UNIVERSITI
TEKNOLOGI
MARA

University Publication Centre (UPENA)

JOURNAL OF MEDIA AND INFORMATION WARFARE

Centre For Media And Information Warfare Studies

Volume 1 JUNE 2008 ISSN 1985-563X

JOURNAL OF MEDIA AND INFORMATION WARFARE
Center For Media And Information Warfare Studies

Journal of Media and Information Warfare is joint published by the Centre of Media and Information Warfare, Faculty of Communication and Media Studies and University Publication Centre (UPENA), Universiti Teknologi MARA, 40450 Shah Alam, Selangor Malaysia.

JOURNAL OF MEDIA AND INFORMATION WARFARE

Center For Media And Information Warfare Studies

Volume 1 JUNE 2008 ISSN 1985-563X

Deleted Mobile Device's Evidences Recovery: A Review International Conference Media & Information Warfare: A Global Challenge In The 21st Century (M-i-war2007)

Lee Fueng, Yap, Andy, Jones

ABSTRACT

This paper presents the finding and results obtained from using commercial forensic investigation software tools to recover deleted evidences from mobile device's SIM cards, internal and external memories. The results obtained from the investigation are classified and discussed and finally, the paper highlights the limitation of the software based techniques deployed for deleted evidences recovery and presents conclusions

1. INTRODUCTION

Mobile forensic is a discipline of digital forensic that has emerged in recent years. This is due to the ubiquitous usage of mobile digital devices such as cell phones or personal digital assistant (PDA) devices in our daily activities; both work or leisure. Another substantial factor that drives the rapid development of the mobile forensics field is the evolution of mobile digital devices into a multi functional gadget with huge storage capacity that incorporates a camera, a multimedia player, a personal organizer, a file storage system, text editor and web browser functionalities as well as offering the most fundamental phone call services. With these capabilities, increasing volumes of data are being stored or exchanged between the mobile digital devices. Hence, mobile devices have become a gold-mine for the forensic investigator in serious crimes investigation (Williams, 2007) because useful evidence can be recovered from these devices.

These critical items of digital evidence are usually found in the internal memory of the mobile device i.e. random access memory (RAM) and read only memory (ROM), the device's external memory storage or the Subscriber Identity Module (SIM) card contained within the Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS) based mobile device. Forensically sounds evidence is retrieved from the mobile devices by examining the devices using digital forensic tools and following the well accepted procedures documented in (Jansen and Ayers. 2007). Some of the advance digital forensic tools available in the market are capable of retrieving deleted data from the mobile devices. Deleted evidence has served as a good source for criminal investigation as useful information may have been deleted from suspects' digital devices before they were seized by law enforcement officers. A recent notorious murder case involved Pastor Helge Fossmo, who was thought to have manipulated another person called Sara Svensson in the killings of Alexandra Fossmo and Daniel Linde in January 2004. The case was solved after the recovery of deleted information from Sara Svensson's phone. As a result of the evidence recovered, Sara Svensson was cleared of the murder charge. (The Local News of Sweden in English., 2006)

The main objective of this paper is to provide an overview and analysis on the state of the art of software-based forensic techniques deployed to recover deleted evidence from the SIM card and internal and external memories of the mobiles devices. The deleted evidence s refer to files that have been logically erased using the mobile devices graphical user interface (GUI) command but that have not been physically expunged from the storage medium. Section 2 of the paper provides a brief introduction to SIM card and mobile devices storage system. Section 3 discusses the known techniques used in the recovery of deleted files. Section 4 presents the results of recovered evidences captured from SIM cards and the memories of mobile devices using off-the-shelf software tools. The shortcomings and limitations of the software techniques are discussed and addressed in Section 5. Finally Section 6 concludes the paper with an assessment of future requirements in mobile device evidence recovery research.

2. Sim Card And Mobile Device's Memory Format

The SIM or Universal Subscriber Identity Module (USIM) is essentially a smart card containing a processor that is used in GSM and UMTS network based mobile devices respectively to securely store information. The storage capacity of SIM and USIM ranges from 2 Kilo Byte (KB) to 1 Giga Byte, but the most common storage capacities of SIMs used in GSM networks are the 32KB, 64KB and 128KB variants.

The SIM file system that has been adopted is a hierarchical structure where the Master File (MF) is the root and the Dedicated File (DF) is a subdirectory to the MF. Data is stored under the lowest layer known as the Elementary Files (EF). EF can be located directly under the MF or under the DF structure. The file allocation of the SIM is standardized through the 3GPP GSM specification, where a fixed number of mandatory files are defined for every SIM. Nevertheless, service providers have the ability to manipulate optional fields to provide customized services to their subscribers. (3GPP TS 11.11 V8.14.0, 2007)

The data stored in a SIM can be broadly classified into two categories, namely network specific information and user specific information. Network specific information consists of an authentication key, the location area identity, international mobile subscriber indentity, the service provider's name, public land mobile network selector information and short messages service (SMS) parameters. This information is usually pre-set by the service provider and is not typically changeable by the user. The most valuable information for forensic investigation purposes is the user specific information stored in the SIM such as phone book information, the SMS text message history, last dialed number and subscriber dialing numbers. Of all this information, the SMS text message is the most appealing to the forensic investigator, as the mobile device owner's interaction with third parties is recorded in the SMS text messages. The information that can be gained from SMS text messages is potentially unlimited. The text message may contain information such as the owner's social networks, business strategies, bank account information and much more.

Flash memory is used widely as the non-volatile solid state storage medium for mobile phones to store a variety of information such as contacts, calendar information, SMS text messages, video and music files, emails and photos. The capacity of flash memory for mobile devices ranges from megabytes to several gigabytes. Data in the flash memory is stored in an array of floating-gate transistors, called «cells». The NAND flash architecture is one of the two flash technologies mainly used in the embedded systems including the mobile devices. (M-System 2003)

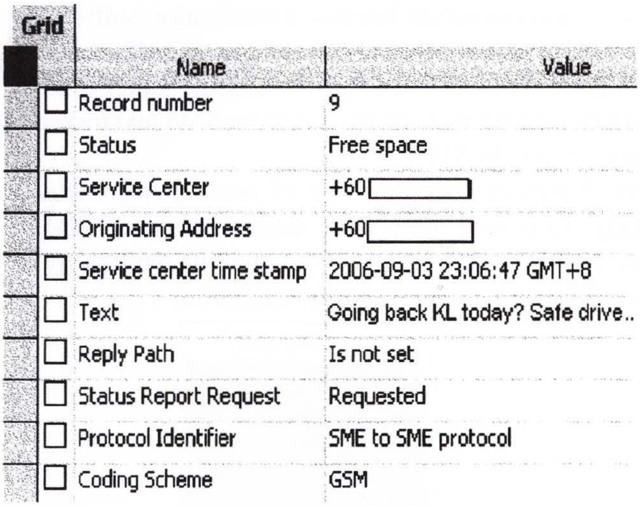
NAND flash memory is accessed or programmed at the granularity of a page. Each page is made-up of multiples of 512 bytes. Within the page a portion of the space, known as the spare area, is allocated for the storage of meta data that describes the status of the page, error correction code and also the logical to physical address mapping information. 32 pages or 64 pages will result in the forming of a block. Erasure of the contents of the flash memory is performed on a block basis. The logical block to physical block address mapping in the NAND flash memory system is typically controlled by the device driver.

Flash memory implementation of the most modern mobile device comes in two forms; internal memory that are soldered directly onto the mobile device's main board or an external memory card that is packaged in forms such as Compact Flash Cards or Smart Media Cards or Memory Sticks. The packaging methods used are usually dependent on the manufacturer and the model of the mobile device.

3. Techniques For Deleted Data Recovery

The method used for deleted SMS text message recovery from SIM is relatively straight forward. In the SIM file system specification, designated spaces are allocated for SMS storage i.e. starting from Elementary File 6F3C. Each SMS slots contain 2 fields namely the 1 byte status fields and 2-176 bytes Transport Protocol Data Unit (TPDU) field. The status byte describes the state and type of the TPDU while the TPDU field contains user data as well as information like SMS service center information, sender information, data coding scheme, protocol identifier and SMS service center time stamp information.

When a message is deleted from the mobile device, typically only the status byte is reset to "0" to mark the slot as a free space. The content of the respective TPDU remains unchanged until overwritten by new data. Hence, by dumping the entire contents of the SMS slot within a SIM using a SIM card reader and SIM card investigation software tool, regardless of its status byte, the entire SMS text message stored in the SIM can possibly be retrieved. These deleted SMS text messages are not accessible merely by browsing the SMS folder through the mobile device's GUI interface. Figure 1 illustrates the content of a deleted SMS recovered by the forensic investigation software tool used in this paper. Note that even the status of the SMS slot is marked as "free space", however, the text field is not empty.



Name	Value
□ Record number	9
□ Status	Free space
□ Service Center	+60[redacted]
□ Originating Address	+60[redacted]
□ Service center time stamp	2006-09-03 23:06:47 GMT+8
□ Text	Going back KL today? Safe drive..
□ Reply Path	Is not set
□ Status Report Request	Requested
□ Protocol Identifier	SME to SME protocol
□ Coding Scheme	GSM

Figure 1: Recovered SMS Format

The analysis and recovery of deleted information from the mobile device's internal and external memories is more complex than the mechanism used in SIM information recovery. First, a low level copy of the whole flash memory contents needs to be acquired for analysis. Next, the extracted data from the flash memory needs to be translated to a file system level that can be understood by a forensic investigation software tool in order for the tool to decode the extracted data into a form that is readable by the investigator. (Breeuwsma 2007) explains in detail some of the methods that can be used to achieve this goal. In short, the first step in the translation process involves an understanding of the NAND array structure of the memory and the spare area assignment. This information is needed in order to decode the logical sector numbers (LSN). The processed LSN information is then used to find the mapping of the physical sector to the actual high level file system. The reconstructed high level file system can then be used by the forensic investigation tool for analysis. The forensic investigation tool used in this paper transparently implements the translation process to the user.

4. Investigation Results

In this paper, a commercial forensic investigation software tool that is capable of performing physical acquisition from the mobile device's memory and SIM was used. An additional open source forensic investigation software tool was also used for SMS text message recovery investigation from the SIM.

Figure 2 summarized the type of deleted information that was successfully recovered from the mobile devices' SIM cards and memories. In this survey only 5 sample mobile devices from Malaysia and United Kingdom are used for investigation.

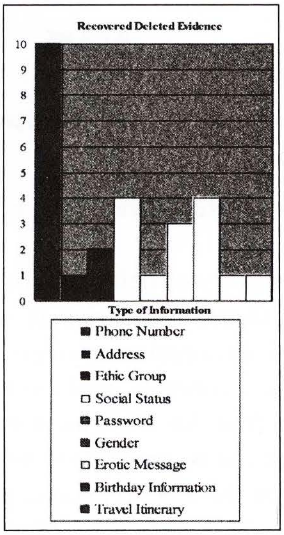


Figure 2 : Type of information recovered

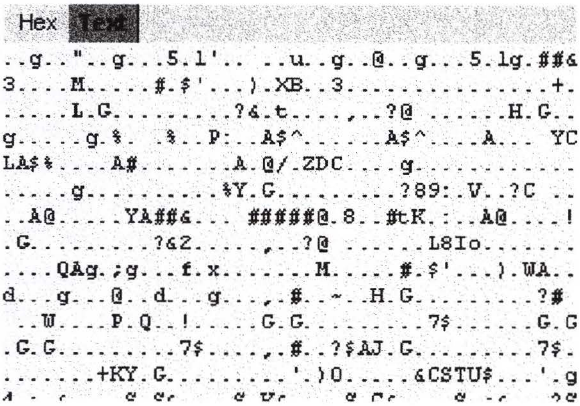
The most frequent deleted information that was recovered from mobile devices was telephone numbers. The second being social status information and erotic messages. Social status information referred to social roles, employment status and organization affiliation i.e. father, wife, paramour, status in a company or organization. The erotic messages recovered from the sample mobile devices are mainly romantic message exchanged between lovers. No hardcore and harassment related messages were recovered from the sample. From the deleted messages, gender information and ethic group of the owners can also often be deduced based on the content analysis of the text messages recovered. Mailing addresses, travel itinerary, user password and birthday information were among the data recovered during the investigation.

From the results of the investigation, it is clear that even when the users have deleted all their private data from their mobile devices before disposing them, the recovered data still contain enough information to allow for user profiling or even the identification and tracking down of the original owner of the mobile device, hence jeopardizing the privacy protection of the previous owner of the mobile device. Also, the investigation results show that a mobile device memory dump contains more useful information than a SIM card SMS slot dump. This implies that a deleted evidence recovery investigation based on SIM card SMS slot dump alone is not sufficient for a thorough investigation. Another observation from the investigation shows that open source forensic investigation software tools perform on par with commercial forensic investigation tools for SIM card based evidence recovery. Nevertheless, only commercial software forensic tools are currently capable of performing flash memory delete evidence recovery.

5. Limitation

Digital forensics is still in its nascent stage and the art of recovering deleted evidences that is forensically sound from mobile devices is still a tortuous task. Although, commercial software is available for performing physical acquisition on the mobile devices as discussed in Section 4, only a limited number of models and brands of the mobile device are supported due to the fact that most mobile devices are implemented using proprietary operating systems and having different file systems. Current forensic investigation software tool technology is not able to provide a complete and comprehensive logical sector to physical sector translation mechanism, as stated in Section 3, for each and every brand and model of mobile device available in the market.

Another challenging problems faced by investigators is on the examination and analysis work of the data grabbed from a dump of the physical memory. Typically, a memory dump contains a large volume junk that makes finding useful information a tedious and time consuming task. Figure 3 shows a screen capture of a typical memory dump using forensic investigation software tools. Although standard forensic investigation software tools come with text search and book marking facilities, the investigator still needs to go through the lines carefully in order to perform meticulous search.



```
..g.."..g...5.1'.. ..u..g..@..g...5.1g.##&
3....M.....#.$'...).XB..3...............+.
.....L.G.........?&.t....,..?@ ......H.G..
g.....g.%. .%..P:..A$^.......A$^....A... YC
LA$%....A#.......A.@/.ZDC....g...........
.....g..........%Y.G..........?89:.V..?C ..
..A@.....YA##&... #####@.8..#tK.:..A@....!
.G.........?&Z.....,..?@ ......L8Io.......
....QAg.;g...f.x........M.....#.$'...).WA..
d...g...@..d...g...,.#..~..H.G.........?#
 ..W....P.Q..!.....G.G.........7$......G.G
.G.G..........7$.....,.#..?$AJ.G.........7$.
........+KY.G..........'.)O.....&CSTU$...'.g
```

Figure 3 : Memory dump from mobile device's memory

Furthermore, most of the new mobile handsets nowadays contains a relatively large amount of storage capacity compared to the previous models. The mobile device manufacturers usually pre-programmed the mobile devices to store the incoming SMS to mobile device's internal or external memory rather than to the SIM card. Even if users are given the choice to select the SMS storage location, they will usually prefer their SMS messages to be stored on the phone memory rather than the SIM card for easy management. Hence, the SIM card is rarely being used for SMS text message storage nowadays for people using the newer generation of mobile devices. This makes the recovery of deleted messages stored in the SIM card using the method described in Section 3 impractical, as there will probably not be any SMS text messages stored in the SMS slot of the SIM card. Nevertheless, the deleted SMS recovery mechanism from SIM cards is still viable for users who store their SMS text messages on the SIM card deliberately or because they are forced to as a result of the limitations of the make and model of the mobile device that they are using.

6. Conclusions

This paper presents an overview of the state of the art in recovering deleted digital evidence. It focuses on the recovery of text messages from mobile device using off-the-shelf software-based forensic investigation tools. More research needs to be conducted to address the limitations highlight in section 5. In addition, efforts in providing privacy data protection and research into finding ways to ease the data recovery from the mobile devices need to be balanced in order to cater for the needs of higher security requirements demanded by the general public, while at the same time not imposing any restriction to forensic investigators in recovering critical evidence from the mobile device for use in resolving a criminal offences.

7. References

3GPP TS 11.11 V8.14.0. 2007. 3rd Generation Partnership Project:Technical Specification Group Terminals Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface. The 3rd Generation Partnership Project

Chris Williams., 2007. Mobile forensics turns up heat on suspects, The Register, [online], http://www.theregister.co.uk/2007/02/11/mobile_forensics_guidance/

M-Systems 2003 Two Technologies Compared: NOR vs. NAND. White Paper [online] http://www.dataio.com/pdf/NAND/MSystems/MSystems_NOR_vs_NAND.pdf

Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff and Mark Roeloffs. 2007 Forensic Data Recovery from Flash Memory. SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 1, NO. 1

The Local News of Sweden in English. 2006. Knutby pastor admits murder, The Local News of Sweden in English, [online], http://www.thelocal.se/4752/20060831/

Wayne Jansen, Rick Ayers., 2007. Guidelines on Cell Phone Forensics. NIST Special Publication 800-101

Lee Fueng, Yap
(British Telecommunications plc., Asian Research Centre, Kuala Lumpur, Malaysia; leefueng.yap@bt.com).

Andy, Jones
(British Telecommunications plc., Security Research Centre,
Ipswich, United Kingdom;
Adjunct, Edith Cowan University, Perth, Australia
ANDREW.28.JONES@BT.COM)