



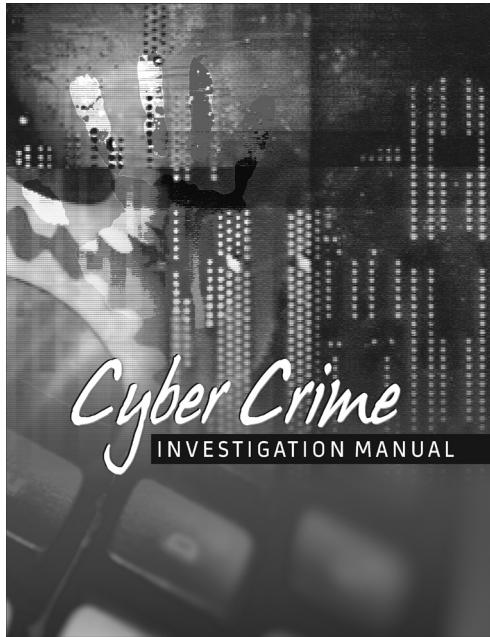
A **NASSCOM**® Initiative

Cyber Crime

INVESTIGATION MANUAL

KNOWLEDGE PARTNER

Deloitte.



Cyber Crime Investigation Manual

DATA SECURITY COUNCIL OF INDIA

Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
Phone: +91-11-26155070, Fax: +91-11-26155072
Email: info@dsci.in, cyberlab@dsci.in

w w w . d s c i . i n

Data Security Council of India (DSCI) is a section 25, not-for-profit company, setup by NASSCOM as an independent Self Regulatory Organization (SRO) to promote data protection, develop security and privacy codes & standards and encourage the IT/BPO industry to implement the same.

For more information about DSCI or this manual, contact:

DATA SECURITY COUNCIL OF INDIA

Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India

Phone: +91-11-26155070, Fax: +91-11-26155072

Email: info@dsci.in

Designed and Printed by
Swati Communications
+91 11 41659877, +91 9213132174

Published in March 2011

Copyright © 2011 DSCI. All rights reserved.

Distribution: Restricted to Enforcement and Investigative Agencies

This manual contains information that is Intellectual Property of DSCI. DSCI expressly disclaims to the maximum limit permissible by law, all warranties, express or implied, including, but not limiting to implied warranties of merchantability, fitness for a particular purpose and non-infringement. DSCI disclaims responsibility for any loss, injury, liability or damage of any kind resulting from and arising out of use of this material/information or part thereof. Views expressed herein are views of DSCI and/or its respective authors and should not be construed as legal advice or legal opinion. Further, the general availability of information or part thereof does not intend to constitute legal advice or to create a Lawyer/ Attorney-Client relationship, in any manner whatsoever.

Contributors

DSCI

Pratap Reddy
COM)
Vinayak Godse
K.Venkatesh Murthy
Vikram Asnani
Mahesh.R.
Karthik. R
Abhishek Kumar
Chaitanya J Belsare
Dinesh Dalvi
Sandip P Gadiya

Director, Cyber Security (NASS-
Director, Data Protection
Program Manager, Cyber labs
Sr. Consultant, Security Practices
Bangalore Cyber Lab
Chennai Cyber Lab
Haryana Cyber Lab
Mumbai Cyber Lab
Mumbai Cyber Lab
Pune Cyber Lab

Deloitte

Vipin Bahl
Avijit Gupta
Anil Kona
Harsha Vardhan Godugula
Ranjith Singh Bellary
Smitha Allola
Bhanu Prakash Kondapally
Siva Prasad Palepu
Varun Pitale
Shabarinath Sharma Kandala
Sumakanth Yepuri
Aradhana Pandey

Director
Director
Sr. Manager
Manager
Sr. Associate
Sr. Associate

Acknowledgements

Central Bureau of Investigation

Sujeet Pandey IPS
Sanjay Gautam
Akansha Gupta

DIG, CBI Academy, Ghaziabad
Inspector, CBI Academy
Inspector, CBI Academy

Central Forensics Sciences laboratory

Krishna Sastry Pendyala

AGEQD, CFSL, Hyderabad

State Police

K.S.R.Charan Reddy IPS
Malini Krishnamoorthy IPS
B.Dayananda IPS
M.D.Sharath
Raghavendra K Hegde
M. Sudhakar
Ramamohan Ukkalam
Bijumon E.S
Sanjay Jadhav
Sanjay Tungar

Deputy Inspector General of Police, CID, Bangalore
Deputy Inspector General of Police, CID, Bangalore
Deputy Inspector General of Police, State Intelligence, Karnataka
Detective Inspector, Cyber Crime PS, CID, Bangalore
Detective Inspector, Cyber Crime PS, CID, Bangalore
Addl. DCP, Chennai Cyber Crime Cell
Addl. SP, Cyber Crimes, CID, Andhra Pradesh
DSP, Kerala Police
ACP, Cyber Crimes, Mumbai
API, Cyber Crime Cell, Pune Police

Foreword

Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. The size of cyberspace continues to grow with increased Internet penetration, and activities that are carried through it including, the exchange of goods or services, financial transactions through banks, credit card payments, email communications, social networking, exchange of pictures, videos or music. The same networks are, however, used by criminals, by exploiting vulnerabilities in various devices, to commit cyber crimes that impact the physical world too. Cyber criminals carry out identity theft and financial fraud; steal corporate information, including intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and others to carry out physical terrorist activities in the world. Cyber attacks are also used to disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in physical space.

India is witnessing sharp rise in cyber crimes. Recently released NCRB data show that in the year 2009, 420 cyber crimes were registered under the IT Act, and 276 under various sections of IPC. Under the former, 288 persons were arrested for crimes that included hacking and obscene transmission, among others. Malware, spam, and phishing incidents are also rising. According to a survey report, India has overtaken the United States in spamming, which is a major source of malware distribution and creation of botnets. These, in turn, are used to launch many types of cyber crimes. Globally also, cyber crimes are rapidly increasing, since the financial payoffs are disproportionately high in comparison to efforts of criminals. United States estimates that it lost over USD one trillion in intellectual property in cyber attacks, while over 350 million records were compromised in security breaches over the last 3 years.

Handling cyber crimes requires an appropriate legal regime, technical infrastructure to analyze cyber forensics data, and a trained police workforce and prosecutors having knowledge of cyber forensics tools for capturing evidence from the scene of crime and related network points, which can be anywhere in the country or in different parts of the world. Judiciary also has to be exposed to these concepts so that it can appreciate cyberforensic evidence to make informed judgments. Capacity building of law-enforcement agencies is, therefore, a key element in bringing cyber criminals to justice.

NASSCOM started an initiative of establishing Cyberlabs in the year 2004 to train police officers. By 2008, these labs were set up in Mumbai, Thane, Pune and Bangalore. With the establishment of Data Security Council of India that is focused on data protection and cyber security, these cyberlabs were transferred to DSCI which expanded this program to set up additional cyberlabs in Chennai, Hyderabad and Haryana. Nearly 7,500 police officers have been trained in the regular training programs conducted in these cyberlabs. The DSCI instructors and industry experts, works closely with police and judiciary on some of the cases.

The knowledge developed, over a period of time, has been systematized in this manual. It also reflects the collaborative effort of police officers, instructors and industry experts, who came together on a common platform provided by DSCI, to discuss their ideas and experiences, and transform them into material that can be of use to those who are investigating cyber crimes. We hope that this **Cyber Crime Investigation Manual** helps police officers, in handling the crimes more effectively.

Dr. Kamlesh Bajaj
CEO, DSCI

About the Manual

The growing threat of Cyber Crimes and the increasing sophistication in the cyber attacks require expertise of technology savvy investigators to solve the crimes. The misuse of technology by the criminals indulging in nefarious activities is making it difficult for the police organizations stuck in the traditional mould of policing to solve such sophisticated crimes. Seasoned investigation experience alone will not be sufficient to solve complex technology crimes but, need a structured approach with technical expertise to address and resolve cyber crimes. The expertise of the IT industry and, partnerships are the best way forward to build models for developing partnerships and capacity building, which will enable law enforcement agencies to adapt themselves to meet the new challenges.

The Cyber Crimes Investigation Manual, is an outcome of one such unique partnership between NASSCOM and DSCI representing Indian IT industry, and the law enforcement agencies across India. This attempt is small but a significant step towards evolution of standardized methodologies for cyber crime investigations. NASSCOM and DSCI, as part of their Cyber Security Initiative, have engaged with various stakeholders and created a platform for interaction with the leading Cyber Crime Investigators, Subject Matter Experts and IT industry in creating the contents of this manual.

To make the content and approach of the manual relevant and end-user focused, the final draft of the manual before print was shared with different agencies that possessed required expertise and domain knowledge in the field of cyber crime investigations and cyber forensics. We gratefully acknowledge the support of various individuals and agencies in this endeavour. The manual is divided into various chapters:

- **Chapter I** provides a brief introduction to cyber crime threats and also emphasizes on the initiatives taken by the Government of India and NASSCOM-DSCI to tackle this fast growing menace.
- **Chapter II** discusses the different types of cyber crimes, basics of digital evidences, expectations and limitations of computer forensics.
- **Chapter III** This chapter maps different cyber crimes with Information Technology (Amendment) Act, 2008 and other Special Local Laws. An insight is also given into laws/guidelines relating to investigation outside India.
- **Chapter IV** focuses on pre-investigation assessment, preliminary review of the scene of offence and issuance of preservation notice for better plan of action in the investigation of cybercrimes.
- **Chapter V** SOPs (Standard Operating Procedures) is created for the Search and Seizure of Digital evidences, Forensic collection of digital media / data, seeking of expert opinion and collection of information from third party service providers etc.
- **Chapter VI** is organized to help the reader by providing guidelines for the investigation of cyber crimes in different scenarios.

Annexures, at the end of this manual, provide background to basic digital devices, list of cyber crime cells and adjudicators in India, list of national nodal officers and other important information that will be useful to investigators during criminal investigations.

This document is intended to be used by the investigators as a reference and IOs are advised to apply the actions discussed in this manual with his/her prudence.

Pratap Reddy IPS
Director, Cyber Security, NASSCOM

Contents

Chapter 1 : Introduction	9
1.1. Overview of Cyber Crimes	9
1.2. Indian Scenario	9
1.3. Government and Law Enforcement Initiatives	10
1.4. NASSCOM – DSCI Initiatives	10
Chapter II: Cyber Crimes	12
2.1. Definitions	12
2.2. Tools and Techniques Used to Commit Cyber Crimes	12
2.3. Types of Cyber Crimes.	13
2.3.1. Crimes targeting computer systems	14
2.3.2. Crimes in which computer systems are used as tools/instruments	15
2.4. What is Digital Evidence and the Nature of Digital Evidence	16
2.5. Digital Devices – Sources for Digital Evidences	17
2.6. Cyber Forensics	19
2.6.1. Definition	19
2.6.2. Classification of Cyber Forensics	20
2.6.3 What Cyber Forensics Can Reveal	21
2.6.4. What can the IO expect from Cyber Forensic Analysis	21
Chapter III: Application of law	22
3.1. Cyber Crimes and Information Technology Act	22
3.2. Cyber Crimes Mapping with ITAA 2008, IPC and Special & Local Laws.	23
3.3. Laws / Guidelines Relating To International Investigations	26
3.3.1. Legal procedure to gather information from outside India	26
3.3.2. Procedure for Sending Letter Rogatory	27
Chapter IV: Pre-Investigation Assessment	28
4.1. Doing the Basics Right	28
4.2. Is it a crime (as per ITAA2008) in the first place?	28
4.3. Preliminary Review of the Scene of Offence	29
4.3.1. Evaluating the Scene of Offence	29
4.3.2. Preliminary Interviews at the Scene of Offence	30
4.4. Pre-Investigation Technical Assessment	30
4.5. Issuance of preservation notice	31
4.6. Containment of the incident / Offence	32
Chapter V: Standard Operating Procedures for investigations	33
5.1. Importance of SOPs in the Investigation	33
5.2. Standard Operating Procedures – A Flow Chart	34
5.3. Crime Scene Investigation: Search and Seizure	35
5.3.1. Steps in Crime Scene Investigation	35
5.3.2. Panchanama (Seizure Memo) and Seizure Proceedings	35

5.4. Chain of Custody and Digital Evidence Collection Form	36
5.4.1. Chain of custody	36
5.4.2. Digital Evidence Collection (DEC) form	38
5.5. Forensic Collection of Digital Media	39
5.5.1. Identifying/Seizing of the devices needs to be forensically imaged for analysis	39
5.5.2 Investigative Tools and Equipment	40
5.6. Collection of Digital evidence	40
5.6.1 Procedure for gathering evidences from switched-off systems	40
5.6.2 Procedure for gathering evidences from live systems (Switched-on Systems)	41
5.6.3 Procedure for gathering evidences from Mobile Phones	42
5.7. Forensic Duplication – A Technical Introduction	43
5.8. Network Drives Imaging and Logical File Collection	45
5.9. Conducting Interviews	46
5.10. Packaging and labeling of the evidence	47
5.11. Transportation of the evidences	47
5.12. Legal procedure to be followed post seizure of evidence	48
5.13. Expert Opinion from the Forensic Examiner	48
5.14. Analyzing External / Third-party information	49
5.14.1. Time Zone Conversion	49
5.14.2. E mail Headers	50
5.14.3. Cases where the Subject Mail Is Not Available	54
5.15. Gathering information from external agencies/companies	55
5.15.1 Availability of information and format from ISPs	55
5.15.2. Information from e mail service	56
5.15.3. Information from Mobile service providers	57
5.15.4. Information from Social networking sites	57
5.14.5. Information from Financial institutions/Internet banking institutions	57
5.15.6. Information from Web site domain/hosting providers	57
5.15.7. Information from VoIP service providers	57
5.15.8. Analyzing and handling the external data	58
5.16. Correlating the external data with lab findings	58

Chapter VI: Guidelines for Investigation of Offences - Scenario Based

6.1. Case Scenarios	59
6.1.1.Preparation of Forged Counterfeits using Computers /Printers/Scanners	59
6.1.2. Phishing Frauds	60
6.1.3. Obscene Profile on a Social Networking Site	62
6.1.4. Data Theft	64
6.1.5. Blocking of Websites:-	66
6.1.6. Kidnapping Case of a minor girl	67
6.1.7. Hacking using Key logger	68
6.2. Guidelines to prepare charge sheet	69
6.3. Tips to Preserve the Seized Digital Media	70
6.4. Tips to prepare for deposition of evidence in the court	70

Annexures

Annexure 1-1: Cyber Crime Units in India	73
Annexure 1-2: NASSCOM-DSCI CYBER LABS	77
Annexure 2-1: Adjudicating officers Under Section 46 of the ITAA 2008	78
Annexure 2-2: Basics of Digital Devices, Networks, Internet and Mobile Phones	80
Annexure 3-1: Information Technology (Amendment) Act, 2008 (Selected Extracts)	98
Annexure 3-2: International Investigations and Letters Rogatory	110
Annexure 4-1: Model Questionnaire for Pre-Investigation Assessment	116
Annexure 4-2: Questionnaire - Additional Information for Network related incidents	117
Annexure 4-3: Evidence Preservation Instructions	118
Annexure 4-4: Evidence Preservation Notice	119
Annexure 5-1: Legal Provisions for Search and Seizure	120
Annexure 5-2: Chain of Custody Form	122
Annexure 5-3: Digital Evidence Collection Form	123
Annexure 5-4: Forensic Science Laboratories	124
Annexure 5-5: Requisition letter to FSL	126
Annexure 5-6: FSL Requisition-Information to be Furnished	128
Annexure 5-7: Contact Details of ISPs/Email Service Providers and Mobile Companies	129
Annexure 5-8: Sample Letter to the Service Provider	130
Annexure 5-9: General Rules followed by Service Providers to assist LEA	131
Annexure 5-10: Certificates under different Sections of the Indian Evidence Act	132

Glossary of Terms

134

Chapter 1 : Introduction

1.1. Overview of Cyber Crimes

Information Technology and the Internet have led to innovation and economic growth, but have also created new avenues for malicious actors to perpetrate crimes. The perpetrators range from sophisticated hackers to common criminals to foreign intelligence agencies and international terrorists. Cyber threats are increasing for governments, commercial enterprises and industry and above all ordinary citizens.

The all pervasive role of internet and computers and the networks can be gauged from the glance of a newspaper on any given day, on the lives of the citizens, corporations and governments world over. Number of lottery scams, fake profiles on social networking websites and, identity theft for fake banking transactions etc., have become news of daily routine and, are affecting increasing number of ordinary citizens. Commercial enterprises are becoming targets of frauds by insiders, commercial espionage and, intellectual property thefts causing enormous damages to reputations of the companies and, potentially huge financial losses. Finally, the threats of cyber terrorism and, espionage are closer to reality than were anytime in the past. The Wiki leaks episode of publishing of the classified diplomatic communications in public domain is a pointer to the things to come in future. Finally, Governments and regimes are being overthrown, through the sheer power of internet and social networks, as a galvanizing force. While some of these acts may not be classified as Cyber Crimes universally, as Law Enforcement Officers, it becomes necessary to understand and investigate the incidents as and when reported. During the discussion throughout this manual, the word 'Cyber Crime(s)' is used and would mean the same as a Computer Crime and/or Digital Crime for convenience, unless explicitly stated.

Thus, Cyber crime is the latest that is affecting the cyberspace and through it causing physical crimes in the real world, where either the computer is an object or subject of the conduct constituting crime. One way of defining cyber crime is: any criminal activity that uses a computer either as an instrument, target, or a means for perpetuating further crimes comes within the ambit of cyber crime, i.e., unlawful acts wherein the computer is either a tool or a target or both.

1.2. Indian Scenario

As is being seen world over, cyber crimes are on the rise in India also and so are the arrests made in cyber crimes cases. According to "Crime in India 2009" report published by NCRB, there has been an increase of over 45% in the number of cyber crimes reported under 'The Information Technology Act 2000 (IT Act) in 2009 over the corresponding figures for 2008. Apart from the crimes registered under IT Act, there were number of crimes which involved usage of computers in commission of crimes, registered under the provisions of Indian Penal Code (IPC), an increase of over 56% in such cases during 2009 over the year 2008. A total of 696 cases under IT Act and cyber crimes under IPC provisions were registered during the year 2009¹. The following four major categories of crimes reported in India as per NCRB constitutes nearly 90% of the cyber crimes:

1. Hacking of Computer System
2. Forgery / counterfeiting using Computers
3. Publication / Transmission of obscene information in electronic form i.e. Pornography
4. Breach of Trust / Frauds.

CERT-In reports also shows similar tendency of increased reporting of computer security incidents during the year 2009².

¹ <http://ncrb.nic.in/CII-2009-NEW/cii-2009/Chapter%2018.pdf>

² <http://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=annualreport09.pdf>

A total of 8266 computer security incidents were reported in 2009 against 2565 incidents in 2008, representing an increase of over 322% of the number of incidents. A closer look at the CERT-In reports of 2009 reveal that 79% of the incidents reported during 2009, related to Website Compromise and Malware Propagation.

Some states which have taken lead in establishing Cyber Crime Police Stations and, Cyber Crime Cells have shown registration of larger number of Cyber Crime cases than the states which do not have such specialized focus.

According to Director CBI, "The use of modern technology has resulted in traditional crime becoming global. This has made the task of investigation more difficult and complex. There are several examples of kidnapping, terrorist attacks, economic crimes, bank frauds and financial scams being committed with the help of computers"³. Thus, the task before the law enforcement authorities is going to grow in complexity and, urgent focus is needed to build capacity to tackle this growing menace .

1.3. Government and Law Enforcement Initiatives

The realization of the growing threat of Cyber Crimes by Government of India,has led to initiation of a concerted program for Cyber Security under the Department of Information Technology along with enactment of the Information Technology Act, 2000, which was amended in the year 2008 retrofitting newer crimes. The Act heralded the legal recognition of electronic documents, digital signatures and transactions done using computers and internet. Further, the Act described the punishment and penalty for criminal offences and contraventions.

Many law enforcement agencies including the Central Bureau of Investigation have created separate units / cells for handling cyber crimes. Bangalore as the IT capital of India rightfully established country's first Cyber Crime Police Station. As on date, different states and units have created Cyber Crime Police Stations and, Cyber Crime Cells to handle the menace of growing cyber crimes. Details of various Cyber Cells and Cyber Crime Police Stations are provided in **Annexure 1-1**.

1.4. NASSCOM – DSCI Initiatives

Data Protection is emerging as a major corporate and Government concern worldwide. The focus is on secure handling of data so as to ensure privacy of customer data and that of corporate data. Different countries have enacted laws to deal with Data Protection and Data Privacy. While the European Union views privacy of personal information as a fundamental right, the United States has sector specific laws on privacy of customer data. These include laws for protecting health information, financial information. Processing of personal information of citizens of these countries by IT and BPO companies in India and in other countries through outsourcing raises concerns about regulatory compliance. In view of the multiplicity of privacy legislations worldwide, the service providers (IT and BPO companies) in India are faced with a major challenge of demonstrating compliance with laws of countries where the data originates. To address this challenge, NASSCOM took three important steps: it established Data Security Council of India (DSCI) as a self-regulatory organization (SRO) to focus on data protection; it established National Skills Registry (NSR) for background checks and verification of IT professionals employed by the industry; and it established the Cyberlabs program to train law-enforcement agencies in handling cyber crimes.

DSCI is an industry initiative to promote data protection, develop security and privacy codes & standards and encourage IT/ BPO industry to implement the same. Its goal is to raise the level of security and privacy of IT and BPO service providers

³ http://www.cbi.gov.in/speech/nasscom_20101122_dcbl.php

to assure their customers and other stakeholders that India is a secure destination for global sourcing. DSCI has developed Best Practices for Data Protection that are in line with global standards and cover emerging disciplines of security and privacy. DSCI also promotes these best practices for domestic industry segments like Banking, Telecom and E-governance. DSCI Security Framework (DSF) and DSCI Privacy Framework (DPF) are under implementation by the industry to secure their information assets, and protection privacy of customer data. One of the important objectives of DSCI is to help in expeditious trial of cyber crimes. This requires building capacity of law-enforcement agencies, prosecutors and judiciary in understanding cyberforensics.

It is for this reason that the Cyber Labs program, started by NASSCOM in the year 2004, to train police officers in handling cyber crimes, was transferred to DSCI. This program has created a common platform where different stakeholders namely, police, judiciary, IT/BPO companies, financial services industry, academia, and civil society, come together to build awareness and methods of dealing with cyber crimes. The Mission of this Program is as follows:

- Establish Cyber Labs in major cities where the IT/BPO industry is concentrated
- Develop cyber forensics capability
- Impart training to police and industry entrepreneurs to effectively deal with cyber crimes
- Standardize the methods of investigation, promote cyber forensics
- Train police and judiciary in the IT (Amendment) Act, 2008
- Organize industry wide surveys to find out trends in cyber crimes
- Suggest measures for prevention/reduction of cyber crime

NASSCOM had established cyberlabs in Mumbai, Thane, Pune, and Bangalore. DSCI has expanded this program by creating cyberlabs in Chennai, Hyderabad and Haryana. These labs so far have trained over 7500 persons belonging to the police, judiciary, prosecution, banking industry, income-tax, military and other departments of central and state governments. This program has been created with the active support of police and state governments; and corporate entities such as Andhra Bank, Lakshmi Vilas Bank, Canara Bank, Genpact and, IBM Daksh. Recently, Department of Information Technology, Ministry of Communications and IT has given this program a boost for opening a cyberlab in Kolkata, and augmenting the existing infrastructure of Mumbai, Bangalore and Pune cyberlabs. This program is further poised to become a full-fledged Cyber Forensics Program for which a proposal is under development for support of Ministry of Home Affairs.

The Contact List of Cyber Labs being operated is provided under **Annexure 1-2**. These cyberlabs offer Basic and Advanced levels of training to the Cyber Crime Investigators; and also training programs for the judiciary, prosecutors and industry.

Chapter II: Cyber Crimes

2.1. Definitions

There are various definitions of Cyber Crimes and couple of them are discussed below:

- Any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution. — U.S. Department of Justice (DOJ)
- The communication addresses computer crime in its broadest sense as any crime involving the use of information technology. The terms “computer crime,” “computer-related crime,” “high-tech crime” and “cyber crime” share the same meaning in that they describe (a) the use of information and communication networks that are free from geographical constraints and (b) the circulation of intangible and volatile data. — EU Council (Justice and Home Affairs)

2.2. Tools and Techniques used to Commit Cyber Crimes

Cyber Crimes make use of various tools and techniques and many of these tools are used for the commission of the cyber crimes and are installed on the victim’s systems through - exploitation of the vulnerabilities in the systems / networks or by surreptitiously gaining access to the victim’s systems which may include physical access or by making use of the intermediary systems or by deceiving the victim to allow access to his system or by gathering the victim information.

Buffer overflow: The condition when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them

Cracking: Cracking is breaking into someone else’s computer system, often on a network; bypassing passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this either for profit, or maliciously, or for some altruistic purpose or cause.

Data Didling: Involves altering the raw data just before a computer processes it and then changing it back after processing is completed.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

Phishing: Using spoof E-mails or directing the people to fake web sites to deceive them into divulging personal financial details so that criminals can access their accounts.

Rootkit: A set of tools that enables continued privileged access to a computer, while actively hiding its presence from the administrator. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network

Salami Attack: A programmed attack which is implemented in small (meant to be unnoticeable) increments. This attack involves making alteration so insignificant that it is easily concealed and would go completely unnoticed. Attacks are used for commission of financial crimes.

Sniffer: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.

Social Engineering: A hacker term which involves non-technical intrusion for deceiving or manipulating unwitting people into giving out information about a network or how to access it.

Spoofing: Refers to a situation in which the incoming information from an attacker is masqueraded as one that appears to come from a trusted source to the recipient or to the recipient network. Often the messages from the fraudster appearing to be from a genuine source (like bank), seeks personally identifiable information to perpetrate fraud on the victim.

Spyware: It is a type of malware that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.

Steganography: The art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. An image file may contain hidden messages between terror groups, which will be known only to the intended recipient and the sender.

Trojan: A malicious program that masquerades as a benign application and can take complete control of the victim's computer system.

Virus: A self-replicating program that runs and spreads by modifying other programs or files.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Zombie: A program that is installed on a system to cause it to attack other systems.

2.3. Types of Cyber Crimes

Cyber crimes cover a wide range of illegal activities, which are either done solely using computer resources (as defined under Section 2 of ITAA, 2008) or, done in conjunction with traditional means using the computer resources and communication devices as tools to commit conventional crimes. The Information Technology (Amendment) Act, 2008 under Section 66, deals with cyber crimes, with the penal provisions for committing any of the acts defined under Section 43 of the ITAA 2008, if the acts were done with fraudulent or dishonest intentions. Apart from Section 66, the amendment to the ITA2000, has introduced the emerging cyber crimes under its ambit.

The crimes dealt under this section (66), thus presuppose that, all these acts were done with dishonest and fraudulent intentions. If the fraudulent or dishonest intentions are not forthcoming, they will be dealt under Section 43 of the IT Act and, will be dealt with by the Adjudicating Officers notified under Section 46 of the IT Act 2000 (List of Adjudicating Officers is at **Annexure 2-1**).

2.3.1. Crimes targeting computer systems

a. Hacking

(Under Section 66 ITAA 2008)

Hacking is a broader term and can be defined as gaining entry into a computer system without the permission, with an intention to cause loss, steal, or destroy the data contained in it. It is often done by people who are well versed with computer technologies by exploiting some of the vulnerabilities that are present in the computer system. This involves various methods of acquiring sensitive information like usernames, passwords, Internet Protocol (IP) addresses and using them to access the computer system.

Hackers use various applications or programs that can penetrate the defense mechanisms employed by the target computer system and send back the critical information like computer configuration, user names, IP addresses, MAC addresses, etc., which can be used by the hacker to gain entry into the system itself. These applications may be in the form of trojans, malware, worms, and viruses, which will install in the targeted system and compromise its security. After hacking and gaining entry into the computer system, the hacker can gain administrative rights and can do anything with the data contained in it. The computer systems can also be used to infect and destroy other systems.

b. Denial of Service (DoS) attack or Distributed Denial-of-Service (DDoS) attack

(Under Section 66 of ITAA 2008)

In this kind of attack, an important service offered by a Web site or a server is denied or disrupted thereby causing loss to the intended users of the service. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

In some cases, DoS attacks have forced the Web sites to temporarily cease operation. This often involves sending large amount of traffic in the form of e-mails and other requests to the targeted network or server so that it occupies the entire bandwidth of the system and ultimately results in a crash. ICMP flooding, teardrop attacks, peer-to-peer attacks, application-level flooding, etc. are few examples of DDoS attacks. These attacks make use of multiple systems to flood the bandwidth of the targeted system.

Remarks: The above description speaks about high-level sophisticated attack, but in general, there are cases where the attacker causes the denial of access to a computer/computer system/computer network by changing/inserting a password.

c. Spreading viruses and malware

(Under Section 66 of ITAA,2008 or Sec.66F ITAA,2008 in case if it is done against country or to strike terror in the people)

Spreading viruses and malware is the biggest crime that is happening today and most of the Internet users are affected by it. These can be generic or targeted to a specific computer system. Injecting and spreading malicious code also can come in the form of viruses, worms, trojans, spyware, adware, and rootkits. These get installed secretly in the victim's computer system and can be used to access and transmit sensitive information about the system, and in some instances, the infected systems can be used as tools to commit other types of cyber crime.

d. Website defacement

(Under Section 66 of ITAA 2008 or Sec.66F ITAA,2008 in case if it is done against country or to strike terror in the people)

It is an attack on a Web site, which will change the visual appearance, and the attacker may post some other indecent, hostile and obscene images, messages, videos, etc., and sometimes make the Web site dysfunctional. It is most commonly done by hackers of one country to the Web sites of other enemy or rival neighbouring country to display their technological superiority and infecting with malware.

e. Cyber terrorism

(Under Section 66F of ITAA 2008)

Whether traditional or cyber terrorism, terrorists these days are using state of the art technology like satellite phones, communicating through encrypted messages, posting messages and recruiting personnel, raising funds, and creating propaganda using Web sites and Internet technology. When it comes to cyber terrorism, they resort to large-scale disruption of computer networks, Web sites, and attack other critical infrastructural facilities governed by computer systems. In all these instances, digital evidence may be present in the computer systems and computer resources in the form of e-mail, Web addresses, encrypted messages, photographs, videos, etc.

f. Spoofing

(Under Section 66A, 66D of ITAA 2008)

Spoofing is the most common method employed for several network attacks. In spoofing, the attacker masquerades the data packets, IP addresses, MAC addresses, and e-mail addresses so as to create an impression that they are originating from somebody else's addresses.

g. Skimming

(Under Section 66C of ITAA 2008)

Skimming is a kind of credit/debit/ATM/chip/SIM card fraud in which a hand-held device called skimmer is used to capture the information contained in it. The data can be transferred on to a computer system later. The information like name, credit card number, expiry date, etc., can be used to create fake credit cards.

Remarks: If the information obtained by using the above technique is used to make any fraudulent transactions, then section 66D of ITAA 2008 is also applicable

h. Pharming

(Under Section 66C, 66D of ITAA 2008)

Pharming is a type of attack in which the user is deceived into entering sensitive data, such as PIN numbers, credit card numbers, passwords etc., into a fake Web site, which impersonates as genuine Web site. It is different from Phishing in such a way that the attacker need not rely on any of the url or link. Instead, it redirects the Web site traffic from a legitimate Web site to a fake one.

i. Spamming

(Under Section 66A of ITAA 2008)

Spamming is an act of sending unsolicited and junk e-mails or messages by anyone for the purpose of causing annoyance or inconvenience.

2.3.2. Crimes in which computer systems are used as tools/instruments

a. Financial fraud

(Several sections under IPC, ITAA 2008 and other applicable laws)

Financial frauds include business frauds, investment frauds, mass marketing frauds, offering jobs overseas, Nigerian Frauds, business opportunity frauds, etc., where unsuspecting people are lured in trap by the promise of such opportunities and deceived of their money and other valuables.

b. Data modification

(Under Section 66 of ITAA 2008 and sections 403,406,408,409 of IPC as applicable)

In this crime, the criminal gains entry into the targeted system like financial systems and modifies or changes the data contained in a computer system. This type of crime can be committed by the authorized users (insiders) of the computers also.

c. Identity theft and its misuse

(Under Section 66C, 66D of ITAA 2008)

It is the theft of sensitive identity information such as date of birth, name, PAN numbers, passport numbers, credit card numbers, e-mail accounts, etc., for fraudulent purposes. The user may obtain the sensitive information by several means like phishing, sending some links to victim's e-mail address and asking them to furnish confidential information, or obtaining the information through social engineering, using key-loggers, etc.

d. Cyber bullying/Stalking

(Under Section 66A of ITAA 2008 and sections 500,504,506,507,508,509 of IPC as applicable)

It is defined as the use of Information and Communication technologies to harass, threaten or intimidate someone. Cyberbullying can include acts such as making threats, sending provocative insults or racial or ethnic slurs, gay bashing, attempting to infect the victim's computer with a virus, and flooding an e-mail inbox with messages.

e. Data theft

(Under Section 66 of ITAA 2008 and section 379 IPC)

Data theft is copying the data without the permission of the owner of the computer/computer system/computer network. It can be in the form of breaking into the system and copying classified and sensitive information often in the workplace/business. The type of data can be anything like official/business communication, contact details of customers, clients, addresses, user names, passwords, credit card numbers, and other related documents.

f. Pornography

(Under Section 66E, 67, 67A and 67 B of ITAA 2008 and section 292 IPC)

Pornography is posting, publishing, and transmitting obscene messages, photographs, videos, and text through e-mail, Web sites, chatting, and other forms over the Internet. Child pornography is one of the biggest ventures on the Internet.

g. Theft of trade secrets and intellectual property

(Under Section 66 of ITAA 2008, IPR laws and other applicable laws)

It is the theft of knowledge based assets and capital, trade designs, logos, ideas and innovations, material that is copyrighted by an individual or an organization. It also includes audio, video, movies, etc. Highest number of cases under intellectual property theft happened with software and its source code.

h. Espionage on protected systems

(Under Sections 66, 70 of ITAA 2008 and other applicable laws)

This kind of spying and espionage on the government systems is often done by the intelligence officials of enemy or neighboring countries. It involves accessing sensitive and classified documents.

2.4. What is Digital Evidence and the Nature of Digital Evidence

Digital evidence or electronic evidence is "any probative information stored or transmitted in digital form that a party to a court case may use at trial"⁴. Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

The main characteristics of digital evidence are, it is latent as fingerprints and DNA, can transcend national borders with ease and speed, highly fragile and can be easily altered, damaged, or destroyed and also time sensitive. For this reason,

⁴ Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier

special precautions should be taken to document, collect, preserve, and examine this type of evidence. When dealing with digital evidence, the principles that should be applied are, actions taken to secure and collect digital evidence should not change that evidence; persons conducting the examination of digital evidence should be trained for this purpose and activity relating to the seizure, examination, storage, or transfer of digital evidence should be fully documented, preserved, and available for review.

2.5. Digital Devices – Sources for Digital Evidences

Throughout this manual an attempt has been made to provide the investigators an understanding of the investigation of cyber crimes or crimes involving computer resources. Towards this primary understanding and knowledge of the digital devices and their uses is assumed. However, to help the investigators to refresh, the basics of digital devices and their uses, **Annexure 2-2** is provided for reference.

To help the understanding of the Investigating Officers, a compilation of various devices and the potential evidences these devices may contain is provided below.

Sl No	Digital Device		Potential evidence
1	A Desktop Computer Cabinet		The device itself may be evidence of component theft, counterfeiting etc. The device contains digital devices with all the files and folders stored including deleted files and information, which may not be seen normally. Cyber Forensics is used to image, retrieve and analyze the data.
2	Display Monitor (CRT/LCD/TFT etc) Screens of Mobile Phones, if switched on		All the graphics and files that are open and visible on the screen in switched on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and, through description in seizure memo.
3	Smart Cards, Dongles and biometric scanners etc.		The device itself, along with the identification/authentication information of the card and the user, level of access, configurations and permissions.
4	Answering Machines		The device can store voice messages and sometimes, the time and date information about when the message was left. It may have details such as last number called, memos, phone numbers & names, caller identification information, deleted messages.
5	Digital Cameras		The device can be looked for images, videos, sounds, removable cartridges, time & date stamps.
6	Handheld Devices(Personal Digital Assistants [PDAs], Electronic Organizers, Smart Phones)		Much information can be obtained from these devices like Address book, Appointment calendars/information, documents, emails, phone book, messages(text and voice), e-mails passwords etc.

Sl No	Digital Device		Potential evidence
7	Hard Drives		The device in itself, as it stores all the information.
8	Local Area Network (LAN) Card or Network Interface Card (NIC)		The device itself and also MAC (Media access control) address can be obtained.
9	Modems, Routers, Hubs and Switches		The device itself. In routers, configuration files contain information related to IP addresses etc.
10	Servers		Information like last logins, mails exchanged, contents downloaded, pages accessed etc can be obtained.
11	Network cables and connectors		Network cables are used to trace back to their respective computers. Connectors help in identifying the types of devices that are connected to the computers.
12	Pagers		The device can be looked for address information, Text messages, and phone numbers
13	Printers		The device has data like number of prints last printed and some maintain usage logs, time & date information. If attached to a network, they may store network identity information. In addition, It can also be examined for fingerprints.
14	Removable storage media and devices		All new generation mobile phones, cameras etc, use these. These devices store files, in which evidence can be found.
15	Scanners		The device itself, having the capability to scan may help prove illegal activity.
16	Telephones		Many telephones can store names, messages (text and voice), memos, passwords, phone numbers, and caller identification information. Additionally, some cellular telephones can store appointment information, and may act as a voice recorder.

Sl No	Digital Device		Potential evidence
17	Copiers		Copiers may contain some documents both physical and electronic, user usage logos, time and date stamps.
18	CD and DVD Drives		These devices store files / data, in which evidence can be found.
19	Credit Card Skimmers		Tracks of magnetic stripe contain Cardholder's information which may include: Card expiration date. User's address. Credit card numbers. User's name.
20	Digital Watches		Some latest digital watches contain information like address book, notes, appointment calendars, phone numbers, emails etc.
21	Facsimile Machines		These devices contain some documents, phone numbers, send/receive logs, film cartridges that can be considered.
22	Global Positioning Systems (GPS)		The device may provide travel logs, home location, previous destinations, way point coordinates, way point name etc.
23	Keyboard & Mouse		These devices can be examined for fingerprints.

2.6. Cyber Forensics

Computer/ Cyber forensics is an emerging practice to discover evidence from digital devices, and prosecute criminals in a court of law. The term "Computer Forensics" was coined back in 1991 in the first training session held by the International Association of Computer investigative Specialists (IACIS) in Portland, Oregon, USA. Like traditional forensics, Computer forensics is a science, and uses specialized skills, tools and programs.

In simple terms from an investigators' perspective, it is the science of extraction of evidences from digital devices without altering the authenticity of the original evidence object.

2.6.1. Definition

Computer forensics is also called Forensic computing or Cyber Forensics, the youngest branch of forensic science, thoroughly peer reviewed techniques/procedures, well tested tools deals with the preservation, identification, extraction, interpretation, and documentation of computer evidence,. There are various definitions, a few are:

- Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence (Judd Robbins⁵).
- Forensic Computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable" (Rodney McKemmish 1999⁶).
- The study of evidence from attacks on computer systems in order to learn what has occurred, how to prevent it from recurring, and the extent of the damage (McGraw-Hill Dictionary of Scientific & Technical Terms).

2.6.2. Classification of Cyber Forensics

The branch of Cyber forensics can be classified into various sub branches. Some of these sub-branches are:

Disk forensics deals with extracting data/information from storage media by searching active, deleted files and also from unallocated, slack spaces.

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

Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyze wireless network traffic data. The data collected can correspond to plain data or, with the broad usage of Voice-over-IP (VoIP) technologies, especially over wireless, can include voice conversations.

Database Forensics is a branch of digital forensic science relating to the forensic study of databases and their related meta-data. A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.

Malware Forensics deals with Investigating and Analyzing Malicious Code for identification of Malware like viruses, Trojans, worms, keylogger's etc and to study their payload.

Mobile device forensics deals with examining and analyzing mobile devices like mobile phones, pagers to retrieve addresses book, call logs (Missed, Dialed, Received), Paired Device History, Incoming/Out Going SMS/MMS, Videos, Photos, Audio.etc.

GPS forensics, also known as SatNav Forensics, is a relatively new discipline within the fast paced world of Mobile Device Forensics. It is used for examining and analyzing GPS devices to retrieve Track Logs, Track points, Waypoints, Routes, Stored Location; Home, Office, etc.,.

E-mail Forensics: Deals with recovery and analysis of e-mails including deleted e-mails, calendars and contacts.

Memory Forensics deals with collecting data from system memory (e.g., system registers, cache, RAM) in raw form and carving the data from the raw dump.

⁵ http://www.giac.org/download.php?p=gsec_559&c=6203efa1e18401f74c8870e2f54fb3b

⁶ McKemmish, R. (1999) What is Forensic Computing? Trends and Issues in Crime and Criminal Justice

2.6.3 What Cyber Forensics Can Reveal

According to Judd Robbins, the expectations from Cyber Forensics are that it:

- **Protects the subject computer system** during the forensic examination from any possible alteration, damage, data corruption, or virus introduction;
- **Discovers all files** on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files;
- **Recovers** all (or as much as possible) of discovered **deleted files**;
- **Reveals** (to the extent possible) **the contents of hidden files as well as temporary or swap files** used by both the application programs and the operating system;
- **Accesses** (if possible and if legally appropriate) the contents of **protected or encrypted files**;
- **Analyzes all possibly relevant data** found in special (and typically inaccessible) areas of a disk;
- **Prints out an overall analysis** of the subject computer system, as well as a listing of all possibly relevant files and discovered file data and,
- **Provides expert consultation and/or testimony**, as required.

Cyber forensics process encompasses five key elements:

- **The identification and acquiring of digital evidence:** Knowing what evidence is present, where it is stored and how it is stored is vital in determining which processes are to be employed to facilitate its recovery. In addition, the Cyber forensic examiner must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it. After the evidence is identified the cyber forensic examiner/ investigator should image/ clone the hard-disk or the storage media.
- **The preservation of digital evidence** is a critical element in the forensic process. Any examination of the electronically stored data can be carried out in the least intrusive manner. Alteration to data that is of evidentiary value must be accounted for and justified.
- **The analysis of digital evidence** —the extraction, processing and interpretation of digital data—is generally regarded as the main element of cyber forensics. Extraction produces a binary junk, which should be processed, to make it human readable.
- **Report the findings**, means giving the findings, in a simple lucid manner, so that any person can understand. The report should be in simple terms, giving the description of the items, process adopted for analysis & chain of custody, the hard & soft copies of the findings, glossary of terms etc.
- **The presentation of digital evidence** involves deposing evidence in the court of law regarding the findings and the credibility of the processes employed during analysis.

2.6.4. What can the IO expect from Cyber Forensic Analysis

- **Data Recovery:** includes recovering and analyzing deleted files that have not been overwritten, as well as carving out portions of files and text from unallocated and slack space.
- **String and Keyword Searching:** involves looking at known and unknown files, as well as unallocated and slack space, to identify readable text within a binary file or to find a file that contains a specific string.
- **Volatile Evidence Analysis:** gives the analyst the ability to see what state the System is currently in by peering into connections, processes and cache tables.
- **Timeline Analysis:** is the process whereby a timeline of events is created and analyzed based on the modified, accessed and changed times associated with all files that were imaged.
- **System File Analysis:** reveals unauthorized changes to system binaries.

Chapter III: Application of Law

3.1. Cyber Crimes and Information Technology Act

Cyber crime is an intangible dimension that is very difficult to govern or enforce. There are various constraints and it is extremely difficult for conventional laws to address the cyber crime related issues. Information Technology Act 2000 is an Omnibus Act for promotion of e-commerce and e-governance, acceptance of electronic documents at par with paper documents, acceptance of digital signatures at par with normal handwritten signatures, and for dealing with some forms of cyber crime to enhance trust in cyberspace.

The ITA 2000 was amended in December 2008 as the IT (Amendment) Act, 2008 (ITAA 2008), and notified for implementation from 27th October 2009. ITAA 2008 has created a strong data protection regime by mandating reasonable security practices to protect sensitive personal information and several provisions for handling cyber crimes like identity theft and cyber terrorism. The Indian Penal Code and the Indian Evidence Act were also amended to include cyber crimes and digital evidences covered by ITA 2000.

Some of the Indian laws and acts which address various aspects of cyber crimes are as follows:

1. Information Technology Amendment Act 2008
2. Indian Penal Code 1860
3. The Indian Evidence Act 1872
4. The Indian Telegraph Act 1885
5. Bankers' Book of Evidence Act 1891.

Some Salient Features of the Information Technology (Amendment) Act, 2008

- The act applies to any offence or contravention committed outside India by any person, irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India (Section 75)
- Certain documents and transactions like negotiable instruments (excluding a cheque), power of attorney, trust(s), will and contract for sale of immoveable property are excluded from the purview of this act.
- Statutory requirements have been prescribed for retention of electronic records in a format which captures the information accurately and which facilitates tracking back. Intermediaries are liable for penal provisions for non compliance under 67C of the ITAA 2008.
- Controller of Certifying Authorities is responsible for issual of licenses to certifying authorities who in turn are licensed to issue digital signatures (Section 18).
- Dishonest and fraudulent contraventions of acts defined under section 43 of the ITAA2008 are offences under section 66 of the ITAA2008. If the acts are simply contraventions, then they will be dealt by the Adjudicating Officers designated by the government under sections 46 of the IT Act. An adjudicating officer can adjudicate and award a compensation of up to Rs 5 crores.
- Officers of the rank of Police Inspectors and above are empowered to investigate offences under the ITAA 2008
- As per Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Secretary in the Ministry of Home Affairs in Government of India and, the Secretary of the Home Department in respective state / union territory governments are authorized to order the interception, monitoring or decryption of information from any computer resource(s).

- As per Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Central Government can designate an officer of the Central Government (not below the rank of a Joint Secretary) to issue directions for blocking public access of any information in computer resources (Section 69 A of the ITAA 2008).
- Computer offences as per the ITAA 2008 are,
 - Computer related offences (include source code tampering, unauthorized access, disruption, damage etc of computer resources) defined under Section 65, 66 and 66 A to D.
 - Obscenity and related offences as defined in Sections 66E, 67, 67A and, 67B
 - threat to unity and integrity of India (cyber terrorism), Section 66F
 - Power to Issue directions by competent authorities to block access, monitor traffic etc., Sec 67C, 69, 69A, 70 and 70B.
 - CERT-In designated as the National Nodal Agency for Critical Information Infrastructure Protection
 - All the offences with upto three years punishment have been made bailable and, as such only sections 66F, 67A, 67B, 69, 69A and 70 of the ITA are non-bailable.

Portions of ITAA 2008 relevant to IOs are furnished at **Annexure 3-1**. Investigators are advised to refer to the full act, for further clarity.

3.2. Cyber Crimes Mapping with ITAA 2008, IPC and Special & Local Laws

Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
1	Mobile phone lost/stolen		Section 379 IPC upto 3 years imprisonment or fine or both
2	Receiving stolen computer/ mobile phone/ data (data or computer or mobile phone owned by you is found in the hands of someone else.)	Section 66 B of ITAA 2008 - upto 3 years imprisonment or Rupees one lakh fine or both	Section 411 IPC - upto 3 years imprisonment or fine or both
3	Data owned by you or your company in any form is stolen	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to rupees five lakh or both	Section 379 IPC - upto 3 years imprisonment or fine or both
4	A password is stolen and used by someone else for fraudulent purpose.	Section 66C of ITAA 2008- upto 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine Section 420 IPC - upto 7 years imprisonment and fine
5	An e-mail is read by someone else by fraudulently making use of password	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
6	A biometric thumb impression is misused	Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
7	An electronic signature or digital signature is misused	Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
8	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine or both

Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
9	Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge	Section 66E of ITAA 2008- upto 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
10	Tampering with computer source Documents	Section 65 of ITAA 2008- upto 3 years imprisonment or fine upto Rupees two lakh or both Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both	
11	Data Modification	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	
12	Sending offensive messages through communication service, etc.	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Section 500 IPC — upto 2 years or fine or both Section 504 IPC — upto 2 years or fine or both Section 506 IPC — upto 2 years or fine or both — if threat be to cause death or grievous hurt, etc. — upto 7 years or fine or both Section 507 IPC — upto 2 years along with punishment under section 506 IPC Section 508 IPC — upto 1 year or fine or both Section 509 IPC — upto 1 years or fine or both of IPC as applicable
13	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA 2008 first conviction - upto 3 years and 5 lakh Second or subsequent conviction - upto 5 years and up to 10 lakh	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
14	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Section 67A of ITAA 2008 first conviction - upto 5 years and up to 10 lakh Second or subsequent conviction - upto 7 years and up to 10 lakh	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
15	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	Section 67B of ITAA 2008 first conviction - upto 5 years and up to 10 lakh Second or subsequent conviction - upto 7 years and up to 10 lakh	Section 292 IP - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
16	Misusing a Wi-Fi connection if done, against the state	Section 66 - upto 3 years imprisonment or fine up to Rupees five lakh or both Section 66F- life imprisonment of ITAA 2008	
17	Planting a computer virus if done, against the state	Section 66 - upto 3 years imprisonment or fine up to Rupees five lakh or both 66F- life imprisonment	
18	Conducting a denial of service attack against a government computer	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of ITAA 2008- life imprisonment	

Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
19	Stealing data from a government computer that has significance from national security perspective	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both, 66F - life imprisonment	
20	Not allowing the authorities to decrypt all communication that passes through computer or network	Section 69 of ITAA 2008 - imprisonment upto 7 years and fine	
21	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69 of ITAA 2008 - imprisonment upto 7 years and fine	
22	Failure to Block Web sites, when ordered	Section 69A of ITAA 2008 - imprisonment upto 7 years and fine	
23	Sending threatening messages by e-mail	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Section 504 - upto 2 years or fine or both
24	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC - upto 1 year or fine or both - IPC as applicable
25	Sending defamatory messages by e-mail	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Section 500 IPC - upto 2 years or fine or both
26	Bogus Web sites, cyber frauds	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 - upto 3 years imprisonment or fine Section 420 IPC - upto 7 years imprisonment and fine
27	E-mail Spoofing	Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC – upto 2 years or fine or both Section 468 IPC – upto 7 years imprisonment and fine
28	Making a false document	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC - upto 2 years or fine or both
29	Forgery for purpose of cheating	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC - upto 7 years imprisonment and fine
30	Forgery for purpose of harming reputation	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section. 469 IPC - upto 3 years and fine
31	E-mail Abuse	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Sec. 500 IPC - upto 2 years or fine or both
32	Punishment for criminal intimidation	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Sec. 506 IPC - upto 2 years or fine or both - if threat be to cause death or grievous hurt, etc. - upto 7 years or fine or both
33	Criminal intimidation by an anonymous communication	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Sec. 507 IPC - upto 2 years along with punishment under section 506 IPC
34	Copyright infringement	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	Sec. 63, 63B Copyrights Act 1957
35	Theft of Computer Hardware		Sec. 379 IPC upto 3 years imprisonment or fine or both
36	Online Sale of Drugs		NDPS Act
37	Online Sale of Arms		Arms Act

* This is a suggested mapping. Applying the IT (Amendment) Act, 2008, IPC and other laws should be carefully done by understanding the complete facts and relevant context of the case.

3.3. Laws / Guidelines Relating To International Investigations

Cyber Space and computers do not recognize national boundaries but, the law is bound by national boundaries. Thus, in a cyber crime, it so happens that, many a times the victim may be residing in one national boundary, the offender may be from another national boundary and, the offender during the commission of crime may have used the boundaries of some other countries. The investigations thus pose very peculiar challenges and, the investigators during the course of investigations need to resort to conduct investigations outside their national boundaries and as per the criminal law of the foreign country. Hence, it is essential that, each Investigator handling cyber crimes possess the requisite knowledge of International investigations as prescribed under law and, mandated by the Government.

3.3.1. Legal procedure to gather information from outside India

MLAT (Mutual Legal Assistance Treaty) and Letter Rogatory

The legal procedure for gathering information from outside India — MLAT and Letter Rogatory / letter of request, guidelines have been issued by the Ministry of Home Affairs⁷, Government of India. Important guidelines are discussed below. Please refer to the reference at **Annexure 3-2** for full details or consult appropriate authorities for more information.

The Code of Criminal Procedure (Cr.P.C) under Sec.166-A and 166-B provides for the process for making a request to any foreign country to help and assist in the investigation.

Provisions of Law:

166-A Cr.P.C. Letter of request to competent authority for investigation in a country or place outside India

- (1). Notwithstanding anything contained in this Code if, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue a letter of request to a Court or an authority in that country or place competent to deal with such request to examine orally any person supposed to be acquainted with the facts and circumstances of the case and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the Court issuing such letter.
- (2) The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf.
- (3) Every statement recorded or document or thing received under sub-section (1) shall be deemed to be the evidence collected during the course of investigation under this Chapter.

Meaning of Letters Rogatory:

Letters rogatory is a formal communication in writing sent by the Court in which action is pending to a foreign court or Judge requesting the testimony of a witness, residing within the jurisdiction of that foreign court, may be formally taken thereon under its direction and transmitted to the issuing court making such request for use in a pending legal contest or action. This request entirely depends upon the committee of court towards each other and usages of the court of another nation. In the Bofors case a letter of rogatory was issued with request to authorities in Switzerland, for freezing certain bank accounts, and the accused did not claim, any amount connected with Bofors case as being deposited in his Swiss Bank, held that it cannot be said that the accused was deprived of his property and that he is not entitled to any prior notice and opportunity of being heard. *Union of India v Chadha (WN) 1993 Cri LJ 859 (SC)*

⁷ <http://cbi.nic.in/interpol/invletterrogatory.php>

166-B- Cr.P.C. Letter of request from a country or place outside India to a Court or an authority for investigation in India

- (1) Upon receipt of a letter of request from a Court or an authority in a country or place outside India competent to issue such letter in that country or place for the examination of any person or production of any document or thing in relation to an offence under investigation in that country or place, the Central Government may, if it thinks fit,
 - (i). Forward the same to the Chief Metropolitan Magistrate or Chief Judicial Magistrate or such Metropolitan Magistrate or Judicial Magistrate as he may appoint in this behalf, who shall thereupon summon the person before him and record his statement or cause the document or thing to be produced ; or
 - (ii). Send the letter to any police officer for investigation, who shall thereupon investigate into the offence in the same manner, as if the offence had been committed within India.
- (2) All the evidence taken or collected under sub-section (1), or authenticated copies thereof or the thing so collected shall be, forwarded by the Magistrate or police officer, as the case may be, to the Central Government for transmission to the Court or the authority issuing the letter of request, in such manner as the Central Government may deem fit.

3.3.2. Procedure for Sending Letter Rogatory

In order to conduct formal investigation and to collect evidence and gather material objects/documents, Section 166-A of the Criminal Procedure Code, 1973 lays down the procedure of sending ‘Letter of Request’ (Letter Rogatory) through a competent Court. Letter Rogatory is forwarded within the ambit of Mutual Legal Assistance Treaty (MLAT) in criminal matters, Memorandum of Understanding (MoU) Arrangement, etc., existing between India and the requested country or on basis of reciprocity in cases where no such treaty or MoU exists.

No request for issue of a Letter Rogatory (Letter of Request) shall be brought before any Court by an Investigating Agency without the prior concurrence of the Central Authority, i.e., Ministry of Home Affairs (MHA), and Government of India.

The request must incorporate the following details:

- The documents, Photographs, and objects, if enclosed with the Letter Rogatory, should be clearly marked and referred to in the body to enable the requested Authority to know clearly what is required to be done with them.
- All the photocopied papers and documents enclosed must be legible and translated into the required language, if required.
- The Letter Rogatory should be neatly bound and page numbered.
- The authenticated translated copies, duly signed by a translator should be enclosed along with the original Letter Rogatory, if required to be submitted in a language as prescribed in the MLAT, MoU, Arrangement, or otherwise.
- At least, five copies of the Letter Rogatory should be prepared, including the original. Three copies along with the translated version, if any, are to be sent to MHA along with a copy to the International Police Cooperation Cell of CBI.

In General,

- The Investigating officer should obtain the NO OBJECTION CERTIFICATE from the Director of Prosecution / Department of Public Prosecution. The NOC will be issued by Dept of Prosecution after looking into the Dual Criminality Principle.
- The Letter of Request along with the NOC obtained should be routed to the Interpol liaison officer, CBI through proper channel.

Chapter IV: Pre-Investigation Assessment

4.1. Doing the Basics Right

It is very important for every Investigating Officer (IO) to do a pre-investigation assessment for each cyber crime / incident that is reported. It should be generally remembered that, before the complainant approaches the police officer or any agency for addressing their problems, they may have made attempts to set the things right all by themselves or with the help of their friends or some other persons. However, these very acts may result in destruction of crucial digital evidence(s). Similarly, sometimes the criminal act may be a crime in progress, which can potentially cause further damage. It is also possible that, the complainants in their anxiety or due to ignorance may not disclose the full facts at the outset. All these factors will have an impact on the outcomes of the investigations.

Depending on the nature of each incident reported, the IO should collect necessary information from complainant(s) / victims as part of the pre-investigation assessment, to understand the full scope of the incident and, the possible outcomes. This will help the IO to build the plan of action/next steps in the investigation. Investigators and technical personnel are aware of the fact that, the digital evidence is very critical and volatile; hence it is necessary to protect and collect the right evidence for the pre-investigation assessment.

The pre-investigations assessment should consider various aspects of crime including the location and the circumstances.

A set of questions have been compiled to help IOs to elicit information on the nature of the case, which will enable them to quickly gauge the scope of the incident and, understand the systems set up at the crime scene. Such a pre-investigation assessment will help the IO to decide on the priority actions that are necessary in the interest of the securing all the digital evidences without giving scope for their destruction, loss or tampering.

4.2. Is it a crime (as per ITAA 2008) in the first place?

The ITAA2008, contains explicit penal provisions for certain offences (66 A to F). However, Section 66 stands on a different footing, in relation to other penal provisions. Section 66 of the IT Act makes it amply clear that only when a person, dishonestly, or fraudulently, does any act(s) referred to in Section 43 of the IT Act, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees, or with both.

Thus, for an act to be investigated under Section 66 of the ITAA2008 as a Cyber Crime, it needs to satisfy two conditions:

Firstly, it has to be an act as defined under Section 43 of the ITAA2008 and,

Secondly, it should have been done by a person with dishonest or fraudulent intentions. The explanation of the words, dishonestly and fraudulently shall have the same meaning as in Section 24 and 25 of the Indian Penal Code.

Thus, to an IO, if the complaint reveals acts as defined under section 43 of ITAA2008 only but does not reveal commission of these acts with dishonest and fraudulent intentions, then it cannot be investigated as a Crime under IT Act. Under these circumstances, these reports of the acts under section 43 need to be resolved before the adjudicating officers, who were notified under Section 46 of the ITAA2008. Typically, the concerned Secretaries of the Information Technology Departments in the State Governments have been designated as the Adjudicating Officers.

It is suggested to consult Cyber crime cell team or any other expert in this field before issuing an FIR to determine the right section of law, especially under ITAA 2008.

Once the information reveals the commission of cognizable offence under the ITAA2008 and other acts, the IO should

- elicit the information regarding the act under report in detail and, ensure that the details of the offences are captured in the complaint, in full.
- indicate the nature/modus operandi of the cyber crime in detail (include the e-mail address, systems, time zones etc.).
- indicate all the details that can be identified from the complaint like,
 - IP address in case of e-mail and Internet.
 - Profile name or user name in case of social networking abuse.
 - Bank details/Internet banking, branch, etc., in case of online fraud.
 - Credit card details and nature of purchase, etc., in case of card fraud, etc.
- include the time and date in the exact format the complainant mentioned or noted in any of the documentation attached with the complaint (such as e-mails) and, Time zone conversion will have to be taken care during the course of investigation

4.3. Preliminary Review of the Scene of Offence

Typically, the scene of offence can be broadly dealt under,

1. Home of individuals with one or more computers.
2. Cyber Café/Public places.
3. Companies / organizations, with one or more computers and in some cases with vast and complicated network of systems.

At the scene of offence (irrespective of the type of the scene of offence), the IO should carefully survey the scene, observe and assess the situation and decide on the steps for proceeding further. The pre-investigation assessment will help the IO to understand the local situation, circumstances and technical details of the systems / network at the scene of the crime before proceeding to seize / preservation of evidences. As mentioned earlier, the digital evidence is highly fragile and volatile. It will be available in a number of devices, locations and in various formats. For example, the copiers, fax machines, routers, hubs etc., apart from the standard storage / computer devices can also contain vital information relevant to the case / incident. Hence, it is utmost important for the IO to do a preliminary review of the entire scene of offence and also take some additional steps before identifying the evidence and conduct search and seizure. It is very important to include such observations/preliminary review notes in the questionnaire that needs to be sent to FSL for expert opinion. As a matter of practice, IO should videograph / photograph and draw the network architecture sketch in 'as is where is' condition of the crime scene and document it in the panchnama / proceedings.

4.3.1. Evaluating the Scene of Offence

- After identifying the scene of offence, IO should secure it and, take note of every individual physically present at the scene of offence and, their role at the time of securing the scene of offence.
- From the information gathered and based on visual inspection of the scene of offence, IO should identify all the potential evidences. These physical evidences may include conventional physical evidences like the manuals, user guides and, other items left behind like passwords on slips, bank account numbers etc. it is also important to note the position of the various equipment and items at the scene of offence. For example, a mouse on the left hand side of the desktop possibly indicates the person operating the computer is a left-handed user.
- While identifying the digital evidence, IO should make sure that, the potentially perishable evidence is identified

and, all the precautions are put in place for its preservation. At the time of review, disturbing or altering the condition of electronic evidences should be avoided.

- If the systems are OFF, they should not be turned ON for the inspection. If systems are on, it is advised to leave them ON.
- If systems are ON at the scene of offence, IO should take appropriate steps to photograph it, plan for the seizure of the evidences at the earliest and document it. IO should notify appropriate technical personnel to support during the seizure process, so that the perishable evidences (volatile data) are appropriately recovered without loss.
- IO should make note of the attached network cables and power lines to the systems. With the help of the complainant or the technical personnel at the agency, make a note of all the network connections, modems, telephone lines and, mark them both the equipment connection end and, from the source in the walls.

4.3.2. Preliminary Interviews at the Scene of Offence

Conducting preliminary interviews at the scene of offence will help IO to identify and seize potential evidence during pre-investigation. Some of the interview questions that IO can make use are

- What steps were taken to contain the issue? (Physical access denied for suspected persons, disconnecting the suspected computers from network, suspending the employee access and so on) along with list of all suspected names, address, etc.
- Were there any logs (system access, etc.) present that cover the issue? Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?
- Did you observe any similar instance before?
- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give a detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred. (Request a letter of confirmation from complaint)
- Do they have similar systems in any of the branch/other offices?
- Whether log register of the Internet users/other users is maintained? (it is very crucial to fix the responsibility. In case of cyber cafes, it is a must to maintain log register of users for specific period as per the rules framed by several state governments.)
- Are there any questions about the issue that have not been answered? (Affected system list, number of people involved, etc.)
- What are the further plans for analysis of the issue?

At the scene of offence, IO should

- Identify the complainant / owner(s) of the various devices and obtain the access details, usernames, service providers' details. IO should ensure that these persons are available along with the search and seizure team for accessing various password protected / secured information in the presence of the panch witnesses.
- Gather information as provided in the questionnaire(s) above, on all the security systems including encryption policies and, off-site data storage and, data centre and disaster recovery policies of the organization or back-up plans etc.
- Identify the list of the people who can identify the network and a schematic diagram of the network will be useful to be prepared during the interviews.

4.4. Pre-Investigation Technical Assessment

As discussed in the previous section, the pre-investigation assessment should be commenced by eliciting all the right and relevant information which will give the IO an idea about the full scope of the incident / crime. With a view to guide the IOs, a set of questions have been compiled which potentially can lead to holistic understanding of the large networks. While the pre-investigation assessment questionnaire gives the IO a set of questions, each IO needs to keep in mind that this list can further be expanded depending on the crime / crime scene situation.

Scene of Offence: Cyber Café

- Identify number of computer systems present in the cyber café.
- Identify number of computer systems connected to Internet.
- Obtain details about the network topology and architecture (client – Server).
- Obtain the CCTV/Web camera clippings, if any.
- Whether any user management software is used by the cyber café owner?
- Obtain the log register of Internet users for the relevant period.
- Check the formatting of storage devices policy adopted by the cyber café owner.
- Check the hardware replacements done by the cyber café owner.
- Check the policy regarding removal media usage on the cyber café systems.

Scene of Offence: Home

- Identify the type of connection (Wi-Fi/Ethernet).
- How many computer systems are used for Internet connection?
- Location of the system and details of persons with access to system(s).
- Obtain the details about the removable storage media (including external hard disk) used/owned by the user.
- Obtain details about the network topology and architecture (client – Server), if any.
- Obtain the details about other computer peripherals (printer/scanner/modem, etc.).

Scene of Offence: Corporate Environment

- **Questionnaire for crime in which computers are used as instrument/means OR repository:** This questionnaire helps the investigating officer to gather the basic information where crime is committed using the computer systems. Please refer to **Annexure 4-1** for model questionnaire.
- **Questionnaire for crime targeting computer systems:** This questionnaire helps the investigation office to gather the relevant information where crime committed is targeted to destroy or affect the services, etc., of a computer system/server using the Internet or any other network. Please refer to **Annexure 4-2** for model questionnaire.

The above format(s) for pre-investigation assessment will help the IO(s) to understand the incident in totality. At the end of the pre-investigation assessment the IO will be able to decide on the issuance of preservation notices for the designated / authorized persons (in case of a company or large establishment with number of systems) or individuals who are owners of the systems and victims. Similarly it will allow the IO to decide on the kind of technical support to be requisitioned, to proceed with the acquisition of evidences. Above all, the Investigating officer decides how to proceed with investigations.

4.5. Issuance of preservation notice

- Based on the information gathered, the IO should come out with issues to be complied immediately by issuing specific do's and don'ts to the complainant/company/agency — e.g. stopping the access, taking backups, or pre-

serving log information, etc. till further orders. For example, continuing access to the e-mail by the accused can enable him to delete the mails which are incriminating in nature.

- A preservation notice needs to be sent to all affected parties to make sure that they do not delete any data that could be relevant to the case. It is ideal to issue this notice, which is necessary for preserving evidence. For model instructions to complainant and other parties, please refer to **Annexure 4-3**.
- The model preservation notice seen in **Annexure 4-4** has been accomplished through a stipulation setting forth a similar procedural framework outlined by the Court in Simon Property Group vs. mySimon, Inc. 94 F.R.D. 639 (SD Ind. 2000) in USA, to ensure retention of all privileges while properly preserving and processing computer evidence as mandated by the court in Gates Rubber Co. vs. Bando Chemical Indus., Ltd. 167 F.R.D. 90, 112 (D.Colo., 1996). The preservation instructions have been adapted from the above stipulation and, have been suitably amended and Section 91 Cr PC can be invoked to issue such instructions. IOs are free to amend the notice to suit the local requirements and use the format.

4.6. Containment of the incident / Offence

It can be embarrassing for the investigating agencies, if after lodging of the complaint and before effectively starting the investigations, any additional incidents occurs, which enumerates the damage is done. Also, it is possible that the issue that is reported to the agencies may be one of incident out of a series of incidents which are part of an ongoing crime or crime in progress. Also, some criminal links in the chain of the original incident may still be active and, necessary steps to isolate the crime and its various links have to be undertaken.

Incident containment refers to the determination of the nature and scope of the incident and then minimizing the damage, if any. Containment steps may include having more rules on the firewalls to block access, taking the affected machines off the network, disabling user access controls, or creating a black hole for the affected machines. These measures are taken by the victim or organization, in consultations with the investigators / agencies.

- In case of financial frauds, the IO should immediately contact the concerned branches of the banks to freeze the beneficiary/suspect/accused person's bank accounts in case of fraudulent money transfers.
- The IO should request the Service Providers to block/remove and at the same time preserve the access details of the fake/defamatory profiles in social networking/community Web sites. The IO should also notify the Service Providers to preserve the access details of the defamatory/obscene contents.
- If the targeted system is to be restored by the affected party immediately for commercial reasons or in public interest, the IO should obtain the services of technical personnel from the Cyber Forensics divisions and, obtain the image copy of the affected system and permit restoration of the system, only after that. These actions need to be documented with enough justification and should be used under rarest of the rare circumstances. Normally, the restoration is done after the seizure of the evidences and not at the immediate stage of the reporting of the crime.

Avoiding alteration of evidence

The primary aim of the pre-investigation assessments is to "avoid alteration of evidences", crucial in successful prosecution of the cyber crimes. Please reach out for forensic examiner's assistance from any regional forensic labs as quickly as possible, if you are not clear or have any doubt regarding incident and, the understanding of the networks.

Chapter V: Standard Operating Procedures for investigations

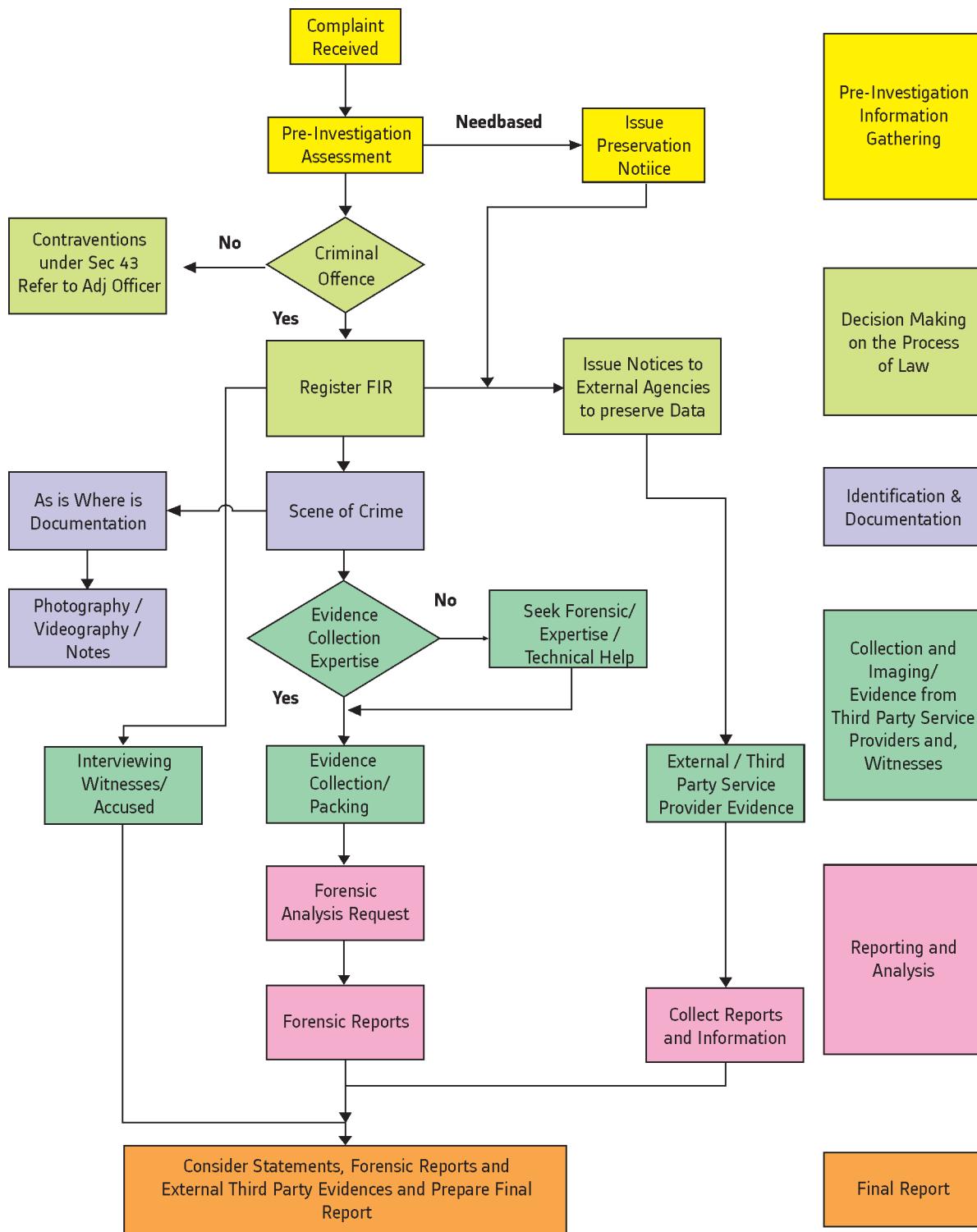
5.1. Importance of SOPs in the Investigation

The SOPs guide us to develop every process in the investigation right from securing the scene and identifying media to be collected, etc., till the time chargesheet is filed and evidence is adduced in the court of law.

Due to the nature and legality of digital evidence, it is clear that investigations in an automated environment requires standard methods and procedures for the following main reasons:

- i. Evidence has to be gathered in a way that will be accepted by a court of law. This will be easier if standard procedures are formulated and followed. This will also facilitate the exchange of evidences in cases having interdepartmental and international ramifications, especially, if investigators from all departments and countries collect evidence in a similar manner.
- ii. Every care must be taken to avoid anything which might corrupt the data or cause any other form of damage, even accidentally. The use of standard methods and procedures minimizes this risk of damage. In some cases, it is inevitable that some data will be changed or over written during the examination process. Thus there is a need for a thorough understanding of technology, which is being used for examination and also need for its documentation so that it would be possible to explain the causes/ effects later on in a court of law.
- iii. Some of the most important reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, incident response training. This may result in a broken chain of custody.

5.2. Standard Operating Procedures – A Flow Chart



Flow Chart for Digital Crime Investigations under ITAA 2008

5.3. Crime Scene Investigation: Search and Seizure

5.3.1. Steps in Crime Scene Investigation

Cyber crime scene is completely different from the conventional crime scene. As mentioned earlier, the digital evidence is highly fragile, and it can be tampered easily and stealthily. Utmost care and, precautions are required during search, collection, preservation, transportation and examination of evidence.

The sequences of steps for digital crime scene investigations are

- Identifying and securing the crime scene
- 'As is where is' documentation of the scene of offence
- Collection of evidence
 - Procedure for gathering evidences from Switched-off Systems
 - Procedure for gathering evidence from live systems
- Forensic duplication
- Conducting interviews
- Labeling and, documenting of the evidence
- Packaging, and transportation of the evidences

The identification and securing of crime scene has been dealt in detail in the Pre-investigation assessment of the Crime and, various guidelines / instructions have been given to ensure capturing of the situation at the scene of crime scene through, 'as is where is documentation' process.

5.3.2. Panchanama (Seizure Memo) and Seizure Proceedings

The legal provisions empowering the IO s to conduct search and seizure are provided under Section 165 Cr PC and, Section 80 of the ITAA 2008(Refer **Annexure 5-1**).

Panchanama and seizure procedure is as important in cyber crime investigation as in any other crime. The Investigating Officer may have to take additional care while conducting panchanama and seizure of digital evidences, keeping in mind the nature of digital evidences. Understanding the basics of digital devices and, ability to conduct a thorough pre-investigation assessment will be of great relevance for a proper search and seizure of relevant and admissible evidences from crime scene. . Below are few guidelines specific to cyber crime. The sequence of steps prescribed above for digital crime scene investigations, should be reflected in the Panchanama.

- Make sure one of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings,to identify the equipment correctly and to guide the IO and witnesses.
- Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding equipment, networks and other communication equipment at the scene of crime.
- Time Zone/System Time play a very critical role in the entire investigation. Please make sure this information is noted carefully in the panchanama, from the systems that are in 'switched on' condition.
- Please DON'T switch ON any device.
- Please make sure a serial number is allotted for each device and the same should be duly noted not only in the panchanama but also in the Chain of Custody and Digital Evidence Collection forms.

- Make sure each device is photographed before starting of the investigation process at their original place along with respective reference like cubicle number or name room soundings, etc.
- Make sure to photograph the Hard Disk Drive or any other internal part along with the system, once removed from the system.
- If possible, please paste the serial number along with PF number/Crime number/section of law
- Capture the information about the system and data you are searching and seizing in the panchanama.
- Brief the witnesses regarding the tools used to perform search and seizure of the digital evidence
- Make sure that the panchas have some knowledge and ability to identify various digital devices
- Document the Chain of Custody and Digital Evidence Collection forms explained below, apart from your regular panchanama as a ‘best practice’, for digital evidences.
- Please make sure all the details mentioned in the forms are completely filled

5.4. Chain of Custody and Digital Evidence Collection Form

5.4.1. Chain of custody

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analyzing the evidence, and so on. As electronic evidence is easy to tamper or to get damaged, it is necessary for us to know exactly who, when, what, where, and why was the evidence transferred to the concerned person. It is possible that defense may level charges of tampering and fabrication of evidence and, it would be difficult to prove the integrity of the evidence, if the chain of custody is not properly maintained. Lack of integrity in the process of custody and, absence of appropriate documentation in this regard, will not only be detrimental to the cyber crime investigation, during trial but also, expose the IOs to criminal liability under Section 72 of the ITAA2008.

Section 72 of the ITAA 2008: Penalty for breach of confidentiality and privacy

"As otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

Needless to say, once the evidence is collected and every time the evidence is transferred, it should be documented and no one else other than the person entrusted with the exhibit shall have access to the evidence.

Important Points to remember for Foolproof Chain of Custody:

- Physically inspect the storage medium — take photographs and systematically record observations.
- Guard against hazards like theft and mechanical failure. Use good physical security and data encryption. House multiple copies in different locations.
- Protect digital magnetic media from external electric and magnetic fields. Ensure protection of digital media particularly optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and data to a minimum.

- Always accompany evidence with their chain-of-custody forms (refer **Annexure 5-2**).
- Give the evidence positive identification at all times that is legible and written with permanent ink.
- Establishing the integrity of the seized evidence through forensically proven procedure by a technically trained investigating officer or with the help of a technical expert will enhance the quality of the evidence when the case is taken forward for prosecution. The integrity of the evidence available on a digital media can be established by using a process called as "Hashing".
- Establish a baseline of contents for authentication and proof of integrity by calculating hash value for the contents. An identical hash value of the original evidence seized under panchanama and, the forensically imaged copy, helps the IO to prove the integrity of the evidence. Similarly, the seized original evidence can be continued to be checked for its integrity by comparing its hash value, to identify any changes to it.

Hashing:

A reliable hash proves that the media contents have not been altered. Hashing program produces a fixed length large integer value (ranging from 80 – 240 bits) representing the digital data on the seized media. Any changes made to the original evidence will result in the change of the hash value.

- **Hash Value Calculator:** Hashing is applying a mathematical algorithm to a file/disk/storage media to produce a value that is unique like fingerprint to that file/disk/dataset and any changes that will be made in the file/dataset will in turn change/alter the hash value. Hash value is one of the widely accepted methods of authenticating any given data set (files/folders/storage media) in the courts of law across the world. The hash value is usually alphanumeric (containing alphabets and numbers). Different types of hash algorithms are available like MD5 (Message Digest 5), SHA256 (secure hash algorithm) for use. The typical MD5 hash value would be like the following example: 2ea029cd5177824a49b9a1a25048a043
- The 128-bit (16-byte) MD5 hashes (also termed message digests) are typically represented as a sequence of 32 hexadecimal digits. The following demonstrates a 43-byte ASCII input and the corresponding MD5 hash:

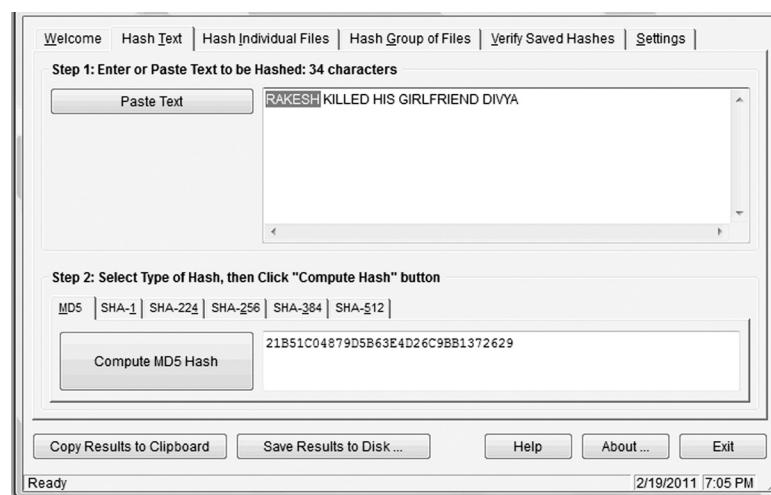


Fig: MD5 Hash of Data "RAKESH KILLED HIS GIRLFRIEND DIVYA"

- Even a small change in the message will (with overwhelming probability) result in an entirely different hash. For example, replacing **k** in the name of Rakesh with letter **j** in the name will result in change of hash value

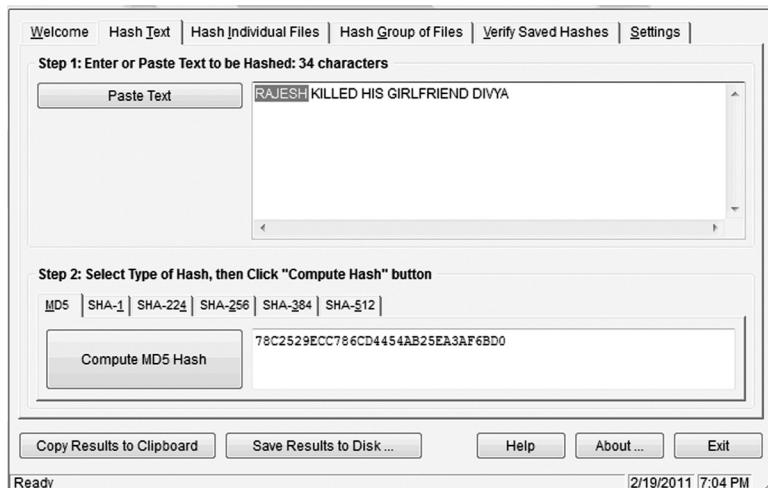


Fig: MD5 Hash of Data "RAJESH KILLED HIS GIRLFRIEND DIVYA". Note an entirely different Hash value when K is replaced with J in the name of Rakesh.

5.4.2. Digital Evidence Collection (DEC) form

Digital Evidence Collection form is one of the most important elements of the forensic process. It is necessary that the steps taken for collection should be accurate and repeatable with the same results every time it is done. For this to happen, a proper documentation of the process used for collection needs to be maintained for every device that is collected. This documentation should contain all the information about the evidence that is visible to the naked eye. It should contain information about the kind of software and version used and the time when the collection process started and ended. This documentation called as the Digital Evidence Collection (DEC) form thus consists of the information on the evidence and the media on which the evidence is being copied to.

If during the process of Digital Evidence collection, the IO is trained or has the technical expert to support him, he should forensically image the evidences and acquire the hash value and note the same in the DEC form as also in the Panchanama. The process, the tool and the hashing algorithm used for hashing should also be reflected in the DEC form (**Annexure 5-3**). The report generated by the forensic tool should form as an enclosure to the DEC.

The standard details captured in a DEC form are given below

- Crime Number / Enquiry Number:
- Applicable Section(s) of the law:
- Date — The date when the equipment is seized/taken for forensic analysis including hash value.
- Name of the Investigating Officer / Enquiry Officer
- Address — Place where the acquisition has taken place

System Information

- Type — Device type which is produced to extract evidence like desktop, laptops, etc.
- Manufacturer — The device manufacturer information to be documented.

- Model Number — The device model number information to be documented.
- Serial Number / any unique identification feature — The device serial number information to be documented.
- Whether acquisition/imaging of the digital media is done at the scene of offence – Yes/No
- If yes
 - Actual Date/Time — Date when the acquisition is performed.
 - Time Zone — The time zone where the acquisition is performed.
- BIOS Date/Time — BIOS information of the device.
- Property Form Number / Evidence Number — Unique number assigned to each device for easy identification by the unit after it is brought to the police station / unit.

Evidence Drive information:

- Type of Media: HDD / USB Drive / Floppy / CD / DVD etc.
- Hard Disk Drive Type — The type of drive that is taken for extracting evidence like SATA/ IDE / SCSI HDD, etc.
- Manufacturer — Name of the manufacturer information to be documented.
- Model Number — The model number of the media information to be documented.
- Serial Number of the media — The serial number information to be documented.
- Sectors imaged / Number of logical partitions— Can be documented from the report after acquisition is performed.
- Jumper settings — If changed, document the settings that are being changed (Graphical representation).
- It is advisable to take a digital photograph of the hard disk to be seized /scene of crime/computer peripherals/ screen shots/processes running/etc.

General acquisition

- Software and Version Number — The forensic software used for acquisition like Cyber Check Suite, Encase, FTK, Helix, etc..
- Write-Protect Device Type — The type of Write Protection device used for protecting the evidence drive from accidental writing.
- Drives information — documenting the information of the two drives where the evidence is extracted, like Original Evidence drive and working copy evidence drive.
- Image file name and Format — Name of the image that is being given and the format for storage of the image e.g., .e01
- Notes — Document all notes starting from the method of acquisition to date and times acquired.

5.5. Forensic Collection of Digital Media

5.5.1. Identifying/Seizing of the devices needs to be forensically imaged for analysis

Ensure that the pre-investigation assessment is complete and, accurate before you commence the Crime Scene Investigation. Make sure you are in a position to identify all the relevant parties and equipment at the scene. This should help you identify all the devices that need to be seized. On-site forensic imaging may be planned, if the IO has the necessary equipment and technical expertise or has technical support to help him. Otherwise, the IO should plan for a simple seizure of the equipment as explained earlier. If the person at the scene of crime is not able to tell you if the device is relevant for investigation, seize it. It may increase your workload, but the chances of you missing something relevant would be reduced.

5.5.2 Investigative Tools and Equipment

Some basic tools and equipment are essentially required to collect electronic evidence. Experience has shown that advances in technology may dictate changes in the tools and equipment required. Preparations should be made to get the equipment required to collect electronic evidence. Investigative agencies should have general crime scene processing equipment, such as cameras, notepads, sketch pads, evidence forms, crime scene tape, and markers. Each aspect of the process (documentation, collection, packaging, and transportation) dictates tools and equipment. The following are some of the basic items that are useful to have in a tool kit at an electronic crime scene:

- Documentation tools such as—
 - Cable tags.
 - Indelible felt-tip markers.
 - Stick-on labels.
- Disassembly and removal tools in a variety of nonmagnetic sizes and types that include—
 - Flat-blade and cross-tip screwdrivers.
 - Hex-nut and secure-bit drivers.
 - Star-type nut drivers.
 - Needle-nose and standard
 - Small tweezers.
 - Specialized screwdrivers (manufacturer specific).
 - Wire cutters.
- Packaging and transporting supplies such as—
 - Antistatic bags and bubble wrap.
 - Cable ties and Evidence bags.
 - Evidence and packing tape.
 - Sturdy boxes of various sizes.
 - Faraday Bags to pack mobile / wireless devices.
- Other items such as—
 - Evidence tags.
 - Evidence tape.
 - Gloves. Forms,
 - A hand truck
 - Large rubber bands
 - A list of contact telephone numbers for assistance.
 - A magnifying glass.
 - Printer paper.
 - A seizure disk.
 - A small flashlight.

5.6. Collection of Digital Evidence

5.6.1 Procedure for gathering evidences from switched-off systems

- Secure and take control the scene of crime both physically and electronically. Physically means sending away all persons from scene of crime and electronically means, disabling the modems, network connections etc

- Make sure that the computer is switched OFF- some screen savers may give the appearance that the computer is switched OFF, but hard drive and monitor activity lights may indicate that the machine is switched ON. Be aware that some laptop computers may power ON by opening the lid. Remove the battery from laptop computers.
- Unplug the power and other devices from sockets.
- Never switch ON the computer, in any circumstances.
- Label and photograph (or video) all the components in-situ and if no camera is available, draw a sketch plan of the system.
- Label the ports and (in and out) cables so that the computer may be reconstructed at a later date, if necessary.
- Carefully open the side casing of CPU or laptop and identify the Hard disk. Detach the hard disk from mother board by disconnecting the data transfer cable and power cable.
- Take out the storage device (Hard disk) carefully and record unique identifiers like make, model, and serial number. If, entire CPU is seized, also note down the any unique identifiers.
- Get the signature of the accused and witness on Hard disk, by using permanent marker. Ensure that all items have signed and completed exhibit labels.
- Search scene of crime for Non-electronic evidences like diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer. Ask the user if there are any passwords and if any off-site data storage. Also ask, for the operating system in the suspected system, the application packages, the various users of the computer etc.,
- After the Hard disk is removed from the suspected system. Switch on the system and go to BIOS. Note down the date and time shown in BIOS.
- Prepare detailed notes giving “when, where, what, why & who” and overall actions taken in relation to the computer equipment.
- Allow any printers to finish printing.
- Connect the suspected hard drive to the investigator computer through write-block device for forensically previewing/ copying/ printing or for duplication. **NEVER CONNECT DIRECTLY WITHOUT THE BLOCKER DEVICE.**

Make detailed notes of all actions taken in relation to the computer equipment

5.6.2 Procedure for gathering evidences from live systems (Switched-ON Systems)

- Secure the area containing the equipment.
- Move people away from computer and power supply.
- Disconnect the modem if attached.
- If the computer is believed to be networked, seek advice from the technically trained officer, in-house forensic analyst or external specialist.
- Do not take advice from the owner / user of the computer.
- Label and photograph or video all the components including the leads in-situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that the computer may be reconstructed at a later date.
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
- Carefully remove the equipment and record the unique identifiers – the main unit, screen, keyboards and other equipment will have different numbers.
- Ensure that all items have signed exhibit labels attached to them as failure to do so may cause difficulty with continuity and cause the equipment to be rejected by the forensic examiners
- Allow the equipment to cool down before removal
- Search area for diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer.
- Consider asking the user if there are any passwords and if these are given, record them accurately.

- Make detailed notes of all actions taken in relation to the computer equipment
- Record what is on the screen by photograph and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph / video and note its content. If password protected is shown, continue as below without any further disturbing the mouse. Record the time and the activity of the use of the mouse in these circumstances.
- Take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory like RAM.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

5.6.3 Procedure for gathering evidences from Mobile Phones

- If the device is "OFF", do not turn "ON".
- With PDAs or cell phones, if device is ON, leave ON. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).
- Label and collect all cables (including power supply) and transport with device.
- Keep the device charged.
- If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in seizure of device and components.

Usage of Faraday bag while seizing mobile phones

A Faraday bag is a bag where a cell phone is placed, so that it cannot receive any Signals. This prevents any changes that may take place in the phone by receiving a Signal.

Benefits for the investigator if a faraday bag is used are:

- 1) Potentially avoids the problem of the mobile phone becoming PIN locked.
- 2) Faraday Window ensures the examiner to view the phone in a 'faraday' condition, thus enabling an 'immediate preview of evidence'.
- 3) Re-usable
- 4) To prevent the data from the networks communicating with the device, therefore stops any chance of evidence being tainted.
- 5) Prevents any chance of evidence being manipulated during covert acquisition.



Mobile Number Portability (MNP):

Slowly and gradually India is joining the other countries of the world which have already given the power to the customers to choose their telephone operator by holding on to their individual mobile number. While from the customer perspective this is a good move, it will definitely throw up new challenges to the Law Enforcement Agencies (LEA) in monitoring and tracking criminals for investigation or intelligence gathering purpose.

Till now our understanding of mobile numbers has been based on the series or the MSN code normally indicated by the first 4 or 5 digits of the mobile number. With these digits we were able to deduce as to which Telephone Operator the number belongs to, which state or circle it pertains to and whether it is GSM or CDMA number. Infact, LEAs maintain database of all series numbers operating in India and refer it to find out this information. This used to be the first step for any further investigation or enquiry. Based on this information only we can approach the concerned Nodal Officer of the Telephone Operator for name and address (SDR), CDR or tower location etc.

As discussed in the previous section, the pre-investigation assessment should be commenced by eliciting all the right and relevant information which will give the IO an idea about the full scope of the incident / crime. With a view to guide the IOs, a set of questions have been compiled which potentially can lead to holistic understanding of the large networks. While the pre-investigation assessment questionnaire gives the IO a set of questions, each IO needs to keep in mind that this list can further be expanded depending on the crime / crime scene situation.

After MNP, this job will get tougher. Numbers belonging to a particular series may belong to more than one operator thereby causing duplication and confusion. We may have to confirm with the Telephone Operator whether the number actually belongs to it or has been ported out to any other operator. This would definitely lead to delay

To overcome this problem DoT is creating a web portal access for which is being given to different LEAs with secure username and password. This portal will contain details of all numbers ported between different operators. While this may solve the problem to some extent, there would still be delay as another verification layer is getting added.

As such MNP has arrived and it is going to stay. In the interest of customer choice, we need to welcome it. At the same time we need to adapt to the changing situation by reorienting our systems and procedures.

5.7. Forensic Duplication – A Technical Introduction

Forensic duplication refers to bit stream imaging of data from the digital media in question. Data resides in all sorts of storage media present in computers, smart phones, GPS devices, USB drives, and so on. We need to be able to get to this information in a manner that it does not change the information on the devices themselves. If the evidence is not collected properly, we face an issue where the results of the forensic exam will be put in doubt. Hence it is necessary to copy the data carefully in a forensically sound manner.

Files can be copied from suspected storage media using two different techniques:

Logical Backup	A logical backup copies the directories and files of a logical volume. It does not capture other data that may be present on the media, such as deleted files or residual data stored in slack space.
Bit Stream Imaging	Also known as disk imaging/ cloning/ bit stream imaging generates a bit-for-bit copy of the original media, including free space and slack space. Bit stream images require more storage space and take longer to perform than logical backups.

- When a bit stream image is executed, either a disk-to-disk or a disk-to-file copy can be performed. A disk-to-disk copy, copies the contents of the media directly to another media. A disk-to-file copy copies the contents of the media to a single logical data file.

- During backups and imaging, the integrity of the original media should be maintained. To ensure that the backup or imaging process does not alter data on the original media, investigator should use a write-blocker while backing up or imaging the media.
 - A write-blocker is a hardware or software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.
 - When using a hardware write-blocker, the suspected storage media used to read the media should be connected directly to the write-blocker, and the write-blocker should be connected to the computer or device used to perform the backup or imaging.
 - When using a software write-blocker, the software should be loaded onto a computer before the media or device used to read the media is connected to the computer.
- After a backup or imaging is performed, it is important to verify that the copied data is an exact duplicate of the original data.
- Computing the message digest of the copied data can be used to verify and ensure data integrity. A message digest is a hash that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated.



- Forensic image files, (i.e., Cyber Check Suite ".p01", Encase ".e01", or SafeBack ".001/.SFB" files) are written as logical files and shall be created on brand new freshly formatted media or forensically wiped sterile media if new media is not available. HDDs are to be used only once for original evidence storage.
- Logical file copies of the forensic image files shall be made on brand new (sterile) HDDs before traveling back to the office. These drive copies shall be labeled as copy of hard drive, etc.,. Using barcode is one of the best methods. In case of nonavailability of barcode, a serial code with relevant information like unit name, year, case number, etc., can be used.

Some of the ways for acquiring data in a forensically sound manner from different devices are:

Hard Drives (Desktops and Laptops): Use forensic software like Cyber Check Suite, Encase, FTK to image the drives. Be sure to connect the evidence drives to a write blocker so that the OS does not accidentally write to the hard drive. The Write blockers restricts any data to be written on to the seized hard disk either intentionally or accidentally. The Write protection device is used as an interface between the seized media and the forensic computer.

Smartphone: Use software like Cellebrite, Paraben Device Seizure to image cell phones. Information like SMS, MMS, call records, contact lists, GPS info, pictures and videos can be acquired from a cellphone. For most cell phones, there is no way to make sure that there is no change on the device, short of taking apart the phone completely and acquiring the information using extremely advanced methods. But the courts accept information that has been gathered using forensic software. Also, precaution should be taken while working with the mobile phones in ON mode, like usage of Network jammers/Faraday's bag.

USB Drives: USB drives can be imaged using software/hardware-based write blockers to connect to the forensic machine and then imaging the drive.

Digital Camera: The memory card and the internal memory present on the camera can be acquired using the technique for USB drives.

Process to be followed when the hard disk drive(s) cannot be removed:

- With laptops shrinking in size and Solid State Drives (SSDs) like in MacBook etc., becoming more prevalent than regular hard drives, it is certain that you would come across laptops wherein it is not possible to remove the hard drive from the laptop easily. Also, there are some other devices like network attached printers and CD/DVD duplicators, which contain their own hard drive and they may be easily removable.
- If the hard drive cannot be removed from the device, then it would be necessary to get the entire device into evidence. This is a better option than going through documentation on how to safely get the drive out or worse, breaking into the device to get the hard drive out.
- If the hard drive cannot be removed, then we have to image the computer using network acquisition. This is done by connecting the evidence computer to the forensic computer via a special Ethernet cable called a cross cable (Network crossover cable). Once the computers are connected, boot the evidence computer from a forensic Distribution like Helix or Linen and connect the forensic computer to the evidence computer using forensic tool like Encase. Now, the acquisition just occurs like a regular hard drive acquisition.

5.8. Network Drives Imaging and Logical File Collection

There are scenarios in which it is not possible to take the evidence machine offline, like the machine may be a file server or a database server serving up business-critical applications. In such cases, we do not shutdown the machine and take the hard drive out. In the course of the interview, we need to determine if the machine has any relevant data and if so, where it is stored. In such cases, data is copied to external drives using forensic tools like Cyber Check Suite, Encase Logical File Collection or tools like robocopy.

Network and Parallel Cable Acquisitions

Another method of acquiring hard drives is via a network cable between a machine containing the target media, booted to forensic tool for DOS, and a second machine running forensic tool in the Windows environment. It often provides the best of both worlds, allowing some of the advantages of a DOS boot (Direct ATA access) combined with the enhanced functionality of the forensic tool in Windows.

If you encounter an HPA (Host Protected Area) or DCO (Device Configuration Overlay), you can place the drive in a safe lab machine and boot to forensic imaging tool for DOS while connected to your regular lab acquisition machine running forensic tool in a Windows environment. Likewise a network cable acquisition is useful for booting from the suspect's machine when encountering geometry mismatches between a legacy BIOS (usually the suspect's machine) and a new BIOS (usually your lab machine) or when encountering RAID configurations. A RAID can be booted to DOS using its native hardware configuration to mount the logical physical device. The forensic imaging tool will see this RAID as a mounted physical device, enabling acquisition and preview via the network cable connection to forensic tool in Windows.

Sometimes removing a hard drive from a laptop is problematic due to physical access or other concerns, such as proprietary security schemes marrying the hard drive to the mother-board. If you are able to access the BIOS and control the boot process, a network cable acquisition is a viable option as long as you use a great degree of care and prudence.

A network cable acquisition is also very handy for “black bag” jobs where you have to quickly acquire a target hard drive when the owner or user of the target hard drive is not physically present. With little disturbance to the physical environment, you can connect your examination laptop to the target machine via a network cable, boot to forensic tool for DOS, and preview or acquire if needed.

The forensic tool for DOS doesn't allow direct previewing of the data; however, when connected via network cable for Windows mode, you can see the drive completely in the GUI environment. In circumstances where the presence of certain images or keywords must be present to warrant seizure, a network cable acquisition is very useful. Thus it is a great tool for a variety of field and lab situations.

Before starting a network acquisition, you must keep a few other considerations in mind. The first is the cable. We have been calling it simply a network cable acquisition, but the cable used is more specifically a network crossover cable. A “yellow” crossover cable .Yellow does not necessarily denote a crossover cable in the field. Twisted-pair cable comes in a variety of colors, and those colors can be used to denote cable for a room, subnet, or any other differentiating purpose. Sometimes there is no purpose—someone needed to make a cable and used whatever color was available. Often a crossover cable has a tag or label to denote it, but don't depend on it!

A crossover cable is a network cable used for special purposes, one of which is to enable two computers to have network connectivity by connecting directly to each other via a single network cable. A regular network cable will not work for this purpose. On a crossover cable, on one end only, the positive and negative “receive” pair are switched with the positive and negative “transmit” pair, respectively with regard to the positive and negative to maintain polarity. In this manner, the machines can “talk” to each other over the network crossover cable.

NOTE: Evidences from Data Centres or large server set ups cannot be immediately acquired. Under these circumstances, the Investigating Officer should ensure that the custodian of the data centre/server setup should be issued with summons under section 91 CrPC to either produce them at the date and time prescribed or to keep them in safe custody for production at later date to be intimated in due course.

5.9. Conducting Interviews

Evidences have always played key role in any investigation. Therefore, before diving deep into facts of the case, court of Law have always been emphasizing over the evidences and its integrity. However, maintenance of integrity of digital evidences presents their unique set of problems owing to their nature when comparing with traditional physical or documentary evidence. There are some cases wherein digital evidences have been altered knowingly or unknowingly before it was handed over to law enforcement. A possible likelihood, situations is when the victim itself discovered and investigated any crime and later on get involved in the law enforcement agency. These evidences, when produced before the prosecuting authorities, may question about the authenticity of evidences and it may not be worth if evidences are used without establishing the chain of custody and authenticity of the evidence.

General Investigative Questions

Ensure that the answers to the following questions are captured during investigation and seizure of evidences:

- 1) When the incident did first came to his notice?
- 2) How it was established that action in question has been performed by any outsider or some user has performed in excess of his privileges provided?

- 3) What are the foreseen damages?
- 4) Who could be the potential intruder (Prime Suspect)?
- 5) What is the main reason of such doubt?
- 6) What could be the major impact on the business?
- 7) What are the major Systems which are required to run the critical functions of the business?
- 8) What actions have been taken to identify, collect, preserve, or analyze the data and the devices involved?
- 9) Had the evidences been collected and devised by a trained person?

5.10. Packaging and labeling of the evidence

Package and labeling refers to the collection of the evidence and then numbering them in a way that it would be easy to go back and retrieve the data at a later date/time. Every piece of evidence needs to get a tag number, which contains all the visible details on the evidence. This information then goes into evidence Database, which contains details of all the evidences and the tag number on it.

It is necessary to understand that tagging is a very important part of the forensics process as it allows us to find the evidence needed among the plethora of evidence that is collected at a crime scene.

Primarily the IO has to choose packaging that is of proper size and material, to fit into the evidence. This is a key point. Do not drop your digital evidences into a plastic grocery bag you commonly find or some make shift package, and then expect it to hold up the digital evidences in good shape. Various types of evidence need special packaging, so you need to come to the scene prepared with a variety of evidence envelopes, bags, and containers. The packaging should also be clean, and preferably new, to avoid contamination. The IO's toolkit as per the check list provided earlier in the manual will help the collection of the evidence in the prescribed manner and in a safe manner without damage.

In addition, each piece of evidence should be packaged separately and then properly labeled, sealed, and documented. These steps are crucial for establishing the chain of custody. As we all know, when a case goes to court, the defense will look for any sign of tampering or poor record keeping to try to get the evidence — and the case — thrown out. So be meticulous with your work, but also be smart.

As much as possible, try and use anti-static bags to transport evidence as these will protect and prevent any localized static electricity charge from being deposited onto the devices as the bags are handled.

5.11. Transportation of the evidences

Diskettes have fragile magnetic media. If they are packed loosely and allowed to strike each other repeatedly during transit, the media could be damaged and the data may be lost. Hard disks should not be subjected to shocks. When transporting a CPU, devices, or media, they should not be placed in a vehicle trunk or area where there will be drastic changes in temperature. Pack the evidence securely. Be careful to guard against electrostatic discharge. Photograph/videotape and document the handling of evidence and ensure that this is appropriately captured/included in the seizure memo (pancha nama) to effectively establish the handling of evidences.

The dispatch and transportation of evidences is another crucial aspect that has to be kept in mind by the IOs. Poor dispatching and transportation practices can physically damage the evidences collected and thereby rendering them useless. Sometimes, the poor handling may result in alteration of the contents of the digital evidences due to shock and external

electro-magnetic interferences. Such changes can put a question mark over the integrity of the evidences collected by the Investigating officer. While sending the evidences to the Forensic Science Laboratories, always ensure that

- The suspected computer storage media is carried by a special messenger but not by Registered / Insured post.
- A fresh hard disk of approximately same capacity should also be submitted for forensic imaging along with the suspected storage media.

5.12. Legal procedure to be followed post-seizure of evidence

Once the digital evidence is seized during the course of investigation, it should be brought to the notice of the jurisdictional court (property form number should be given by the IO) and

- a. Obtain orders of the competent court to retain the seized properties in the custody of the investigating officer for the purpose of investigations.
- b. Obtain necessary orders from the competent court to Image/send the digital evidence for forensic analysis and expert opinion. The PF number should be mentioned in all the transactions included in the chain of custody.
- c. In cases where the accused persons or the owners of the property seized approaches the court for release of the impounded properties, the IO should carefully prepare objections for such applications and ensure that no original evidences are returned which have a bearing on the prosecution of the case. Wherever, the court orders for release of the seized properties, IO should ensure that only a forensically imaged copy of the seized property is given to the accused/owner and never return the original material seized, unless the court orders so.

The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence [ACPO] suggests four principles when dealing with digital evidence, summarized here:

- No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- An audit trail or other record of applied processes, suitable for replication of the results by an independent third-party, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

5.13. Expert Opinion from the Forensic Examiner

The following guidelines should be kept in mind by the IOs while forwarding the digital evidences for forensic analysis from Forensic Sciences Laboratories or any other Government recognized examiner of electronic evidence authorized to offer such services. **Annexure 5-4** lists various Forensic Science Laboratories in India.

The forwarding letter to the FSL for scientific analysis and opinion should mention the following information.

- Brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of crime
- The condition of the computer system (on or off) at the scene of crime
- Is the photograph of the scene of crime is taken?
- Is it a stand-alone computer or a network?
- Is the computer has any Internet connection or any means to communicate with external computers?

- The investigating officer should interview the accused for obtaining the following information:
 - The name of the operating system
 - The application software packages used in the computer system with specific reference to the case like TALLY, FOCUS etc.
 - Any files which were password protected and if the accused cooperates, the passwords for the files
 - The employees who have access to the computer systems, their names, designations and their nature of work.
- Is the BIOS date and time stamps were taken, or not? If taken the date and time should be mentioned?
- Is the storage media forensically imaged and hashed for maintaining the integrity of the evidence? If so the HASH value should be mentioned & the algorithm used for hashing.
- The signature of accused along with two witnesses should be taken on the suspected storage media.
- Is the storage media previewed, if so, is the preview done forensically or not?
- Some keywords useful and relevant to the case.
- The date and time at which the panchanama of the seized computer system was written
- The questionnaire should include
 - The printout of important files relevant to the case
 - Output from the application software packages
- ✖ The investigating officer should avoid questions like
 - Printout of all the files existing in the computer system
 - In which country / place the operating system was loadedAny incriminating material relevant to the case.
 - Please list out all frauds committed by the accused using this laptop.
- At the time of forensic analysis of the image of the suspected computer storage media if the forensic expert feels that the investigating officer presence is necessary at the forensic lab the investigating officer should be available for the same.

All the electronic evidence requires an expert examination. (refer to Section 79 A of ITAA 2008). While sending the seized digital media to the FSL, it is very important to inform the case history, persons involved, reasons IO relied on to seize various systems, etc. Template for forwarding electronic evidence to the FSL for scientific analysis is provided at **Annexure 5-5**.A set of sample questions are provided at **Annexure 5-6**, which will guide the IOs to seek expert opinion based on the facts of the case and type of crime. IO should share the information gathered by them vide **Annexure 4-1** and / or **Annexure 4-2** to the forensic examiner, so as to enable him to have a full understanding of the case under investigation / analysis. This will help the forensic examiner to take some additional steps in analyzing and extracting the information.

5.14. Analyzing External / Third-party information

5.14.1. Time Zone Conversion

Time Zones and their conversions play a very important role in attributing acts / incidents to the accused. A time zone is a region of the earth that has uniform standard time, usually referred to as the local time. By convention, time zones compute their local time as an offset from UTC (Greenwich Mean Time). Local time is UTC, plus the current time zone offset for the considered location.

For each computer system/server time zone set to its current location/local time. It is very important to know the time zone of that system to establish the exact time of offence and subsequent actions of the crime as supportive evidence.

Since the time zone/difference may vary more than 12 hours for few locations for example United States of America, date of the occurrence of the crime may also change. This is very critical and important especially in crimes involved in sending e-mails from servers out of India. Time zone Conversion plays an important role in converting all the acts and incidents to one common time (usually the local time), so that the offences and the offender can be clearly linked. There are number of online Web sites/applications that are available to convert the time to Indian standard time (IST) and vice-versa. A useful link is, <http://www.timeanddate.com/worldclock/meeting.html>.

5.14.2. E-mail Headers

In most of the cyber crime where e-mails are involved, analysis of e-mail headers plays a very important role. Each e-mail whether it is a company e-mail or Web-based e-mail like hotmail, yahoo, etc., carries lot of information about that e-mail. Information like sender IP address, e-mail address, time and date when the e-mail sent, through which server it passed, etc.

E-mail header analysis can help an investigator to find out the IP address of the e-mail sender. E-mail message headers are digital histories that are attached to every e-mail message that are sent and received. Headers record important information, including servers that the e-mail has traveled through, and the date and time that the message was received or forwarded.

E-mail messages

- Are attached automatically to every e-mail message that's sent and received.
- Comprise of 2 sections.
 - **Message Description:** Contains details of the sender and recipients, subject line, and sending date.
 - **Message Path:**
 - Contains the server name and timestamp for every server the message travelled through.
 - Displays entries in the message path in reverse chronological order.
 - The header details can be copied and pasted into 'notepad' or similar program and, then the information is analyzed.
 - Some free and popular tools on the internet, offer e-mail header analysis on-line. One such tool is available from CDAC at <http://www.cyberforensics.in/OnlineEmailTracer/index.aspx>. One has to simply paste the copied header information into the designated window of the website and, the tool provides the analysis of the e-mail header. However, it will be of great value, if the IO understands some basics of the e-mail header analysis.

E-mail Header components

- Message headers are easiest to view if you copy and paste them in a text program, such as Notepad.
- Get them printed with along with the subject line in the presence of the IO and witnesses, to avoid allegations of tampering at a later date.
- For header analysis, it is best if you delete out the message description from the header as it is not necessary for our investigation. The description is present in the message when you view it normally, so keeping it in the header during analysis would be a redundancy.
- Here is an example of a message header

Received: from EXIC1.lse.ac.uk ([158.143.216.121]) by ExF2.lse.ac.uk with Microsoft SMTPSVC(5.0.2195.5329); Tue, 15 Jul 2003 12:16:56 +0100
Email passed from Exchange gateway servers to staff mailbox server
Received: from EXAV2.pc.lse.ac.uk ([158.143.216.132]) by EXIC1.lse.ac.uk with Microsoft SMTPSVC (5.0.2195.5329);
Tue, 15 Jul 2003 12:16:55 +0100 Email passed from antivirus servers to Exchange gateway server
Received: From exas1.lse.ac.uk ([158.143.216.135]) by EXAV2.pc.lse.ac.uk (WebShield SMTP v4.5 MR1a);
id 1058267813844; Tue, 15 Jul 2003 12:16:53 +0100 Email passed from anti-spam servers to antivirus servers Content-

Class: urn:content-classes:message X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4910.0300
 Received: from **web60003.mail.yahoo.com** ([216.109.116.226]) by exas1.lse.ac.uk with Microsoft SMTPSVC (5.0.2195.5329);
 Tue, 15 Jul 2003 12:14:24 +0100
 Message-ID: <20030715111424.6388.qmail@web60003.mail.yahoo.com>. Received: from [158.143.113.49] by web60003.mail.yahoo.com via HTTP; Tue, 15 Jul 2003 12:14:24 BST

- Here we see that the e-mail originated from the IP address **158.143.113.49** and was received by **web60003.mail.yahoo.com**. Now, the e-mail traversed the path as given in the header to the victim's e-mail address in reverse. In such a case, first do a reverse DNS lookup on the IP address by going to your forensic machine which is connected to the Internet and type this command in the command prompt "nslookup 158.143.113.49". This should give you the domain name of the machine. Now, go to a free online whois Web site, e.g.: www.apnic.net and type the IP address in the text box. It will tell you who the IP address is registered to and the contact details.
- Now you can further your investigation by contacting the ISP of the IP address or the company to which the IP address belongs to provide the physical address details.

Limitations of E-mail Headers as Investigative Tools

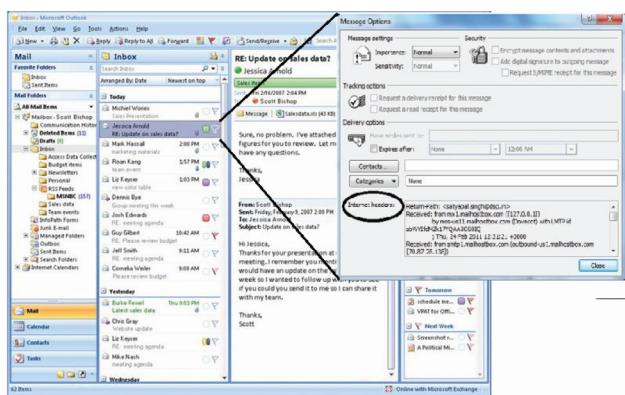
It may not be always possible to trace the originating IP address of the email message under investigation due to reasons such as,

- Mail Service Providers like Google mask the originating IP address of the email and hence simple header analysis cannot give the IO any clue regarding the origin of the email. In these cases, the IO has to rely upon the information furnished by the mail service provider to trace the origin of the mail.
- I.P spoofing and proxy servers can mislead the Investigating Officer by directing them to a wrong origin of the mail location or in some cases no useful conclusion can be drawn from the header analysis. Under such circumstances, the IO should seek expert help to further proceed with the investigations.

Accessing Message Headers

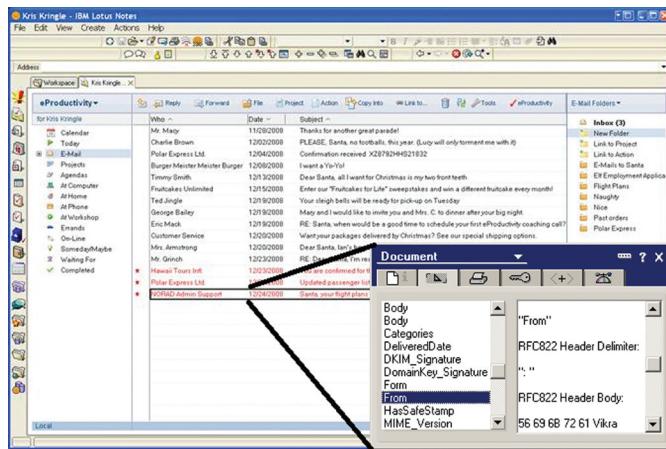
Outlook 2007: Outlook is one of the most popular e-mail clients. To obtain header information of individual mails from Outlook,

- Open Outlook and then open the **message**.
- On the **Message** tab, in **Options** group, click **Dialog Box Launcher** icon image.
- In the **Message Options** dialog box, the headers appear in the **Internet headers** box.



Lotus Notes: Lotus notes is also one of the most popular e-mail client. To obtain header information of individual mails from the outlook

1. Open Lotus notes and then open the **message**.
2. On the **Message** tab, in **Options** group, click **Dialog Box Launcher** icon image.
3. In the **Message Options** dialog box, the headers appear in the **Internet headers** box.



Gmail: One of the most popular web-based e-mail service providers. However, google masks the originating information with respect to mails originating from its own mail accounts. For example, if abc@gmail.com sends mails to accounts say xyz@indiatimes.com and def@gmail.com, the originating IP information will not be reflected in the e-mail received both the recipients. However, if a gmail e-mail account receives the mails from different service providers, the originating IP address will be reflected in the mail headers.

In cases pertaining to gmail originating e-mails, the IP address and other relevant information can be obtained by the Investigating officer by sending requisition to Google under relevant provisions (eg., Section 91 CrPC).

1. Log into your GMail Account.
2. Open the Email for which one need to view the headers.
3. One can see a little arrow pointing down next to Reply. Click on this down arrow next to Reply.
4. A drop down menu will open up. Select Show original in this menu.
5. The full headers will now appear in a new window.

The screenshot shows a Gmail message window for 'The eEye Research Team'. The message content is about a Microsoft Patch Disclosure. The 'Reply' dropdown menu is open, and the 'Show original' option is highlighted with a yellow box. Other options in the menu include 'Forward', 'Filter messages like this', 'Print', 'Add The eEye Research Team to Contacts list', 'Delete this message', 'Report phishing', 'Message text garbled?', and 'Translate message'.

Yahoo mail: Y!Mail is the second largest web-based email service with two versions, Yahoo Mail Classic and New Yahoo Mail.

Yahoo Mail Classic

- Log into your Yahoo! Mail account.
- Click on the email and open it
- On the bottom right corner is a link called “Full Header”
- Once you click on “Full Header” the header will show up at the top of the email message.

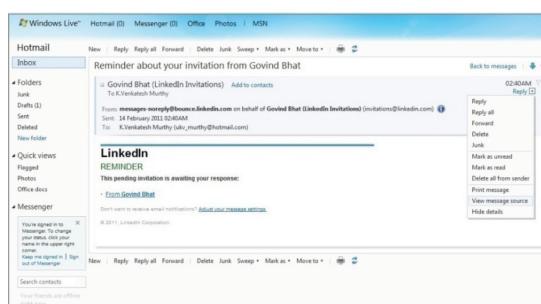
New Yahoo Mail

- Click on the Inbox to see the list of your messages.
- Click on the message and open the email.
- On the top right corner of the email message you will see “Standard Header” and an arrow next to it. Click on this arrow and then click on “Full Headers”
- A new window will open with the header information.



Hotmail: Formerly known as MSN Hotmail was the first free email service providers. The current version is known as ‘Windows Live Hotmail’.

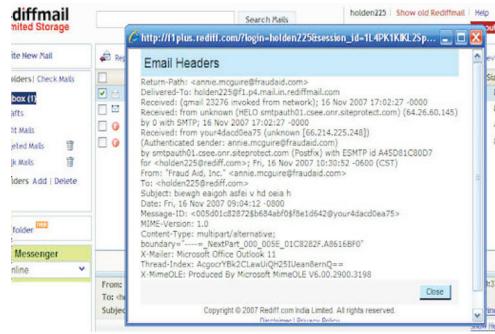
1. Click on “Options”.
2. Click on “Preferences.”
3. Choose “Other Hotmail Options” or “Additional Options/Mail Display Options.”
4. Click on “Message Headers.”
5. Click on “Advanced” or “Full” and then “OK.”
6. Click on “View Email Message Source.”



Rediffmail: Rediffmail is another free web-based email service, allowing individuals to send and receive mails in many Indian languages.

1. Open your Inbox (or other folder) and Right Click on the email
2. Click on Properties in the drop down menu

3. A new window will open displaying the Email Headers (See above figure). These are the Full Headers. Highlight and copy the Headers.



5.14.3. Cases where the Subject Mail Is Not Available

In cases where only email id is available and no other email transactions are possession, the I.O may use the services of the email tracking.

E-mail tracking is a method for monitoring the e-mail delivery to intended recipient. Most tracking technologies utilize some form of digitally time-stamped record to reveal the exact time and date that your e-mail was received or opened, as well the IP address of the recipient. E-mail tracking is useful when the sender wants to know if the intended recipient actually received the e-mail, or if they clicked the links. However, due to the nature of the technology, e-mail tracking cannot be considered an absolutely accurate indicator that a message was opened or read by the recipient.



www.readnotify.com



www.didtheyreadit.com

Steps:-

1. Register in any of the above tracking solutions website using an undercover email ID
2. Send a mail to the suspect
3. View the personal tracking page regularly to check for the read receipt along with the IP address, browser details, Operating systems etc.,

■ **IP location trace**

In computer networking, IP addresses do not correspond exactly to geographic locations. It is still theoretically possible, however, to determine the physical location of IP addresses in many cases. So-called Geo -location systems attempt to map IP addresses to geographic locations using large computer databases. This helps you to find out where the machine is physically located on the Internet. However, in case of corporate systems, we can find the systems by checking with the system administrator as most of the network is mapped. To find out where an IP address is located, go to a Web site like <http://www.apnic.net> or <http://www.dnsstuff.com> or <http://ipgeolocation.nmonitoring.com>

Along with location, these Web sites also provides some basic information about the company/individual using that IP address, which may be a great clue in the investigation.

■ **BIOS time check of systems.** As discussed above, system time/time zone can be changed by any user of the computer system. However, the BIOS time which runs the mother board of any system cannot be changed easily. Hence, this time plays key/critical evidence in the cyber crimes.

To check the BIOS date/time, first remove the HDD from the machine. Then boot the machine. When the machine is starting up, press the appropriate key to enter into the BIOS. The appropriate key can be found by looking at the monitor when the computer is booting up. The display should say something like "Press F10 for Setup". For this case, press F10 while the computer is starting and then you will get into the BIOS. The key changes for different models of BIOS and different manufacturers, so you have to be sure to press the correct key. If you have removed the hard drive and other USB/CD from the computer, then pressing the wrong key while trying to enter BIOS should not change any information.

5.15. Gathering information from external agencies/companies

Various companies/Internet service providers (ISPs) are liable under various laws and regulations including ITAA 2008 to preserve and provide information to the law enforcement. The Investigating Officer can send Letter of Request to get this information from these agencies/providers. A list of contact information of these companies and nodal officers is provided in **Annexure 5-7**.

5.15.1 Availability of information and format from ISPs:

It is very important for Investigating Officer to understand what information/evidence relevant to the investigation is available with third-party companies/providers, which can be very useful and relevant to reconstruct the crime. Sample letter to third party, companies, and service providers is provided in **Annexure 5-8**. All the service providers enable queries by e-mail from pre-registered e-mail ids of the IOs and, such e-mail have to be from their official e-mail id. For example, a mail from CCPS@gmail.com will not be entertained for providing information for investigation purposes but, it has to be from CCPS@gov.in or CCPS@police.org kind of mail ids, which are the official ids.

Information from ISP (Internet Service Provider): ISP will typically provide the following information, based on a law enforcement request.

- User name
- Telephone number in case of DSL/CDMA/3G, and Dial up
- Personal details like name, e-mail ID, address, etc., mentioned in the CAF form
- Day-wise activity i.e., when and how long used, etc.
- Physical address of the IP address

Fig: ISP Subscription / Billing Details of the Customer

Fig: ISP Customer Information including Address

5.15.2. Information from e-mail service

- User name
- Details of all incoming and outgoing e-mails along with mails stored in Draft folder
- The IP address from where the e-mail ID is accessed.
- Registration details like IP address, date and time, other services availed, secondary e-mail ID etc
- User activity, i.e., date and time of logged in and time it is active, etc.

A typical reply from the e-mail service provider looks like the following,

Dear Sir,
Following are the details as required.

A/c No :- 220977
Customer Name :- Mrxxxxxxxxx
Customer Address :- kdjfklijdsklfjkd
e mail ID :-
Phone No :-

Following are the login details :

IP Addr	Start Date	Start Time	End Date	End Time
1xx.201.132.241	3/24/2010	23:44	3/25/2010	1:46
1xx.201.209.126	3/25/2010	8:43	3/25/2010	9:49
1xx.201.209.80	3/25/2010	19:59	3/26/2010	1:04
1xx.201.209.74	3/26/2010	21:43	3/27/2010	5:43
xx3.201.209.74	3/27/2010	5:44	3/27/2010	6:30
1x3.201.132.209	3/28/2010	10:17	3/28/2010	16:13
1xx.201.132.235	3/28/2010	19:23	3/28/2010	21:56

The e-mail and other service providers have law enforcement designated nodal officers, who coordinate the requests from Police. Service providers do have laid down policies, in compliance with local laws and, laws of the country in which they are registered. A general rule followed by service providers in furnishing information to the police (law enforcement authorities) is enclosed at **Annexure 5-9**.

5.15.3. Information from Mobile service providers

- Customer Acquisition Forms (CAF) Forms — Personal details like name, address, etc.
- Calling number, called number, time, type of call (ISD/STD/Local/SMS, etc.)
- Roaming to other cities, etc.
- Tower locations — Latitude and Longitude of the tower
- Tower data

5.15.4. Information from Social networking sites like facebook, Orkut etc

- User name
- Personal details updated in the profile
- The IP address from where the profile is accessed
- User activity, i.e., date and time of logged in and duration of the active sessions, etc.
- Friends and groups with which the user is associated, etc.
- E-mail IDs updated in the personal information.

5.14.5. Information from Financial institutions/Internet banking institutions

- Personal details updated in the profile of the account holder
- Transactional details
- CAF and other supporting documents submitted by the customer along with the introducer details
- IP address from where the transaction happened in case of Internet banking

5.15.6. Information from Web site domain/hosting providers:

- Registration details
- Access details
- FTP logs
- Payment details
- Technical/administrative/owner of the domain
- Details of Web site developer

5.15.7. Information from VoIP service providers

- Registration details

- Access details
- IP addresses
- Payment details
- Called/Calling numbers

The above information has to be certified by the third-party company/Providers under the Indian Evidence Act, 1872. A sample certification is enclosed in **Annexure 5-10.**

5.15.8. Analyzing and handling the external data

As discussed above, digital evidence are available from various sources, including system used as target, used as means, used as repository, and from various other third-party companies/agencies/ service providers. It is very critical for Investigating Officer to collect this information from various sources by chronological order to reconstruct the crime, as well as build the right evidence/witness.

The Investigating Officer is required to follow the procedure in collecting the external data under proper notice/request letter as per the Law to make the evidence admissible in the court of law.

5.16. Correlating the external data with lab findings

It is very important to correlate the external data above collected, the data IOs able to elicit using the above tools with the lab findings. This is a two-way correlation. We need to support the third-party information collected with the lab findings and at the same time, we should be able to support the lab findings with the additional evidence collected from the third party, as well as our own investigation findings. This way we can build the integrity of the case as well as fully reconstruct the crime.

Investigating Officer is advised to maintain his notes/case files organized so that the details requested and received along with further information gathered from analysis are properly matched and evidence is analyzed.

Hence, it is highly recommended that the IO should keep the plan of action/process plan till he collects all the evidence and prepares the charge sheet.

Chapter VI: Guidelines for Investigation of Offences

6.1. Case Scenarios

6.1.1. Preparation of Forged Counterfeits using Computers/Printers/Scanners

Background

Adarsh, an engineering college student, secured 75% in his final semester while one of his classmates Narayan failed in 3 subjects. Adarsh appeared for a job interview and was surprised to see Narayan appearing for the same interview. He was further surprised when his resume was rejected and Narayan was selected for the job.

Adarsh suspected that Narayan might have created counterfeit documents to secure the job. He approached the university along with few class mates and submitted his observations. The university conducted a syndicate meeting and inquired into the matter. Academic records obtained from the recruiting firm revealed that Narayan had submitted forged documents of the university. The university decided to take criminal action against Narayan and gave a written complaint to the jurisdictional police station.

Applicable Laws

- Section 464 IPC : Making a false document including a false electronic record.
- Section 465 IPC : Punishment for forgery
- Section 468 IPC : Forgery for the purpose of Cheating
- Section 471 IPC : Using as genuine a forged Document or electronic record
- Section 473 IPC : Making or possessing counterfeit seal etc

Information gathered

From Complainant: Attested copies of the counterfeit copies of the marks sheet, accused details and his contact information.

From recruiting company: Alleged forged documents which were submitted by Narayan for obtaining the job.

Investigation

The police obtained the mobile phone number used by the accused Narayan and found that the number was switched off. The investigating officer wrote a letter to the mobile phone service provider under section 91 CrPC to provide the following details:

- Customer Application Form
- Alternative mobile/landline number if any given at the time of subscription
- CDR details for the specified period including Cell tower details

After obtaining above details, the IO observed that there were no calls made from the number for the last few weeks. Meanwhile, the location of the last call was traced.

The IO asked Narayan's colleagues about his connection with the city from which the last call was made. One of his colleagues disclosed that in the said city Narayan's uncle was residing. The IO visited the city and found Narayan residing with his uncle. On interrogation, Narayan revealed that it was Akbar who printed the counterfeit marks sheet for him and was doing for many other students as well.

Search and Seizure of Computer / Digital Evidences

The investigating officer conducted a search at the residence of Akbar and found computers, scanners and printers which were used for creating false documents. The IO found Akbar working on a computer at the scene of offence and, was in the process of designing some fake marks sheets. The survey of the crime scene revealed, stationery, rubber stamps and seals of various universities. A number of SIM cards and mobile phones were also found at the scene of crime.

At the scene of crime, the IO made a visual survey of the digital equipment and found that one of the systems was switched on and a laptop was found in a switched off condition. He seized the computer system/printer/scanner with due care, as per the standard digital evidence gathering procedures, for switched on and switched off systems, after ascertaining the identity of the suspect systems, used for preparation of the counterfeit documents. As the IO did not have the technical expertise or support for doing onsite forensics, the equipment were seized, the panchanama was drawn and Digital Evidence Collection forms were filled up.

Forensic Analysis of Digital Evidences

Now, to establish that the seized computer contained the counterfeit marks sheet copy, the IO obtained permission from the competent court and sent them for the expert opinion from the Computer Forensics Laboratory along with sample documents and questionnaire. The requisition letter to the FSL contained all the background information and details needed by the FSL scientists to analyse the evidences. The forensic scientist analysed the seized media and found that the seized computers were used for preparation of the counterfeit marks sheets and degrees of various universities, including the forged marks sheet of Narayan. The forged documents and the printer along with ink were sent to FSL for forensic examination and expert opinion revealed that the forged documents were printed from the same printer found at Akbar's place.

Third Party Information

Supporting evidences such as Mobile Phone Call details, e-mail exchanges between Narayan with Akbar and also e-mails of Akbar with various prospective customers were obtained. The CDR analysis of the phone call records were linked with the accused persons and the actual counterfeiting.

Finalization of Case

The crime though was a traditional offence under IPC, imade use of the computer equipment to create forged documents and hence the IO needed good understanding of the digital evidences. Following best practices prescribed for digital evidence collection, the IO was able to prove the offence with evidence supported by expert opinion from FSL.

6.1.2. Phishing Frauds

Background

Raghavendra was working as assistant professor at a prestigious college and was doing his PhD and spent most of his time on internet browsing to acquire requisite information. While checking his email ID, he found new message with the subject line **"URGENT: ATTENTION REQUIRED - MESSAGE FROM XYZ BANK"**. On opening the mail, he found that the financial institution (bank), in which he was holding a savings bank account, had sent a communication as shown below:

To: raghavendra@abc.com
From: customercare@xyzbank
Subject: "URGENT ATTENTION REQUIRED- MESSAGE FROM ABC BANK"
Date & Time: 26th January 2011, 11:00 AM (IST)

Dear Valued customer,

For security purposes, your account has been randomly chosen for verification. To verify your account, we are asking you to provide us with all the data we are requesting. If you do not provide these details, then we may not be able to verify your identity and access to your account may be denied. Please click on the below link to get secure page
<http://www.xyzbank.com/verifyaccountinfomration.html>

Thanking you

Customer care,

XYZ Bank.

Upon reading the mail, the professor visited the hyperlink. He landed on a webpage purported to be of his bank. The website contained fields asking him to update his personal information including account number, password and transaction password. He duly updated the information without giving a second thought. He was under the impression that the message was genuinely from his bank. After some days, he was shocked to realize that an amount of Rs 68,000 was debited from his account for some online purchase. The professor lodged a criminal complaint with the local police station.

Applicable Sections of Law

66C and 66D of Information Technology (Amendment) Act, 2008 and Section 420 of IPC – Identity theft, cheating by impersonation using computer resources and cheating.

Issue to be kept in mind while registering FIR

After registration, the investigation has to be undertaken by an officer of the rank of Police Inspector or above (as per ITAA 2008).

Information gathered

From complainant: Self attested copies of the printout of phishing email along with full headers printed at the police station and soft copies of the same with date and time stamps. Details of the bank account of the victim.

From Bank:

- The account statement of the complainant, which included fraudulent transaction details.
- Transaction IP address of the fraudulent transaction.
- Details of the beneficiaries (company to which the amount was credited for the online purchase of the electronic gadgets) and, the delivery address of the electronic equipment.

From Website Hosting Company: Particulars of the persons responsible for hosting the phishing website.

Investigation

Upon receiving reply from the bank, the investigating officer observed that the accused had made purchase of electronic gadgets from an online store. The IO contacted the online store and issued them a notice to furnish details of the equipment purchased, including delivery address of the electronic goods. The investigation revealed that the address mentioned for the delivery of goods was fraudulent and the accused had collected the goods from the courier agency directly by showing some fake ids. The fraudulently purchased electronic gadgets included a laptop and a mobile phone. The IO obtained IMEI number of the gadget. The IMEI number is unique and captured by all mobile service providers. The IO wrote a letter to all the service providers to check whether the given IMEI number belonged to their network. One of the service providers replied that the said IMEI number was found on their network. Based on this information, the IO obtained further information from the Mobile Service Provider like

- CAF form
- Call details
- Alternative mobile number given at the time of availing the connection

The service provider gave all the details and the IO analyzed the call details and found that the user had made maximum number of calls to a particular number and investigations led him to the called person. The IO received full details of the user (accused) of the mobile phone, which was purchased using the defrauded funds and was finally confronted. The laptop was also in the possession of the accused and the same was recovered.

The laptop thus seized was sent to the FSL for identifying the origin of the phishing mail and fraudulent transaction. The IO gave keywords like raghavendra@abc.com, etc to the FSL to establish link between the victim and the accused. No useful information regarding the phishing mail or internet banking transaction(s) was available with the accused. However, interrogation revealed that the accused was a recruit (money mule) on behalf of an unknown gang. The accused was simply acting as a conduit to deliver fraudulently obtained goods and to transfer money to the account to his recruiter. However, in the said case, the recruit did not turn up to collect the goods for sometime. Efforts to trace the unknown recruiter, who used to frequent him for collecting the gadgets / money, was untraced, despite serious efforts.

Investigation

The Investigating officer checked the full headers of the phishing mail received by the complainant to trace the IP address of the origin of the phishing email. The IP address was traced to a location outside India. However, detailed investigations revealed that the IP address was spoofed and originated from a country which was notoriously lax in implementing cyber security laws. Hence, the investigation reached a dead end with respect to tracking the original host of the phishing website. Further, with the growing sophistication of phishing attacks, it is difficult to identify the real hosts of these websites. The IO duly notified the CERT-In and the concerned Bank to pull down the phishing website.

Finalization of the Case: The case was finalized arresting the intermediary and recovery of the gadgets procured using fraudulently compromised account.

6.1.3. Obscene Profile on a Social Networking Site

Priya was working as voice support at a well known BPO and was very friendly with her colleagues. Mahesh, one of her colleagues, was interested in her. But Priya's proximity to Lokesh (another colleague) irritated Mahesh who decided to take revenge on her.

Mahesh visited the profile of Priya on a social networking sites and downloaded her photographs. He also downloaded a free morphing tool and created a fake obscene picture with Priya's face. Using the morphed obscene photographs of Priya, Mahesh created a fake profile over social networking website and uploaded and sent friendship requests in Priya's genuine profile.

Priya's friends called over phone and expressed their unhappiness after seeing her profile. Priya was shocked after looking at the fake profile and lodged a complaint with the police.

Applicable Laws: Section 465, 469 of IPC (Forgery, Forgery for purposes of harming reputation) and Section 67 of IT Act (publication or transmission of obscene material in electronic form).

Pre-Case assessment: Issue to be kept in mind while registering the FIR: Investigation to be done by an officer of the rank of Police Inspector or above (in case of ITAA 2008).

Issues to be kept in mind while seeking / collection of information from complainant / accused / witnesses and service providers: The relevant date and timestamps, shall always be collected.

Information gathered

From complainant: Self attested copies of the printout of the fake profiles printed at the police station and soft copies of the offensive content with date and time stamps (self attested copies of the printout of the friendship requests received by Priya's friends and soft copies of the offensive content with date and time stamps

Obtaining 3rd party information from service providers

From Social Networking website company: Registration, Access details of the fake profile created by the accused. Details such as name, date of birth, IP address, email IDs given by the accused while creating the fake profile.

From Email Service Provider: Access details of the subject email ID.

From Internet Service Provider: Physical address of the IP address provided by the social networking company/ email service provider used by the accused to post offensive content.

Collection of Evidences from Accused / Scene of Offence

Upon collecting information about IP address from the internet service provider or based on local investigations about relevant scene of offence, the IO planned his actions for search / seizure as per legal provisions under Cr PC. At the suspected place of offence, the IO identified the computer used by the accused, the digital evidence was seized by following best practices as covered in this manual

Search & Seizure of digital evidence

- Do not take the assistance of the accused himself to switch on / log in to the system – prevent the chances of the accused tampering with the evidence.
- if the systems were to be previewed or assessed to take a decision on whether a system contains incriminating information or not, trained cyber crime investigators adept at using write protect devices or technical experts services have to be used. If in doubt, follow the recommended practices for seizure of digital evidences and pack the systems for later preview or examination.
- Please remember that, at the time of seizure of the digital evidence, the monitors of desktops kind of computers and keyboards / mouses do not contain digital evidences. Hence, their seizure is not needed, unless IO is searching for any fingerprints / DNA samples on them.
- Please follow the suggested best practices for seeking FSL examinations of digital evidences and obtain the reports, as this case involves expert opinion seeking from Cyber Forensic Expert.

CYBER FORENSICS ANALYSIS

Objectives for obtaining the opinion: To determine whether seized digital evidence from accused contained evidence regarding usage of the system for creating the offensive photographs of the complainant using morphing software. Ensure that all the details relevant are furnished along with the expert opinion request. Please see the FSL requisition form in the manual and, guidance given.

Chain of custody: please refer the attached form and, ensure that the chain of custody is scrupulously maintained. Considerations of the Cyber Forensics Expert while dealing with requests from Investigators.

Assessment: Forensic Expert reviewed the case that the IO requested for analysis. The search warrant provided legal authority to the IO and the forensic investigator, who provided all information pertaining to obscene photographs, access dates, ownership of the computer and the sample photograph of the complainant. Expert satisfied himself that the equipment needed for analysis was available in the forensic lab.

Acquisition: The hardware configuration was documented and a duplicate of the hard drive was created in a manner that protected and preserved the evidence. The CMOS information, including the time and date, was documented.

Examination: The directory and file structures, including file dates and times, were recorded. A file header search was conducted to locate all graphic images. The image files were reviewed and those files containing images of what appeared to be complainant were preserved. Shortcut files were recovered that pointed to files on USB drives with sexually explicit file name with complainant's name. The last accessed time and date of the files indicated the incriminating files were accessed 10 days before the hard disk was seized.

Documentation and Reporting: The investigator was given a report describing the findings of the examination. The forensic examination confirmed the role of accused but, also revealed usage of a USB memory stick for storing images. This memory stick was not known to the IO till this stage.

Finalization of the case

The IO briefed the jurisdictional court and, obtained search warrant for accused home for recovery of the USB memory stick used for storing of images. During the subsequent search, a couple of USB drives were discovered at the accused's house. IO used the expertise of the technical experts to preview the USB drives to assess that the said USB drives contained the offensive material (if no technical expertise is available, please pack the USB drives for sending them for examination by technical experts for preview or for a full Forensic examination of the USB). The drives revealed additional morphed obscene images of the complainant including images which was used by the accused to host the fake profile and report from forensic experts obtained.

The IO diligently worked along with technical experts

- To map the information from the social networking site company, ISP, e-mail service provider of the accused and, connected it to the victim profile and, the friend's requests received by the victim's friends.
- The accused was connected to the crime (as the accused took the defense that, his user name and systems were compromised and used by an unknown third person) through investigations and witnesses statements.
- Importantly, the IO has taken care to see that the time stamps on the evidences collected were in uniform format for comparison and collation purposes (GMT as a standard time zone stamp was used for comparison, as majority of the service providers were international companies).
- The seizure procedures and accessing of account information of the accused and, analysis of the inbox contents of the e-mail account of the accused was done in the presence of witnesses and was documented.
- All original hard disks / USB drives were forensically imaged and, the analysis of the evidences was done on the images of the evidences. The original evidences (hard disks / USB drives) were preserved in a sealed condition in appropriate packing material to avoid damaging of original exhibits. The chain of custody form for each of the exhibit was carefully documented and enclosed along with the exhibits that were submitted to the court, to establish the integrity of the evidence gathered / seized evidences from the accused.
- All the findings and evidences were connected and, charge sheet filed against the accused.

6.1.4. Data Theft

Background

Police arrested a celebrity who was accused in a drug trafficking case. The accused was brought to the police station after obtaining permission from the competent court for further interrogation. The police station housed a hitech interrogation

room comprising of all the latest gadgets. The interrogation proceedings were recorded on the CCTV installed in different places in the interrogation room.

The investigation agency was surprised to see the interrogation clippings in television news channels and video sharing websites. Police registered an FIR against unknown person who had stolen the CCTV clippings and shared with the media.

Applicable Laws: Section 66 read with section 43 of the ITA 2000 and Section 66(B) of ITAA2008

Pre-Case assessment:

Information collected from complainant: Since the case is registered by the police on suo motto, the IO had to collect all relevant details like the copy of the video clipping broadcasted by the media/internet. Original CCTV clippings for future comparison.

Obtaining 3rd party information from service providers:

From Television channel company: Letter requesting for the video files of the date and time of the telecast of the incriminating program comprising the broadcast of the subject CCTV clippings.

From video sharing website: IP address/email ID of the person who has uploaded the subject clippings

From Internet Service Provider: The Physical address of the IP address provided by the video sharing website company/ email service provider.

Search & Seizure of digital evidence: The IO seized the storage media which stored the CCTV clippings in the interrogation room and sent it for forensic analysis at the FSL. The IO had made a specific request to identify and report the details of the removable media inserted in the computer since its inception.

- Please follow the suggested best practices for seeking FSL examinations of digital evidences and obtain the reports, as this case involves expert opinion seeking from Cyber Forensic Expert.

CYBER FORENSICS ANALYSIS

Objectives for obtaining the opinion: To determine whether seized digital evidence contained evidence regarding the transfer of the video clipping from the seized media to any external media. Ensure that all the relevant details are furnished including chain of custody form and the Digital Evidence Collection Form (DEC).

Acquisition: The hardware configuration was documented and a duplicate of the hard drive was created in the FSL in a manner that protected and preserved the evidence. The CMOS information, including the time and date, was also documented.

Examination: The directory and file structures, including file dates and times, were recorded. A latest forensic tool was executed on the seized hard disk to give a report regarding usage of removable media. The report showed that an USB storage drive of company A, make bearing serial number xxxx76x88x was inserted on the previous day before the clippings were broadcast. Also the accessed time and date of the video files indicated that they were last accessed 18hours prior to the telecast.

Documentation and reporting: The investigator was given a report describing the findings of the examination. The forensic examination confirmed the role of accused but, also revealed usage of a USB memory stick for storing images.

Finalization of the case: After obtaining the forensic report from the FSL, the IO summoned all the personnel who had access to the interrogation room. No valid information was obtained by enquiring them. But, upon examining the log register which was maintained, it was found that Mr. X who belonged to the CCTV servicing company had made a log entry to check the computer system in agreement with the warranty offered at the initial stages. Based on the forensic reports, the IO went on to recover the USB storage device from the accused. The serial number and make of the USB storage drive matched with the one mentioned in the FSL report. On further interrogation, it came to notice that Mr.Y had received the said clippings and had uploaded them on to the website. Accused were arrested and chargesheet was filed.

6.1.5. Blocking of Websites

Background

A member of an allegedly notorious terrorist organization was shot dead by the police during encounter. His admirers/ supporters started staging protests on websites / blogs and carried out anti-Indian statements. The blogs also generated communal disharmony. There was a public outcry over such a blatant anti-Indian propaganda. The law enforcement agency and the government felt that continuation of the access to the website hosting anti-national contents will threaten national security and communal harmony.

Applicable Law: Section 69 A, empowers the competent authorities notified under ITAA 2008 to block public access of notified websites.

Power to issue directions for blocking public access to any information through computer resource

1. Where the Central Government or any of its officers, specially authorized by it in this behalf, is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states, or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of Sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public, or cause to be blocked for access by public any information generated, transmitted, received, stored, or hosted in any computer resource.
2. The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
3. The intermediary who fails to comply with the direction issued under Sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Information collected: The investigating officer saved all the web pages in the subject website by using a special application by offline browsing and saved it into a CD-ROM. The IO also took the printout of the web pages.

Process for Blocking Websites: Based on the above Government notification, the Police moved an application for the blocking of the websites and submitted to the Government of India through the State Home Department.

GSR 781(E) of Gazette of India notification dated 27th Oct, 2009 prescribes the rules and process to be followed for blocking of websites. The detailed notification can be accessed at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/ltrules301009.pdf.

6.1.6. Kidnapping of Minor Girl

Background

Manik lal filed a written complaint that his daughter who was studying in class 9th was missing since two days. She had gone missing after celebrating her 15th year birthday. He further stated in his complaint that Naveen, who was his neighbor's son, was also missing and suspected that Naveen might have kidnapped his daughter.

Applicable Laws: No applicable sections for "Missing Case" but, in case if there is suspicion that some known person might have kidnapped, in such cases section 363 of IPC is applicable.

Pre-Case Assessment:

Issues to be kept in mind: SHO of the police station can register the case under 363 IPC and the investigation should be carried out by an officer not below the rank of Police Inspector.

Information to be collected from the complainant:

1. Proof for Age-Date of Birth
2. Photograph of the missing person
3. Physical features
4. Languages known- to speak/write
5. Mobile phone number-if available
6. Email ID- if available

Investigation:

1. The IO sent a requisition letter to the mobile service provider under section 91 CrPC to provide the call details and tower locations details of the mobile phone used by the missing person
2. The call details thus obtained did not disclose any useful information because the mobile phone was switched off from the day the girl was missing and there were no entries found in the CDR.
3. The IO created an undercover email ID and sent a tracking mail to the missing girl's email ID that was shared by the complainant at the time of registering the complaint.
4. The tracking email was sent by using free tracking email service like www.ReadNotify.com or www.DidTheyReadIt.com
5. The tracking mail thus sent was opened by the user and notification was obtained in the undercover email id created by the IO
6. The notification page carried information like
 - a. IP address
 - b. Date and time of opening the mail
 - c. No. of time opened etc
7. The internet service provider was identified and a requisition letter was sent to provide the physical address details
8. The internet service provider provided the details
9. The IO made a visit to the address and found that the girl was residing with Naveen.
10. The IO arrested Naveen under the applicable sections
11. The IO recorded the statement of both the accused and victim and emphasized on reason for kidnapping in the statement and the conventional investigative procedures were followed.

6.1.7. Hacking using Key logger

Sandip was working as manager at a well known IT company. His company had implemented strong information security policy and so he was not allowed to carry mobile phone or browse internet in the office. Hence, Sandip used to visit cyber café located next to his office to do online banking and other personal transactions over internet.

One day, Sandip visited a Jeweller's showroom and made a purchase of some ornaments and offered his debit card to make payment for the purchase. The vendor swiped the card and found that sufficient balance was not available in the account. Sandip was surprised as his salary was credited the day before.

When contacted, the bank informed that an amount of Rs.85,000 was transferred from his account to some other account. Sandip decided to lodge a complaint with the police.

Applicable Sections of Law:

Section 66C, ITAA 2008: Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password, or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D, ITAA 2008: Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Information collected from complainant: attested copies of email/sms received from any source other than the legitimate bank. Bank statement (if available)

Information collected from financial institution:

1. Statement of the account of the complainant during the fraudulent activity period
2. Transaction IP address of the subject transaction
3. CAF form of the beneficiary account(in case if it is same bank)
4. Details of the beneficiary bank(name of bank, branch, account number etc.,)

Investigation

1. The Investigating officer wrote a letter to the beneficiary bank to provide the CAF form and other details.
2. A requisition letter was sent to freeze the beneficiary account which will prevent any further withdrawal but will not affect the deposition of money.
3. Letter to the internet service provider was sent to provide the physical address details of the IP address given by the bank (transaction IP address).
4. The IP address was traced to many cyber cafes and to the one located next to the complainant's office, also.
5. The IO visited the cyber cafés and found that the cyber café owners had not maintained proper log register for the visitors of the cyber café but, upon investigation based on the logs of the transaction received from the bank and the logs available on respective computers systems in the cyber café, the IO was able to identify the suspect. The cyber café owner did not maintain the complete records of the users (i.e. copy of I-Cards, name, Address, etc.) visiting the facility but had a CCTV installed. Based on the review of CCTV logs, the suspect was identified

6. The cyber café owner confirmed that the identified suspect (person who was captured in the CCTV during the fraudulent transactions) used to visit the cyber café very often. The IO instructed the cyber café owner to notify him, next time when the suspect visits the cyber café.
7. Few days later, the IO received a call from the cyber café owner and was told that the suspect person was browsing internet in his cyber café.
8. The IO rushed to cyber café and questioned the suspect, who confessed about fraudulent transaction.
9. On further interrogation, it was disclosed that the accused person used to visit many cybercafés in vicinity of IT companies and had installed the keylogger program (a keylogger is an application which is used to capture the user activity like key strokes on keyboard etc.,)
10. The accused used to install the key logger program every 4th week of month hoping to collect the credentials of the IT employees who visited the cybercafé to check their salary credit.
11. Using the captured data, he used to transfer funds.
12. The accused did not use any storage media to save the keystrokes, instead uploaded it into his email ID.
13. The CCTV clippings and the hard disk from the cyber café was seized and sent to the FSL for expert opinion about the following:
 - a. Identify the person in the CCTV clippings
 - b. Presence of the keylogger program in the seized hard disk
 - c. Email ID of the accused which was used to upload the key log file
 - d. Account number of the victims.

CYBER CAFÉ:

Cyber Cafés facilitate online communication. However, poorly regulated cyber cafes notoriously lax in implementing guidelines issued by the local police and authorities. As such, Government of India has proposed to bring in new rules under section 79 of the ITAA 2008. These rules may please be referred to at http://www.mit.gov.in/sites/upload_files/dit/files/guidelines4cybercafe0702_11.pdf.

6.2. Guidelines to prepare charge sheet

Inadequate skill in drafting the charge-sheet is one of the reasons which help the accused to get away with cybercrime committed by them. Many cases fail before the Courts of Law just because of the defective framing of charge-sheets. There are a number of incidents, where the IO has failed to file the charge sheet with all required information / documentation in cyber crimes and cases acquitted by courts of law.

Below are few guidelines for IO to include in the charge sheet.

- All the relevant information shared by the complainants during registering the FIR/course of investigation should be included in the charge sheet.
- Please make sure the sections mentioned in FIR are still applicable for the case OR it is advised to file a requisition to change of sections before the case including appropriate ITAA 2008 and other supportive IPC, special and local laws. (there are number of incidents, IO filing the charge sheet under wrong sections of IT Act)
- Make sure the search and seizure procedure along with Chain of custody and DEC form are included in the charge sheet.
- Make sure the nature of cybercrime and the necessary information / analysis requested from FSL or forensic examiner are incorporated properly in the charge sheet.
- Please provide the detailed information about the crime scene and the process IO followed to identify the systems used / affected in the crime.
- Please include all the technical persons who identified, produced and analyzed the digital in the case as witness.

- Please include the incidents occurred in the chronological order of time to establish the crime along with the findings.
- Time plays a very critical evidence in proving cyber crimes, please mention the time stamps in a chronological order
 - System Time
 - BIOS Time
 - Access Time
 - Log times
 - Physical Access Time etc

6.3. Tips to Preserve the Seized Digital Media

After filing the charge sheet another important task for IO is to preserve the digital media till the end of the case.

Please follow the below guidelines to preserve the digital evidence:

- Please keep the digital media always in an anti-static cover with all details and tag / barcode.
- Please create a separate inventory list for all the media seized with case number and other reference numbers (bar code)
- Please store in a dry and cool place.
- If possible, store in a good storage device which is fire proof and tamper proof.
- Please keep update the chain of custody, if the media is taken out for any reason.

Last but not the least, the digital evidence may look simple to acquire or keep, but maintaining its legal relevance is not an easy task; professionalism has to take charge. Though digital evidence is more involving compared to real or ‘hard’ evidence, the point remains that both have to be reliable and accurate for them to be legally relevant.

6.4. Tips to prepare for deposition of evidence in court

The Investigating Officer should prepare well to depose the evidence in the court of law like any other case. All the digital evidences will be presented as exhibits and introduced as evidence to establish the process used to identify, collect, preserve, transport, store, analyze, interpret, attribute, and/or reconstruct the information.

Re-constructing the scene of offence and the cyber crime with the sequence of actions by each system and user is very important in the deposition.

To depose the evidence, Investigating Officers are requested to prepare their notes in the below order.

- Complaint received
- Collected relevant information
- Crime Scene visit
- Evidence Identification
- Collection
- Preservation
- Transport to FSL
- Request for Analysis
- Interpret the reports received from FSL
- Reconstruct the case
- Prepared the charge sheet

Annexures

Annexure 1-1: Cyber Crime Units in India

Name of the Unit	Designation of the Officer in-charge & Address	Contact Numbers & E-mail	Jurisdiction
CBI			
Cyber Crime Investigation Cell	Superintendent of Police, Cyber Crime Investigation Cell, Central Bureau of Investigation, 5 th Floor, Block No:3, Lodhi Road, New Delhi 110003	011- 24361271 speou9del@cbi.gov.in	All Over India* * Jurisdiction is bound by consent of State Government. However, original jurisdiction in Union Territory of Delhi
Arunachal Pradesh			
Police HQ		arpolice@rediffmail.com	Entire State of Arunachal Pradesh
Assam			
CID HQ	Additional DGP, CID Ulubari, Guwahati - 781007	0361-2521618 ssp_cid@assampolice.com	Assam State
Andhra Pradesh			
Cyber Crime Police Station, Hyderabad City Police	ACP, Cyber Crime Police Station, Beside Control Room, Opp Kalanjali, Beside L.B. Stadium, Hyderabad	040- 27852040, cybercell_hyd@hyd.appolice. gov.in	Hyderabad City Commissionerate
Cyber Crime Police Station, Cyberabad City Police	Police Commissioner's Office Old Mumbai Road, Jayabheri Pine Valley, Gachibowli Hyderabad, Andhra Pradesh 500032	040-27854031 sho_cybercrime@cyb.appolice. gov.in	Cyberabad City Commissionerate
Cyber Crime Police Station, CID, Hyderabad	I/c Cyber Cell, 3rd Floor, Crimes Investigation Department, A C Guards, Hyderabad	040-23307256 cybercrimeps@cid.appolice.gov.in	Rest of Andhra Pradesh except Hyderabad and Cyberabad Commissionerates.
Bihar			
Cyber Crime Investigation Unit (CCIU),	Dy.S.P,Kotwali police station, Patna	9431818398 cciu-bih@nic.in	Bihar State
Gujarat			
State CID, Crime & Rly, Gujarat State	DIG, CID Crime, 4th Floor, Police Bhavan, Sector-18, Gandhinagar	079-23250798,079-23254931/32 cc-cid@gujarat.gov.in Office of the DIG CID Crime:	Gujarat State
Deputy Commissioner of Police, Crime	Gaikwad Haveli, Jamalpur, Ahmedabad	079-25330170 dcp-crime-ahd@gujarat.gov.in	Ahmedabad City
Haryana			
Cyber Crime and Technical Investigation Cell, Gurgaon	Old S.P. Office complex, Civil Lines, Gurgaon	Joint Commissioner of Police jtcp.ggn@hry.nic.in 0124-2329988 DCP Crime 0124-2322662 dcpcrimegrg@hry.nic.in	Haryana State
Himachal Pradesh			
CID HeadQuarters,	Dy.SPCID Head Quarter, Kusumpati, Shimla-9, Himachal Pradesh	+91-9418039449 soodbrijesh9@gmail.com	Entire State of Himachal Pradesh

Name of the Unit	Designation of the Officer in-charge & Address	Contact Numbers & E-mail	Jurisdiction
Jammu & Kashmir			
SSP, Crime	CPO complex, panjirthi, Jammu-180004	0191-2578901 sspcrmjmu-jk@nic.in	Entire State of Jammu and Kashmir
Jharkhand			
CID, Organized Crime	IG, CID, Rajarani Building, Doranda Ranchi, 834002	0651-2491532, 2444703, agupta@jharkhandpolice.gov.in	Jharkhand State
Karnataka			
Cyber Crime Police Station,	S.P, Cyber Crime police station, C.I.D Headquarters, Carlton House, # 1, Palace Road, Bangalore - 560 001	080-22094563 ccps@kar.nic.in	Entire State Of Karnataka
Kerala			
Cyber Crime Police Station	DySP, Cyber crime Police Station SCRB Building Pattom P.O. Trivandrum, Kerala	0471-2449090,2556179 09497990330 cyberps@keralapolice.gov.in	Trivandrum City**
Hi-Tech Crime Enquiry Cell	Police Head Quarters, Trivandrum	0471-2721547 hitechcell@keralapolice.gov.in	Dealing with Cyber Crime Petitions and Technical assistance to IOs.
Cyber Cell,	Sub-Inspector of Police, Office of the Inspector General of Police, Ernakulam Range, Ernakulam	0484 2382600, 94979760045 - Office no sicybercell@kochicitypolice.org, cybercellekmcity@keralapolice.gov.in	Kochi City
Manipur			
SP, CID Crime branch	SP, CID, Crime branch, Jail Road, 1st bat Manipur rifle campus, Imphal, Pin: 795001	0385-2451501 9436027465 cid-cb@man.nic.in	Manipur State
Madhya Pradesh			
State Cyber Police	IGP, Cyber Cell Police Radio Headquarters Campus, Bhadadhadaa Road, Bhopal MP	0755-2770248 mpcyberpolice@gmail.com www.mpcyberpolice.nic.in	Madhya Pradesh
Maharashtra			
Cyber Crime Investigation Cell, Pune City Police	Dy. Commissioner of Police, EOW & Cyber,Office of the Commissioner of Police, 2, Sadhu Vaswani Road, Camp, Pune - 411001	020-2612 3346 crimencyber.pune@nic.in	Pune City
Cyber Crime Police Station, Mumbai City	Assistant Commissioner of Police, CCPS, BKC Police Station Complex, Mumbai	022 - 26504008 cybercell.mumbai@mahapolice.gov.in	Mumbai City
Cyber Crime Cell, Thane City Police	Cyber Crime Investigation Cell, 3rd Floor, Opp Thane Police school, Near Kharkar Lane, Thane(w) - 400601	022-25429804 / 25424444, cp.thane.ccic@mahapolice.gov.in	Thane City
Cyber Crime Cell, Nagpur City	I/C Officer - DCP (EOW & Cyber), PSI, Cyber Crime Cell, Nagpur City,Crime Branch, New Administrative Building, 4th floor, Civil Lines, Nagpur - 440001	0712-2566766	Nagpur City

Name of the Unit	Designation of the Officer in-charge & Address	Contact Numbers & E-mail	Jurisdiction
Meghalaya			
SP, SCRB	SP, SCRB, Police Headquarters, Secretariat Hill, Shillong-793001, Meghalaya	09863064997 meghcld2002@yahoo.com scrb-meg@nic.in demanjyrrwa@yahoo.com	Meghalaya State
Orissa			
CID, Crime Branch	SP Crime Branch, CID Crime Branch office, Buxybazzar, Cuttack, Orissa Pin - 753001	09437450370 sp1cidcb.orpol@nic.in	Orissa State
Rajasthan			
Special Operations Group	Jhalana Mahal, Jagatpura Road, Malviya Nagar , Jaipur	splcrimejpr@gmail.com 01412759779	Rajasthan
Tamil Nadu			
Cyber Crime Cell, Chennai City	Commissioner office Campus Egmore, Chennai- 600008	cyberac@rediffmail.com 044-55498211	Chennai city
Cyber Crime Cell, CID, Chennai	No.3, SIDCO Electronic Complex, I Floor, Guindy, Chennai - 32	044-22502512 cbcbyer@nic.in	For Rest of Tamil Nadu
Tripura			
SP, CID	SP, CID, Arunthati nagar, Agartala-799003	0381-2376963 spcid-tri@nic.in	Tripura State
Uttar Pradesh			
Cyber Complaints Redressal cell	Agra Range 7, Kutchery Road, Baluganj, Agra - 232001 (UP), India	9410837559, digraga@up.nic.in, info@cybercellagra.com	Entire State of Uttar Pradesh
Uttarakhand			
Special Task force	DIG, STF, PHQ, 12 subhash road , Dehradun, Uttrakhand 248001	9897937917 9412370272 STF office : 0135-2640982 dgc-police-ua@nic.in	Uttrakhand State
West Bengal			
CID, , Cyber Crime, West Bengal	CID Cyber Crime Cell, Bhabani Bhaban, Alipur, Kolkata	033-24506163 occyber@cidwestbengal.gov.in,	Entire state of West Bengal Except Kolkata City
Kolkata Police, Cyber Crime Police Station	ACP, Cyber Crime Police Station, Lal Bazaar, Kolkata	033-22505120, 033-22141420 cyberps@kolkatapolice.gov.in	Kolkata City
North 24 Parganas Dist. Cyber Crime Cell	S.I Cyber Crime Cell, 1st Floor, of Bidhannagar North Police Station, Beside Tank No : 6, Saltlake, Kolkata-64	09836272121	North 24 Parganas Dist.
New Delhi			
Assistant Commissioner of Police, Cyber Crime	Economic Offenses Wing, Police Training School Complex Malviya Nagar, New Delhi	011-26515229 acp-cybercell-dl@nic.in	
Chandigarh			
Cyber Crime Cell, Chandigarh	Inspector of Police, Cyber Crime Cell, Crime Branch Office, Sector -11, Chandigarh	0172-2746280, 09872281713 - PI cybercrime-chd@nic.in	Chandigarh

Name of the Unit	Designation of the Officer in-charge & Address	Contact Numbers & E-mail	Jurisdiction

NOTE: THIS PAGE IS LEFT INTENTIONALLY BLANK TO UPDATE THE CONTACT DETAILS

Annexure 1-2: NASSCOM-DSCI CYBER LABS

K.Venkatesh Murthy

Program Manager- Cyber labs,
Data Security Council of India,
Cyber Crime Police Station,
No. 1, Carlton House, CID Headquarters,
Palace Road, Bangalore-560 001.

Phone: 080-22374726, email: venkatesh.murthy@dsci.in

KARNATAKA:

Bangalore Cyber Lab

Cyber Crime Police Station,
No. 1, Carlton House, CID Headquarters,
Palace Road, Bangalore-560 001.

Contact person: **Mr. Mahesh.R, Project Manager**,
Phone: 080-22374726.
Email: mahesh.r@dsci.in

MAHARASTRA:

Mumbai Cyber Lab,

Cyber Police Station, 1st Flr, BKC Police Station,
Bandra-Kurla Complex, Opp ICICI Office, BKC,
Bandra(E), Mumbai 51.
Contact person: **Mr.Chaitanya J Belsare, Project Manager**
Phone: 022-26540540
Email: chaitanya.belsare@dsci.in

Pune Cyber Lab,

Police Manoranjan Kendra,
Police Head Quarter, Shivajinagar
Pune-411005
Contact person: **Mr. Sandip P Gadiya, Project Manager**
Email: sandip.gadiya@dsci.in

Thane Cyber Lab,

Office of Commissioner of police,
Third floor ,Opposite Thane Police School,
Near Kharkar lane, Thane (W) – 400601
Contact person: **Mr.Chaitanya J Belsare, Project Manager**
Email: chaitanya.belsare@dsci.in

HARYANA:

Haryana Cyber Lab,

Multimedia Hub,
Haryana Police Academy,
Madhuban, Haryana-132037

Contact person: **Mr Abhishek Kumar, Project Manager**
Phone: 0184-2390601
Email: abhishek.kumar@dsci.in

TAMIL NADU:

Chennai Cyber Lab,

Tamilnadu Police Academy,
Kellambakkam Road, Vandalur
Chennai- 600 048.

Contact person: **Mr. Karthik R N, Project Manager**
Phone: 044-22752444
Email: karthik.r@dsci.in

ANDHRA PRADESH:

Hyderabad Cyber Lab,

Cyber Crime Police Station,
Crime Investigation Department, AC guards, Masab
Tank, Hyderabad.
Email: cyberlab@dsci.in

Annexure 2-1: Adjudicating officers under Section 46 of ITAA

Sl. No	State	Address	Tel / Fax
1	Andhra Pradesh	Principal Secretary, IT&C Department, Government of Andhra Pradesh, Room No.431/A, D-Block,3rd Floor, Secretariat, Hyderabad 500022	040-23456401(0), 040-23450041 (0) 040-23450103 (F)
2	Arunachal Pradesh	Commissioner (IT), Govt. of Arunachal Pradesh, Civil Secretariat, Itanagar - 791 111, Arunachal Pradesh	0360-2212390 (0), 0360-2290251 (F) Mob.: 9436040057
3	Assam	Comm. & Secretary IT, Govt. of Assam, Block D, 3 rd Floor, Assam Secretariat, Dispur, Guwahati - 781 006 Assam	0361-2237230 (T/F), 0361-2261607 (F) Mob.: 9435032706
4	Bihar	Principal Secretary, Information Technology Ground Floor, Technology Bhawan, Baily Road, Patna	0612-2545315 (0) 0612-2545316 (F)
5	Chhattisgarh	Special Secretary,Incharge Secretary, CM Secretariat, Mantralaya, Raipur - 492001, Chhattisgarh	0771-4080793 (0), 0771-2221304 (0) 0771-2221304 (F)
6	Goa	Secretary IT, New Secretariat Complex Porvorim, Bardez, Goa-403521	0832-2419407(0) Mob.:09422416609
7	Gujarat	Secretary IT, Govt. of Gujarat, Block -7, 5th Floor, New Sachivalaya Complex, Gandhinagar - 382010	079-23250321 (0), 079 23259999 (0) 079-23254504 (F), 079-23250325 (F)
8	Haryana	Financial Commissioner & Principal Secretary IT & Industries, R. No. 46, 9th Floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001, Haryana	0172-2740009 (0) 0172-2740009 (F)
9	Himachal Pradesh	Principal Secretary (IT), Address: Room No.A-532, Armsdale Building, HP Secretariat, Shimla-171002 (HP)	0177-2621586 (0), 0177-2880716 (0)
10	Jammu & Kashmir	Principal Secretary, Information Tech. Department, Government of Jammu & Kashmir	Jammu Office No's: 0191-2544636 (0) 0191-2566055 (F),0191-2434663 ® Srinagar Office No's: 0194-2452269 (F) 0194-2450523 (0), 0194-2472914 (R)
11	Jharkhand	Secretary IT, Room No.307, 3rd Floor, Project Building, Dhurwa, Ranchi - 834 001	0651-2400001(0), 0651-2245110 (0) 0651-2400956 (F), Mob.: 9431109828
12	Karnataka	Prn.Secretary IT, BT and S&T, 6th Floor, 5th Stage M.S.Building, Dr. B.R.Ambedkar Veedhi, Bangalore-560 001, Karnataka	080-22280562 (0), 080-22374314 (0) 080-22288340 (F),
		Prn Secretary to Government, Govt.of Karnataka, DPAR(e-Governance), Room No.106, 1st Floor, M.S.Building, Gate No.2, Bangalore -560001	080-22353953(0) 080-22259109(F)
13	Kerala	Secretary IT, ICT Campus, Vellayambalam Kerala Secretariat Govt. Of Kerala ,Trivandrum 695 033	0471-2327438 (T/F) Mob.: 9446028801
14	Madhya Pradesh	Secretary IT, Dept. of IT, Room No.533, Mantralaya, Bhopal 462 004	0755-2441062 (0), 0755-2441101 (F) Mob.: 09425020285
15	Maharashtra	Secretary IT, Room No. 514, Anex 5th Floor, Mantralaya, Mumbai-400 032, Maharashtra.	022-22026534 (0), 022-22815087 (F) Mob.: 09870015000
16	Manipur	Comm. and Secretary S&T and IT, Room No. 5, North Block, Manipur Secretariat, Imphal-795001, Manipur	0385-2450682 (T/F) Mob.: 9612157732
17	Meghalaya	Prn. Secretary IT, Govt. of Meghalaya, Main Secretariat Building , Shillong-793 001, Meghalaya	0364-2224221(0) Mob.: 9436709150
		Commissioner & Secretary IT, Department Govt. of Meghalaya, Room No. 315, Addl. Secretariat Building, Shillong - 793 001	0364 - 2226978 (0) 0364 - 2224201 - (Extn) 2401, Mob.: 9862011111
18	Mizoram	Secretary IT, Department of Information & Communication Technology, Mizoram.Civil Secretariat Annex I, Aizawl, Mizoram-796001.	0389-2328741 (0) 0389-2300138 (F)

Sl. No	State	Address	Tel / Fax
19	Nagaland	Secretary, Department of Information Technology & Communication, Nagaland Civil Secretariat, Kohima, Nagaland.	0370-2270253 (O) 0370-2270253 (F)
20	Orissa	Comm. & Secretary IT, Information Technology Dept. Orissa Computer Application Centre Building, Jayadev Vihar, Bhubaneswar-751001, Orissa	0674-2586584 (O), 0674-2588280 (O) 0674-2582842 (F)
21	Punjab	Principal Secretary , Room No. 714/7, Punjab Mini Sect., Sector 9, Chandigarh-09	0172-2741346 (T/F) Mob.: 98720-00616
22	Rajasthan	Room No. 2024, Main Bldg, Secretariat, Jaipur- 302005	0141-2227110 (O), 0141-2227503(F) 0141-2709144 ®, Mob.: 9414181018
23	Sikkim	Top Floor, Annexe-I Secretariat, Kazi Road, Gangtok-737101 Sikkim	03592-202691(0), 03592-207426 (F) Mob:9434044774
24	Tamil Nadu	Secretary to the Government, IT Dept. Secretariat, Chennai - 600 009	044-25670783 (T/F) 044-25670505 (F), 044-26535060 (R)
25	Tripura	Principal Secretary, Room No. 303 Block- 7, New Secretariat Building, Capital Complex, Agartala 799006	0381-2412463 (T/F) Mob.: 9436541983
26	Uttar Pradesh	Prn. Secretary IT, 1st Floor, Bapu Bhawan, Lucknow- 226 001, Uttar Pradesh	0522-2238122 (O)
27	Uttarakhand	Secretary IT, Govt. of Uttarakhand, Uttaranchal Secretariat, Subash Road, Dehradun- 248001, Uttarakhand	0135-2712066 (T) 0135-2714106 (F)
28	West Bengal	Secretary IT, Govt. of WB, Dept. of IT, Advantage Bengal Building, 4, Camac Street, 7 th Floor, Kolkata 700 016	033-22821946 (O) 033-22876740 (F) Mob: 9903031997

Union Territories

Sl. No	Union Territory	Address	Tel / Fax
1	Andaman & Nicobar	Secretary IT, Andaman & Nicobar Admn. Secretariat, Port Blair-744101	03192-233227 (O), 03192-232236 (F) Mob.: 943428002
2	Chandigarh	Finance Secretary-cum-Secretary IT, UT Secretariat, Sector 9, Chandigarh UT	0172-2740017 (O), 0172-2740070 (F) Mob.: 9814073164
3	Dadra & Nagar Haveli	Finance Secretary, 1st Floor, Secretariat, 66 KV Road, Amla,SILVASSA - 396 230, Dadra & Nagar Haveli UT	0260-2642777 (O), 0260-2642303 (F)
4	Daman & Diu	Finance Secretary, Secretariat, Fort Area, Moti Daman, DAMAN-396220 (UT of Daman & Diu)	011-23392254 (O), 011-23392396 (F)
5	Delhi	Secretary IT, Deptt. of IT, Room No. 902, 9th Level, B Wing, Delhi Secretariat, IP Estate, New Delhi- 110002	04896-263950 (O), 04896-262307 (F) Mob: 9868050930
6	Lakshadweep	Secretary IT, Department of IT, Secretariat, UT of Lakshadweep,Kavarati - 682 555	04896-263950 (O), 04896-262307 (F) Mob.: 9446083950
		Director IT, Department of IT, UT of Lakshadweep, Kavaratti - 682 555, Lakshadweep UT	04896-262510 (O), 04896-262511 (F) Mob.: 9447063728
7	Puducherry	Special Secretary Transport & IT, Govt. of Puducherry, Gobert Avenue, Chief Secretariat, Puducherry - 605 001	0413-2280130 (O)

Annexure 2-2: Basics of Digital Devices, Networks, Internet and Mobile Phones

Computer is basically an electronic device that is used for processing the data which is given as input and provides that processed data as an output. Speed, accuracy, reliability, diligence, and multitasking are some of the important aspects of a computer. A typical computer consists of both hardware and software components. Every computer has input devices like keyboards, mouse, etc., and any instructions, and commands can be given as inputs. The Central Processing Unit (CPU) is the brain of the computer where the data inputs are processed. It consists of a microprocessor where actual calculations are done and the output is given to the user through output devices like monitor, printers, speakers, etc.

What constitutes evidence?

Any data that is contained in a computer or a computer resource like e mails, documents, spreadsheets, text files, log files, registry entries, images/Pictures, audio, video files, text, chat messages, databases, source code, programs, etc., that is likely to have some relevance to the incident or case.

Types of Digital Devices and their Use

Desktops: The most common computer used in today's world is the desktop computers which were specially built for personal use is it at home or work. Most desktop computers are equipped with two primary hardware solutions — the monitor and a casing inside which the CPU is housed, the motherboard, the graphic card, storage devices, buses, power supply, and so on. A desktop computer is also equipped with a keyboard and mouse which are connector to their appropriate ports at the back of the casing.



Laptop: A Laptop computer which is also known as notebook computer is a smaller computer that can be carried. It has all the components like monitor, keyboard, mouse, and speakers, etc., in to a single unit. It is powered through an AC adapter and can store the energy in a rechargeable battery. The battery can store energy up to three to five hours depending on computer usage, configuration, and power management settings.



Server: A server is a computer which can provide services to a group of computers either inside an organization or to public users across Internet. Many servers have dedicated functionality, such as Web servers, file servers, print servers, database servers, mail servers, etc. Sometimes, they have different kinds of hardware and operating systems that makes them efficient in providing services. In a hardware sense, It can range anywhere between a simple laptop to a huge, towering workstation, which has several drives and cables connected to it.



Digital Storage Devices

Hard drives: Hard drives or hard disks are the main storage devices that are used in the computer to store the data. The data stored in hard drive is nonvolatile and will remain there, unless it is deleted by the user. These are the magnetic storage devices on to which data is written and read by read/write heads on the magnetic platters. Hard drives come in different varieties based on their speed, size, and connecting types. The common types of hard drives that are usually encountered are 1) IDE, 2) SATA, 3) SCSI, and 4) ZIF/SSD.

IDE hard drive: IDE hard drives, also known as Parallel ATA (PATA) were the most commonly used hard drives, but now are being replaced by SATA drives. An IDE hard drive uses 40 or 80 pin flat ribbon cables to transfer data. IDE hard drive has smaller pin-like attachments called jumpers which will decide whether the hard drive is connected as a master or slave to the computer.



SATA hard drive: SATA drives are similar in mechanism to that of IDE drive, but the connecting interface is different. The data transfer is done serially and is faster than IDE drives.



SCSI hard drives: SCSI stands for sSmall Computer System Interface. These hard drives were widely used before and are still being used in servers and RAID systems, and can be connected as arrays both internally and externally.



ZIF Drives: ZIF stands for zero insertion force. That means that connectors to these drives do not need any force to insert and extract from the sockets or other connections. This kind of storage devices are now being used in several laptop computers.



CDS ,DVDS and Blu-ray: CDs and DVDs are optical storage devices that are used to store data like audio, video, and several other types of files. CDs can be written once (CD-R-Recordable) or data can be erased and re-written (CD-RW-Rewritable). The maximum size of a CD is 800 Megabytes and that of a DVD is 9.0 Gigabytes. They are available in the form of mini CDs

and mini DVDs also. DVDs come in single- and dual-layer varieties.



Blu-ray is the name of a new optical disc format developed to enable recording, rewriting and playback of high-definition video (HD), as well as storing large amounts of data. The format offers more than five times the storage capacity of traditional DVDs and can hold up to 25GB on a single-layer disc and 50GB on a dual-layer disc. This extra capacity combined with the use of advanced video and audio codecs will offer consumers an unprecedented HD experience.



Floppy disks: Floppy disks are magnetic storage media that are encased in a rectangular plastic case. They usually come in three different sizes 8 inches, 5 1/2 inches, and 3 1/2 inches. 8 and 5 1/2 inches have become obsolete now. Floppy disks have a write-protection option or read-only option.



Flash drives: Flash drives are generally flash memory data storage devices that are integrated with a USB interface. These are removable and portable media which are rewritable and are much smaller in size than the typical floppy disk drive. Storage capacities of these USB flash drives can be up to 256 Gigabytes. USB flash drives are smaller, faster, and more durable.



Memory sticks: Memory stick is removable media based on flash memory.. The capacities of the memory sticks can be from 128 MB to 32 GB.These memory cards are generally used in mobile phones, digital cameras, Camcorders/video recorders, etc.



Tape backup: Tape drive is a data storage device with a magnetic tape on to which data is written and read from. Tape drives are usually used to take regular backups for large servers periodically. The data backup can be restored on the computer for analysis. Backups are either done manually or can be automated with the use of the software. Tape drives come with several types of interfaces (SCSI,SATA,USB, and Fiber Channel) and capacities up to several Gigabytes. Liner type open (LTO) is the most commonly used tape drive.



NAS: Network attached storage (NAS) is a storage system that allows computers on network to share large amounts of data across high-speed Local Area Network (LAN) networks. NAS can store data in the files such as e-mail boxes, Web content, and remote system backups. It is usually composed of an array of hard drives that are connected to a computer system.



Printers and Scanners: Printers and scanners usually have cache memory which temporarily lines up (spools) the files or pages that are currently being printed. Once switched off, that memory is usually lost. Some large printers and scanners have inbuilt hard drives, which may contain the details of the documents printed or copied using these devices.



HAND-HELD DEVICES

Pagers: A Pager is a device that is used for short messages. Pagers can be one way, which can send or receive messages with limited digits or they can be alphanumeric, two-way pagers which can even send and receive messages etc.



Personal Digital Assistant (PDA): PDAs are Palm top computers that functions as personal information manager or organizer which can be used to store several types of personal data, browse Internet, etc. PDAs also have expandable memory and wireless Internet connectivity. Modern PDAs have Bluetooth facility to connect to keyboards, headset, GPS receivers, etc.



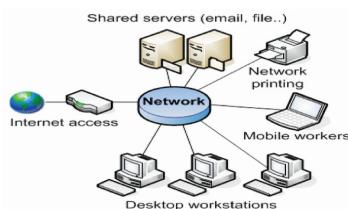
Ipads: Ipads are tablet computers manufactured by apple computers. It has same operating system as iphone and ipod (iOS). IPad comes in 16, 32, and 64 GB varieties. This can be used as a typical computer to store data, browse Internet, make phone calls, Play games, read e-books, etc.



Electronic readers/e-readers: Electronic readers are devices that are used to store, download, and read e-books and play games. These devices are wireless Internet enabled and come in different storage capacities.



Network



Hub: In computer networking, a Hub is a small device that joins multiple computers together. Ethernet hubs vary in the speed they support.

Switch: A network switch is a hardware device that joins multiple computers within one LAN. Network switches not only allows network packets from them, but also examines or inspects them to determine their source and destination. Different models of network switches support different number of connected devices.

Router: In Network environment, a Router is a physical device that joins multiple wired or wireless networks together. Routers are usually located at gateways. It intercepts the data packets and decides where the signals have to go. A Router can have different interface connections for different types of physical networks.

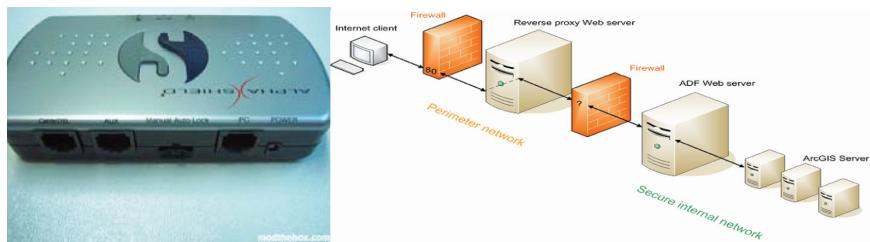


RAID (Redundant Array of Inexpensive Disks)



RAID (Redundant Array of Inexpensive Disks) is method of storing the same data in different places (thus, redundantly) on several **hard disks**. By placing data on multiple disks, **I/O** (input/output) operations can overlap in a balanced way, improving performance. Since multiple disks increases the mean time between failures (**MTBF**), storing data redundantly also increases **fault tolerance**.

Firewall: A Firewall in a computer system or network is a device that allows only authorized traffic (data) into or out of a computer or a computer network. It continuously inspects the data packets that are going in and out of a computer network and blocks any unauthorized and malicious traffic and serves as a security mechanism. A Firewall can be hardware, software, or a combination of both. They can be installed at several levels and are of several types like packet filter, Application gateway, Circuit-level gateway, Proxy server, etc.



Intrusion Detection system/Intrusion Prevention system (IDS and IPS): An Intrusion detection system is a security mechanism that monitors all the incoming and outgoing traffic of computer network and identifies suspicious files, programs, and patterns in the traffic. It also detects the misuse and errors in using certain computer resources like software. IDS can also watch the attacks that originate from within the system or network. Intrusion Prevention systems on the other hand, not only detects threats and attacks in the network, but also prevents or blocks them. It usually sends the alarm, resets the connections, drops the malicious data packet, or blocks the attacker's IP address.

Telephones: These communication devices are also sometimes the best source of digital evidence. Desk phones may contain information like last dialed numbers, frequently dialed numbers, and voicemail messages that are left by callers and alternative phone numbers in case of any call diversions, etc.



Answering machines: Answering machines are devices that are used with desk telephones. These devices will play a message to the caller when the call cannot be answered and then the caller can leave a message which will be recorded in the answering machine. All the messages recorded in such a way can be played later directly from the machine itself.



Fax Machines: Fax which is a short form for facsimile, is any document sent over a telephone line. The contents of the document are scanned and sent over the telephone line. It is received by the recipient's fax machine and gets printed. Nowadays, wireless fax machines are also available. In many corporate environments, fax servers are installed, which can store the incoming fax messages electronically and sends them through e-mail to the users or prints them on the paper.



Mobile phones: Phones that can be easily carried with the person and works on Cellular network signals. Mobile phones are used to make phone calls, send text messages, voice and picture/video messages (Multimedia messages — MMS), and take pictures and videos, etc. Mobile Phones can be GSM (Global system for mobile communication) or Code Division Multiple Access (CDMA). A GSM mobile phone usually has a SIM card specific to the service provider. Time Division Multiple Access (TDMA) is another standard of mobile phones.



Smart phones: Smart phones are advanced type of mobile phones and offers services like high-speed Internet, advanced computing, and connectivity. They run on complete operating system software like typical computers and can be considered as a pocket computer. They provide services like Internet, e-mail, Wi-Fi, and WLAN connectivity. GPS navigation can be used as a Personal Digital assistant apart from using it as mobile phone for making calls and sending messages.



MISCELLANEOUS ELECTRONIC ITEMS

Digital cameras: Digital cameras are cameras that can take pictures and videos and records them digitally on to the memory present in them. They are available in wide range of sizes and capabilities like resolution, zooming, editing features, etc. They also support expandable memory by using multimedia cards like SD cards and CF cards, and more advance cameras have hard drives that can store pictures and videos. These cameras can be directly connected to computer to transfer the contents.



Camcorders: Camcorders are the digital video recorders used to capture video footages and record them digitally on to CDs, Cassettes, Multimedia cards, hard drives, etc. Camcorders like digital cameras are available in a wide variety based on their sizes, lens resolutions, etc.



Photocopiers: A Photocopier is a machine that can reproduce a document and make multiple copies of it quickly. It uses a technology called xerography in making the replicas of the documents. Advanced photocopiers have features like sending the photocopy electronically to the e-mail and storing them in the hard drives when large numbers of documents are to be copied.



Global positioning devices: Global positioning system is a Satellite-based navigation system which provides the exact location and time information anywhere on the earth with the help of the GPS-enabled devices or GPS devices. GPS devices have receivers for GPS satellite and provide information, such as location, directions, traffic conditions, and nearby facilities like restaurants, fuel stations, etc., through maps and text and voice.



Digital watches: Digital watches are instruments that show time in digital format and also have other facilities like compass, temperature sensors, music players, and in some embedded cameras also. Some advanced digital watches also have USB data connectivity to store and transfer data.



Basics of Networks and Internet

Basics of Internet Protocol (IP)

Internet Protocol is a set of rules used for transmitting data packets across the Internet. It is the protocol that runs behind the Internet along with Transmission control protocol (TCP) and is responsible for addressing the host computers on the network and transmits the data packets from source host to destination host. A host is either a computer or a group of computers on network. The first version of IP was IP4 which is still in use and being replaced by IP version 6(IPv6). IP uses a unique addressing system called IP addressing to all the computers that are connected to a network. An IP address is a unique identifier that distinguishes one computer to another in a network. The IP address is 32 bit numeric address written as four sets of numbers separated by a dot (e.g., 10.1.1.255). Each set of number can be 0 to 255. An IP address consists of two parts, one part identifies the network and the second part identifies the host on the network. The class of an IP address determines which part is network address and which part belongs to host address.

Public and Private IP

Three groups of IP addresses are specifically reserved for use by any private network and are not seen on the public Internet. If you see these IP addresses as the suspect address, then do not try to find out from the ISP about them. Information for these IP addresses comes from the owner of the network. The ranges are:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

All other IP addresses can be seen on the Internet and are called public IP address.

IP Version 4 Vs Version 6

As indicated by the number 4, IPV4 is the fourth generation of Internet addresses. It is a simple protocol based on Ethernet and other switching networks.

The Internet Protocol Version 6 (IPv6) on the other hand is designed as the successor of the Internet Protocol version 4 (IPv4). The IPv6 is also an Internet Layer protocol that works on Ethernet and other packet switching networks. However, it was designed primarily to address the issues of the exhaustion of the number of unique IP addresses that the Internet Protocol version 4 (IPv4) could offer.

The **Internet Protocol Version 6 (IPv6)** uses a **128-bit address**, whereas **IPv4 uses only 32 bits**. Thus, it can be easily computed that the Internet Protocol Version 6 (IPv6) supports 2¹²⁸ (about 3.4×10³⁸) addresses. This expansion will provide a great deal of leeway in providing unique IP addresses to the rapidly booming number of internet devices.

Another upgrade provided by the Internet Protocol Version 6 (IPv6) over the Internet Protocol Version 4 (Ipv4) is the **ability to eliminate the need for network address translation (NAT)**.

Also, a particularly noteworthy difference between IPv6 and IPv4 is that there is a simplification of the aspects of address assignment (stateless address auto-configuration) and network renumbering (prefix and router announcements). This makes it much easier to switch between various internet service providers. Also, there has been a standardization of the Internet Protocol Version 6 (IPv6) subnet size. This has enabled automatic formatting of the host identifier from media addressing information (MAC address).

Computer Networks

Description: A computer network consists of two or more computers linked by data cables or by wireless connections that share or are capable of sharing resources and data. A computer network often includes printers, other peripheral devices, and data routing devices such as hubs, switches, and routers.

OR

A computer network, often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources. Networks may be classified according to a wide variety of characteristics.

Computer networks can be used for several purposes:

- Facilitating communications. Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.
- Sharing hardware. In a networked environment, each computer on a network may access and use hardware resources on the network, such as printing a document on a shared network printer.
- Sharing files, data, and information. In a network environment, authorized user may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks.
- Sharing software. Users connected to a network may run application programs on remote computers.
- Information preservation.
- Security.
- Sharing software. Users connected to a network may run application programs on remote computers.
- Information preservation.

A Computer Network and Its Requirements

A network is a group of interconnected systems that share services and interact through a communications link. So, for a network to exist there must be two or more individual systems with something to share, like data. And, in order for these individual systems to share, they must be connected through some type of physical pathway or transmission medium. Now, if data is being sent over the transmission medium, all these individual systems must follow a set of common communication rules in order for the data to arrive at its intended destination or for the systems to properly understand each other in order to receive the data. These rules that govern how the systems communicate are known as protocols.

Now, just having a transmission pathway should not suggest that communication is automatic, because in order for two systems to communicate, they must be able to understand each other. Data cannot simply be exchanged. The data that is received must be understood. So, the true goal of computer networking is not just to exchange data, but also to be able to understand and use the data that has been received.

So, to quickly summarize a network, there are four things that must be present:

- two or more individual systems
- something to share (ex: data)
- a physical pathway or transmission medium
- rules of communication or protocols

Network classification

The following list presents categories used for classifying networks.

Connection method: Computer networks can be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as optical fiber, Ethernet or wireless LAN

Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges, or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium. Technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.

Wired technologies: Twisted pair wire is the most widely used medium for telecommunication. Twisted-pair wires are ordinary telephone wires which consist of two insulated copper wires twisted into pairs and are used for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 100 million bits per second.

Coaxial cable is widely used for cable television systems, office buildings, and other worksites for local area networks. The cables consist of copper or aluminum wire wrapped with insulating layer typically of a flexible material with a high dielectric constant, all of which are surrounded by a conductive layer. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second.

Optical fiber cable consists of one or more filaments of glass fiber wrapped in protective layers. It transmits light which can travel over extended distances. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed may reach trillions of bits per second. The transmission speed of fiber optics is hundreds of times faster than for coaxial cables and thousands of times faster than a twisted-pair wire.

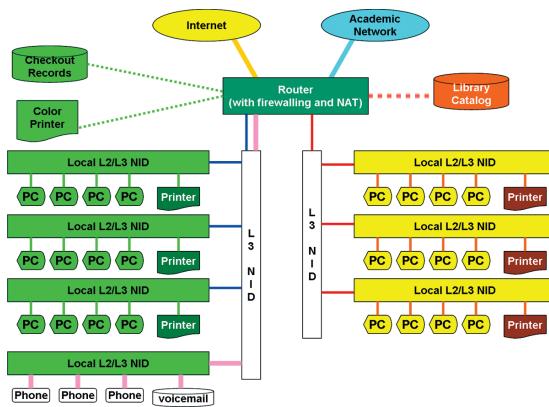
Wireless LANs: Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area.

Network topology: Computer networks may be classified according to the network topology upon which the network is based, such as bus network, star network, ring network, mesh network. Network topology is the coordination by which devices in the network are arranged in their logical relations to one another, independent of physical arrangement. Even if networked computers are physically placed in a linear arrangement and are connected to a hub, the network has a star topology, rather than a bus topology. In this regard the visual and operational characteristics of a network are distinct. Networks may be classified based on the method of data used to convey the data, these include digital and analog networks.

Types of networks based on physical scope

Common types of computer networks may be identified by their scale.

Local area network: A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines). Typical library network, in a branching tree topology and controlled access to resources



All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 mbips Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called “layer 3 switches” because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks’ customer access routers.

The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10 gbps. This is the data transfer rate. IEEE has projects investigating the standardization of 40 and 100 gbps.

Personal area network: A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

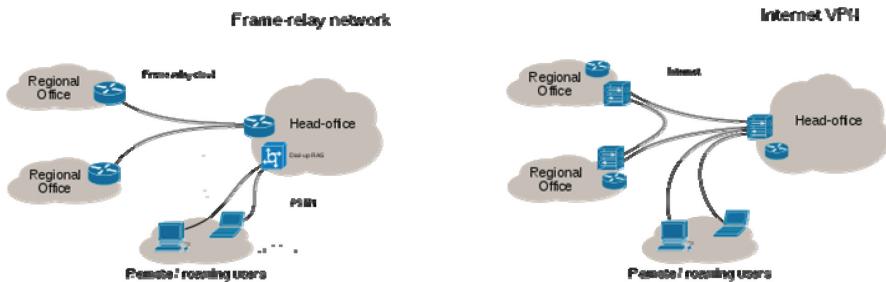
Home area network: A home area network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a CATV or Digital Subscriber Line (DSL) provider. It can also be referred as an office area network (OAN).

Wide area network: A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media

such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

Campus network: A campus network is a computer network made up of an interconnection of local area networks (LAN's) within a limited geographical area. The networking equipments (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.). In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including; academic departments, the university library and student residence halls.

Metropolitan area network: A Metropolitan area network is a large computer network that usually spans a city or a large campus.



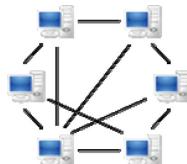
Sample EPN made of Frame relay WAN connections and dialup remote access. Sample VPN used to interconnect 3 offices and remote users

Enterprise private network: An enterprise private network is a network build by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

Virtual private network: A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply, and clients consume.



Peer-to-peer systems present a unique problem as many of the illegal software, TV shows and movies are downloaded using these technologies. It was first popularized by Napster and now we have other systems such as Morpheus, Kazaa, Limewire, Gnutella and one of the biggest systems, BitTorrent is one of the most used peer-to-peer file sharing protocol used for distributing large amounts of data. BitTorrent is one of the most common protocols for transferring large files, and it has been estimated that it accounted for roughly 27% to 55% of all Internet traffic.

- **Client-Server Architecture:** The client-server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server machine is a host that is running one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests

The client-server characteristic describes the relationship of cooperating programs in an application. The server component provides a function or service to one or many clients, which initiate requests for such services.

Functions such as email exchange, web access and database access, are built on the client-server model. Users accessing banking services from their computer use a web browser client to send a request to a web server at a bank. That program may in turn forward the request to its own database client program that sends a request to a database server at another bank computer to retrieve the account information. The balance is returned to the bank database client, which in turn serves it back to the web browser client displaying the results to the user. The client-server model has become one of the central ideas of network computing. Many business applications being written today use the client-server model.

Specific types of clients include web browsers, email clients, and online chat clients.

Specific types of servers include web servers, ftp servers, application servers, database servers, name servers, mail servers, file servers, print servers, and terminal servers.

Off Site Storage: It adopts the idea of storing the critical data out of the location of the office. This can be accomplished by either sending the data physically by removable storage media (CDROM etc) or can be sent electronically by using the Remote services. This will help to get the computer systems reloaded with the backup in case of any damage/error to the system.

Data Centre: It is the place where computer systems and associated components, such as telecommunications and storage systems are located. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.



Mail Server: A mail server is an application that receives incoming e-mail from local users and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Ex-

change, qmail, Exim and sendmail are among the more common mail server programs.

The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an e-mail message, your e-mail program, such as Outlook or Eudora, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

Top Level Domains: A top-level domain (TLD) is one of the domains at the highest level in the hierarchical Domain Name System of the Internet. The top-level domain names are installed in the root zone of the name space. For all domains in lower levels, it is the last part of the domain name, that is, the last label of a fully qualified domain name. For example, in the domain name www.example.com, the top-level domain is com, or COM, as domain names are not case-sensitive.

.com	commercial	This is an open TLD; any person or entity is permitted to register. Originally intended for for-profit business entities. However, lots of others including certain police organizations are using the .com domain.
.edu	Educational	For Educational institutions
.gov	Government	For Government
.in	Geographical	For India

For complete listing of TLDs, please visit <http://www.icann.org>

Internetwork: An internetwork is the connection of two or more private computer networks via a common routing technology (OSI Layer 3) using routers. The Internet is an aggregation of many internetworks; hence its name was shortened to Internet.

Internet: The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW). Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Corporation for Assigned Names and Numbers (ICANN) and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

WiMAX: WiMAX is an IP based, wireless broadband access technology that provides performance similar to Wi-Fi networks. WiMAX is also an acronym meaning "Worldwide Interoperability for Microwave Access (WiMAX). WiMAX finds its application in the following:

- Broadband internet connectivity across the cities
- Wireless internet replacing cables.
- Providing data, telecommunications (VoIP) and IPTV services.

Domain Name System or Service (DNS): Domain name system is an Internet facility or service that converts the domain names like www.abc.com in to an IP address like 1.0.0.255 because the Internet really works on IP addressing system. Every time a domain name which is alphabetic is entered in the Web browser, a DNS service must translate the name into

corresponding IP address. The DNS assigns domain names to a group of Internet resources and users. The DNS servers are a part of very big database on the Internet that has the information of billions of IP addresses and domain names currently in use.

Uniform Resource Locator (URL): The URL is an identifier that informs the user where on the Internet a resource is available and how to access it. Often URL appears as a link by clicking which it takes the user to the location on the Internet. It can also be copied and pasted in the Web browser. The first part of the URL address is the protocol identifier that indicates what protocol is in use (http and ftp) and the second part is the resource name which specifies the IP address or the domain name where the resource is located. The protocol identifier and resource name are separated by a colon and two forward slashes.

Web site basics

Web site: A Web site is a collection of Web pages (html pages), pictures, videos, and text which can be accessed through the Internet when the content is hosted on the Web server. Usually, all the information related to a company/organization/individual is posted on the Web site so that it can be accessed easily from anywhere in the world through Internet.

Nowadays, all the commercial transactions like online banking, shopping (e-commerce), etc., are being done through Web sites. Governments are posting important information related to several departments, government orders, notifications, gazettes, recruitment results, facilitating online submissions of several petitions, application forms, etc., Web sites are also a good source of knowledge where people can learn lot of new subjects, attend online courses, and get certifications and degrees. Lastly, it is a good source of entertainment where lots of games, music, movies, and other related literature is available

Web site hosting: Web sites are usually hosted on to Internet from a server or a Web server. The first thing to host a Web site to acquire a domain name from registrars authorized by Internet Corporation for Assigned names and numbers (ICANN) and then a DNS server needs to be setup for the acquired domain name. Once and domain name and DNS are set then the Web site should be hosted from a server. The Web site actually is made up of content like html pages, images, videos, text, etc. All this information is stored on the Web server and can be accessed through the Internet with the help of domain name. How much information can be accessed and how fast depends on the storage space on the server and the bandwidth or the data transfer speed of the server. Many Internet service providers (ISP) offer the free Web hosting service to the subscribers.

Internet service provider: An Internet service provider is a company that offers Internet services like Web site access, hosting to its customers. It offers these services with the help of several data transmission technologies like cable modem, wireless, dial-up, DSL, etc. The ISPs have the equipment and telecommunication line access required to have a presence on the Internet. Larger ISPs have high-speed leased lines so that they are less dependent on telecommunication providers. They also have a fixed range of IP addresses from which the individual IP addresses are randomly assigned to the users whenever they connect to the Internet.

Application server: An Application server is server software or programs that acts as interface and handles all the operations between the users of an organization and the back-end business applications, or databases. It is typically used for high-end, transaction-based applications. The application servers are usually dedicated high-performance servers.

Database servers: A database server is an application or programs that is at the back-end of a database application and provides database services to other computers. It is the server where actual data is stored that is entered from several computers in an organization.

Mobile Phones: Usage of mobile phones by criminals has proved to be very useful for the Investigating officer to relate or track the offender. The Cell phone may have in its possession some vital information with regard to the mobile phone user's actions, contact details, communication patterns and other information like photographs, video and audio recordings which can prove to be an important lead for an Investing Officer to detect the case. The Investigating officer may also use the seized mobile phone to prove or disprove any allegations in the court of law. This has also given birth to a new area of computer forensics termed as Mobile Phone or Cell Phone forensics.

Important terminologies used in mobile phones

IMEI: It is abbreviated as International Mobile Equipment Identity. It is the serial number of the mobile handset, it can be compared to a chassis number of a car. It is introduced by the mobile phone manufacture with the intention to keep each and every handset they manufacture to be Unique. The IMEI number plays key role in investigation of stolen/missing/absconding mobile phones. The IMEI number may also reveal the country of origin and year of manufacture. The IMEI number can be found at the backside of the handset where battery is placed or in the manufacturer's box or by typing *#06# (Star-Hash-06-Hash) on the mobile phone.

A sample IMEI number looks like this:

3		3		0		8		4		1		9		7		8		1		2		5		1		4		9
---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---

First eight digits

“Type Allocation Code” (TAC)-Identifies make, model and country of origin (not necessarily where it was manufactured)

Ninth through fourteenth digits –

“Serial number” (SNR) that is uniquely assigned to that handset

Fifteenth digit- “Check Digit” (CD)

Used to check the validity of the IMEI

SIM card: SIM (Subscriber Identity Module) card provided by the mobile service provider (eg., BSNL, Airtel, Vodafone etc) contains the important information about the subscriber of the mobile phone. It contains the authentication program and may also store phone book entries and text messages (usually in older versions). The SIM card plays a vital role in the mobile phone forensics since it is used to identify/authenticate the subscriber to the network.

IMSI (International Mobile Subscriber Identity): The mobile phone network operator identifies the subscriber by IMSI. It is analogous to a customer/consumer number. It is stored inside the SIM card and communicates to the network through mobile handset device. It may also reveal name and country of issuing service provider. The IMSI is a fixed 15-digit length. It consists of a 3-digit Mobile Country Code (MCC), a 3-digit Mobile Network Code (MNC), and a 9-digit Mobile Station Identification Number (MSIN).

Storage of information in Mobile handsets

We may find data in a number of locations:-

1. SIM Card
2. Internal Memory of the Phone
3. Removable media (Memory Card)

Evidences in mobile phones

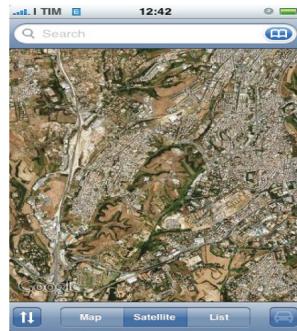
Address book: The address book in a mobile phone stores the contact details. Analyzing the address book of the mobile phone used by the accused, it is possible for the Investigating officer to gain an insight into the social network of the accused.

Call history: The call history gives a deeper insight into the activities of the accused like last dialed/received numbers as well as their duration of the conversation.

Short Message Service (in new phones emails as well): The SMS or Email messages stored in the mobile phones will provide the direct information unlike the call history and address book which provide only indirect information (the details of the conversation is unknown) but SMS/Emails can contain original text sent/received which can be used as evidence in the court of law.

Calendar: The calendar gives an overview over past and planned activities of the owner. It can be used to link the owner to certain location and times as well as indicate possible witness.

Camera: Newer generation mobile phone device contain lot of other information as well. Pictures and videos captured using the camera inbuilt in the seized mobile phone can be of great help to the investigating officer. The meta data available on each photograph or video film may contain vital information like date, time and in some cases if the mobile hand set is equipped with GPS, it stores location also. So the owner can be linked to possible crime scenes or alibis.



Information available with mobile service providers

The mobile service providers can provide valuable information to help the investigators. The following information can be obtained from the mobile service providers based on a formal request from

- Calling/Called party number
- Name, Address of customer
- IMEI/ESN/IMSI
- Call Detail Records (incoming and outgoing)
- Duration of the call
- Type of the call (roaming)
- Time of the calls/sms
- Tower location details

Abbreviations

3G (3rd Generation): A generic term referring to any of the recent wireless communication networks, providing high speed data transmission services such as video calling and broadband internet access.

Bluetooth: An ad-hoc wireless communication standard built into the majority of new mobile phones. In its most common form, Bluetooth provides direct communication between devices to a range of approximately 10 metres.

CDMA (Code Division Multiple Access): A 2G wireless communication network standard, originally implemented by telecommunications service provider Qualcomm.

ESN (Electronic Serial Number): A unique identifier assigned to every mobile device within a CDMA network.

GSM (Global System for Mobile Communications): A 2G wireless communication network standard, originally developed in Europe to provide a single standard across the entire continent.

IMEI (International Mobile Equipment Identity): A unique identifier assigned to every ME within a GSM network.

IMSI (International Mobile Subscriber Identity): A unique identifier assigned to every SIM card within a GSM network.

SIM (Subscriber Identity Module): A smartcard which identifies subscribers within a GSM network. The SIM card is placed within a GSM mobile phone, and is required to join the network.

SMS (Short Message Service): A messaging service, originally implemented for use in GSM networks, which enables short text messages to be sent between subscribers.

IRMC (Infrared Mobile Communications): A synchronization protocol, originally designed for use over Infrared, which enables information stored in a mobile device, such as calendar entries and contacts, to be synchronized with that stored in a PC application such as Microsoft Outlook.

MMS (Multimedia Messaging System): A messaging service similar to SMS which enables messages comprising of images, audio and/or video to be sent over a wireless communication network.

PIN (Personal Identification Number): A number which must be given to a mobile phone / SIM card before it will allow access to its features and/or connect to the network.

PUK (Personal Unblocking Key): A number which unlocks a SIM card in the event that the incorrect SIM PIN is entered three times in succession. The PUK is stored by the service provider.

SD (Secure Digital) Card: A form of removable storage commonly used in mobile phones, cameras and MP3 players.

Annexure 3-1: Information Technology (Amendment) Act, 2008 (Selected Extracts)

Definitions (Section 2)

- (1) In this Act, unless the context otherwise requires,
- (a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
 - (b) "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
 - (c) "Adjudicating Officer" means adjudicating officer appointed under subsection (1) of section 46;
 - (d) "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;
 - (e) "Appropriate Government" means as respects any matter.
 - (i) enumerated in List II of the Seventh Schedule to the Constitution;
 - (ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;
 - (f) "Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
 - (g) "Certifying Authority" means a person who has been granted a licence to issue a Electronic Signature Certificate under section 24;
 - (h) "Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;
 - (ha) "communication Device" means cell phones, personal digital assistance, or combination of both or any other device used to communicate, send or transmit any text,video, audio, or image.
 - (i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
 - (j) "Computer Network" means the interconnection of one or more computers or computer systems or Communication device through-
 - (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
 - (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;
 - (k) "Computer Resource" means computer, communication device, computer system, computer network,data, computer database or software;
 - (l) "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
 - (m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;

- (n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48;
- (na) "Cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.
- (nb) "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- (o) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network. ,and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
- (p) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
- (q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;
- (r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
- (s) "Electronic Gazette" means official Gazette published in the electronic form;
- (t) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
- (ta) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature
- (tb) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"
- (u) "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
- (ua) "Indian Computer Emergency Response team" means an agency established under sub-section (1) of section 70 B
- (v) "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;
- (w) "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes,
- (x) "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
- (y) "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder
- (z) "Licence" means a licence granted to a Certifying Authority under section 24;
- (za) "Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
- (zb) "Prescribed" means prescribed by rules made under this Act;
- (zc) "Private Key" means the key of a key pair used to create a digital signature;

- (zd) "Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
- (ze) "Secure System" means computer hardware, software, and procedure that -:
- are reasonably secure from unauthorised access and misuse;
 - provide a reasonable level of reliability and correct operation;
 - are reasonably suited to performing the intended functions; and
 - adhere to generally accepted security procedures;
- (zf) "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;
- (zg) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued;
- (zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether
- the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
 - the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

The proliferation of computers, the social influence of information technology, and the ability to store information in digital form have all required Indian law to be amended to include provisions on the appreciation of digital evidence.

The Information Technology Act based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce, together with amendments to the Indian Evidence Act 1872, the Indian Penal Code 1860, and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world.

"Evidence" always plays a vital role in securing the interest of the parties involved in the dispute. Information Technology Act 2000 and its various amendment has caused number of changes in the Indian Evidence Act, 1872; Indian penal Code, 1862; and other related laws.

These are few sections and with limited explanation for the purpose of highlighting the few key issues covered along with the power of police, etc., please refer the complete act and all relevant other Laws, special and local laws applicable.

Civil Remedies (Penalties, Compensation, and Adjudication)

Section – 43

Penalty and Compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in charge of a computer, computer system, or computer network –

- Accesses or secures access to such computer, computer system, or computer network or computer resource
- Downloads copies or extracts any data, computer data base, or information from such computer, computer system, or computer network, including information or data held or stored in any removable storage medium;
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system, or computer network;
- Damages or causes to be damaged any computer, computer system or computer network, data, computer data base, or any other programs residing in such computer, computer system, or computer network;
- Disrupts or causes disruption of any computer, computer system, or computer network;
- Denies or causes the denial of access to any person authorized to access any computer, computer system, or

- computer network by any means;
- (g). Provides any assistance to any person to facilitate access to a computer, computer system, or computer network in contravention of the provisions of this act, rules, or regulations made thereunder;
 - (h). Charges the services availed by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
 - (i). Destroys, deletes, or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
 - (j). Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, **shall be liable to pay damages by way of compensation to the person so affected.**

Section – 43 A

Compensation for failure to protect data

Where a body corporate, possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls, or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Offences

Section – 65

Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system, or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years or with fine which may extend up to two lakh rupees, or with both.

Section – 66

Computer-related offences

If any person, dishonestly, or fraudulently, does any act referred to in Section 43, shall be punishable with imprisonment for a term which may extend to **three** years or with fine which may extend to five lakh rupees, or with both.

Explanation: For the purpose of this section:

- (a) The word "dishonestly" shall have the meaning assigned to it in Section 24 of the Indian Penal Code;
- (b) The word "fraudulently" shall have the meaning assigned to it in Section 25 of the Indian Penal Code.

Section – 66 A

Punishment for sending offensive messages through communication service, etc

Any person who sends, by means of a computer resource or a communication device:

- (a) Any **information** that is grossly offensive or has menacing character; or
- (b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,
- (c) **Any electronic mail or electronic mail message** for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

Shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource, or communication device, including attachments in text, image, audio, video, and any other electronic record, which may be transmitted with the message.

Section – 66 B

Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh, or with both.

Section – 66C

Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password, or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section – 66D

Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section – 66E

Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation – For the purposes of this Section –

- (a). "Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;
- (b). "Capture," with respect to an image, means to videotape, photograph, film, or record by any means;
- (c). "Private area" means the naked or undergarment clad genitals, pubic area, buttocks, or female breast;
- (d). "Publishes" means reproduction in the printed or electronic form and making it available for public;
- (e). "Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that –
 - (i) He or she disrobe in privacy, without being concerned that an image of his private area was being captured; or
 - (ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in public or private place.

Section – 66F

Punishment for cyber terrorism

(1)Whoever:

- (A). With an intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror in the people or any section of the people by –
- i. Denying or cause the denial of access to any person authorized to access computer resource
 - ii. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access
 - iii. Introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70
- (B). Knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data, or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data, or computer database, with reasons to believe that such information, data, or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals, or otherwise, commits the offence of cyber terrorism.

(2). Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section – 67

Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see, or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to **three** years and with fine which may extend to five lakh rupees and 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 10 lakh rupees.

Section – 67 A

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

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to **five** years and with fine which may extend to 10 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 10 lakh rupees.

Section – 67 B

Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form

Whoever:

- (a). Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct

- (b). Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges, or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner
- (c) Cultivates, entices, or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource
- (d) Facilitates abusing children online
- (e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to 10 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 10 lakh rupees.

Exceptions: Provided that provisions of Sec 67, 67A and this section does not extend to any book, pamphlet, paper or writing, drawing, painting representation or figure in electronic form – if it is for public good, in the interest of science, literature, art or learning or other objects of general concern; or, if it is kept for bonafide heritage or religious purposes.

Explanation: For the purposes of this section, “children” means a person who has not completed the age of 18 years.

Section – 67 C

Preservation and retention of information by intermediaries

- (1). Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- (2). Any intermediary who intentionally or knowingly contravenes the provisions of Sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Other important sections

Section – 68

Power of Controller to give directions

- (1). The Controller may, by order, direct a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this act, rules, or any regulations made thereunder.
- (2). Any person who intentionally or knowingly fails to comply with any order under Sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

Section – 69

Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

- (1). Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if it is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign states, or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of Sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate government to intercept, monitor, or decrypt or cause to be intercepted or monitored or decrypted any information transmitted, received, or stored

through any computer resource.

- (2). The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
- (3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under Sub-section (1), extend all facilities and technical assistance to:
 - (a). Provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving, or storing such information
 - (b). Intercept or monitor or decrypt the information, as the case may be
 - (c). Provide information contained stored in computer resource

The subscriber or intermediary or any person who fails to assist the agency referred to in Sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section – 69 A

Power to issue directions for blocking for public access of any information through any computer resource

- (1). Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states, or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of Sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public, or cause to be blocked for access by public any information generated, transmitted, received, stored, or hosted in any computer resource.
- (2). The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
- (3). The intermediary who fails to comply with the direction issued under Sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section – 69B

Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

- (1). The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource.
- (2). The intermediary or any person in-charge of the computer resource shall when called upon by the agency which has been authorized under Sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving, or storing such traffic data or information.
- (3). The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
- (4). Any intermediary who intentionally or knowingly contravenes the provisions of Sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

- (I) "Computer Contaminant" shall have the meaning assigned to it in Section 43
- (II). "Traffic data" means any data identifying or purporting to identify any person, computer system, or computer

network or location to or from which the communication is or may be transmitted and includes communications' origin, destination, route, time, date, size, duration, or type of underlying service or any other information.

Section – 70

Protected system

- (1). The appropriate government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health, or safety.
- (2), The appropriate government may, by order in writing, authorize the persons who are authorized to access protected systems notified under Sub-section (1).
- (3). Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to 10 years and shall also be liable to fine.
- (4). The Central Government shall prescribe the information security practices and procedures for such protected system.

Section – 70 A

National Nodal Agency

- (1). The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
- (2). The national nodal agency designated under Sub-section (1) shall be responsible for all measures, including Research and Development relating to protection of Critical Information Infrastructure.
- (3). The manner of performing functions and duties of the agency referred to in Sub-section (1) shall be such as may be prescribed.

Section – 70 B

Indian Computer Emergency Response team to serve as national agency for incident response

The Indian Computer Emergency Response team shall serve as the national agency for performing the following functions in the area of Cyber Security:

- Collection, analysis, and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incidents response activities
- Issue guidelines, advisories, vulnerability notes, and white papers relating to information security practices, procedures, prevention, response, and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

Section – 71

Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with 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

Breach of confidentiality and privacy

Save as otherwise provided in this act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this act, rules, or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document, or other material to any other person shall be punished with 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

Punishment for disclosure of information in breach of lawful contract

Save as otherwise provided in this act or any other law for the time being in force, any person, including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees, or with both.

Section – 73

Penalty for publishing electronic Signature Certificate false in certain particulars

- (1). No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that:
 - a. The Certifying Authority listed in the certificate has not issued it,
 - b. The subscriber listed in the certificate has not accepted it,
 - c. The certificate has been revoked or suspended,unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
- (2). Any person who contravenes the provisions of Sub-section (1) shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees, or with both.

Section – 74

Publication for fraudulent purpose

Whoever knowingly creates, publishes, or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees, or with both

Section – 75

Act to apply for offence or contraventions committed outside India

- (1). Subject to the provisions of Sub-section (2), the provisions of this act shall apply also to any offence or contravention committed outside India by any person irrespective of his/her nationality.
- (2). For the purposes of Sub-section (1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system, or computer network located in India.

Section – 76

Confiscation

Any computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto, in respect of which any provision of this act, rules, orders, or regulations made there under has been or is being contravened, shall

be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power, or control of any such computer, computer system, floppies, compact disks, tape drives, or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this act, rules, orders, or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto, make such other order authorized by this act against the person contravening of the provisions of this act, rules, orders, or regulations made there under as it may think fit.

Section – 77

Compensation, penalties, or confiscation not to interfere with other punishment

No compensation awarded, penalty imposed, or confiscation made under this act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

Section – 77 A

Compounding of Offences

A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this act.

Provided that the court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the court shall not compound any offence where such offence affects the socioeconomic conditions of the country or has been committed against a child below the age of 18 years or a woman.

The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of Section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Section – 77 B

Offences with three years imprisonment to be cognizable

Notwithstanding anything contained in Criminal Procedures Code, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Section – 79 A

Central Government to notify Examiner of Electronic Evidence

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body, or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Section – 84 B

Punishment for abetment of offences

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this act for the punishment for such abetment, be punished with the punishment provided for the offence under this Act.

Section – 84C

Punishment for attempt to commit offence

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both

Power of IO to investigate/enter/search/seize/arrest under IT (Amendment) Act, 2008**Section – 78****Power to investigate offences**

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

Section – 80**Power of Police Officer and Other Officers to Enter, Search, etc.**

- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Annexure 3-2: International Investigations and Letters Rogatory

No. 25016/14/2007-Legal Cell

Government of India

Ministry of Home Affairs

Internal Security Division

COMPREHENSIVE GUIDELINES REFERRED TO IN LETTER NO. 25016/14/2007- LEGAL CELL DATED 31ST DEC., 2007 OF INTERNAL SECURITY DIVISION, MINISTRY OF HOME AFFAIRS REGARDING INVESTIGATION ABROAD AND ISSUE OF LETTERS ROGATORY AND ALSO THE PROCEDURE FOR EXTRADITION REQUESTS AND CONTACT WITH FOREIGN POLICE/LEGAL ATTACHES
(from <http://cbi.nic.in/interpol/invletterrogatory.php>)

A. INVESTIGATION ABROAD

1. It may be necessary to gather information or conduct formal investigation abroad, in cases, where accused person(s) has escaped from the country after committing the crime or part of the crime has been committed outside the country or the witnesses and other material evidence are available in another country.
2. However, it may not be necessary to gather formal evidence in all such cases and in many cases/ enquiry; the investigation agency may only need information or lead in the first instance. The Investigation Agency may get informal information/material/leads collected through Interpol or diplomatic channels. [Intelligence sharing, however, is required to be done by designated intelligence agencies]. The International Police Cooperation Cell (hereinafter referred as IPCC) of CBI, New Delhi is the designated agency for routing requests for informal enquiries to be made with National Central Bureau of other countries, Interpol Headquarters as well as our Missions abroad.
3. For getting informal investigation conducted through the Interpol channels or our Missions abroad, a self contained request, along with necessary details, may be addressed to Assistant Director, IPCC, Block # 4, CGO Complex, Central Bureau of Investigation, New Delhi. In case, information is to be collected/ enquiries are to be conducted in more than one country, separate self contained requests may be sent for each country. The request may be routed through the head of Crime Investigation Department (CID) of the State Police.
4. The request must incorporate the following details:
 - i. The FIR number along with names of the accused and sections of law under which case has been registered.
 - ii. The gist of the allegations in the FIR/ Preliminary Enquiry or any other Investigation Process.
 - iii. The detail of information required. In order to facilitate requested country/ its NCB providing information the specific relevant details must be furnished.
5. It is necessary that material being furnished should be carefully examined and scrutinised at an appropriate level especially as regards accuracy of facts and figures. It must be noted the information so collected cannot be treated as formal evidence.

B. VISIT OF POLICE OFFICERS ABROAD FOR INVESTIGATION

1. Sometimes, it may become necessary to send Police Officer(s) from India to foreign country for the purpose of execution of LR or for collecting information or leads during the course of investigation of a case keeping in view the importance of the case and the complicated nature of offences under investigation.
2. As any police officer including that of the CBI would enjoy no Police powers in a foreign country and any such visit

by a police officer without the express consent of any country may be considered interference in the sovereignty of that country unless some required formalities are observed.

3. When it is considered necessary to send a team of Officers abroad, the State Government will send a proposal to IPCC, CBI, India which in turn will obtain the approval of MHA for the proposed visit, whenever necessary.
4. The following information needs to be sent to the IPCC, CBI India for taking up the matter with the country to which such team is proposed to be sent:
 - i. A brief note detailing the reasons for sending the team, nature of enquiries required to be made in the requested country. This is to enable the authorities to assess whether the request is justified.
 - ii. All available particulars about identity or particulars of the person to be contacted or documents to be scrutinised etc. This would help the requested country to make all necessary preparations.
 - iii. Information about penal offence to which mission relates.
 - iv. Whether Article 3 of the ICPO (Interpol) Constitution or some other legal provision restricting international cooperation is attracted.
 - v. Exact date and duration of the mission and information about the police officers such as their names and ranks.
 - vi. Any other relevant information which may be relevant in processing such a request.
5. The visit will not commence before the required permission is received. The officers must get in touch with Indian Mission on their arrival. In case, the country does not have a mission, the accredited mission for India may be kept informed as regards visit of the officers.

C. GUIDELINES FOR ISSUANCE OF LETTERS ROGATORY FOR INVESTIGATION ABROAD UNDER SECTION 166-A CrPC, 1973

1. In order to conduct formal investigation and to collect evidence and gather material objects/documents Section 166-A of the Criminal Procedure Code 1973 lays down the procedure of sending Letter of Request (Letters Rogatory) through a competent Court. Letters Rogatory is forwarded within the ambit of Mutual Legal Assistance Treaty (MLAT), Memorandum of Understanding (MoU)/ Arrangement etc. existing between India and requested country or on basis of reciprocity in case no such treaty and MoU exists. In certain cases, it may also be possible to use the provisions of an International Convention, providing for such mutual cooperation, to which both India and the requested country are signatory for sending such Letters Rogatory.
2. No request for issue of Letters Rogatory (Letter of Request) shall be brought before any Court by an Investigation Agency without prior concurrence of the Central Authority i.e. the Ministry of Home Affairs (MHA).
3. In case, it is considered necessary to get a Letters Rogatory (Letter of Request) issued, a self contained proposal may be sent to Under Secretary (Legal), Internal Security Division, Ministry of Home Affairs, Lok Nayak Bhawan, New Delhi- 110 003 to be routed through the Home Department of the State in case of State Police, and directly to MHA in case of DSPE (CBI) for obtaining concurrence of the Government before filing an application in the Competent Court.
4. Before making a proposal to the MHA, the Investigating Agency concerned may examine the matter in detail whether it is absolutely necessary to get investigation conducted abroad for taking the case to a logical conclusion. The provisions of the MLAT, MoU, Arrangement or International Convention as well as requirement of the law of requested country such as principle of dual criminality, assurance of reciprocity etc., may be studied with view to determine that such a request would fall within the parameters of legal requirements of the requested country. It is important as it would have to be specifically mentioned as to under what provisions of Treaty, MoU, Arrangement or International Convention the request was being made. Where no such bilateral or multilateral arrangements exist Letters Rogatory may be made on the basis of assurance of reciprocity.
5. Certain countries do insist that a Letters Rogatory be sent in particular language or format. If so, the requirements

thereof of making such a request may be studied to comply with them. Assistance of IPCC, CBI, New Delhi may be taken for the purpose, if required.

6. For obtaining the concurrence of MHA, the Investigating Agency concerned would send the following in triplicate:
 - i. A self-contained note containing brief facts of the case incorporating the allegations, names of the accused and particulars of the offences committed with details of Sections of Law and a copy of First Information Report (FIR). The FIR may be neatly word processed and must accompany with an English translation if written in vernacular.
 - ii. The need to conduct investigation abroad along with the legal opinion of Director of Prosecution or the senior most Law Officer commenting on the need for such Letters Rogatory (Letter of Request), that it would fall within the ambit of MLAT, MoU, Arrangement, International Convention and laws of the requested Country on the principles of dual criminality etc. Relevance of statement of witnesses to be examined and collection of documents/ material being requested to be seized to the investigation of the case may also be commented upon.
 - iii. The relevant provisions of the MLAT or MoU or Agreement or Arrangement or an International Convention under which the Letters Rogatory (Letter of Request) is to be made may be enclosed. In case it is to be sent on assurance of reciprocity the same may be mentioned.
 - iv. The draft application proposed to be filed in the Competent court for issues of Letters Rogatory may be enclosed. The application should contain the following:
 - a. Background Note with brief facts of the case, the allegations and name of the accused and particulars of the offences committed with extract of Sections of Law and a neatly word processed copy of First Information Report (FIR) as enclosure .
 - b. The details of investigation to be carried in the requested country. Care must be taken that request made is specific as no country would allow fishing enquiries/ investigation.
 - c. Particulars of the witnesses to be examined, their identity and addresses if available along with detailed questionnaire for examination of each witness.
 - d. Description of the documents/articles to be collected and procedure for the same.
 - e. Extract of the corresponding Sections of laws of the requested country which would constitute an offence/s or similar allegations under investigation in India. It may be stated in particular if under the laws of the requested country principle of dual criminality or any other requirement is essential requirement for execution of Letters Rogatory.
 - f. Extract of relevant provisions of the MLAT, MoU, Arrangement or International Convention etc. providing for such assistance by the requested country.
 - g. Declaration that the proposed Letters Rogatory would be in compliance of all the requirements of the requested country and that the case under investigation is not of political, military, racial or religious character.
 - h. A draft Assurance of Reciprocity in case the request is being made to a country with whom no MLAT, MoU, Arrangement exists or the request does not fall within the ambit of an International Convention.
 - i. Whether a visit by Investigating or any other officer is proposed to assist the authorities in the requested country to execute the Letters Rogatory.
7. The following precautions may be taken by the Investigating Agency while preparing a Letters Rogatory:
 - i. The documents, photographs and objects, if enclosed with the Letters Rogatory, should be clearly marked and referred to in the body to enable the requested Authority to know clearly what is required to be done with them.

- ii. All the photocopied papers/ documents enclosed must be legible and translated in the required language, if required.
 - iii. The Letters Rogatory should be neatly bound and page numbered.
 - iv. The authenticated translated copies, duly singed by a translator, be enclosed along with original LR, if required to submitted in a language as prescribed in the MLAT, MoU, Arrangement or otherwise.
 - v. At least, five copies of the Letters Rogatory should be prepared including the original. Three copies along with the translated version, if any, would need to be sent to the MHA along with a copy to the International Police Cooperation Cell of CBI.
8. MHA may consult CBI whenever required and convey its concurrence to the proposal to be filed in the Competent Court for issue of a Letters Rogatory and also mark a copy of its concurrence to IPCC, CBI, New Delhi.
 9. After obtaining the concurrence of the MHA, an application may be filed in the Court of competent jurisdiction for issue of Letters Rogatory addressed to the competent authorities of the requested country. The Competent Court may decide to issue a Letters Rogatory addressed to the competent authority in the requested country as prayed for or otherwise.
 10. In case, the request is accepted, the Court would issue the Letters Rogatory under its seal and authority. A format and contents of the Letters Rogatory are given in the annexure to the guidelines.

D. PROCEDURE TO BE FOLLOWED AFTER ISSUE OF LR BY THE COMPETENT COURT

1. The Investigating agency will send three copies of the LR to IPCC, CBI, New Delhi and one copy to MHA. IPCC, CBI, New Delhi will forward the same to the competent authority in the requested country through the Indian Missions under intimation to MHA.
2. The Indian Mission will take prompt action to present/ send the LR to the competent authority and communicate the exact date of such presentation/ submission to IPCC, CBI, New Delhi. The Mission and IPCC will follow up the execution of LR with the competent authority in the requested country.
3. In event of requested country seeking clarifications, additional material etc., the Mission will directly communicate the same to the IPCC, CBI, New Delhi, who may take necessary action in the matter under intimation to MHA & MEA.
4. The execution report, along with evidence and supporting material, received from the requested country would be directly sent by our Mission abroad to the IPCC, CBI, New Delhi, who would in return send the same to the Agency concerned under intimation to MHA and MEA.

E. HANDLING OF INCOMING LETTERS ROGATORY (LR)

1. All incoming LR will be received by Under Secretary (Legal), Internal Security Division, Ministry of Home Affairs, Lok Nayak Bhawan, New Delhi 110 003 and will be entrusted to an Investigation Agency (State Police/CBI) in consultation with Joint Director (Policy) in CBI.
2. Where LR needs to be executed through the State Police, it will be sent to IPCC, CBI for getting it executed by the State Police concerned.
3. The agency entrusted with the task of execution of LR will do so at the earliest. The letters rogatory would be executed in terms of the provisions of the MLAT, MoU and Arrangement etc., if it exists with the requesting country otherwise the evidence shall be gathered under the provisions of Indian laws, as applicable.
4. The following precautions may be taken while preparing the Execution Report:
 - i. The documents, photographs and objects, if enclosed with the Execution Report, should be clearly marked and referred to in the body.

- ii. All the photocopied papers/ documents enclosed must be legible and authenticated as per provisions of Indian Evidence Act unless otherwise provided in the MLAT, MoU, Arrangement etc.
 - iii. The Execution Report should be neatly bound and page numbered.
 - iv. At least, four copies of the Execution Report should be prepared including the original. Three copies including the original may be sent to the IPCC, CBI, New Delhi while a copy is retained by the executing agency for future reference.
5. After execution, the investigation agency will forward the execution report to the IPCC, CBI, New Delhi along with the evidence and material collected who will forward the same to the Central Authority of the requesting country through the MEA under intimation to MHA.

F. HANDLING OF EXTRADITION REQUESTS

1. Extradition if either done under Extradition Treaty or other Extradition Arrangement or Assurance of Reciprocity with the requesting country.
2. Extradition request can be normally made only after a charge-sheet has been filed in the court and the court has taken cognisance of the case. If the accused available in the other country is to be arrested and produced in the court in India, the requisite action to bring such accused to India is through Extradition Process and not through LR.
3. Extradition requests are not accepted for political offences. The principle of dual criminality is invariably followed for extradition requests. An accused extradited for a particular offence can be tried only for that offence by the receiving country.
4. The State investigating agency will send extradition requests to the IPCC, CBI, New Delhi through the State Home Department who would in turn send the same to MEA for further necessary action.

G. CONTACT BY AND WITH FOREIGN POLICE/ LEGAL OFFICERS/ATTACHES

1. Foreign Police Personnel/ Legal Attaches are not permitted to establish any direct contact with the police personnel at the State Level unless specifically authorized by MHA.
2. Any attempt by such foreign police /legal personnel to establish direct contact with the State Police Authorities should immediately be brought to the notice of MHA.

(Continuation of MHA Circular)

**No. 25016/17/2007-Legal Cell Government of India Ministry of Home Affairs, IS Division-II:Legal Cell
New Delhi, dated the 11th Feb, 2009**

To

The Home Secretaries of all States/UTs, The DGPs and IGPs of all States/UTs.

Sub: Comprehensive guidelines regarding service of summons/notices/ Judicial process on the persons residing abroad.

Sir,

Section 105 of Criminal Procedure Code (Cr.P.C.) provides for reciprocal arrangements to be made by Central Government with the foreign governments with regard to the service of summons/ warrants/ judicial processes. MHA has entered into Mutual Legal Assistance Treaty/ Arrangements with 25 countries. In respect of other countries, the Ministry attempts to serve the judicial papers by giving an assurance of reciprocity. However, despite this Ministry's best efforts the summons and other judicial process get delayed for various reasons.

With a view to streamlining the procedure, MHA has examined the matter and comprehensive guidelines are enclosed covering various aspects of service of the summons/ Notices/ Judicial process on persons residing abroad.

You are requested to kindly have these comprehensive guidelines circulated amongst all courts/ all investigating officers under your jurisdiction for strict compliance.

Yours faithfully,

Sd/-
(Amar Chand)
Under Secy. To the Govt. of India

Encl : As above.

Copy to :

- i) M/o Law and Justice , Deptt. Of Legal Affairs, Shastri Bhawan, New Delhi
- ii) M/o External Affairs, CPV Division, Patiala House Annexe, Tilak Marg, New Delhi.
- iii) JS(PP), MHA, Lok Nayak Bhawan, Khan Market, New Delhi
- iv) JD(Policy), CBI, North Block, New Delhi
- v) Joint Director, IB, New Delhi.

Annexure 4-1: Model Questionnaire for Pre-Investigation Assessment

Basic Information Gathering to Assess the Crime / Incident

- What is the nature of the incident that occurred?
- Who discovered the incident and when? What alerted the person of the incident?
- What is the extent of loss, if any?
- Who are the people working when the incident took place/discovered?
- Who are the team members that are usually present?
- What applications and software, databases are being used by the organization?
- Who are the developers of the applications that are used?
- Who provides the support and maintenance for the applications?
- Where are the actual servers located?
- Who has the administrative and super user privileges?
- What is the backup policy of the organization?
- What kind of backups is taken and how long they are retained?
- What are the services offered by the organization?
- Who are affected by the incident occurred? Were they informed?
- What kind of security measures are being used(Antivirus, Firewall, and IDS/IPS)
- Is logging enabled by any of the applications that are being used?
- What levels of access are given to employees?
- What is the information security policy of the organization? How frequently this audited / checked for compliance?
- What are the physical security measures in place?
- Is there an e-mail server present if so where is it located?
- What are the HR Policies of the organization and, any suspects from the recently left employees?

Annexure 4-2: Questionnaire - Additional Information for Network related incidents

- Who is the ISP for the organization?
- What is the domain name and IP address of the organization
- From where the Web site is hosted, who administers it?
- How many servers are there and what is their configuration?
- What are the different operating systems that are being used?
- Who is the administrator and DBA of the servers?
- What level of security settings are being implemented Firewall/IDS/IPS/Antivirus?
- Any alarms given by Firewall, IDS/IPS, or any suspicious activity noted?
- How is the backup policy, how often backups are taken and how long they are retained?
- When the incident took places, who are the people at work?
- Are there any suspects?
- Do they have any IP address, MAC address, Web address, e-mail address of the suspect?
- What actions were taken up by the organization in response to the incident?
- Is there any previous record of any breach or attack?
- If yes, what happened then?
- What levels of access was given to employees? Are they allowed carry thumb drives, CDs, or other devices?
- Can any employee install any applications on his/her own?
- Has anybody access to remote login or VPN to any of the servers?
- Are the employees permitted to use the official laptops for accessing internet?
- How often the employees' laptops/desktops are changed?
- What applications and software are installed in the servers?
- Is there any file-server, e-mail, or ftp servers?
- Is logging enabled in any of the applications that are being used? If yes, where are they stored?

Annexure 4-3: Evidence Preservation Instructions

Evidence Preservation Notice as a policy can be adapted by the Investigating Officer in cases of Government / Statutory bodies where in the person supervising the networks is not a suspect and, the organizational head is not under suspicion. Sometimes, it is not feasible for the IO to immediately decide on the full extent of evidence to be seized and, also in case of large networks it is not practical to plan for seizure of the entire setup. It will be useful for the Investigating officers to issue a preservation notice to the identified personnel who are custodians to keep the requested equipment / information in safe custody to be produced before the investigating agency at the time and place to be decided at a future date. Section 91 of Cr PC empowers the IOs to direct the concerned to do the needful and abide by the lawful instructions.

Directions/Instructions to employees/individuals:

- Send directions to the authorized custodians of the resources to preserve all the electronic and hard copy documents related to this case until further notice.
- Do not move, shift, or replace any of the computer systems involved in the incident.
- Do not alter, modify, edit, copy, or delete any files/folders/software.
- Restrict the access to the scene of incident/offence. Lock it up if possible.
- Do not allow anybody who are related to the incident to go out on leave or absence.
- Preserve all the logs, backups, access registers, telephone logs, calendars, and appointment books
- Preserve all the hard copies of the manuals, technical specifications of the hardware, and software
- Preserve all the storage devices like thumb drives, hard drives, CDs, DVDs, Flash drives, and other devices.
- Preserve any business agreements with clients, license agreements, etc.
- Preserve all the e-mails and other communications relating to this case.

Instructions/Directions for Network/Database Administrators:

- Do not restore the backups and, Do not reuse the backup tapes.
- Preserve all the network diagrams, technical specifications, and manuals.
- Do not delete any files stored on remote or off-site servers.
- Do not delete any log files created (access logs, database logs, etc.).
- Disable the access to these servers or computers if any suspected individuals involved.
- Archive all e-mails and other network share drives from the date of preservation notice.
- Preserve all audit logs of the system.
- Update the inventory list of all systems/PDAs, etc., and cross check with all the suspected persons.

Please prepare an inventory of hardware and software involved in the issue.

Annexure 4-4: Evidence Preservation Notice

(Suggested Template)

Crime Number: / Enquiry Reference: Sections of Law

Police Station:

To

Name and address of the person to whom the notice is served:

Please refer to the case / enquiry mentioned above. The undersigned is investigating / enquiring into the matter. As per the complaint / investigations, it is learnt that / established that, critical evidence in this matter exists in the form of electronic records contained in the computer systems of , This is a notice to you and demand that such evidence identified must be immediately preserved and retained by you until further written notice from the undersigned. This request is essential, as a paper printout of text contained in a computer file does not completely reflect all information contained within the electronic file. This request is made as per the provisions of the Section 91 Cr PC.

Additionally, the continued operation of the computer systems identified herein will likely result in the destruction of relevant evidence due to the fact that electronic evidence can be easily altered, deleted, or otherwise modified. Failure to comply with the notice will make you liable for legal action as per IPC and, other relevant laws.

- For purposes of this notice, “Electronic Record” has the same meaning as defined under ITAA and, shall include, but not be limited to, all text files (including word processing documents), spread sheets, e-mail files and information concerning e-mail (including logs of e-mail history and usage, header information, and “deleted” files), Internet history files and preferences, graphical image format (GIF) files, databases, calendar and scheduling information, computer system activity logs, and all file fragments and backup files containing Electronic Data.
- Please preserve and retain all Electronic records generated or received (relating to the enquiry) (give details).
- Please preserve and retain all Electronic records containing any information about (the enquiry) (give details).
- You must refrain from operating (or removing or altering fixed or external drives and media attached thereto) standalone personal computers, network workstations, notebook and/or laptop computers operated by (accused) (give details).
- You must retain and preserve all backup tapes or other storage media, whether online or offline, and refrain from overwriting or deleting information contained thereon, which may contain Electronic records identified above.

Please contact the undersigned if you have any questions regarding this notice.

(To be signed by the Enquiry Officer / IO with official seal)

Annexure 5-1: Legal Provisions for Search and Seizure

Section 165 Cr.Pc:- Search by police officer.

- (1) Whenever an officer in charge of police station or a police officer making an investigation has reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorized to investigate may be found in any place within the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as possible the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station.
- (2) A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person.
- (3) If he is unable to conduct the search in person, and there is no other person competent to make the search present at the time, he may, after recording in writing his reasons for so doing, require any officer subordinate to him to make the search, and he shall deliver to such subordinate officer an order in writing, specifying the place to be searched, and so far as possible, the thing for which search is to be made; and such subordinate officer may thereupon search for such thing in such place.
- (4) The provisions of this Code as to search warrants and the general provisions as to searches contained in section 100 shall, so far as may be, apply to a search made under this section.
- (5) Copies of any record made under sub-section (1) or sub-section (3) shall forth- with be sent to the nearest Magistrate empowered to take cognizance to the offence, and the owner or occupier of the place searched shall, on application, be furnished, free of cost, with a copy of the same by the Magistrate.

Section 100 Cr.Pc Persons in charge of closed place to allow search.

- (1) Whenever any place liable to search or inspection under this Chapter is closed, any person residing in, or being in charge of, such place, shall, on demand of the officer or other person executing the warrant, and on production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein-
- (2) If ingress into such place cannot be so obtained, the officer or other person executing the warrant may proceed in the manner provided by sub-section (2) of section 47.
- (3) Where any person in or about such place is reasonably suspected of concealing about his person any article for which search should be made, such person may be searched and if such person is a woman, the search shall be made by another woman with strict regard to decency.
- (4) Before making a search under this Chapter, the officer or other person about to make it shall call upon two or more independent and respectable inhabitants of the locality in which the place to be searched is situate or of any other locality if no such inhabitant of the said locality is available or is willing to be a witness to the search, to attend and witness the search and may issue an order in writing to them or any of them so to do.
- (5) The search shall be made in their presence, and a list of all things seized in the course of such search and of the places in which they are respectively found shall be prepared by such officer or other person and signed by such witness; but no person witnessing a search under this section shall be required to attend the court as a witness of the search unless specially summoned by it.
- (6) The occupant of the place searched, or some person in his behalf, shall, in every instance, be permitted to attend during the search, and a copy of the list prepared under this section, signed by the said witnesses, shall be delivered to such occupant or person.

- (7) When any person is searched under sub-section (3), a list of all things taken possession of shall be prepared, and a copy thereof shall be delivered to such person.
- (8) Any person who, without reasonable cause, refuses or neglects to attend and witness a search under this section, when called upon to do so by an order in writing delivered or tendered to him, shall be deemed to have committed an offence under section 187 of the Indian Penal Code (45 of 1860).

Section 80 of IT Act 2000 (Amended 2008)

Power of police officer and other officers to enter, search, etc.

- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Police Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act
Explanation.—For the purposes of this sub-section, the expression “public place” includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.
- (2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
- (3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Annexure 5-2: Chain of Custody Form

CHAIN OF CUSTODY					
DETAILS OF THE DIGITAL EVIDENCE					
Crime number.....	Date of Seizure.....				
Name of the I.O.....	Time.....				
P.F.Number.....					
TECHNICAL INFORMATION					
MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER		
DESCRIPTION					
CHAIN OF CUSTODY					
REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

Reason /action: IO shall ensure documentation of the reasons for transferring the seized evidence to other custodians in chronological order.

Annexure 5-3: Digital Evidence Collection Form

Digital Evidence Collection Form			
Crime Number:		Date:	
PS/Circle/SDPO:		Time:	
IO Name		Item Number:	
Location :		Custodian / Suspect Name:	
Computer Information			
<input type="checkbox"/> Laptop	<input type="checkbox"/> Desktop	Manufacturer	
<input type="checkbox"/> HDD Only	<input type="checkbox"/> External HDD	Model Number	
<input type="checkbox"/> Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	
Evidence Drive			
Acquired By		Date of Acquisition	
Signature of I.O		Time of Acquisition	
Acquisition Information			
<input type="checkbox"/> IDE	<input type="checkbox"/> SCSI	Manufacturer	
<input type="checkbox"/> SATA	<input type="checkbox"/> Other	Model Number	
		Serial Number	
		HDD Size	
Collection Details		Destination Drive Details	
Software used		Manufacturer	
Version		Model Number	
Write Protect Device Used		Serial Number	
Verified By		HDD Size	
Image File Name			
Notes			

Annexure 5-4: Forensic Science Laboratories

Address and Location	Office	Fax
Central Forensic Sciences Laboratories		
Central Forensic Science Laboratory ,Sector 36-A, Plot - 2, Dakshin Marg, Chandigarh, Punjab - 160 036	0172 2615068 dircfsl_chd@dfs.gov.in	0172 2605923
Central Forensic Science Laboratory, Ramanthapur, Amberpet Post, Hyderabad, Andhra Pradesh - 500 013 Dy. Director, NAA Unit of CFSL, Hyderabad,	040-27038429 dircfsl_hyd@dfs.gov.in cfsl_hyd@rediffmail.com	040 27039281
ACD, BARC, Trombay, Mumbai - 400 085	022- 25505334	
Central Forensic Science Laboratory, 30, Gorachand Road Kolkata, West Bengal - 700 014	033 22841638 / 3247 dircfsl_kol@dfs.gov.in geqd_kol@dfs.gov.in	033 22840642
Central Forensic Science Laboratory (CBI), CBI Complex Block 3, Lodhi Road, CGO Complex, New Delhi - 110003	011-24361396 dcfsl@cbi.gov.in	01124360742
State Forensic Sciences Laboratories		
Forensic Science Laboratory, Red Hills, Opp. Niloufer Hospital Andhra Pradesh , Hyderabad - 500004	040-23390398	040-23394449
State Forensic Science Laboratory, Kahlipara, Assam , Guwahati - 781 019	0361-2381305, 0361-2381385 0361-2381696	0361-2381305
State Forensic Science Laboratory, Arunachal Pradesh , Banderdewa - 791 123	0360-2218190	0360-2211433
State Forensic Science Laboratory, J L N Marg, P.O. Shastri Nagar, Bihar , Patna - 800 023	0612-2287535	0612-2281273
State Forensic Science Laboratory, Police Line Campus, Tikrapara, Raipur, Chhattisgarh - 492 002	0771-2251258	0771-2251258
State Forensic Science Laboratory, Behind Police Bhawan, Sector 18 A, Gujarat , Gandhi Nagar	079-23256250	079-23256251
State Forensic Science Laboratory, Madhuban, Karnal, Haryana - 132 037	0184-2380104	0184-2380104
State Forensic Science Laboratory, Junga, Himachal Pradesh - 173 216	0177-2752527	0177-2752527
J & K Forensic Science Laboratory, Bikram Chowk, Jammu Tawi (Winter) J & K Forensic Science Laboratory, Dalgate, Srinagar (Summer)	0191-2435249 0194-2473155	0191-2435249 0194-2473155
State Forensic Science Laboratory, Line Tank Road, Near Old Jail, Jharkhand , Ranchi - 834 001	0651-2280540 0651-2283834	0651-2280540
State Forensic Science Laboratory, Madiwala, Karnataka , Bangalore - 560 068	080-25532910	080-25532910
State Forensic Science Laboratory, State Forensic Science Laboratory, Bank House, Compound, Villayambalam, Thiruvananthapuram, Kerala - 695 010	0471-2721533	0471-2721533
Forensic Science Laboratory, 5, Civil Lines, Sagar, Madhya Pradesh - 470 001	07582-267707, 07582-267791	07582-267707
State Forensic Science Laboratory, Hans Bhugra Marg, Santacruz (E), Vidyanagari, Mumbai, Maharashtra - 400 098	022-26670760	022-26670844
State Forensic Science Laboratory, Pangei, Manipur - 795 114	0385-2224253	0385-2224253

Address and Location	Office	Fax
State Forensic Science Laboratory, Lumshyiap, Shillong, Meghalaya - 793 001	0364-2226801	0364-2226801
Forensic Science Laboratory, Mualpui, Mizoram , Aizawl - 796 001	0389-2322315	0389-2334310, 0389-2335578
Mini Forensic Science Laboratory, Dimapur, Nagaland - 797 112	03862-233340	011-27555890
Forensic Science Laboratory, Govt. of NCT of Delhi, Madhuban Chowk, Rohini, New Delhi - 110 085	011-27555890	0674-2586187
State Forensic Science Laboratory, Rasulgarh, Bhubneshwar, Orissa - 751 010	0674-2586187 0674-2586417	
Forensic Science Laboratory, 'A' Block, Mini Secretariat Sector - 9, Chandigarh, Punjab - 160 017	0172-2742797	0172-2742797
Police Forensic Science Laboratory, Jaipur, Rajasthan - 302 016	0141-2301584	0141-2301584
Forensic Science Department, "Forensic House", 30-A, Kamarajar Salai, Mylapore, Chennai, Tamil Nadu - 600 004, e-mail : forensic@tn.nic.in	044-28447767	044-28447767
State Forensic Science Laboratory, Nursingarh, P.O. Bimangarh, Tripura , Agartala - 799 015	0381-2341266	0381-2341266
Forensic Science Laboratory, Post Box No. 9, P.O. Mahanagar, Lucknow, Uttar Pradesh - 226 006	0522-2371232	0522-2371232
State Forensic Science Laboratory, Near New Basant Vihar Police Stn., Police Housing Colony, Uttarakhand , Dehradun	0135-2714101	
State Forensic Science Laboratory, 37/1/2, Belgachia Road West Bengal , Kolkata - 700 037	033-25565430	033-25565430
Forensic Science Laboratory, Andaman and Nicobar Islands	03192-232244	03192-232244

Annexure 5-5: Requisition letter to FSL

Forwarding Note

(In all cases where examination of any material is required at the laboratory, a copy of this form duly filled in should accompany the exhibits.)

Case No.- /20xx	Police Station -
Section of Law -	Dist.-
Date - / /	State -

I. Nature of Crime

Nature of Crime.....

.....

Brief History

.....

Any other relevant details.....

II – List of Exhibits for Examination

Sr. No. / Barcode	Description of Exhibits	How, when, and by whom found	Source of exhibits	Remarks

III – Nature of Examination required

Sr. No. / Barcode	Description of Exhibits	Nature of Examination required	Date or any keyword or filter	Remarks

IOs are advised to pay additional attention to this section, as this plays a critical component in the investigation. Apart from requesting the information required for the investigation like files, deleted information, etc., from the digital evidence, lot of other information, which can be developed as supporting (secondary) evidence in the investigations like login time, users list, various applications installed, IP address, printers connected, etc.

IOs are suggested to contact the forensic lab professionals to understand what kind of information can be retrieved from these digital media which can be vital evidence.

Sr. No.	Full Name	Occupation	Sex	Date and Time of arrest	Whether bailed, court or Police Custody
Seal	Rank and Sign. of the I. O.				
O/W No.-	Date -				
Forwarded to the Director,.....					
Specimen Seal/s impression/s on exhibits or parcel/s	Sign and Designation of Forwarding Officer				

Certificate of Authority

Certified that the Director

has the authority to examine the exhibits sent to him in connection with Case No.

..... u/s Pol. St

Date of State versus

Date:	
Place:	Sign and Designation of Forwarding Authority

Annexure 5-6: FSL Requisition-Information to be Furnished

Information needs to be furnished to forensic examiner and request for specific information based on the type of crime:

- Questions and information common to most of the cases/incidents
 - Brief facts of the case
 - Details/description of the objects
 - Date and time of collection of the objects
 - Status of the objects when collected (powered on and powered off)
 - Seized from — person, organization, location, etc.
 - Seized by — person and organization
 - Please recover all the deleted folders and files from the system
 - Please provide the list of all files and folders from the system
- Questions to be asked in case of “Computer as a target” cyber crime
 - What type of operating system has been installed in the computer?
 - When was the operating system installed?
 - Please provide the user names/users present in the system
 - What programs or software is installed in the computer?
 - What is the IP address assigned to the system, if any?
 - What is the MAC address of the system?
 - Are there any information relating e-mail addresses present in the computer system?
 - Are there any chat messenger software installed. If so, are there any chat IDs/profiles?
 - Any suspicious or malicious software installed?
 - Please provide the Internet history of the computer (Web sites accessed, files uploaded, downloaded, etc.)?
 - Are there any firewall logs available in the system?
- Questions to be asked in case of “sending threatening e-mail”
 - Whether sender’s e-mail address is present in the seized hard disk.
 - Whether receiver’s e-mail address is present in the seized hard disk.
 - Whether the contents of the e-mail message (subject mail of case) is present in the hard disk.
 - Any information relating to the IP addresses are available?
- Questions to be asked in case of “Creation of obscene profile/hosting of obscene videos”
 - Whether the obscene information (subject in the case) is present in the seized hard disk
 - Whether any e-mail ID relating to the hosting of the obscene profile is present
- Questions to be asked in case of “Computer as an Instrument/Repository”
 - What is the operating system of the computer?
 - Which are the user accounts that are present in the computer?
 - What financial applications/software applications are installed in the system?
 - Are there any logs available for these applications?
 - Please provide the list of files/filenames that were recently accessed
 - What external devices (like thumb drives/external hard drives) were connected to the computer?
 - Are there any databases and excel spread sheets available in active or deleted state?
 - Are there any accounting packages/software installed?
 - Are there any encrypted or password-protected files available? If so, please extract the content from them?
 - Are there any pornographic images/videos present in the computer system?
 - Was the system date and time changed at any point of time?

Annexure 5-7: Contact Details of Nodal Officers for Mobile, Email Service Providers

Mobile Service Providers			
Service Provider & Nodal Officer	Contact Details	Service Provider & Nodal Officer	Contact Details
Aircel Mr. GULSHAN ARORA Corporate Nodal Officer	Mobile No. +919716199515 Address: NTC Building, 2nd floor, Plot No.1, Sector - 18, Near Sahrol Mode, Old Delhi-Gurgaon Road, GURGAON - 15. Email: gulshan.arora@aircel.co.in	MTS Capt. RAKESH BAKHSHI- National Nodal Officer	Mobile : +91 9136001400, +91 9818116606
AIRTEL Sushil Kr Chopra Head Nodal Officer	Bharti Airtel Ltd, D-184, Okhla Indl. Area, Phase - I, New Delhi. Email: s.chopra@airtel.in Mobile No: +91 9560049496	RELIANCE C. S. Rao, National Head for Regulatory	Email: cs.rao@relianceada.com Mobile: +91 9844097400
BSNL K S GULIANI, PGM (Regulation) Corporate Nodal Officer	Ph - 011 23734174, Fax - 011 23734097, Email: ddg_reg@bsnl.co.in	TATA B. N. Singh, Senior Manager/ Chief Nodal Officer	Email: b.n.singh@tatatel.co.in Mobile No: +91 9212102880
IDEA Mr. ANIL TANDAN, Corporate Chief Nodal Officer	Idea Cellular Ltd, 5th Floor, "WINDSOR", CST Road, Near Vidyanagari, Kalina, Santacruz (East) Mumbai. Mobile: 919702003300 Office: 919594003300 Email: anil.tandan@idea.adityabirla.com	VODAFONE Padmakar A Naik, Chief Nodal Officer	Vodafone Essar South Ltd, Peninsula Corporate Park, Ganpatrao Kadam Marg, Lower Parel, Mumbai-400013. Mobile: +919820018205; Office: +919619215992 Email: padmakar.naik@vodafone.com Nodaldesk.ild@vodafone.com
C.A.J PRAKASH, General Manager & Corporate Nodal Officer (Operations),	Mobile: 919702003011 Office: 919594003011 Email: caj.pракаш@idea.adityabirla.com	UNINOR Subodh K Singh Senior Manager/ Chief Nodal Officer	Email : subodh.singh@uninor.in Mobile No: +91 9711596720

E-mail Service Providers			
Internet Service Provider Name and Contact Person	Contact Details	Internet Service Provider Name and Contact Person	Contact Details
Yahoo Mail Robin Fernandes Mr Amitabh Das Ms Bhagyesh Gupte	robinfe@yahoo-inc.com amitdas@yahoo-inc.com bgupte@yahoo-inc.com	Rediff Ms D Jyothi Mr Dixon D'Mello	jyotid@rediff.co.in dixond@rediff.co.in
Google Ms Gitanjli Duggal	gitanjli@google.com	Hotmail Mr T Alvares	indiacc@microsoft.com talvares@microsoft.com

Annexure 5-8: Sample Letter to the Service Provider

From: Name of the Investigating Officer or Supervisory Officer (Police Inspector or above) Provide Full address, phone number and Official Mail ID.		Place Date
--	--	---------------

<p>NOTICE UNDER SECTION 91 CrPC</p> <p>To,</p> <p>The Manager ABC Company ISP Division, Mumbai.</p> <p>Sub: Request to furnish the details about the IP address.</p> <p>Ref: Crime Number: xxxxxxxxx u/s xxxxxxxx of ITAA2008 of xxxxxxx Police Station, xxxxxxx City / District</p> <p>With reference to the above cited subject, the undersigned is investigating officer of the criminal case mentioned above. For the purposes of investigation, details of the subscriber and his/her physical address details are required as per below mentioned IP addresses.</p> <p>203.94.218.220 on 07 Feb 2008 at 05:01:24 pm GMT (22:31:24 in IST)</p> <p>Please treat the matter as most urgent.</p>
--

	(Signature of the Investigating Officer or Supervisory Officer Demanding Information)
---	--

Annexure 5-9: General Rules followed by Service Providers to assist LEA

What Information Can you get from a Service Provider?

■ Subscriber Information

- Subscriber information supplied by the user at the time of registration, including name, location, date account created, and services used.
- IP addresses associated with log-ins to a user account.
- Registration IP address data available for IDs.

■ Mail

Any email available in the user's mail account, including IP address of computer used to send email.
Can not search for or produce deleted emails.

■ Instant Messaging System:

- Friends List
- Time, date, and IP address logs for Chat and Messenger use for limited period.
- Archives of Messenger communications may be available on the user's computer if the user has chosen to archive communications.
- Archives of Messenger communications may be stored service providers servers if at least one party to the communication chose to archive communications.

■ Groups

- Member list, email addresses of members, and date when members joined the Group. Information about Group moderators.
- Contents of the Files, Photos, and Messages sections.
- Group activity log describing when members subscribe and unsubscribe, post or delete files, and similar events.

Note: Message Archive may not contain attachments to messages.

What kind of Information is Preserved?

- Preserves subscriber information and log-in IP addresses for periods prescribed or as per company policies.
- A formal preservation notice needs to be sent to the service provider, failing which the information may be deleted after the prescribed period.
- Subscriber information is available as long as the account is active. Inactive accounts data gets deleted as per service providers policies.

Emergency Information Disclosure

Emergencies involving death or serious physical injury can be brought to the notice of the service providers along with justification in the prescribed format, to obtain information regarding subscriber accounts, pending formal legal orders.

Annexure 5-10: Certificates under different Sections of the Indian Evidence Act

Certificate

(u/s 65B (4) (a) of the Evidence Act 1872)

Certified that this electronic record/computer output containing the statement of Shri has been produced from (description of the system) using (description of the output device) and that its contents are true reproduction of the original to the best of my knowledge and belief.

Certificate

(u/s 65B (4) (b) of the Evidence Act 1872)

Certified that this electronic record/computer output has been produced from (description of the system) using (description of the output device) and that its contents are true reproduction of the original to the best of my knowledge and belief

Certificate

(u/s 65B (4) (c) of the Evidence Act 1872)

Certified that this computer output/electronic record has been produced from (description of the system) using (description of the output device) and its contents are true reproduction of the original to the best of my knowledge and belief

Further certified that conditions as laid down in section 65B(2) (a) to 65B(2) (d) of Evidence Ad, 1872 regarding the admissibility of computer output in relation to the information and the computer in question are fully satisfied in all aspects. These certificates are to be issued by a person occupying a responsible position in relation to the operation of the relevant system or the management of the relevant activities, whichever is appropriate.

The first of the three certificates pertains to an electronic record containing a statement This implies that a witness can now be examined through e-mail also, provided a certificate u/s 65B (4) (a) is obtained.

This becomes significant in cases where the witnesses are residing abroad or at faraway places in the country. Another significant amendment has been made in the Banker's Books Evidence Act 1891. Prior to this amendment, Section 2 of this act provided that a copy of a bank statement would be admissible in the court only when it is certified to the effect.

However, since the banks have started maintaining their records on computers, they were finding it difficult to issue such a certificate. Keeping this in mind, the Banker's Books Evidence Act 1891 was amended vide Third Schedule of the Information Technology Act 2000. After this amendment, printouts of the data stored in a floppy, disk, tape, or any other electromagnetic media have also been made admissible provided the same are certified as per Section 2A of this act.

u/s 2A of Bankers Book Evidence Act, 1891

It is certified that the above information is a true extract in printed form of the relevant data created in the usual and ordinary course of business and stored on the hard disk of the computer system installed at Branch of the Bank.

It is further certified that the Access to the Computer System and the date stored thereon is controlled by pre-defined user

permissions exercised through unique user ID and associated passwords;

That physical access to the computer/server room is prevented by locking the server room and the branch after office hours. Detection of any unauthorized changes in the data after day-end and before day-again activity is carried through procedures which are built into the application program. Unauthorized changes in the data during regular working hours are prevented/detected through verification of outputs with authorized inputs;

That in case of system failure, the data is retrieved from the backup kept on tape/floppy/cartridge/hard disk, which is under the control of System Administrator/designated employee of the branch;

That backup is verified by the system during the process of transfer of data to backup media;

That physical and logical labels identify the data storage devices;

That backup devices and media are kept under lock and key which are in the custody of a designated staff member; and

That physical and logical access controls are in place as safeguards against tampering of the systems.

It is further certified that to the best of our knowledge and belief, the computer system that generated and stored this information operated properly at the time of such generation/storage of the date and the printout represents correctly the relevant data.

System Administrator

Branch Manager

Seals of the signatures may also be affixed.

(Name of responsible official)

Designation

***** Please Note:**

The above-mentioned language of the certificate may vary, to some extent, from one bank to another. Therefore, the investigating officers are advised to make suitable changes as per the advice of the system administrator.

If these amended provisions are not adhered to, the electronic evidence collected during the investigation can be rendered inadmissible and evidence which is not admissible is no evidence. Therefore, it is of utmost importance for investigating officers to keep these new provisions in mind while investigating Cyber Crimes.

Glossary of Terms

Advance Fee Fraud

(also known as Nigerian Scam or 419 Fraud)

Fraudsters convince or exploit the greed in victims by promising huge sums of money often camouflaging it as a win from lottery, transfer of treasures or acceptance of business deal. In return for the delivery of promised money, certain amount of money in advance is demanded and, the victim is tricked into paying the amount.

Backdoor

Is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection.

Cyber Bullying

When individuals, specifically when the victim is a child, is threatened, harassed or targeted using communication means like computers and internet or mobile devices it is called cyber bullying.

Cyber Defamation

Defaming an individual or a company's web site thereby causing embarrassment and also loss.

Cyber pornography

Using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Cyber squatting

Preemptively reserving domain names which are trademarks of others.

Cyber Stalking

Defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victim's pet, vandalizing victim's property, leaving written messages or objects.

Denial-of-service attack (DoS attack)

An attempt to make a computer resource unavailable to its intended users.

Distributed Denial-of-Service (DDoS) attack

It is a multitude of compromised systems attack a single target computer, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Email bombing

Email bombing is sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing

Hacking

Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network

Identity theft

Theft of one's identity for illegal use.

Logic bomb

Also called slag code, programming code added to the software of an application or operating system that lies dormant until an event occurs, triggering the code into action such as terminating the programmers employment

Phishing

A form of social engineering attack, wherein sensitive personal information particularly financial information is obtained by the criminals by masquerading as someone trustworthy. For e.g., a mail purported to be from the bank wherein victim has account originates from the criminal seeking details of the sensitive personal information like passwords, credit card details etc.

Spamming

Spamming is sending unsolicited mails and messages.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet.

Vishing

"Vishing" or "Voice Phishing" is the act of leveraging a new technology called Voice over Internet Protocol (VoIP) in using the telephone system to falsely claim to be a legitimate enterprise in an attempt to scam users into disclosing personal information. Government, financial institutions, as well as online auctions and their payment services, can be targets of Voice Phishing

Web jacking

Occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website

DATA SECURITY COUNCIL OF INDIA

A **NASSCOM**[®] Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India

P: +91-11-26155071 | F: +91-11-26155070 | E: info@dsci.in | W: www.dsci.in