techniques are established, the acquisition of physical data does not result in useful data.

3. Currently used data extraction techniques from encrypted mobile devices

In this section, the main current techniques for extracting forensic data from modern mobile devices, along with the flaws of the device's security features are presented. While there are some exceptions in practice where more data mining methods are available, for example when the target device is already “jailbroken” or “rooted”, we rule out such scenarios in this paper.

3.1 Manual / Logical Extraction

In cases where the examiner can obtain the user authentication credentials required to unlock the device, or the target device is not locked, the examiner can manually process the device and perform manual or logical extraction. The user authentication credentials required to unlock the device can be a password, passcode, pattern, or biometric feature (fingerprint, voice, face, or other biometric features). If a biometric feature is used to authenticate a user, law enforcement investigators in some jurisdictions may be able to spoof the authentication by capturing and copying the device owner's fingerprint, then using it to unlock the target device. Note that in most cases, biometric authentication only works if the target device is in a post-first unlock (AFU) state, and is not equipped with other advanced security features such as time-of-inactivity detection procedures. AFU means the target device is in a booted state, unlocked with user secret at least once after boot, and hasn't been turned off since. When the target mobile device is in a state before first unlocking (BFU) (never unlocked since the last boot, or has been turned off), a password, passcode or pattern is required to unlock the device and enable biometric authentication. Additionally, most biometric authentication methods have a limited time range (eg, 48 hours for current iOS devices) in which biometric properties can be used before a BFU token is required again. To unlock the device, examiners should note that there is a “panic” password option available on some recent smartphones. When setting, password panic can implement a hidden rule, such as clearing data or disabling some phone functions. If panic password is used instead of legitimate unlock password before data extraction, manual extraction will fail, and there is a high chance that the data is unrecoverable. Modern mobile devices are also equipped with anti-brute impact technologies. After a specified number of failed authentication attempts with incorrect user authentication credentials, the device becomes unavailable for a specified period of time. In the worst case, the data on the target device can be erased and become unrecoverable.

Once the target device is successfully unlocked, the logical extraction can be done by sending backup commands through user-level communication interfaces on the device, such as USB, external storage, Wi-Fi, and Bluetooth. The target phone must be configured to accept commands from the connected computer to extract data. On some modern mobile devices, rooting (administrator privilege escalation) is required. Data access management is generally controlled at the application level, and forensic software can use this function to copy specific application-related data to an attached storage device. However, on modern mobile devices, applications may choose not to be part of the backups supported by the operating system. If user data from an opt-out app is required for extraction, downgrading the app version on the target smartphone may allow examiners to extract user data. However, since this process modifies the target smartphone directly, it should be considered as the last option.

3.2 File system extraction

When performing basic manual or logical extraction of data acquisition, the examiner can only collect files and folders related to specific applications or communication protocols, and the deleted data cannot be recovered. Traditionally, this is where mobile forensic examiners decide whether or not to initiate physical acquisition. However, since most modern mobile devices use well-known file systems (for example, APFS for Apple iOS devices, ext4 for Android devices), and their data is stored on non-volatile memory in a structured file system format, obtaining a complete or partial file system data from Through non-destructive methods is currently a common technique of data mining for forensic purposes. Compared with traditional logical extraction, file system extraction allows examiners to get more data, including deleted data leftovers. All data related to applications is collected, and the forensic tool does not have to connect and acquire individual data through an application level API. Thus the examiner can access databases, system files, and logs related to applications. As long as the remains of the deleted data remain in the database, the examiner can recover some of the deleted data through file system extraction. In order to perform effective file system extraction, rooting the device is required. Without rooting, testers can only obtain partial data, and data recovery may be limited.

3.3 Cloud data acquisition

Modern mobile devices store data not only on the physical device, but also on cloud servers provided by manufacturers or vendors of operating systems. In fact, because the physical device has limited storage, some apps upload the old data to the cloud, and then delete it from the local storage. Once a law enforcement investigator obtains the information required to access the cloud server from the target devices (i.e. user credentials), the investigator may access the cloud server, collecting information belonging to the target device. While some forensic tools already have cloud data acquisition capabilities, as this acquisition requires the use of user credentials, as well as data transmission over the Internet from different jurisdictions, court orders and other additional legal procedures are often required. Legal issues related to this procedure are discussed in Section 5.

3.4 Bypassing device lock/extracting lock-related information

Accessing user data stored in the internal memory of locked and encrypted devices usually requires unlocking with the correct user authentication credentials. However, the user's credentials will likely remain unknown to investigators in most cases. Moreover, as mentioned earlier, enforcing all possible passcodes/passwords/patterns is unrealistic due to protective techniques applied to modern mobile devices as discussed in 3.1. Therefore, ways to either bypass or disable hardware locks of modern mobile devices have been explored by security researchers. Methods such as deleting lock-related data on the target device, or modifying boot processes to bypass the locking process, have been developed in order to bypass locking mechanisms and access user data. In addition to disabling and bypassing the lock, ways to disable timing constraints against brute force, enabling brute force directly on the target device (Skorobogatov, 2016) [47] have also been explored. When defining actions to bypass lock or timing constraints, system vulnerabilities are often exploited (Fenollosa, 2019; Austinlog and Andro, 2015) [17, 3]. Through the exploit, the examiner can force the user's authentication credentials to the device itself, or extract intermediate information from the device that can be used to restore the user's authentication credentials through the account on a specific system outside the device. If the intermediate information is located only on the volatile memory on the target device, then obtaining the required information through exploiting the vulnerabilities is only effective when the device is in an AFU state.

3.5 Extraction of physical data

Having the physical data of the target mobile device allows examiners to bypass its locking mechanism, and allows them to access the internal data directly. Since data decryption procedures are required on modern mobile devices after physical data is acquired, extensive reverse engineering has been done by security researchers to define decryption methods. Through the authors' experience, data decoding methods have been developed for many models of modern mobile devices. For these models, physical data can be obtained by the methods described below.

3.5.1 Physical chip-off

Chip-off analysis (Willassen *et al.* 2005; Fukami *et al.* 2017; Breeuwsma *et al.* 2007) [15, 18] refers to a forensic process in which a target device's memory chip is physically detached, and then internal data is discarded to reconstruct data that humans can Read it later. Detailed detailed analysis procedures can be found in Breeuwsma *et al*. (2007). During chip separation, the non-volatile memory chip is physically removed from the circuit board, and its content is extracted through a specialized reader. Since physical cutting is a destructive procedure, it is important for the examiner to know if there is any other component on the board that is required to decode the data. This is especially important if chip implantation procedures (Heckmann *et al.* 2018) are to be performed for severely affected phones.

3.5.2 In-system-programming (ISP)

While chip separation requires destructive operation of the target device, if the device pins required to read the target memory chip can be accessed without disconnecting the chip itself from the circuit board, the examiner can perform in-system programming (ISP) for physical data extraction (Silveira *et al.* 2020) [45]. By connecting a memory reader with electrical traces attached to the memory chip on a circuit board, the examiner can access the memory chip and create a bit-by-bit copy of the target memory without harming the operational state of the target mobile device. In order to successfully get the data through the ISP, the relevant part of the circuit board of the target device must be faulty. In some cases, where no trace is available on the circuit board surface, the partial capsule of the chip may need to be removed using laser ablation to perform the ISP. When conducting an ISP, the examiner needs to have a sound understanding of signal integrity and other electrical details. eMMCs (Embedded Multimedia Cards) and eMCPs (Embedded Multi-Chip Packages), which have been widely used in embedded devices, use single-terminal signals, so linking traces may allow examiners to read memory data. However, new memory technologies such as UFS (Universal Flash Storage) use high-speed differential signals (JEDEC, 2020) [27]. So the performance of the ISP becomes a challenge because making an external connection on the circuit board can greatly disturb the integrity of the signal.

3.6 Data acquisition with custom boot loaders

If the tester manages to load a custom boot loader into the target device during the boot process and boot it, there is a high chance of dealing with the device by running arbitrary code, making physical data acquisition possible. Traditionally, loading a custom boot loader has been enabled by the device manufacturer. Special modes (i.e. download mode or rescue mode) allowed users to run a custom bootloader on the target system during startup. However, in modern devices, in order to maintain system integrity, manufacturers enable boot loaders to run only after they have properly verified their signature, allowing only their codes to run on the device. Bootloaders are responsible for initializing the hardware components and loading the operating system which then starts the device including encryption. When booting a modern mobile device, several boot loaders are performed in series. The first boot loader that is statically encoded in the application processor ROM is called bootROM or Primary Boot Loader (PBL), and the one loaded by this bootROM is called Secondary Boot Loader (SBL). SBL usually loads another bootloader that finally loads the operating system (Hay, 2017) [27]. Only when the checks are passed does the boot loader load into the system memory, allowing the system to start normal boot processes. Boot loaders are loaded through a download mode at the SBL level. The checks are usually done by checking if each bootloader has been properly digitally signed. This process uses the initial validation key, which is stored in the one-time programmable memory area of the application processor, thus ensuring that the key is never tampered with.

For some recent mobile device models, signed bootloaders may be publicly available (Hay, 2017) [27]. By flashing bootloaders with known vulnerabilities in the target smartphone, the examiner may obtain the highest privilege in the target phone, which in turn takes full control of the device, allowing the memory data to be successfully obtained. The examiner can also attempt to downgrade parts of the boot chain to lower versions as long as rollback prevention mechanisms are not implemented on the target mobile device. By doing this, the tester can exploit known vulnerabilities that have been fixed by security updates in the actual version of the boot chain. However, the most powerful way to break into the boot chain to run random code is to exploit the bootROM vulnerability, and this technique has been explored and used to access data in modern mobile devices (Katalov, 2019) [28].

While modern mobile devices prevent users from loading custom bootloaders, it is now widely known that flashing at the PBL level is possible by booting the device in a special boot mode at the processor level. The name of this boot mode is different for each manufacturer. It's called Emergency Download (EDL) for Qualcomm chipset, Device Firmware Update (DFU) mode for Apple chipset, and Download mode for MediaTek chipset. These modes allow phone manufacturers to flash software on their devices. Thus, forensic examiners can use these modes and the flash-made boot loader in the target smartphone, which helps them to obtain user data without modifying it. Unless any additional authorization mechanism is implemented, a set of commands, a special cable, or hardware modifications cause the target devices to switch to those special modes. Capturing data using dedicated bootloaders is becoming popular because the same technology can run on a wide variety of devices with the same chipset, and it is usually difficult for mobile device manufacturers to patch vulnerabilities at the processor level. Research has already demonstrated that vulnerabilities at the bootloader level on common chips can be useful for user data acquisition (Hay, 2017; Alendal *et al.* 2018) [3, 27].

4. Emerging techniques

In addition to the forensic data acquisition techniques described in the previous section, the following methods have been investigated as possible useful techniques for extracting forensic data from modern mobile devices.

4.1 Side-channel analysis

When integrated circuits (ICs) operate on a circuit board, information about these integrated circuits may leak out in the form of current flow or electromagnetic emission (EM). This information can sometimes be used to extract internal secrets such as encryption keys (Sayakkara *et al.* 2019) [41]. This type of analysis is called Side Channel Analysis (SCA), which has been a popular security research area for smart cards and other security technologies. Recent work has demonstrated that SCA can be used to retrieve an encryption key from an application processor in a modern mobile device (Vassell *et al.* 2019). Although research is required for each application processor because processors are unique, SCA is a promising technology for obtaining encryption keys from modern mobile devices. Once obtained, the key can be used to decrypt bootloaders. Meanwhile, in addition to shrinking the scale of technology, device manufacturers are adding features such as heterogeneous operation and voltage frequency optimization to reduce SCA vulnerabilities.

4.2 Fault injection

Fault injection is a technique in which controller inputs are manipulated for the purpose of causing illegitimate behaviors of the target system. Examples of fault injection techniques include faulty or underpowered power supply, electromagnetic signal transmission, and optical beam injection. Research has already been done to show the efficiency of error injection to attack the boot sequence and extract the code with the highest privileges from an Android device (Vassell *et al.* 2020) [51]. False injection may also be useful for disabling debug interface locking such as JTAG on the target machine.

4.3 SoC reverse engineering

The on-chip (SoC) for die-level reverse engineering virtually accesses the inside of SoCs on mobile devices, examining internal circuits using highly specialized laboratory equipment. By reverse engineering at the SoC level, one can learn how to structure the system by checking the connections of the internal circuit. A semiconductor template consists of multiple layers interconnected with each other. By delaying each layer, and translating the connection into a circuit, one can retrieve the overall design and try to figure out and understand how the target system works. SoCs have been reverse engineered to achieve multiple goals, including reasons for hacking or counterfeiting (Quadir *et al.* 2016) [16]. A major driver of template-level reverse engineering of the SoC for forensic purposes is the recovery of key hardware-associated information, which is stored in the one-time programmable memory area of the SoC, as discussed in Section 3.6.

5. New portable forensic model

As we saw through Section 3 and Section 4, current methods of accessing user data in modern mobile devices have changed significantly from traditional methods. Traditionally, forensic data mining techniques have focused on obtaining physical data, which when analyzed later can recover deleted data. This method was effective because the data was stored in clear text on non-volatile memory on mobile devices. As a result, a five-level data extraction model was followed as a standard model. However, with the implementation of encryption and other complex security features, just getting the raw data doesn't help in recovering user data anymore. Even worse, destructive actions such as chip cutting may destroy basic components needed to decrypt the acquired data. Moreover, the secure deletion of mobile features can effectively delete the leftover data on the system, and recovering the deleted data from the physical data is almost impossible. Additionally, without user authentication credentials, obtaining user data, whether logical or physical, becomes a huge challenge, regardless of acquisition level. Therefore, the classification of the mobile data extraction method by the type of data extracted is becoming less effective. Currently, cleartext data mining, or encryption key extraction is the main objective in forensic data mining. Without proper user authentication, this can only be achieved by exploiting system vulnerabilities on the target device or by identifying and accessing stored encryption keys. However, both methodologies require extensive reverse engineering before working on the target mobile device. Taking into account the current situation, we propose a new model for forensic data extraction as follows:

- **User secret-based acquisition:** If the examiner can unlock the phone with the correct user authentication, the target smartphone can be turned on manually, and it can be set up in a way that allows data extraction through its user interfaces. The manual and logical extraction presented in Section 3.1 fall into this category. As discussed in Section 5, forced password disclosure from the device owner is not an appropriate method. However, the takeover may be made possible by grabbing the device owner's biometric information. After the device is unlocked, the examiner can modify the device setting and extract the logical data, file system or physical data by rooting the device.
- **Reverse-engineering based acquisition:** Reverse engineering of modern mobile devices is essential in the study of forensics. Reverse engineering can be done in both software and hardware. Once the examiner learns the internal structure of the operation of the target mobile device through reverse engineering, the examiner may be able to reconstruct the original user data. One example is defining the encryption mechanism and retrieving the encryption key. Once this information has been retrieved, the examiner can obtain the physical data from the target smartphone by the methods discussed in Section 3.5, and then decrypt the data outside the device.
- **Vulnerability exploitation-based acquisition:** When the target device is locked and encrypted, these features must be bypassed or disabled for data extraction. Bypassing or disabling device lock, encryption, and other security features generally requires exploiting system vulnerabilities. Exploiting vulnerabilities may require a combination of hardware and software attacks. Once these features are bypassed, examiners can choose to have full or partial logical data, a file system, or physical data. As discussed in Section 5, the use of open and unpatched vulnerabilities is justified from a legal perspective. However, in many cases, zero-day vulnerabilities found through extensive reverse engineering are required for effective data mining. Several works have already demonstrated the effectiveness of exploiting vulnerabilities in digital forensics (Alendal *et al.* 2018; Hay, 2017; Shwartz *et al.* 2017) [3, 27, 44].

Figure 1 shows a simple flowchart for choosing an appropriate data extraction technique. Each technique is categorized according to the aforementioned model.

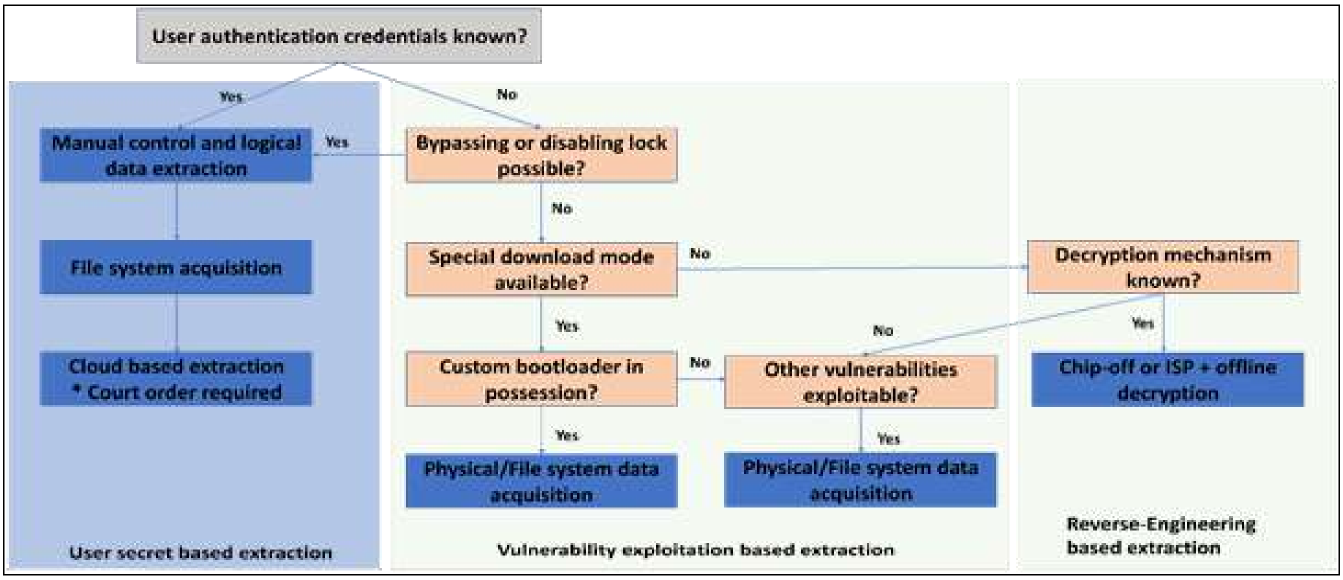
User authentication credentials known?
Yes
No
Manual control and logical data extraction
Yes
Bypassing or disabling lock possible?
No
File system acquisition
Special download mode available?
No
Decryption mechanism known?
Yes
No
Yes
Cloud based extraction * Court order required
Custom bootloader in possession?
No
Other vulnerabilities exploitable?
Chip-off or ISP + offline decryption
Yes
Yes
Physical/File system data acquisition
Physical/File system data acquisition
Reverse-Engineering based extraction
User secret based extraction
Vulnerability exploitation based extraction

Fig 1: A new mobile model for forensic data mining.

Essentially, without proper user authentication credentials, the exploit must be implemented. On the other hand, once the user secret is available, the examiner can use it to manually operate the target phone. Some vendors of portable forensic tools already provide automated versions of the exploits and data mining procedures shown in Figure 1. When testing and evaluating these tools, the acquisition level can be categorized using this new model.

7. Conclusions and recommendations

Due to the growing security and privacy concerns by mobile device users, manufacturers aggressively implement encryption and other complex security mechanisms. This trend significantly affects the traditional capabilities of obtaining forensic data. Traditionally, obtaining raw data from non-volatile memory on a mobile device will yield useful data - including deleted information - that can then be used in criminal investigations. Therefore, chip separation and micro-reading have always been considered the highest level of effective techniques in forensic data acquisition. However, as we have discussed in this paper, current physical data acquisition practices cannot provide human-readable data due to encryption. Also, the effective data erasure functions at the operating system level make it difficult to find data leftovers in the physical data. At the same time, other security features make it difficult for forensic examiners to obtain even live data on the target device. Therefore, bypassing or disabling device locking and encryption while maintaining the integrity of user data has become one of the most important forensic techniques for modern mobile devices. Extensive reverse engineering, as well as exploiting vulnerabilities, has become essential for forensic examiners when conducting mobile forensics. The vulnerabilities found through reverse engineering have already been used to obtain evidence data from locked and encrypted mobile devices.

Meanwhile, the use of backdoors and weaknesses in forensic analysis has generated controversy and sparked political debates by lawmakers and human rights organizations. While it is unlikely that exceptional access would be granted by manufacturers, the use of known vulnerabilities could be justified in the absence of less intrusive investigative measures to gain access to evidence. Currently, there is no clear legislative rule about using zero-day exploits to obtain data from encrypted devices. However, responsible disclosure may provide a reasonable baseline for forensic examiners to follow.

As suggested in our new mobile forensic data mining model, exploiting mobile device system vulnerabilities is essential in extracting evidence data from modern encrypted mobile devices for forensic investigation. Correct understanding of technical details, along with properly following legal requirements is fundamentally important for forensic examiners when performing forensic data acquisition.

8. References

1. Abraha, HH Abraha. How compatible is the US CLOUD Act with cloud computing? Brief analysis International Data Privacy Law. 2019;9:207-215. 10.1093/idpl/ipz009.
2. Al-Dhaqm A, Razak S, Ikuesan RA, Kebande VR, Duqm, *et al.* Review mobile criminal investigation process models Access to IEEE, 2020.
3. Alendal GO, Dyrkolbotn S, Alendal G, *et al.* Axelsson Forensic Evidence Gain - Common Standards Setting Analysis to enforce and Circumvent Samsung Secure Boot number. Invest. 2018;24:S60-S67. 10.1016/ j.diin.2018.01.088 Apple, 2020 Apple platform security Google Scholar Austinlog and Andro, 2015 UT Austin ISO Blog Bypass screen lock for Android 5.x (cve-2015-3860) Google Scholar.
4. Ayers R, Brothers S, Ayers W, *et al.* Jansen Mobile Forensics Guidelines National Institute of Standards and Technology Google Scholar, 2014.
5. Barmpatsalou K, Damopoulos D, Kambourakis G, Barmpatsalou V, *et al.* Katos Critical review of 7 years of mobile forensics number. Investment. 2013;10:323-349. 10.1016/j.diin.2013.10.003 Article Download PDF View Record at Scopus Google Scholar.
6. Beaulieu R, Shors D, Smith J, Tetman-Clark S, Weeks B, Beaulieu L, *et al.* Wingers Simon and speck: Banning Ciphers for the Internet of Things, IACR Cryptole Print Arch. 2015;(2015):585p. View log in Scopus Google Scholar Board of Directors, 2020 EDP. Board Opinion 23/2018 on Commission Proposals for

European Production Orders and Preservation of Electronic Evidence in Criminal Matters (Article 70.1.b)https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence Final opinion en.pdf (2020), accessed September 26, 2018 Google Scholar.

7. Priusma Im, Jung C Claver, Knife R, Roilofs Priusma M, *et al.* Recover forensic data from flash memory Journal of Forensic Medicine for Small Scale Digital Devices, 2007, 1. Google Scholar.
8. Bowdish RH, BU Gasser Budish, *et al.* Crypto policy and its international implications: A framework for understanding the effects of extraterritorial ripples URL, 2018. https://dash.harvard.edu/handle/1/36291726 (2018) Google Scholar.
9. Casey J, Fellowes M, Geiger J, Casey E, *et al.* Stelatus The growing impact of full disk encryption on digital forensics number. Invest. 2011;8:129-134. 10.1016/j.diin.2011.09.005, Standards, Professionalism and Quality in Digital Forensics URL: http://www.sciencedirect.com/science/article/pii/S1742287611000727 Article Download PDF View Record at Scopus Google Scholar.
10. Chernyshev S, Zidley Z, Paige A, Chernyshev M, *et al.* Woodward Mobile forensics: developments, challenges, and research opportunities IEEE Security and Privacy. 2017;15: 42-51.View log in Scopus Google Scholar.
11. Council of Europe. Council of Europe Draft Second Additional Protocol to the Cybercrime Convention (ets 185) T-CY, 2018, 23. Countryside. URL: https://www.coe.int/en/web/cybercrime/t-cy-drafting-groupVisited on 2020-10-21 Google Scholar.
12. Council of the European Union. Council of the European Union Commission services report on the second round of negotiations in light of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 2018-2019. URL: https://www.statewatch.org/media/documents/news/2019/nov/eu-council-usa-e-evidence-13713-19.pdf, accessed October 21, 2020 Google Scholar.
13. Courbon S, Skorobogatov C, Woods Corbon F, *et al.* Reversal of geometric EEPROM flicker memories using scanning electron microscopy K. Lemke-Rust, M. Tunstall (Eds.), Smart Card Research and Advanced Applications, Springer International Publishing, Cham, 2017, 57-72. View a PDF Cross Ref View Record file in Scopus Google Scholar.
14. Legal Criminal News. Legal Criminal News Parallel Construction: Building Criminal Cases Using Secret and Unconstitutional Surveillance, 2018. URL: https://www.criminallegalnews.org/news/2018/may/14/parallel-construction-building-criminal-cases-using-secret-unconstitutional-surveillance/ (2018), entry date June 30, 2020 Google Scholar.
15. ENISA. ENISA Opinion paper on encryption Strong encryption protects our digital identity, 2016. URL: https://www.enisa.europa.eu/publications/enisa-position papers-and-opinions/enisas-opinion-paper-on-encryption (2016) Google Scholar.
16. Europol, ENISA. EUROPOL and ENISA In legal forensic investigation that respects data protection in the twenty-first century, 2016. URL: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-research-that-respects-21st-Century-data-protection (2016) Google Scholar.
17. Fenollosa C Vinulosa. checkm8: What you need to know to keep your iPhone safe, 2019. URL: https://cfenollosa.com/blog/checkm8-what-you-need-to-know-to-keep-your-iphone-safe.html (2019) Google Scholar
18. Fukami S, Juice YLo YK, Wlotlo Fukami O, *et al.* Improving the reliability of forensic analysis of nand flash memory devices, digital investigation. 2017;20:S1-S11. URL:http://www.sciencedirect.com/science/article/pii/S1742287617300415 https://doi.org/10.1016/j.diin.2017.01.011
19. dFRWS 2017 Europe Article Download PDF Google Scholar.
20. Gothel Q, Liger A, Hetman J, Egger M, Crawford Gutheil, *et al.* Legal Frameworks for Hacking by Law Enforcement: Identifying, Evaluating and Comparing Practices, European Parliament, 2017. Google Scholar.
21. Hargreaves, Chivers, Jim Hargreaves H Chivers, Recovering encryption keys from memory using linear scanning 2008 Third International Conference on Availability, Reliability and Security, 2008, 1369-1376. 10.1109/ARES.2008.109 View PDF View history in Scopus Google Scholar.
22. Hey R, Hi Fastboot. OEM vuln: Android bootloader vulnerabilities in vendor customizations 11th USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association, Vancouver, BC, 2017. URL: https://www.usenix.org/conference/woot17/workshop-program/presentation/hay Google Scholar
23. Hickman K, Markantonakis D, Naqash T, Hickman T, *et al.* 2018. Sovignite Smartphone Forensic Analysis with Adhesives: Implanting Package Components on the Packaging number. Investment. 2018;26:29-39. 10.1016/j.diin.2018.05.005
24. URL:http://www.sciencedirect.com/science/article/pii/S1742287618301117 Article Download PDF View Record at Scopus Google Scholar.
25. Human Rights Watch. Human Rights Watch US: Secret Evidence Undermines Fair Trial Rights, 2018. https://www.hrw.org/news/2018/01/09/us-secret-evidence-erodes-fair-trial-rights (2018), entry date 30 June 2020 Google Scholar.
26. Jacobsen K. Jacobsen Game Phones, Data Isn't Coming: Modern Mobile OS Cryptography and Its Dreadful Impact on Law Enforcement George Wash. Rev. Law. 2017;85:566-612. URL: http://www.gwlr.org/wp-content/uploads/2017/03/85-Geo.-Wash.-L.-Rev.-566.pdf View Scopus Google Scholar Recording.
27. JEDEC, JEDEC universal flash storage (ufs), version 3.1, jedec solid state technology association, 2020. Google Scholar
28. Katalov. in Katalov Get an iOS device with checkra1n jailbreak, 2019. URL: https://blog.elcomsoft.com/2019/11/ios-device-acquisition-with-checkra1n-jailbreak/ (2019) Google Scholar
29. Cops, Costa, b- c. Cobbs, E. Costa Seeking some light through the lens of 'crypto war' history: Policy options

for law enforcement against 'going into the dark' computer. law security. Rep. 2018;34:890-900. 10.1016/j.clsr.2018.06.003

30. URL:https://linkinghub.elsevier.com/retrieve/pii/S0267364918302413 Article Download PDF View Record at Scopus Google Scholar.
31. Kornblum JD Kornblum. Bitlocker drive encryption implementation for forensic analysis number. Investment. 2009;5:75-84. 10.1016 / j.diin.2009.01.001 Article Download PDFView Record at Scopus Google Scholar
32. Lewis JA, Zheng DE, Carter WA Lewis, *et al.* CSIS Technology and Public Policy Program, Dr. Center for Strategic and International Studies (Washington, Washington, The impact of encryption on legal access to communications and data). OCLC, 2017, 984904060. View Scopus Google Scholar Recording.
33. Liguori C Liguori. Exploring legal hacking as a possible answer to the darkness debate Scientific Paper ID SSRN 3606601, Social Science Research Network, Rochester, NY, 2020. URL:https://papers.ssrn.com/abstract=3606601 Google Scholar
34. Loftus R, Bowman M. Android 7 file-based encryption and attacks against it, 2017. URL:http://delaat.net/rp/2016-2017/p45/report.pdf (2017) Google Scholar
35. Bell. Spelling you can't always get what you want: How will law enforcement get what they need in the post-CALEA era, the age of crypto-centric cybersecurity? NCJ Law Technol. 2016;17:599p. URL:https://scholarship.law.unc.edu/ncjolt/vol17/iss4/3 View Scopus Google Scholar Recording.
36. Penny Gibbs, Penny S, Gibbs D. Law Enforcement Access to Encrypted Data: Legislative and Charter Responses Paper ID SSRN 3331348, Social Science Research Network, Rochester, NY, 2017. URL:https://papers.ssrn.com/abstract=3331348 Google Scholar.
37. Pichan M, Lazarescu S, Soh Pichan TA, *et al.* Cloud Forensics: Technical Challenges, Solutions, and Comparative Analysis number. Investment. 2015;13:38-57. 10.1016 / j.diin.2015.03.002 URL: https://linkinghub.elsevier.com/retrieve/pii/S1742287615000407 Article Download PDF View Record at Scopus Google Scholar.
38. Pobelo A, Ferreira C, Varisco Pupillo, *et al.* Governmental Disclosure Decision Processes Disclosure of Software Vulnerabilities in Europe, CEPS, 2018. Google Scholar
39. Quadir SE, Chen J, Forte D, Asadizanjani N, Shahbazmohamadi S, Quadir M, *et al.* On-chip scanning to reverse engineering system, 2016, 13. URL: https://doi.org/10.1145/2755563 (2016) Google Scholar
40. Reddy P Reddy. Interpol Digital Evidence, 2020. Review 2016-2019, International Forensic Science: Synergy URL:http://www.sciencedirect.com/science/article/pii/S2589871X20300152 (2020) https://doi.org/10.1016/j.fsisyn.2020.01.015 Google Scholar
41. Sayakkara A, Le Khak NA, Scanlon M, Sayakkara, *et al.* Benefit from electromagnetic side channel analysis to examine iot devices number. Invest. 2019;29:S94-S103. 10.1016 / j.diin.2019.04.012 URL: http://www.sciencedirect.com/science/article/pii/S1742287619301616 Article Download PDF View Record at Scopus Google Scholar.
42. Schneier B. ISO rejected two NSA algorithms, 2018. URL:https://www.schneier.com/blog/archives/2018/04/two_nsa_algorit.html Google Scholar.
43. Shah R Shah. Law enforcement and data privacy: a forward-looking approach Yale Lou c, 2015,125. URL: https://digitalcommons.law.yale.edu/ylj/vol125/iss2/5 Google Scholar.
44. Schwartz A, Cohen A, Shabtai Y, Orin Schwartz, *et al.* Shattered Trust: When Smartphone Replacement Components Attack 11th USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association, Vancouver, BC, 2017. URL: https://www.usenix.org/conference/woot17/workshop-program/presentation/shwartz Google Scholar
45. Silveira C, de Sousa Junior R, Albuquerque R, Amvame Nze G, García Villalba Silveira *et al.* A methodology for reconstructing forensic data on android mobile devices that applies in-system programming and composite firmware Science, App, 2020;10:4231pp. 10.3390 / application 10124231 View PDF.
46. Sibel B Sippel. Legislative train, European production and preservation orders for electronic evidence in criminal matters, 2021. URL:https://www.europarl.europa.eu/legislativetrain/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence (2021), accessed On May 21. 2021 Google Scholar.
47. Skorobogatov. The bumpy road to Iphone 5c Nand Mirroring, 2016. Ar Xiv: arXiv: 1609.04327 Google Scholar
48. Statista. Android OS all over the world share OS version, 2013. From 2013 to 2020 and 2020 URL:https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/Google Scholar.
49. Teefl B, Zefferr T, stromberger c Teufl *et al.* Mobile encryption systems International Conference on Information Security IFIP, 2013. Google Scholar. Cloud Law. 2018, Google Scholar.
50. Vaselle A, Maurine P, Cozzi M, Vaselle, *et al.* Breaking mobile firmware encryption through side channel near field analysis Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop, ASHES'19, Association for Computing Machinery, New York, NY, USA, 2019, 23-32. 10.1145/3338508.3359571 URL: View PDF View history in Scopus Google Scholar.
51. Vasselle A, Thiebeauld H, Maouhoub Q, Morisset A, Ermeneux S, Vaselle *et al.* Laser-induced injection on smartphone to bypass Extended Secure Boot version IEEE Trans. Comput. 2020;69:1449-1459. 10.1109/TC2018.2860010 View PDF View history in Scopus Google Scholar
52. Chang C, Kristen N, Vidas T, *et al.* Towards a general assembly methodology for Android devices number. Invest. 2011;8:S14-S24. 10.1016 / j.diin.2011.05.003 URL:http://www.sciencedirect.com/science/article/pii/S1742287611000272(Proceedings of the eleventh annual conference DFRWS) Article Download PDF Google

Scholar.

53. Walden, First Walden. 'Heaven is falling!' - Responses to the darkness problem computer. law security. Rep. 2018;34:901-907. 10.1016/j.clsr.2018.05.013 URL: http://www.sciencedirect.com/science/article/pii/S0267364918301973 Article Download PDFView Record at ScopusGoogle Scholar.
54. Willassen S, *et al*. Forensic analysis of the internal memory of a mobile phone Bullitt, S.; Shinoy (Eds.), Advances in Digital Forensics, Springer US, Boston, MA, 2005, 191-204.Google Scholar
55. Zawad S, Hassan R. Cloud forensics: a meta-study of open challenges, approaches, and problems, 2013. https://arxiv.org/pdf/1302.6312.pdf (2013) Google Scholar