World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:1, No:8, 2007

Data Acquisition from Cell Phone using Logical Approach

Keonwoo Kim, Dowon Hong, Kyoil Chung, and Jae-Cheol Ryou

***Abstract*—**Cell phone forensics to acquire and analyze data in the cellular phone is nowadays being used in a national investigation organization and a private company. In order to collect cellular phone flash memory data, we have two methods. Firstly, it is a logical method which acquires files and directories from the file system of the cell phone flash memory. Secondly, we can get all data from bit-by-bit copy of entire physical memory using a low level access method. In this paper, we describe a forensic tool to acquire cell phone flash memory data using a logical level approach. By our tool, we can get EFS file system and peek memory data with an arbitrary region from Korea CDMA cell phone.

***Keywords*—**Forensics, logical method, acquisition, cell phone, flash memory.

I. Introduction

AS digital evidence that kept in the various electronic media such as a computer and a mobile device in the digital crime is recently increasing, digital forensic technology to prove the crime is being more and more important. Especially, if the critical evidence is stored in the mobile devices, mobile forensic technology is demanded to find out the evidence without damage of the evidence. Mobile devices include small scale digital devices, embedded system, portable storage devices, and obscure devices. And, as to the small scale digital devices, there are various types of cell phones, USIM, PDA, navigation system, game player, and so on.

In this paper, we are focusing in acquiring and analyzing data in the cell phone. User data such as phonebook, call history, SMS, and photo and hardware-related data such as IMSI, MIN, and ESN are mainly stored in the NAND flash memory and the NOR flash memory of the cell phone. In case of Korea, most of CDMA cell phone nowadays adopts the NAND flash memory. For this cell phone forensics, the mutually different interfacing and analysis method are needed for each cellular phone manufacturer and its own model. In the mean time, forensic tools for the CDMA phones are not as much as tools for the GSM phones and all of cell phone forensic tools are not applied to the cell phones used for Korean mobile service provider.

Our final goal for mobile forensics is to completely acquire all data from CMDA cell phone flash memory and its mobile storage media. As a first step to do that, we developed cell phone forensic tool to get logically file system of the cell phone NAND flash memory. Our tool can obtain a specific folder and a file structure for some cell phones. But, it can't completely acquire all data in the memory because logically accessible memory region is limited. So, we also introduce cell phone forensics technology by a physical method as well as by a logical method.

This work was supported by the IT R&D program of MIC/IITA [2007-S019-01, Development of Digital Forensic System for Information Transparency].

K. Kim is with Electronics and Telecommunications Research Institute, 161 Gajeong-Dong Yuseong-Gu, Daejeon, 305-350, Korea (phone: +82-42-860-1521, fax: +82-42-860-5611, e-mail : wootopian@etri.re.kr).

D. Hong is with Electronics and Telecommunications Research Institute, 161 Gajeong-Dong Yuseong-Gu, Daejeon, 305-350, Korea (phone: +82-42-860-6147, fax: +82-42-860-5611, e-mail : dwhong@etri.re.kr).

K. Chung is with Electronics and Telecommunications Research Institute, 161 Gajeong-Dong Yuseong-Gu, Daejeon, 305-350, Korea (phone: +82-42-860-1920, fax: +82-42-860-5611, e-mail : kyoil@etri.re.kr).

J.-C. Ryou is with Electrical Engineering and Information & Communication Engineering Division, Chungnam National University, 220 Gung-Dong, Yuseong-Gu, Daejeon, 305-764, Korea (e-mail: jcryou@home.cnu.ac.kr).

II. Cell Phone Forensics

Cell phone forensics can be largely divided by memory forensics and SIM forensics.

Mobile phone based on GSM/WCDMA telecommunication technology stores data such as phone book, SMS message, and, IMSI in SIM/USIM. So, (U)SIM forensics is required to extract data from the cell phone with memory forensics. In the process of (U)SIM forensics, an user PIN(Personal Identification Number) may be demanded according to the access condition of EF(Elementary File) in which data is stored. In Korea, a mobile subscriber can select whether he stores data like SMS and phonebook in the USIM or in the memory. The USIM forensic tool can be made with reference to ISO-7816 series, GSM SIM, and, 3GPP USIM related standard.

The goal of memory forensics is to extract data stored in the flash memory of the cellular phone and to find out the meaningful evidence. There is two kinds of in the method for acquiring data stored in the flash memory.

- Data acquisition by a logical approach
  Data stored in the memory are acquired by using the file system or the protocol of a chip provider.

- Data acquisition by a physical approach
  Entire data of the physical memory dumped to bit-by-bit. And then, it is possible to acquire even data with unallocated area on the memory.

In the CDMA mobile communication system of Korea, since the SIM/USIM card is not used, only the memory forensic technology is applied to acquire and analyze the meaningful data. And, both all of the memory forensics and USIM forensics have to be applied in the WCDMA mobile communication system.

A. Memory Forensics by Logical Method

NIST provides the analyzed result about some cell phone forensic tools through its published document [1] and [2]. Most of cell phone forensic tools have facilities acquiring digital evidence contained on the flash memory of a cell phone using some logical protocol between a cell phone and a host PC. In order to avoid the change of the original image, tools should make the copy image of the device case. And then, tools analyze file system from the copied image to find out the meaningful data as the evidence. Copy of image is done to guarantee the integrity of evidence data during analysis process. Recently, GuidanceSoftware [3] has released the Cell Phone Forensic Tool called a Neutrino. Neutrino is coupled with an Encase 6.5. However, all of cell phone forensic tools in the world are not applied to cell phones for mobile service providers of Korea.

	Function	Target Devices
PDA Seizure[7]	Acquisition, Examination, Reporting	▪ Palm OS, Windows Mobile/Pocket PC, and Blackberry devices
Pilot-Link	Acquisition	▪ Palm OS devices
Secure View	Acquisition Examination Reporting	▪ TDMA, CDMA, and GSM phones ▪ SIMs
Cell Seizure[8]	Acquisition, Examination, Reporting	▪ TDMA, CDMA, and GSM phones ▪ SIMs and USIMs
GSM .XRY	Acquisition, Examination, Reporting	▪ GSM and CDMA phones ▪ SIMs and USIMs
Phonebase	Acquisition, Examination, Reporting	▪ GSM phones ▪ SIMs and USIMs
MobilEdit!	Acquisition, Examination, Reporting	▪ GSM phones ▪ SIMs
TULP 2G	Acquisition, Reporting	▪ GSM phones ▪ SIMs
	Function	**Target Devices**
Forensic Card Reader	Acquisition, Reporting	▪ SIMs
ForensicSIM	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMCon	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMIS	Acquisition, Examination, Reporting	▪ SIMs and USIMs
BitPIM	Acquisition, Examination	▪ Certain CDMA phones using Qualcomm chipsets
Oxygen PM (forensic version)	Acquisition, Examination, Reporting	▪ Nokia phones
Oxygen PM for Symbian (forensic version)	Acquisition, Examination, Reporting	▪ Symbian phones

Fig. 1 Cell phone forensics tools
(source : : NIST "Guidelines on Cell Phone Forensics")

The CDMA cellular phone of Korea has the Qualcomm software and hardware architecture. Because a cell phone maker usually has a specific communication interface to access the internal memory of its cell phone, the separate interface development is needed for each cellular phone model to acquire data in the flash memory and to extract the meaningful data. As well, acquiring data from some part or whole region of memory is not same to each cell phone models because non-volatile memory of cell phone has its own independent structure according to the memory manufacturing company. Therefore, although we can approach to the arbitrary area of the memory by using the forensic tool, the method for analyzing the raw data is each other different for each cell phone.

B. Memory Forensics by Physical Method

Data acquisition from entire address region of flash memory can be done using physical method by low level approach. The physical level access method can enhance the recovery rate for deleted data than when using the logical level access method. There is a three method to acquire data using a physical level approach [4].

Firstly, flasher tools, which are mostly used by manufacturer for debugging and diagnostics of a cell phone, can be used as forensic tool that copies flash memory data. They have a simple hardware connection with a connector of cell phone, so that memory is no need to be separated from the cellular phone. There are some tools such as Twist flasher boxer and D500 OneNAND Downloader [4]. However, all flasher tools cannot be applied to all cell phone models because each cell phone has its own dedicated memory interface in a memory chip. In some case, there are flasher tools to read only some part of memory not full memory copy or to skip the spare region. Therefore, flasher tool is not a perfect memory forensic tool using physical method.

Secondly, we can use JTAG test access port to acquire data from flash memory. We can get not only NVM (Non-Volatile Memory) data but also volatile memory data by a memory forensics using a JTAG port [5]. If we search for the JTAG pin hidden on the PCB of the cellular phone and can connect it to the JTAG emulator, all area of whole physical memory can be dumped by bit -by-bit approach. However, it is very difficult to find out JTAG pin since most of cell phone manufacturers usually conceal pins in the cell phones that is recently coming out. Memory dump by JTAG interface makes a complete forensic image to investigate the evidence. Fig. 2 presents a system configuration for memory dump using a JTAG interface. After acquiring raw image data, it is also required to extract forensically meaningful evidence from raw image and to present it to a format that represented visually well.

Fig. 2 Memory dump using JTAG

Thirdly, we can also get memory data if we physically remove a flash memory from a board in the cell phone and read

memory content with a memory chip reader. This method is useful when a cell phone is severely damaged or we cannot use a logical method or a JTAG method.

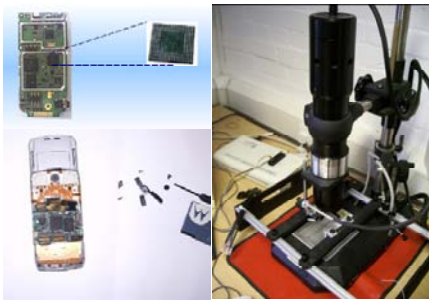

Fig. 3 Reading memory using chip reader

III. Data Acquisition Tool Design of CDMA Cellular Phone

In this chapter, we explain how to design a forensic tool to acquire data from the flash memory of CDMA cellular phone by a logical method. Cell phone made in Korea used for Korean SP (Service Provider) has a software platform based on DMSS provided by Qualcomm and each SP's specific application. Most of cell phones in Korea use REX as their OS and we are especially interested in fs_task and nv_task as forensic-related tasks of REX OS.

In the meantime, many embedded linux systems use JFFS2 or YAFFS as a file system to support NAND flash memory.[6] But, cell phone file system in Korea is EFS(Embedded File System) in MSM5000 series and earlier cell phones and EFS2 in MSM6000 series and after cell phones.

Our tool works on the PC with Microsoft Window OS and it communicates with target cell phone using RS-232C serial interface. We have designed the functionalities of file system access and memory peek as a way to logically acquire data in the cell phone flash memory.

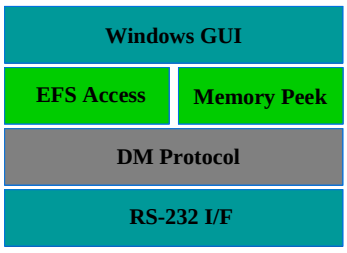

Fig. 4 Design of data acquisition tool

A. EFS Access Part

EFS/EFS2 is a file system to create, store, and, manage file in the CDMA cellular phone of Korea. We can access NV items like MIN(Mobile Identification Number) and ESN(Electronic Serial Number) and well as evidence data like call history, phonebook, and SMS stored in a file system.

If only our tool sends a request message to access files and directories of the NAND flash memory, EFS processes the request and activates device driver in order to access an actual flash memory. Procedure to acquire data in the EFS Access part is as follows:

1) We appoint a specific folder or root folder of EFS.
2) EFS Access part deliveries the information to DM Protocol part.
3) DM Protocol part acquires file system.
4) EFS Access part reconfigures file system on Windows GUI.

Our acquisition tool accesses file system by only fs_task, so that we don't need to know about underlying REX.

B. Memory Peek Part

Memory Peek part acquires data by accessing an arbitrary address of a flash memory. Procedure to acquire data in the Memory Peek part is as follows.

1) We appoint starting address and length of peek region.
2) Memory Peek part deliveries the information to DM Protocol part.
3) DM Protocol part acquires memory data.
4) Memory Peek part stores memory data file and shows it on Windows GUI.

However, since accessible region of flash memory is sometimes limited or blocked off, memory peek by logical level approach is not the best solution to acquire all memory data.

C. DM Protocol Part

DM is used for cell phone debugging, air service monitoring, NV access, EFS access, air message logging, and so on. Of those functions of DM, we implemented NV access function and EFS access function for our tool. DM Protocol part processes a request from EFS Access part and Memory Peek part, acquires data from the flash memory and returns acquired data to EFS Access parts and Memory Peek part.

IV. Memory Data Acquisition Using Our Tool

Data acquisition tool on PC is connected to the cell phone using a USB-Serial cable. Used cell phone models for the test are SAMSUNG SCH-E470 and SCH-V330.

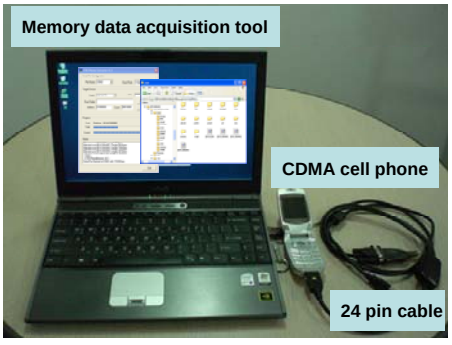

Fig. 5 Testbed for data acquisition

EFS file and directory are acquired by appointing a specific folder or a root after setting of port and baud rate and the selection of cell phone model in the Fig. 6. As a result, file system extracted from EFS of the cell phone is copied to

Windows PC as a first picture of Fig. 7.

Structure of acquired file and directory is different per a model because each cell phones store data using its own specific folder structure and file structure. Generally, we can extract a phonebook, call history, SMS, and photo data from the cell phone using this logical method. But, our tool does not guarantee to completely acquire intentionally deleted data or data stored in the unallocated address.

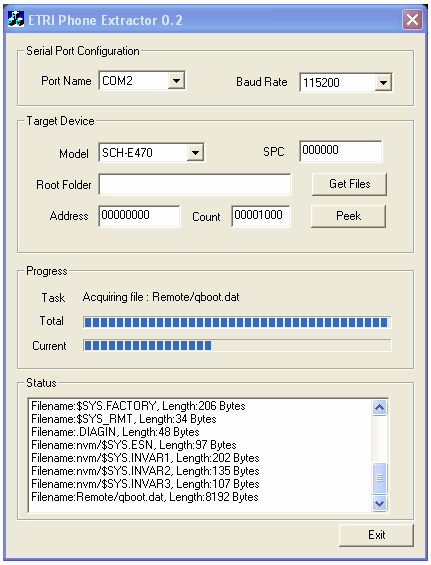

Fig. 6 Cell phone data acquisition tool

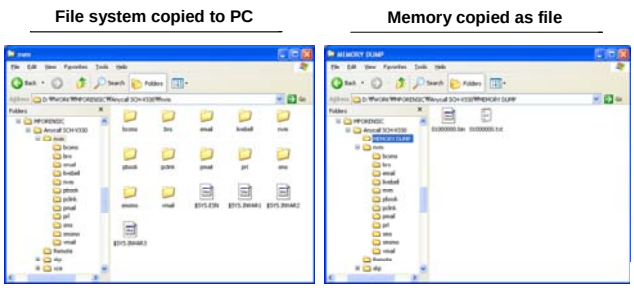

Fig. 7 Data acquired from the cell phone flash memory

As a second method to acquire data, memory data in arbitrary address region can be also obtained by appointing a starting address and a length of region. Extracted data from the flash memory are stored into PC file as a second picture of Fig. 7. Our tool creates a 'bin' file that original cell phone memory is copied and a 'txt' file that memory address and copied data are shown as a text format.

When analyzing memory data, we need to distinguish code region and data region to extract meaningful data. Generally, there is a boot image space in staring address region of ROM address space, and code space and data space are sequentially arranged. For forensically meaningful evidence, all data of memory space should be acquired. Therefore, we need to develop an acquisition tool considering that address space of flash memory is not same to every model.

V. Conclusion

In this paper, we provide a tool that copies file system of CDMA cellular phone and peeks data with an arbitrary address space from flash memory. But, our tool is not commonly applied to all cell phones since each other different service code is required to access to e cell phone and logically accessible memory region is limited.

Therefore, data acquisition by a low level approach using JTAG is the best method to collect all data within flash memory regardless of the cellular phone kinds. By forensic tool using JTAG interface, we can well recover the deleted data even though a suspect has deleted data such as SMS, photos, and call history intentionally or accidentally. Henceforth, we are going to study to acquire binary data by a low level method and to decode forensically meaningful data from the binary data through the analysis of EFS and FTL (Flash Translation Layer), and cell phone flash memory structure.

References

[1] NIST, Cell Phone Forensic Tools: An Overview and Analysis. NISTIR 7250, 2005.
[2] NIST, Guidelines on Cell Phone Forensics. Draft Special Publication 800-101.
[3] http://www.guidancesoftware.com/
[4] Marcel B., Martien de J, Coert K, Ronald van der K and Mark R., Forensic Data Recovery from Flash Memory. Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007.
[5] M. F. Breeuwsma, Forensic imaging of embedded systems using JTAG (boundary-scan). Digital Investigation, Vol. 3, Ed. 1, March 2006.
[6] Eran G. and Sivan T. Algorithms and data structure for flash memories. ACM Computing ACM Computing Surveys, Vol. 37, No. 2, June 2005, pp. 138–163.