IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Unravelling the Unpredictability of Mobile Forensics: A Comprehensive Case Study

Ashmit Sharma[1]

[1]Lead Forensic Analyst, Sardar Vallabhbhai Patel National Police Academy, Ministry of Home Affairs, GOI

Abstract: Mobile phones have become an indispensable tool in today's modern world. In criminal investigations, digital evidence plays a crucial role, and as law enforcement officials, we understand the significance of preserving data integrity. Given the vulnerabilities of mobile phones to various external threats, we adhere to specific protocols to ensure the extraction of data from mobile devices without tampering with the original hash values. Court-approved tools such as UFED4PC and Oxygen Forensics are utilized to extract data, while physical extraction remains the ideal method in mobile forensics. However, due to the increasing levels of encryption, obtaining physical extraction from the latest smartphones, which employ File-Based Encryption (FBE), has become nearly impossible. Nevertheless, in some cases, chipset-based full file system extraction can be achieved, aiding in the recovery of deleted data from smartphones. This paper shares the author's experience in attempting to extract data from two devices of the same make and model but with different Android OS version and Security Patch, leading to unexpected results during the full file system extraction. The insights provided in this paper will assist other digital forensic experts in similar data extraction scenarios and also aid mobile phone manufacturers in refining their firmware.

Keywords: Mobile Forensics, Security Patch, File-Based Encryption (FBE), Android OS, One Plus etc

[1]***Corresponding Author**: (Lead Forensic Analyst, Sardar Vallabhbhai Patel National Police Academy, Ministry of Home Affairs, Govt. Of India)

I. Introduction

Mobile phones have become an indispensable aspect of modern life, serving not only as communication devices but also as repositories of highly personal and sensitive information. Consequently, the analysis of mobile devices and their data plays a critical role in criminal investigations and digital forensics, aiding in the discovery of evidence and resolution of cases. However, mobile forensic investigators encounter significant challenges due to the rapidly evolving nature of mobile device technology, particularly in the realm of Android devices.

Android, (1) being the most prevalent mobile operating system, undergoes frequent updates and security patches released by Google. Security patches, (2) in particular, are crucial for addressing security vulnerabilities and protecting user data. They are released periodically to address known security risks, vulnerabilities, and exploits that could potentially be leveraged by malicious actors. By promptly installing these security patches, users can minimize their exposure to security threats and ensure a safer mobile experience.

The advent of File-Based Encryption (FBE) in recent Android (3) versions has significantly elevated the level of complexity in extracting data from encrypted devices, particularly when employing physical extraction methods.

This paper presents a compelling case study in which the author encountered unexpected outcomes during a full file system extraction from two devices of identical make and model but featuring different Android OS versions and security patch levels. This case study offers valuable insights into the intricate complexities and implications of Android updates within the realm of mobile forensics.

By sharing experiences and lessons learned from grappling with the impact of Android updates, this paper aims to assist both forensic investigators and mobile forensics tool manufacturers in refining their methodologies and firmware. This refinement is essential for ensuring the effective extraction and preservation of digital evidence, ultimately advancing the field of mobile forensics in its pursuit of truth and justice.

II. Materials and Methods

Android operating system developed by Google powers millions of devices worldwide, offering a user-friendly interface and a vast ecosystem of applications. As an operating system, Android provides the foundation for device functionality, managing hardware resources and enabling various software components to work together seamlessly.

This case study reveals intriguing findings where a mobile phone, denoted as Fig-I, was submitted to the laboratory for forensic examination as part of a criminal investigation. The device in question belongs to the OnePlus brand, with a specific model identified as AC2001. It operated on Android 10 as the operating system (OS), with a recorded security patch level of 2020-12-01.

Of notable interest is the comparison between Fig-I and another mobile phone owned by the author, which shares the same make and model. However, this second device diverges from Fig-I in terms of the OS version and security patch applied (referred to as Fig-II in the study). This discrepancy presents a unique opportunity for analysis, as it allows for an investigation into the potential implications and effects of differing software configurations on forensic examinations.

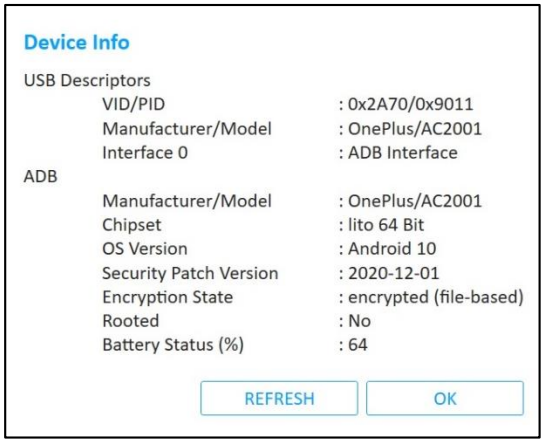

Fig-I

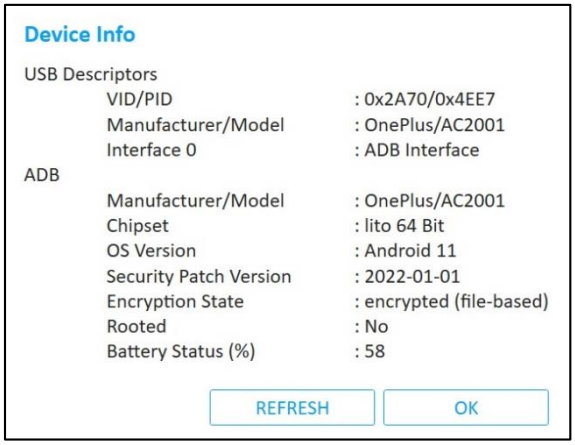

Fig-II

In this case study, the Cellebrite UFED4PC tool, widely recognized in the field of mobile forensics, was utilized to extract the details from the mobile devices under examination. Notably, the mobile phone presented as the crime exhibit (referred to as Fig-I) remained isolated and therefore could not be regularly updated. On the other hand, the author's mobile phone received regular updates, implying that it would likely possess better security measures and patch fixes.

Given this context, it became evident that physical extraction was not feasible for either device, as both implemented file-based encryption. Consequently, the next viable extraction method was full file system extraction (4). This approach not only facilitates the retrieval of logical data and data files but also offers the potential to recover deleted content.

Upon performing full file system extraction on both devices, the results were astonishingly contradictory to expectations. It was anticipated that the crime exhibit, with its older OS version and security patch, would yield a greater amount of recoverable data compared to the author's regularly updated mobile phone. However, the actual outcomes proved to be quite the opposite.

The crime exhibit posed challenges in terms of accessing its memory (Fig-III) and extracting potential evidence. The older OS version and security patch implemented on the device hindered effective debugging and extraction processes. In contrast, the author's mobile phone, benefiting from regular updates, granted smooth access to its memory, allowing for successful full file system extraction (Fig-IV).

Fig-III

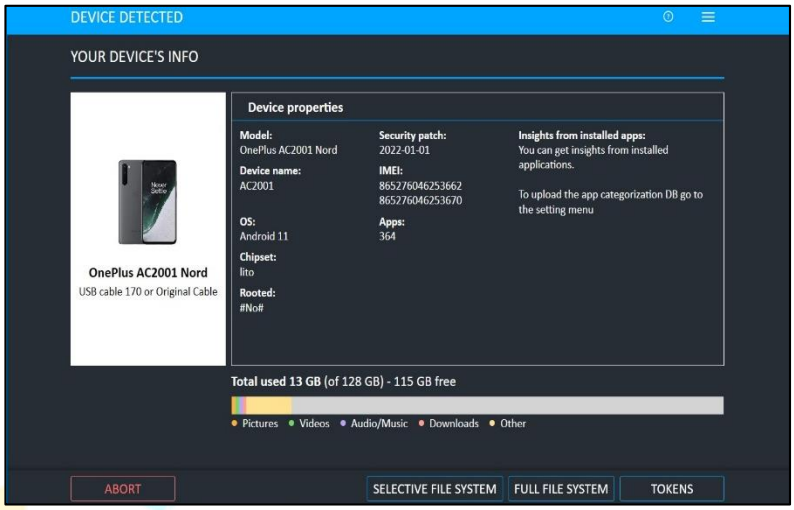

Fig-IV

III. Conclusion and Discussions

Despite the diligent application of regular updates to mobile phones, it is crucial to acknowledge that ensuring absolute security is not always assured. Although these updates are designed to address known vulnerabilities and bolster overall device security, they can inadvertently introduce fresh issues that were previously resolved in earlier iterations. This dynamic nature of updates creates an unpredictable landscape for mobile forensics.

In the realm of mobile forensics, the task of extracting and analyzing digital evidence from mobile devices can be highly unpredictable. Each mobile device presents a unique set of challenges and complexities, making it difficult to predict the outcome of forensic examinations. Factors such as device make and model, operating system version, security patches, and encryption mechanisms can significantly impact the success and scope of forensic investigations.

Furthermore, the evolution of mobile technology, including advancements in encryption methods and security features, adds to the unpredictability of mobile forensics. As manufacturers implement stronger security measures, such as file-based encryption and secure boot, the traditional methods of physical extraction and data recovery become increasingly challenging. Mobile forensic experts must constantly adapt their techniques and tools to keep pace with these advancements.

In essence, while regular updates confer a significant layer of security to mobile phones, they do not guarantee absolute invulnerability. It is incumbent upon users to proactively implement comprehensive security measures and embrace a multifaceted strategy to mitigate risks and safeguard their devices and personal information. Likewise, mobile forensic investigators must remain adaptable and continually update their knowledge and techniques to navigate the unpredictable landscape of mobile forensics.

IV. References

1. Anindya Sen, Jyotsna Dei: Investigation on Trends of Mobile Operating Systems

2. Vincent F. Taylor, Ivan Martinovic: To Update or Not to Update: Insights from a Two-Year Study of Android App Evolution

3. Ronan Loftus, Marwin Baumann: Android 7 File Based Encryption and the Attacks Against It

4. Christos Sgaras, M-Tahar Kechadi & Nhien-An Le-Khac: Forensics Acquisition and Analysis of Instant Messaging and VoIP Application