Forensics for Korean Cell Phone

Keonwoo Kim
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350, Korea
+82-42-860-1521
wootopian@etri.re.kr

Dowon Hong
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350, Korea
+82-42-860-6147
dwhong@etri.re.kr

Kyoil Chung
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350, Korea
+82-42-860-1920
kyoil@etri.re.kr

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. First method is a logical approach 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 some Korean CDMA cell phones.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms
Design

Keywords
Forensics, logical method, acquisition, cell phone, flash memory

1. INTRODUCTION
In a recent digital crime, digital evidence that stored in the various electronic devices such as a computer and a mobile device is increasing. So, digital forensic technology to prove the truth of 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 other obscure devices. Especially, as to the small scale digital devices, there are various types of cell phones, (U)SIM, 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 a 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 has a NAND flash memory as its storage device. For this cell phone forensics, mutually different interfacing and analysis method are needed for different cellular phone manufacturers and their own models. And, forensic tools for the CDMA phones are not as much as tools for the GSM phones. Moreover, 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 a 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 low level method as well as by a logical method.

2. CELL PHONE FORENSICS
Cell phone forensics can be largely divided by memory forensics and (U)SIM forensics.

Mobile phone based on GSM/WCDMA telecommunication technology stores data such as phone book, SMS message, and, IMSI in (U)SIM. So, (U)SIM forensics is needed to extract data from the GSM 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 Korea, a mobile subscriber can choose whether he/she stores data in the USIM or in the memory. 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 retrieve data stored in the flash memory of the cellular phone and to find out the meaningful evidences. There are two methods 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 low level approach

  Entire memory data are dumped by bit-by-bit. And then, it is possible to acquire data on the unallocated area of the memory.

In the CDMA mobile communication system of Korea, since the (U)SIM is not used, only the memory forensic technology is

* Conference name: e-Forensics 2008

e-Forensics 2008, January 21-23, 2008, Adelaide, Australia.

needed to acquire and analyze the meaningful data. Of course, both memory forensics and (U)SIM forensics have to be applied in the WCDMA mobile communication system.

2.1 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 in the flash memory of the cell phone using some logical protocol between a cell phone and a host PC. In order to avoid changing the original image, tools make the copied image of the device case. And then, tools analyze file system from the 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, which is coupled with an Encase 6.5 and over. However, there are thousands of cell phone models in the market and new models are coming out at rapid rate. Phone hardware and software can vary depending on network system, carrier, company, model, and OS. So, lack of consistent standard in cell phone structure means each new phone needs to be handled differently.

While most of tools in the [1] and [2] are for GSM phone, BITPIM[7] is a free forensic tool for CDMA phone. It needs a data cable and a driver for specific phone. After connecting to phone correctly, it can dump file system data, and interpret phonebook, wallpapers, ringers, calendar entries, memos, call log, and, text messages. To access phone data, diagnostic mode is available in all Qualcomm MSM chipsets. DM mode provides a direct access to EFS(Embedded File System). And, some data can be recovered with protocol specific to manufacturer and model. Size of fields in protocol is different for every model, therefore, new versions of program need to be released to support new phone models. As well, BREW can also be used to interact with phone. BREW is an application development platform that runs between the application and the chip operating system. As another feature of BITPIM, it provides a protocol analyzer where users can view detailed communication with the phone including protocol, brew command, and others. Through the analyzer, we can see detailed communication protocol log showing protocols and BREW commands used to access data. Consequently, we show merits and demerits of BITPIM in the table 1.

Table 1. Features of BITPIM

Merits	Demerits
- Free - Customizable - User friendly GUI - Forensically sound - Protocol analyzer	- Support on new phones depends on developers - Need cable, drivers - Can't access 'Dead' phone

However, all cell phone forensic tools including BITPIM are not applied to cell phones for mobile service providers of Korea. The Korean CDMA cellular phone has Qualcomm software and hardware architecture. Because a cell phone maker usually has a its own specific communication interface to access the internal memory, separate interface development is needed for each cellular phone model. As well, acquiring data from some part or whole region of memory is not same to each cell phone model because non-volatile memory of cell phone has its own independent structure. 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.

On the other hand, phone hacking and development tools for forensics purpose may also be used to access the memory and other important settings of a phone. Such a software tool like UniCDMA is often used by small shops and underground to unlock phones, change OS firmware, change language, access data, and others. But, it is not recommended by NIST because it's not stable to retrieve phone data and not originally designed for forensic tool.

2.2 Memory forensics by low level method

Data acquisition from entire flash memory can be done by low level approach method.[4] The method can enhance the recovery rate of deleted data and hidden data than when using the logical level access method.

Firstly, 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 can search for the JTAG pin hidden on the PCB of the phone and can connect it to the JTAG emulator, all memory area can be dumped by bit-by-bit approach. However, it is difficult to find out JTAG pin since most of cell phone manufacturers do not usually reveal pins on the PCB of the phone. Even though JTAG pin is founded, we should develop cmm programming using JTAG emulator or debugger. None the less, memory dump by JTAG interface makes a complete forensic image to investigate the evidence. Figure 1 presents a system configuration for memory dump using a JTAG interface and a pin configuration between phone and JTAG emulator. 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.

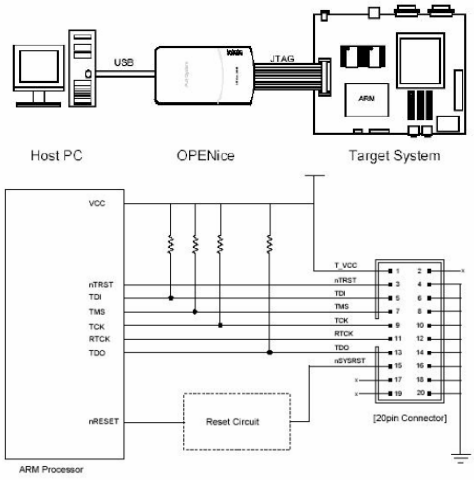

Figure 1. Configuration for memory dump using JTAG

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

content using a memory chip reader. This can perform forensic analysis when a phone is not well working or when we cannot use a logical method and a JTAG method. Recently, about 97% of cell phones use MCP technology for memory. Various types of memory can be combined into a single package. Smaller area and increased memory density offer different memory types for different needs. For example, some MCP consists of standard NAND flash for storing program code, gigabyte class NAND flash for storing user data, and, SDRAM for working memory. However, it's not easy to access MCP chip. Pins are typically underneath the board, not on the edges. Board is multilayered, therefore, pins of the chip are not easily accessible.

3. FORENSIC TOOL DESIGN FOR KOREAN 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 service provider has a software platform based on Qualcomm DMSS and each SP's specific application. And, most of Korean cell phones use REX as their OS. REX uses the preemptive scheduler of the fixed type based on priority. And, it provides API for task management, task synchronization, mutual exclusion, timer, and interrupt control. Task is an execution entity performed independently. Especially, we are interested in *nv_task* and *efs_task* as forensic-related tasks. *nv_task* is a task that controls access of permanent data of a cell phone. There is an allocated space to store NV items such as ESN and MIN in a phone. Reading and writing data in NV space by other tasks, such as watchdog task, handset task, UI task, and DM task, should be done by only NV task. *efs_task* is a task which provides the file system service used to store data with the general file format unlike NV. EFS data is mainly used in processing independent data on the phone unlike NV items. For example, when saving the picture file, the file is stored in the EFS area through the EFS task.

For many embedded linux systems, JFFS2 or YAFFS is used as a file system to support NAND flash memory.[6] But, cell phone file system in Korea is EFS in MSM5000 series and earlier cell phones and EFS2 in MSM6000 series and after cell phones. Recently, a phone manufacturer often uses its own file system like TFS as well as EFS/EFS2.

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

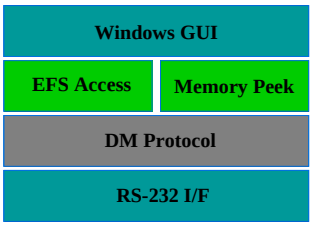

Figure 2. Design of data acquisition tool

EFS/EFS2 is a file system to create, store, and, manage file in the Korean CDMA cellular phone. We can access NV items like MIN and ESN as 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.

As another method to retrieve memory data, 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.

DM is for cell phone debugging, air service monitoring, NV access, EFS access, air message logging, and so on. As interface for the DM coupling, there are hardware interface and software interface. In this paper, we made a use of hardware interface using RS-232C and USB. Software interface makes DM task communicate with packet of the AHDLC(Asynchronous High-level Data Link Control) mode through the diagnostic monitoring service. DM is able to apply to most of cellular phones produced in Korea. It downloads active files saved in the cellular phone. And, we might also recover partially deleted data since some phone models may include the deleted records within active files.

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, extracts data from the flash memory and returns acquired data to EFS Access parts and Memory Peek part.

4. MEMORY DATA ACQUISITION USING OUR TOOL

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

EFS file and directory are acquired by appointing a specific folder after setting of port and baud rate and the selection of cell phone model as shown in the figure 3. As a result, file system extracted

from EFS of the cell phone is copied to Windows PC as a first picture of figure 4.

Structure of acquired file and directory is different from each model because each cell phone stores 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 and hidden data stored in the unallocated address.

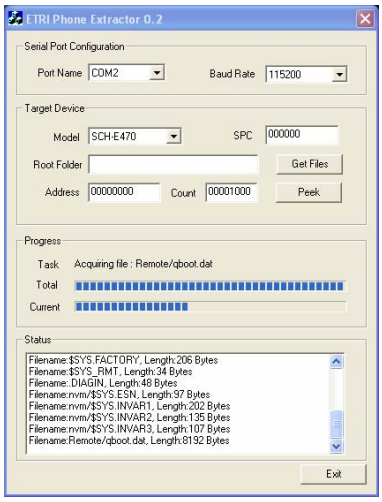

Figure 3. Cell phone data acquisition tool

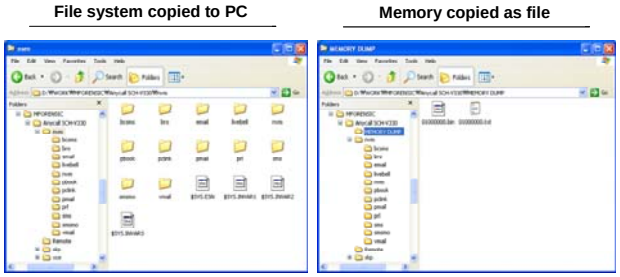

Figure 4. Data acquired from the cell phone flash memory

As a second method to acquire data, memory data at 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 files as a second picture of figure 4. Our tool makes a *'bin'* file recording binary memory data, and a *'txt'* file with a text format.

Generally, there is a boot image space in staring address region of flash memory. And, code space and data space are sequentially arranged. Data space, which is also called flash file system area, is data area with EFS/EFS2. User data and DB are stored in this area.

For forensically meaningful evidence, all data from entire memory space should be acquired. Therefore, we need to develop an acquisition tool using not only DM-based method but also low level approach by JTAG interface.

5. 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 different service code is needed to access to each 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 types. 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 research to acquire binary data by a low level method and to decode forensically meaningful data from that binary data.

6. ACKNOWLEDGMENTS

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

7. 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] Available at 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.

[7] Available at http://www.bitpim.org/