CYBER CRIMES

a Practical guide for Investigators

Telangana State Police

Cybercrimes – A Practical Guide for Investigators

B. Ravi Kumar Reddy,
Dy Superintendent of Police,
Cyber Crimes, CID,
Telangana State,
Hyderabad.

Preface

The instances of cybercrime are growing, and the need of the hour of all the Investigating Officers is to equip themselves to investigate the cybercrime.

It is at this juncture, and having put-up years of experience in the investigation of the cyber offences, I wanted to share the practical knowledge to all the investigating officers (IOs) in their efforts to handle the cyber offences.

In this work mostly the practical issues i.e., interpretation of law given under IT Act, line of investigation, evidences to be gathered with a special focus on the standard operating procedure (SOP) for all variants of cyber offences, keeping in view the IOs who do not have requisite technical knowledge are covered. In this book all provisions of Information Technology Act 2000 that are required for Law Enforcement Agencies (LEAs) are incorporated for ready reference.

The standard operating procedure (SOP) or plan of action given for each penal provision pertains to secure basic methods of investigation and collection of basic evidences. However, the investigating officer (IO) as per the requirement of the case that is under investigation may work out on the other leads / clues to detect the case and collect other evidences (oral, circumstantial, documentary, electronic etc) as per the requirement of the case.

I hope this work will definitely useful to the IOs to investigate all variants of cyber offences.

B. Ravi Kumar Reddy
Dy Superintendent of Police,

CONTENTS

***

Cybercrime

The world is more interconnected today than ever before. The use of computers, Internet, mobile phones etc has revolutionised such interconnection of people. Further the dependence of people on the computers and Internet for e-governance, communication, fund transfer, e-commerce etc is growing. This inter connection of population and dependence on the technology, has many advantages, but such increased connectivity and dependence brings increased risk of cyber offences i.e., online fraud, cyber stalking, phishing etc. The scenario is the same in India and thus Indian netizens have become vulnerable to cyber crimes. However the law enforcement agencies (LEAs) in India have been increasing their capabilities and equipped to safeguard people against cyber crime, and thereby striving for a secure cyberspace in India.

What is Cybercrime?

The general meaning of cyber crime is unlawful activities wherein computer is used as a tool, target or both. For instance in a scenario where in 'A' has sent an obscene e-mail to 'B', then 'A' has used his computer to commit an offence. In this scenario computer is used as tool to commit cyber offence. Other scenario wherein 'A' has hacked the computer of 'B', then the target of cyber offence is the computer of 'B'. In the second scenario the computer is a tool on one side and on the other it is target of an offence. The other meaning of cybercrime is criminal activity done with the use of computers and / or Internet.

Classification of Cybercrimes:-

A detailed discussion on cyber crime is covered while discussing on different provisions of Information Technology Act. However, for a broad understanding cyber crimes can be classified as follows

1. **Cyber Crimes committed against persons** due to personal rivalry, vendetta etc:

- Under this category, offences like cyber stalking, circulation of e-mails, creating fake or obscene profiles over social networking media can be categorised.

    - ✓ Cyber staking is repeated use of the Internet or other electronic communication methods to harass or frighten someone.
      Acts like sending abusive, obscene or threat e-mails, posting the identities; his or her name, photo, phone numbers etc of the victims on obscene or x-rated websites.

      Further, acts like creating fake profiles over social networking websites with the identities of the victim like name, photo, phone numbers etc and adding them objectionable content.

2. **Cybercrimes against property** are committed to gain financial benefit.

   Under this category two major streams can be observed basing on the usage of technology. In cases of phishing, debit / credit cards, online cheating cases the usage of technology is minimum but mostly the victim are deceived to divulge information and pay amounts, Whereas, in some other offences like ransomware usage of technology in perpetrating the offence is high. This latter category also considered as cyber crimes against technology

- Phishing
    - ✓ Phishing is to acquire critical information such as Internet banking usernames, passwords often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication i.e., emails

- Debit, Credit Cards Frauds.
    - ✓ Theft and fraud committed using a payment cards, such as credit cards or debit cards. This involves identity theft that is stealing critical information i.e., card numbers, CVV, PIN numbers, card expiry date, name as appears on the card etc pertaining to the Credit / Debit Cards by means of skimming, vishing (Tele phishing) etc

Skimming is the theft of payment card information through skimmer machines clandestinely placed at ATM centres, shops and establishments etc where the cards are swiped for legitimate transactions.

In Tele phishing (vishing) the victims are called over phone by scammers pretending legitimate representative of banks and luring the victims into thinking that they are speaking with a trusted organisation and thus sensitive information such as credit card details are collected and misused.

- Nigerian Fraud / Lottery Scam / Advance Fee Scam.
  - ✓ Online lottery / prize scam is promising the victim a significant share of a large sum of money in the form of prize / lottery, and to get the same the fraudster requires a small up-front payment. If a victim makes the payment, the fraudster goes on requiring further amounts on different pretexts like advance fee, fee to get NOC etc from the victim; the promised prize will never be paid because it does not exist at all.

- Romance & Dating Scam
  - ✓ A romance scam is a confidence trick involving feigned romantic intentions towards a victims, gaining their affection, and then using that goodwill to commit fraud

Cyber Crimes against technology:

It is to be noted that of late these offences are mostly committed for financial gain, hither to youngsters used to commit these offences to get recognition, to expose vulnerabilities etc but this is no more the situation. Particularly, the incidence of ransome ware, defacement of websites a variant of hacking is growing.

- Hacking
  - ✓ Hacking is exploiting the weaknesses or vulnerabilities in a computer system or computer network and gaining access to such systems may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment etc.

- Denial of Service Attack

- ✓ Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users.

- Virus and worm attacks etc
  - ✓ Virus and worm attacks are infecting the computer systems with malware may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment etc.

- Ransom ware
  - ✓ A type of malicious software designed to block access to a computer system until a sum of money is paid.

3. **Cybercrimes against Intellectual Property Rights (IPRs**).

In this offence Intellectual Property Rights are violated and IPR violation is the main offence. In these offences IT Act provisions are invoked along with the provisions of Copy Rights etc.

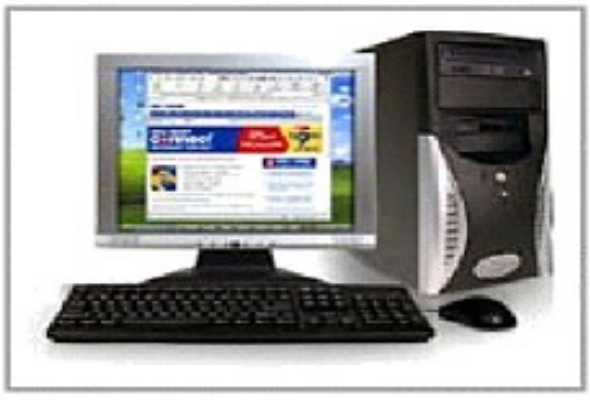
While classifying as above the intent is not to view cyber offences in such a compartmentalised manner, but it only for simple understanding. In Police parlance various offences are grouped under different heads i.e., murder, murder for gain, robbery, theft etc. If the cyber crime is to be looked in that way, the grouping broadly can be one head for each section of law Section 65, 66 r/w 43, 66-B to 66-F, 67 and 67 B Information Technology Act, 2000. The same can be done in other manner also: 1. Source Code Tampering, 2. General Computer Related Offence like hacking, virus & worm attacks etc. 3. Identity Theft cases, 4. Online Frauds, 5. Cases of Obscene Content and 6. Other Cyber Crime Cases.

Computer - Meaning and its main parts.

The important component of cyber crime is computer, though Internet, mobile phones are also other tools of it. Therefore, let us know what a computer is? Computer is an electronic machine with four main parts i.e., CPU, monitor, keyboard and mouse, and it takes input from the user, process it and gives output in a systematic manner. Among the four main

parts, keyboard and mouse are input devises and monitor is the output devise. The Central Processing Unit is in between the input devices and the output device. Central Processing Unit (CPU) is in fact a chasses, a cabinet or a metallic frame on which other electronic items and storage media that are connected or fitted together to have a shape. Such electronic items are mother board, processor, random access memory (RAM), Hard Disk, CD Drive, floppy drive etc. These items are also called as system hardware. Among all these the processor is very important for the point of view of a computer because it has computing ability and all the computations, processes that are performed by the computer are carried out by this item. However from the investigation purposes hard disk is essential because it is a storage device as it holds data or information which is the electronic evidence to establish a cyber offence. Therefore, seizure of hard disk of a computer is primary concern of investigating officer.

It shall also be noted that apart from hardware, computer system will also has software which is a set of instructions that makes a computer work. There are two major types of software: system software and application software. System software provides the basic functionality of the computer. For example operating systems (OSs), device drivers etc, whereas application software is a programme that makes computer to perform specific type functionality. For example MS Office, Excel Spread Sheets etc.



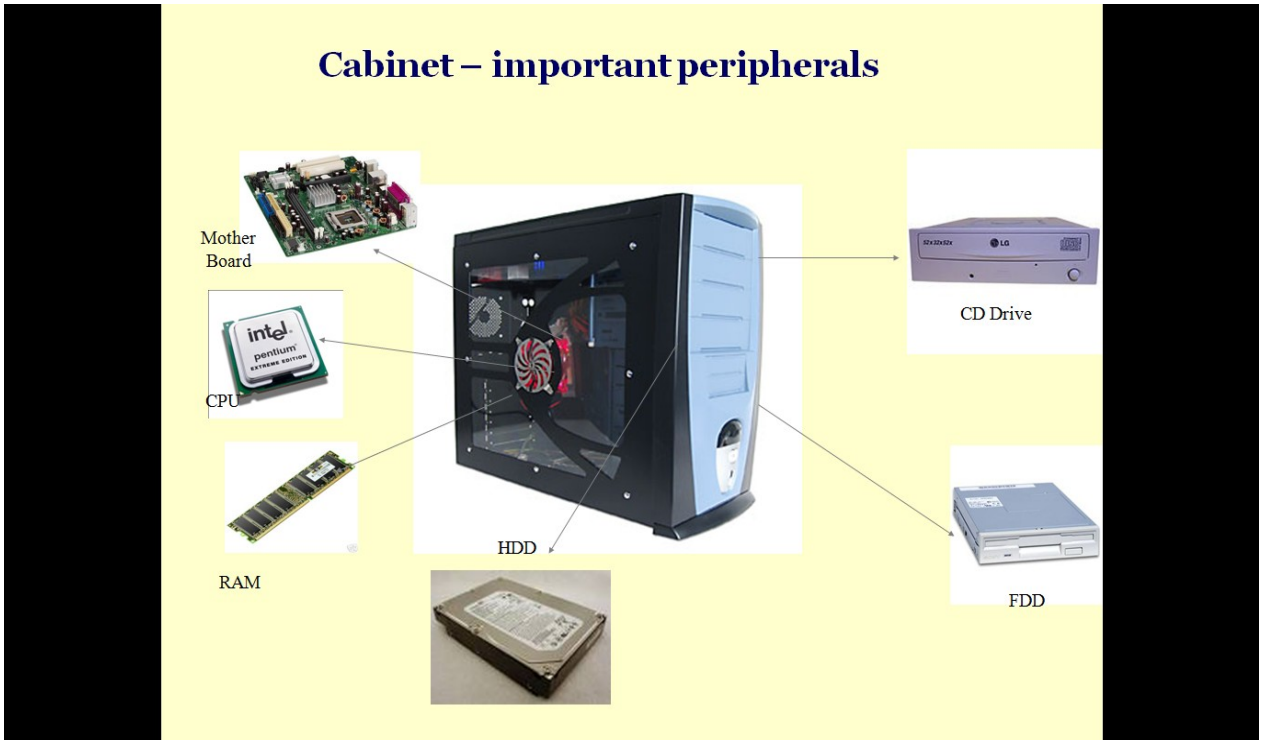
Computer

Cabinet - Central Processing Unit (CPU)

Monitor

Keyboard

Mouse



Other storage media:-

Apart from hard disk there are other storage devices like pen drives, floppy disks, compact disks, mobile phones, SIM cards, memory sticks, digital cameras etc also will have memory that also contain data (electronic evidence). Depending on the requirement of the case, the Investigating Officer shall recover any of these electronic devices if he feels that they contain electronic evidence to establish the case.

Hard Disk

Pendrive

Zip floppy

Mobile phone

DVD

Recovery /Seizure of electronic material objects:-

As per the requirement of the case computers or other electronic storage media will be recovered either from the scene of offence under cover of observation-cum-seizure panchnama / report or from the scene of offence

at the instance of the accused in pursuance of confession-cum-seizure panchanama / report or while conducting searches and seizure.

The main steps that are to be followed in cybercrime scene of offence are:-

- Identification and securing by cordoning the scene of offence.
- Documentation of the scene of offence.
- Collection of electronic evidences from systems that either switched-on or switched-off state.
- Examination of witnesses who are acquainted with the facts of the case at scene of offence.
- As per the requirement of the case making on-sight analysis of material objects, forensic duplication or imaging of the hard disks etc.
- Documentation of evidences that are recovered.
- Packing, labelling and transportation of the evidences that are recovered.

The scenes of offence in cybercrime mostly, but not limited to, are located in the following places.

- Residence.
- Cyber Café
- Offices of organisation, institutions with or without networks

The Investigating Officer while going to scene of offence may be ready with, not limited to, the following

- Two independent mediators, seizure forms / proformas, search warrant.
- For documentation required papers, cable tags, stick-on labels, markers, cameras, notepads etc.
- Required toolkits for disassembling the computers and servers.
- Packing materials like antistatic bags, air bubble tape, hard board boxes.

- If available on-sight cyber forensic analysis tools like EnCase Prtable.

If the scene of offence is a cyber café then IO shall make an effort to identify the computer that was used by the accused by questioning the person who was manning the cyber café, collect CC camera footage/ web camera clippings if so, collect the log register of the Internet users for the relevant period, verify there is any user management software is installed, check for the formatting or replacement policy with regard to the storage devices. If the scene of offence is office premises then apart from the said investigative steps the topology (client –server), many be known, the colleagues of the suspect can be examined to identify the computer used in the offence. If the scene of offence is a home then the type of Internet connection (Wi-Fi/ cable) may be verified.

Another challenge that the I.Os may come across in the scene of offence is the state of the computer whether it is switched-on or off. If the computer is switched-off, to make sure by observing the hard drive and monitor lights, which may indicate that the machine is switched-on. Never switch-on the computer that was already switched-off. Unplug the power and other devices from the sockets. If the computer is switched-on then record what is on the computer screen by making a written note of the contents and photograph the screen. If the screen is blank or screen saver is active, as per the advice of an expert can make small movement of the mouse, get the screen restore then complete the process. If password protected is shown, then take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory i.e., RAM. If such support is not available, then for windows system remove the power supply from the back of the computer, without closing down the programme. However for UNIX

systems gracefully shutting down the system with shut down command is recommended.

The general belief is that in most of the cyber offences if hard disk of the computer is recovered that is sufficient, but it is advisable to seize to CPU/Cabinet because the hard disk would inside safely, and it will also reveal other information for forensic purpose. But what to recover and what is not to be recovered depend on the case that is under investigation. Further to recover hard disk the cabinet / chasses shall be opened and the hard disk shall be carefully taken out and it's description like make, model, serial number, capacity etc shall be noted in the seizure report. Hard disk shall also be carefully packed and preserved. First it shall be kept in anti static polythene cover, then it shall be wrapped in air bubble roll and then it shall be kept in think hard board box. If the investigating officer (IO) does not have the skill to open the cabinet / chasses then it may also not incorrect that the whole cabinet / chasses is recovered so that the hard disk will be there in side of the cabinet safely. In the latter case the description like colour, make of the cabinet shall only be noted in seizure report. If the cabinet is recovered it can be wrapped in white cloth and tied with twine and seals can be put on the knots. It shall be kept in mind that while recording the seizure report complete description of the whole computer like how it is placed, what kind of peripherals like keyboard, mouse, monitor, printer etc are attached to it shall also be noted descriptively in the seizure report and from such state what actually (hard disk or cabinet) has been recovered shall be clearly mentioned in seizure report. The other procedure like following the provisions of Criminal Procedure Code (Cr.P.C), Police Manual etc are all as they are adhered to while investigating the regular conventional cases. The only recommended thing will be care may be taken that at least one among the independent mediators is with computer knowledge so that they will be in a position to identify various electronic objects. Further, any other storage media i.e., pendrive, compact disk (CD) that IO comes

across in the scene of offence and he feels that it also contain evidence relating to the case under investigation, such storage media may also be recovered. If more than one electronic device is recovered, then they shall be allotted a serial number each and all such details are incorporated in the seizure report.

While a pen drive is recovered then also the detailed description of the state, location where it was found may be incorporated in the seizure report. Further its description like make, colour, size shall be incorporated in the seizure report.

Imaging of hard drives and network acquisition:

Imaging of hard drives and network acquisition can be done with the support of experts with required forensic tools. Forensic duplication is also known as disk imaging of cloning or bit stream imaging. In this process a bit by bit transfer of every bit of the hard drive to a new hard drive including free space and slack space.

There will be certain occasions the IO cannot recover hard drive in original because the computer / server may be required for the other public purposes then the process of imaging is done and the original is collected for the investigation purpose leaving the image for the functioning of the computer / server. For imaging special forensic imaging tolls e.g., Falcon Disk Imager and sterile hard drive that has the equal space or higher space that of the original are required. The imaging tool will also generate hash value which is an indicator of data integrity. Hash value is 32 digit alphanumeric value and IT Act allows both MD5 and SHA1 algorithms.

For imaging network drives and file collection network acquisition process is followed. This is done by connecting the evidence computer to the forensic computer via special Ethernet cable called cross over network cable.

	MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity.	
	In cryptography, **SHA-1** (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. However, SHA-1 is no longer considered secure against well-funded opponents. In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use, and since 2010 many organizations have recommended its replacement by SHA-2 or SHA-3. But, the available standard is on date SHA-1	

Recovery of mobile phones:-

A Mobile / Cell Phone is an electronic device by which we can make and receive telephone calls making use of radio signals while moving around a wide geographic area.

The following are different serviced offered by mobile phones and such services provide different kinds of electronic evidences pertaining to the offences committed with the use of mobile phones.

- Make phone calls
- Store contact information
- Send text messages and MMSs
- Make task or to-do lists
- Keep track of appointments and set reminders
- Use the built-in calculator for mathematic calculations.
- Play audio and video
- Take photos & videos
- Play games
- Browse Internet
- Send or receive e-mail
- Get information (news, entertainment, stock quotes) from the Internet
- Watch TV
- Use it for social media communications like Facebook, WhatsApp etc

There will be instances where mobile phones are to be recovered from the scene of offence under cover of observation-cum-seizure panchnama / report or from the scene of offence at the instance of the accused in pursuance of confession-cum-seizure panchanama / report. In such scenarios also care shall be taken while recovering them.

- The mobile phone must be isolated from the mobile network if the phone is switched-on it can never be switched off, it can be kept in flight mode, and Bluetooth, GPRS & InfraRed services are closed, and it can be placed in a shielded secure container or faraday bag so that undesirable changes are not caused, and further, the phone shall be forwarded to the forensic science laboratory (FSL) as soon

as possible for further analysis. If possible the phone may be supplied with portable battery backup keeping the phone in switched-on mode.

- If the mobile is already switched-on then while recovering Mobile Handset, the details like outer appearance, manufacture, model, colour may only be noted in the seizure note.

  It shall be kept in mind that removal of SIM requires removal of battery then the date and time of the device may be lost. This would also be caused it the battery is allowed to discharge.

- If the mobile is already switched off then while recovering Mobile Handset, the details like outer appearance, manufacture, model, colour and IMEI (GSM) / ESN (CDMA) number of the handset may be noted. Further the details of SIM Card like Integrated Circuit Card Identifier (ICCID), name of the service provider that is printed on the SIM and memory card details like manufacture, type (SD / Mini SD / Micro) and capacity of Memory Card may be noted in the seizure note.

- The switched-off mobile phone shall be packed in hard card box while forwarding to FSL so that its safety can be taken care of.

Flowchart in the preservation phase of mobile phone
START
CORDON THE CRIME SCENE
EXCLUDE ALL UNAUTHORISED PERSONS FROM THE CRIME SCENE
COLLECT THE PHONE DEVICES

IF THE DEVICE IS ON PUT THE DEVICE IN RADIO ISOLATED CONTAINER OR PUT IT IN FLIGHT MODE
DOCUMENT ALL THE STEPS
TRASPORT THE CONTAINER / PHONE TO THE FORENSIC LAB
END

	A Faraday bag or Faraday shield is an enclosure used to block electric fields. It is formed by conductive material or by a mesh of such materials. Faraday cages are named after the English scientist Michael Faraday, who invented them in 1836. Play media.	

		
	An antistatic bag is a bag used for storing electronic components, which are prone to damage caused by electrostatic discharge (ESD).	
		

Important do's and don'ts with electronic material objects:-

Once any electronic material object i.e., computer, pendrive, mobile phone etc is recovered it shall never be operated further for the reasons that if the computer is switched on the time stamp / meta data will be altered, if the time stamp on the hard disk is later than the date and time of recovery then it will be fatal to the prosecution case.

	Metadata is data that describes other data. Meta is a prefix that in most information technology usages means "an underlying definition or description." Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier. For example, author, date created and date modified and file size are examples of very basic document metadata. Having the abilty to filter through that metadata makes it much easier for someone to locate a specific document. In addition to document files, metadata is used for images, videos, spreadsheets and web pages. The use of metadata on web pages can be very important. Metadata for web pages contain descriptions of the page's contents, as well as keywords linked to the content. These are usually expressed in the form of metatags. Thus, it is "data [information] that provides information about other data". Three distinct types of metadata exist: descriptive metadata, structural metadata, and administrative metadata. Descriptive metadata describes a resource for purposes such as discovery and identification. It can include elements such as title, abstract, author, and keywords. Structural metadata is metadata about containers of metadata and indicates how compound objects are put together, for example, how pages are ordered to form chapters. Administrative metadata provides information to help manage a resource, such as when and how it was created, file type	

	and other technical information, and who can access it.	

Electronic MO – Handling:-

With regard to the electronic MO an important do is, when ever any electronic material object is recovered it may be forwarded to forensic science laboratory (FSL) for analysis and report. The important reasons for forwarding electronic MO to FSL are as follows:-

- The data in the electronic MOs i.e., hard disk, pendrive may be permanent to some extent, but it is not permanent for ever because accidentally the data may be lost. If the MO is fallen to the ground, moisture, strong magnetic field, high voltage electricity and extreme temperature may cause damage to the contents. Sometimes even the static current of human body may cause damage to the sensitive parts of the hard disk. While handling the hard disk care shall be taken and it shall be held on its sides. The printed circuit board shall not be touched with hands or tools. Further, hard disk shall not be dropped, bumped or shacked. Care shall also be taken that water or coffee etc liquids are not fallen on to it, it shall not be exposed to the strong magnetic field, high voltage electricity or extreme temperatures.
- The data or contents of the electronic MO are not visible for a normal view. Hence, if it is forwarded to an expert along with a letter of advise or forwarding note, then the expert will be in position to open the data or contents of the electronic MO with special forensic tools, analyses the contents and provides expert report /opinion.
- The presiding judicial officer relies on the expert's report about the electronic evidence and further the prosecution cannot expect the presiding officer to open the contents of an MO and perceive for himself.

Thus for the reasons sated above it is recommended that whenever any electronic material object is recovered it shall be forwarded to FSL for analysis and report.

Electronic MO - Letter of Advise (Forwarding Note):-

In the letter of advise (forwarding note), some general questions like whether the material object is working condition or not, the data that is recorded on to such material object is recorded in normal course of activity? etc may be asked. Then specific questions may be raised. If the material object is recovered in a case of obscene e-mail then question may be raised for analysis of disk memory for retrieving and furnishing the contents of the alleged e-mail. In a fake Facebook profile case the associated contents of such profile can be collected.

If a mobile phone is forwarded the questionnaire may include the analysis of phone, SIM and memory card memory and for retrieving SMS and MMS messages, recovering call logs, recovering contact lists, pictures, dialled numbers etc., identification of the IMEI, IMSI, ICCID numbers and internal contents etc.

With advent of smart phones the questionnaire that may be raised may include for recovering web browsing activity, emails, chat messages, social networking service posts, wireless network settings including information about previously connected WIFI access points etc. The following are some model questionnaire that may be asked in a case of harassment through WhatsApp chat and calls.

1. Whether the MO (mobile phone) is working condition or not?
2. If so whether the contents / data recorded is in normal course of functionality or not
3. The memories of phone and SIM card etc may be analysed and all WhatsApp messages /chat (text, images, videos etc) that were sent from mobile No 1234567899 (Accused) and to the mobile number 9987654321 (Victim) may be retrieved and furnished.

4. The memories of phone and SIM card may be analysed and data / logs pertaining to WhatsApp calls from mobile No 1234567899 (Accused) and to the mobile number 9987654321 (Victim) may be retrieved and furnished.

5. Analyse the settings of the MO and any information to establish that the mobile number 1234567899 of accused is blocked on the MO may be furnished.
6. The IMEI, IMSI and SIM numbers of the MO may be identified and furnished.

The I.Os shall take special care while transporting the electronic material object to the FSL. Any electronic material object shall be transported through a special messenger who also may be made to understand that the M.O is sensitive and shall never be exposed to moisture, heat, high voltage electricity, any magnetic field and high sound in the transit.

Information Technology Act 2000.

Information Technology Act is a central Act, enacted by Parliament of India with main objectives "*to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto".*

Information Technology Act has provisions related to Digital Signature, Certifying Authorities etc which may not be quite relevant for the routine functioning of LEAs; however different offences are covered under chapter XI and these are discussed in this book, from the perspective of LEAs on

aspects like interpretation of law, application of law, line of investigation, basic evidences to be collected to establish the case etc.

IT Act – Important Definitions:-

The IT Act has certain definitions incorporated under section 2 which make clear the meanings of the terminology used therein. Among them the following are more relevant for the Law Enforcement Agencies.

(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 through— (i) the use of satellite, microwave, terrestrial line or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

(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;

(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;

The following are the penal provisions that are listed in chapter XI of Information and Technology Act

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 programme, 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.

When the ingredients of the section are analysed it become clear how to make out a case under this section? The culprit shall have mensria (*knowingly or intentionally, and* should 'conceal' meaning to hide or to take away from the view or steal, or 'destroy' meaning causing destruction or deletion, or 'alter' meaning to make changes, and thus the culprit with mensria shall *conceal, destroy or alter any 'computer source code'* then it is an offence under section 65 IT Act. Source code means *'the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form'.* There are many computer programming languages like C, C+, Java, .Net, ASP etc. A set of commands written by using one of these computer programming languages is computer source code.

To make out a case under this provision the typical narration of the complaint will be as follows; "*To SHO, …PS, Sir, I have XYZ Company and I have hired around 100 employees. We all divided into groups and developed a computer application with name 'ABC' by using C+ language working for last one year. While this is os we came to know that one of employees resigned from the company and while leaving he has take the programmes developed at our company and made alterations and claiming as if he has developed on his own. With that I have suffered loss. Hence it is requested for taking necessary action".* When these kinds of complaints are reported then the section applicable to register a case is section 65 Information Technology Act.

Section 65 - standard operating procedure (SOP)

The standard operating procedures (SOPs): During the course of investigation the following verifications shall be made and electronic evidences shall be gathered.

- The foremost thing shall be establishing the ownership of the complainant on computer programme (source code) that was allegedly stolen and/ or tampered.

- Ownership on the source code can be established by verification that whether the complainant has Copy Rights on that programme or not, if yes ownership is established with such copy rights, if not the computer programme life cycle shall be verified.
- Computer programme life cycle is the course of development of the application over a period of time. While developing coding of a programme employees would be divided into groups, and some groups would develop coding and such different pieces of coding (modules) may be integrated and lastly tested. This course of development of a programme may be written in the form of comments which are facilitated by any programming language.
- Ownership on the source code can also be established with the technology that was used while developing a software prgramme. This means what is the programming language i.e., C or Java or ASP that was used in the development of programme. If the complainant's application is in ASP and the suspect has developed his programme in different programming language like C++ then the programme logic, may be identified. If the technology and programme logic are different then case may not be made out.
- What kind of front end? What is the backend data base can also be verified.
- Further the Investigating Officer can also recover supposed to be the original programme from the complainant, and he can also recover the alleged stolen and tampered version from the alleged accused, and forward both to an expert for comparison and report.
- On getting report and if the report confirms the original and tampered version of accused/ accused's company then the case is established and accordingly necessary further action can be taken against the alleged accused.

- Further in these cases the fact, as to, how the source code was taken away shall also be proved. Whether it was transmitted out through e-mails or copied on to portable media may also be verified and such electronic portable media may also be recovered in pursuance of the confession of the accused under the cover of a mediator report. If the source code was sent out through e-mails, then the connected e-mail IDs and their association with the suspected people will become evidences to established the case.
- The recovered electronic portable media shall also be forwarded to the Forensic Science Laboratory (FSL) under a Letter of Advise and an analysis report may be obtained.

  If any laptop was used for stealing the source code such laptop shall be recovered at the instance of the accused or otherwise. The laptop shall be forwarded to FSL for analysis.
- If stealing of the source code is by former employees of the complainant's company then the appointment letters, non disclosure agreements (NDAs) etc may also be collected to prove that the accused was in fact worked in the complainant's company. To this effect examination of HR (Human Resource) Manger is required.
- Examination and recording the statements of the complainant, and also the colleagues like team leads, team members of the accused persons shall also be done.
- Certificate from Authorities of Copy Right, certificates of registrar of companies (ROC) depending on the requirement of the case can also be collected.

Thus the case can be established with required oral, circumstantial, electronic evidence.

Section 66: Computer Related Offences

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

This means that section 66 is penal provision and 'acts' or 'offences' are listed under section 43 of IT Act, under which the following different 'acts' are listed from 'a' to 'j' sub-sections. It shall be noted that the term 'computer related offences' given under section 66 IT act is vary vast. In order to classify an offence under this section, it is necessary to establish the culprit with dishonest and fraudulent intent had caused destruction, disruption, damage, deletion, denial, concealment, tampering, manipulation,, stealing, alteration, diminishing the value of the information that is in the computer or computer resources.

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 -

(a) accesses or secures access to such computer, computer system or computer network or computer resource

(b) 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;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised 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 there under,

(h) charges the services availed of 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,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Under provision 43, sub-section 'a' cases of hacking (unauthorised access), website defacement are covered. Under sub-section 'b' downloading, copying protected information are covered. Infecting a computer with virus or computer contaminant is punishable under sub-

section ‘c’. Similarly different general offences that are related to computers are covered.

"Computer Contaminant" means any set of computer instructions that are designed - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

"Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

It is important to note that the term ‘hacking’ per se is not defined under Information Technology Act, nevertheless, the section 66 read with 43 sub-section (a) is the relevant provision for authorised access which is otherwise hacking.

A case of hacking – standard operating procedure (SOP):-

The following standard operating procedures (SOPs) may be followed in a case of hacking which is un-authorised access of a computer resource.

- As per the ingredients mentioned under section 43 sub-class ‘a’, if any person without the permission of the owner or without the permission of the person who is in-charge of the such computer, accesses such computer then it is an offence punishable under section 66 I T At. Therefore this section is applicable for unauthorised access which is otherwise known as ‘hacking’.
- To establish un-authorised access the computer system logs may be collected. Computer system logs may include web logs, server logs, file transfer protocol (FTP) log, firewall logs. These logs may be analysed and the IP Addresses that are associated with the un-

authorised access may be identified and collected on a compact disk under the cover of mediator report. This analysis can be done with the help an expert and such proceedings may be recorded.

- The concerned people who manage the server / computer that was hacked need to be examined and their statements are to be recorded incorporating the facts: what were the security measures on place, when the hacking was realised? Etc

- After identification of the suspected IP Addresses, the source of such IP Addresses can be traced with the information provided by the Internet service providers.

  The IP Addresses may be searched for lookup on websites like www.apnic.net, www.domaintools.com, www.whois.net etc the IP Address assignee, which can be usually am Internet Service Provider (ISP) information may be ascertained.

  In the next step by writing or by sending an email request to the ISP the end user details of the IP Addresses may be collected and thereby the name and address of the person who has made unauthorised access is known.

- Thus the suspect can be identified and he may be questioned and if he admits, his confession may be recorded before mediators and in pursuance of such confession and, at the instance of the culprit the tool of offence which could be a computer, laptop or mobile phone that was used for committing the offence may be recovered.

- The recovered tool of offence (computer, laptop or mobile) may be forwarded to the Forensic Science Laboratory (FSL) under a Letter of Advice with a proper relevant questionnaire and a analysis report may be obtained.

  The specific question, to the expert in these cases is to analyse the MO for the presence of an IP, any tool of hacking or any linking

electronic evidence between the hacker computer and the target computer and to retrieve the same and furnish.

- In these cases the IO can also recover the gadget i.e., data card etc that is used by the accused, to access Internet. Examination of the nodal officer of the ISP is also required.
- Thus the case may be established with proper documentary (electronic), oral, circumstantial, scientific evidences.
  - Cases of website defacement will also come under this category, hence a similar line of investigation may be followed to trace the culprits.
  - If the IP Address leads to a foreign country the procedure of issuing Letter of Request (Letter Rogatory) as per section 166-A Criminal Procedure Code and the guidelines issued by Central Bureau of Investigation (CBI) at http://cbi.nic.in/interpol/invletterrogatory.php shall be followed to secure information / evidences from other countries.

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 two three years and with fine.

Struck down of Section 66-A by the Hon'ble Supreme Court of India:-

It shall be noted that this **section 66- A IT Act was struck down by the Hon'ble Supreme Court of India** in the judgement dated March 24, 2015 in a batch of writ petitions filed before it for the reasons that the terminology "grossly offensive", "menacing" "annoyance," "inconvenience," or "obstruction" given in the section is vague, the section is coming in the way of freedom of expression provided by Constitution of India.

The back ground of the issue is that two girls were arrested by the Mumbai police in 2012 for expressing their displeasure, by posting their remarks over their facebook profiles at the bandh called in the wake of Shiv Sena chief Bal Thackery's death. The arrested women were released later on and it was decided to close the criminal cases against them, yet the arrests attracted widespread public protest. It was felt that the police has misused its power by invoking section 66A inter alia contending that it violates the freedom of speech and expression. The apex court judgment came on a batch of petitions challenging the constitutional validity of

Section 66A of the IT Act on the grounds of its vague and ambiguous and was being misused by the law enforcing authorities.

Struck down of Section 66-A – Effects, and alterative provisions:-

Thus, in view of the Apex Court's verdict the Police shall not register cases under section 66- A IT Act. Then the question comes, what to do if such cases are reported attracting the provisions given in 66-A IT Act. For instance a female approaching the police with a complaint that a fake facebook profile was created with her identities like photograph, her name, phone number or something objectionable content is posted against her in the social networking media, and such contents have caused her insult, annoyance or harassment. In these situations the police can look for other sections in IPC or in any other special act. For the contentions above relevant section IPC may be 354-D which can be invoked for causing stalking, harassment by online means through the use of computer resources and also physical harassment despite the victim resists. Further section 509 IPC can also be invoked. According to the situation 354 –A IPC sexual harassment (making sexually coloured remarks, shall be guilty of the offence of sexual harassment) may also be relevant.

It also be noted that hither to the Police used to invoke section 66 – A IT Act for communal sensitive remarks and degrading the gods or goddesses of the different religions under this provision. After this section is stuck down the Police may have to look for the provisions 153 –A and 505 (2) that are relevant under Indian Penal Code as per the situation, the contents of the complaint and nature of the offence.

Social networking media refer to the mode of communication among people on the cyber space with use of Internet. These include social media networking sites (Facebook), micro blogging sites (Twitter), video sharing websites (Youtube), wikis I Wikipedia) etc.

The following different variants of offences may be reported with regard to the Facebook.

- Creating impersonating profiles with the identities like name, photographs of the victim.
- Sending and posting obscene content.
- Hacking of a profile.
- Sending obscene and derogatory content to a profile.
- Posting material which hurts the feelings and sentiments of a community.

Misuse of social networking media – standard operating procedure (SOP):-

The line of investigation shall be with an aim to trace the culprit and to gather sufficient electronic evidence to establish the case, and to that effect the standard operating procedure given below may be followed.

- The contents of web pages (facebook, youtube etc) along with the URL (universal resource locator) where the alleged contents are existing may be taken as computer prints, before independent mediators so that the authenticity of existence of web contents can be proved. With this the Investigating Officer will be in position to prove that the fake profile or web pages had in fact existed at the

time of offence. Otherwise, the fake profile or web pages may be deactivated / deleted by the culprit or someone else fearing legal action. In case of the Facebook profile has been deleted or deactivated at the time of complaint and if at all the victim has taken prints while it had existed such prints may be collected.

Further the people who have seen such web pages or people who have received friend requests from such fake facebook profiles may be examined and their statements are recorded towards corroborative evidence.

If the harassment is through e-mails the prints of all such e-mails shall be collected towards documentary proof.

Further, if the harassment is through SMS, MMS or WhatsApp chats then a mediator report may be drafted and the description of the alleged contents may be recorded. The messages can also be collected in the form of prints by connecting the mobile to the computer or with PC suite software e.g., Nokia PC Suite, Kies, Itunes. But care shall be taken that he contents are not deleted accidentally by the IO or by the victim. If the victim is ready to hand over the mobile phone then it can be recovered before mediators and can be forwarded to FSL for further analysis.

The IO can also collect the CDRs of the mobile numbers of the victim or the accused so that further corroboration for sending the messages (SMS, MMS or harassment phone calls) may be secured. Further the customer application forms (CAF) and associated address and ID proofs of the mobile numbers of the victim or the accused may also be collected from the mobile service providers so that the ownership and possession of them is established. If the mobile numbers (SIM) are not issued in the names of the victim ot the accused the person in whose name SIM were issued may be examined as witnesses.

- The next step in the course of investigation is securing all the relevant information including IP Addresses, mobile number if any, alternate e-mail account that are associated with alleged profile or web pages from the social networking service provider for example www.facebook.com .

  At this stage the service provider www.facebook.com, if the offence is through facebook profile or e-mail service provider like Gmail, shall be contacted by sending a letters / notices (PDF Documents) through e-mails and relevant information (registration information and IP address track shall be collected. To secure such information IOs can take the help of Cyber Crime Police. While contacting the Cyber Crime Police the IOs shall identify the web address / ID of the profile that may be traced. The web address / ID is uniform resource locator (url) of the profile to be traced. The example of the same is as given under.
  https://www.facebook.com/profile.php?id=100008532245343
  https://www.facebook.com/abcxyz
  The information that is furnished by the service provider may contain phone number that was given when the profile or E-mail ID was created, secondary e-mail and IP logs which can be used to work out further leads and clues.

- During the course of further investigation the accused can be traced through the IP Addresses and other information that was obtained from the service provider and the computer or mobile phone or any other electronic device that was used in the offence can be identified.

- Thus by working out relevant leads, clues both electronic or circumstantial the offender can be identified. Then the culprit may be taken into to custody and on questioning his confession may be elicited. At the instance of the accused and in pursuance of the

confession of the accused the tool of offence i.e., computer or mobile phone or any other electronic device may be recovered.

After the accused is caught, and the tool of the offence is a mobile phone then ascertain the password, PIN or pattern if the phone is locked, recover the phone before the mediators at the instance in pursuance of the confession of the accused, record the navigation path of the alleged contents from the sent items etc

- The process of gathering of electronic evidence will not stop there. The tool of offence i.e., computer or mobile phone or any other electronic device shall be forwarded to Forensic Science Laboratory (FSL) along with correctly drafted Letter of Advise, basing on which the expert will analyse the materiel object and retrieve relevant electronic evidence i.e., contents of profiles, web contents etc and furnish report that can be furnished to the Court to establish the case.
- The statements of service providers (Nodal Officers) who furnished IP Address logs and user details of IP addresses may be recorded and required certificate under section 65-B Indian Evidence Act may be collected.
- Therefore the point to be noted here is that though the offence is under the provisions of the IPC the evidence to be gathered can be oral, circumstantial, documentary and electronic.
- Further, these offences are usually committed by known people to the victim with personal grudge and therefore the oral or circumstantial evidence related to the personal rivalry between the victim and the accused may also be gathered, apart from the electronic evidences as narrated above and thus the motive is also established.

What is the URL? URL stands for Uniform Resource Locator, and is used to specify

addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files). URLs have the format: protocol://hostname/other_information.

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.

This is provision is parallel to 411 IPC as per which receiving stolen movable property knowing that they have been stolen is an offence, whereas as per section 66 – B receiving stolen computers or mobile phones knowing that they have stole is an offence.

However, it shall be kept in view that the section does not confined to the physical theft, even if the resource of the computer i.e., software is received by anyone with knowledge that it was stolen then also the section applies. Thus, this section has the relevance for violation of intellectual property rights.

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.

This is a very important provision provided by Information Technology Act. Hitherto, what we have seen is theft of movable property. Now this section provides punishment for stealing identities. Then, what are identities; one's user names, passwords, card pin numbers etc are identities. If someone fraudulently or dishonestly make use of some such identities then it is an offence.

Under this provision cases related to phishing, tele-phishing (vishing), misuse of bank accounts online, Debit, Credit Card misuse etc.

Phishing is to acquire critical information such as usernames, passwords, and credit card details often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. A typical narration of complaint will be that the victim is having a bank account, he is getting an un-solicited e-mail with a similar web page of the bank where the victim has bank account, and in the e-mail it is mentioned "Dear valued customer on our routine check up we found something wrong with your account and you are requested to revalidate the account", underneath a hyperlink is given. If gullible victim believe it and click on the link which will open in a new page the victim is made to enter critical information of his online bank account like user names, passwords etc. The gullible victim think that the given information will go to the bank but in fact it will land in the hands of online fraudster. Once the fraudster knows the Internet banking user name and password with in no time he will transfer amounts that are left the victim bank account.

Another variant of phishing is the victims get e-mail pretending from Income Tax Dept with a e-mail content " Dear Values tax payer, there is tax refund for you and you are requested to furnish your bank details to credit you tax refund to your account". The fake e-mail will have national emblem on it. If Gullible people fall prey to such e-mail and click on the link it will seek critical information of his bank account then people will be defrauded.

The registration of case can be under 66 – C IT Act and relevant other provisions of IPC. In these cases there is deception, wrongful loss to the victim and wrongful gain to fraudster; hence section 420 IPC can be invoked. Further an e-mail, which is an electronic record, pretending Income Tax Dept is sent that means a fake electronic record (document) is produced as if genuine to deceive the victim and hence section 471 IPC can also be invoked. Thus the registration of the case can be under section 66-D IT Act, 420 and 471 IPC. However once an IT Act provision is invoked in the FIR then as per the legal stipulation the investigation of such an offence shall be of and above the rank of Inspector of Police.

For instance a phishing case committed pretending Income Tax Dept can be discussed in detail, focussing the line of investigation, evidence shall be gathered from FIR to charge sheet. A typical complaint will be as mentioned below. The section law applicable are 66-C IT Act, 420 & 471 IPC.

"*To*
The SHO,
……Police Station.
TS State.

Sir,

I submit that I have ICICI Bank account bearing number A/c 123456789 and I have Internet Banking Facility and Debit card on my account. I do all my transactions from my house where I have internet connection. I have my e-mail ID abc@xyz.com and mobile number 9848012345 that are associated with my bank accout.

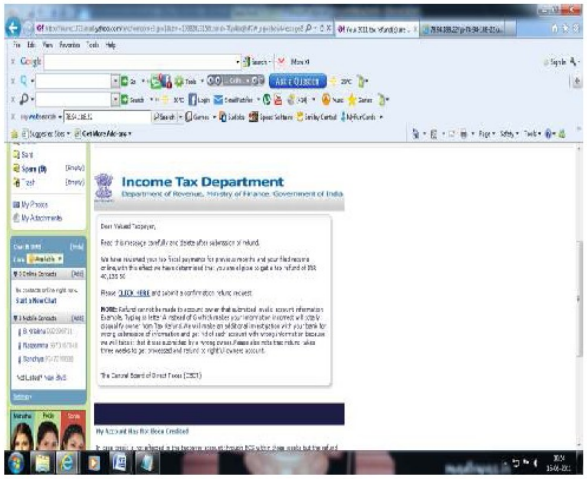
While this is so on 01-01-2015 I received an e-mail to my e-mail ID from an e-mail ID as if from Income Tax Department mentioning that that I have tax refund to claim and a link is given below. Believing it to the true I clicked on the link given there and it lead me to a new webpage where I was made to enter my bank account number, Internet user name and password, my mobile number that is associated with my bank account etc. After I entered all those details when I checked the page went blank.

But to my surprise an amount Rs 90,000/- was deducted from my bank account such mobile alerts came on to my phone. Immediately I realised that these transactions are being done without my knowledge and contacted the bank authorities who informed that three laptops were purchased online through e-Bay a online shopping website.

Thus I suspect that some culprit in the name of Income Tax Dept sent false e-mail and deceiving me collected by bank account critical information and misused my bank account details and caused my wrongful loss of Rs 90,000/- .

Therefore I request that necessary action may be taken in this regard

Sincerely



Xxxxxxx

"

Phishing - standard operating procedure (SOP)

In the line of investigation the following standard operating procedure (SOP) may be followed:-

- The Investigating Officer shall react fast. He shall collect the print of the e-mail that the victim has received before independent mediators or under the cover of a certificate issued under section 65 – B Indian Evidence Act by the victim towards documentary proof that such deceptive e-mail was in fact received by the victim.
- Then the I.O shall contact the concerned bank to know the route of the amounts and to that effect shall collect the transaction statement of the bank account for which the misused debit card was used.
- The IO shall also collect information about the goods (laptops, mobile phones etc), or services (mobile recharge, booking tickets etc) purchased and the amounts were used. If the amounts were used to buy goods online, then it shall be known as to what was the merchant website? And what was shipping address to which the delivery of goods was made? Further it shall also be known which the courier service was? And what are the IP Addresses that are associated with the fraudulent transactions.
- Physical verification of the addresses that were collected for the IP Address end user, shipping address of the goods shall be made.

  By working out these leads the case can be detected or can be taken to a logical conclusion.
- Once the fraudster is identified, under his confession the tool of offence which may a desk computer / laptop shall be recovered and

it shall also be forwarded to the FSL for the purpose of analysis and to know whether the deceptive e-mail that was sent to the victim is available in such materiel object or not.

This is the basic investigation that can be conducted in a case of phishing, however depending on the case the line of investigation and the leads to be worked out may differ

Cases of Debit & Credit Cards misuse:-

Further under this provision cases of Debit & Credit Cards frauds can also be investigated. Debit /Credit card is a plastic card issued by banks. These are accepted as legal tender at ATM centres and shops & establishments. Debit & Credit Cards misuse cases include skimming and cloning, shoulder surfing, swapping of cards at ATM centres etc.

Skimming and cloning is that the card's critical information is collected by a small gadget namely a 'skimmer' that may be installed at the ATM machine's slot and pinhole camera is fitted above in the ATM centre. These will be deceptively placed to collect the card critical information from the magnetic strip of the card and the PIN numbers while they are pinned by the user. By using such fraudulently gained information new card which is called 'a clone' will be created and such counterfeit cards are misused. In these cases the Card will be with the victim but amounts are drawn from a different place.

Skimmers vary in size and they will be in the size; they will be in the size of a cigarette box but modern skimmers are so small in size they can be fitted into the slot of an ATM where usually the cards are inserted while drawing amounts. Skimming may also occur at retail outlets – bars & restaurants, petrol filling stations etc.

Skimming and cloning – The line of investigation:-

- The line of investigation in these cases shall be finding out the place of compromise of the card. That means knowing from the victim, before the fraud has happened, what was his genuine transaction? Place of compromise is where the critical data of the card was stolen by the fraudster, before it was misused.
- Once this is known an effort can be made to work out leads at the place of compromise. The place of compromise can be an ATM centre or a place where the victim made a purchase of goods at any shop. If such place is identified then it can be visited and an effort may be made to collect CC camera footage, verification can be made for the presence of any skimming gadget etc.
- The transaction statement of the bank account of the victim can be collected and the ATM centres from which cash withdrawals are made can identified basing the ATM centre ID and from such an ID further the physical location of the ATM centre can be identified and further by contacting the concerned bank nodal team CC camera

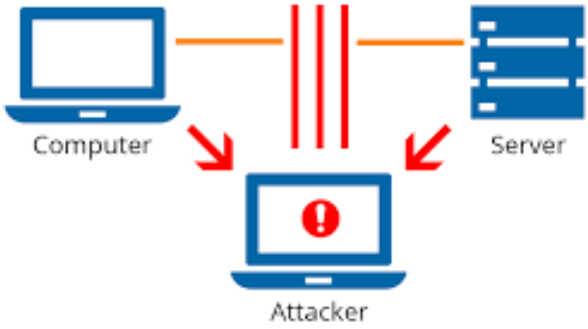
footages of the culprits can be identified, and thus efforts can be made to identify the culprits.

Sometimes the cloned cards are used for purchasing goods at shops and establishments, and hence such shops and establishments shall be identified. Those shall be visited and the sales people who allowed the un-authorised transactions may be examined for working out leads / clues to identify the culprits.

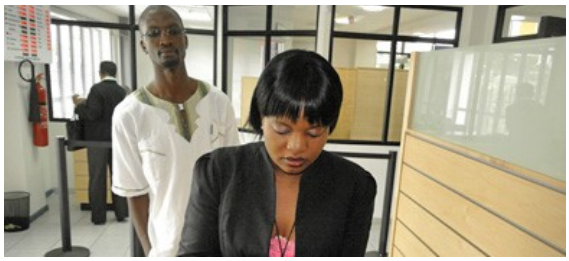
- Thus in these cases the identification of the place of compromise and place of withdrawals of the amounts or places (shops) where the card is being swiped is very essential to work out clues and leads towards detection of the case.

Man in the middle attack:-

The card critical data can also be compromised by `**man in the middle attack'** which means that the victim may be making purchases of goods or services online on an unprotected website then the critical data that will be transferred online in an unencrypted way which may be tapped by any hacker who reads the data in the mid way. This is further elaborated that, while online financial transactions are made the card numbers, bank account numbers, passwords, pin numbers, CVV numbers etc will traverse from the victim's computer to the bank server and also to the merchant's server. During such transmission critical data may be captured and by using so collected information a new card (a clone) may be created and misused.



Shoulder surfing is also committed at ATM centre. When the victim visits and while doing his genuine transaction the fraudster looks at the victim's card and notes down the card number and PIN number etc and by using such fraudulently gained information online purchases can be made.



Shoulder surfing – line of investigation:-

In these cases also the place of compromise may be identified, at such place the CC camera footages may be collected. In these cases usually goods or services will be purchased online. Thus, the details of such purchases including the shipping addresses can be secured and efforts can be worked out to trace the culprit.

Further in all the case wherein the goods (laptops, mobile phones etc), or services (mobile recharge, booking tickets etc) were purchased online, the IP Addresses along with date and time can be collected from the bank and also from the merchant website and efforts can be made to the trace the culprit by finding out the user details of the IP Addresses from the concerned Internet service provider (ISP)

Tele phishing or vishing is a fraudulent technique where in the victim receive a phone call from a stranger who pretends to be bank employee and further deceptively states that the account of the victim is being linked to ADHAAR, and for doing so collects details of card including CVV number from the gullible victim. The culprits further deceives the victim saying that while his account is connected to ADHAAR a code is generated and the same reflected on to the mobile number of the victim and subsequently calls the victim secure the one time password (OTP) from the victims. The victim will realise the fraud only when he receives mobile alerts for the amounts deducted from his bank account. By the time the illegal transaction are completed.

Thus vishing is a kind of social engineering technique of convincing people to reveals confidential information of the debits cards and by using same fraudulent transactions are made.

In these cases the section of law that is attracted for issuing FIR is 66-C IT Act and 420 IPC.

Tele phishing or vishing – The line of investigation:-

- In these cases an important lead is mobile number from which the victim was called when he was deceived. For such mobile number call data records (CDRs) can be secured, and further customer application form (CAF) along with the address and ID proof that were furnished at the time of getting SIM can be obtained and efforts can be made to work out clues and leads to trace the culprit.
- In addition to this, what were the service or goods that were purchased and from which website (merchant website) such purchases were made can also be identified from the transaction statement of the bank account of the victim, and by contacting the merchant website the shipping address i.e., delivery address of the goods can be known and thus efforts can be made to trace the fraudster.
- Usually the misuses of debit card in these cases will done by purchasing goods (laptops, mobile phones etc), or services (mobile recharge, booking tickets etc) online. Therefore, if the IOs can act fast and alert any of the organisations i.e., bank, merchant website, payment gateway, acquirer bank etc the illegal transaction can be aborted and charge back (restoration of the amounts) can be secured to the victim.
- Further the IP Address corresponding to the online transactions can be collected from the bank or merchant website (web stores). The user details for such IPs can be collected from the ISP and basing on the same the address of the fraudster can be secured.
- Physical verification of the addresses that were secured for the subscriber address of SIM, shipping address and IP end user shall be made.
- If mobile recharges are made the details of the numbers foe which recharges were made can be ascertained and their subscriber details be known from the mobile service provider (MSP and such addresses shall be verified for knowing where they made the recharge etc details.

- Verification with courier service boy who delivered goods at the shipping address will also be a good lead to detect the case.
- IO shall not forget to examine who ever may be the circumstantial witness i.e., the representative of bank, merchant website, courier service so that the case can be established with proper orall and circumstantial evidences.

Further other types of card frauds may be lost and stolen card frauds: These types of frauds happen when the card is lost and lands up in the hands of another person who can misuse it or the card is stolen by a fraudster and subsequently misused. Cards are also stolen at ATM centres. The fraudster in the pretext of helping the victim while he draws the amount may take away the card of the victim and hands over a duplicate card to the victim.

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.

Under this provision case of online cheating can be registered. These may include the following

Nigerian Fraud / Lottery Scam / Advance Fee Scam: These scams are called Nigerian Frauds because in most of the cases nationals of Nigeria will involve. They are also called advance fee scams because in most of these offences a demand for advance fees will be there.

In these cases the course of offence will be gullible victims will receive unsolicited messages to the their mobile phones or e-mails are received to their email IDs mentioning their mobile numbers or e-mail ID have won million of dollars or pounds in Microsoft, International Cricket Cup draw etc, and victim are asked to contact to their e-mail IDs. If gullible people fall prey to these temptations, and then gradually amounts are asked to pay into bank accounts furnished by the fraudsters on different pretexts like advance fee, processing fee, transfer charges, fee to get no objection certificates (NOC), to get money laundering clearance, Income Tax Dept, etc. The fraudsters pretend that they are ambassadors, diplomats. There are instances where in the fraudsters come to the houses of the victims and hand over a suite case / trolley bags that contain a metallic chest. The incoming fraudster will open the chest and take out bundles of black papers and state that due to security reasons the prize amount is turned black and parcelled, and if the same is cleaned with a special chemical the notes will come to original form. To buy the chemical again amounts are demanded. Ultimately the promised prize will never be paid because it does not exist at all.

On such complaints cases can be registered under the section 66-D IT Act because it is basically cheating by personation through e-mails and other electronic resource taking the names of different reputed organisations, and also pretending as ambassadors, diplomats. There is also deception, wrongful loss to the victim and wrongful gain to the fraudster hence section 420 IPC is attracted. The false e-mails (electronic records) with fake certificates in the names reputed organisation like Microsoft,, Yahoo etc are sent as if they are genuine; hence 471 IPC can also be invoked.


NIGERIAN 419 SCAM
It's Not A Scam, Really, Here's Your Percentage, He'll Wire It To You, No Really, It's True...


Divison of Yahoo Internet Lottery
YAHOO! NEWS
YAHOO! MAIL Lottery
"ONE MILLION UNITED STATE DOLLARS"
CONGRATULATIONS !!!!
YOU WON Â£1,000.000.00 DOLLARS!
YOU HAVE BEEN ANNOUNCED AS ONE OF TOP 25 LUCKY WINNERS !!!
CONGRATULATIONS!
Yahoo!! Internationsl Lottery Organization
Bangkok Branch Office
Address: 3 Rajdamnern Avenue


Microsoft
FONDATION INTERNATIONALE BILLGATES
DIRECTION DE LA PROMOTION DE L'INTERNET ET DU JEUX
DIRECTION DE LOTERIE
LOTERIE INTERNATIONALE BILL GATES
250.000€
FELICITACIONES!! FELICIDADES FELICIDADES!!!

ICC CRICKET WORLD CUP LOTTERY
INTERNATIONAL 2011.

This certificate is the original specimen and valid document from the treasury and security department of the 2011 Cricket Lottery Award Group. The Agreement therein contained are true, correct and binding on the parties. Alteration made on this specimen after it has been legally issued and accepted renders this document null and void.

This Is To certify That:
D. Somesh
Has Been Awarded £1,000,000.00
Great Britain Pound Sterling.
ICC Cricket World Cup
2011

Official

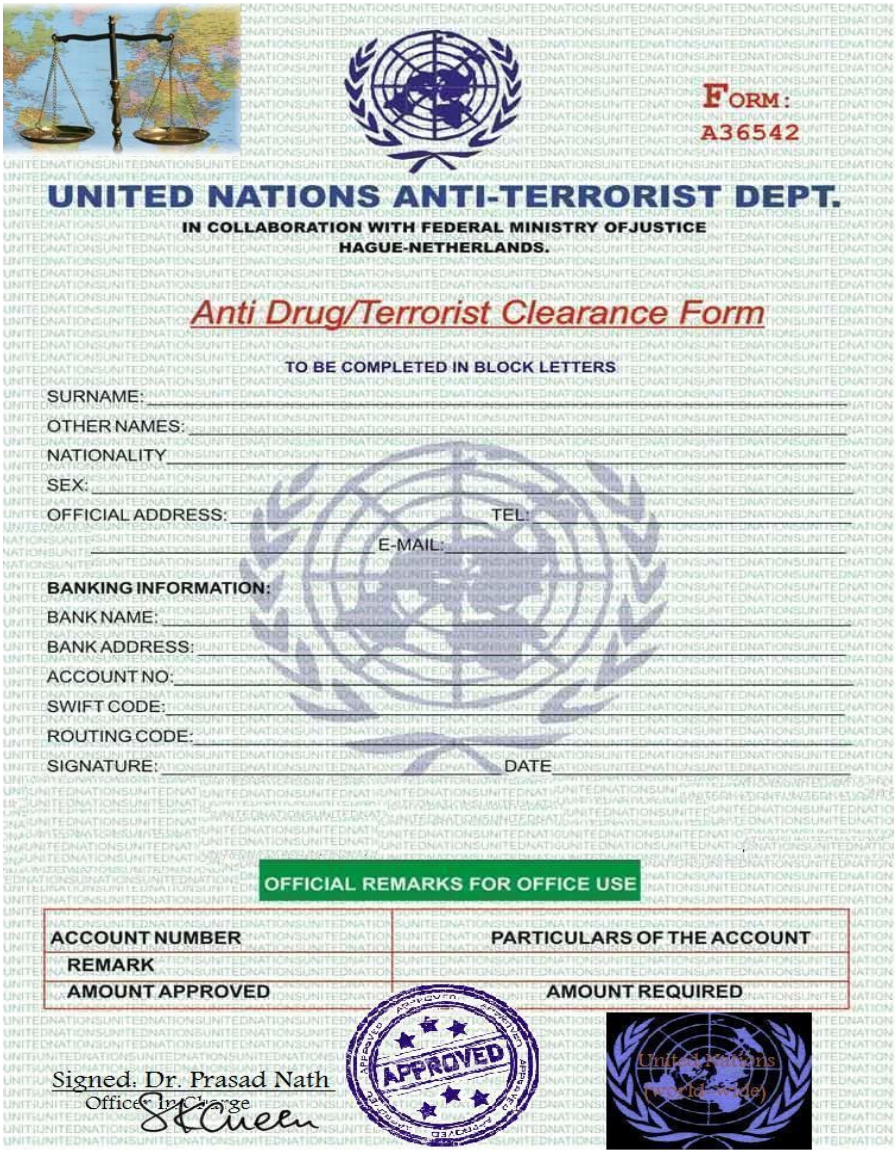
CERTIFIED

For: ICC Cricket Promotional Award Team, London, U.K.

Ban Ki-Moon
United Nations Secretary General.

Dr. Zafer Inceoglu
Dr. Mark Judge

FOREIGN PAYMENT RELEASE OFFICER,
CRICKET 2011 LOTTERY BOARD



FORM:
A36542

UNITED NATIONS ANTI-TERRORIST DEPT.

IN COLLABORATION WITH FEDERAL MINISTRY OFJUSTICE
HAGUE-NETHERLANDS.

Anti Drug/Terrorist Clearance Form

TO BE COMPLETED IN BLOCK LETTERS

SURNAME:
OTHER NAMES:
NATIONALITY
SEX:
OFFICIAL ADDRESS: TEL:
E-MAIL:

BANKING INFORMATION:
BANK NAME:
BANK ADDRESS:
ACCOUNT NO:
SWIFT CODE:
ROUTING CODE:
SIGNATURE: DATE

OFFICIAL REMARKS FOR OFFICE USE

ACCOUNT NUMBER	PARTICULARS OF THE ACCOUNT
REMARK	
AMOUNT APPROVED	AMOUNT REQUIRED

APPROVED

Signed. Dr. Prasad Nath
Officer In Charge

Nigerian frauds – standard operating procedure (SOP):-

During the course of investigation

- All the e-mail correspondence between the victim and fraudsters shall be collected towards documentary proof to establish deception, demand for money etc.

  Further, whatever bogus certificates i.e., 'winning certificate' 'immigration clearance certificate' etc that were sent to the victims as attachments in the e-mails that were sent to victim shall be collected as prints towards documentary proofs.

- All deposit slips corresponding to the deposits made by the victim into different bank accounts as demanded by the fraudsters shall also be collected.
- The account opening forms of all bank accounts into which the amounts were deposited by the victims and transaction statements of them having been deceived by the fraudsters shall also be collected towards further documentary proof.

  This information i.e., address as given in the account opening form, mobile number given to receive phone alerts, address & ID proofs given at the time of opening of the accounts can also be used to work out leads to detect the case.

  The transaction statement of the bank account of the victim can be collected and the ATM centres from which cash withdrawals are made can identified basing the ATM centre ID. From such an ATM ID further the physical location of the ATM centre can be identified and by contacting the concerned bank nodal team CC camera footages of the culprits can be identified and thus efforts can be made to identify the culprits.

- An investigative effort can also be made to trace the e-mail ID with IP Addresses. For this the full headers of the emails sent by the fraudsters shall be verified and the source IP address may be identified and such IP Address may be traced.

- Further in these cases the victims are contacted from different mobile numbers and hence for all such mobile numbers customer application forms (CAFs) along with address proofs and ID proofs shall also be collected.
- After getting these entire can the case be detected? The answer is may or may not, because the addresses that may be identified basing bank account forms or SIM application forms may be insufficient, incorrect or false. However, all these laborious process of investigation shall be completed. The real challenge how to locate the culprits? The suitable answer for this could be while the fraudster is in contact with the victim over mobile number, such numbers can be tracked basing on mobile tower locations which is however difficult to zero in but the only feasible solution to detect these type of cases.
- If the fraudsters are identified a verification may be made with them for the presence of mobile numbers (SIMs) from which the victims were contacted while perpetrating the offence. Further verification may be made for the presence of deceptive e-mails that were sent to victims in their laptops. Such incriminating materials i.e., mobile phone, laptops etc shall be recovered and they shall be forwarded to the FSL for analysis and recovery of electronic evidence.
- While search is made at the house of Nigerians it is advisable such searches are conducted with a search warrant. Further if Nigerians are arrested care shall be taken that arrest information is given to the Nigerian Embassy. Further is Nigerians or other foreigners are arrested then addition of Sections 12 of Foreigners Act is also necessary because their involvements in an offence amounts to violation of the conditions of travel documents i.e., visa, passport etc

Other online frauds:-

Frauds by chatting friends:

Other variants of offences that can be registered under this provision are frauds committed by chatting friends. The people who chat online with strangers usually fall prey to these frauds. The chatting friend will pretend as business man abroad, and he has plans to expand hi business in India. In that process on one day he put forth his idea by saying that he is coming to India and after a few days he will call as if he is detained at the immigration check because he is carrying a valuable gift to the victim and request to pay clearance fee which will be in some lakhs into the bank account that he furnishes to get immigration clearance. Gullible victims without thinking the consequences pay and get defrauded.

Frauds over matrimonial websites:

Similarly frauds committed over matrimonial websites. The victims who have profiles on different matrimonial websites are contacted from purportedly a prospective grooms and gradually the confidence and

affection of the victim are gained and using such good will amounts are collected from the victims. In these cases also the basic sections of law attracted are 66 – D IT Act, then 420 IPC and as per the contents of the complaint other sections can also be invoked. The evidences that shall be collected include the registration details and profiles of the victim and also the accused. This information may be gathered from the concerned people of matrimony website as per the section 65 – B Indian Evidence Act so that the evidentiary value of it may be higher as it is collected from a neutral source. The deposit slips corresponding to the cash deposits made shall be collected from the victim. Required bank transaction statement as per 65 – B Indian Evidence Act or Bankers Books Evidence Act may be collected.

Frauds over classified websites like www.olx.inm, www.quikr.com etc

Further the offences that are committed by misusing the www.olx.com, www.quikr.com etc will also come under this category. www.olx.com, www.quikr.com are websites that allow people to post advertisement for selling their used or new items for free. Some fraudsters misuse this service and sell stolen goods, collect money but do not deliver any goods. In some other occasions the culprits post false classified in the names of other whom they want to harass. Sometimes false advertisement posts offering jobs in reputed companies will be posted on these websites and gullible job seekers are defrauded in the pretext of providing job through back doors methods.

Thus different types of online frauds can be registered and investigated under this section 66- D IT Act, and of course invoking other relevant provisions of IPC.

In these cases apart from following the line of investigation given above for the online frauds some specific case dependent evidences may be collected. In the case of fraud committed by chatting friends the chat logs

may be collected before mediators or at least they shall be collected from victim after getting prints attested by the victim himself.

With regard to the frauds over matrimonial websites the registration information and IP Address track of profiles of the victim as well as of the culprits shall be collected from the concerned service provider under certificate given as per section 65 – B Indian Evidence Act. Similarly the details of the false advertisement posts and their corresponding IP Address track logs may be collected from the classified service provider under a certificate biven as per section 65 – B Indian Evidence Act.

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 could 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 a public or private place.

Under this section the acts like taking pictures of the persons by any means while they are having bath, when their private parts exposed under unexpected circumstances, their cloths slip due to unexpected reasons. Keeping the contents of the complaint Section 354 – C IPC may also be invoked along with section 66-E IT Act. The important difference between 66-E IT Act and 354- C IPC is section 66-E IT Act is neutral in terms of gender, whereas section 354 – C IPC gender specific meaning the victim can be only a female. Under 345 – C IPC applies for mere looking at the private acts of the female.

Further to make out a case under 66 – E IT Act committing any of the acts i.e., '*captures, publishes or transmits*' is sufficient. That means mere capturing the image of private area any person is also sufficient to make out a case. However, in these cases the offence may not stop with mere capturing images of the victim, further such images are posted or circulated over Internet or WhatsApp. Sometimes such images are used to blackmail the victim leading to extortion. In such situation as per the overt acts of the culprits relevant other provisions of the IT Act and IPC can be invoked. If the images of the victims so captured are posted over any pornographic website then section 67 IT Act can be applied. If the images of the victims so captured are used for extortion then 384 IPC can be invoked.

Section 66-E – *violation of privacy* - standard operating procedure (SOP):-

- The basic line of investigation is these case is that verification and recovery of the gadget i.e., mobile phone, digital camera etc may be

made, and if the alleged content is found it shall be recovered under the cover mediator report at the instance of the accused.

- If the investigation establishes that the alleged images are published or transmitted by the accused then such evidences shall be collected.

  If the contents are circulated through Internet over web pages or e-mails prints of such web pages or e-mails shall be recovered and the peoples who have seen such pages may be examined and their statements may be recorded for corroborative purpose.

- Computer/laptop/mobile phone that were used for circulating such material may be recovered and such materials objects shall be forwarded to the Forensic Science Laboratory along with Letter of Advise and required electronic evidence shall be gathered under a FSL Analysis Report.

Section 66F: Punishment for cyber terrorism

(1) Whoever,-

(A) with 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; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(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, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation 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'.

Under this provision the acts like hacking, intrusion of virus or computer contaminant, denial of service etc are committed and such acts threaten the sovereignty of the India or the effect of it to a such extent that the life of people is affected, then such act can be termed a cyber terrorism. Herein the gravity of offence is very serious and therefore the punishment prescribed is up to 'life imprisonment'.

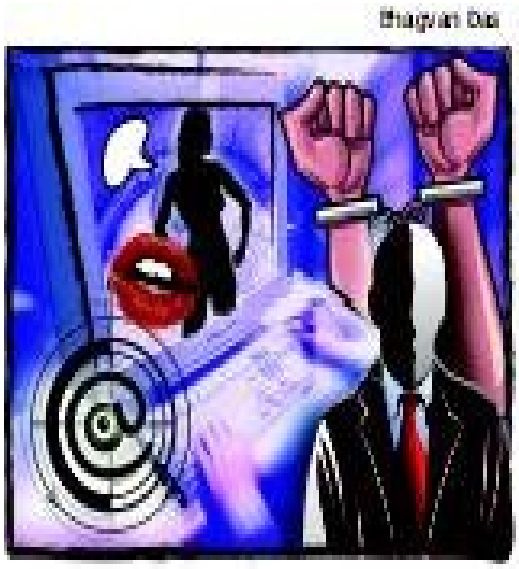
Targets of these attacks may include, but are not limited to, power plants, military installations, air traffic control centres,, and such other vital installations affecting lives of many people.

The line of investigation for these offence will be in similar lines that of the standard operating procedure (SOP) for a case of hacking

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 two 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 ten lakh rupees.

This section is parallel to 292 IPC, the difference is that under section 292 pornography is in books, pamphlets, posters etc where as under section 67 the obscenity in electronic form, and that shall be published or transmitted in electronic form. Therefore this section is applicable to the pornographic websites, and also for acts of sending, transmitting or circulation of obscene e-mails.



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

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

Therefore it is clear that section 67 and 67 –A prohibits pornography in electronic form. The main difference between these sections is, 67 prohibits pornography in the form of text, images or picture etc in electronic form whereas 67 – A is related to pornography in videos in electronic form and their circulation.

It shall also be born in mind these sections do not apply to any contents in any form if such contents has scientific, literary, artistic value or that has bona fide use for religious purposes.

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 or

(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 or

(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 or

(d) facilitates abusing children online or

(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 ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either

description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

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

Section 67 – B IT Act is a section that prohibits child pornography. As per the ingredients incorporated in section 67 – B IT Act it is clear that browsing, watching, downloading pornography with regard to children is an offence. Thus, as provided in the section browsing, watching pornography within the confines of four walls which can in one's bedroom, cyber café and whatever is an offence. Therefore this section provides a great protection to children and prohibits child pornography.

Sections 67, 67-A and 67-B -Standard Operating Procedure (SOP):-

All the three sections 67, 67-A and 67-B IT Act are related pornography. Hence the operating procedure is as follows.

- The existence of the alleged pornography shall be established. For this purpose the web pages where such content appeared shall be secured towards documentary proof to establish that such content has in fact exited.

  If the circulation of pornography is through e-mails, such emails shall be collected towards documentary proofs to establish that such emails were in fact transmitted or circulated.

  This collection may be by taking such web pages or e-mails as prints before mediators under a cover of mediators report.

  Depending on the circumstances of the case nay other witnesses who have seen the alleged web contents or received the alleged e-mail may also be examined and their statements may be recorded.

- The web contents or e-mails shall be traced by securing the IP Address (IP Data Records) tracks that are associated with the web

pages where the alleged web contents are posted or e-mail IDs through which the alleged content is transmitted or circulated.

The IP Address (IP Data Records) tracks may be collected from the concerned service providers which may be social networking service provider like www.facebook.com or e-mail service provider like www.gamil.com.

- After getting IP Data Records, the IP Addresses may be searched for lookup on websites like www.apnic.net, www.domaintools.com, www.whois.net etc the IP Address assignee which can be usually an Internet Service Provider (ISP) information may be ascertained.
- In the next step by writing or by sending an email request to the ISP the end user details of the IP Addresses may be collected and thereby the name and address of the person who created web pages where the alleged web contents are posted or e-mail IDs through which the alleged contents were transmitted or circulated, is known.
- Thus when the suspect is identified and he may be questioned and if he admits, his confession may be recorded before mediators, and in pursuance of such confession and the instance of the culprit the tool of offence which could be a computer, laptop or mobile phone that was used for committing the offence may be recovered.
- The recovered tool of offence (computer, laptop or mobile) may be forwarded to the Forensic Science Laboratory (FSL) under a Letter of Advice with a proper relevant questionnaire and a analysis report may be obtained.
- Thus the case may be established with proper documentary (electronic), oral, circumstantial, scientific evidences.

Thus, sections 65, 66 r/w 43, 66-B to F and 67, 67-A & 67-B are the cognizable and important penal provisions that are provided under Information Technology Act.

The standard operating procedure (SOP) or plan of action given for each penal provision pertains to secure basic methods of investigation and collection of basic evidences. However, the investigating officer (IO) as per the requirement of the case that is under investigation may work out on the other leads / clues to detect the case and collect other evidences (oral, circumstantial, documentary, electronic etc) as per the requirement of the case.

Apart from these provisions discussed above the following are the other relevant provisions for the Law Enforcement Agencies (LEAs).

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 pursuant of any of the powers conferred under this Act, rules or regulations made there under, 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.

This section can be invoked at instances where in if the service providers discloses an information that they have secured in due course of business as authorised under this statute are liable to be punished under this section. However, this provision is non-cognizable.

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 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

This provision makes it clear that any offence is committed targeting computer system or an individual in India by an individual outside of India cognizance of it may be taken by registering a case in India.

Section 77 A: Compounding of Offences

(1) 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 socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) 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.

This section makes it clear that the offences under IT Act that punishable up to 3 years (sections 65, 66 r/w 43, 66-B to E and 67) are compoundable before the trail Court.

Section 77 B: Offences with three years imprisonment to be cognizable

(1) Notwithstanding anything contained in Criminal Procedure 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 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

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

This section makes it clear that even the search and seizure under this Act shall be of and above the rank of Inspector of Police. This also implies that the searches without a search warrant under this Act are restricted to is in public place. Thus it further implied to conducted searches in private place search warrant is essential. Therefore, it is advised where ever applicable invoking IPC provisions is required so that the restriction on searches in private places to some extent can be mitigated.

Amendments to the Indian Penal Code, 1860 and the Indian Evidence Act, 1872

With the enactment of Information Technology Act the majors Acts Indian Penal Code and Indian Evidence Act were amended. The net effect of the amendments to IPC is that where ever the word 'document' is there in IPC and that is added with 'or electronic record', except section 467 IPC :forgery of valuable security. The effect of the amendments to IPC is that the 'electronic record' has an equal value with that of a 'document'. Therefore whatever offences that can be registered with respect of documents can be registered with regard to the electronic records.

In IPC a new Sec 29-A was inserted: "The words 'electronic record' shall have the meaning assigned to them in I T Act 2000"

As per Sec 2 (t) IT Act "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;

As per the amendment to Indian Evidence Act (IEA) 'electronic records' considered under documentary evidence.

Section: 3 Interpretation clauses:

"Evidence": [All documents 'including Electronic records' produced for the inspection of the courts], such documents are called documentary evidence.

The Electronic records shall have the same meaning respectively assigned to it in the I.T.Act 2000

*[the expressions; "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "**electronic records**". "Information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.]*

17. Admission defined

An admission is a statement, [oral or documentary or contained in electronic form], which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned.

34. Entries in books of account when relevant

[Entries in the books of account, including those maintained in an electronic form], regularly kept in the course of business, are relevant whenever they refer to a matter into which the court has to inquire but

such statements shall not alone be sufficient evidence to charge any person with liability.

35. Relevancy of entry in public record made in performance of duty

An entry in any public or other official book, register or 8A[record or an electronic record], stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty, or by any other person in performance of a duty specially enjoined by the law of the country in which such book, register, or 8A[record or an electronic record] is kept, is itself a relevant fact.

The following new sections were included to the Indian Evidence Act with the enactment of Information Technology Act, 2000.

22A. when oral admission as to contents of electronic records are relevant

Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.]

47A. Opinion as to digital signature where relevant

When the Court has to form an opinion as to the digital signature or any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.]

65A. Special provisions as to evidence relating to electronic record

The contents of electronic records may be proved in accordance with the provisions of section 65B

65B. Admissibility of electronic records

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer

(hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein or which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely :-

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the materiel part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the functions of storing or processing information for the purposes of any activities of any regularly carried on

over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.- For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.]

67A. Proof as to digital signature

Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.]

73A. Proofs as to verification of digital signature

In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the court may direct-

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by the person.

81A. Presumption as to Gazettes in electronic forms

The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.]

85A. Presumption as to electronic agreements.

The Court shall presume that every electronic record purporting to be an agreement containing the digital signature of the parties was so concluded by affixing the digital signature of the parties.

85B. Presumption as to electronic record and digital signatures

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that-

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

85B. Presumption as to electronic record and digital signatures

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that-

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

(b) except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

85C. Presumption as to Digital Signature Certificates

The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.]

88A. Presumption as to electronic messages

The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.- For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively

assigned to them in clause (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.]

90A. Presumption as to electronic records five year old

Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular was so affixed by him or any person authorized by him in this behalf.

Explanation.- Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This Explanation applies also to section 81A.]

131. Production of documents or electronic records which another person, having possession, could refuse to produce

No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.]

Section 65 B IEA - Admissibility of electronic records:-

Among all the amendments that are incorporated to Indian Evidence Act, section 65 – B has special importance with regard to the investigation and collection of electronic evidence. While presenting documents to the Courts the Investigating Agencies will produce originals. With regard to the 'electronic records' that originals will be in the form of contents of

hard disks, pen drives, mobile phones and other such storage devices. If such devices are recovered or seized and they are subjected for analysis and required analysis reports are obtained and finally presented for the appreciation of the Judiciary then it amounts to we are presenting the original electronic records to the appreciation of judiciary.

There will be certain occasions where the LAEs will not be in a position to recover such electronic items in the form of originals because they are in the servers or computers of banks in the form of transaction statement of the accounts, mobile service providers in the form of call data records (CDRs), CC Camera Footage etc. Then the option is to collect the output of such electronic record in the form of a computer print out or copying the electronic record on to a compact disc (CD). Here the point to be noted is once output is taken in the form of a copy then the evidentiary value of such electronic records will come down. So, to overcome this kind of limitation, provision 65- B in the Indian Evidence Act was incorporated in Indian Evidence Act with enactment of the Information Technology Act. As per this provision the LEAs shall get a certificate in the form of a signed original hard copy from the person who is giving a copy or output of such electronic record or from the person who in charge of such computer or server incorporating the following main conditions.

- That such data / information has been recorded on to the servers / computers in normal course of transactions
- That only authorised persons with their secure user names and passwords are only permitted to login on the servers / computers.
- That proper security measures are installed on the servers / computers to prevent, from any breach of data and damage from the viruses, worms etc.
- That such data / information after it was recorded on the servers / computer, it has in no way altered.

- That such data / information as is available on the servers / computers was presented in the form of computer output to the police on their request.

Thus the computer / server output is taken supported by the certificate under section 65 – B Indian Evidence Act then such an output will have an equal value with that of a original electronic record. Then the only option to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence to Court or its copy supported by certificate under sections 65A/65B of Evidence Act.

Therefore the IOs shall take special care to secure certificates under section 65- B Indian Evidence Act while they are securing transaction statement of the accounts, call data records (CDRs), CC Camera Footage to establish a case. The same is also true with regard to the IPC cases. However, while working out clues and leads IOs may secure such information but for the entire certificate may not necessary. Once such information is taken before the Judiciary in the form of charge sheet to establish a case then production of 65-B certificate is very required.

Format for the 65 – B IEA as Prescribed by the CBI, India.

FORMAT / PROFROMA

CERTIFICATE UNDER SECTION 65-B OF INDIAN EVIDENCE ACT, 1872

(Authenticity of Electronic Records)

I, ... (name) state that I am employed in .....(Organisation) as ..... (designation).

2. I state that being employed in ..... (organisation). I have personally supervised in preparation of the following electronic records as noted below, through computer terminals in my/our office, by me/our staff under my direct supervision.

a. A DVD-R bearing No. ..... containing true copy of all electronic records pertaining to ..... Email account, original of which are available in our computers. The hash value of the contents of the DVD-R is .....

b. A DVD-R bearing No. ..... containing true copy of all electronic records pertaining to ..... email accounts, original of which are available in my / our computers.

c. A computer printout numbering from page ..... to ..... marked as ..... containing true copy of ..... electronic records pertaining to ..... original of which are available in our computers.

(Please note that print out of an electronic records stored in a computer is also an electronic record)

(a b c ..... is the list all the electronic documents which are being certified and sent under this certificate. It should be clearly identifiable and therefore the DVR-R or the printout should bear a seal/handwritten note/printed note/signature and which should be made note of in the certificate).

(Each page of print out should be carrying a seal of the office/officer sending it).

(Furnishing the hash value of the contents of the record furnished is not compulsory but desirable in the certificate)

3. I further state that all the electronic records contained in digital media/print outs as noted in para 2 above are true copies made of the original electronic records maintained in our computers in our establishment and the same have been produced using the computers in our establishment under my command identifiable as noted below:

a. Computer Number/Computer Series/Server Number .....

b. Printer .....

c. .....

(Section 65 B (4b) requires that the certificate should give such particulars of any device involved in the production of the electronic record as may be appropriate for the purpose of showing that the electronic record was produced by the computer and also describing the manner in which the electronic records were produced).

4. In respect of the records provided above and the information contained therein, it is further certified that:

a. The computer output containing the information was produced by our computers during the period over which computer was used regularly to store and / or process information for the purposes of any

activities regularly carried on over that period by our authorised employees.

b. During the said period, the information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities.

c. Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation for that part of the period, was not such as to affect the electronic record or the accuracy of its contents.

d. The information contained in the electronic record reproduces or it derived from such information fed into computer in ordinary course of said activities.

5. This is stated to the best of my knowledge and belief.

Place:

Date: Signature

Name and Designation

(with seal preferably)

(***The text in italic is only for guidance in making the certificate)***

IP (Internet Protocol) Address and its tracing:-

During the course of investigation of cyber crimes at many occasions a situation may come up where in the culprits who send objectionable, obscene e-mails or post objectionable, obscene content over social networking websites are to be traced. This kind of tracing and identification of the culprits is done by tracing the IP Address which a unique number assigned to a computer that is connected to the Internet.

The Internet is huge network, net work of networks or network established through satellites and cables laid underneath seas. Thus, on the Internet millions of computers across that world are connected on this huge network. When so many computers are connected over network, they shall be identified uniquely, and are to be differentiated from one another. Such identification of the computers can be made with an IP Address. Therefore, IP Address is simply an address of a computer that is connected on the Internet. For example 118.140.29.20 is an IP address. It can be noticed that in the IP Address the numbers are grouped into four and separated by dots. This is called dotted – decimal notation which has a pattern created by following some pattern or standard or protocols to serve the functioning of Internet and that is why it is called Internet Protocol Address.

The analogy is that there are so many peoples across the world and they will be differentiated from one another basing on their address which also will have a pattern i.e., name of the individual, door number, name of the street, name of the town, name of the city etc by which a postal letter is routed and ultimately reached the addressee. In the similar fashion the computer over Internet is routed and is identified.

On the Internet there are so many service providers will be operating. They would be Internet Service Providers (ISPs) which provide access to Internet to individual users, e-mail service like Gmail, social networking service providers like facebook etc. Every service provider will have server which are basically a big computers. Whenever any user is accessing their service by logging on to their servers the IP Address of the individual computer is captured and logged in the server logs. Basing such login track the computer of the culprit who committed any criminal activity can be traced. Therefore the investigating officers shall try to obtain the IP Address log from the service providers when ever criminal activity is done

by creating a fake profile over facebook or an objectionable or obscene e-mail is sent from an e-mail account.

Cyber Crimes – challenges – scene of offence:-

With emergence of cyber crime there are many challenges that the investigating agencies are facing. One among them is with scene of offence and jurisdiction. A narration is given hereunder, let us assume one person is living in the limits of police station 'W', he has bank account located in the limits of police station 'X', he works from an office located from the limits of police station 'Y' and one day while on his way to office from his residence he received a mobile alert that an amount of Rs 1 lakhs was debited from his account and credited to some other bank account falling in the limits of a distant police station 'Z' which may belong to some other State other than the victim belong. In this scenarios there are police stations i.e., W X Y and Z are figuring. Now the questions are whether there is scene of office is there and which police station has jurisdiction over the offence. The analysis is that in this scenario there is no scene of offence in the strict sense of meaning that we conventionally perceive. If at all scene of offence is there it is spread to the limits of all the four police stations and therefore all the police stations have jurisdiction and at all of them case can be registered. However, the police station where the victim is residing may be comes first and it is on priority this is keeping in view of the convenience of the victim because the victim is already victimised and he cannot be expected to go to a distant police station for getting a case registered.

We come across a similar kind of situation while dealing with offences committed over social media. Let us say, frauds committed by a friend befriended over Facebook etc and stalking over social media over Facebook, emails etc. In these instances we need to think that the scene of offence is somewhere in cyber space, a virtual world. As such when we open the social media like Facebook profile, e-mails on a computer system that has Internet we need to assume that we are in a way observing scene of offence. Thus, whatever investigation process that we conduct in the conventional investigation like writing observation-cum-recovery etc., we need to conduct in cyber offence. Open Facebook profile, e-mails etc before mediators and take such contents as printouts and get them signed by the mediators, so that we will be in a position to establish such fake FB profile existed or such objectionable / obscene e-mails were actually sent to the victim.

Cyber Crime filling POO, DOO and name of accused in FIR:-

While filling the columns of first information report (FIR) also care shall be taken that the place of offence (POO) is the address of the victim when the case is registered at the police station in which limits the victim is residing. In the same way if the case is registered in the police station which has jurisdiction over the branch then the POO is the address of the branch. Further while filling the date of occurrence of offence (DOO), if on one day the amount was transferred that day can be mentioned or if a series of transactions are made during different dates then a period from

so and so date to so and so date is to be mentioned. Then other important column of name / names of the accused / accuseds . While filling it basing on the content of the complaint user of the mobile number, email ID or holder of a bank account as disclosed in the complaint may be mentioned instead of simply mentioning as 'unknown'

Cyber Crimes – difficulties in detection of cases:-

Though the criminals can be traced through IP Address, the same is not always possible because the criminal uses counter forensics tools and cover their tracks, IP Addresses etc. It is difficult to detect, if not impossible, the cases, which are from other countries and it is also difficult to trace the culprit if the activity done from cyber cafes.

***

ANNEXURE - I

Draft Template for Letters Rogatory

To: The Competent Authority of the (Requested State)

REQUEST FOR MUTUAL LEGAL ASSISTANCE
IN A CRIMINAL MATTER

(**CERTIFICATE ON BEHALF OF THE (REQUESTING PARTY**)

I, (name of the presiding officer of the court), am authorized to make this request for mutual legal assistance in criminal matters, respectfully request the assistance of the Government (name of the Requested party) in the criminal matter.

REQUEST:

This request is made by the Government of the Republic of India for assistance in accordance with the provisions (describe the relevant provisions) of Treaty between Republic of India and (name of the Requested country) or United Nations convention Against corruption or United Nations convention Against Transnational Organized crime or SAARC Convention or Harare Scheme (or any other Treaty which is relevant).

Or

This request is made by the Government of the Republic of India for assistance in accordance with the Assurance of Reciprocity in similar matters.

Original Assurance of Reciprocity issued by Ministry of Home Affairs, Govt. of the Republic of India, who is central authority of India, is attached herewith.

NATURE OF REQUEST:

This request relates to [describe subject of criminal matter]. The Authority/agency conducting the investigation/prosecution of the criminal matter is [describe authority/agency concerned with the criminal matter.

[Indicate whether judicial proceedings have been, or are to be, instituted or concluded, as the case may be, and provide details of such proceedings (example the level of the court].

CRIMINAL OFFENCES / APPLICABLE LEGISLATION / PENALTIES:

Set out the offences alleged to have been contravened in relation to the criminal proceedings as well as the maximum penalties for these offences and attach copies of applicable legislative provisions. State identity of suspect/accused person, if known. If the matter pertains to enforcement of foreign confiscation order etc., then state also the legal provisions pursuant to which the foreign confiscation order was / is intended to be made, as the case may be.

PERIOD OF LIMITATIONS: Here it may also be mentioned that the offence is not time barred or punishment is not lapsed, citing relevant provision of period of limitation of Indian Law.

STATEMENT OF FACTS (This column is to be filled up on case to case basis)

1. Describe the material facts of the criminal matter including, in particular, those necessary to establish circumstances in the Requesting Country ie. India connected to the evidence or assistance sought, and the relevance of the evidence in India in the criminal matter. Clearly state the connection of material sought. E.g. if bank records are sought, the connection of bank accounts in requested state with the investigation being conducted in India may be specifically mentioned,. If the bank accounts have been utilized in the commission of crime, that may also be invariably mentioned.

2. Indicate whether and how any person(s) has carried on or benefited from the offence(s) committed in the Requesting State. State how the thing sought to be produced by this Request (whether by itself or with another thing) will be of substantial value to the criminal matter.

3. State also whether a foreign confiscation order has been or may be made in such proceeding and whether any person(s) affected or will be affected by such an order has been notified of the proceedings in accordance with the Domestic Law. Provide details of seizure, confiscation, restitution of the property to the Requested Party against which restraint / enforcement is sought and how such property is bonafide linked to the offence.

PURPOSE OF THE REQEUST:

State purpose which is intended to be achieved by the assistance sought, e.g. investigation, prosecution, prevention, suppression of crime, freezing, seizure, confiscation and return of the proceeds of crime in a criminal matter and secure admissible evidence to be used in the trial.

ASSITANCE REQUESTED (use only relevant portion which is related to the case)

The competent authority of Government of (name of the Requested country) is requested to take such steps as are necessary for:

(a) examination of a witness in the Requested Party;
(e.g.) Mr. X of ABC Co. Ltd., (address) is to be orally examined on the following matters:

- (Specify clearly the relevant issues/areas relating to the subject-matter of the criminal proceedings/investigation on which evidence of the witness is sought and/or provide a list of the relevant questions. (***Specify clearly the manner of examination and applicable legal safeguards as well (witness rights as per India Law).***
- Include all available personal details of the witness (including name, nationality, location, passport information and gender etc).
- State the status of the witness (suspect/accused, or simply a witness).
- Include a clear explanation of how the information sought from the witness is relevant to the case.

(b) Production of documents, records or items before a court (and obtaining of oral evidence of the witness producing such material for the purpose of identifying and providing the material produced);

(e.g.) Director of ABC Co. Ltd., (address), is required to produce (describe the form of evidence e.g. "certified copies") the following documents, records or items for the period (store relevant time frame):

- (Specify documents, records or items or classes thereof.
  (The above witness to be orally examined on the following matters for the purpose of identifying and proving the documents, records or items produced)

  (state relevant particulars, e.g. to provide confirmation as to his position in a company/office and that he is responsible for keeping/maintaining/holding the documents, records or items in relation to the subject-matter of the investigation; that the is authorized by the relevant law of the Requested Party to make the statement; to confirm that he has access to the documents, records or items kept in relation to the subject-matter of the investigation in the normal course of his duties; to confirm the authenticity of the copies of the documents, records or items supplied; to confirm that the documents, records or items were created in the ordinary course of business)

(c) Search of person of premises for documents, records or items; (read section 105 of Cr.PC)

(e.g.) The premises of ABC Co. Ltd., (address) to be searched under a search warrant for the seizure of the following from the company:

- (provide details of the documents, records or items sought to be searched for and seized),
- (support any request for originals of documents, records or items seized with reasons),
- (support the belief that relevant documents would be available in the premises of the ABC Co. Ltd.)
- Search being a coercive procedure, the information/evidence supplied shall invariably show the nexus of the premises/computer/electronic device with the Crime/Criminal to establish reasonable suspicion/probable cause.
- State how the items seized will be relevant to the case.

(d) Production of documents, records or items through production orders;

(e.g.) Manager of ABC Bank Ltd., (address) to be required to produce copies of the following documents, records or items under a production order:

- (describe) particulars of material required to be produced and where located).
- (state grounds for believing that the material sought is likely to be of substantial value to the criminal matter).
- (Support any request for the production of originals of documents with reasons).
- (If original cannot be produced request for authenticated copies of the same).
- For bank document, indication of the name and address of the bank, account number, account holder name, time period for the production of the bank statements, types of banking documents requested (account opening documents, statement, wires, loan agreements, among others), relation of the bank account with the crimes committed along with the certificate provided in the respective Statute.

(e) Arrangement of travel of person/persons in custody or an expert from (name of Requested Party) to assist in a criminal matter; (read Section 105B of Cr.PC).

(e.g.) Arrangements to be made for Mr. X (address to travel to (name of Requesting Party) to give assistance in a (criminal matter) by rendering the following assistance:

- (specify the assistance sought)

- (provide the undertakings required by the law of (name of Requested party)
- (provide details of the allowances to which the person will be entitled, and of the arrangements for security and accommodation of the person, while the person is in (name of Requesting party) pursuant to the request).

(f) Enforcement of a forfeiture order/request to assist in the restraining of dealing in property; (Read section 105 Cr.PC)

- Include an official, certified copy of the relevant order(s)
- Include an official, certified copy of the conviction of the person
- Include the provisions of the relevant proceeds of crime laws (including information about restraint and forfeiture regimes)
- Provide confirmation that the conviction and the order are final and are not subject to appeal.
- Include information about the location and particulars of the assets to be restrained, forfeited or used to satisfy a pecuniary order.
- Include as much information as possible to link the criminal conduct of the person to the assets located in Requesting country (including evidence of transfers or other financial information)
- Include any information if there is any third party interest in any of the properties in the Requested country.

(g) Assistance in locating / identifying and locating a person who is suspected to be involved in/to have benefited from the commission of a serious offence;

(e.g.)Arrangements to be made to locate / identify and locate Mr. X who is believed to be in (name of Requested Party) with the last known address at (address).

- (state particulars of person concerned)

(h) Assistance in tracing property suspected to be connected to a serious offence.

(e.g.) Arrangements to be made to trace (description of property) believed to be in (name of Requested Party)

- (state particulars of property concerned)

(i) Arrangement of examination of a person as witness through commission to assist in a criminal matter; (read Section 285 of Cr.PC)

- (Specify clearly the relevant issues / areas relating to the subject-matter of the criminal proceedings/investigation on which evidence of the witness is

sought and/or provide a list of the relevant questions. Specify clearly the manner of examination and applicable legal safeguards as well)

- Attach original order of the court issuing the commission.

(j) If electronic evidence is being sought, the connection, if relevant email/Twitter/ Facebook account with crime and criminal may be mentioned. How the said account has been used in the commission of crime may also be highlighted. It may also be mentioned that preservation request has already be sent to concern ISPs.

MANDATORY ASSURANCE AND UNDERTAKINGS:

It is confirmed that this request:

(a) Neither relates to the investigation prosecution or punishment of a person for a criminal offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character nor it is made for the purposes of investigating, prosecuting, punishing or otherwise causing prejudice to a person on account of that person's race, religion, sex, ethnic origin nationality or political opinions.

(b) Does not relate to the investigation, prosecution or punishment of a person for an offence in a case where the person has been convicted, acquitted or pardoned by a competent court or other authority of the Republic of India or has undergone the punishment provided by the laws of the Republic of India, in respect of that offence or of another offence constituted by the same act or commission as that offence.

(c) As per Indian Law it is not necessary to give any notice to the accused either before issuing the LR or before examining him as a witness/accused.

(d) **Cost**: Generally, the cost of execution of letter of Request shall be borne by requesting state as pr the provisions of the Mutual Legal Assistance Treaty. However, if there are significant….. are involved like travel of witnesses/Cost of obtaining Expert Opinion…. mention the readiness to meet the expenditure to be incurred.

(e) Should the Judicial Authority of the Requested State require the return of any information / evidence / thing obtained in pursuant to this request at the conclusion of the criminal proceeding, the same shall be returned to the Judicial Authority of the Requested State.

(f) The person(s) whose attendance is requested shall not:

i. Be detained, prosecuted, punished and subjected to any other restriction of personal liberty in the territory of Republic of India for any acts, omissions of convictions which preceded the person(s)

departure from the Requested States other than ……. to which the Request relates.

ii. Be subjected to any civil .. respect of any act or omission of the person that is alleged to have occurred or that had occurred before the person's departure from the Requested State.

iii. Be required to give evidence in any proceeding or to assist in any investigation(s) other than the proceeding or investigation(s) to which the request relates, without the persons consent.

Paragraph (f) shall cease to apply if a person being free to leave the country has not left within 30 days or for any period , agreed upon or after receiving official notification that the persons attendance is no longer required has remained voluntarily in the territory of the country on having left has voluntarily returned.

LIMITATIONS OF USE:

Unless otherwise agreed, **the Investigation agency of India, who is conducting investigation in the present case**, shall not without the consent of the Requested State, use or transfer information or evidence provided by the Requested State for Investigations or proceedings other than those stated tin the request. However, in cases where the charge is altered, the material provided may be used in so far as the offence, as charged, is an offence in respect of which mutual assistance could be provided under the present Treaty.

FOREIGN LAW IMMUNITY CERTIFICATE (for Singapore only)

Foreign Law Immunity Certificates is requested by the Singapore authorities declaring that under the law of the (Requesting ……) namely (state legal provision(s) and enclose copies), a person can be requirement in criminal proceedings instituted under the law of the (Requesting Party), to …….. such questions as are sought to be asked through this Request is enclosed with his Request.

EXECUTION OF REQUEST:

Procedure to be followed:

- (State details of manner and form in which evidence is to be taken and transmitted to Requesting Party, if relevant)
- (State any special requirements as to certification / authentication of documents.)
- (State if attendance by representative of appropriate authority of Requesting Party is required at examination of witnesses / execution of request and if so, the title of the office held by the proposed representative.)

PERIOD OF EXECUTION:

If required, state that it is requested that the request be executed urgently / within (state period giving reasons i.e. specify likely trial or hearing dates or any other dates / reasons relevant to the execution of the request.

CONFIDENTIALITY: here explicitly mention the confidentiality requirement during handling of the request by requested state if any.

Eg: “The details of this investigation are considered sensitive. Therefore, please treat this request, its contents, the fact that the request has been made and the results of its execution as confidential and do not disclose it and share it with any subjects, except all those who are dealing with this request for the purpose of its execution, without the consent of the Requesting Authority.”

LIAISON

Provide the details of the officers who are handling this request for liaising with requested state:

State name of officer(s):
Address:
Telephone Number:
Facsimile Number:
Electronic mail address:

Please accept the assurance of our highest consideration.

(Signature along with seal)

Name of the Presiding Officer of the case:

Office:

Date:

CERTIFICATE UNDER SECTION 78(6) OF INDIAN EVIDENCE ACT, 1872
(AUTHENTICITY OF FOREIGN PUBLIC DOCUMENT)

I, ... (name) state that I am employed in ..... (organisation) in State / Republic of ..... (name of the country) as ..... (designation.

2. I state that being Legal Custodian in ..... (organisation), I duly certify that the original public documents in our office as noted below are in my direct legal custody.

Sl. No.	Description of documents held in original	True copies of the document being furnish and certified.
1.	For example - Driving Licence No. ..... dt.	True copy of Driving Licence No. ..... at Page No.1-3.
2.	For example - CDR No. ..... dt.....	True copy of CDR No..... at page No.4-10.
3.	For example - Passport No. ..... dt.	True copy of Passport No..... at Page No. 11-15.

3. It is further stated that the certified true copies of the above said public documents are prepared and compared from or with the original public documents and annexed along with this certificate as noted in above column.

4. According to the law of the State/Republic ..... (name of the Country) the above said certified copy could be used as proof of the original public document by the requesting State/Country and the said certified copy in itself is a proof of the original document.

5. This is stated to the best of my knowledge and belief.

Place: Signature
Date: Name & Designation
(with seal preferably)

(the marked text is only for guidance in making the certificate)

CERTIFICATE OF NOTARY PUBLIC OR INDIAN CONSUL OR DIPLOMATIC AGENT

I, ... (Name of the Designation of the person) in the capacity of (Notary Public or Indian Consul or Diplomatic Agent) certify that the copy of foreign public document is duly certified by the officer having the legal custody of the original, and upon proof of the character of the document according to the law of the ..... (Name of the Country/Republic).

Signature
Name & Designation
(with seal preferably)

ANNEXURE –II

NODAL CONTACTS / EMAIL IDs OF VARIOUS AGENCIES / SERVICE PROVIDERS

(NOTE: SUBJECT TO CHANGE)

BANKS

ORGANISATION	EMAIL_ID
ANDHRA BANK	frmg@andhrabank.co.in
AXIS BANK	statutory.notice@axisbank.com
BANK OF BARODA	gm.ops.ho@bankofbaroda.com
HDFC BANK	SomaSekhar.RaoDaduwai@hdfcbank.com
HSBC BANK	nodalofficerinm@hsbc.co.in
HSBC BANK	srinivas1naidu@hsbc.co.in
ICICI BANK	rangachary.kv@icicibank.com
ING VYSYA BANK	nodalofficer@ingvysyabank.com
IOB	creditcard@iobnet.co.in
KOTAK	escalations@kotak.com
KOTAK	service.bank@kotak.com
PNB	skbansal@pnb.co.in
PNB	vsrinivasan@pnb.co.in

SBH	cmgrievances@sbhyd.co.in
SBI	agmvig.lhohyd@sbi.co.in
SBI	helpline.lhohyd@sbi.co.in
SBI-CARDS	Nodalofficer@sbicard.com
SCB	principal.nodalofficer@sc.com

INTERNET SERVICE PROVIDERS (ISPs)

ORGANISATION	EMAIL_ID
ACTTV	nodalofficer@acttv.in
BEAM CABLE (ACT)	ajay.banda@actcorp.in
BSNL	sdetecvig@bsnl.co.in
EXCELL MEDIA	ramakrishna@excellmedia.net
NETX	skept@netxconnect.com
PIONEER ONLINE	support@pol.net.in
SIFY	luithelp@sify.com
SKYTEL	rajskytel@gmail.com
SOUTHERN ONLINE	support@sol.net.in
SRITEL	vamsi@sritel.in
TIKONA	jaydeep.sampat@tikona.in
VAINAVI	padmaja@vainavi.net
VAINAVI	nodal@vainavi.net
VSNL	VIGILANCE.mumbai@tatacommunications.com
YOUTELE	idc@youbroadband.co.in
ZYTEL	anilkumar.ch@zyetel.com

MERCHANTS (ONLINE SHOPPING)

ORGANISATION	EMAIL_ID
ARZOO	rajesh.m@arzoo.com

BHARAT MATRIMONY	legal@consim.com
CLEARTRIP	hotelcs@cleartrip.com
EBAY	contactIndiafit@ebay.com
FLIPKART	cs@flipkart.com
FLIPKART	grievance.officer@flipkart.com
IRCTC	care@irctc.co.in
MOBIKWIK	support@mobikwik.com
OLX	grievance-officer@olx.in
PAYTM	security@paytm.com
RECHARGEITNOW	care@rechargeitnow.com
WAY2SMS	support@way2online.com

MOBILE SERVICE PROVIDERS

ORGANISATION	EMAIL_ID
AIRCEL	ap.nodaldesk@aircel.co.in
AIRTEL	nodalofficer3.ap@in.airtel.com
BSNL	vightd10@bsnl.co.in
CELLONE	techcellone_hyd@bsnl.co.in
IDEA	Inodal.ap1@idea.adityabirla.com
MTNL	gmvigil@mtnl.net.in
RELIANCE	RCom.APNodalOfficer@relianceada.com
TATA	APSecurity.Wing@tatatel.co.in
UNINOR	CNO.AP@uninor.in
VODAFONE	nodaldd.andhrapradesh@vodafone.com

E-MAIL SERVICE PROVIDERS

ORGANISATION	EMAIL_ID
GOOGLE	lis-apac@google.com
HOTMAIL	msnwwcc@microsoft.com
MICROSOFT	indiacc@microsoft.com
REDIFF	legal@rediff.co.in
YAHOO INDIA	robinfe@yahoo-inc.com

PAYMENT GATEWAYS

ORGANISATION	EMAIL_ID
PAYTM	cybercell@paytm.com
BILL DESK	genius@billdesk.com
CCAVENUES	risk@ccavenue.com

ANNEXURE –IV

- Model NOTICE to Google / Gmail that is addressed at its nodal contact e-mail ID: lis-apac@google.com is mentioned below.
- The notice may be prepared in word document and after signing on it, the document shall be scanned and sent to the e-mail ID lis-apac@google.com of Google authorities from the official ID of the Investigating officer (IO).
- Official email ID means the one that is assigned by the Police Department which may be in the form : xyz@tspolice.gov.in
- Note: Notices under Criminal Procedure Code shall be issued after registration of a case (issuing of FIR).

Government of Telangana
(Police Department)

OFFICE OF THE
ADDL SUPERINTENDENT OF POLICE,
CYBER CRIMES, CID,
TS, HYDERABAD.

Date: 24-02-2017

Notice U/section 91 Code of Criminal Procedure, 1973

(Reference: Crime Number 24/2016 U/s 67 IT Act, 2000 and 354-D, 509 IPC of CID PS, TS, Hyderabad)

-oOo-

It is to inform that the user of the following gmail e-mail IDs is circulating defamatory, vulgar and annoying e-mails causing deep mental agony to the victim.

abc2016@gmail.com
xyz2017@gmail.com

Therefore it is requested to furnish the **Registration & IP log details of the said email IDs from activation of them to till date.**

Early action would be highly appreciated.

(B. Ravi Kumar Reddy)
Inspector of Police,
Cyber Crime PS, CID,
Hyderabad

To
Google Inc.,
Mountain View,
CA, USA.

CYBER CRIMES

a Practical guide for Investigators

Telangana State Police

www.tspolice.gov.in