IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498,
Vol.2, No.1, 2012

A Digital Forensic Tool for Cyber Crime Data mining

Sindhu. K. K.
Computer Engineering Department,
Shah and Anchor Engineering, Mumbai University
Mumbai, India.

Dr. B. B. Meshram
Computer Engineering Department,
Veeramtha Jijabai Technological Institute,
Mumbai, India.

Abstract: - **Digital forensics is the science of identifying, extracting, analysing and presenting the digital evidence that has been stored in the digital devices. Various digital tools and techniques are being used to achieve this. Our paper explains emerging cyber crimes, forensic analysis steps in the storage media, hidden data analysis in the file system, network forensic methods and cyber crime data mining. This paper proposes a new tool which is the combination of digital forensic investigation and crime data mining. The proposed system is designed for finding motive, pattern of cyber attacks and counts of attacks types happened during a period. Hence the proposed tool enables the system administrators to minimise the system vulnerability.**

Keywords:- ***Cyber Forensic, Digital forensic tool, Network forensic tool, Crime data mining.***

I. INTRODUCTION

Computer forensics is the process that applies computer science and technology to collect and analyze evidence which is crucial and admissible to cyber investigations. Network forensics is used to find out attackers' behaviours and trace them by collecting and analyzing log and status information.
A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyber space or digital world. The investigation process is as follows. (As per National Institute of Standards and Technology).[2]

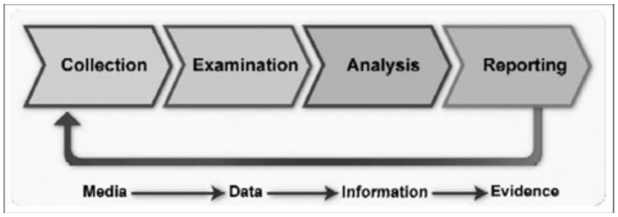

Figure 1.Digital Forensic Investigation processes.[2]

Collection phase: The first step in the forensic process is to identify potential sources of data and acquire forensic data from them. Major sources of data are desktops, storage media, Routers, Cell Phones, Digital Camera etc. A plan is developed to acquire data according to their importance, volatility and amount of effort to collect. [2].

Examination: Once data has been collected, the next phase is to examine it, which involves assessing and extracting the relevant pieces of information from the collected data.

Analysis: Extracted and relevant data has been analysed to draw conclusions. If additional data is sought for detail investigation will call for in depth data collection.

Reporting: This is the process of preparing and presenting the outcome of the Analysis phase.

Digital Forensic Science covers Computer forensics, Disk forensics, Network forensics, Firewall forensics, Device forensics, Database forensics, Mobile device forensics, Software forensics, live systems forensics etc. In this paper we explain file system forensics and network forensics.

II. EMERGING CYBER CRIMES

Computers are integral part of our life. A significant percentage of today’s transactions and processes take place using information technology and the future is pregnant with innovations, including nanotechnology, silicon chips, quantum computers and even biochips. People have readily adopted this technology and have innocently trusted it while performing many tasks, with ignorance about the limitations and threats to their securities. With this advance in technology, an equally advanced form of crimes has emerged. The crimes being committed in the cyberspace like Internet fraud, business espionage, pornography, sexual assault, on-line child exploitation, cyber terrorism and more are on the rise. Following statistical data shows various attacks and their total percentage.

Attack	Reported cases
Data Theft	33%
Email abuse	22%
Unauthorized Access	19%
Data alteration	15%
Virus attacks	5%
DoS attacks	3%
Others	3%

Table 1. Statistical data of Emerging Cybercrimes

A. Data Theft

Data is a precious asset in this modern age of Cyberworld . Data is an important raw-material, for business organizations Call Centres and I.T. Companies. Data has also become an important tool and weapon for companies, to capture larger market shares. Due to the importance of Data, in this new age, its' security has become a major issue in the I.T. industry. The piracy of Data, is a threat, faced by the I.T. players, who spend millions to compile or buy Data from the market. Their profits depend upon the security of the Data. Above statistics reveals 33% of cybercrime is data stealing.

A case reported at Bangalore (9 Crore loss) some key employees of the company stolen source code and they launched a new product based on stolen source code and mailed into former clients.

Table 2. Cyber attacks

Types of attack	Description
Hacking	illegal intrusion into a computer system without the permission of the computer owner/user.
DoS	attempts to "flood" a network, thereby preventing legitimate network traffic
DDoS	large numbers of compromised systems (sometimes called botnet) attack a single target.
Software Piracy	Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
Pornography	Child prornography refers to images or and in some cases writings depicting sexually explicit activities involving a; as such, child pornography is a record of child sexual abuse
Spoofing	Hiding source of attack and do the attack
Virus	A program that infects computer files,
Threatening	Sending threatening mails
Phishing	phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details
Salami Attack	Collecting fraction of money from different accounts
ZeroDay attack	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public
War Driving	A method of gaining entry into wireless computer networks

Social engineering techniques can also applying to do this attack. For example A beautiful lady meets young system admin and collected the username and password.

B. Email abuse

Email abuse takes many forms, for example: unsolicited commercial email, unsolicited bulk email, mail bombs, email harassment, email containing abusive or offensive content. The format for submitting reports to the abuse department regarding abuse of email is always the same whatever the offence.

C. Unauthorized access

Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner. The popular term is “hacking”. By hacking viewing private accounts, messages, files and resources when one has not been given permission from the owner to do so.

Viewing confidential information without permission or qualifications can result in legal action.

D. Data Alteration

By changing /modifying / deleting data causes major losses in the Cyber world. A crime reported in USA (Cybermurder) , a patient file data altered by a criminal cause overdose of medicine and patient get killed.

E. Denial of Service (DoS)

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target. Dos causes

- attempts to "flood" a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person

Impact of the DoS is Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization. Secondly some denial-of-service attacks can be executed with limited resources against a large, sophisticated site.

F. Malicious codes

Viruses, worms and Trojans are the types of malicious code which enters into the system without permission of the user and deletes, modifies and captures the user files and data

III. File System Forensic.

File system investigation is the identification, collection and analysis of the evidence from the storage media. File systems or file management systems is a part of operating system which organize and locate sectors for file storage.[5,6]

A. Basic Steps in storage media investigation.

1. Replication of forensic image: - Nonintrusive acquisition of a replicated image of data extracted from the questioned device.
2. For integrity perform Hash value calculation.
3. Conducting a file-fragment recovery procedure to recover files and folders to a new location.
4. Examine all files especially deleted files
5. Reviewing typical evidentiary objects such as:
    a. Analyse free spaces, slack spaces and bad sectors
    b. Application software file.
    c. Digital camera, printer and ancillary devices.
    d. E-mails, Games & Graphics images
    e. Internet chat logs & Network activity logs
    f. Recycle folders
    g. System and file date / time objects
    h. User-created directories, folders, and files
    i. Latent data extraction from page, temp, and registry space.
6. Copy the content of the evidentiary object into text files.
7. Searching for key-term strings.
8. Reviewing file notations.
9. Scrutinize applications or indications of as file eradications, file encryption, file compressors or file hiding utilities.
10. Preparing evidence summaries, exhibits, reports, and expert findings based on evidentiary extracts and investigative analysis.

B. Creation of image of attacked system

Windows File system using WinHex[13]

a. open WinHex
b. open particular drive (Tools →open disk)
c. Calculate Hash value of the drive/disk
    i. (Tools →compute hash)
    Store hash value in a text file.
d. save disk content as image file extension .img file

Linux File system - using *dd* command

```
dd if =/dev/<suspect drive>  bs=512  of=</some
dir/imagename>  bs=512
```

if: The disk image to read from
of: The output file to save to
bs: The size of the block to read each time, 512 bytes is the default
skip: The number of blocks to skip before reading, each of size bs
count: The number of blocks to copy from the input to the output, each of size bs 63. In many cases, we will want to use a 512-byte block size because that is the size of a sector. The default block size for dd is also 512 bytes

Example:

```
# dd if=/dev/zero of=/dev/forensic/image1
2+0 records in
2+0 records out
```

C. Perform Integrity Checking (Hash Value Calculation).

a. Open winHex[13]
b. Calculate Hash value of image (Select Tools menu →compute hash)
c. Select the Algorithm for hash finding checksum , MD5, SHA-1, SHA-2
d. The calculate value save it into text file for checking integrity

In Linux the MD5SUM command

```
#md5sum forensic/image1
3b85ec9a456984b91070128be6bbd25eb  image1 file
```

D. Hidden Evidence Analysis in the file system.

Suspects can hide their sensitive data in various areas of the file system such as Volume slack; file slack, bad clusters, deleted file spaces. [8]

1) *Hard disk:* The maintenance track / Protected Area on ATA disks are used to hide information. The evidence collection tools can copy the above contents.

2) *File System Tables*: A file allocation table in FAT and Master File Table in NTFS are used to keep track of files. These entries are manipulated to hide vital and sensitive information. [8]

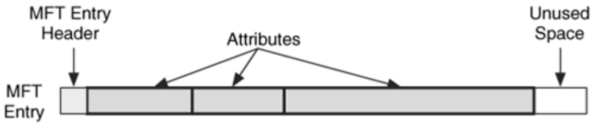

Figure 2 MFT Structure.[8]

3) *File Deletion*: When a file is deleted, the record of the file is removed from the table, thereby making it appear that it does not exist anymore. The clusters used by the deleted file are marked as being free and can now be used to store other data. However, although the record is gone, the data may still reside

in the clusters of the hard disk. That data we can recover by calculate starting and end of the file in Hex format and copy it into a text file and save with corresponding extension.

Recover a JPEG file

a. Open file in the hex format
b. Check the file signature
c. Copy From starting signature upto ending signature.
d. For example (JPEG/JPG/JPE/JFIF file starting signature is FF D8 FF E1 XX XX 45 78 69 66 00 (EXIF in ascii Exchangeable image file format trailer is FF D9).
e. Open the file with corresponding application.

4) *Partition Tables*: Information about how partitions are set up on a machine is stored in a partition table, which is a part of the Master Boot Record (MBR). When the computer is booted, the partition table allows the computer to understand how the hard disk is organized and then passes this information to the operating system. When a partition is deleted, the entry in the partition table is removed, making the data inaccessible. However, even though the partition entry has been removed, the data still resides on the hard disk.

5) *Slack space*: A file system may not use an entire partition. The space after the end of the volume called *volume slack* that can be used to hide data. The space between Partitions is also vulnerable for hiding data. *file slack* space is another hidden storage. When a file does not end on a sector boundary, operating systems prior to Windows 95 a fill the rest of the sector with data from RAM, giving it the name *RAM slack.* When a file is deleted, its entry in the file system is updated to indicate its deleted status and the clusters that were previously allocated to storing are *unallocated* and can be reused to store a new file. However, the data are left on the disk and it is often possible to retrieve a file immediately after it has been deleted. The data will remain on the disk until a new file overwrites them however, if the new file does not take up the entire cluster, a portion of the old file might remain in the slack space. In this case, a portion of a file can be retrieved long after it has been deleted and partially overwritten.

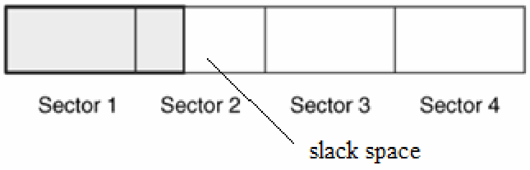

Figure 3. File slack [8]

6) *Free space*: However, when a file is moved from one hard disk or partition to another, it is actually a multistep process of copying and deleting the file. First, a new copy of the file is created on the target partition. After the file has been copied, the original file is then deleted. This process also requires some housekeeping in the FAT or MFT tables. A new entry is created in the table on the partition where it has been copied, whereas the record for the deleted file is removed from the table on its partition. When a file get deleted, that space considered as free space, there also criminal can hide sensitive information.[8]

7) *Faked Bad Clusters:* Clusters marked as bad may be used to hide data. In NFTS, bad clusters are marked in metadata file called $BadClus, which is in MFT entry 8. Originally, $BadClus is a sparse file which file size is set to the size of entire file system. When bad clusters are detected, they will be allocated to this file. The size of data that can be hidden with this technique is unlimited. Suspects can simply allocate more clusters.[8][9]

Following commands extracts the slack space of file with MFT number 25. To get the file size using Slueth Kit.

a) Display details of a meta-data structure FAT or MFT

```
./istat .f ntfs /forensic/image1 25
```

b) Calculate the RAM slack and drive slack

```
file slack = allocated size . real size
drive slack = int(file slack / 512) * 512
RAM slack = file slack - drive slack
```

To extract the entire file with MFT number 25 including its file slack

c) icat command to save the data located at that particular NTFS or inode.

```
./icat .sf ntfs /forensic/image1 25 > /forensic/file25
```

Assume that the file size is 229875 and RAM slack is 300 bytes.

d) To extract RAM slack command dd using as follows

```
dd if=/forensic/file25 of=/forensic/RAMslack bs=1
skip=229875 count=300
```

e) To extract drive slack command dd using as follows

```
dd if=/forensic/file25 of=/Forensic/driveslack bs=512
skip=235 count=1
```

Faked Bad Clusters: Clusters marked as bad may be used to hide data. In NFTS, bad clusters are marked in metadata file called $BadClus, which is in MFT entry 8. Originally, $BadClus is a sparse file which file size is set to the size of entire file system. When bad clusters are detected, they will be allocated to this file. The size of data that can be hidden with this technique is unlimited. Suspects can simply allocate more clusters.[8][9]

Using Sleuth Kit – The following command $BAD attribute allocated to bad Clusters by Master File table (MFT)

```
istat /forensic/image1 .f ntfs 8
```

'dcat' command of Sleuth Kit checks the bad clusters. However, this only reveal hidden data if the data is stored in ASCII encoding.

In this example, let.s assume cluster 383624-383635 are marked as bad cluster and suspected to contain hidden data.

```
dcat /forensic/image1 .f ntfs 383624 12
```

```
dd if=/forensic/image1 bs=4096 skip=383624 count=12
of=/forensic/badclusters.img
```

open forensic/badclusters file in winHex and recover the content into a file.

E) Keyword Search

Keyword search can also be performed with WinHex, strings or other tools if part of the content of the hidden file is known.

```
#strings /forensic/image1 | grep keyword
```

III. NETWORK FORENSIC ANALYSIS

Network forensics is capturing, recording and analysis of network events in order to discover the source of cyber attacks. In network forensics there are two major types of investigation [1][7] i.e. Network Traffic Analysis & Log Files Analysis.

A. Network Traffic Analysis

Network traffic analysis can be used to reconstruct and analyse network-based attacks, inappropriate network usage. The content of communications carried over networks, such as e-mail, chat etc can also support of an investigation. A Packet Sniffer tool is used for capturing network traffic. The header information encapsulated in the captured packet can be analysed by the forensic analyst. [3]
Identification of an event of Interest

There are two types of identification will come.

1. Someone within the organization – system administrator, network administrator, user or employee.
2. Some monitoring system like IDS or Firewall alerts showing a incident happened.[7].

Network traffic Analysis an Example:
Investigation of Network Traffic Example ICMP attacks:

a. Capture packets
b. First analyze packet header of ICMP
c. Find the status code of ICMP.
d. Check the parameter values Type and Code
e. Create rule sets
f. Find the attack.

'Internet Control and Messaging Protocol' (ICMP) it is a error reporting and messaging protocol

Type	**Name**	**Code**
0	Echo Reply	0 No Code
03	Destination Unreachable	0 Net Unreachable 1 Host Unreachable 2 Protocol Unreachable
04	Source Quench	0 No Code
05	Redirect	0 Redirect Datagram for

Table 3. Status code of ICMP

Attacks on ICMP protocol	Attack Description	Parameters
ICMP sweep	By sending a series of ICMP echo request□ packets to every IP on a network segment, an attacker will receive ICMP replies confirming a sweep, finding active hosts and perform more direct targeted attacks specific to those hosts.	Type =8 and code=0
Ping of death	The attacker sends excessively large ICMP messages to a target host. Attacker can send an ICMP packet greater than the maximum of 65535 octets allowed . It will crash the connection or host.	Total IP packet size > 655355bytes

Table 4. ICMP attacks and parameters

Algorithm for finding malicious traffic or ICMP attacks.
ICMP Sweep attack

```
1.    Take the header of the captured packet
2.    Extract the header attributes.
3.    IF type = 8 and code = 0 THEN Pattern= ICMP
        sweep attack
4.    Check for the IP addresses
      (IF source IP!= host IP THEN) THEN record IP
        ,Date, time
```

5. Increment or update a counter variable.

Finding Ping of Death

1. Take the header of the captured packet
2. Extract the header attributes.
3. IF TotalsizeofIPpacket > 65535 bytes THEN Pattern=Ping of Death

Using above rule sets finding suspicious packets and marks packets, using counter variable pseudo-code adds and updates the value of corresponding counts which is used to validate the attacks. The threshold values are compared with this counts which results in the attack information. (statistical method validate the attacks).[15]

Child pornography investigation examination process would include

1. Examining all graphics or video files from network traffic,
2. Examining all Web sites accessed.
3. Examining all Internet communications such as IRC, Instant Messaging (IM), and e-mail.
4. A search for specific usernames and keywords to locate additional data that may be relevant.
5. Once most of the relevant data to the investigation have been extracted from network traffic.
6. Extracted Data made readable,
7. They can be organized in ways that help an individual analyze them
8. Gain an understanding of the crime.

B. *Log files Analysis:*

During investigation to recognize malicious activities by mining user log files. Access logs can contain vast amount of data regarding each user activities. [10].

Analysis steps:

1. Input a server log file.
2. Identify each sessions.
3. Log file parser converts dump file into formatted order.
4. Using a Search function find the required data. Or Data mining algorithms give relations or sequential patterns.

IV. Data Mining For Digital Forensics

Cyber Crime Data mining is the extraction of Computer crime related data to determine crime patterns. With the growing sizes of databases, law enforcement and intelligence agencies face the challenge of analysing large volumes of data involved in criminal and terrorist activities. Thus, a suitable scientific method for digital forensics is data mining. Crime data mining is classified as follows. [11][12]

1) *Entity extraction* has been used to automatically identify person, login ID, Password, ID no, IP of the system, and personal properties from reports or logs.

2) *Clustering techniques* such as “concept space” have been used to automatically associate different objects (such as persons, organizations, hardware systems) in crime records.

3) *Deviation detection* has been applied in fraud detection, network intrusion detection, and other crime analyses that involve tracing abnormal activities.

4) *Association* rule has been applied to finding aassociations and sequential patterns between web transactions are based on the Apriori Algorithm.

Mining results shows motive, pattern and counts of similar types of attacks happened during a period.

A) *Crime Data mining Algorithm*

1. Identify variables/ itemsets from Case investigation report (our proposed system stores these variables as attributes of tables)

2. Find frequent item sets by using Apriori algorithm

   Employs an iterative level to find set of frequent itemsets

   E.g. if an attacker attacked database login attempt results a data loss / Data tampering case report show attributes Data deleted ,Login attempt , attack type=SQL injection,

   If these item sets are frequent then we can set rule “motive of attack is Data theft”

3. Make Association rules.

   i.e. It is a rule in the form X→Y showing an association between X and Y that

   if X occurs then Y will occur. If the attacker accessed operating system files then we can say motive of attack is system Crash. If the attacker attacked Database login and password steel then we can say criminal motive for data theft/ data change.

4. This maximum frequent item sets also shows attack patterns.
5. Finding other signs of evidence Correlation, contingences. (Consider these values while making rule sets)
6. Set SQL queries according to the rules.
7. Retrieve data.

V. DECISION MAKING FORENSIC TOOL FOR CYBER CRIME INVESTIGATION

Our proposed model is the combination of digital forensics and data mining. Our proposed system helps to increase the security of the organization. When an incident reported, it investigates and report is saved in the database. Using crime data mining tool the nature of the attack is identified and alert administrator about similar attacks in future. Proactive measures can be initiated to prevent future cyber attacks.

A Block diagram of the proposed system:

Graphical User Interface: - It is used by the forensic investigator to enter case details and apply tools (File system, Network) to collect evidences. Investigators can input their queries in the system. This also displays the result of the query in the form of Bar chart or report. It is the presentation layer of our three tier architecture.

File system Tool: - This tool Collects evidence from the file system, it recovers all files, searches data in the free space, slack spaces and deleted spaces.

Network Tool: - This tool collects data from the network traffics and server log files.

Database: - Database loader collects evidences from the above tools and loader loads into the database as attributes of the tables. OLTP (Online Transaction Processing): Set relations between the tables of the detected crime attributes. This applies data mining and extracts of required data. OLAP (Online Analytical processing) apply analytical queries and retrieves the output / decisions. Database server helps to store and retrieve crime attributes and results.

B) Software design of the System

Network Forensic Module is equipped with a traffic monitoring tool for data / evidence collection. A packet analyser provides live forensic information about an attack. Java has API Jpcap captures information from the live network. The Network Analysis module analyse different types of packets ICMP, TCP, UDP.

Log file analyser module parses the web server logs, syslogs and searches required keywords and patterns, which helps investigator to detect attacks like SQL injection, Brute Force attack for the login attempt.

File system Analyser module finding the evidence from the deleted files, free spaces (File slack, Volume slack).

The above modules give the output to flat file or CSV file.
A Java program module (File converter / Database Loader) converts as Table format and loads into the database. Apply an Association mining (Apriori Algorithm) finding relation between these item sets of Crime Data and generate a prediction.

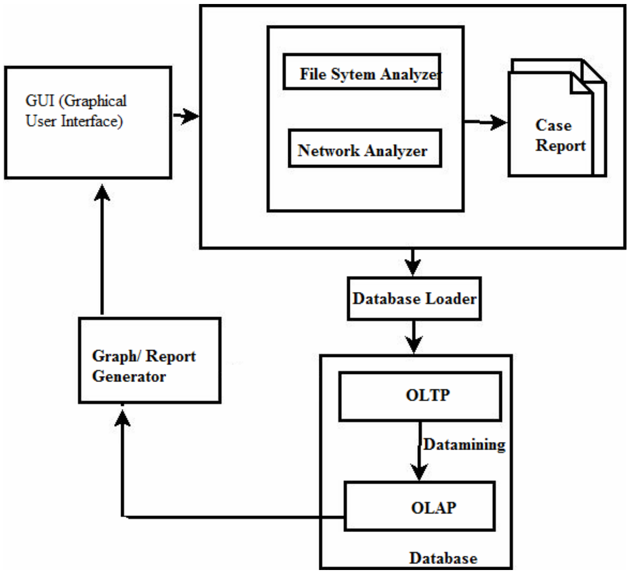

Figure 4 Block Diagram of proposed model.

Graphical visualization module generates the required results in the form of Bar Charts or Graphs.

Conclusion

This paper explains the hidden evidence acquisition from file system. Second section explains investigation on the Network. There are two types of investigation in network, live data acquisition (Packet capturing and analysis) and log file analysis. Third section explains crime data mining. On the basis we propose a new system with Digital forensic tool for decision making in the computer security domain.

References

[1]. H. Achi, A. Hellany & M. Nagrial. Network Security Approach for Digital Forensics Analysis 2008 IEEE

[2]. Karen Kent, Suzanne Chevaller, Tim Grance, Hung Dang. Guide to Integrating Forensic Techniques into incident response.

[3]. Eoghan Casey Network traffic as a source of evidence: Tool strengths, weaknesses, and future needs; Digital investigation Journal December 2003.

[4]. Stephen K. Brannon, and Thomas Song Computer Forensics: Digital Forensic Analysis Methodology. Compter Forensics Journal January 2008 Volume 56

[5]. Dava Klieiman , Kevin,Timothy, Micheil Cross The official CHFI Study guide for forensic Investigators.

[6]. Brian Carrier . File system Forensic Analysis. Publisher addison Wesley Professional .publication Date. March 17, 2005

[7] Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A.Tools And Techniques For Network Forensics, USA International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,April 2009.

[8]. Cheong Kaiwee. Analysis of Hidden Data in NTFS File system. whitepaper

[9]. Mamoun, Alazab, Sitalakshmi Venktraman, Paul Watters. Effective Digital forensic Analysis of the NTFS Disk Image. Ubicc Journal, vol 4.

[10]. Ali Reza Arasteh, Mourad Debbabi, Assaad Sakha, Mohamed Saleh Analyzing multiple logs for forensic evidence Digital investigations Journal Science Direct.

[11]. Vitoras Justickis Criminal Datamining, chapter 33 of Security handbook of electronic Security and Digital Forensics.

[12]. Chen, H., Chung, W., Qin, Y., Chau, M., Xu, J. J., Wang, G., Zheng, R.,Atabakhsh, H. (2003). Crime Data Mining: An Overview and Case Studies. ACM International Conference Proceeding Series; Vol. 130, 1-5

[13] www.winHex.Org.

Author profile

Dr. B. B. Meshram is working as Professor in Computer Technology Dept., VJTI, Matunga, Mumbai. He is Ph.D. in Computer Engineering and has published international journal is 25, National journal is 1, international conference is 70 and national conference 39 papers to his credit. He has taught various subjects such as Object Oriented Software Engg., Network Security, Advanced Databases, Advanced Computer Network (TCP/IP), Data warehouse and Data mining, etc at Post Graduate Level. He has guided several projects at graduate and post graduate level. He is the life member of CSI and Institute of Engineers, etc.

Sindhu.K.K is working as Lecturer in Computer Engineering Dept. Shah and Anchor Kutchhi Engineering College , Mumbai. She is pursuing her M Tech in Computer Engineering with specialization in Network Infrastructure management System, VJTI, Matunga. and has published her papers international journal as well as international conferences. She has taught various subjects such as Web Technologies, Web Engineering , Internet Programming , Network Security at Graduate Level. She has guided several projects at graduate level . She worked as counsellor in IGNOU for MCA, BCA . She is also Associate member of Institution of Engineers (India) . She is interested in digital Forensic so doing Certification of Digital Evidence Analyst from Asian school of Law India.