THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 10 | Number 4 Article 3

2015

Data Extraction on MTK-based Android Mobile Phone Forensics

Joe Kong
The University of Hong Kong

Follow this and additional works at: http://commons.erau.edu/jdfsl

 Part of the Computer Law Commons, and the Information Security Commons

Recommended Citation
Kong, Joe (2015) "Data Extraction on MTK-based Android Mobile Phone Forensics," *Journal of Digital Forensics, Security and Law*: Vol. 10 : No. 4 , Article 3.
DOI: https://doi.org/10.15394/jdfsl.2015.1209
Available at: http://commons.erau.edu/jdfsl/vol10/iss4/3

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE Aeronautical University SCHOLARLY COMMONS

(c)ADFSL

DATA EXTRACTION ON MTK-BASED ANDROID MOBILE PHONE FORENSICS

Joe Kong
Mphil Student in Computer Science
The University of Hong Kong
jkongyc@connect.hku.hk

ABSTRACT

In conducting criminal investigations it is quite common that forensic examiners need to recover evidentiary data from smartphones used by offenders. However, examiners encountered difficulties in acquiring complete memory dump from MTK Android phones, a popular brand of smartphones, due to a lack of technical knowledge on the phone architecture and that system manuals are not always available. This research will perform tests to capture data from MTK Android phone by applying selected forensic tools and compare their effectiveness by analyzing the extracted results. It is anticipated that a generic extraction tool, once identified, can be used on different brands of smartphones equipped with the same CPU chipset.

Keywords: Mobile forensics, MTK Android phones, Android forensics, physical extraction, flash memory, MT6582

1. INTRODUCTION

Smartphones are frequently used in cyber-crimes or by offenders for coordinating their criminal activities as the device allows users to perform online communication and store personal or commercial information and data such as messages, emails, documents, photographs, videos, GPS locations, etc. in a concentrated and portable form. Customized applications can also be downloaded and installed into smartphones to extend their functionalities.

MediaTek ("MTK") Android phones are frequently used in crime cases [1][2] because of its low selling price and high price / performance ratios of the CPU. The existing extraction tools, however, can only handle a limited number of MTK Android phones and the latest models are often not included [3]. This research attempts to explore a generic forensic tool that is applicable to these phone models and set up standard operational procedures for its implementation.

1.1 The Current Problem

Low and mid-range China-branded Android phones are growing popular in the Asian market. In this research paper extraction performance tests are conducted on the quad-core MT6582 processor [4], a processor chip which is used in more than 140 Android phone models [5].

Apparently live memory extraction and analysis is crucial to forensic examinations. Unlike examining a desktop or laptop computer, examiners may inadvertently modify the original device when capturing a full forensic image for data analysis as a mobile device does not have a standalone hard drive which can be shut down and disassemble from the phone without altering the data stored

© 2015 ADFSL

therein. For Android phones the extraction process is even more complicated owing to its ever-changing proprietary hardware as well as the vast variety of applications and security settings. Besides, Android versions, which users can download them from Google, are constantly updated. Thus examiners will need to carry out extensive testing and validation on the latest forensic toolkits.

1.2 Extraction methodology

Forensic tools used in extracting data from Android phones are largely supported by two methods:

a. File System (logical) Acquisition – it does not normally produce any deleted file and user's shell permission is required to run the file extraction process; and

b. Physical Data Acquisition – to make a bit-by-bit copy of the mobile device with maximum amount of "deleted data or files" recovered [3]. The process is similar to computer forensics and is widely used by forensic examiners.

Either physical extraction [the boot pre-loader or Android Debug Bridge ("ADB") options] or logical acquisition process (by copying from the backup mode) is able to extract data from MTK-based smartphones. As the two processes are regarded as less invasive to the physical phone when compared to the "JTAG" or "Chip-off" method, they are frequently used in forensic investigations. Besides, physical extraction has the benefit of recovering maximum amount of "deleted data or files" by copying bit-by-bit from physical flash memory storage [3] and its acquisition process can bypass the device's pattern locks or passcodes in many investigation cases [6]. The experiments conducted in this research are intended to identify an extraction method that suits best to MTK Android phone forensics.

1.3 Objective of This Paper

This paper will focus on the use of three extraction tools to capture complete memory dump of the phone under test. The competency and compatibility of these methods will be evaluated by comparing their test results.

In summary the objectives set down for this project are:

a. to conduct literature review pertaining to mobile forensics on MTK Android phones;

b. based on the actual amount of forensic data acquired, to compare the test results on the application of forensic tools developed by different vendors and evaluate their effectiveness; and

c. to identify a suitable extraction tool to cope with different brands of smartphones equipped with the same CPU chipset and review the best process for its use.

1.4 Document Structure

Chapter 2 provides literature review on researches conducted on Android forensics, in particular the MTK devices.

Chapter 3 discusses the methodology.

Chapter 4 outlines the implementation of extraction process by the three selected extraction tools.

Chapter 5 compares the test results by referring to the forensic tools and methodology under test.

Chapter 6 is the conclusion. It sums up the challenges to forensics conducted on MTK Android devices. It will also explore possible areas for future study in the mobile phone industry.

 © 2015 ADFSL

2. PAST STUDY AND EXPERIENCE

There are plenty of research studies on Android Forensics but only a few covers the realm of MTK Android Forensics. A list of the relevant works is listed here.

2.1 Studies on Android Forensics

In 2011 Joe Sylve introduced a tool on memory acquisition, the Droid Memory Dumper ("DMD") [7], which captures a copy of the memory data, runs an address translation of each memory page and writes them to a TCP socket. The DMD module, however, has its restrictions:

a. the ADB of the Android device has to be turned on in order for the DMD to tether data using network protocol via the virtual USB port;

b. root privileges are to be executed in order to capture system data.

In 2012 Ismael Valenzuela presented an enhanced module of the DMD, LiME Forensics, which is purportedly the first software to dump full contents of internal memory from an Android device [8]. The new tool requires the "rooting" of the device which may alter the state of the target phone and thus, casts doubt on the integrity of the evidentiary data so recovered.

Lessard and Kessler (Lessard & Kessler, 2010) [9] investigated Android smartphones by acquiring a logical and physical image of the phone using 'dd' command. They further used Cellebrite, a mobile forensic tool, to acquire the same image for comparing the two methods.

In his research work, Timothy Vidas et al. (Vidas, Zhang & Christin, 2011) [10] made use of a custom recovery image to boot the device instead of loading the operating system. The recovered image can support functions like dumping the Flash Memory, allowing the execution of the 'su' command to gain root access and adding some custom transfer binaries. The adb tool will collect data from the device and transfer them to a connecting computer via the USB port.

Vijith Vijayan in his thesis, "Android Forensic Capability and Evaluation of Extraction Tools" [11], compared the effectiveness of logical extraction of two HTC Android phones by three mobile forensic tools. The test results however showed that a full memory dump could not be achieved.

2.2 A Study on MTK Android Forensics

MTK Android phones have a short product cycle as they are mostly designed for low-end to middle range products. A new phone model could have replaced the current one before analysis on its hardware specifications or system architecture is complete. Hence, there are few researches conducted on MTK forensics. After review it is found that China branded phone forensics was referred to in a research paper entitled "Digital Forensic on MTK-based Shanzhai Mobile Phone with NAND Flash" [12]. The authors uncovered 90% of the "Shanzhai" phones had been using the core processor, peripheral hardware prototype and software development platform of MTK or Spreadtrum. Nevertheless, their research confined only to extracting specific data such as locating file repository of phone books, call records, SMS and web-browsing records without obtaining a full memory dump.

3. EXPERIMENT METHOD AND PROCEDURE

Traditionally a number of forensic tools have been using the ADB as a communication interface to access the Android system via a

computer installed with extraction software. In order to extract complete memory data, the Android device must be made available for 'super user' privilege of access (also known as "rooting the device") [13] so that the examiner can make a copy of all system partitions and access files that are not originally accessible by normal users. The Android phone has to be powered up as usual and the USB Debugging mode turned on manually in the system menu of the phone. So if the mobile device is protected by power-on password or pattern lock, the extraction process cannot be executed.

Alternatively the device can be put into the Download mode, a state in which the Flash Memory can be formatted and reprogrammed. The Flash Memory holds all binary information [which includes internal memory of the device, drivers, applications and other types of data in memory structure like Read Only Memory (ROM) and Non-Volatile Random Access Memory (NVRAM)] required for the device to boot up and function. With an unlocked bootloader which is commonly found in MTK Android phones, the Flash Memory can be reprogrammed in a way to establish connection of the target phone with any storage media. The above procedure is similar to computer forensics where a forensic boot disk is used to operate the cloning process for acquiring data from the target computer without affecting the original hard disk. The uniqueness of this method is that there is no need to "rooting the device" or enabling the USB Debugging mode before extraction, thereby resolve the difficult problem of accessing a password-protected phone. The entire process is forensically sound as it will not interfere with the internal storage of the device.

In this experiment, Volcano Box has used the method of "rooting the device" while SP Flash Tools is an example of applying the Download mode. After making a physical copy of the mobile phone, the important task for an examiner is to identify the files that are of interest to the investigation. Message records and photos recovered will be searched to locate relevant files for the test process. The results will be analyzed to confirm the effectiveness of the methodology and the competency of the tools under test. Besides, the extracted data will be cross-referenced with the examination result conducted by the Cellebrite UFED ("Universal Forensic Extraction Device") Touch [14].

3.1 Terminology

SP Flash Tools [15] is an application that captures memory images or binary data from a mobile phone. It can erase phone data or modify codes / data and then write them back to the phone. The tool employs the boot ROM kernel library ("BROM_DLL") and Download Agent ("DA") program to download, read or erase files from the target phone's Flash Memory via a USB port connection. In practice, SP Flash Tools reads a length of memory from the target phone by using a scatter-file which begins at a start address and a given length. Each read back file is a continuous memory dump from the Flash Memory. Multiple blocks starting at different addresses can be read and copied into image files for storing in the forensic workstation.

Volcano Box [16] supports a large number of MTK based phones including earlier feature phones to the latest Android phone models. It can capture internal information of the target phone, read / write flash, unlock user code, backup phone data and run those advanced features such as clear up the Flash Memory, repair IMEI, fix receive signals and read / write NVRAM files for MTK phones. It is in fact a tool designed for repairing, upgrading or modifying the phone system.

 © 2015 ADFSL

Cellebrite UFED is an expansive and well-known forensic tool used in more than 60 countries. So far as the target device is on its support list, the auto-detection mechanism of the software can provide a step-by-step guide for the extraction process. For unlisted devices, UFED has also developed a generic profile to provide support.

4. THE EXPERIMENT PROCESS

The Lenovo A850 smartphone, being used for experiment, is equipped with MT6582 processor, a popular model in the MTK Android market and is installed with WhatsApp, Line and WeChat. To begin the process, a forensic workstation was set up and configured. Phone calls were made and photos taken in order to carry out the subsequent physical extraction for retrieving user's data.

4.1 The Experiment on Lenovo A850

The mobile phone is running Android OS 4.2.2 and the sequences of extraction process were as follows:

a. Physical Extraction Using SP Flash Tools

The phone was turned off initially. It turned on automatically when plugged into the USB port of the forensic workstation running the SP Flash Tools and started up the injected boot programs for the extraction process. A total number of 20 image files were extracted as listed in Table 1. The accumulated size of those saved files was 3,800,192KB. The phone was then turned off completely by taking out the battery.

b. Physical Extraction Using Volcano Box

The phone had been powered on with debugging mode enabled when plugged into the specific port of the physical Volcano Box (Picture 1). The Box was connected via USB cable to the forensic workstation running the corresponding software. The "Backup EMMC" option was used and one single image file with size 3,779,712KB had been extracted. The phone was then turned off completely by taking out the battery.

Table 1.
Image files extracted from Lenovo A850

Block Map	(KB)	Block Map	(KB)	Block Map	(KB)
android	1048576	usrdata	2281088	bootimg	6144
cache	129024	ebr1	512	ebr2	512
expdb	10240	logo	3072	mbr	512
misc	512	nvram	5120	preload	256000
preloader	20480	pro-info	3072	protect-f	10240
protect-s	10240	recovery	8192	sec_ro	6144
seccfg	128	uboot	384		

Picture 1. Cable connection using Volcano Box

c. Physical Extraction Using Cellebrite UFED Touch

The phone had been powered on with debugging mode enabled when plugged into the USB port of the physical Cellebrite UFED Touch. The device was connected via USB cable to the forensic workstation running the corresponding software. The "Generic ADB for Chinese Android" option was used and one single binary file with size 3,779,712KB had been extracted.

A summary to show the memory size and files captured by the tools is shown at Table 2.

5. EVALUATION

In order to compare the test results of these three tools, the X-Ways Forensics [17], an integrated computer forensics software, was also used to mount the extracted images (for SP Flash Tools, only USR Data Image file and in the case of Volcano Box and Cellebrite, the full memory dump) from the experiment. The examination is confined to look at the user data partition of each mounted image, which purportedly contains application databases, event logs and user data for which forensic examiners are tasked to investigate information relating to criminal activities or leading to possible traces.

Table 2.
Test results of three extracted methods.

Lenovo A850	**SP Flash Tools**	**Volcano Box**	**Cellebrite UFED**
Image Size	3,800,192KB	3,779,712KB	3,779,712KB
No. of Files in user partition	2,321	2,297	2,328

 © 2015 ADFSL

There were 20 image files recovered by SP Flash Tools. The table above shows that it has captured the largest image while the image size captured by Volcano Box and Cellebrite UFED is the same. It is noted that when the test process was conducted by Volcano Box and Cellebrite, system and application log files were created or modified whenever the phone was switched on for the extraction (this is a feature of the phone when data in memory are automatically altered once it is powered up). For instance, in the user partition, Cellebrite UFED image got 53 new files which were not found in Volcano Box and vice versa, Volcano Box had 23 new files not recovered by Cellebrite UFED image. These 76 files are system start-up event files. Besides, there are 1,173 common existing files which are different in size and they are all system log or application library files. All these files mentioned above were activated as part of the system boot up process without user's intervention. To further evaluate the results, UFED Physical Analyzer 4.2.1 [18] was used to conduct user data carving from the acquired images (Table 3).

Table 3.
Comparison of data extracted among three tools

Model:Lenovo A850	SP Flash Tool	VolcanoBox	Cellebrite UFED
Analyzed Data			
Calender	1	1	1
Call Log	4	4	4
Chats	22	22	22
Contacts	81	81	81
Cookies	157	157	157
Locations	15	15	15
Emails	1	1	1
Installed Applications	37	37	37
Passwords	9	9	9
Searched Items	1	1	1
SMS Messages	1	1	1
User Accounts	15	15	15
Web Bookmarks	13	13	13
Web History	14	14	14
Wireless Networks	2	2	2
Data Files			
Audio	59	59	59
Images	518	518	518
Videos	4	4	4

Unlike single memory dump file captured by Volcano Box and Cellebrite UFED, SP Flash Tools acquired different image files according to the information on memory allocation recorded in the scatter-file. The decoding process was carried out on the USRData.img, Android.img and Preload.img files. In conclusion the three tools have produced the same result on the recovery of crucial data and files.

In proving the merit of using a controlled boot program, SP Flash Tools were being used three times consecutively to acquire the USRData.img file from Lenovo A850. Having examined the mounted images using X-Ways Forensics, all the files and records extracted from these three extractions are found identical. It is fair to conclude that no file creation or modification has been made to the internal memory when the phone is booted up for data acquisition.

6. CONCLUSION

Based on the data analyzed in table 3, the three tools produce similar test results in retrieving data or files that are of interest to forensic investigations but SP Flash Tools provides more comprehensive steps for user operations and is considered to be highly adhered to the principle on digital forensics because:

a. The tool can extract full range of data even if the phone is (*i*) password-locked; (*ii*) USB debugging mode is disabled; or (*iii*) in the absence of root access right.

b. Data integrity of the mobile phone is maintained by taking control during the boot up process and suppresses the running of installed applications of the phone except relevant download agent for extraction, On the other hand, the other two forensic tools perform live extraction of data while the phone applications are running.

c. The USRData.img file is acquired based on memory allocation information contained in the scatter-file. The analysis process is conducted more efficiently on the userland data when compared with the work conducted on full image dump extracted by other tools.

d. The tool is open sourced and free-of-charge, i.e. incur no cost or recurrent charges on the extraction process, but its drawback lies with the lack of providing technical support on bug fixing or product development in future.

e. The tool seamlessly provides an extraction method that can apply to all Android smartphones, irrespective of the phone brands or models (the upcoming models are also included), which are running on the same designated MTK based CPU chipsets. Currently, the tool supports 13 types of MTK processors in the market including the octa-core devices launched in 2014.

6.1 Future Study

The development in mobile forensics grows rapidly as new mobile devices with more powerful CPU and storage capacity are launching every day. Nevertheless, it is observed that forensic examiners are getting behind in exploring a competent forensic tool to extract full range of data from these devices. Efforts should be made to work out a comprehensive framework for researching applicable extraction method and evaluating mobile forensic toolkits which allows the

 © 2015 ADFSL

extracted data, after analysis, is likely to be admissible as evidence in court proceedings.

Low-end Android phones can be a useful device for offenders in view of their low price and that they can be easily disposed of either by destroying them physically or throwing them away. Past experience of forensic examinations has showed that physical extraction of data from these phones is not easy to achieve. In spite of this, considering these low-end Android phones could have used the same chips or similar form factors to cut cost, it is highly possible that a particular generic extraction tool, once identified, can be used on other CPU chipsets such as Qualcomm or the newer SnapDragon. Such extraction tool may assist in seamlessly gathering all objects and data structure from Android devices as well as bypass any hurdle created by password or encryption mechanism in an orderly manner. This will provide a good lead for conducting future study.

© 2015 ADFSL

REFERENCES

Kidnapping & extortion: Police ecstatic over toys to tackle cell phone crime, published in The Express Tribune, October 19, 2012, http://tribune.com.pk/story/453569/kidnapping-extortion-police-ecstatic-over-toys-to-tackle-cell-phone-crime/

Investigating and analyzing the web-based contents on Chinese Shanzhai mobile phones, IEEE/SADFE 2012, http://hub.hku.hk/bitstream/10722/189648/1/Content.pdf

Det. Cynthia A. Murphy , Developing Process for Mobile Device Forensics, http://www.mobileforensicscentral.com/mfc/documents/Mobile%20Device%20Forensic%20Process%20v3.0.pdf

MediaTek from Wikipedia, http://en.wikipedia.org/wiki/

MediaTek Top 140 quad-core MT6582 dual sim phones listed with specifications, GizChina.com, March 3, 2014, http://www.gizchina.com/2014/03/03/top-140-quad-core-mt6582-dual-sim-phones-listed-specifications/

Persistent Challenges with Smartphone Forensics, Digital Forensic Investigator, February 8, 2013, http://www.dfinews.com/articles/2013/02/6-persistent-challenges-smartphone-forensics J. Sylve et al., Android Memory Capture and Applications for Security and Privacy, University of New Orleans Theses and Dissertations. Paper 1400, 2011, http://scholarworks.uno.edu/cgi/viewcontent.cgi?article=2348&context=td

Joseph T. Sylve, Android Memory Capture and Applications for Security and Privacy, University of New Orleans Theses and Dissertations, 2011, http://scholarworks.uno.edu/cgi/viewcontent.cgi?article=2348&context=td

Ismael Valenzuela, Acquiring volatile memory from Android based devices with LiME Forensics Part I, Ismael Valenzuela, April 23, 2012, http://blog.opensecurityresearch.com/2012/04/acquiring-volatile-memory-from-android.html

Lessard J, Kessler G.C.,Android Forensics: Simplifying Cell Phone Examinations, ECU Publications Pre.2011, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7480&context=ecuworks

Vidas, Zhang & Christin, 2011, Toward a general collection methodology for Android devices, http://www.dfrws.org/2011/proceedings/07-339.pdf

Vijith Vijayan, Android Forensic Capability and Evaluation of Extraction Tools, April 2012, http://www.academia.edu/1632597/Android_Forensic_Capability_and_Evaluation_of_Extraction_Tools)

Digital Forensic on MTK-based Shanzhai Mobile Phone with NAND Flash, ICDFI, Beijing, China 2012, http://secmeeting.ihep.ac.cn/paper/Paper_Mengfei_He_ICDFI2012.pdf

FlashTool V3.1004.00 Application Note, MediaTek, January 27,2009, http://www.mtk2000.ucoz.ru/FlashTool_V3.1004.00_Application_Note.pdf

UFED Touch Ultimate, Cellebrite, https://www.cellebrite.com/images/stories/brochures/UFED-Touch-Ultimate-ENGLISH-web.pdf

 © 2015 ADFSL

SP Flash Tool + MediaTek MT65XX Drivers Download and Installation Guide including Bricked Devices, updated July 31, 2014, http://laurentiumihet.ro/sp-flash-tool-mediatek-mt65xx-drivers-download-and-installation-guide-including-bricked-devices/

Volcano Box, http://www.volcano-box.com/features.html

X-Ways Forensics, http://www.x-ways.net/forensics/

UFED Physical Analyzer, Cellebrite, http://www.cellebrite.com/mobile-forensics/products/applications/ufed-physical-analyzer

© 2015 ADFSL

 © 2015 ADFSL