Digital Investigation 14 (2015) S68–S76

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2015 USA

New acquisition method based on firmware update protocols for Android smartphones

Seung Jei Yang[*], Jung Ho Choi, Ki Bom Kim, Taejoo Chang

The Affiliated Institute of ETRI, P.O. Box 1, Yuseong, Daejeon, 305-600, Republic of Korea

Keywords:
Android forensics
Android physical acquisition
Firmware update protocol
Flash memory read command
Bootloader

ABSTRACT

Android remains the dominant OS in the smartphone market even though the iOS share of the market increased during the iPhone 6 release period. As various types of Android smartphones are being launched in the market, forensic studies are being conducted to test data acquisition and analysis. However, since the application of new Android security technologies, it has become more difficult to acquire data using existing forensic methods. In order to address this problem, we propose a new acquisition method based on analyzing the firmware update protocols of Android smartphones. A physical acquisition of Android smartphones can be achieved using the flash memory read command by reverse engineering the firmware update protocol in the bootloader. Our experimental results demonstrate that the proposed method is superior to existing forensic methods in terms of the integrity guarantee, acquisition speed, and physical dump with screen-locked smartphones (USB debugging disabled).

Introduction

The Android OS accounted for approximately 84% of the market share in the third quarter of 2014 (Smartphone OS Market Share Q3 2014). The size of the Android smartphone market now exceeds that of the PC market and various technologies are emerging continuously for personal and business use (Bring your own device, 2014). This trend is increasing the importance of Android forensics, where research into the physical acquisition of flash memory is particularly necessary to aid the recovery and analysis of deleted files.

The existing Android physical acquisition methods have the following problems.

First, most forensic tools acquire data from smartphones by exploiting Android kernel vulnerabilities or using custom images (Rooting (Android OS), 2014; Vidas et al., 2011). However, these vulnerabilities have been patched as the Android OS has been upgraded and physical memory dumping is not supported in the latest OS until a new vulnerability can be found. Furthermore, the recent applications of security technologies (Secure boot, 2014; Samsung KNOX, 2014) make it even harder to acquire data from smartphones.

Second, the dump method based on changing the custom recovery image (Son et al., 2013) is the only approach that takes into account the integrity of the user data. However, this method cannot guarantee the integrity of the entire flash memory dump because it also flashes the custom recovery image.

Third, existing forensic tools use the Android Debug Bridge (ADB) protocol to acquire data from smartphones. Thus, it is difficult to acquire data when smartphones are locked by a pattern or user password (USB debugging disabled).

[*] Corresponding author. Tel.: +82 42 870 2343, +82 10 2321 4588; fax: +82 42 870 2222.
E-mail addresses: sjyang@nsr.re.kr, sjyangub@dreamwiz.com (S.J. Yang).

http://dx.doi.org/10.1016/j.diin.2015.05.008

In order to address these problems, we propose a new physical acquisition method based on analyzing the firmware update protocols of Android smartphones.

Related work

Software (S/W)-based and hardware (H/W)-based acquisition methods are mainly used to acquire data from Android smartphones.

The S/W-based acquisition methods are divided into logical acquisition and physical acquisition.

Logical acquisition methods acquire user data stored on a smartphone via ADB Backup (Android Backup Extractor, 2014) or Content Provider (Hoog, 2011). However, this method only retrieves stored files such as the call history and pictures, and it cannot recover deleted files.

Physical acquisition methods extract the overall data directly from the smartphone's flash memory after connecting a USB cable. To perform a physical dump of the flash memory, the rooting process required to obtain an administrative privilege must be performed first. The rooting-based acquisition studies were introduced in the scholarly works (Hoog, 2009; Lessard and Kessler, 2010). These studies discussed Android forensics, including acquisition methods that root the HTC smartphones and use ADB shell. However, these methods can only be used to acquire data when the USB debugging mode is enabled. Commercial forensic tools (Oxygen Forensics, 2014; AccessData MPE+, 2014; MSAB XRY, 2015) also use this method. However, because the rooting exploitation process is executed after the smartphone is booted; the integrity is damaged whenever data is acquired. In addition, existing rooting vulnerabilities are patched whenever the Android OS is updated with a new version; hence, a new rooting technique must be found whenever the Android OS is updated.

Cellebrite UFED 4PC (2015) basically supports an ADB physical memory dump via rooting exploitation, while some Samsung models support physical memory dumping via a custom bootloader. However, this method has the problem that each model has to upload a different bootloader rather than uploading a common loader for physical memory dump. Because the physical dump is not supported in some models in the same Galaxy series, this method is not regarded as stable.

An acquisition method based on changing the custom recovery image has been studied in the scholarly works (Vidas et al., 2011; Son et al., 2013). Use of the custom recovery image guarantees the integrity of the user data. However, this method cannot guarantee the integrity of the entire flash memory dump because it also flashes the custom recovery image. The acquisition method must have USB debugging enabled because it uses the ADB shell protocol to acquire data from smartphones. However, because USB debugging is usually disabled, this method is not applicable if the pattern lock or user password is set. Moreover, the Secure Boot and Samsung KNOX technologies applied recently to Android place restrictions on the flashing of custom images, which will make it difficult when using this acquisition method in the future.

Flasher tools (RIFF box, 2014; ORT tool, 2014; Z3X box, 2014) are also used to extract data from mobile devices. However, the main function of these tools is to fix the bricked phones that have S/W damages. So these tools are not considered as general forensic tools.

Representative H/W-based acquisition methods include JTAG-based acquisition (Kim et al., 2008; Breeuwsma et al., 2007) and Chip-off-based acquisition (Jovanovic, 2012). The JTAG-based acquisition method extracts data from the flash memory using the JTAG debug interface on the smartphone's PCB board. The Chip-off-based method physically removes flash memory chips from the PCB board of smartphones and acquires the raw data of the flash memory. The JTAG-based acquisition method is problematic because not all smartphones support JTAG and it takes a long time to acquire data. The Chip-off-based acquisition method is utilized in limited situations because it separates the flash memory.

Also, there were various studies conducted on Android forensics. As the capacity of the main memory grows in Android smartphones, the forensic research for volatile memory was introduced (Sylve et al., 2012). The analysis of social networking applications (Mutawa et al., 2012), the prototype enterprise monitoring system for Android smartphones (Grover, 2013), and the Kindle forensics (Hannay, 2011; Iqbal et al., 2013) were also studied.

Background

Flash memory is used mainly to store data on smartphones. Because the flash memory is small and it can store a large amount of data, it is used widely in embedded devices such as smartphones and feature phones. Recently embedded Multi-Media Card (eMMC) that integrates NAND flash and a controller into a package has been used; this manages stored data by efficiently using the EXTended file system 4 (EXT4). Moreover, it mounts and operates partitions such as BOOT, RECOVERY, SYSTEM, and USERDATA.

An administrative privilege must be obtained before the physical dump of the entire flash memory. Thus, a custom image is overwritten in the BOOT partition in order to obtain the administrative privilege, and an app (SuperUser.apk) and a binary (/system/su) are installed in the SYSTEM partition. In addition, the administrative privilege is obtained via rooting exploitation in the recovery mode or by exploiting vulnerabilities in the Android OS.

In general, Google's FASTBOOT (Android software development-fastboot, 2014) is used for flashing a custom image. Each manufacturer provides their own firmware update programs (Samsung Kies, 2014; Samsung Odin, 2014; LG Software & tools Download, 2014; Pantech Self-Upgrade, 2014; HTC Sync Manager, 2014; Sony PC Companion, 2014; Xiaomi Download MiFlash for Xiaomi Smartphone, 2015) in order to prevent the simple flashing through FASTBOOT provided by Google, and they do not publish a protocol so only the original firmware can flash. The firmware update process runs only when smartphones enter a special mode called firmware update, or the download mode. Only the bootloader and USB function can operate in this mode and a new system firmware can be flashed.