I. J. Computer Network and Information Security, **2012, 4, 39-48**
Published Online May 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.04.05

Digital Forensic Investigation Tools and Procedures

K. K. Sindhu, Dr. B. B. Meshram
Shah And Anchor Kutchhi Engg College. Mumbai, India, Veermata Jijabai Technological Institute, Mumbai, India
kksindu@gmail.com. bbmeshram@vjti.org.in.

Abstract — Due to the significance of Data, in this new age, its' security has become a major issue in the I.T. industry. Cyber attacks from various sources are demanding its prevention in the new era of information security. Digital forensic is a relatively new fields that is the collection, analysis and documentation of a Cyber attacks. It is becoming increasingly important as criminals aggressively expand the use of technology in their enterprise of illegal activities. Digital forensics investigators have access to a wide variety of tools, both commercial and open source, which assist in the preservation and analysis of digital evidence. A small percentage of cyber criminals being convicted confirm the difficulty in detection of digital crime and its consequent procedural proving in the court of law. An established forensic analyst mines the crucial evidence from susceptible locations to comprehend attacker's intension. The typical goal of an investigation is to collect evidence using generally acceptable methods in order to make the evidence is accepted and admitted on the court. Efficient digital Tools and procedures are needed to effectively search for, locate, and preserve all types of electronic evidence. Main focus of this paper is the complete investigation procedure of storage media. Our paper also explains emerging cyber crimes and its digital forensic investigation procedures using digital forensic tools and techniques.

Index Terms **—** Digital Forensic Investigation, Digital forensic tools, Cyber crime, Storage media forensic

I. Introduction

Different types of cyber attacks from various sources may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself. So the companies and products aim to take assistance of legal and computer Forensics. Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices. Digital information is fragile in that it can be easily modified, duplicated, restored or destroyed, etc. In the course of the investigation, the investigator should assure that digital evidence is not modified without proper authorization .Various digital tools and techniques are being used to achieve this. Forensic tools and techniques are integral part of criminal investigations used to investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. This paper first section explains introduction and second section describes different steps in the digital forensic investigation and third part explains about the types of cyber crimes Fourth section explains the investigation procedure of different cyber crimes including complete investigation of storage media. Any crime committed in the computer or cyber world starts from the basic investigation procedure of storage system. So our paper helps an investigation become easier and faster.

II. Digital Forensic Investigation.

A computer forensic investigator follows certain stages and procedures when working on a case. First he identifies the crime, along with the computer and other tools used to commit the crime. Then he gathers evidence and builds a suitable chain of custody. The investigator must follow these procedures as thoroughly as possible. Once he recovers data, he must image, duplicate, and replicate it, and then analyze the duplicated evidence. After the evidence has been analyzed, the investigator must act as an expert witness and present the evidence in court. The investigator becomes the tool which law enforcement uses to track and prosecute cyber criminals.

Forensic investigator follows all of these steps and that the process contains no misinformation that could ruin his reputation or the reputation of an organization.

1. Company personnel call the corporate lawyer for legal advice.
2. The forensic investigator prepares a First Response of Procedures (FRP).
3. The forensic investigator seizes the evidence at the crime scene and transports it to the forensic lab.
4. The forensic investigator prepares bit-stream images of the files and creates a MD5 # of the files.
5. The forensic investigator examines the evidence for proof of a crime, and prepares an investigative report before concluding the investigation.

6. The forensic investigator hands the sensitive report information to the client, who reviews it to see whether they want to press charges.

A) Stages of Forensic Investigation

Digital forensics includes Assess, preserving, collecting, confirming, identifying, analyzing, recording, and presenting crime scene information.

1. Assess the Crime scene: To conduct a computer investigation, first one need to obtain proper authorization. That process begins with the step of assessing the case, asking people questions, and documenting the results in an effort to identify the crime and the location of the evidence. Review the organization's policies and laws and build a team for the investigation. Conduct a thorough assessment of the crime scene. In this investigators prioritise the actions and justify the resources for the internal investigation.

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]. Evidence is most commonly found in files and Databases that are stored on hard drives and storage devices and media. Finding the evidence, discovering relevant data, preparing an Order of Volatility, eradicating external avenues of alteration, gathering the evidence, and preparing a chain of custody are the main steps in the collection phase.
   Maintaining the chain of custody is the important step. Identification of the evidence must be preserved to maintain its integrity. So Hash calculation is applying into each collected evidence.. Sometimes a computer and its related evidence can determine the chain of events leading to a crime for the investigator as well as provide the evidence which can lead to conviction.

3. Analysis phase: Examine the collected data/files and finding out the actual evidence. The computer forensic investigator must trace, filter, and extract hidden data during the process.

4. Report phase: The audience will be able to understand the evidence data which has been acquired from the evidence collection and analysis phases. The report generation phase records the evidence data found out by each analysis component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody

B) Chain-of-custody and Documentation

Documentation is essential to the investigation. For evidence to be reliable in court, integrity has to be preserved. Safe storage and tamper protection is needed, so is also the documenting of handling, i.e. who has accessed the evidence while it was in custody. Chain of custody prevents accusation in court that the evidence has been tempered with. Evidence need to be identified and labelled as soon as it is collected. All actions performed by the investigator should be documented, including the reasons for doing so. In digital forensics, this means logging all actions and integrity checks.

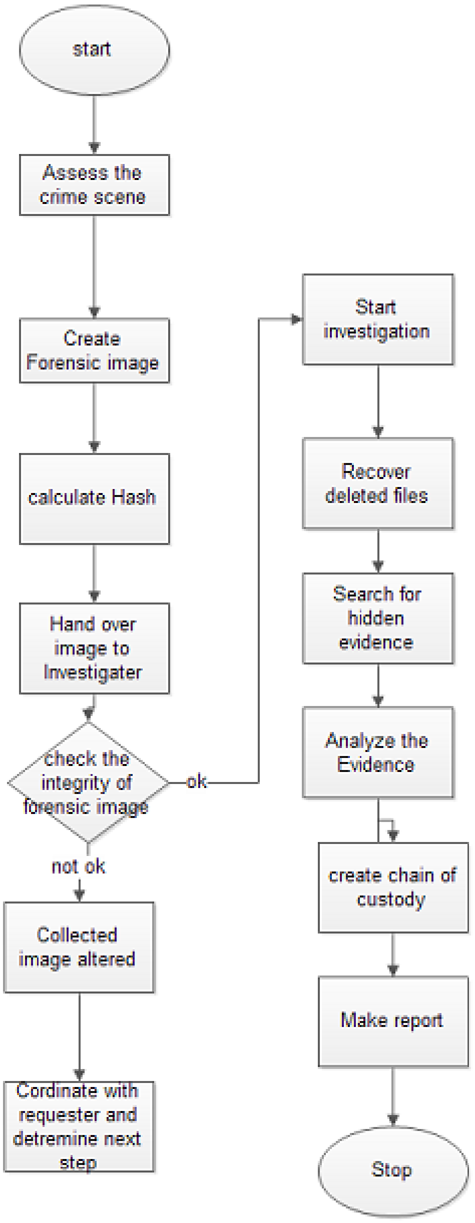


Figure 1 Shows Flow chart of Digital Forensic Investigation processes

III. Emerging Cyber Crimes

A cyber crime can be defined as Crime committed in the cyberspace or Crime committed with the assistance of the Internet. In cybercrime externally or internally computer takes the part of the attack .Cyber crime investigations are always difficult because the evidences are very critical ie the life of data are sometime within fraction of second. Evidences in the running memory , registers are available only some seconds. Digital Evidence [4] at present, the analysis of digital evidence must depend on the forensics tools such as Forensic Toolkit (FTK) of Encase, or WinHex. Most of them are commercial software and are too expensive for the small enterprises or individual. Digital evidence is stored in computer can play a major role in a wide range of crimes, including murder, rape, computer intrusions, espionage, and child pornography in proof of a fact about what did or did not happen.

C). Types of cybercrimes

The crimes being committed in the cyberspace like Data theft, 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.

Table 1 shows the statistical data about different types of attacks reported.

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

Intellectual Property Theft / Data Theft: IPR crimes like act that allows access to patent, trade secrets, customer data, sales trends, and any confidential information. Data is a precious asset in this modern age of Cyber world. 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. 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.

Damage of company service networks This can occur if someone plants a Trojan horse, conducts a denial of service attack, installs an unauthorized modem, or installs a back door to allow others to gain access to the network or system.

Financial fraud: This pertains to anything that uses fraudulent solicitation to prospective victims to conduct fraudulent transactions.

Hacker system penetrations: These occur via the use of sniffers, rootkits, and other tools that take advantage of vulnerabilities of systems or software.

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.

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 or 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.

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

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 bonnet) 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.

Distribution and execution of viruses and worms : 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.

Child pornography: Child pornography refers to images or and in some cases writings depicting sexually explicit activities involving as such, child pornography is a record of child sexual abuse.

D). Sources of Cyber Crimes.

Cyber crimes such as network intrusion, hacking, virus distribution, denial of service attacks, hijacking (a computer or network), defacing Web sites, cyberstalking, and cyberterrorism are included in this category.

Basically the computer itself becomes the “target” as well as “Source” of the crime. That is “unauthorized access” to the targeted system. The transmission of a program, information, code, or command, and as a result of intentionally causes damage without authorization, to a protected computer.

1. Program/ program source code
2. Disgruntled employees.
3. Teenagers.
4. Political Hacker.
5. Professional Hackers.
6. Business Rival.
7. Desperados
8. Terrorists

Credit card fraud and identity theft :

1. E- mails from spoofed IP address.
   The e-mail directs the user to visit a Web site where he/she is asked to update personal information, such as passwords, credit card, social security, and bank account numbers that any legitimate organization already would have had. The Web site, however, is bogus and set up only to steal the user’s information. So Phishing, also referred to *as brand spoofing or carding.*
2. Duplicated websites.(E-commerce or E-Banking).

E). Child pornography

Generally Technological progress and advancement is valued by society. However, it seems that every technological advance is quickly embraced by offenders for illegal purposes, particularly when applied to child pornography. For example:

1. Digital cameras or mobiles are affordable and carry no risk to the owner of the fear of being discovered in external film development.
2. Computer usage of the children.
3. Everyone has access to vast amounts of child pornography via the Internet.
4. Photographs and movies are easily organized, concealed, and stored in a user’s collections.
5. Use of chat rooms, e-mail, and so forth, allows offenders to reach out to like-minded individuals to validate their deviant behavior and activities.
6. Many children congregate on the Internet in social networks giving offenders a large potential victim pool.

F). Evidence Collection From Storage Media

1. Creation of image of compromised system
2. For integrity perform Hash value calculation.
3. Recover files and folders to a new location.
4. Examine all files especially deleted files
5. Collecting evidences from:
   a. Free spaces, slack spaces and bad sectors
   b. Application software file.
   c. Digital camera, printer and auxillary 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 evidences into text files.
7. Searching for key-term strings.
8. Scrutinize applications or indications of as file eradications, file encryption, file compressors or file hiding utilities.
9. Preparing evidence summaries, exhibits, reports, and expert findings based on evidentiary extracts and investigative analysis.

III. Digital Forensic Tools

Many Digital tools are available during a digital investigation, some are specialized toward forensics. The different phases from the digital forensic investigation present in Section 2 need different hardware and software tools providing the investigator to collect and analyze the evidence.

Data collection / Acquisition Tools: are help to collect needed evidence for the investigation.

EnCase Forensic Suite: EnCase [] from Guidance Software is a Windows-based comprehensive and complete forensic application. EnCase is recognized as a court-validated standard in computer forensics software.

Encase can have the following functionalities.

1. File signature analysis
2. Filter conditions and queries
3. View deleted files and file fragments in unallocated or slack space
4. Folder recovery
5. Log file and event log analysis
6. File type search
7. Registry viewer, external file viewer

WinHex Tool **:** WinHex is a universal hex editor, particularly helpful in computer forensics, data recovery, low-level data editing. Main Functions of WinHex Tool:[10]

1. Disk cloning and imaging,
2. Hex View of File.
3. Mass hash calculation for files (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, ...)
4. Gathering slack space, free space, inter-partition space, and generic text from drives and images
5. File and directory catalog creation for all computer media
6. Concatenating and splitting files, unifying and dividing odd and even bytes/words
7. Analyzing and comparing files
8. Particularly flexible search and replace functions
10. Easy detection of and access to NTFS alternate data streams (ADS)
11. Lightning fast powerful physical and logical search capabilities for many search terms at the same time

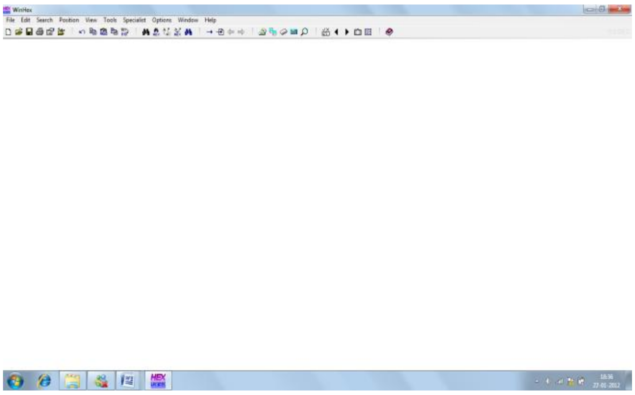


Figure 2. Shows the Screen shot of WinHex Tool[10]

Table.2. List of important forensic tools.

No	Name of the Software	Website
1	X ways Forensics 16.3 Integrated computer forensics software	www.X-ways.net.
2	WinHex 16.3 : Computer Forensics & Data Recovery software ,Hex Editor & Disk Editor	www.X-ways.net.
3	Forensic Tool Kit - FTK is the industry-standard in computer forensics software used by government agencies and law enforcement for digital investigations.	http://accessdata.com/products/computer-forensics/ftk
4	Encase forensics V 7	http://www.guidancesoftware.com.
5	S tools (Stegnography tool) : text files hiding inside images.	http://www.spychecker.com/program/stools.html.
6	Camouflage - hide your files inside a jpeg image!	http://freesoftwareproject.weebly.com/free-file-camouflage.html.
7	Slueth Kit + Autopsy Browser – Forensic Tool Set	http://www.sleuthkit.org.
8	Passware Kit: Password Cracking	http://www.lostpassword.com/kit-enterprise.htm.
9	History viewer (Show all browser as well as user activities)	http://www.historyviewer.net/index.html.
10	Child Key logger/ family Key logger – Storing key strokes	http://www.familykeylogger.com/.
11	Stegnos privacy suite -2012 provide secret safe. Deposit all your important documents, private photos and videos in Steganos Safe 2012 – out of reach for others and highly secure	http://www.steganos.com.

12	Email Tracker pro – Email tracing and Spam filtering	http://www.emailtrackerpro.com.
13	Wireshark (Network protocol analyzer)	http://www.wireshark.org/download.html.

A. *Hidden data analysis in storage media*

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]

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

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]

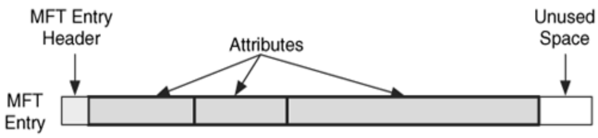


Figure 3 . MFT Structure.[8]

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

- Open file in the hex format
- Check the file signature
- Copy From starting signature upto ending signature.

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).

Open the file with corresponding application.

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.

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 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.

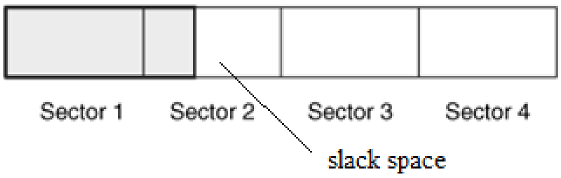


Figure 4. file slack [8]

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.[16]

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]

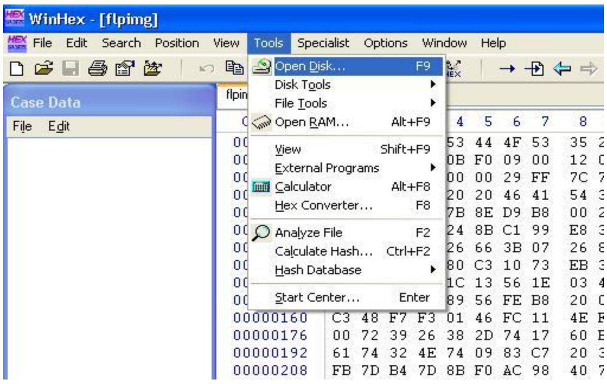
B. *Storage Media Investigation using WinHex Tool.[10]*

1. Assesses the crime Scene
2. Evidence Collection

2.1 Select a Tool eg: WinHex[10]
2.2 Create image of the compromised system disk.
2.3 open WinHex
2.4 open particular drive (Tools →open disk)
2.5 Calculate Hash value of the drive/disk
(Tools →compute hash)
Store hash value in a text file.
2.6 Recover the necessary files and deleted files from the disk image.(Specialist →Interpret as image)
2.7 Copied into a folder.
2.8 Start analysis of the content recovered files of files.
2.9 Image analysis ie hidden data inside an image can be analyse using Stegnography tools (Stools),
2.10 Check Header and footer of application file. Copy header and footer and paste into text pad.

Examples with WinHex [10]:

1)Create an image of DISK using WinHex Tool[10]



```
            4  5  6  7   8
00000160  C3 48 F7 F3 01 46 FC 11  4E F
00000176  00 72 39 26 38 2D 74 17  60 E
00000192  61 74 32 4E 74 09 83 C7  20 3
00000208  FB 7D B4 7D 8B F0 AC 98  40 7
```

Figure 5. Screen shot of creation of disk image

3. Analyse the Disk image

3.1.1 Calculate Hash value of image (Tools→compute hash)

3.1.2 Compare the Hash value of original with image. If equal start analysis else acquired data altered.

3.2 Recover the necessary files and deleted files from the disk image.(Specialist →Interpret as image)

3.3 Copied into a folder.

3.4 Start analysis of the content recovered files of files.

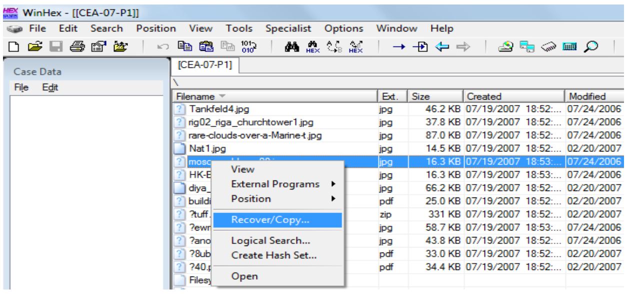
3.5 Image analysis ie hidden data inside an image can be analyse using Stegnography tools (Stools)

4. Check Header and footer of application file. Copy header and footer and paste into text pad. Sometimes evidence should be present in Header and footers.Conclude the investigation and Generate Report.

Recover Deleted file using WinHex.

1) Open Drive image
2) Make as file view mode
3) Recover the necessary files and deleted files from the disk image.(Specialist →Interpret as image)
4) Copied into a folder.
5) Start analysis of the content recovered files.

Open drive image – select file and right click



Filename	Ext.	Size	Created	Modified
Tankfeld4.jpg	jpg	46.2 KB	07/19/2007 18:52:...	07/24/2006
rig02_riga_churchtower1.jpg	jpg	37.8 KB	07/19/2007 18:52:...	07/24/2006
rare-clouds-over-a-Marine-t.jpg	jpg	87.0 KB	07/19/2007 18:52:...	07/24/2006
Nat1.jpg	jpg	14.5 KB	07/19/2007 18:52:...	02/20/2007
mosc	jpg	16.3 KB	07/19/2007 18:53:...	07/24/2006
HK-E	jpg	16.3 KB	07/19/2007 18:53:...	07/24/2006
diya_	jpg	66.2 KB	07/19/2007 18:52:...	02/20/2007
buildi	pdf	25.0 KB	07/19/2007 18:52:...	02/20/2007
?tuff	zip	331 KB	07/19/2007 18:52:...	02/20/2007
?ewr	jpg	58.7 KB	07/19/2007 18:53:...	07/24/2006
?ano	jpg	43.8 KB	07/19/2007 18:52:...	07/24/2006
?8ub	pdf	33.0 KB	07/19/2007 18:52:...	02/20/2007
?40.p	pdf	34.4 KB	07/19/2007 18:52:...	02/20/2007
Filesy				

Figure. 6. Screen shot of Recover/copy deleted file.

C. *Investigation procedure of a source code theft*

1. Assess the crime scene
2. Find which source code files are theft.
3. Calculate Hash value of the theft files and save it into text file.
4. Find out who are involves in the project.
5. Investigate their USB's and PC's – Take an image of all drives using Winhex tool..
6. Investigate their Email accounts.- take an image of Email folders using Winhex tool.
7. Analyse the drives – Open drive images in Winhex (Tools →open disk)
8. Calculate Hash value of the drive/disk (Tools →compute hash)
9. Store hash value in a text file.
10. Find out source codes are available in drives .
11. If deleted recover all deleted files using winHex (Right click on the files folder and recover).
12. Again calculate the hash value of the recovered files.
13. If the hash value of the recovered source code files are equal . Then commit the crime happened by the person who owned by the above files.
14. Sometimes source code can hide inside the image.
15. We can find out the hidden data using stenography tools or Dtsearch tools click the particular image in the winHex and check the content displaying window. If the content containing hidden text data then it will display directly.

D. investigating Email Abuse

Email is an essential type of communication in the current fast world. It is most preferred form of communication. The ease, speed and relative secrecy of email has made it a powerful tool for criminals. Following are the major email related Crimes

1. Email Spoofing.
2. Sending malicious codes through email.
3. Email bombing
4. Sending threatening emails.
5. Defamatory emails.
6. Email frauds.

Email investigation procedure.

Email investigation can be done with two methods that are Email tracking and Email tracing, Email tracking tells us to Tracking down an IP address will give a general idea of what city, state and other geographical information pertains to the original sender. You can also determine what ISP a computer user is networked with through an IP address lookup tool. www.ReadNotify.com is a online service for Email tracking. It tracks an email as to when it was read/re-opened/forwarded and much more. In cases where only an email ID is obtained as clue to track the sender of an email, services like ReadNotify.com can prove very helpful.

Email Tracing gives other information, such as how many times an email was sent to various servers and is an important method used for determining the original source of an email. By tracing an email you can determine the original sender's IP address, therefore giving you a geographical location of the email sender.

1. Assess the crime scene
2. Take a copy of compromised email folder.
3. Analyse Email folder.
   - 3.1 open Email folders – inbox, outbox, sparm
   - 3.2 open each mails and analyse Header of email.
   - 3.3 From header can identify IP address of source
4. Analyse Body message .
   - 4.1 Copy body message into a notepad (text file).It shows any hidden formatted messages.
5. Down load any attachments the particular email have

It contains any images, then check with Stegnography tools. All these analysis give the necessary evidence of the email crime.

E. A child Pornography Investigation

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.

Some time forensic evidence should be available in the network can be reconstruct and examine and conclude the result of the case.

F. Linux And Digital Forensics

Linux has number of simple utilities that make imaging and basic analysis of suspect disks and drives comparatively easy.

a) Usage of the Linux Commands

Fdisk is used for finding the structure of the disk

```
Fdisk -l /dev/hda -lists available
partitions.

 fdisk -l /dev/hda > fdisk.disk1-
redirects output to a file
```

```
fdisk –l /dev/hda
Disk /dev/hda: 255 heads, 63 sectors, 1582 cylinders
Units = cylinders of 16065 * 512 bytes
Device    Boot  Start  End  Blocks  Id   System
/dev/hda1  1     255 2  048256 b Win95 FAT32
/dev/hda2 *    256 638 3076447+ 83 Linux
/dev/hda3      639 649 88357+ 82 Linux swap
/dev/hda4     650 1582 7494322+ f Win95 Ext'd (LBA)
```

Figure 6 Output of fdisk command.

b) Creating forensic image of the suspected system.

Make an image of the practice disk. This is your standard forensic image of a suspect disk. This takes your suspected device (/dev/fd0) as the input file (if) and writes the output file (of) called forensicimage.disk1 in the current directory (/root/evidence/). The **bs** option specifies the block size. This is really not needed for most block devices (hard drives, etc.) as the Linux kernel handles the actual block size.

```
  dd if=/dev/fd0
of=forensicimage.disk1 bs=512
```

For the sake of safety and practice, change the read-write permissions of forensic image to read-only.

```
  chmod 444 forensicimage.disk1
```

c) To create a special mount point for all physical subject disk analysis

```
  mkdir /mnt/analysis
```

d) loading forensic image

```
  # mount -t vfat -o ro,noexec
/dev/fd0 /mnt/analysis
```

Linux commands	Description
dd	Creating forensic image of the suspected system
md5sum and sha1sum	For Integrety checking – compute hash value of the disk image
grep	Search strings or keywords
file	Reads a file’s header information in an attempt to ascertain its type, regardless of name or extension.
xxd	command line hexdump tool. For viewing a file in hex mode.
Ghex and khexedit	the Gnome and KDE (X Window interfaces) hex editors. Both have primitive search and byte selection capabilities.
Fdisk	Determining structure of the disk

Table3. Linux Commands, can use as Forensic Tools

e) Compute hash value of forensic Image for integrity checking.

One important step in any analysis is verifying the integrity of your data both before after the analysis is complete. You can get a hash (CRC, MD5, or SHA) of each file in a number of different ways. We will use the SHA hash. SHA is a hash signature generator that supplies a 160-bit “fingerprint” of a file or disk.

```
  sha1sum /dev/fd0 or sha1sum
/dev/fd0 > SHA.disk1
```

md5 computation

```
  md5sum /dev/fd0 or md5sum
/dev/fd0 > md5.disk1
```

compute hash value of the files in the image and stores in a file filelist.list.

```
  find . -type f -exec sha1sum {}
\; > /root/evidence/SHA.filelist
```

This command says “find, starting in the *current* directory (signified by the “**.**”), any regular file (-type f) and execute (-exec) the command sha1sum on all files found (**{}**). Redirect the output to *SHA.filelist* in the /root/evidence directory (where we are storing all of our evidence files). The “**\;**” is an escape sequence that ends the –exec command.

Sha1sum –c option

You can also use Linux to do your verification for you. To verify that nothing has been changed on the original floppy, you can use the -c option with sha1sum. If the disk was not altered, the command will return “ok”. Make sure the floppy is in the drive and type:

```
  sha1sum -c /root/evidence/SHA.disk1
```

f) making a list of all files

```
  ls -laiRtu >
/root/evidence/file.list
```

This will show all the hidden files (-a), give the list in long format to identify permission, date, etc. (-l). You can also use the –R option to list recursively through directories. use the –i option to include the inode in the list, the –u option can be used so that the output will include and sort by access time (when used with the –t option).

g) Search files for strings, key words or extensions

`grep -i jpg filelist.list` this command search for files with extension jpg .

h) viewing contents of file

```
  cat filename
```

IV. Conclusion.

The attackers have the methods to violate the security. Then comes the role of forensic analyst who should have a thorough knowledge in investigation techniques for extracting hidden evidences. Digital forensics investigators have access to a wide variety of tools, both commercial and open source, which assist in the preservation and analysis of digital evidence. Our paper contributes a major role in this area. We are explaining Tools and techniques for Digital forensic investigation. We are also explains emerging cyber crimes and steps for the investigation of these crimes.

REFERENCES

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

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

[3] Cheong Kaiwee. Analysis of Hidden Data in NTFS File system. Whitepaper.

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

[5].Timothy R. Leschke. Cyber Dumpster-Diving: $Recycle.Bin Forensics for Windows 7 and Windows Vista.

[6].Keith J. Jones Forensic Analysis of Microsoft Windows Recycle Bin Records.

[7]. Gao Qinquan,Wu shunxiang. Research of Recycle Bin Forensic Analysis Platform Based On XML Techniques.

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

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

[10] http://www.WinHex.com

Dr. B. B. Meshram is the Head of Computer Technology Dept., VJTI, Matunga, Mumbai. He is the most prominent professor in Computer Engineering and has publication of 25 international journals, 70 international conference and 39 national conference papers to his credit. He is a extravagant teaching experience surfaced with impeccable information resource about contemporary software domain. He is a well known expert for research community in Mumbai. His expertise covers subjects of recent trend like Object Oriented Software Engg, Network Security, Advanced Databases, Advanced Computer Network (TCP / IP), Data warehouse and Data mining, etc at 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. Presently under the guidance of Dr. B. B. Meshram and published her papers international journal and international conferences. She worked as counsellor in IGNOU for MCA, BCA She is Associate member of Institution of Engineers(India) . Her research interests are Web security and Digital Forensic. She is doing Certification of Digital Evidence Analyst from Asian school of Cyber Law India.