# Research on Android Anti-Forensic Tools

Ren-Jie Chen[1] Chung-Huang Yang[2]
[1]Graduate Institute of Information and computer Education
National Kaohsiung Normal University, Taiwan
s491140601@hotmail.com
[2]Graduate Institute of Information and computer Education
National Kaohsiung Normal University, Taiwan
chyang@nknucc.nknu.edu.tw

## Abstract

This paper focus on destroying evidence in anti-forensics technology, and develops a deleting tool with Java and Android SDK (Software Development Kit) to delete the files and information in Android smart phones, purposes to reduce possibility of sensitive information leakage, and provides a counterexample to the mobile forensic tool developers.

**Keywords:** Smart phone; Android; Mobile forensics; Anti-forensics

# Research on Android Anti-Forensic Tools

## 1 INTRODUCTION

With the advancement of technology, whether in business or entertainment, mobile phone has became an indispensable item in recent years. Growth of technology makes smart phones become the mainstream of mobile phone, and Android is a prominent one of them. People can now handle lots of things what they handled with computer in the past with smart phones, including transfer and video conference, but in the device, they may leave some information around the user what can be acquired via some programs.

In addition to these programs, some forensic or management tools can easily acquire personal information such as photo, browser history, contacts, call logs or SMS (Short Message Service) in the device, and then cause economy or reputational losses of the user (Zhou, Zhang, Jiang and Freeh, 2011), even though some users might make a spontaneous data deletion. To prevent leaks of information, recovery is effectual, but it removes custom applications and is inconvenient to use.

In this research we develop a tools with Android SDK, purpose to achieve data protection by deleting information stored in the smart phone, and make sure it won't be acquired by attacker.

## 2 RELATED WORK

In this research we focus on destroying evidence in anti-forensics and operate in the Android environment. The following literature reviews are based on relevant terms that be mentioned in this research.

### 2.1 Smart Phone

Smart phones equip with voice communication, PIM (Personal Information management) application, faster processing speed and larger space for data storing, they can provide users with personal computer-like functions as internet connection, e-mail, installing and executing external application. Common system includes Symbian, Windows Mobile, iOS, Android, and BlackBerry OS.

### 2.2 Android

Android is a system of smart phones, developed by OHA (Open Handset Alliance) in 2007, the latest version on mobile phones is v2.4, and v3.2 on tablet PC.

Since using Linux as a core, Android must be ruled by LGPL (Lesser General Public License) to meet the standards of open-source and free. With Java and Android SDK, the feature that developers have the freedom of programming and releasing makes lots of people invest in program developing. Owing costless developmental environment and free platform for sharing causes Android applications increase steadily since 2009 (Android Lib, 2011), and the

survey by Canalys shows that Android's market share approach 50% since the second quarter of 2011 (Canalys, 2011).

The major components of Android OS are shown in Figure 1, known as Linux kernel, Libraries and Android Runtime, Application Framework and Application (Android developers – Device Guido, 2011), and will be described in detail in following contents respectively.

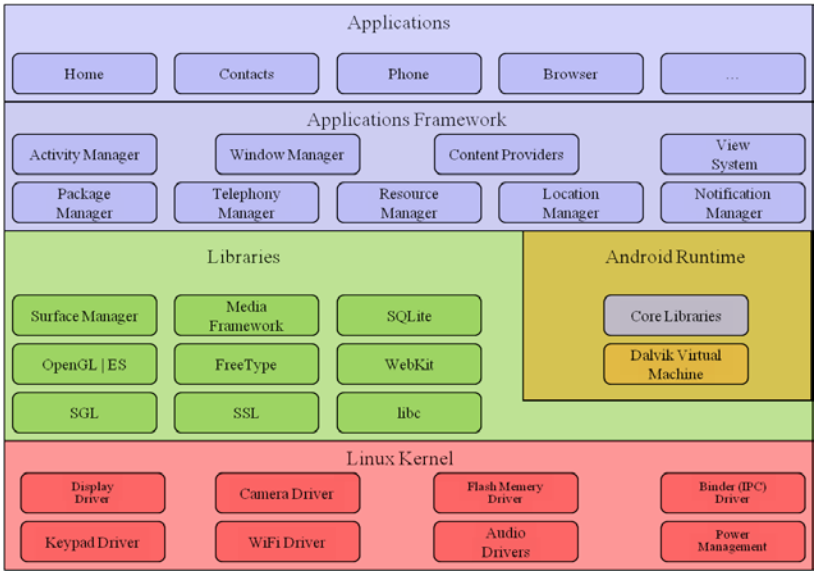


**Figure 1. Android Architecture**

### 2.2.1 Linux kernel

Android OS uses Linux kernel v2.6 as a core system to provide services such as security, memory management, network stack and driver model, and applications can execute on it.

### 2.2.2 Libraries and android runtime

Android includes a set of C/C++ libraries that provide services through the Android application framework and execute on Android runtime. Android runtime includes Dalvik virtual machine, gets excellent evaluation in the high-speed usage of memory and high performance on low-speed CPU. Every application will have an independent Dalvik virtual machine and execute on it.

### 2.2.3 Application framework

An API (Application programming interface) framework for writing core applications, purposes to simplify the structure of program development and accelerate the process.

### 2.2.4 Application

Applications are variety programs written with Java programming language and execute on virtual machine, and some of them has been bound in Android OS since developing.

### 2.3 Mobile Forensics

With the advancement of the functions, information in mobile phones includes not only text but also videos, music, pictures and other files which contain lots of personal information and mobile forensics means to preserve, acquire, examine and analyze the data in a standard way, and report the digital evidence on devices.

According to the guidelines of NIST (National Institute of Standards and Technology), the process of digital forensics should comply the standards of the operational process such as preservation, acquisition, examination and analysis, and reporting (Jansen and Ayers, 2007).

Common forensic tools can be divided into software tools and hardware toolboxes, and software tools such as Android Forensics, MOBILedit! Forensics, Oxygen Forensic Suite and kinds of mobile phone management tools such as MobileGo and WanDouJia that are executed on computers and connect phones with USB, Bluetooth or infrared, acquire data on phones and transfer them back to computers.

Hardware toolboxes are mostly commodities such as UFED Physical Pro and XRY, achieving forensics with various cables, SIM card reader and other tools in toolboxes.

### 2.4 Anti-Forensics

Anti-forensics means the methods, tools or techniques that impede the process and effect of forensics, and purpose to make negative impacts on the existence, quantity or quality of acquired digital evidences, or impede the examination and analysis (Kessler, 2007).

Techniques of anti-forensics can be divided into Destroying evidence, Hiding evidence, Eliminating evidence sources and Counterfeiting evidence (Distefano et al.,2010), and will be described in detail in following contents respectively.

#### 2.4.1 Destroying evidence

Destroying evidence such as wipe, overwriting and physical destruction means to destroy the sensitive information and make it can’t be read in the investigation.

#### 2.4.2 Hiding evidence

Hiding evidence such as steganography, data hiding and encryption means to hide the sensitive information in various ways, and reduces the quantity of digital evidences.

#### 2.4.3 Eliminating evidence sources

Eliminating evidence sources means to keep the sensitive information constant and modifies sources of the sensitive information selectively to impede the acquisition of investigation.

#### 2.4.4 Counterfeiting evidence

Counterfeiting evidence means to modify the attributes such as content, type or access time to reduce the sensitivity of information, and purpose to make investigators ignore the modified

information.

# 3 CURRENT AND TECHNOLOGY ABOUT ANTI-FORENSICS

The initial definition of anti-forensics means to delete or destroy evidences to invalidate the methods of forensics, and targets on the evidential data only. With the growth and procedure of forensics, anti-forensics changes to target on each phase of forensics to impede the formations of the evidences chain, makes the information suspected, destroys the data that are acquired by investigators, reduces the quantity and quality of the sensitive information, cleans the evidential information in the system or extends the period of investigation to reduce the efficiency, and increases the difficulty and cost of forensics (Distefano et al., 2010) (Zhang et al., 2007).

In the past, anti-forensics targeted on escaping from the security detections and invading the system, and left lots of neglected information that had been applied to forensic investigation in recent years. Therefore, computer crimes tended to have a well prepared when they were tracked and cleaned up the residual information in the device of the target and attacker both. With the advancement, anti-forensics began to be applied to other areas and brought negative impacts such as modification or destruction of evidence might release a guilty one, and counterfeiting evidence might implicate a innocent one and cause the investigation more difficult; but in the positive side, these techniques such as data hiding might be applied to ensure that no leakage of important data such as personal information or commercial confidentiality, and analyses of the process and method could be useful references for the technique and performance of forensic tools (Kessler, G. C., 2007) ( Zhang et al., 2007).

Some methods of anti-forensics will be described in detail in following contents respectively (Garfinkel, 2007).

## 3.1 Overwriting

Overwriting means to cover blocks that have been written before with a large number of data randomly and makes the original data substituted and unable to acquire. This method can be applied to general data and metadata, and is divided into overwriting the entire media, the individual files and files that were previously deleted but left on the drive.

## 3.2 Wipe

Wipe means to overwrite several times or demagnetize the disk to make the data recovery too costly to achieve. Wipe generally means Department of Defense 5220-22.M (overwriting for three times), German VISITR Standard (overwriting for seven times) or Peter Gutmann’s Algorithm (overwriting for thirty-five times), and Peter Gutmann’s Algorithm has the best result of the three.

## 3.3 Physical Destruction

Physical destruction means to destroy the hard disk with irreversible methods such as cutting,

scratch, drilling and bend to ensure that track is incomplete or distortion and can't be read.

### 3.4 Steganography

Steganography is a skill of writing hidden messages in a cover file and ensure that no one besides the intended recipient. Cover files are usually multimedia files such as JEPG, MBP, MP3, WAV and AU files. Steganography troubles investigators a lot, and is applied to carry malware to invade one's computer, however the method can only act on one file at the same time and be limited by time spending.

### 3.5 Data Hiding

Data hiding does not hide messages in a visible file, but hides them in unallocated or unreachable locations that are ignored by investigators and current forensic tools. Using tools that act on comparing the size of entire partition with existing files can discover the hidden files.

### 3.6 Encryption

Encryption means to change and store data or files into a status that can't be read directly through encryption algorithm or tools, and have to decrypts them if needing to read contents (Distefano et al., 2010). Encrypted files can't be accessed if the visitors don't have the key or password and destroying the unique key may trouble the investigation a lot. Although encryption is effective in hiding evidences, encrypted files are prominent and easily detected.

## 4 SYSTEM ARCHITECTURE AND IMPLEMENTATION

### 4.1 System Architecture

In this research, we develop an anti-forensics application and execute it on Android mobile phone to delete the data in the device such as contacts, call logs, SMS, browser history and photos logically. We use tools such as Oxygen (Trail), MOBILedit! Forensic or MobileGo to acquire the data in device before we delete it, and do it again after deleting, than we compare the two results to verify that the tool is valid or not. The system architecture is shown in Figure 2.

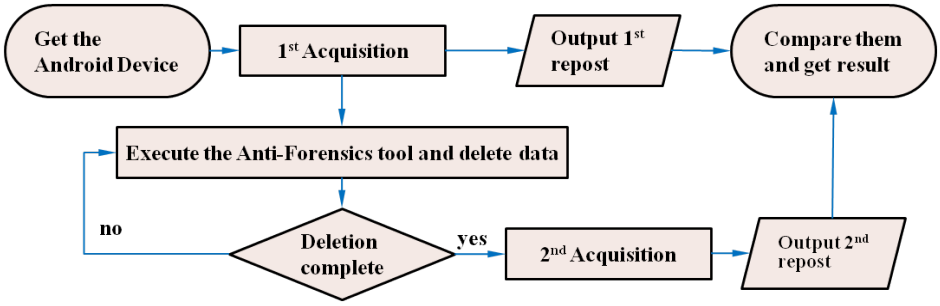


**Figure 2. Research Flowchart**

## 4.2 System Implementation

### 4.2.1 Developmental tools and environment

In this research we develop the anti-forensic tool with Java and Android API, and purpose to achieve a preliminary information protection by deleting the information in the device logically. The developmental tools and environment are showed in Table 1.

**Table 1. Development tools and environment**

| | |
|---|---|
| Developmental environment | Windows 7 |
| Developmental tools | 1. Eclipse 3.6<br>2. Android SDK |
| Programming language | Java |
| Devices for testing | 1. LG P500<br>2. HTC Desire |
| Tools for testing | 1. Oxygen(Trial)<br>2. MobileGo<br>3. MOBILedit Forensic |

### 4.2.2 System functions and interface

The tool we develop with Java and Android API in this research has five functions to delete the data such as contacts, call logs, SMS, browser history and photos logically and the function menu is shown in Figure 3.

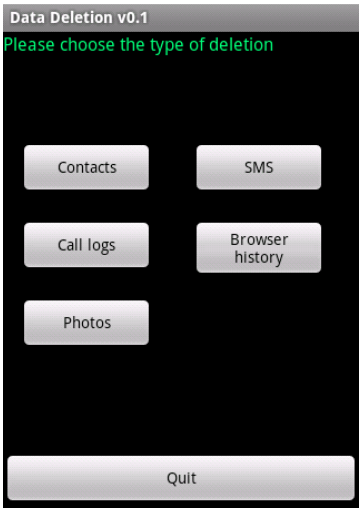


**Figure 3. Function menu**


**Figure 4. Contacts deletion**

When pressing the “contacts” button, the tool shows contacts that are stored in the device as a list (shown in Figure 4). Pressing any contact will activate a dialog to make a confirmation of deletion.

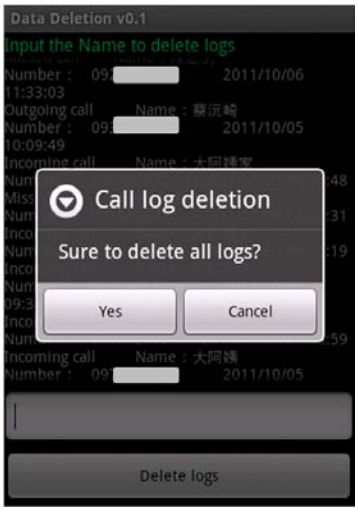


**Figure 5. Call logs deletion**

When pressing the “Call Logs” button, the tool shows the information of logs such as types, caller’s name, phone number and date as a text (shown in Figure 5) and sorts them with descending date. Users can delete logs of the caller by input the one’s name.


**Figure 6. SMS deletion**

When pressing the “SMS” button, the tool show the information of SMS such as type, sent time, sender and body as a test (shown in Figure 6) and sorts them with descending date. Users can delete a SMS message by input it’s ID.


**Figure 7. Photos deletion**

In photo deletion, we overwrite a part of Adapter method to show the photos in Gallery (shown in Figure 7) and the users can delete any of them by pressing the button ”delete” below the photo.

These functions can also delete all data in the device at one-time by pressing the “Delete all” button in the optional menu.

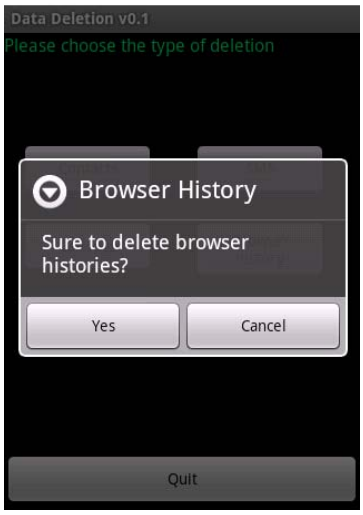


**Figure 8. Browser history deletion**

When pressing the “Browser” button, tools will achieve a dialog to make a confirmation of deleting all browser histories in the device (shown in Figure 8).

### 4.2.3 System Operation

In this research we implement deletions of data in the device to deduce the possibility of data leakage. To verify the result of data deletion is valid or not, we acquire the data before deletion and get the first report (shown in Figure 9).

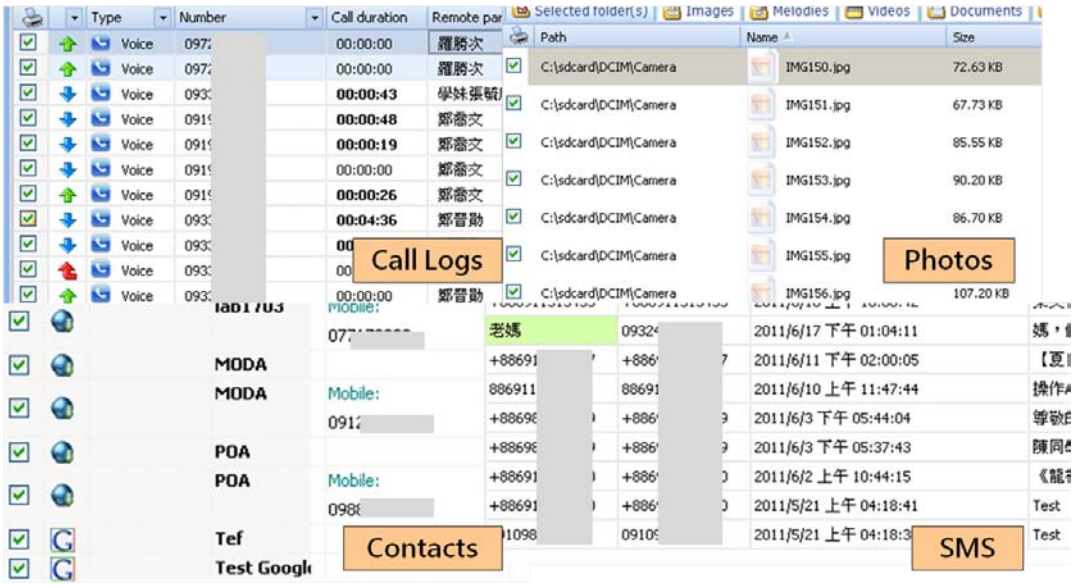


**Figure 9. Data acquisition (before deletion)**

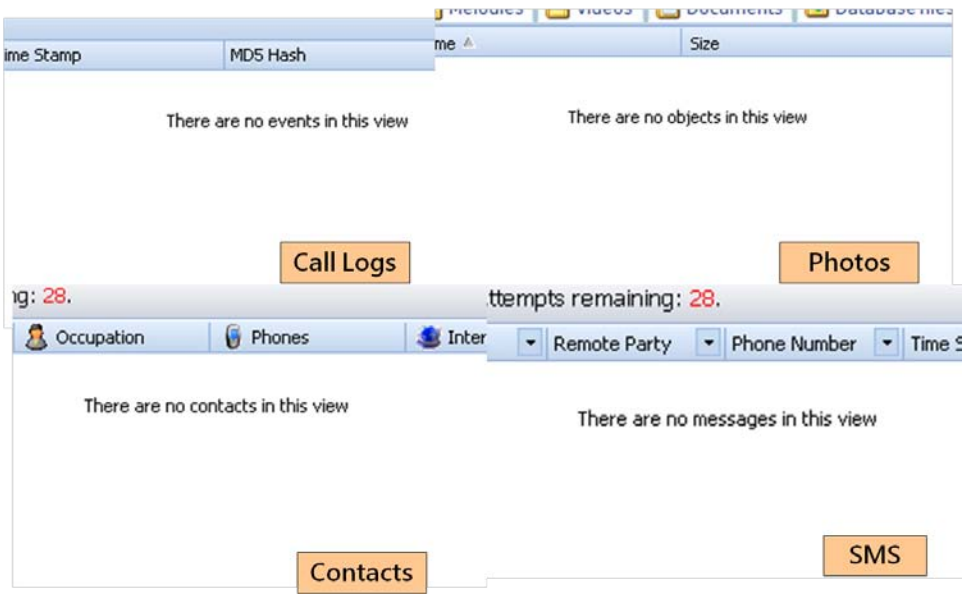


**Figure 10. Data acquisition (after deletion)**

After acquiring, we delete the data in the device with the function "Delete all" and then we take an acquisition of data again to get the second report (shown in Figure 10). According to the reports, we can find that there are no acquisitions in the second report and it shows that the method of logical deletion which we raise in this research is valid.

## 5 CONCLUSION

Most of the existing open source or trial forensic and management tools acquire data logically. Tool users execute applications on mobile phones, acquire data and transport them to computers for examination, analyzing and showing reports. In this research, we develop an anti-forensics application with Java and Android API, execute it on Android mobile phone to delete the data in the device such as contacts, call logs, SMS, browser history and photos logically. We successfully ensure that tools that acquire data through a logical way won't be effective to acquire the deleted data and it is valid to reduce the personal information leakages.

### References

1. Android developers – Device Guido "What is Android?," http://developer.android.com/guide/basics/what-is-android.html, 12-AUG-2011.
2. Android Lib "Number of New Applications in Android Market by month," http://www.androlib.com/appstats.aspx, 12-AUG-2011.
3. Canalys "Android takes almost 50% share of worldwide smart phone market," http://www.canalys.com/newsroom/android-takes-almost-50-share-worldwide-smart-phone-market, 12-AUG-2011.
4. Distefano, A., Me, G., and Pace, F. "Android anti-forensics through a local paradigm," Digital Investigation, May, 2010, s83-s94.

5. Erasani, S. “Implementation of Anti-Forensic Mechanisms and Testing with Forensic Methods,” Texas A&M University, Corpus Christi, U.S.A., 2010.
6. Garfinkel. S. “Anti-Forensics: Techniques, Detection and Countermeasures,” 2nd International Conference on i-Warfare and Security, MAR., 2007, pp77-84.
7. Jansen, W. and Ayers, R. “Guidelines on Cell Phone Forensics,” NIST, May, 2007, SP 800-101.
8. Kessler, G. C. “Anti-Forensics and the Digital Investigator,” Proceedings of the 5th Australian Digital Forensics Conference, DEC., 2007, pp.1-7.
9. NIST “Smart Phone Tool Specification,” http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf, 10-SEP-2011.
10. Youdong Zhang, Jiandong Wang, Wujia Zhu “Research on Computer anti-forensics,” Journal of Hohai University (Natural Sciences), JAN., 2007, 35(1):104-107.
11. Yajin Zhou, Xinwen Zhang, Xuxian Jiang and Freeh, Vincent W. “Taming Information-Stealing Smartphone Applications (on Android)” 4th International Conference on Trust and Trustworthy Computing, JUN., 2011, 93-107.

# Android 手機端的反鑑識工具研究

陳仁傑[1]　　楊中皇[2]

[1]高雄師範大學資訊教育學系 s491140601@hotmail.com

[2]高雄師範大學資訊教育學系 chyang@nknucc.nknu.edu.tw

## 摘要

本研究針對反鑑識技術中抹除證據的部分，利用 Java 與 Android SDK(Software Development Kit)開發一個資料刪除工具，對 Android 智慧型手機內的檔案資料進行刪除，以降低敏感性資訊外洩的可能性，同時可作為鑑識技術的反面例證，以供鑑識工具開發人員作為參考。

**關鍵字：**智慧型手機；Android；手機鑑識；反鑑識