Abstract – In recent years traditional mobile-phones, used only to make calls and send text messages, have evolved into even more versatile and powerful devices (SmartPhone, Tablet, etc.). These devices use a NAND flash memory type to store data, due to it being a memory that has been optimized for the fast updating of data. These flash memory drives contain sensitive data that could be a possible danger to the user’s privacy. This article proposes a new Anti-forensics technique for mobile devices with the Android OS. The technique makes it possible to modify and erase, safely and selectively, the digital evidence on an Android device without having to use any cryptographic primitives or make any file system changes. While the use of cryptographic primitives or changes to the file system create considerable suspicion in a forensic analysis, the proposed technique uses simple software tools commonly used in \* nix-like Operating Systems such as Android.

Index Terms – Digital Forensics; Mobile Forensics; Anti-Forensics; Mobile Anti-Forensics; Counter-Forensics; Android OS; Android Forensics; Android Anti-Forensics; Flash Memory; NAND; Secure Deletion; Sanitization.

I. INTRODUCTION

Gartner claimed [1] that in 2011 468 million mobile devices would be sold, i.e. 57.7% more than last year. In addition, according to the same research agency, in 2012 there will be 632 million smartphones in the world and in 2015, 1.1 billion. In 2012, half (49.2%) of the 632 million smartphones in circulation will work on the Android OS.

The data stored in a smartphone can be a threat to the user’s privacy. It is worth recalling that a classic mobile phone contains a large amount of private information (contacts, text messages, call lists). Additional sensitive information stored on smartphones includes e-mails, websites visited, chat messages, geo-location information, etc.. All this information can give a well-defined profile of its user in order to reconstruct his actions at a specific time. An individual who wants to protect his privacy and in particular delete or modify in a safe and selective way any digital evidence stored on the smartphone can use anti-forensics techniques.

A definition of anti-forensics, according to [2], is “...we will consider anti-forensics to be any attempts to compromise the availability or usefulness of evidence to the forensics process. Compromising evidence availability includes any attempts to prevent evidence from existing, hiding existing evidence or otherwise manipulating evidence to ensure that it is no longer within reach of the investigator. Usefulness maybe compromised by obliterating the evidence itself or by destroying its integrity.”.

While there are currently no papers dealing with the problem of secure modification in flash memories (to the best of the authors’ knowledge), several studies have proposed techniques for the secure erasing of NAND flash memory drives that are commonly used in smartphones.

Flash memory drives (NANDs) differ from hard drives in both the technology used to store data (flash chips vs. magnetic disks) as well as the algorithms used to manage and access the data. NANDs maintain a layer of indirection between the logical block addresses that computer systems use to access data and the raw flash addresses that identify physical storage. The layer of indirection enhances NAND performance and reliability by hiding the idiosyncratic interface of the flash memory and managing its limited lifetime. However, it can also produce copies of the data that are invisible to the user but that a smart attacker can recover. The differences between NANDs and hard drives make it uncertain whether techniques and commands developed for hard drives will be effective on NANDs.

In [3] and [4], all the data is encrypted, each file has its own encryption key which is stored in the header of the file. When wanting to delete a single file, simply delete or overwrite the header. Encrypting the file system or modifying it in order to apply anti-forensics techniques creates a great of suspicion during a forensic analysis.

In [5], exploiting a security feature of Android, it is possible that digital evidence is hidden in private folder which is inaccessible to third-party applications. The private folder is a private directory, created when an application is installed, in which it is possible to save any file type (e.g., text files, multimedia files).

According to [5], when a given common Android application is uninstalled, the entire set of the related information, including data files and directories, is logically deleted from the File System.

This paper introduces a new Anti-Forensics technique for mobile devices running the Android OS that makes it possible to edit and delete, securely and selectively, the digital evidence generated by the Android OS by using simple software tools, without making changes to the file system and using any cryptographic primitives.

The paper is organized as follows: Section II briefly describes the Android OS, paying particular attention to the type of file system generally adopted by Android devices as well as the media storage (NAND) generally used. Section III contains the main forensic techniques used on Android devices. Section IV describes the proposed anti-forensics technique, while Section V describes the examples on Android devices, of these techniques that have been designed, implemented and tested. The conclusions are made in Section VI.