Cyber Forensic Investigation

-A Beginer's Guide

FORnSEC SOLUTIONS
Sachin Sathe

CYBER FORENSIC INVESTIGATION

-A BEGINERR'S GUIDE

Cyber Forensic Investigation

-A Beginer's Guide

Author

Sachin Sathe

Editor

Aransha Badge

Published By

Copyright

Year of Printing

2020

AUTHORS' PROFILE

MR. SACHIN SATHE (PDGC, CHFI , B.E. , Cyber Forensic Expert)

I have been occupying a responsible official position i.e. Cyber Forensic Expert in FORnSEC Solutions. It is both an honor and privilege of mine to serve cyber forensic services to the society

I have handled various cyber forensic Investigation cases for various Law Enforcement Agencies in Nagpur and out of Nagpur.

I have done post graduation in cyber forensic, nagpur and is certified cyber forensic investigator from EC-Council USA. I have more than 8 Years of experience in cyber forensic investigation field. With that I had also Investigated more than 3000 LEA cases and 1000 private cases. In some matters I had also attended the court personally for further process of LEA.

From past few years I have been providing Cyber Forensic Consultancy for Nagpur Gramin Cyber Cell, Nagpur City Cyber Cell & Other Local Police Station in Nagpur as well as for private colleges and institutions. I had also provided training and guest lectures to various police department and colleges.

CONTENTS

Chapter 1

Introduction and Overview

The purpose of this book is to create awareness about cyber crime and assist law enforcement agencies with proper techniques and primary level of cyber forensic investigation.

As the technology has advanced at such a rapid rate that things have now become electronic, technical and computer-based. With the increasing rate of computer crimes; cyber criminals such as hackers, fraudsters, and others cyber criminals have become more powerful than before and have begun occupying middle spaces and bulletins of the newspaper and other forms of media. So, with the frequency and sophistication of cyber attacks; it has now become very essential to know about computer forensics and the different ways to deal with it.

This book is mainly about First Responder Basket which contains a variety of digital forensic tools and hardware which assist in conducting productive computer investigation.The book will help you to deal with digital evidence at the crime scene by applying proper protocol and procedures while acquitting digital data with the support of basic computer forensic tools. This book also offer information about filling up 'punchnama' at the crime scene while seizing the digital evidence and creating report generation with the checksum of the digital evidence which can be legally hold up in a court. It is essential to handle digital evidence safely and store it in a secure place to avoid data loss and destruction of vital information. It will also guide you through the most common situations and problems encountered during the examination of digital evidence.

At the end of the book, case studies examples have been presented for practical approaches and experiences. The tools and methods offered in the booklet will assist you in carrying out cyber crime investigations in the most effective approach.

Chapter 2

Cyber Crime

Cyber crime are the crimes that involve digital evidences such as computer, mobile and internet. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been used as the target of the crime.

In simple words, cyber crime is a criminal activity committed using computers, mobile and the internet which is against the law.

2.1 : Classification of Cyber Crime

Cyber crimes can be classified broadly into the following three categories -

Cyber crimes against individual-

Cyber crimes against the person include various crimes like Cyber Harassment, Denial of Service Attacks, Cyber Stalking, Child Pornography, Email crimes, etc. These crimes are directed against an individual for various purposes ranging from greed to personal revenge. This type of cyber crime is a big threat to the youngsters and, if not controlled will leave an undesirable imprint on them.

Cyber crimes against property -

This kind of cyber crime is directed against all forms of property and includes computer theft also. This is a growing problem and has increased manifold with the increase in access to technology. 'Property' in this context not only refers to the computer or its components but also refers to software, copyrights, trademarks and computer source code. These kinds of crimes are generally targeted against the organization for various motives.

Cyber crimes against government and society -

The growth of the internet has enabled to attack government and society. Sensitive websites of the government and the military are hacked. These organizations keep changing their tactics and method to attack government websites and banks.

2.2 : Types of Cyber Crime

There are many types of cyber crimes and the most common ones are explained below:

Financial Crime - Financial crimes, as the name suggests, are committed for financial gain. Money is the common motive behind all the crimes. Cyber crimes are mainly committed for financial gain rather than for fun or revenge or challenge. Many new techniques are formulated every minute for cheating people. Financial crimes include, but are not limited to cheating, credit card frauds, hacking into bank servers and financial scams.

Information Theft - For any organization, information is the main asset of the company. Theft information can range from revenge to industrial spying. Such thefts are growing phenomenally over the past few years. In most cases, an insider is responsible for the information theft than intruders. As more and more security measures are developed to protect the information, newer areas of vulnerability are opened up for information theft.

Cyber Extortion- Cyber extortion is a crime involving an attack or threat of attack against an enterprise, generally using Denial of Service attacks (DoS) or other kinds of attacks coupled with a demand for money to stop the attack. DoS attack occurs when a computer is flooded with more requests that it can handle. This attack denies service to its authorized users. At times, a cyber extortion may involve a huge money without guaranteeing to stop the attack. These attacks are controlled from remote places or countries using fake identities so that it could get difficult to find the culprit.

Harassment- The virtual harassment has risen up heavily. Thousands of social networking harassment cases are registered everyday. Harassment is generally done to women but can also be aimed at specific group involving race or religion and so on. Harassment is done through email or by facebook posts or transmission of obscene and offensive content on social networking applications. These defaming and annoying messages are generally sent to the victims through a false email account.

Cyber Stalking - Cyber stalking means pursuing a person's movements on the internet and posting email messages, chat rooms, social media and any other online medium that bombard him/her on the sites she frequently visits. By collecting sufficient personal details about the person, they plan for the harassment.

Intellectual Property Theft - It means the ownership of rights related to software, copyrights, trademarks and other such intangible assets. When these rights of the owner are deprived of completely or partially, it is said to be an Intellectual Property Rights (IPR). They make software available for free download or in exchange for uploaded programs.

Computer Vandalism - It leads to any physical computer harm or its parts are called Computer Vandalism. It can include theft of a computer, its parts or peripherals or any type of damage or any type of damage caused to them.

2.3 : Techniques of Cyber Crimes

Computer Viruses and Worms - Virus is a malicious program that can cause damage to the computer. It is a self-replicating program that produces its own code by attaching copies of itself into other executable codes. The virus can corrupt or delete the data.

The worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs. It causes the system to slow down. A worm spreads itself into the network, automatically.

Phishing / Spoofing - This attack is the fast growing online scam. In this type of attack, a cyber criminal creates a fake website page which looks real and is usually sent via email and marks as a trust worthy organization. This technique is called phishing. The cyber criminal may also send you a lottery email and ask for your details like credit card details, bank account details, and other such information.

Denial of Service Attack - This attack is a technique that makes the website or a service unavailable. Typically, this is achieved by using multiple computers by repeatedly making requests that make the site or a network down. This type of attack might stop your website from functioning temporarily or permanently and may result in data and financial loss.

Social Engineering - It is a method where cyber criminals make use of emails or phone calls. They try to gain your confidence and assert as a real identity and get the information they need. This information can be about your bank account details, money, your company or anything that can be useful to the cyber criminals.

Identity Theft- Identity theft is one of the most common types of cybercrime. The term Identity Theft is used, when a person intends to be some other person to do a fraud for financial gains. The most usual source to steal identity information of others is from data breaches of private, government or federal websites that contain financial details.

Chapter 3

Digital Evidence

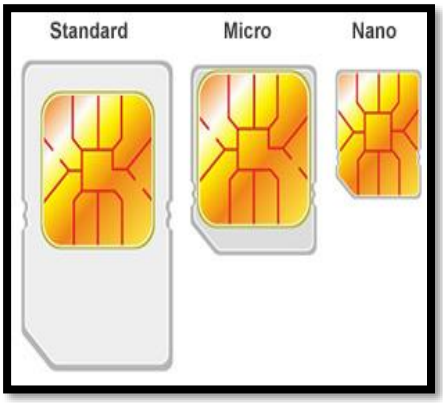
Digital evidence or **electronic evidence** is any evidence is any valuable information which is stored or transmitted in digital form to the party which may be used in the court for the case trial.

In other words, digital evidence is defined as information and data value to an investigation that is stored, received or transmitted by an electronic device.

In today's era, digital gadgets are used by nearly everybody and all over the place. Digital evidence comes into a play when a cyber crime is done by using digital gadgetssuch as computers, mobile phones, laptops, tablets and other electronics devices. These are used as a medium for a cyber attack. Every time, when a cyber crime is committed traces of digital prints are left behind which helps in locating cyber criminals. These prints can be obtained after proper seizing and examination of digital devices found at the crime scene followed by appropriate acquiring techniques. The digital evidence can be acquired from such as e-mails, social networking sites, ATM logs and much more.

Here, we need the first responder to conduct an investigation at the crime scene. His responsibility is to identify, collect and transport the digital evidence without having any adverse effect on safeguarding of evidence such as to prevent them from damaging like extreme temperatures, moisture, and static electricity.

SanDisk
SDHC Card
LOCK
16GB


Standard
Micro
Nano

SanDisk
16GB
micro SD HC

WD
4 TB
SATA / 64 MB Cache
WD40EZRX
WD Green
Desktop Hard Drive

There are many sources of digital evidence and the most common ones are found on-

1.Internet.

2.Computers.

3.Mobile Phones.

For acquiring of these evidence different procedures, techniques, and forensic tools are used in practice.

1. Internet :

The most vital and essential medium needed to commit a crime is 'Internet'. The Internet has each data which is required. With the help of the internet, global access to the information the crime rate has risen very high. Cyber criminals mostly target government websites or portals, banks, networks and other systems through the internet to steal money, identity, bank account details, personal details, and other valuable data.Whenever a crime is committed over the internet,most of the time it leaves a clue of evidence which helps in theinvestigation as well as it makes easier to locate a criminal.

For example - An email fraud can be cracked down by backtracking IP address. It includes the details about the location and the owner's information to whom IP address was allocated and thus, the culprit can be found out.

2. Computers :

A computer is an another necessary major source of medium to commit a crime. As the definition says, internet and a computer are two important means. At the same time, when a crime is committed from a computer,traces of digital evidence are usually settled down on a computer hard drive. For carrying out the investigation at the crime scene, seizing of the hard drive is a very important source of collecting digital evidence and also other peripheral devices including pendrive, external hard disks, CD-ROM discs, and other digital media.This evidence needed to be analyzed with the help of digital forensic tools with different procedures and techniques to carry out a successful investigation.

For example - Recently, there was a case that a convict sent a threatning message to a minister. To track down the message from the computer, we analyzed the hard-disk with a forensic tool and we successfully retrieved the message and the culprit was held guilty in the court of law.

3. Mobile phones :

Nowadays, mobile phones now are taking the place of computers for efficient working. A cell phone contains all the essential information such as location, personal documents, contacts, messages, call history, digital photographs, credit card details and many. Commonly, cyber criminals use the method of injecting viruses or malware through the network for accessing these details. Evidence in a mobile phone can be collected using mobile forensic tools.

For example - Information posted on social networking such as Facebook may contain details about device or location of the place from where it was being posted. By conducting a proper investigation the digitalevidence can yield valuable information and be proved lawfully in a court.

3.1 : Points to be considered while 'Punchnama'

1. Opening and closing time.

First, mention the starting time then analyze the crime scene and then generate the hash value. Then, after generating the hash checksum close the punchnama.

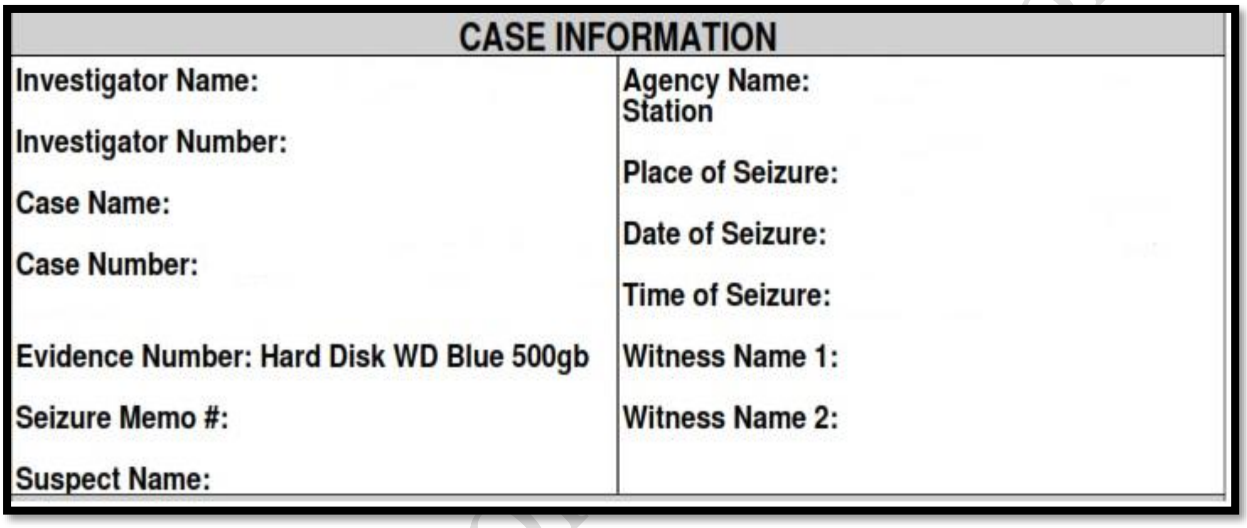
Note - Before closing the punchnama, the hash value of the digital device must be generated. In case, if the hash value is generated after closing the punchnama, the digital evidence would not have a validity.

2.While punchnama , maintain a chain of custody such as collect all the preliminary digital devices, accessories, writing of complete details about all hardware devices,information regarding seized devices and complete detailed information.

3. After punchnama, do not open or access the original evidence without using a write blocker tool.

4. Presence of 2 witness are compulsary at the time of punchnama.

5. Example–Case Infromation Need to Put into Punchnama



CASE INFORMATION	
Investigator Name:	Agency Name: Station
Investigator Number:	Place of Seizure:
Case Name:	Date of Seizure:
Case Number:	Time of Seizure:
Evidence Number: Hard Disk WD Blue 500gb	Witness Name 1:
Seizure Memo #:	Witness Name 2:
Suspect Name:	

Chapter 4

Digital Forensics

Digital forensics (sometimes known as **digital forensic science**) is a branch of forensic science that includes the recovery and investigation of the information found in digital devices often in relation to computer crime.

In other words, digital forensics help with acquisition, analysis, recovery and report of electronics devices such as computers, mobile phones, PDA's and other memory storage devices.

The procedure of acquiring the digital evidence must be done in such a way that it must preserve its evidence value and to assure its admissibility in legalproceedings.

The digital forensic process commonly consists of 3 stages -

1. Acquisition / Imaging - It involves hashing and capturing of the electronic devices and create an exact duplicate of the media, often using write blocking device to prevent modification or destroying evidence of the original.

2.Analysis - An analysis is mostly performed on a captured image rather than on original device because the original device needed to be preserved so that it can uphold in the court. This analysis is conducted with the help of digital forensics tool by proper methodologies. In every analysis, the procedures varies but common methodologies such as searching for keywords within files, deleted or recovery data.

3. Reporting - After analysis investigation the findings is presented in a clear, concise and structured report. Both acquired and the original image are hashed and the values compared to verify the copy is accurate using hash algorithms such as SHA-1 or MD5. The need for calculating the hash value in a forensic investigation is to prove the accuracy of digital data and no other modification are being done.

4.1 : Types of Digital Forensics

Digital forensics includes several sub-branches related to the investigation of various types of devices and media.

1. Computer Forensics :

In computer forensics, the goal is to analyze the storage device such as hard disk or other removable devices. It deals with the extraction of images, videos, documents and other evidence from thehard disk.

2. Mobile Forensics :

Mobile forensics is related to recovering of presented or deleted data from mobile phones or tablets. It also deals with the analysis of Simcard data and retrieval of contacts, IMSI, messages and other several essential information. Furthermore, investigation of WhatsApp and other social networking applications is done.

3. Network Forensics :

Network forensics is related to the monitoring and analysis of computer network traffic for the purpose of information gathering, evidence collection or intrusion detection.

Chapter 5

Primary Investigation Steps -

1. Identify the computer crime.

- After reaching at the crime scene, identity which type of cybercrime has taken place and investigate, accordingly.

2. Collect preliminary evidence.

- Collect primary evidence before reaching at the crime scene.

3. Obtain court/higher authority permission for seizure (if necessary).

- For private raid, you must carry permission letter.

4. Perform first responder tool.

- If the computer is in 'on mode' then use first responder tool to gather internet accessed information, cookies, etc and then properly shut down the computer and remove the harddisk. In case of 'off mode', remove the harddisk of the computer.

5. Seize evidence at the crime.

- Remove the harddisk from the computer properly and then generate the hash value of the evidence and then pack the evidence in anti-static bag. In case of mobile, seize the mobile in faraday bag.

6. Create two-bit stream copies of the evidence.

- One for the user from who we have seized the harddisk and one for the analysis.

7. Generate SHA1 checksum on the image.

- Generate hash value for integrity.

8.Maintain chain of custody.

- Follow the proper procedure for investigating a crime and note down the case details systematically.

9. Transport evidence to the forensic laboratory.

- For analysis purpose transport the evidence.

10. Store the original evidence in a secure location.

- Store the evidence in a free moisture and metallic place so that the integrity should not get affect.

11. Analyze the image copy for evidence.

- By using write blocker tool analyze/recover the duplicate copy for acquiring digital proof.

12. Prepare a forensic report.

- Generate the forensic report of the digital evidence and attach it with the chargesheet.

13. If required, attend the court and testify as an expert.

Chapter 6

First Responder Toolkit

This basket is specifically designed for law enforcement agency (LEA) to assist them with the primary investigation of cyber crime on the crime scene.

The First Responder includes -

6.1 :Forensic Imager Software - Forensic Replicator

6.2 :Hash Calculator - Hash Calculator and Report Generation

6.3 : USB Protect - Write Block Tool

6.4 : SIM Card Reader

6.4.1 : SIM Card Data Analysis Software - SIM Card Seizure

6.5 : Signal Blocking - Faraday Bag

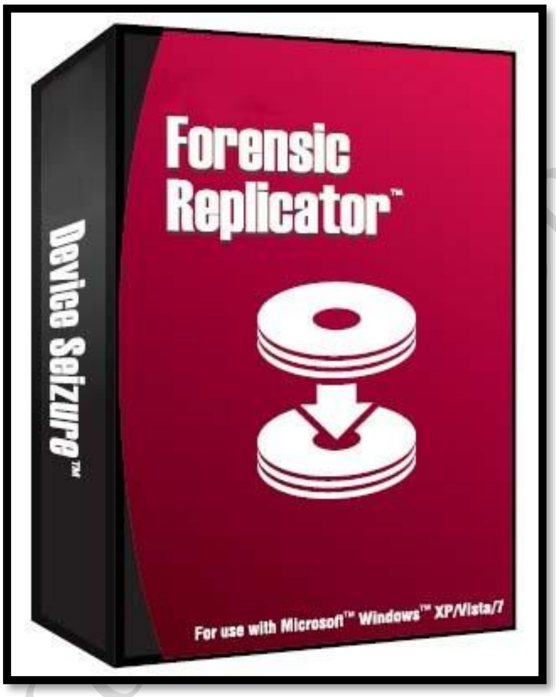
6.6 : Mobile Data Recovery Software - Dr.Fone Wondershare

6.7 : Evidence Collection Bag - Anti-Static Bag

6.8 : Memory Card Reader

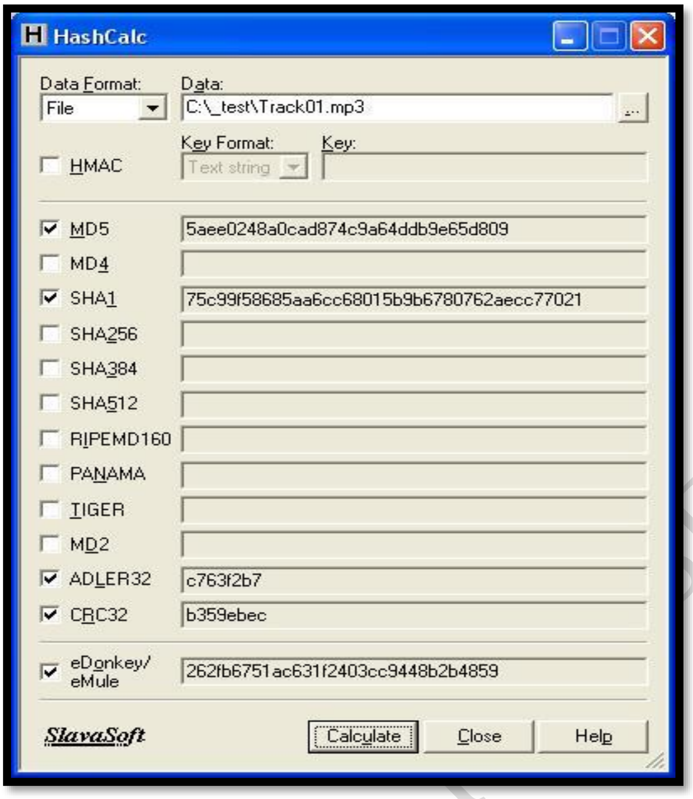
6.1 : Forensic Imager Software - Forensic Replicator

Forensic Replicator is a tool which is used for bit-stream creation. Forensic Replicator is a Windows based tool that creates bit-by-bit raw DD images of hard drives and related media. You can also create images in PFR format to encrypt the image, compress it, or break it up into smaller pieces.. You can create bit-by-bit forensic images, verify your image integrity with hash calculation, document use of write blockers in your report, view an image's contents, and much more. Forensic Replicator goes to great lengths to preserve your evidence. Built in software-based write protection helps ensure you won't write to your evidence. Hash verification and detailed reporting also help maintain the integrity of your data.

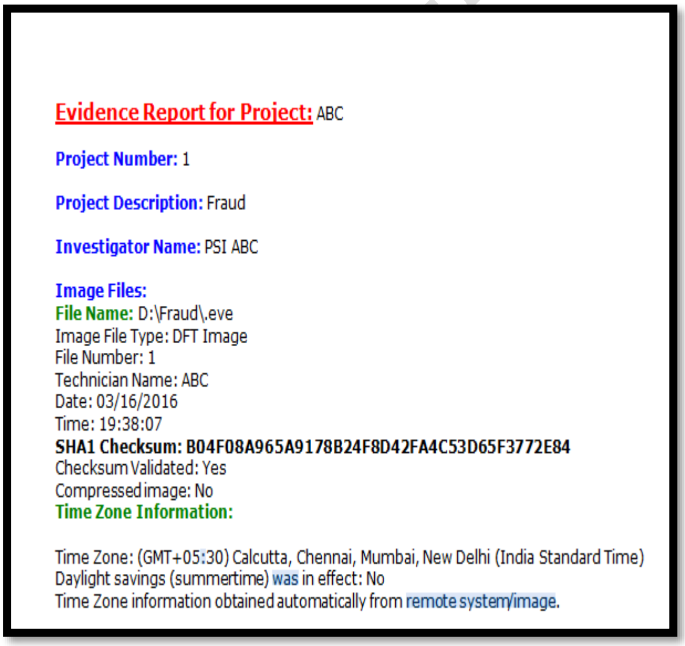


6.2 : Hash Calculator - Hash Calculator and Report Generation

It is the last process of the primary investigation. Hash is calculated to prove that the evidence that is seized from the crime scene using forensic tools is authentic and no modification or changes have been done. It calculates a checksum on the evidence and creates a value with a report.



Data Format: File
Data: C:_test\Track01.mp3
☐ HMAC Key Format: Text string Key:
☑ MD5 5aee0248a0cad874c9a64ddb9e65d809
☐ MD4
☑ SHA1 75c99f58685aa6cc68015b9b6780762aecc77021
☐ SHA256
☐ SHA384
☐ SHA512
☐ RIPEMD160
☐ PANAMA
☐ TIGER
☐ MD2
☑ ADLER32 c763f2b7
☑ CRC32 b359ebec
☑ eDonkey/ eMule 262fb6751ac631f2403cc9448b2b4859



Evidence Report for Project: ABC

Project Number: 1

Project Description: Fraud

Investigator Name: PSI ABC

Image Files:
File Name: D:\Fraud\.eve
Image File Type: DFT Image
File Number: 1
Technician Name: ABC
Date: 03/16/2016
Time: 19:38:07
SHA1 Checksum: B04F08A965A9178B24F8D42FA4C53D65F3772E84
Checksum Validated: Yes
Compressed image: No
Time Zone Information:

Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained automatically from remote system/image.

6.3 : USB Protect - Write Block Tool

Write protection tool is available in a hardware or software form. Write protection is a technique used in computer forensic in order to maintain the integrity of data storage devices. By preventing all write operations to the device, e.g. a hard_drive, it can be ensured that the device remains unaltered by data recovery methods.

6.4 : SIM Card Reader

For analysis of a SIM card, a SIM card reader is required.

6.4.1 : SIM Card Data Analysis Software - SIM Card Seizure

This forensic tool is used to analyze a SIM Card and acquire the data.Paraben SIM Card Seizure is a comprehensive forensics tool that lets you have access to the data contained on SIM cards without affecting its integrity. It is designed to retrieve data such as phone numbers, addresses, dates, times, etc and provide ways of searching and adding bookmarks to the data. SIM Card Seizure is a very useful tool for acquiring and examining this information, and will be extremely valuable in your investigations Recover deleted SMS/text messages and perform acomprehensive analysis of SIM card data. SIM Card Seizure takes the SIM Card acquisition and analysis components from Paraben's Device Seizure and puts it into a specialized SIM Card forensic acquisition and analysis tool. SIM Card Seizure includes the software as well as a Forensic SIM Card Reader.. This tool is for the investigator who only wants to acquire SIM Cards and does not want to perform forensic exams of all cell phone data.

6.5 : Signal Blocking - Faraday Bag

What is faraday bag ?

A faraday bag is also known as (Radio Frequency) **shielding bag** is used to collect devices such as cell phones in order to prevent outside signals from interfering with the contents of the device.

Need -

Cell phones are devices that connect to telecommunication networks through wireless signals. Some cell phones can also connect to Bluetooth devices or wireless networks. If the security features are not enabled on the cell phone, then it may be possible to connect to the phone and alter, delete, or add digital evidence to the phone. It prevents tracking of a cell phone. It is very important that the digital evidence is preserved from the time of seizure until it is presented as evidence in court. If evidence is suspected of being tampered with, it could be ruled as inadmissible in court. Therefore, it is important to preserve digital evidence by using a Faraday bag and noting its usage on the chain of evidence from.

6.6 : Mobile Data Recovery Software - Dr. Fone Wondershare

Wondershare Dr.Fone for Android is a powerful toolkit for Android users to recover deleted data from Android phones and tablets including data lost from internal memory cards and external memory cards, rescue data from broken Android devices, and remove Android lock screen. It is able to recover text messages, photos, contacts, call history, videos, WhatsApp messages, audio files, and more whether you accidently deleted or lost due to OS crash or ROM flashing. The Android file recovery - Wondershare Dr.Fone for Android, performs very well to recover deleted files on Android devices.

Besides recovering text messages, photos, contacts, WhatsApp messages, videos, call log, and audio files, Wondershare Dr.Fone - Android Data Recovery is able to help you recover deleted documents, like Microsoft Word documents, Excel worksheets, PowerPoint presentation files, PDF documents and more.

Wondershare
Dr.Fone™
Version: 1.0.2
Data Recovery for iPhone and iPad series
Copyright © 2012 Wondershare. All Rights Reserved.
wondershare™

6.7 : Evidence Collection Bag - Anti-Static Bag

The anti-static bag is used for storing electronic storage devices and components which are prone to damage caused by electrostatic discharge.

These bags are usually plastic **polyethylene terephthalate** (PET) and have a distinctive color. . Multiple layers of protection are often used to protect from both mechanical damage and electrostatic damage. It is important that the bags should only be opened at static-free workstations.

6.8 : Memory Card Reader

A **memory card reader** is a device for accessing the data on a memory card such as a CompactFlash (CF), Secure Digital(SD) or MultiMediaCard (MMC). Most card readers also offer write capability, and together with the card, this can function as a pen drive.

Chapter 7

IT ACT : 2008

The Information Technology Act, 2008 has come into force on 27th October 2009.

Important Sections-

Section 43 - Damaging computers systems, computers, etc.

Penalty - Compensation not exceeding one crore rupees to the person so affected.

Section 43 A -Compensation for failure to protect data.

Penalty - Compensation not exceeding five crore rupees to the person so affected.

Section 65 - Tampering with computer source documents.

Penalty - Imprisonment up to three years, or with fine which may extend up to two lakhs rupees, or with both.

Section 66 - Computer-relatedoffenses.

Penalty - Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Section 66 A - Punishment for sending offensive messages through communication service, etc.

Penalty - Imprisonment for a term which may extend to three years and with afine.

Section 66 B - Punishment for dishonestly receiving stolen computer resource or communication device.

Penalty- Imprisonment for a term which may to three years or with fine which may extend to rupees one lakh or with both.

Section 66 C - Punishment for identity theft.

Penalty- Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66 D - Punishment for cheating by personating by using computer resource.

Penalty- Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66 E - Punishment for violation of privacy.

Penalty- Imprisonment which may extend to three years or with afine not exceeding two lakh rupees, or with both.

Section 66 F - Punishment for cyber terrorism.

Penalty- Imprisonment which may extend to imprisonment for life.

Section 67 - Punishment for publishing or transmitting obscene material in electronic form.

Penalty- Imprisonment for a term which may extend to three years and with fine which may extend to five lakh rupees & in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67 A - Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

Penalty- Imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67 B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc.

Penalty - Imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67C - Preservation and retention of information by intermediaries.

Penalty - Imprisonment for a term which may extend to three years and shall also be liable to fine.

Section 70 - Unauthorized access to theprotected system.

Penalty - Imprisonment for a term which may extend to ten years and shall also be liable to fine.

Section 72 - Breach of Confidentiality and Privacy.

Penalty - Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72 A - Disclosure of information in breach of contract.

Penalty- Imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Chapter 8

Case Studies

Case 1 - Facebook

Problem - As today's youngsters are very familiar with using technology and are on almost every social networking site; a college youngster sent vulgar images and illicit messages to a school principal in her personal chats.

Solution - The principal registered a complaint against the person at her nearest police station and discussed her problem with the police officer. The policeman asked the account details of the woman and had a look on the messages sent by the youngster. To verify the case from a cyber crime expert, the policeman called me at the police station. The police officer discussed the woman's case with me and I had a glance at the images and also on messages. To investigate the matter, I seized the mobile phone of the culprit and did forensic analysis of the electronic gadget. Within no time, I found those images and messages sent by him to the mobile phone. I also took several computer screenshots of the principal's facebook account containing those messages as an evidence and generated the SHA-1 hash value of the individual image. Along with that, I provided 65(B) admissibility of electronics record evidence act report, so that the case can hold up in the court of law and the culprit must admit his wrong doings. The case was registered under the act Section 67 A.

Case 2 - Email and Facebook

Problem - In a recent case, a youngster was sending threatening and harassment emails to a girl. He was pressurizing her to be with him and also threatened her about her family.He sent misleading frauds emails about the girl in his friend's circle. Not only with this he had also sent defaming messages on Facebook to her families and other relatives and also used to keep a track of her movements.

Solution - The girl registered a complaint at our office and narrated her incident. After listening to her, I requested her email account details to had a look on those emails. To trace the perpetrator and its location, I investigated the IP address and also the email header in search of if I could get any clue.In no time, I found that the user used a private IP address for the cyber crime and the Google masks the private IP address. Then, to get the information details of the source and to find out other information, I went through the Law Enforcement Agencies and requested for details to Google Headquarters, USA.The case was registered under the act Section 67 A.

Case 3 - Murder

Problem - On 15th march 2016, Nagpur, two people murdered an individual with a knife. The incident was booked at night.

Solution - The incident was immediately registered and I was called up to the crime scene by the police officers. After reaching the crime spot, I analyzed the place and came out with the solution to collect CCTV footage from the nearby places. The incident was captured on their CCTV surveillance and the murder footage was present. I collected the videos from three different places to get three different angles to identify the suspect. Those videos were collected in different pen drives and to preserve the integrity of the pen drives, we calculated the hash value of CCTV footage and generated the SHA-1 report under the section 65-B. The case was registered under the section 134,177.

Case 4 - Video Confession

Problem - In a mysterious murder case, a person murdered his friend, both were drunk what's more, the individual killed his companion by venturing stone at his face over some civil argument. To identify the suspect there was not any proof or evidence to hold the suspect in the court of law. There was no CCTV cameras or any eye witness.

Solution - There was no evidence nor any eye witness of the murder and was getting difficult to investigate the case. In the meantime, the person who killed his companion came forward confessing the crime. A person's statement is not held up legal unless there is any evidence against them. Then I took the person's video confession of murder crime from the webcam at the police station. I stored the video in a memory card and generated the SHA-1 hash value of the memory card to preserve the original evidence from tampering. The evidence held true in the court of law. The case was registered under the section 302, 34.

Reference

1) https://www.google.com/search?biw=1366&bih=662&tbm=isch&sa=1&ei=_lwfW-T8O5C2rQHNx43gAw&q=sandisk+16gb&oq=sandisk+1&gs_l=img.1.1.0l10.360300.362011.0.363511.2.2.0.0.0.0.170.332.0j2.2.0....0...1c.1.64.img..0.2.330...0i67k1.0.aKxL3KCu5uk#imgrc=ubfhBT2dvNzY8M:
2) https://www.google.com/search?biw=1366&bih=662&tbm=isch&sa=1&ei=iF4fW6SuCdKy9QOSiaWYAg&q=forensic+replicator&oq=Forensic+Repl&gs_l=img.3.0.0i24k1.87285.91282.0.93255.14.14.0.0.0.0.279.2094.0j6j4.10.0....0...1c.1.64.img..4.10.2091.0..0j35i39k1.0.GpasKkQrmWY#imgrc=_
3) https://www.google.com/search?biw=1366&bih=662&tbm=isch&sa=1&ei=7F4fW--7OM-w9QOQwZmICQ&q=hash+calculator&oq=hash+calculator&gs_l=img.3...237049.241877.0.242160.16.11.0.0.0.0.0.0..0.0....0...1c.1.64.img..16.0.0.0...0.IghVSlbTh2s#imgrc=BJlVLyAJBzF3jM:
4) https://www.google.com/search?biw=1366&bih=613&tbm=isch&sa=1&ei=5l8fW-TjB5j_9QONgLOwDg&q=sim+card+seizure&oq=sim+card+seizure&gs_l=img.3..0i30k1j0i24k1l3.1463594.1471534.0.1472803.17.11.0.6.6.0.264.2215.2-10.10.0....0...1c.1.64.img..1.16.2259.0..0j0i67k1j0i10k1j0i5i30k1.0.tSSVO98TlTU#imgrc=3qMI52i37LFTQM:
5) https://www.google.com/search?biw=1366&bih=613&tbm=isch&sa=1&ei=pWcfW877E4HO0gTH9a2wDg&q=dr.phone+wondershare&oq=Dr.phone+won&gs_l=img.3.0.0i24k1.8331.15753.0.18564.13.13.0.0.0.0.522.2058.2-5j0j1j1.7.0....0...1c.1.64.img..6.7.2056.0..0j35i39k1j0i67k1j0i30k1.0.bdPTr_H2rRs
6) https://www.google.com/search?biw=1366&bih=613&tbm=isch&sa=1&ei=umcfW_TUJcLJ0gTK5YawCw&q=evidence+collection+bag+and+faraday+bag&oq=evidence+collection+bag+and+faraday+bag&gs_l=img.3...29527.58230.0.58562.53.43.4.4.4.0.424.5270.0j2j18j1j1.22.0....0...1c.1.64.img..23.23.3465.0..0j35i39k1j0i67k1j0i10i24k1j0i30k1.0.l9r7TKtUMDs

7) https://www.google.com/search?q=sim+card+reader&source=lnms&tbm=isch&sa=X&ved=0ahUKEwin95KzjM7bAhXFp48KHcGsC6wQ_AUICigB&biw=1366&bih=613