Pioneering Approach of Damage Recovery of Forensics Evidence Images

Shilpi Dubey*
Nitesh Dubey**

Abstract

Digital Forensic is the application of science and engineering to the legal problem of digital evidence with the reference of computer and related fields. It is a synthesis of science and law. Digital Forensic is application of forensics techniques and method in Computer, Internet, Mobile, Database, and other Digital Memory media. Because of some unique features and applications making the application of classical computer forensic techniques are very difficult nowadays. The different forensic techniques are required to gather the evidences images from the computer and store it in a digital storage media. The stored images can be damaged due to unexpected internal and external electromagnetic effects. Because of the security reasons we cannot make multiple copies of evidences images. Therefore we need some recovery techniques to get the damaged images back. We will discuss different algorithms of damage recovery. There are some major limitations of existing block recovery methods. I proposed a new block recovery format with the combination of CRC and MD5.

Keywords - *Computer forensic, Network forensic, Mobile forensic, Cellular communication, GSM, Subscriber Identity Modules, CDMA.*

Introduction

During the last twenty years, smart computer users using their machine to commit crimes have fascinated the world and generated a strange feeling composed of admiration and fear. Two words are commonly found in literature: "computer crime" and "cyber-crime". Cyber-crimes are computer crimes committed in a cyber-culture context. Mobile phones are the latest means of cyber crime. Mobile forensic is the application of science and engineering to the legal problem of digital evidence with the reference of cellular communication. It is a synthesis of science and law.

While cell phones are becoming more like desktop computers functionally, their organization and operation are quite different in certain areas. For example, most cell phones do not contain a hard drive and rely instead on flash memory for persistent storage. Cell phones are also designed more as special-purpose appliances that perform a set of predefined tasks using proprietary embedded software, rather than general-purpose extensible systems that run common operating system software. Such differences make the application of classical computer forensic techniques difficult.

It is however important that the information contained in the system is retrieved with a forensically sound method. Therefore different forensic techniques are required to gather the evidences images from the computer and store it in a digital storage media. Apart from gathering the evidence images the efficient way storage of images are also very important. The stored images can be damaged due to unexpected internal and external electromagnetic effects. Because of the security reasons we cannot make multiple copies of evidences images. Therefore we need some recovery techniques to get the damaged images back. We will discuss different algorithms of damage recovery. There are some major limitations of existing block recovery methods.

Fundamentals of Forensics

Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word *forensics* means "to bring to the court.") Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive.

*Student, Shri Ram Institute of Technology, Jabalpur
**HOD, Global Nature Care Sangathan's Group of Institutions, Jabalpur

Computer Forensics

Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information. In other words we can define the computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law [11]. This computer evidence is useful in criminal cases, civil disputes, and human resources/ employment proceedings. Many times computer evidence is created transparently by a computer's operating system and without the knowledge of the computer user. Such information is often hidden from view so that special forensic software tools and techniques are required to preserve, identify, extract and document it. It is frequently this information that benefits law enforcement and military agencies the most while gathering evidence during an investigation.

Network Forensics

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis. The second form of Network forensics relates to law enforcement. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions.

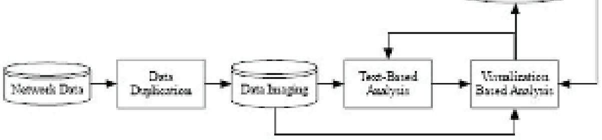


Figure-1: *Network Forensic Process*

Mobile Forensics

The mobile, compact handheld device can contain personal information including call history, text messages, e-mails, digital photographs, videos, calendar items, memos, address books, passwords, and credit card numbers. These devices can be used to communicate, exchange photographs, connect to social networks, blog, take notes, record and consume video and audio, sketch, access the Internet, and much more.

Mobile devices such as cell phones and smart phones have become an integral part of peoples' daily lives, and as such, they are prone to facilitating criminal activity or otherwise being involved when crimes occur. Importance of mobile devices from a forensic perspective is that they can contain deleted information even after an individual has attempted to render it unrecoverable. The underlying reason for this persistence of deleted data on mobile devices is in the use of Flash memory chips to store data. Flash memory is physically durable against impact, high temperature, and pressure, making it more difficult to destroy. In addition, Flash memory has a limited number of writes and can only be erased block-by-block, and mobile devices generally wait until a block is full before erasing data.

Fundamentals of Mobile Device Technology

Mobile devices are simple computers with a CPU, memory, batteries, input interfaces such as a keypad or mouthpiece, and output interfaces such as a screen or earpiece. The central unit of the phone is the CPU. The CPU controls the communication circuits of the phone, in addition to control the communication with the user. For intermediary storage, the CPU uses a RAM. RAM is used for all intermediary storage during communication and user interaction. The RAM can be implemented as a separate intergraded circuit or it can be integrated with the CPU in a single integrated circuit [9].

The phone also needs a secondary non-volatile storage. This is needed for storage of all data pertaining to user and communication that needs to persist during a power failure. Secondary storage can be implemented in various ways. The most common implementation today on mobile phones is a separate

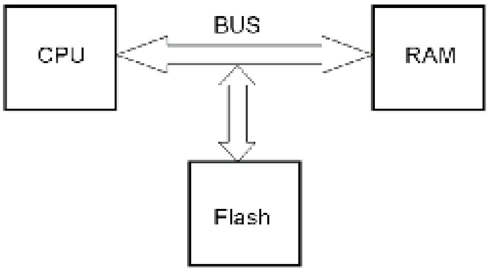


***Figure 2:** General mobile phone architecture*

flash memory integrated circuit on the system board. In addition to these elements, the CPU has communication with the SIM, and optionally other external storage media. It is also common to have a special unit to control the usage of power in a mobile phone.

Evidences in The Mobile Equipment

The following contents of modern mobile phones can have value as evidence:

- Phonebook - list of names and numbers stored.
- Call records - dialled, received and missed calls. The device may also store a recipient/sender log for messages
- SMS - short message service: all text messages stored
- MMS messages – these are messages that can be sent from and received by a mobile phone with media files such as photos and videos attached. They can also contain text messages
- Email messages - newer models of mobile phones can send and receive email messages over the internet
- Push Messages – these are specially formatted text messages that display an alert on your mobile phone. It gives the option to connect directly through a web link via the mobile phone's internet browser
- Pictures - photos can be captured directly from a mobile phone's camera or downloaded from the internet. Pictures may also be transferred to a mobile phone from another digital device
- Videos - videos captured by the phone's camera, downloaded from the internet or transferred from another device
- Audio recordings - audio/voice can be recorded by an inbuilt microphone, downloaded from the internet or transferred from another device
- Music – can be downloaded from the internet or transferred from another device
- Documents – can be created using the device's applications, downloaded from the internet or transferred from another device
- WAP - wireless application protocol, provides internet access and web browsing, storing recent history and bookmarks.
- Organizer details - calendar entries/notes/tasks are stored
- Bluetooth details – keeps a record of wireless communication between devices.
- Deleted data - deleted information can sometimes be recovered from digital circuitry, such as SIM cards.

Damage of Forensic Evidences

In computer and mobile forensic, evidence images are stored on the disk by a forensic tool. However, the stored images can be damaged due to unexpected internal and external electromagnetic effects. Existing forensic tools only provide integrity and authenticity of the evidence images by utilizing legacy cryptographic methods, i.e., applying hash values and digital signatures. Accordingly, such integrity and authenticity applied to those evidence images can be easily corrupted when the disk is damaged. Here, we focus on such limitations of the existing forensic tools and introduce a new scheme that can recover and protect the evidence images on the disk. Specifically, evidence images are divided into blocks; linkage relations between those blocks are formed; and a meta-block is applied to restore the damaged blocks. Blocks in the damaged areas detected using CRC information are subject to a multi-dimensional block operation for recovery of damaged blocks and protection for evidence images.

Evidence File Format

Encase Evidence File Format Structure

EnCase Evidence File developed by Guidance Software is the evidence image format specified for EnCase. EnCase provides high compatibility with evidence images supported by diverse forensic tools. EnCase evidence image format, as in Figure-3, consists of case information, CRC, data block and MD5 hash value.

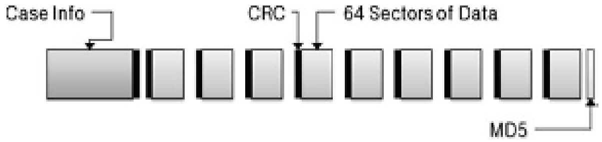
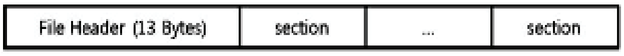


Figure-3: *Encase Evidence File*

EWF format structure

EWF (Expert Witness Compressed Format) is an industry standard image format provided by ASR Data. The maximum size of the segment file is 2Gbyte, and each segment file starts with a 13-byte file header. EWF, as in Figure-4, consists largely of a file header and sections.

The file header is divided into an 8-byte signature and a 5-byte field parts. The signature part in the EWF file header includes the signature information representing the file is in EWF evidence image format, while the field part includes the information on the quantities of segments. Every section starts with 76-byte information on the section.



File Header (13 Bytes)	section	...	section

Figure-4: *Expert Witness Compression Format structure*

Evidence Image Recovery

For recovery of a partially damaged block, Recovery Blocks are inserted as in Figure-5. Terms used in the evidence image format are defined as below.

- Data Block: the block including the CRC and data segment expressed in evidence images.

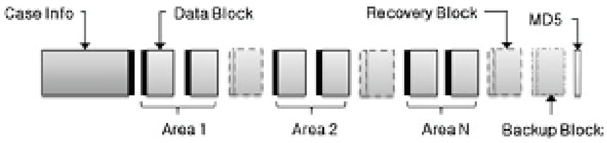


Figure-5: *The structure of evidence image format with recovery blocks inserted*

- Recovery Block: the block generated by XOR operation applied to the specific number of data blocks (Figure-6)

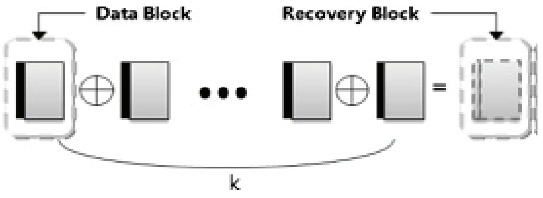


Figure-6: *Generating a Recovery Block with data blocks*

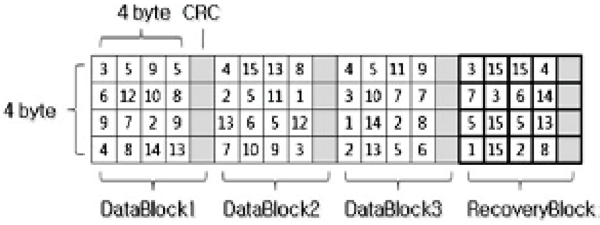
- Backup Block: the block generated by applying XOR to the specific number of recovery blocks
- Group: A group of a certain number of data blocks (group size: n)
- Area: The group involved in generating a recovery block when the group size is 1, it is not a group but a cluster of data blocks (area size: k)
- TDA (Two Dimension Area): The size of a vertical axis in case recovery blocks are arrayed in 2D (2nd area size: m).

Recovery Algorithm Using Recovery Blocks

Supposing the data blocks of an evidence image format are A, B and C and the recovery block is R, the recovery block R can be used to recover one of A, B and C, if damaged.

$$A \oplus B \oplus C = R \quad A \oplus B \oplus R = C$$
$$A \oplus R \oplus C = B \quad R \oplus B \oplus C = A$$

Damaged data blocks can be found with the CRC value. Figure-7 assumes that the data block size is 20Byte including a 4-Byte CRC value and that the recovery block is present along with a group of 3 data blocks.



DataBlock1					DataBlock2					DataBlock3					RecoveryBlock				
3	5	9	5		4	15	13	8		4	5	11	9		3	15	15	4	
6	12	10	8		2	5	11	1		3	10	7	7		7	3	6	14	
9	7	2	9		13	6	5	12		1	14	2	8		5	15	5	13	
4	8	14	13		7	10	9	3		2	13	5	6		1	15	2	8	

Figure-7: *Data allocated to data and recovery blocks*

Limitation of Existing Recovery Technique with 2D Array

In a structure where recovery blocks are arrayed in a 2D form, recovery is applicable only when no damaged data block exists in 4 points exists in 4 points where two vertical and another two horizontal lines cross. If all of the 4 crossing points have damaged data blocks, recovery is impossible. To verify this, a sample of 4×4 data and recovery block was extracted to analyze possible recovery for each type of damage. The 4 lines are defined as L1, L2, L3 and L4, and recovery is done by conducting block operations following horizontal and vertical areas. As seen in Figure-8, when damaged data blocks exist at the crossing points where two horizontal and vertical lines meet, recovery is not possible [13].

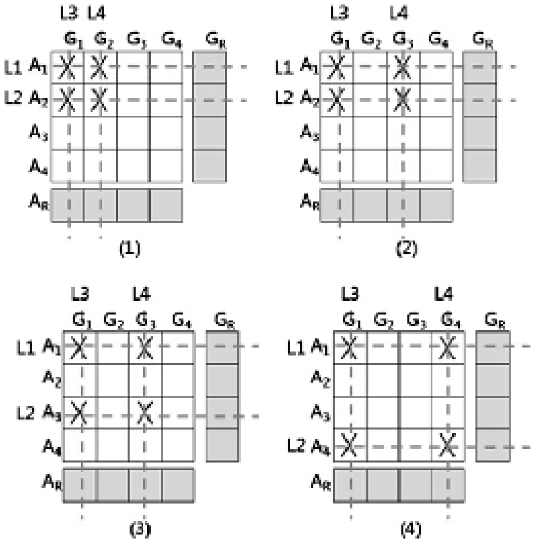


Figure-8: *Some cases of Not Recoverable damages*

Proposed Technique

We proposed an innovative approach by modifying the existing format and algorithm. This new technique comprises following:

1. Proposal of New structure (Cluster) of evidence image format with recovery blocks.
2. Proposal of New Recovery Algorithm Using new structure of Recovery Blocks.

Proposed New Structure

Proposed method is based on the concepts as discussed in section 4.4 of Chapter 4. That is, for recovery of a partially damaged block, Recovery Blocks are inserted as in Figure-9.

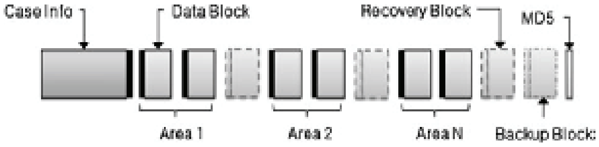


Figure-9: *Structure of evidence image format with recovery blocks inserted*

For efficient utilization of data area, we proposed to that the Area must contain at least four data blocks. That is, for recovery of a partially damaged block, the recovery-blocks are inserted after every four data-blocks, as in Figure-10.

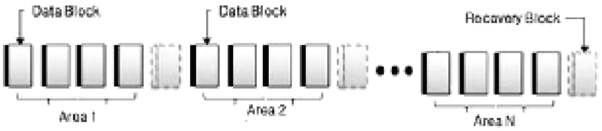
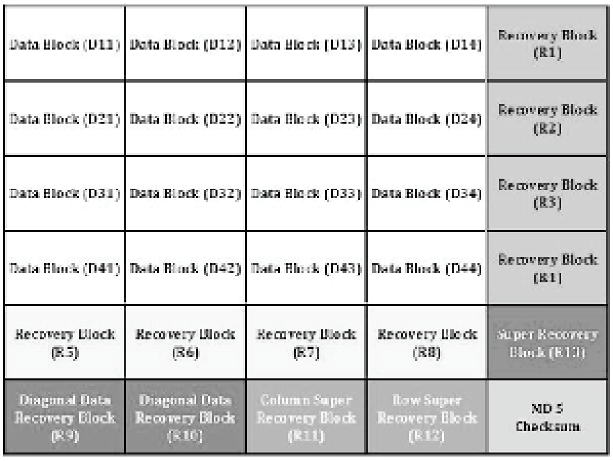


Figure-10: *New structure of evidence image format with recovery blocks*

We also proposed two-dimensional array representation (Figure-11) of data and recovery blocks (called a Cluster) to increase probability of recovery.

The minimum dimension of a cluster (2D array) is (6, 5), where 6 is number of rows and 5 is number of column. In general the size will be multiple of 6 and 5 in row and column respectively. In case of lack of multiplicity dummy data blocks can be added into rows and columns to form a cluster of required size. We also proposed one additional block for MD-5 in each cluster to make integrity of data and recovery blocks.



Data Block (D11)	Data Block (D12)	Data Block (D13)	Data Block (D14)	Recovery Block (R1)
Data Block (D21)	Data Block (D22)	Data Block (D23)	Data Block (D24)	Recovery Block (R2)
Data Block (D31)	Data Block (D32)	Data Block (D33)	Data Block (D34)	Recovery Block (R3)
Data Block (D41)	Data Block (D42)	Data Block (D43)	Data Block (D44)	Recovery Block (R4)
Recovery Block (R5)	Recovery Block (R6)	Recovery Block (R7)	Recovery Block (R8)	Super Recovery Block (R13)
Diagonal Data Recovery Block (R9)	Diagonal Data Recovery Block (R10)	Column Super Recovery Block (R11)	Row Super Recovery Block (R12)	MD 5 Checksum

Figure-11: *Cluster –The two-dimensional array representation of blocks*

The details of each block of proposed cluster are described in following section:

Recovery Blocks (R1- R8)

A Recovery block is inserted for each row and column in the cluster. Therefore for minimum configuration we require four recovery blocks (R1 to R4) for rows, and four recovery blocks (R5 to R8) for columns. The recovery blocks are generated by XOR operation applied to the specific number of data blocks.

Special Recovery Blocks (R9- R13)

These blocks are the strength of the proposed method. We proposed five additional recovery blocks to insure maximum recovery probabilities. The five additional recovery blocks are:

1. Diagonal Data Recovery Block (R9)
2. Diagonal Data Recovery Block (R10)
3. Column Super Recovery Block (R11)
4. Row Super Recovery Block (R12)
5. Super Recovery Block (R13)

Diagonal Data Recovery Blocks (R9, R10)

In existing method recovery is applicable only when no damaged data block exists in four points where two vertical and another two horizontal lines cross of 2D array of block. That is, if all of the four crossing points have damaged data blocks, recovery is impossible. Diagonal Data Recovery Blocks are the remedy of this limitation. The diagonal data recovery blocks are generated by XOR operation applied to the all data blocks of a diagonal of a cluster. With reference to Figure-5.3, the equations are as follows:

$$R9 = D11 \oplus D22 \oplus D33 \oplus D44$$

$$R10 = D14 \oplus D23 \oplus D32 \oplus D41$$

Super Recovery Blocks

Apart of data damage if some damages occurred in the recovery block itself then recovery of all blocks is nearly impossible. To overcome to this problem we also proposed the concept of Super Recovery block. That is, the Super Recovery blocks are able to recover the damaged recovery blocks. We proposed three different Super Recovery blocks:

1. Column Super Recovery Block (R11)
2. Row Super Recovery Block (R12)
3. Super Recovery Block (R13)

Column Super Recovery Block (R11)

This is to recovery of all recovery blocks comes in a single column. It is obtain by performing XOR operation in between all recovery blocks belongs to a column. With reference to Figure-5.3, the equation of R11 is as follows:

$$R11 = R1 \oplus R2 \oplus R3 \oplus R4$$

Row Super Recovery Block (R12)

This is to recovery of all recovery blocks comes in a single row. It is obtain by performing XOR operation in between all recovery blocks belongs to a row. With reference to Figure-5.3, the equation of R11 is as follows:

$$R12 = R5 \oplus R6 \oplus R7 \oplus R8$$

Super Recovery Block (R13)

It is the master recovery block used to recovery all special recovery blocks. It is obtain by performing XOR operation in between all special recovery blocks, from R9 to R12. The equation of R13 is as follows:

$$R13 = R9 \oplus R10 \oplus R11 \oplus R12$$

Algorithm for Recovery of Damaged Blocks

Perform following steps to recover damaged block:

Step 1: Get a Cluster from evidence image file as an input.

Step 2: Let the size of 2D array is (4, 4), initialize damageFlag[n] equal to zero for Recovery Block R1 to R10, value of n is from 1 to 10. In general, for (m, m) size of 2D array of data block, the size of damageFlag[] array, n, will be (2m+2). Therefore,

Set damageFlag[n] = {0}

Step 3: Get a Data Block D_{ij} from Cluster and Check for any damage. In case of damage found go to Step-4.

Otherwise, if all data blocks of a Cluster have been processed (End-of Cluster) then go to Step-6, otherwise go to Step-3.

Step 4: Perform following steps for Dij

a). damageFlag[i]++

b). damageFlag[j+4]++

c). if D_{ij} is in first diagonal then damageFlag[n-1]++

d). if D_{ij} is in second diagonal then damageFlag[n]++

Step 5: If all data blocks of a Cluster have been processed (End-of Cluster) then go to Step-6, otherwise go to Step-3.

Step 6: If all damageFlag[ ] are equal to zero (i.e. No Damage at all), then go to Step-9. If more than four damageFlag[ ] are equal to two, then recovery is not possible. Go to Step-9. Otherwise, start recovery of data block by performing following steps.

Step 7: Find damageFlag[i] such that damageFlag[i] = 1, then

a). Recover its corresponding data block (say D_{pq})

b). damageFlag[p] –-

c). damageFlag[q+4] –-

d). if D_{pq} is in first diagonal then damageFlag[n-1]--

e). if D_{pq} is in second diagonal then damageFlag[n]--

Step 8: If all damageFlag[ ] are not equal to zero, go to Step-7; otherwise go to Step-9.

Step 9: If End-of-file (EOF) then Stop as the procedure has been completed, otherwise go to Step-1.

Conclusion

At last I would like to conclude that as compare to the existing algorithm proposed algorithm is very efficient for partial damage recovery. The recovery ratio is too high and we also able to recover mostly all damaged data blocks exist at the all crossing points where two horizontal and vertical lines meet in case of two-dimensional array representation. This is the strength of the proposed algorithm. But full recovery in all cases is still not possible.

References

1. Wayne A. Jansen & Aurelien Delaitre- " Reference Material For Assessing Forensic SIM Tools", Paper No. ICCST 2007-74.
2. A Small Scale Digital Device Forensics ontology, David Christopher Harrill and Richard P. Mislan, Small Scale Digital Device Forensics Journal, VOL. 1, NO. 1, JUNE 2007-1.
3. Mobile Forensic Reference Materials: A Methodology and Reification Wayne Jansen Aurélien Delaitre ,Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, October 2009.
4. Forensics and SIM cards: an Overview, Fabio Casadei, Antonio Savoldi, Paolo Gubian, International Journal of Digital Evidence Fall 2006, Volume 5, Issue 1, University of Brescia.
5. iPod Forensics Update, Matthew Kiley, Tim Shinbara Marcus Rogers, Purdue University Cyber Forensics Laboratory, Department of Computer and Information Technology Purdue University, International Journal of Digital Evidence Spring 2007, Volume 6, Issue 1.
6. iPod Forensics, Christopher V. Marsico, Marcus K. Rogers, Purdue University Cyber Forensics Lab, Department of Computer Technology, Purdue University, International Journal of Digital Evidence Fall 2005, Volume 4, Issue 2.
7. Forensics and the GSM mobile telephone system, Svein Yngvar Willassen, M.Sc, Senior Investigator, Computer Forensics, Ibas AS. International Journal of Digital Evidence Spring 2003, Volume 2, Issue 1.
8. Kenneth E. Melson, Director, Computer Forensics, January 2008 Volume 56 Number 1 United States, Department of Justice, Executive Office for United States Attorneys, Washington, DC, 20530.
9. Svein Y. Willassen, Forensic analysis of mobile phone internal memory, Norwegian University of Science and Technology.
10. Eoghan Casey and Benjamin Turnbull, Digital Evidence on Mobile Devices, Digital Evidence and Computer Crime, Third Edition 2011, Published by Elsevier Inc.
11. US-CERT, Computer Forensics, Produced 2008 by US-CERT, a government organization. Updated 2008.
12. Mark M. Pollitt, An Ad Hoc Review of Digital Forensic Models, Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07).
13. Eun-Gyeom Jang & Byong-Soo Koh & Yong-Rak Choi, A study on block-based recovery of damaged digital forensic evidence image, Multimed Tools Appl (2012), February 2011, Springer Science.
14. Wayne Jansen, Aurélien Delaitre, Ludovic Moenner, Overcoming Impediments to Cell Phone Forensics, NIST.
15. Wayne Jansen, Rick Ayers, Forensic Software Tools for Cell Phone Subscriber Identity Modules, National Institute of Standards and Technology.
16. Wayne Jansen, Rick Ayers, Guidelines on Cell Phone Forensics, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, May 2007.