DESIGN OF A FRAMEWORK FOR DATA EXTRACTION AND ANALYSIS FROM ANDROID-EMBEDDED SMARTPHONES

[1]ASLAM.J.KARJAGI ,[2] S. A.QUADRI
[1]Assistant Professor, [2]Professor
[1]Department of CSE, Secab Institute of Engineering and Technology, Vijayapura586109, Karnataka, India
[2]Department of CSE, Secab Institute of Engineering and Technology, Vijayapura 586 109, Karnataka, India

Abstract. *Mobile forensic acquisition is a critical aspect of modern criminal investigations, as mobile devices have become an essential part of our daily lives. Yet, forensic investigators aiming to extract data from current mobile devices in a forensically sound manner have faced substantial difficulties due to the robust security features of these devices, such as encryption. Conventional forensic data-collecting techniques are no longer viable, necessitating the development of new techniques that work by evading security measures and taking advantage of system flaws. The CLOUD Act is a US law that gives foreign governments the authority to demand information from US-based Cloud Service Providers or to eavesdrop on conversations, which makes it more difficult to do forensic analysis on mobile devices. To address these issues and evaluate contemporary forensic data extraction approaches in light of the contentious regulation of encryption and governmental access to encrypted devices, this article suggests a new model for mobile forensic acquisition. One of the major challenges faced by forensic investigators is the constantly evolving nature of mobile devices and their software. As manufacturers release new models with different security features and operating systems, forensic experts must adapt their techniques to keep up with these changes. Additionally, the use of encryption is becoming more widespread among consumers, which makes it more difficult for forensic experts to access data on these devices. Therefore, it is essential that forensic investigators stay up to date with the latest advancements in mobile technology and develop new techniques for data extraction that can keep pace with these advancements.*

Key words:*Android, Mobile Forensics (MF), Digital Forensics, Extraction, Analysis, Cybersecurity.*

1. INTRODUCTION

Mobile devices are now an integral part of daily life and are being used more frequently in homicide investigations. Law enforcement organizations must do forensic examinations of mobile devices in order to properly retrieve evidential data from these devices. Yet, the inclusion of strong security features like encryption on modern mobile devices has made it challenging for forensics experts to extract the data from them. New techniques that rely on getting beyond security measures and exploiting system flaws are required because the old methods of forensic data gathering are no longer effective. We examine current forensic data extraction methods in this study in the light of the disputed regulation of encryption and the government's access to encrypted devices, and we present a fresh approach to forensic acquisition that addresses these problems. In order to address the difficulties presented by encryption in contemporary mobile devices, this study attempts to provide a thorough knowledge of the influence of encryption on forensic analysis and the necessity for new forensic techniques that can be employed to perform a sound forensic investigation to leave no evidences behind.

2. THE CHANGING LANDSCAPE OF DIGITAL FORENSICS: A SHIFT IN PARADIGM

The introduction of cutting-edge technologies in contemporary mobile devices has significantly altered mobile forensic approaches. This section examines the widespread use of encryption and other protection measures in mobile devices, examines how these features affect conventional means of mobile forensic data acquisition, and provides a general outline of the conventional methods used in smartphone forensic data acquisition.

1. LEGACY METHODS FOR MOBILE DEVICE FORENSIC ANALYSIS

For a variety of mobile device platforms, mobile forensic strategies have been developed and tested. The National Institute of Standards and Technology (NIST) has categorized these methods into five categories: manual extraction, logical extraction, hex dumping/JTAG, chip-off, and micro read. Physical extraction gets raw data, including traces of erased data, while logical extraction gets data

that can be read by humans. Chip-off data capture, which avoids user authentication methods and does not require the equipment to be in standard booting mode, is frequently used by law enforcement authorities. The maximum level of extraction, known as a micro read, is not seen as viable in mobile forensics.

A detailed explanation of the 5 techniques is as follows,

A. TIER 1: MANUAL EXTRACTION

The examiner utilizes the mobile device's input interface to control it directly (e.g. keypads, buttons). The examiner records whatever is shown on the device's screen. No data extraction software or hardware is used.

B. TIER 2: LOGICAL EXTRACTION

Both wireless and wired interfaces are used to extract data (such as files and directories) from the mobile device. Extracted data is presented in a readable format for humans that computer programs can understand. Requires data extraction software to communicate with the mobile device.

C. TIER 3: PHYSICAL EXTRACTION

The mobile device's storage media's full or part of the raw data (hex dump) is obtained. Hex dumping is carried out on the mobile device via the debug interface (like JTAG). This category includes methods that can acquire raw data without destroying the hardware.

D. TIER 4: CHIP-OFF

Requires physically removing the mobile device's non-volatile memory chip. An examiner can receive an exact duplicate of the mobile device's whole raw data, which might include remnants from deleted data. Considered a high-tier data extraction technique and is widely used by law enforcement agencies.

E. TIER 5: MICRO READ

A highly specialized method that involves directly inspecting the memory block inside of the non-volatile memory chip in order to extract data in the form of electrical properties. Although it is the highest in the classification system, due to its complexity and expense, it is not frequently utilized in practice. Physical data is what is obtained using this method, and it may contain remnants from deleted data.

Traditionally, it is believed that the higher the tier of acquisition used in mobile forensics, the greater the chance of successfully recovering forensic data. Higher tiers of acquisition allow access to a wider range of data, and physical acquisition techniques can bypass user authentication mechanisms and can be performed even if the device is not booting normally. For these reasons, law enforcement organizations favor chip-off data capture, the most advanced method for obtaining information from mobile devices. Although micro read is the top rank in the categorization system, despite some research suggesting its potential efficacy, it is not regarded as a realistic technique for mobile data extraction.

3. METHODS USED FOR RETRIEVING INFORMATION FROM ENCRYPTED MOBILE DEVICE

The following section outlines the main forensic data extraction techniques that are presently utilized on modern mobile devices, as well as the security features that can hinder the process. It should be noted that there are some cases where supplementary data extraction methods may be applicable, such as when the target device has "privileged" or "superuser" access. However, this paper will focus on methods that do not involve such scenarios.

1. LOGICAL DATA EXTRACTION

The main techniques for manually or logically extracting data from mobile devices used in forensic investigations are described in this section. The user login credentials are required to unlock the device using these methods, unless it is already unlocked. A password, passcode, paper pattern, or biometric attributes like a fingerprint, voice, or other features could be used as the credentials. Nevertheless, biometric authentication cannot be employed if the device is not in an After First Unlock (AFU) state and does not have additional cutting-edge security features like inactivity-time detection mechanisms. Biometric authentication cannot be enabled when the target device is still in its Before First Unlock (BFU) state without a password, passcode, or pattern drawing.Also, the BFU

code would be required once more after the time period connected to the majority of biometric authentication techniques. It is crucial to remember that contemporary mobile devices have anti-brute-forcing features that disable for a predetermined period of time after a predetermined number of unsuccessful login attempts using erroneous user credentials. By leveraging user-level communication ports on the device, such as USB, external storage, Wi-Fi, and Bluetooth, backup commands can be sent once the device has been successfully unlocked. To increase administrator access on some contemporary devices, however, rooting may be necessary before sending backup commands. Data access management is frequently governed by applications, and forensic software can exploit this functionality to copy particular app-relevant data to a connected storage device. In some circumstances where the OS does not support programs backup operations, downgrading the app version on the targeted smartphone may be the only option left to extract the user data. The target smartphone is altered during this process, thus it should only be utilized as a last resort. Examiners should also exercise caution when using the "panic" password option because it may carry out a secret command that renders data unrecoverable by erasing it or deactivating certain phone features.

2. NON-DESTRUCTIVE FILE SYSTEM EXTRACTION

The quantity of data that can be manually or logically extracted from mobile devices is frequently constrained, and lost data cannot usually be recovered. In contrast, non-destructive file system extraction enables examiners to obtain all or a portion of the file system data. This method is becoming more and more common for forensic purposes due to the structured file system format of modern smart phones along with the implementation of well-known file systems such as Apple iOS devices' APFS& ext4 for Android smartphones.File System Extraction, as compared to Logical Extraction, gives users access to information about the apps, including logs, system files, and databases. The examiner can recover the deleted data traces from the database by rooting the smartphone. Without rooting, the amount of data that can be acquired is limited, and data recovery may be considerably difficult. Therefore, File System Extraction is an effective technique for acquiring more data, potentially including deleted data, and is a non-destructive approach for conducting forensic investigations.

3. CLOUD DATA ACQUISITION

Cloud data acquisition is a valuable source of evidence in mobile forensic investigations. By accessing cloud data, examiners can potentially access more data than can be obtained from the physical device or even file system extraction. Cloud data may include backups, photos, videos, messages, emails, call logs, and more. Additionally, cloud data can be used to verify or corroborate evidence already obtained from the device. However, acquiring cloud data presents some unique challenges. As mentioned, access to the cloud server requires user credentials, which may be difficult to obtain. Additionally, obtaining cloud data may require transferring data over the internet from many countries, which can impede legal processes. Furthermore, cloud data may be subject to encryption or other security measures that can make it more difficult to access.Given these challenges, it is important for forensic examiners to have a clear understanding of the legal and technical requirements for accessing cloud data. This may involve obtaining a court order, working with internet service providers or cloud service providers, and using specialized forensic tools to access and analyze the data.

4. CIRCUMVENTING DEVICE LOCKS AND EXTRACTING RELATED INFORMATION

Investigators normally need to unlock the device using the proper user authentication credential in order to access the user data contained on locked and encrypted devices. The login credentials, however, are frequently unknown to investigators. Furthermore, due to the security mechanisms of contemporary mobile devices covered in 3.1, brute-forcing every potential combination of passcodes, passwords, or patterns is not practical. Security experts have therefore looked for ways to get through or turn off device locks. In order to overcome lock systems and gain access to user data, several researchers have developed ways to delete lock-related information stored on the target device or alter the boot process to bypass the lockstep. Researchers have also looked into ways to remove temporal restrictions that prevent brute-forcing, allowing brute-forcing to take place directly on the target device. These techniques usually exploit security holes, allowing the investigator to brute-force the user authentication code on the device directly or get intermediary data from the device. Calculations based on the intermediate data can be used to establish the user authentication credential on a chosen system away from the device. Nevertheless, if the target device's volatile memory is the sole place where the intermediate data is stored, then vulnerabilities can only be

exploited when the target device is in the AFU state.

5. CUSTOM BOOT LOADERS FOR DATA ACQUISITION

A locked and encrypted device can be unlocked using a custom boot loader, enabling the execution of arbitrary code and the capture of physical data. However, modern devices make it challenging for examiners to load a custom boot loader by only allowing validated and signed boot loaders to operate during the boot-up process. It is possible to load boot loaders using download mode, but only if each boot loader has a valid digital signature. Examiners can successfully obtain memory data by controlling the device and flashing boot loaders that include existing vulnerabilities in the target device. It is also feasible to downgrade some boot chain elements if anti-rollback methods are not applied. Exploiting the bootROM vulnerability, which has been used to gain access to data in contemporary mobile devices, is the most potent method of breaking into the boot chain. While it is forbidden for users to load custom boot loaders, forensic investigators can employ the emergency download (EDL) or device firmware update (DFU) modes to flash customized boot loaders into the target device, granting them to extract user data without altering it. As the same technique may be used on a variety of devices with the same chipset and because it is frequently challenging for mobile device producers to fix vulnerabilities at the processor level, data harvesting with customized boot loaders is becoming more widespread.

6. PHYSICAL DATA EXTRACTION

Examiners can immediately access the internal data of a mobile device and get beyond its lock mechanism by physically acquiring its data. To identify decryption techniques, security experts have extensively reverse-engineered data decryption processes for contemporary mobile devices. Based on their experience, the writers have developed data decryption techniques for a number of popular mobile device models. The following methods can be used to acquire physical data for these models:

A. PHYSICAL CHIP-OFF

The "chip-off analysis," a forensic technique, entails physically removing the target device's memory chip and dumping its internal data to reconstruct human-readable data later. In particular, if chip transplant treatments are required for highly damaged phones, this damaging technique necessitates an examiner to evaluate if any additional component on the circuit board is required for the decryption of the data.

B. IN-SYSTEM PROGRAMMING (ISP)

Examiners can use In-System-Programming (ISP) for physical data extraction if the appropriate device pins for accessing the target memory chip are reachable without detaching the chip from the circuit board. Examiners can access the memory chip and make a bit-by-bit replica of the target memory without affecting the target mobile device's operational status by linking a memory reader to electrical traces on the circuit board that are attached to the memory chip. For data to be correctly captured via an ISP, the target device's circuit board should be free of any faults in the relevant area. If there are no traces on the circuit board's surface, ISP may require partial chip de-capsulation with laser ablation. Before concluding ISP, the examiner should have a firm grasp of signal integrity and other electrical issues. When employing new memory technologies like UFS, which rely on high-speed differential signals, it is challenging to perform ISP because doing so could seriously compromise the signal integrity.

4. MOBILE FORENSIC ANALYSIS

The forensic analysis process can start after the data from the mobile device has been obtained. Mobile forensic analysis is looking into the information gathered from the mobile device in order to find pertinent facts that can be utilised in court. The data from the mobile device will be identified, preserved, extracted, interpreted, and documented utilising forensic tools and techniques. Some of the crucial procedures in mobile forensic analysis include the ones listed below:

1. DATA FILTERING AND PRIORITIZATION

Due to the sometimes-overwhelming volume of data collected from mobile devices, data filtering and prioritizing are crucial steps in the forensic research process. In this step, relevant data are separated from irrelevant data, identified, and prioritized according to their importance and relevance to the case. The time and resources needed for the succeeding analysis procedures may be decreased as a result of this step.

2. DATA DECODING AND PARSING

After identifying and prioritizing important data, the following step is to decode and parse the data. Using forensic tools, data is extracted from the device's file system, databases, and other storage areas. This data is then decoded and analysed so that people can understand it. The data is subsequently evaluated in order to look for trends, correlations, or other information important to the study. This phase can be difficult and requires a thorough understanding of the device's components.

3. DATA ANALYSIS AND INTERPRETATION

The parsed data is then analyzed and interpreted to identify potential evidence that can be used in legal proceedings. This step involves using forensic techniques to correlate the data and identify potential connections between different pieces of evidence. For example, call logs and text messages can be analyzed to identify potential communication patterns between suspects.

4. REPORTING AND DOCUMENTATION

The final step in mobile forensic analysis involves documenting the findings and presenting them in a clear and concise manner. This step involves creating reports that summarize the key findings and include all relevant evidence. These reports must be accurate, thorough, and well-documented to ensure their admissibility in court.

In summary, mobile forensic analysis is a complex process that involves several steps, including data filtering and prioritization, data decoding and parsing, data analysis and interpretation, and reporting and documentation. By following these steps, mobile forensic examiners can extract relevant information from mobile devices that can be used in legal proceedings

5. LEGAL CONSIDERATIONS REGARDING CONTEMPORARY FORENSIC ANALYSIS

Forensic investigators must be familiar with the legal framework guiding the decryption of digital evidence since forensic data may be used as evidence in court. The following four historical legislative strategies have been used to provide law enforcement authorities with decryption capabilities: Exploiting vulnerabilities is just one of four options, along with extraordinary access, decryption orders, and cloud data access. This section goes into great detail about each strategy:

1. VULNERABILITY EXPLOITATION

Lawful hacking, which refers to the use of vulnerabilities in a system to gain access to data, has become a topic of interest for law enforcement agencies worldwide. However, it is important to note that such measures must be used as a last resort, and other less intrusive methods must be explored before resorting to hacking. Exploiting system vulnerabilities carries significant risks, such as potential privacy violations, data leakage, and threats to security. Moreover, the use of zero-day exploits—vulnerabilities that have not yet been found—which may create a market for vulnerabilities for law enforcement, may not follow the proportionality and subsidiarity rules. Therefore, it is crucial that legal framework that takes into account aspects like legal scope, deployment requirements, the creation and dissemination of penetration testing tools, accountability, the identification of vulnerabilities, and jurisdictional considerations control legitimate hacking. National laws on legal hacking offer certain protections for human rights and to stop police misuse of authority. These protections include judicial approval, setting time and crime type restrictions on the measure, and tight reporting and monitoring of legal hacking. Nonetheless, there are still issues with maintaining the accountability and openness of law enforcement organizations, notably with regard to vulnerability disclosure procedures.Several countries don't have a defined procedure for vulnerability disclosure, which might lead to undesirable actions like withholding vulnerabilities from providers or consumers in order to further exploit them for eavesdropping. In certain situations, forensic investigators can be given the authority to decide on legal matters, which could jeopardize civil liberties and rights. To ensure the preservation of human liberties and rights, a legal framework for legitimate hacking must be established. Such a framework should be designed to regulate the use of vulnerabilities for evidence acquisition, and should provide guidelines for the disclosure of vulnerabilities by law enforcement agencies. While the use of zero-day exploits should be limited to serious crimes or acts of terrorism, accessing evidence through the use of common vulnerabilities may be appropriate. Given the global consequences of such activities, a European Regulation or perhaps an International Convention may be more appropriate to address these issues.

2. EXCEPTIONAL ACCESS

There have been a number of methods suggested in the past for law enforcement authorities to access encrypted data, including backdoors in hardware and software, key escrow systems, and shoddy cryptographic algorithms. Key escrow makes it possible for private parties to covertly work with law enforcement and use a backdoor to decode communication. However, politicians and security professionals oppose these methods due to their possible detrimental effects on human rights, civil liberties, data protection, and privacy. Moreover, they may usher in a golden period of surveillance, weaken international security, and increase public vulnerability to criminal activity. Also, they demand high development costs. Backdoors and key escrow should therefore be prohibited, according to ENISA and EUROPOL's recommendations. Hence, for even forensic data extraction, technical cooperation between manufacturers of mobile devices and law enforcement organizations is improbable. Furthermore, the use of exceptional access and coerced disclosure presents significant legal and ethical concerns. Many view compelled disclosure, in which persons are forced to provide their encryption keys, to be a violation of the right against self-incrimination and the assumption of innocent until proven guilty. It is also criticized for being ineffectual because individuals can refuse to reveal their encryption keys or pretend to have forgotten them. Additionally, the evolution of exceptional access and compelled disclosure could lead to a slippery slope in which governments utilise these powers for purposes other than what they were intended for, such as political monitoring or dissent repression. This is especially problematic considering the global trend towards authoritarianism in many countries.

3. DECRYPTION ORDERS

Decryption orders are a legal strategy that deals with encryption issues in criminal investigations without needing special access. These orders give law enforcement agencies the power to demand information or cooperation from service providers or manufacturers, with penalties enacted for non-compliance. For instance, failure to disclose an encryption key may result in criminal charges in the UK and France, while failure to cooperate with law enforcement in Belgium may subject service providers to civil or even criminal liabilities. Although Norway's laws were updated in 2017 to allow for the use of biometrics to unlock devices, forcing suspects to reveal their passwords is still controversial and is likely to only be used in extreme cases due to concerns over self-incrimination, the privilege of staying silent, and abuse of government power. Yet, because it is uncertain how providers can adhere to demands to decipher communication without backdoors, decryption orders for collaboration with makers or providers can have significant privacy and security ramifications. Although in-house digital forensics by suppliers and manufacturers is also in question, law enforcement may only be supplied encrypted data without knowledge of the forensic technology used, its trustworthiness, or the accuracy of the results.

4. CLOUD DATA ACCESS

A US law known as the CLOUD Act enables foreign governments with whom the US government has bilateral agreements to oblige US-based Cloud Service Providers (CSPs) to reveal stored data or intercept communications. The law, however, does not require providers to be able to decode the data. This means that law enforcement will need to use additional methods to decode the data if the provider is unable to determine its plain text content. A regulation on European Production and Preservation Orders for electronic evidence in criminal proceedings is currently under consideration by the EU, although it has been delayed for two years due to concerns from the European data protection board about the absence of protections. In light of the difficulties inherent in establishing an EU-based e-evidence system, the EU Commission is seeking an agreement on cross-border access to digital evidence with the US. The CLOUD Act, on the other hand, has come under fire for its unclear definitions of digital evidence, data categories, and the types of "severe offenses" that necessitate cloud access, lack of judicial review, low protection of privacy, and lack of protection of procedural rights. Due to remote acquisition, reliance on CSP help, loss of volatile data in virtual machines, and encryption, cloud forensics also faces reliability problems. An international convention is required to govern encryption, cloud data access, and the sharing of digital evidence in accordance with universally recognized digital forensic standards. Aside from the difficulties associated with authorized access to encrypted data, there are also worries about the misuse of such access by governments or their agents. The Snowden leaks in 2013 revealed that the US government had exploited extraordinary access to spy on individuals and organizations with little oversight or accountability. Furthermore, the usage of backdoors or poor encryption techniques for extraordinary access could create weaknesses that bad actors, such as criminal groups and hostile governments, could exploit. This was proved in 2017, when a cyber-attack that took use of a weakness generated by the NSA's use of a backdoor in Microsoft software caused extensive harm, notably to hospitals in

the United Kingdom.

6. CONCLUSION:

The paper proposes a comprehensive understanding of the impact of encryption on the forensic analysis of mobile devices and the need for new forensic methods to overcome the challenges posed by encryption in modern mobile devices. In addition to exploring the increasing usage of encryption and other security mechanisms in mobile devices, the article also looks at how these security features have an influence on the traditional methods employed in mobile device forensic data collecting. The main methods of manual or logical data extraction from smartphones used in forensic investigations are described in the paper, along with the drawbacks of these methods and numerous approaches to accessing user data on locked and encrypted devices. Additionally, the paper discusses different forensic analysis processes, including data filtering and prioritizing, data decoding and parsing, data analysis and interpretation, and reporting and documentation. Overall, the paper highlights the importance of mobile forensic analysis in legal proceedings and emphasizes the need for forensic examiners to have a clear understanding of the legal and technical requirements for accessing and analyzing mobile device data. The use of encryption and other security measures is one of the key difficulties in mobile device forensics. It is difficult for forensic investigators to retrieve evidence from mobile devices since the encryption is employed to safeguard sensitive data on these devices from unwanted access. Forensic investigators now face greater difficulties when attempting to retrieve data from mobile devices due to the manufacturers' increased emphasis on security in recent years. As a result, new forensic methods and tools have been created that are intended to get beyond encryption and other security features in mobile devices. The quick development of mobile technology presents another difficulty for mobile device forensics. New types of mobile devices are regularly released, and their design is continuously changing. These devices are equipped with new features, more powerful hardware, and increased security measures. As a result, forensic examiners must constantly adapt to keep up with these changes. They must always come up with new ways to retrieve information from the newest mobile devices and stay current with the tools and techniques available. Additionally, when new procedures or tools are required, forensics experts must be capable of recognizing the constraints of their current approaches and be ready to create them.

REFERENCES

1. Abraha, H.H., 2019. How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis. International Data Privacy Law 9, 207-215. https://doi.org/10.1093/idpl/ipz009.
2. Al-Dhaqm, A., Razak, S., Ikuesan, R.A., Kebande, V.R., 2020. A review of mobile forensic investigation process models. IEEE access, 1-1.
3. Alendal, G., Dyrkolbotn, G.O., Axelsson, S., 2018. Forensics acquisition and analysis and circumvention of samsung secure boot enforced common criteria mode. Digit. Invest. 24, S60-S67. https://doi.org/10.1016/j.diin.2018.01.008.
4. Apple, 2020. Apple platform security. https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf.
5. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). Simon and speck: block ciphers for the internet of things, IACR Cryptol. ePrint Arch 2015, 585.
6. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics. National Institute of Standards and Technology.
7. UT Austin ISO Blog. (2015). Android 5.x lockscreen bypass (cve-2015-3860). Retrieved from https://sites.utexas.edu/iso/2015/09/15/android-5-lockscreen-bypass/.
8. Hargreaves, C., & Chivers, H. (2008). Recovery of encryption keys from memory using a linear scan. In: 2008 Third International Conference on Availability, Reliability and Security, pp. 1369e1376. https://doi.org/10.1109/ARES.2008.109.
9. Heckmann, T., Markantonakis, K., Naccache, D., & Souvignet, T. (2018). Forensic smartphone analysis using adhesives: transplantation of package on package components. Digit. Invest. 26, 29e39. https://doi.org/10.1016/j.diin.2018.05.005.
10. Hargreaves, C., & Chivers, H. (2008). Recovery of encryption keys from memory using a linear scan. In: 2008 Third International Conference on Availability, Reliability and Security, pp. 1369e1376. https://doi.org/10.1109/ARES.2008.109.