CHAPTER V
PREVENTION AND INVESTIGATION

1. DEFINITION OF INVESTIGATION

The word "Investigation" is derived from Latin word “Investigare” which means “to trace out or to search into” i.e. to probe into for finding out the truth. Richard H. Ward says, “The primary function of the criminal investigator is to gather information determine the validity of the information, identify and locate the perpetrator of the crime and provide evidence of his guilt for a court of law.” Inherent in this function is the responsibility to protect the innocent. He continues, “The mean by which the investigator carries out this function may be classified into two ways - Internal and External.”

*Internal* refers to the process of logic, expertise intuition, experience and knowledge that he brings to the investigation.

*External* refers to the tools, scientific aids, additional personal and other resources that he brings to bear on the investigation.¹

Section 2(h) of Cr. P.C., 1973, “Investigation” includes all the proceedings under this code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorized by a Magistrate in this behalf.²

The Word “investigation” cannot be limited only to police investigation but on the other hand, the said word is with wider connotation and flexible so as to include the investigation carried on by any agency whether he be a police officer under or empowered or authorized officer or a person not being a police officer under the direction of a Magistrate to make an investigation vested with the power of investigation.³

---

Difference between Investigation and Inquiry

In criminal matters the inquiry is something different from a trial. Inquiry stops when trial begins. Inquiry is wider than trial. Trial presupposes the idea of an offence but inquiry relates to offences and matters which are not offences vide security proceedings and other proceedings and other inquiries relating to dispute about possession of immovable property etc. All those proceedings before a Magistrate prior to the framing of a charge which do not result in conviction can be termed as inquiry.\(^1\) An inquiry preparatory to commitment of a case to the sessions under section 209 is inquiry within the meaning of section 2(g).\(^2\) Similarly, the proceedings under section 209 fall within the term inquiry.\(^3\) The three term “investigation”, “inquiry” and “trial” denote three different stages of a criminal case. The first stage is reached when a police officer either by himself or under orders of a Magistrate investigates into a case (S. 202). If he find that no offence has been committed he reports the fact to a Magistrate who drops the proceedings and the case comes to an end (S.203). But if he is of a contrary opinion, he sends up the case to a Magistrate. Then begins the second stage, which is either a trial or an inquiry. The Magistrate may deal with the case himself, and either convict the accused, or discharge or acquit him. In cases of serious offences the trial is before the session court which may either discharge the accused or convict or acquit him. The main purpose of an investigation is collection of evidence and it must be conducted by a police officer or a person enjoying the powers of a police officer or authorized by a Magistrate is his behalf or a person in authority.\(^4\)

Collection of Evidence

The definition of the term is not exhaustive. An “investigation” means search for material and facts in order to find out whether or not an offence has been committed. It does not matter whether it is made by a police officer or a

---

1. Alim and other, 1982 Cr. L.J. 1264 (All).
custom officer or any other officer authorized to investigate into the matter of an
offence committed under a law other than the IPC. The arrest and detention of a
person for the purpose of investigation of a crime forms an integral part of the
process of investigation. Examining witness and arranging raids for the purpose
of dealing with a complaint by an inspector of Anti-corruption Dept. was included
within the meaning of the word “investigation”. Searches are also proceeding for
the collection of evidence and therefore part of investigation under S.2 (h).
Medical examination of the arrested person also forms part of the investigation.
The word “investigation” has to be read and understood in the light of not only the
powers conferred on police officers but the restrictions placed on them in the use
and exercise of such powers.

The Supreme Court has viewed the investigation of an offence as generally
consisting of—

(1) Proceeding to the spot;
(2) Ascertainment of the facts and circumstances of the case;
(3) Discovery and arrest of the suspected offender;
(4) Collection of evidence relating to the commission of the offence which
   may consist of-
   (a) the examination of various person (including the accused) and the
   reduction of their statements into writing if the officers think fit.
   (b) the search of places or seizure of things considered necessary for the
   investigation or to be produced at the trial; and
(5) Formation of the opinion as to whether on the materials collected there is a
case to place the accused before a Magistrate for trial, and if so taking the
necessary steps for the same by the filing of a charge sheet under s. 173.
Two important steps in the process of investigation, viz. discovery and arrest of the suspected offender and the search of places and seizure of things considered necessary for the investigation, inquiry, or trial.¹

2. CRIMINAL PROCEDURE AS APPLICABLE TO REAL WORLD CRIMES

Section 80 of Information Technology Act clearly stated that:

(1) Notwithstanding anything contained in the code of criminal procedure, 1973 any police officer, not below the rank of an Inspector² 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 or having committed or of committing or of being about to commit any offence under this Act.

Explanation: For the purposes of this sub section the expression “public place” includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.³

(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.

² Substituted Inspector by Information Technology (Amendment) Act, 2008
The following are the ingredients of sub-section (1) of section 80-

- The power to enter any public place and search and arrest without warrant any person found therein, is vested only in a police officer not below the rank of an Inspector or any other officer of the Central Government or a State Government who is authorized by the Central Government;

- This Power can be exercised only in a “public place” which as per the Explanation to section 80 includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public;

- This Power to enter any public place and search and arrest without Warrant any person found therein, can be exercised only on the ground that such person is reasonably suspected of having committed or of committing or of being about to commit any offence under the IT (Amendment) Act, 2008.

As is apparent, an accused any arrested without warrant under section 80 of the IT (Amendment) Act, 2008 only from a public place and no other place, and he can be arrested either for having committed or for committing or for being about to commit any offence under the IT (Amendment) Act. On first glance, section 80 of the IT (Amendment) Act, 2008 appears to be clear and simple but on a closer examination, it creates confusion in the law and leads to absurd results. On a plain construction of this provision, three situations could be covered therein:

- A person is alleged to have committed an offence under the IT (Amendment) Act in a place other than a public place, but is found in a public place;

- A person is alleged to have committed an offence under the IT (Amendment) Act in a public place, but is found in some other public place;

- A person is alleged to have committed or is committing or is about to commit an offence under the IT (Amendment) Act, in a public place and is found in that very public place;

The aforesaid construction of the provision is based on its silence as to the place of commission of the offence. It only speaks of the place where the accused
is found when he is sought to be arrested, which has to be a public place. Since the words “of committing or of being about to commit” refer to the point of time of arrest, therefore, the third situation as aforesaid arises. If the legislature had intended to restrict the application of section 80 to only the third situation as aforesaid, the words “in such public place” should have been added at the end of sub-section (1).¹

By restricting the Power of arrest without warrant only from public place, section 80 becomes vulnerable for being defeated luxuriously which is apparent from the following examples:

Example 1: A is reasonably suspected of having committed the offence of hacking under IT Act from his (A’s) house. After committing the said offence, he (A) goes to a hotel. As per section 80, A can be arrested without warrant from the hotel which is a public place. However, if A remains in his house after committing the said offence of hacking, he cannot be arrested without warrant as per section 80.

Example 2: If A is reasonably suspected of having committed the offence of hacking under the IT Act from a cyber cafe, he can be arrested without warrant under section 80 only if he is found in the cyber cafe itself or in some other public place. But if he (A) goes home and stays there, after committing the cyber crime in the cyber cafe, then he cannot be arrested without warrant.

Therefore, as and when necessary, one is expected to invoke the relevant statutory provisions of Cr. P.C., 1973 in a given contextual situation. When we consider the ambit of investigation, essentially the following different facts form part, as it primarily aims at processes yielding collection and presentment of evidence.

2.1 Power of Police to Initiate Investigation and Arrest

(1) Police, When to Investigate: - The principle agency for carrying out investigation of offences is the police; and the police can proceed to investigate-

(i) on the information received from any person as to the commission of any cognizable offence¹; or

(ii) even without any such information, but if they have reason to suspect the commission of any cognizable offence, or

(iii) On receiving any order (to investigate) from any judicial Magistrate empowered to take cognizance of any offence under section 190.²

(2) Investigation process

(A) In respect of cognizable offence:— Any person aware of the commission of any cognizable offence may give information to the police and may, thereby set the criminal law in motion. Such information is to be given to the officer in charge of the police station having jurisdiction to investigate the offence. The information so received shall be recorded in such a form and manner as is provided in section 154. That section is intended to ensure the making of an accurate record of the information given to the police. According to that section:-

(a) If the information is given orally to the officer-in-charge of the police station, it shall be reduced to writing by the officer himself or under his direction.

(b) If the information is given in writing, or if reduced to writing as aforesaid, the writing shall be signed by the informant.

(c) The information as taken down in writing shall be read over to the informant.

(d) The substance of the information shall then be entered, by the police officer, in a book to be kept by such an officer in the form prescribed by the State Government. This book is called the Station Diary or General Diary.

(e) A copy of the information as recorded above shall be given forth with, free of cost, to the informant.

² Section 156 (3) of Cr. P.C., 1973
If the officer-in-charge of the police station refuses to record the information, any person aggrieved by such refusal may send, in writing and by post, the substance of such information to the superintendent of police concerned. If the superintendent is satisfied that such information discloses the commission of a cognizable offence, he shall either investigate the case himself or direct an investigation to be made by any police officer subordinate to him. Such an officer shall have all the powers of an officer-in-charge of the police station in relation to that offence.

The information as recorded under section 154 is usually known and referred to as the first information report or simply as FIR.¹

According to section 154 (3), if any person is aggrieved by a refusal on the part of the police officer-in-charge of a police station to record the information, he may send by post the substance of such information in writing to the superintendent of police concerned. If the superintendent is satisfied that the information discloses the commission of a cognizable offence, he shall either investigate the case himself or direct an investigation to be made by a subordinate police officer in the manner provided by the code.²

**When to start investigation**

Section 156 of the Cr. P.C., any officer-in-charge of a police station may, without the order of a Magistrate, investigate any cognizable case falling within the jurisdiction of such police station. The courts do not interfere in the matters of investigation.

**Procedure for investigation**

1. The investigation of a cognizable offence begins when a police officer-in-charge of a police station has reason to suspect the commission of a cognizable offence. Though the basis for the suspicion is essentially the

---

¹ Kelkar’s R.V. Revised by Dr. K.N. Chandrasekharan Pillai, *Lectures on Criminal Procedure*, Eastern Book Company, Lucknow, Ed. 2007, pp. 49-50
first information report as recorded under section 154, yet it is legally possible that the suspicion may be based on any other information of the police.\(^1\)

2. Where a reasonable suspicion of the commission of a cognizable offence exists the station house officer must immediately send a report of the circumstances creating the suspicion, to a Magistrate having power to take cognizance of such an offence on a police report\(^2\). This provision is really designed to keep the Magistrate informed of the investigation of such a cognizable offence so as to be able to control the investigation and if necessary to give appropriate direction under section 159.\(^3\) The Magistrate mentioned in section 156 (3) and 157 (1) is the judicial Magistrate\(^4\). Every such report, if the State Government so directs, shall be submitted through such a superior officer of police as may be appointed by the State Government for this purpose. On receiving the report, the superior officer may give such instruction to the station house officer as he thinks fit, and shall, after recording such instructions on the report, transmit the same without delay to the Magistrate.\(^5\)

3. The station house officer shall then proceed in person or shall depute his subordinate officer to proceed, to the spot, to investigate the facts and circumstances of the case; and if necessary, to take measures for the discovery and arrest of the offender.\(^6\)

There are, however, two circumstances in which it is not necessary for the station house officer to proceed in person or depute a subordinate officer to make an investigation on the spot. These circumstances are as follows:

(a) Where the case is not of a serious nature and the information as to the commission of the offence has been given against any person by name

---

1 Section 157 (1) of Cr.P.C.
2 Section 157 (1)
5 Section 158 of Cr. P.C.
6 Section 157 (1) of Cr. P.C.
[proviso (a) to S.157(1)]. The police officer in such a case is required to state in his report to the Magistrate his reasons for not proceeding to make an investigation on the spot.¹ If the police officer makes a wrong assessment as to the seriousness of the case, the superior police officer through whom the report is sent to the Magistrate, can always give appropriate directions to the officer-in-charge of the police station to set right the course of his action.

(b) When it appears to the officer in charge of a police station that there is no sufficient ground for entering on an investigation [Proviso (b) to S. 157 (1)].

Here again the police officer is required to state in his report of the Magistrate his reasons for not proceeding to investigate the case. The police officer is further required to notify immediately to the informant, if any, in the manner prescribed by the State Government, the fact that he would not investigate the case or cause it to be investigated.²

This would enable the informant to approach a Magistrate or a superior police officer for redress, if he feels aggrieved by the view taken by the station house officer. As the report to the Magistrate is to pass through the superior police officer, he can issue appropriate instructions to the station house officer.

4. The Magistrate, on receiving the report of the station house officer, may direct an investigation, or may at once proceed, or depute any Magistrate subordinate to him to proceed, to hold a preliminary inquiry into, or otherwise to dispose of the case in the manner provided in the code.³ The power of the police to investigate any cognizable offence is uncontrolled by the Magistrate, and it is only in cases where the police decides not to investigate the case (on sufficient grounds) that the Magistrate can intervene and either direct investigation, or as an alternative, himself

¹ Section 157(2) of Cr. P.C.
² Section 157 (2) of Cr. P.C.
³ Section 159 of Cr. P.C.
proceed, or depute a Magistrate subordinate to him to proceed, to inquire into the case.\footnote{1}{S.N. Sharma v. Bipen Kumar, (1970)1 SCC 653 at p. 656-57 : 1970 SCC (Cri) 258 : 1970 Cri. L.J. 764 at p. 766}

5. When the police officer reaches the spot he shall proceed to investigate the facts and circumstances of the case, and to arrest the offender.

(B) In respect of non-cognizable offence:- If any person gives information to an officer-in-charge of a police station of the commission of a non-cognizable offence,\footnote{2}{“Non-cognizable offence” means an offence for which, and “non-cognizable case” means a case in which, a police officer has no authority to arrest without warrant. Section 2(L) of Cr. P.C., 1973} the officer shall enter or have cause to enter the substances of the information in a book to be kept by such an officer in the form prescribed by the State Government. The officer shall then refer the informant to the Magistrate.\footnote{3}{Section 155 (1) of Cr. P.C.}

As mentioned earlier, non-cognizable offences are more or less considered as private criminal wrongs; the code therefore enjoins that a police officer shall not investigate a non-cognizable case without the order of a competent Magistrate.\footnote{4}{Section 155 (2) of Cr. P.C.} But once such an order is given by the Magistrate, the police officer receiving the order may exercise the same powers in respect of the investigation (except the power to arrest without warrant) as an officer in charge of a police station may exercise in a cognizable case.\footnote{5}{Section 155 (3) of Cr. P.C.}

Where a case relates to two or more offences, and at least one of such offences is cognizable, the case shall be deemed to be a cognizable case even though the other offences are non cognizable.\footnote{6}{Section 155 (4) of Cr. P.C.}

**Power to interrogate witnesses and to record their statements**

Police officer making an investigation has been empowered to require the attendance of persons, who from the information given or otherwise, appears to be acquainted with the facts and circumstances of the case. He can also orally
examine such witnesses and based on their replies prepare a written record of the statement\textsuperscript{1} made to him during the examination.\textsuperscript{2} Thereafter, depending upon the context and information available, the investigative process may lead to arrest of suspected persons. At this juncture, relevant understanding as to the power of arrest on the part of investigative police officer as envisaged by the statutory provisions and circumscribed by judicial interpretation is necessary.

**When police may arrest**

*Section 41* is stated that:-

(i) Any police officer may without an order from a Magistrate and without a warrant, arrested any person:-

(a) who commits, in the presence of a police officer, a cognizable offence;

(b) against whom a reasonable complaint has been made, or credible information has been received, or a reasonable suspicion exists that he has committed a cognizable offence punishable with imprisonment for a term which may be less than seven years or which may extend to seven years whether with or without fine, if the following conditions are satisfied, namely:-

(i) the police officer has reason to believe on the basis of such complaint, information, or suspicion that such person has committed the said offence;

(ii) the police officer is satisfied that such arrest is necessary:-

(a) to prevent such person from committing any further offence; or

(b) for proper investigation of the offence; or

\textsuperscript{1} In Section 161 of the principal Act, in Sub-section (3), the following provision shall be inserted by Code of Criminal Procedure (Amendment) Act, 2008 :- “Provided that statement made under this sub-section may also be recorded by audio-video electronic means, www.taxindiaonline.com/RC2/pdfdocs/Crpc.pdf.

\textsuperscript{2} Section 161 of Cr. P.C.
(c) to prevent such person from causing the evidence of the offence to disappear or tampering with such evidence in any manner; or

(d) to prevent such person from making any inducement, threat or promise to any person acquainted with the facts of the court or to the police officer; or

(e) as unless such person is arrested, his presence in the court whenever required cannot be ensured;

and the police officer shall record while making such arrest, his reason in writing.

(ba) against whom credible information has been received that he has committed a cognizable offence punishable with imprisonment for a term which may extend to more than seven years whether with or without fine or with death sentence and the police officer has reason to believe on the basis of that information that such person has committed the said offence;¹

(ii) for sub-section (2), the following sub-section shall be substituted, namely:-

2. Subject to the provisions of section 42, no person concerned in a non-cognizable offence or against whom a complaint has been made or credible information has been received or reasonable suspicion exists of his having so concerned, shall be arrested except under a warrant or order of a Magistrate.²

Section 41A- (1) the police officer may, in all cases where the arrest of a person is not required under the provisions of sub-section (1) of section 41, issue a notice directing the person against whom a reasonable suspicion exists that he has committed a cognizable offence, to appear before him or at such other place as may be specified in the notice.

¹ Section 41 sub-section (1) for clauses (a) and (b) shall be substituted by Code of Criminal Procedure (Amendment) Act, 2008; http://www.lawyersclubindia.com/forum/files/38_the_code_ofcriminalprocedure_amendment_bill_2008.pdf.

(2) Where such a notice is issued to any person, it shall be the duty of that person to comply with the terms of the notice.

(3) Where such person complies and continues to comply with the notice, he shall not be arrested in respect of the offence referred to in the notice unless, for reasons to be recorded, the police officers is of the opinion that he ought to be arrested.

(4) Where such person, at any time, fails to comply with the term of the notice it shall be lawful for the police officer to arrest him for the offence mentioned in the notice, subject to such orders as may have been passed in this behalf by a competent court.¹

*Section 41B:* Every police officer while making an arrest shall :-

(a) bear an accurate, visible and clear identification of his name which will facilitate easy identification;

(b) prepare a memorandum of arrest which shall be-

(i) arrested by at least one witness, who is a member of the family of the person arrested or a respectable member of the locality where the arrest is made;

(ii) Countersigned by the person arrested; and

(c) inform the person arrested, unless the memorandum is attested by a member of his family, that he has a right to have a relative or a friend named by him to be informed of his arrest.²

*Section 41C:* (1) The State Government shall establish a police control room-

(a) in every district; and

(b) at state level

(2) The State Government shall cause to be displayed on the notice board kept outside the control room at every district, the names and address of the

---

persons arrested and the name and designation of the police officers who made the arrests.

(3) The control room at the police Headquarters at the state level shall collect from time to time, details about the persons arrested, nature of the offence with which they are charged and maintain a database for the information of the general public.1

Section 41D: when any person is arrested and interrogated by the police, he shall be entitled to meet an advocate of his choice during interrogation, though not throughout interrogation.2

The term “arrest” is not defined either in the code or in the various substantive Acts. The word “arrest” is derived from the French “arrester” meaning “to stop or stay”, and signifies a restraint of the person.3 The word “arrest”, when used is its ordinary and natural sense, means the apprehension or restraint or the deprivation of one’s personal liberty. When used in the legal sense, in the procedure connected with criminal offence, an arrest consists in the taking into custody of another person, under authority empowered by law, for the purpose of holding or detaining him to answer a criminal charge or of preventing the commission of a criminal offence. The essential elements required to institute an arrest, in the above sense, are that there must be an intent to arrest under the authority, accompanied by a seizure or detention of the person, in the manner known to law, which is so understood by the person arrested.4 In every arrest there is custody but not vice versa and both the words ‘custody’ and ‘arrest’ are not synonymous terms.5 The term ‘custody’ cannot be interpreted as actual physical custody. If the child is under the supervision and control of a recognized

5 Directorate of Enforcement v. Deepak Mahajan, 1994 Cr. L.J. 2279 (2284) (SC)
institution or agency where it is registered and if the trained social worker or superintendent of such institution has taken the responsibility for the child and has kept the child under observation and under his or her control the direction, such an institution is in the custody of the child, it would be in a position to make a child study report and get a medical report of such a child. The custody, therefore, of a recognized institution should be broadly interpreted to mean not physical custody but custody in the sense of supervision and control over the child so that the institution can arrange for a child's individual care or medical treatment whenever required.¹

An arrest made by any one, be it a police officer, a private person or a Magistrate as provided under sections 41 to 44 of the code, will come within the meaning of the term "arrest" occurring in section 167 (5). Once a person is arrested, for the purpose of investigation, the remand is made under section 167. A Division Bench of the Kerala High court² has held that in cases where the accused persons were not arrested by the police, but surrendered before the Magistrates, the taking into custody of such persons by Magistrates will come within the ambit of the term “arrest”. This view was adopted by the Madras High Court³ and the Supreme Court.⁴

It an information relating to a cognizable offence is brought to the notice of the police officer, through he has the power to arrest, he can still refrain from arresting person, depending upon the nature of the offence and the circumstances unfurled not only in the complaint but also during the course of investigation. This section, of course, gives wide powers to the police officer to make an arrest and, naturally it is necessary while exercising such large powers to be cautious and circumspect.⁵

⁴ Niranjana Singh v. Prabhakar, AIR 1980 SC 785
The power to arrest under this section shall not be exercised arbitrarily violating dignity and the liberty of an individual. An arrestee has the right to be informed about his arrest and to consult privately with lawyer. These rights are inherent in Article 21 and 22 (1) of the constitution and require to be recognized and scrupulously protected. For effective enforcement of these fundamental rights, the Supreme Court has issued the following instructions, for compliance:-

1. An arrested person being held in custody is entitled, if he so requests, to have one friend, relative or other person who is known to him or likely to take an interest in his welfare told, as far as is practicable, that he has been arrested and where he is being detained.

2. The police officer shall inform the arrested person when he is brought to the police station, of this right.

3. An entry shall be required to be made in the diary as to who was informed of the arrest.

4. It shall be the duty of the Magistrate, before whom the arrestee person is produced, to satisfy himself that these requirements have been complied with.2

"May............arrest"-the words may arrest show that the power of arrest is discretionary. A police officer is not always bound to arrest for a cognizable offence.3 The power of arrest under S. 41 given to the police is not absolute and is not to be exercised in arbitrary manner, but judiciously.4

While arresting a female person, all efforts should be made to keep a lady constable present but in circumstances where the arresting officer is reasonably satisfied that such presence of a lady constable is not available or possible and/or the delay in arresting caused by securing the presence of a lady constable would impede the course of investigation such arresting officer for reasons to be recorded either before the arrest or immediately after the arrest the permitted to arrest a

---

1 Kajal Dey v. State of Assam, 1989 Cr. L.J. 1209 (Gau)
3 Deenam v. Jayalalitha, 1989 Mad LW (Crl) 395
4 State of Rajasthan v. Bhera, 1997 Cr. L.J. 1237 (Raj-DB)
female person for lawful reasons at any time of the day or night depending on the circumstances of the case even without the presence of a lady constable.¹

2.2 Power of Police to Carry out Search and Seizure

The next process leads to search and seizure with a view to collect any incriminating evidence which connects the crime to the criminal. In this connection the following provisions of Cr. P.C., 1973 require a basic understanding.

Whenever a police officer making an investigation has reasonable grounds to believe that anything necessary for the purpose of an investigation into an offence, which he is authorized to investigate, may be found in any place within the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without under delay may, after recording in writing the grounds of his belief, search or cause search to be made for such thing in any place within the limits of such station.² Copies of the record in which the reasons for his belief is stated shall be forwarded forthwith to the nearest Magistrate empowered to take cognizance to the offence. If the thing to be searched for falls within the limits of another police station the investigating officer can also request the in charge of that police station and in such cases that police officer will conduct the search and forward any seized things to the investigating officer.³

Person in charge of closed place to allow search

Section 100 of Criminal Procedure Code stated that-

1. Whenever any place liable to search or inspection under this chapter is closed, any person residing in, or being in charge of, such place, shall, on demand of the officer or other person executing the warrant, and on production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein.

---

² Section 165 of Criminal Procedure Code 1973
³ Section 166 of Criminal Procedure Code, 1973

396
2. If ingress into such place cannot be so obtained, the officer or other person executing the warrant may proceed in the manner provided by sub-section (2) of section 47.

3. Where any person is or about such place is reasonable suspected of concealing about his person any article for which search should be made, such person may be searched and if such person is a woman, the search shall be made by another woman with strict regard to decency.

4. Before making a search under this chapter, the officer or other person about to make it shall call upon two or more independent and respectable inhabitants of the locality in which the place to be searched is situate or of any other locality if no such inhabitant of the said locality is available or is willing to be a witness to the search, to attend and witness the search and may issue an order in writing to them or any of them so to do.

5. The search shall be made in their presence, and a list of all things seized in the course of such search and of the places in which they are respectively found shall be prepared by such officer or other person and signed by such witnesses; but no person witnessing a search under this section shall be required to attend the court as a witness of the search unless specially summoned by it.

6. The occupant of the place searched, or some person in his behalf, shall, in every instance, be permitted to attend during the search, and a copy of the list prepared under this section, signed by the said witnesses, shall be delivered to such occupant or person.

7. When any person is searched under sub-section (3), a list of all things taken possession of shall be prepared, and a copy thereof shall be delivered to such person.

8. Any person who, without reasonable cause, refuses or neglects to attend and witness a search under this section, when called upon to do so by an order in writing delivered or tendered to him, shall be deemed to have
committed an offence under Section 187 of the Indian Penal Code (45 of 1860).\(^1\)

The object of the section is two-fold; first, it provides for the right of free ingress in case of closed premises on demand and on production of the warrant of search by the police officer and, secondly, it seeks to ensure that searches are conducted fairly and squarely and that there is no “planting” of articles by the police. In order to achieve that object the law makes it obligatory, first, that at least two independent and respectable witness of the locality should be present. Only if no such persons are available or willing to be witness to search, then two such persons of another locality may attend and witness the search. The word “independent and respectable” will equally govern the latter case. Secondly, the search should be made in their presence; and the list of things seized in the search should be signed by them. Thirdly, the occupant of the place searched or his representative should be permitted to attend during the search, and to have a copy of the list prepared. When provisions of this section and s. 165 of the code are contravened the search can be resisted by the persons whose premises are sought to be searched.\(^2\)

When a search has been conducted under this section, evidence can be given regarding the things seized in the course of the search and regarding the place in which they were found, in addition to the evidence of the list which the law directs to be drawn up relating to the particulars of the property found.\(^3\)

When all witnesses belong to the police department and no effort was made to associate independent persons of the locality, conviction is not sustainable.\(^4\) It is unsafe to rely on the statements of police officials to convict persons wherever independent witnesses from the locality can be joined before carrying out the search and recovery, but in exceptional cases if the police officer is so trustworthy his evidence can be acted upon.\(^5\)

---

3 Solai Naik, (1910) 34 Mad 349 FB
4 State of H.P. v. Sudarshan Kumar, 1989 (3) Crimes 608 (HP-DB)
5 Islamuddin v. State, 1975 Cr. L.J. 841 (Del).
It is necessary to approach the evidence of punch witnesses, who were involved in criminal cases and residing near the police station, with care and caution.¹

Non-compliance of the provisions of sub-section (4) of s.100 may be an irregularity not affecting the legality of the proceedings, but each case will have to be judged on its own merits.² If punch witnesses are not respectable persons of the same locality but from another locality, it may amount only to an irregularity, not affecting the legality of the proceedings and that it is a matter for courts of fact to consider.³ Non-compliance with the requirements of this section is merely for irregularity and the same cannot be challenged after recording of an order of conviction unless prejudice has been shown to have been caused to the accused.⁴ Although the failure to comply with the provisions regulating searches may cast doubt upon the bonafide of the officers conducting the search, there is nothing in law which makes the evidence relating to an irregular search inadmissible and a conviction based on such evidence is not invalid on that ground alone.⁵ When no efforts were taken to call independent witnesses of the locality who were readily available, there was violation of the section entitling the accused to get an acquittal.⁶ Irregularity in compliance with the provision affects only the weight of evidence and not the legality thereof.⁷ When the procedure prescribed by this provision is not followed the seizure becomes illegal.⁸

Where no independent witness is available the evidence requires scrutiny by the court.⁹ The words “respectable inhabitants of the locality in which the place

4  Dorik Sah v. State of Bihar, 1975 Cr. L.J. 865 (Pat)
7  Khalil v. State, 1976 Cr. L.J. 465 (All)
to be searched is situate" clearly refer to the search of a place and this section does not apply to the search of a person.¹

The burden is always on prosecution to explain the circumstances under which it was not possible to comply with the requirements of this provision of law of associating two independent witnesses of the locality. Merely stating that other persons were asked who did not associate without anything else is not enough. Necessity of shading the prosecution with the burden to justify the breach of the salutary provision of this section, flowed from the constitutional requirement of "reasonable procedure" inscribed in Article 21 of the constitution which enjoined a positive duty on the court to carefully and judicially screen the evidence of search and seizure in the light of the relevant legal provision in case where on the evidence of articles seized, the accused was liable to be convicted for any offence.²

Seizure is not sustainable when witnesses who did not personally see the seizure but on being told of the same later have signed the mahazar.³ The search should be made in the presence of punches. It is not a sufficient compliance with the provisions of this clause that the punches should be summoned and kept present outside a building while the search is being carried on within it.⁴ When independent witnesses kept standing outside the room and were called inside and shown the charges and told that it had been recovered from the room but no copy of the recovery memo prepared or delivered to the accused or any other person, the possibility that the charas, even if held to have been found on search, did not belong to the accused cannot be ruled out, the accused is entitled to the benefit of doubt.⁵

**Disposal of things found in search beyond jurisdiction**

Things found in search at a place beyond the local limits of the court are taken before it, unless the place is nearer to the Magistrate having jurisdiction than

---

¹ Parmeshwar Singh, (1963) 1 Cr. L.J. 342
⁴ Rustam Lari, (1931) 34 Bom LR 267.
⁵ State of H.P. v. Sudarshan Kumar, 1989 (3) Crimes 608 (HP-DB)
to such court, in which case they are taken before that Magistrate who makes an order to take them to such court.¹

**Definition of Seize**

The word 'seize' means to take in actual physical custody.²

The ordinary dictionary and natural meaning of the word “seize” is: “to lay hold of suddenly or forcibly; to take hold of; “to reach and grasp” to clutch; to take possession of by the legal authority”.³

The word “seizure” has been used in this code in connection with the taking of actual physical possession of some moveable property. In the same sense, it has been used in section 83 (3) and section 100. Therefore, a police officer cannot order prohibiting the payment of a debt by the debtor to any body.⁴ It must be borne in mind that in order that an act may amount to a 'seizure' the police must take the property in their physical possession. If the police officer does take the property in his possession, there is no seizure.⁵

**Power of Police Officer to Seize certain Property**

Section 102 of Cr. P.C., 1973 is stated that-

1. Any police officer may seize any property which may be alleged or suspected to have been stolen or which may be found under circumstances which create suspicion of the commission of any offence.

2. Such police officer, if subordinate to the officer in charge of a police station, shall forthwith report the seizure to that officer.

3. Every police officer acting under sub-section(1) shall forthwith report the seizure to the Magistrate having jurisdiction and where the property seized in such that it cannot be conveniently transported to the court,⁶ [or where

---

¹ Section 101 of Cr. P.C., 1973
³ Malnad Construction Co. v. State of Karnataka, 1994 Cri L.J. 645 at 648 (Kant.)
⁵ Kulasana Singh v. H.I. Singh, (1963)2 Cr. L.J. 100 (Para 6).
⁶ Inserted by the Cr. P.C. (Amendment) Act, 2005, Sec. 13(a)
there is difficulty in securing proper accommodation for the custody of such property, or where the continued retention of the property in police custody may not be considered necessary for the purpose of investigation, he may give custody thereof to any person on his executing a bond undertaking to produce the property before the court as and when required and to give effect to the further orders of the court as to the disposal of the same.

1[Provided that where the property seized under sub-section (1) is subject to speedy and natural decay and if the person entitled to the possession of such property is unknown or absent and the value of such property is less than five hundred rupees, it may forthwith be sold by auction under the orders of the superintendent of police and the provisions of section 457 and 458 shall, as nearly as may be practicable, apply to the net proceeds of such sale]

Search by a Police Officer

Section 165 of Cr. P.C., 1973 stated that-

1. Whenever an officer in charge of a police station or a police officer making an investigation has reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorized to investigate may be found in any place within the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as possible, the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station.

2. A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person.

1 Inserted by the Cr. P.C. (Amendment) Act, 2005, Sec. 13(b)
3. If he is unable to conduct the search in person, and there is no other person competent to make the search present at the time, he may, after recording in writing his reasons for so doing, require any officer subordinate to him to make the search, and he shall deliver to such subordinate officer an order in writing, specifying the place to be searched, and so far as possible the thing for which search is to be made; and such subordinate officer may thereupon search for such thing in such place.

4. The provisions of this code as to search warrants and the general provisions as to searches contained in section 100 shall, so far as may be, apply to a search made under this section.

5. Copies of any record made under sub-section (1) or sub-section (3) shall forthwith be sent to the nearest Magistrate empowered to take cognizance of the offence, and the owner or occupier of the place searched shall, on application, be furnished, free of cost, with a copy of the same by the Magistrate.¹

This section now authorizes a general search on the chance that something might be found. But the officer acting under this sub-section (1) or sub-section (3) must record in writing his reasons for the making of a search: and under subsections (1) and (3) the thing shall be specified as far as possible. The provisions of s.100 and 165, are mandatory.²

The recording of reasons is an important step in the matter of search and to ignore it is to ignore the material part of the provision governing searches. If that can be ignored, it cannot be said that the search is carried out in accordance with the provisions of the code, it would be a search made in contravention of the provisions of the code.³

² Selvan v. State, 1991 Cr. L.J. 1942, 1945 (Mad)
The non-conformity with any of the requirements of the provision must be confined to that part of the investigation which relates to the actual search and seizure but once the search and seize is complete that provision ceases to have any application to the subsequent steps in the investigation.\(^1\)

2.3 Process to Compel Production of things

When (a) a court, or (b) an officer in charge of a police-station considers that a document or thing in necessary or desirable for any investigation, inquiry or trial or other proceeding, the court may issue a summons, or the officer an order, to the person in whose possession or power it is to produce it at a specified time and place. Such document or thing may be produced by the person himself or by someone on his behalf.\(^2\)

If the document (letter or telegram) or thing (Parcel) is in the custody of the postal or telegraph authorities, the District Magistrate, the Chief Judicial Magistrate, Court of Session or the High Court may require such authorities to deliver it to such person as the court directs. If such document or thing is wanted by any other Magistrate, or the Commissions of Police, or the District Superintendent of Police, he may require the postal or telegraph authorities to search for and detain it pending the orders of the District Magistrate, Chief Judicial Magistrate or the court.\(^3\)

When any court has reason to believe that a person to whom an order or requisition to produce or obtain a thing has been issued will not or would not produce the document or thing, or where the court considers that he purposes of any proceeding under the Cr.P.C. will be served by a general search or inspection, or such document or thing is not known to the court to be in the possession of any person, it may issue a search-warrant and the person to whom such warrant is directed, may search or inspect in accordance the conditions of the warrant and the

\(^2\) Section 91 of Cr. P.C. 1973; Om Prakash Sharma v. CBI, AIR 2000 SC 2335.
\(^3\) Section 92 of Cr. P.C., 1973
provisions contained in Cr. P.C. in this regard. A person in charge of a closed place where the proposed search is to be carried out by a police officer has a duty to allow the search.

2.4 Filing of Charge-sheet

Once the investigative police officer collects the required evidence which would sustain in the court of law, with the help of prosecutor, files the concerned charge-sheet along with a detailed report as envisaged by section 173 of Cr. P.C.

Report of the Police on Completion of Investigation

Section 173 of Cr. P.C., 1973 stated that-

1. Every investigation under this chapter shall be completed without unnecessary delay.

1A. The investigation in relation to rape of a child may be completed within three months from the date on which the information was recorded by the office-in-charge of the police station.

2(i). As soon as it is completed, the officer-in-charge of the police station shall forward to a Magistrate empowered to take cognizance of the offence on a police report, a report in the form prescribed by the State Government, stating-

(a) the name of the parties;
(b) the nature of the information;
(c) the names of the persons who appear to be acquainted with the circumstances of the case;
(d) whether any offence appears to have been committed and, if so, by whom;
(e) whether the accused has been arrested;

---

1 Section 93 to 101 of Cr. P.C.
2 Section 100 of Cr. P.C.
3 Section 173 sub section (1) clause (1A) inserted by Code of Criminal Procedure (Amendment) Act, 2008
whether he has been released on his bond and, if so, whether with or without sureties;

whether he has been forwarded in custody under section 170.

whether the report of medical examination of the woman has been attached where investigation relates to an offence under sections 376, 376A, 376B, 376C or 376D of the Indian Penal Code.

The officer shall also communicate, in such manner as may be prescribed by the State Government, the action taken by him, to the person, if any, by whom the information relating to the commission of the offence was first given.

Where a superior officer of police has been appointed under section 158, the report shall, in any case in which the State Government by general or special order so directs, be submitted through that officer, and he may, pending the orders of the Magistrate, direct the officer in charge of the police station to make further investigation.

Whenever it appears from a report forwarded under this section that the accused has been released on his bond, the Magistrate shall make such order for the discharge of such bond or otherwise as he thinks fit.

When such report is in respect of a case to which section 170 applies, the police officer shall forward to the Magistrate along with the report-

(a) all documents or relevant extracts thereof on which the prosecution proposes to rely other than those already sent to the Magistrate during investigation;

(b) the statements recorded under section 161 of all the persons whom the prosecution proposes to examine as its witnesses.

If the police officer is of opinion that any part of any such statement is not relevant to the subject-matter of the proceedings or that its disclosure to the accused is not essential in the interests of justice and is inexpedient in the

---

1 Section 173 sub-section (2 (i)) clause (h) inserted by Code of Criminal Procedure (Amendment) Act, 2008.
public interest, he shall indicate that part of the statement and append a note requesting the Magistrate to exclude that part from the copies to be granted to the accused and stating his reasons for making such request.

7. Where the police officer investigating the case finds it convenient so to do, he may furnish to the accused copies of all or any of the documents referred to in sub-section (5).

8. Nothing in this section shall be deemed to preclude further investigation in respect of an offence after a report under sub-section(2) has been forwarded to the Magistrate and, where upon such investigation, the officer-in-charge of the police station obtains further evidence, oral or documentary, he shall forward to the Magistrate a further report or reports regarding such evidence in the form prescribed; and the provisions of sub-sections (2) to (6) shall, as far as may be, apply in relation to such report or reports as they apply in relation to a report forwarded under sub-section(2).

There are three different kinds of reports to be made by police-officers at three different stages of investigation. (1) Section 157 requires a preliminary report from the officer-in-charge of a police station to the Magistrate. (2) Section 168 requires reports from a subordinate police officer to the officer-in-charge of the station. (3) Section 173 requires a final report of the police officer as soon as investigation is completed to the Magistrate. Seven years delay was held a good ground for setting aside the order of conviction.¹

The word “shall” in S.173, is only directory and not mandatory; non-compliance of the provisions of the section does not vitiate the trial.²

The phraseology “charge-sheet” not at all find mention in any of the provisions of the code.³ The report under this section is called ‘Completion Report’. It is also known as ‘charge-sheet’. Such a report is absolutely necessary.⁴ The report should contain the particulars referred to in sub-clauses (a) to (g) of cl.

---

¹ Mihir Kumar v. State of W.B., 1990 Cr. L.J. 26 (Cal)
² Bhole v. State of M.P., 1993 Cr. L.J. 2821 (MP)
³ Sakkarai Ramaswamy v. Alangara Muni, 1990 Mad LW (Cri) 151 (DB)
⁴ Appa Ragho, (1914) 17 Bom LR 69
(i). A Magistrate who has disposed of a police report is competent to revise his order and call for a ‘charge-sheet’.¹

The final report submitted by the investigating officer is not final, where the investigating officer has not conducted the case properly, has acted negligently and carelessly, there is material on the record and there is further scope for investigation, the Magistrate may order for further investigation under S.156(3) Cr.P.C.²

Once a detailed report under this section is submitted after complete investigation and the Magistrate on the basis of such report passes an order, “complaint recorded as mistake of law” to the effect that there was no case; such an order is judicial and becomes final and unless that is set aside, and without any permission from the court, re-investigation on the same case in illegal.³

2.5 Additional Evidence During Trial

However, under certain circumstances, even after filing charge-sheet, the investigative police officer is empowered to file additional investigative report in the form of additional evidence before the court of law. This is facilitated by section 173 (8).

The power of the police to conduct further investigation, after filing final report, is recognized under S. 173(8) Cr. P.C. Even after the court took cognizance of any offence on the strength of police report first submitted, it is open to the police to conduct further investigation. This section confers an express and specific power in the police to carry out further investigation after cognizance is taken by the court.⁴ Even after taking cognizance of the matter the court is entitled to direct the investigating officer to make further investigation in the case.⁵ An order for further investigation is not a judicial order and hence no precise reasons

¹ Uma Singh, (1932) 12 Pat 234
² Dilip Kumar Roy v. State, 1994 Cr. L.J. 3489, 3493 (Cal).
³ Namsivayam v. State, 1982 Cr. L.J. 707 (Mad).
be given in the order. The matter as to whether there exist sufficient and valid grounds for further investigation is entirely for the consideration of the investigating officer, and the court cannot give any direction restraining the investigating officer from conducting further investigation.

This sub-section is based on the necessity to confer express power on the police to make further investigation and submit supplemental reports. Whenever fresh facts occur to be the police resulting in further investigation, it is the duty of the police to send a supplemental report based on such materials to the Magistrate and this statutory duty cannot be lightly dealt with. The power of the investigating agency to investigate and submit further report is recognized by this provision. This provision permits filing of revised report on getting fresh materials. A second charge-sheet cannot be filed without further investigation and without obtaining further evidence. Cognizance of a Magistrate does not bar further investigation.

Sub-section(8) is inserted as a new provision and the circumstances mentioned are only enumerative and not exhaustive in character. If a new interpretation of the material is brought to the notice of the investigating officer, he can certainly file an additional charge-sheet through there may not be strictly speaking any further investigation and collection of new material. Supplementary charge-sheet cannot be submitted without making further evidence. The Court of Session has power to direct further investigation by police under s. 173 (8).

Further investigation can be conducted by the same agency which initially investigated the case and not by a different agency. Even where Magistrate has
Further investigation can be conducted by the same agency which initially investigated the case and not by a different agency.\(^1\) Even where Magistrate has accepted report filed under S.173(2), on fresh material further investigation under S.173(8) is permissible. Notice to the accused is not necessary, under S.173(8) after investigation further report is to be submitted s. 173 (8) does not contemplate any supplementary report.\(^2\) Where further investigation brings to light fresh material, the Magistrate is not barred from taking cognizance merely because he has accepted final report.\(^3\) The Magistrate after taking cognizance of an offence cannot pass an order for further investigation under s. 173 (8) by CBI unless the police makes an application praying for formal sanction of the court for further investigation.\(^4\) Once cognizance has been taken by the court on the basis of case-diary and *prima facie* case, subsequent reopening of investigation without any basis, or material on record is illegal and not sustainable.\(^5\) The investigating officer is not vested with unbridled power to re-investigate and rope in any person without sufficient evidence to proceed against.\(^6\) More persons can be added as accused when there is adequate material and evidence collected by the investigating agency by passing a speaking order.\(^7\)

### 2.6 Evidence during sentence hearing

If the court records conviction, at the stage of hearing also the investigative police officer is empowered to adduce relevant evidence to sustains a particular form of punishment. This is facilitated by section 235 (2).

### 2.7 Judgment of Acquittal or Conviction

Section 235 of Cr. P.C. stated that-

1. After hearing arguments and points of law (if any), the judge shall give a judgment in the case.

---

The provision in clause (2) of this section was newly added and it did not exist in the old code of 1898.

3. **Investigation of Cyber Crime**

Cyber crime are difficult to detect and even more difficult to prove. Criminals often leave no trace. Cyber crimes may even transcend national borders making investigations complicated. Recovery of computer based evidence is a difficult task involving data recovery techniques. Search and seizure of electronic evidence also demands high technical skills.

Computer investigation require a considerable amount of time because of the large volume of data to be scanned for detecting the crime and for evidential purposes. The investigations also involve interaction with victims. Victims could be experts and sometimes the perpetrators of the crime themselves. Technical knowledge of computer systems, operating systems and various computer software would be a must for effective investigation.

3.1. **Power to Investigate Offences**

Section 78 of I.T. Act states that, Notwithstanding anything contained in the Cr.P.C., 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act (Amended vide ITAA 2008).

3.2. **Steps for Investigation**

The first step is the preparation for FIR completion for legal formalities prior to inspection of the scene of crime besides forming a core team. In FIR, it must include the description of the offence and relevant section of I.T. Act, date, time and place of offence, suspects or accused, date and time when the offence was discovered, by whom and how discovered, suspect organizations or companies, if any, victim company or organization, details of hardware and software configuration of the computer system which have been the target of attack, details of damage caused including extent of financial loss caused, details of damage caused including extent of financial loss caused besides e-mail address of the host computer etc.
attack, details of damage caused including extent of financial loss caused, details of damage caused including extent of financial loss caused besides e-mail address of the host computer etc.

The investigator must determine the Modus Operandi or motive behind the Cyber crime. Whether the damage caused is due to hardware failure or software failure, or whether it happened due to negligence or carelessness, or whether it is caused by mischief, willfully malicious act, who is the real beneficiary for the kind of acts, etc.

1st Step-FIR:-

The following information should be incorporated in the First Information Report:

(a) Description of the offence and relevant sections of law
(b) Date, time and place of offence
(c) Suspects or accused
(d) Date and time when the offence was discovered, by whom and how discovered
(e) Suspect companies or organizations
(f) Victim organization
(g) Details of hardware and software configuration of the computer system which have been the target of attack
(h) Phone number and E-mail of host computer
(i) Details of damage caused including extent of financial loss caused
(j) Modus operandi
(k) Details of the informant or complainant and how he/she came across the information
(l) Details of the inspection of the computer system conducted, if any, to detect the crime and status of the computer systems at the time of such inspection.

Interpol has already designed a standard cyber crime message format, which could be used by the member countries. There is need for rapid
IInd Step

Investigation of computer related crimes requires computer skills. Various technical experts may also have to be associated with the investigations. One of the most difficult tasks for the investigator is to isolated machine failure from human failure such as errors and mischief. The investigator has to determine:

(a) What is the damage caused?
(b) Was is caused by hardware failure?
(c) What is caused by software failure?
(d) Was there negligence or carelessness on the part of human beings?
(e) Was it caused by mischief- a willful and malicious act?
(f) What was the motive- fun, financial loss to the organization and corresponding gain to the perpetration?
(g) Who was the beneficiary?

IIIrd Step

(1)(a) The first step would be to thoroughly inspect the computer systems which were used by the criminal to commit the crime. This could be done with the help of technical experts in hardware and software of the subject organization.

(b) Before checking the files, it may be necessary to check the system for VIRUSES. Virus check and inspection of the computer system should be properly documented. Virus check includes virus scan, identification of the viruses present and their removal. It may have to be investigated whether the viruses were introduced into the systems by the hacker alter commission of the crime.

(c) An inventory of the computer systems, hardware, operating system, utility software, DBMS/RDBMS packages used, application software, data communication and networking systems, peripherals such as scanners, printers, modems, etc. should be prepared.

(d) Details of backup facilities, backup tapes, a listing of authorized users of the system and their password including the super user or system
communication and networking systems, peripherals such as scanners, printers, modems, etc. should be prepared.

(d) Details of backup facilities, backup tapes, a listing of authorized users of the system and their password including the super user or system administrator’s password should be obtained and documented. The computer system may have to be impounded depending on the damage done to the system and the possibilities of manipulations of destruction of computer based evidence,

(e) A description of the data security features of the system, if any, should be made. This would include physical security, access restrictions, details of authorized users and their log-in user ID, user name, and password which could be listed with the help of the system administrator or the person in charge of the computer system. The computer system will have to be examined to find the access right of each individual authorized user and whether any recent changes were made in the access rights of any user.

(2) A listing or backup of all files in the system could be prepared using a backup tape or optical disk. The log-in details of the system for one or two months preceding the crime incident should be obtained from the system with the help of a technical expert in the presence of the system and database administrator of the system.

(3) Details of employees - past and present should be obtained and their presence or where about obtained.

(4) All the employees - past and present should be examined to ascertain their antecedents, their financial needs, recent financial transactions or acquisition of assets, extent of their technical knowledge and their loyalty to the organization concerned. It is necessary to identify whether any employee was disgruntled and whether any employee was included to break the trust reposed in him or her. Usually insiders are suspects in computer related crimes.

(5) All user and technical manuals of the system including software listing should be obtained and examined.
also modems and communication lines or telephone lines should be thoroughly inspected. The inspection of computer systems should be done by an expert in the presence of the owner of the system, if available, and in the presence of two independent witnesses. Presence of notebook or portable computers should also be checked as it is possible to establish communication with the target computer systems through a notebook computer with modem connected to any telephone line.

A listing of telephone calls made from the telephone or telephones installed in the premises may be useful for ascertaining whether any telephonic link was established with the computer system in question on the relevant data and at the relevant time.

**Vth Step: Tracking and Examination of Suspects or Accused Persons**

Suspects should be immediately traced and apprehended. In a case reported by Roger Addelson, an Amsterdam bank officer had fraudulently transferred $15.1 million to a Swiss account opened by two accomplices. The banker had used the password of an executive network failure, a second transfer could not be effected and the system’s apology for the failure exposed the fraud. The Swiss bankers and the police were quickly notified and when the culprits tried to withdraw part of the funds in Zurich, they were apprehended by the police.

The following persons who are connected with the target computer system should be examined by the police:

(a) Database Administrator
(b) System Administrator
(c) System Analysts/Programmers attending to the maintenance of the system
(d) System Analysts/Programmers who developed the application software used
(e) Computer operations.

**VIth Step**

Identifying the time of break in (logging in and logging out), the log-in name used for break in and the communication channel used may be crucial to the
(c) Computer operations.

**VIth Step**

Identifying the time of break in (logging in and logging out), the log-in name used for break in and the communication channel used may be crucial to the investigations. For identifying the communication channel, the telephone number and address of the target called would have to be ascertained.

**VIIth Step Analytical Tools**

Operating systems or programs which do the basic tasks of a computer, closely monitor the activities of anyone using the system. The operating system should be examined by the computer expert or forensic computer technologist to list the log of all users of the system and the files accessed by the users prior to the incident in question and relevant to the incident. These may serve as audit trails or electronic footprints.

In the case of physical break in and criminal trespass, it may be necessary to look for latent fingerprints of the criminal. The keyboard or the mouse may have to be examined by fingerprint experts in this connection.

Handwriting examination may also become relevant in the case if funds transferred and collect at the destination against a voucher filled in by the criminal or his associate.

### 3.3. Handling, Labeling & Packing of Computer Evidence

It is advisable to collect all relevant material from the scene of crime including all hardware, software, computer diskettes, tape and other storage media, documents found at the scene, peripheral equipment including printers, modems, cables, etc., discarded documentation, printouts, printer ribbons and trash collected from waste bin.

(A) The investigating officer should, however, follow certain guidelines in handling the potential. Following are some do’s and don’ts:

**Do not**

- Don’t disconnect the power before evaluating the overall problem
Do

- Videotape the scene to document the system configuration and the initial condition of the site on your arrival and the condition of the equipment you see.
- Photograph the equipment with its serial number, model number and wiring schemes.
- Label all evidence so that cables and other equipment can be reassembled in the same exact configuration.
- Write-protects all diskettes at the scene and make sure that they are labeled.
- In case of mainframe computer, secure the equipment and determine relevant parts of hardware and software that require close scrutiny and then collect the same. Connect a dialed number recorded to telephone or auto dialed for tracing the intruder. Place an outgoing call recorded through each auto dialed or telephone number storage board and obtain a printed record of the stored telephone number or telephone access code within the resident memory.

The following auditing tools and utilities can be used depending upon the nature of investigation:-

1. Test data method which modifies the processing accuracy of the computer application systems.
2. Integrated test facility which reviews those functions of auto applications that are internal to the computer.
3. Similar simulation which processes live data files and simulates normal computer application processing.
4. Snap shot which takes a picture of an computer memory that contains the data elements in a computerized decision making process at the time the decision is made.
5. Mapping which assesses the extent of computer testing and identifies specific program logic that has not been tested.
4. Snap shot which takes a picture of an computer memory that contains the data elements in a computerized decision making process at the time the decision is made.

5. Mapping which assesses the extent of computer testing and identifies specific program logic that has not been tested.

6. Code comparison which compares two copies made at different times, of the program coding for a particular application.

7. Check sums which provide a numerical value to the execution module that can be computer to later suspected modules.

(b) The following guidelines prepared by the Computer Analysis and Response Team of FBI Hqrs. Lab, Washington DC are useful for Investigators;

1. For wrapping the equipment or media, anti-static plastic material should be used.

2. Before wrapping, all the equipment should be disconnected from power and should be brought to room temperature.

3. Since the physical machine might not actually be part of the evidence, a copy of the hard disk should be made first to conduct major part of the investigation.

4. The Central Processing Unit (CPU) should be thoroughly checked and the hard disk drive read/write heads should be secured with appropriate software commands. The drive should not be removed from the computer. The monitor and the CPU should be separately wrapped after duly labeling each part including cables and ports. The keyboard should be separately packed. Any external or removable hardware, floppy diskette devices should be wrapped separately after proper labeling.

In case of printers and plotters, the dip switch settings should be noted and the ribbon removed carefully as it may provide information on most recent text printed. The modems and other coupling devices should be disconnected from the
All manuals, hardware, notes, loose sheets, pads and other documents should be handled with gloves to preserve latent fingerprints for examinations. Similarly, the printouts, listings should also be carefully handled for latent fingerprint examinations and all these items can be packed in cardboard boxes.

3.4 Examination of Computer Evidence

After following the rules of chain of custody of evidence, actual examination can be undertaken in the following steps:

1. Mark and initial each piece of evidence and segregate them for undertaking different types of studies such as accounting, latent fingerprint examinations, cryptography record verification and other minute analysis.

2. Instead of using the suspect system disk and the software, the investigator should use his own system disk to examine the computer.

3. If the system involved in the cyber crime is operational, check to determine if the system is fully operational at the time of seizure if not take logical steps to make the system operational.

4. Write protect all diskettes, identify the computer to be used for examination, convert the operating system, if necessary, create directory or subdirectory testing’s and check for deleted or deleted files using custom software and take a printout of all files.

5. After making a detailed analysis in conjunction with related data obtained from various sources and observations made during analysis, prepare a report documenting the process adopted for analysis in a chronological order.

6. The report should include the printouts and other observations and conclusions on each of the points raised in the investigation. Finally, repack all the hardware as packed initially.

Standard tools such as compilers, assemblers, dissemblers and debuggers are required for reverse engineering of software that is essential for interpretation of evidence. Digital storage oscilloscopes and logic analyzers to computer
6. The report should include the printouts and other observations and conclusions on each of the points raised in the investigation. Finally, repack all the hardware as packed initially.

Standard tools such as compilers, assemblers, dissemblers and debuggers are required for reverse engineering of software that is essential for interpretation of evidence. Digital storage oscilloscopes and logic analyzers to computer hardware and communication protocols are required for reliable and non-destructive analysis of hardware evidence.

3.5. Search and Seizure

Conducting search in a computer environment is, no doubt, a new challenge to the law enforcement officers. By way of adopting the new skills and thought processes, the principles of search and seizure and the procedure, should be adopted. The assistance of expert to the investigating officer is essential in the process of search and seizure of an electronic device like computer.

Preliminary preparation

Before taking actual search, preliminary preparation is necessary. At first, the investigating officer must clear in his mind about three things—(1) the kind of search environment and other concerns about (2) where to conduct the examination of evidence, and (3) when the search is to be conducted.

Search environments

The search is to be conducted depends upon how the computers are connected and what function they performs. The search site may comprise any one or a combination of the following:

(i) **Stand above computers:** A computer ordinarily comprises of a Central Processing Unit (CPU) as input device (such as keyboard), an output device (such as monitor or printer). It may also be having additional devices for input, output or storage. Stand above computer means that it is self contained and is not directly connected to another computer. It has its
(iii) **Mainframes:** In this type of environment, many terminals are attached to a large computer. There terminals do not have the ability to process information. All of that is done at the mainframe. It processes, prints, stores and directs information to terminals. It is the solitary and central “brain” in the system.

**Searching place**

The examination of electronic evidence should be conducted only in two places —

1. at the place where it is found, and
2. at the laboratory.

**Timing**

When the search is to be conducted, it has to be decided upon two factors—

(a) states of the computer system, and
(b) presence or absence of particular persons.

Late night or early morning will be ideal to undertake the search, as the computer are likely to be found either down or engaged in off-line functions.

**Actual Search**

After obtaining the search warrant, the first duty of the law enforcement officer is to secure a scene i.e. take control of location and persons therein for several reasons after entering upon the location. After securing the scene from physical and environmental threats-separate people from computers, and determine if any evidence is at immediate risk. Close up photography of all connections between individual pieces of hardware is required.

Once the above tasks is completed, it is important to establish a stable working environment and I.O. may begin the actual search besides allowing to lift the finger prints from each computer components by the experts, if necessary, should be marked as to where cables are connected. Either a descriptive (i.e. LPT I Serial port, monitor connector) or numerical (i.e. Port I, connector I) labeling system may be used.
Once the above tasks is completed, it is important to establish a stable working environment and I.O. may begin the actual search besides allowing to lift the finger prints from each computer components by the experts, if necessary, should be marked as to where cables are connected. Either a descriptive (i.e. LPT I Serial port, monitor connector) or numerical (i.e. Port 1, connector 1) labeling system may be used.

Once all of the documentation of the system is complete, disassembling can begin. Where there are multiple computer systems, it is important to keep items from one system separate from others. It is necessary to handle the computer equipment gently.

**On Scene Examination**

Depending on the legal, practical and logistical concerns present, it may be necessary to conduct an examination of the evidence on site. Conversely, of there is very large volume of material, a limited examination may need to be conducted to eliminate non-pertinent machines and/or media. It is necessary to seize those items which are likely to contain evidence.

**Mark and Initial Items**

Before disconnecting or disassembling any computer components, everything should be labeled or tagged, initiated and dated. It is suggested that items with a single Central Processing Unit be assigned a single item number with appropriate sub-numbers. If the room in which the computer is seized marked as “F”, a single computer might have marked as “F-5”. The keyboard might be assigned on “F-5-1”, the monitor “F-5-2” and CPU as “F-5-3” and so on. It is also necessary that cabling be documented precisely prior to removal. This is accomplished by using tape and/or tags to mark each end. A corresponding tape or mark is placed on the device to which it is connected.

**Initial and Dated on Seized Items**

Each item should be initialed and dated by the seizing person. This will ensure that if a single item is entered into evidence, there will be a solid chain of custody.
Further, I.O. must keep in mind the provisions of the Criminal Procedure Code in relation to any entry, search or arrest made in this regard. (Sec. 80 of I.T.(Amendment) Act, 2008).¹

4. CHALLENGES IN THE INVESTIGATION OF CYBER CRIMES

The word community as a whole is increasingly being dependent upon information technology in managing all its affairs. The very attraction of the cyberspace for conducting these affairs in a more speedy and efficacious way has also brought in increased danger from the activities of criminals and perverted persons. An analysis of the ‘criminogenic’ factors shows that modern computer and communication networks have specific characteristics which are highly useful for perpetuators but which imply difficulties for potential victims and for law enforcement agencies.

The law enforcement agencies and society through out the world are facing many challenges in their fight against the compute crimes in a network environment. These challenges are following:-

4.1 Lack of Realization About Crime

Many a time the victims are not even aware of the fact that a crime has been committed against them. For example innumerable number of worms and virus attacks take place in the cyber world but only when they carry out visible damages that they get noticed. Similarly many a PC user will never be aware of the Trojan horses that might infect their computer when they surf the internet. The individual might not ever realize misuse or improper use without consent, of personal data given out in the internet.

4.2. Non-Reporting of Crime

It has been suggested that what Crime is being reported in the cyber context is only a tip of the iceberg. Coupled with the non-realization of the incidence of crime is the fact that many a victim chooses not to report the incidence at all.

individual might not ever realize misuse or improper use without consent, of personal data given out in the internet.

4.2. Non-Reporting of Crime

It has been suggested that what Crime is being reported in the cyber context is only a tip of the iceberg. Coupled with the non-realization of the incidence of crime is the fact that many a victim chooses not to report the incidence at all.

4.3 Geographic Indeterminacy

Another challenge before the investigating agencies is the virtual features of geographically extended sharing of scattered resources of the Internet that renders the network technologically indifferent to physical location. So insensitive is the network to geography, that it is frequently impossible to determine the physical location of a resource or user. Such information is unimportant to the network’s function or to the purpose of its creators, and the network’s design thus makes little provision for geographic discernment. Internet protocols were not designed to facilitate geographic documentation; in general, they ignore it. Internet machines do have “addresses”, but these locate the machine on the network, and not in real space. Of course, some internet addresses do include geographic designators, or designators that might be geographically identifiable. For example, an Internet address containing the domain “.uk” located in the United Kingdom. However such extensions of a domain-style name may not tell you anything about who maintains the computer corresponding to that address, or even (despite country codes) where that machine is located.

There is nothing for a user to do to conceal his geographic location when she is logging on to internet. Geographic anonymity is an inherent characteristic of the Net. The facility of remote log-on anticipate only the most routine uses of the Internet’s capabilities; they do not involve advanced technology, such as public key cryptography or anonymous remailers that could be used to actively conceal a

---

4.4 Inadequacy of Law and Procedure

The worldwide experience shows that the traditional laws and procedures dealing with crimes are not sufficient in dealing with computer crimes or cybercrimes.1

cyber crime is no longer the problem afflicting only the developed countries and hence all the nations should now treat this menace seriously. Writing a virus programme or denial of service attacks etc., are not ordinary crimes that should be taken lightly, since they may involve huge financial and security implications. To effectively combat the cybercrime, it is not sufficient to successfully investigate the crime and nab the criminal, but more important is to prosecute and administer justice, according to the law of the land. This requires an effective legal framework, which fully supports the detection and prosecution of cyber criminals. The traditional techniques for investigation of computer crime and the prosecution procedure are inadequate. The judiciary must also appreciate the intricacies of the digital evidence that is collected and presented in the courts of law, in spite of the technical and operational hurdles the investigator faces.2

In the G8 Nations Cyber Crime Conference in Pairs, the French President Jacques Chirac had stated, “what we need is the rule of law at an international level and a universal legal framework, which is equal to the worldwide reach of the internet.” It is therefore, necessary to make appropriate dynamic laws pertaining to cybercrime. It cannot take the usual snail’s pace of law making, since the technology changes at a very fast rate. The laws made today for yesterdays technology might become out dated by the time they are enacted.

4.5 Diverse National Legal Response

Though cybercrime is an international phenomenon the response to it, as of now, is national in nature. There is a huge variation in national responses to each variant of cybercrimes and this also contributes to the problems of investigators in conducting transnational investigations. The difference in substantive laws defining offences, make it difficult to obtain extradition of accused persons to stand trial in another country’s court. Even more difficult is the problem caused by different procedural laws relating to search, seizure and evidence etc.

4.6 Technical Nature of Crimes

The technical nature of most of the cybercrimes\(^1\) makes it difficult for the traditional laws enforcement agencies to investigate them.

The investigating agencies must have a dedicated team of professionals who thoroughly understand computer as well as communication technology. They should also be trained and equipped in the art of computer crime investigation to assist the regular law enforcement agencies and prosecutors. They should be in a position to quickly respond to an incident, as their response time is paramount in most of the cases. In case of delay, the evidence may be destroyed or lost forever. There is a severe shortage of adequately trained computer forensic scientists. Advanced in technology are made every day, causing the constant updated need for training in this area.

The complexity of these technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a fulltime basis, immersing themselves in computer related investigations and prosecutions.\(^2\)

---

1. Even in simple crimes that are amenable to a layman, the investigation and evidence collection may require relatively higher technical knowledge.

5. PROBLEMS OF REAL WORLD LAW

In traditional procedural laws, these exist some cooperation in the form of conventional mutual assistance agreements, particularly the procedure of the letter regatory. This procedure in which a state is requested to undertake an investigation on its own territory on behalf of the investigating State is highly time consuming one. While performing investigatory actions in case of cybercrimes, the suddenness can only be achieved by different factors-time, place, character and made of measures implemented by the investigators. The interrogation of convicted persons showed that in 71% of cases they were surprised by the place and time of carrying out the investigatory action; in 46.5% of cases the unexpectedness was achieved by the factor itself of realizing the investigatory action, circle of persons drawn in it and character of used evidences. Therefore, any process that is time consuming will be practically of no use since it becomes easy for the accused to destroy any evidence of his act. Some of the specific issues faced by real world law in investigating virtual world crimes are briefly discussed in the following sub-para:-

5.1 Search and Seizure in Automated Information Systems

Investigation of cybercrimes often requires collecting and evaluating data stored in some systems. In a transnational computer crime the data may be stored in a system located in another country.

As for as the information stored in a corporeal data carrier, the real world law does not find much problem since its provision as to search and seizure of things or documents of likely evidentiary value could well cover such instances. The power of search and seizure conferred on police officers under criminal

As for as the information stored in a corporeal data carrier, the real world law does not find much problem since its provision as to search and seizure of things or documents of likely evidentiary value could well cover such instances. The power of search and seizure conferred on police officers under criminal procedure would also include the power to inspect or analyze the internal contents or memories of the seized articles of data carriers such as Floppy, CD etc.

However the inadequacy of the real world procedural rules becomes eminent, when we have to deal with data that are not permanently stored in a corporeal carrier. Indian Information Technology Act, 2000 has, to some extent, addressed these issues by amending the Indian Evidence Act, 1872 and including the terms ‘electronic record’ in the definition of the term ‘evidence’. The available computer forensic software tools permit the investigating agencies to make such electronic records. Also, the newly inserted Section 22A of Indian Evidence Act permits oral evidence as to the contents of electronic records Where the genuineness of the electronic record produced in question. However, these question desperately need global answers to empower the investigative agencies to deal with cybercrimes.

Question also arise as to what degree the power of search and seizure include the power to use technical equipment and programs belonging to a witness or to an accused, in order to search and/or fix computer data. Many legal systems of the world are salient in this aspect.

5.2. Duties of Active Cooperation

---


2 Section 165 of Cr.P.C. The words used in the section are “anything necessary for the purpose of investigation” and hence the section covers not only corporeal things but also even magnetic impulses in electronic data carriers.

3 The term ‘electronic record’ will have the same meaning assigned to it in the Information Technology (Amendment) Act,2008 i.e. ‘electronic record’ means date, record, or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.
reasonable facilities for a search therein. Such duty to cooperate in searches and to surrender the seizable objects can help the investigating officers in selecting specific data carries from among the many that are usually stored in a computer centre. However, these provisions are not found in many of the countries and thus pose difficulties for the investigators in identifying and securing data that are of evidentiary value even when they are held in the custody of persons other than the perpetuators of the crime.

(ii) Duty to testify

The second important instrument of active cooperation is the duty to testify. The Cr. P.C. also contain provisions1 as to the power of investigating officers to require attendance of witnesses and their examination. However, this duty of the possible witnesses to attend the examination and give out correct replies only include a duty to testify what is known to him and does not amount to a duty to find out the truth and then speak the same. Therefore, these provisions may not place any duty on a person to search for correct information and produce the same before police.

To make investigation of computerized environment more efficient, some countries have enacted or suggested new compulsory duties to produce specific information. For example, the Police and Criminal Evidence Act, 1984 of the United Kingdom provides that the constable “may require any information which is contained in a computer and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible”. This provision confer a duty upon the persons in charge to produce copies of printouts of the information contained in their systems and thus make the duty of active cooperation more meaningful in the context of cyber crime investigations. In India, section 29 (2)2 of the Information Technology Act, 2008 confers such a

---

1 Section 160 to 163 of Cr. P.C.
2 Section 29 (2) of I.T. Act, 2008 States that: For the purpose of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.
provision confer a duty upon the persons in charge to produce copies of printouts of the information contained in their systems and thus make the duty of active cooperation more meaningful in the context of cyber crime investigations. In India, section 29 (2)\(^1\) of the Information Technology Act, 2008 confers such a duty of active cooperation upon person in charge of computer systems or data. In Canada, the Mutual Legal Assistance Act provides for an evidence gathering order addressed to a person “to make a copy of a record or to make a record from data and to bring the copy or record with him”. However, with respect to data accessible via international telecommunication networks, these provisions leave open the question whether and to what degree a State, in accordance with international public law, has the right to oblige its citizens to gather evidence in foreign countries. Furthermore, other than in respect of recognized privileges, it is unclear under which conditions citizens have the right to deny cooperation.

5.3. Wire Tapping and “eavesdropping”

Tapping of telecommunication lines and eavesdropping on computer networks is unavoidable in investigating cyber crimes especially where data are only transmitted and not permanently stored, or where data merely cross a country or where permanent observation of telecommunication or computer activities is necessary.\(^2\) However, unlike search and seizure that amounts to visible interference for a limited timeframe, interception of an communication amounts to more severe intrusion into the right to privacy of an individual. Therefore, power of intercepting and recording of communication channels are subjected to stringent procedural controls in most of the countries.

Further, the question whether the traditional powers of wire-tapping can be applied to tapping other telecommunication services and computer systems is

---

1 Section 29 (2) of I.T. Act, 2008 States that: For the purpose of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

from aural communication (covered by the Omnibus Crime Control and Safe Street Act of 1968) to electronic communication. Similarly, in the Federal Republic of Germany, an amendment to the Criminal Procedural Code in 1989 extended the possible use of wire-tapping to public telecommunication networks. With respect to future policy-making, such clarifications are helpful since telecommunication between computers probably does not merit more protection than telecommunication between persons.

In India, traditional wiretapping powers of the Government are contained in sub-section (2) of section 5 of the Indian Telegraph Act, 1885. This section permits Governments to carry out interception of telecommunication lines under certain circumstances of importance. Apart from this general provision, some special legislations, like the Prevention of Terrorism Act, 2002 also contained power to intercept communication networks and information flow in order to deal with organized crimes and terrorism.¹ Specific power to intercept information transmitted through any computer resources is provided by section 69 of the Information Technology (Amendment) Act, 2008.

Section 69 of Information Technology (Amendment) Act, 2008 States –

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

¹ Chapter V of Prevention of Terrorism Act, 2002 and Section 14 to 16 of the Maharashtra Control of Organized Crime Act, 1999 contain examples of authorization of interception of wire, electronic or oral communications.
necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resources.

2. The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

3. The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to-
   (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
   (b) intercept or monitor or decrypt the information, as the case may be; or
   (c) provide information stored in computer resource.

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

Section 69 A of Information Technology (Amendment) Act, 2008 states-

1. Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub section (2) for reasons to be recoded in writing, by order direct any agency of the government or
3. The intermediary who fails to comply with the direction issued under subsection (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section 69B of Information Technology (Amendment) Act, 2008 states:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The intermediary or any person in-charge of the computer resource shall when called upon by the agency which has been authorized under subsection (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) “Computer Contaminant” shall have the meaning assigned to it in section 43

(ii) “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

(ii) “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

6. EXPERIENCE OF OUR OWN CYBER POLICE STATION

The strategy to combat cyber crimes, lies in creating a Cyber Police Force for which adequate empowerment in terms of training, infrastructure, motivation and other logistics are required. India has taken a lot of initiatives in meeting the technological challenges of cyber crime investigation. Though it may be too much to demand universal awareness on the information technology and computer forensics among our police forces, these is a realization as to the need for such an objective, and some concrete action towards this end. Bangalore, keeping with its fame in information technology, was the first Indian city to have a dedicated Cyber Police Station. Subsequently, Mumbai, Delhi and Hyderabad also have established such dedicated police stations to deal with cyber crimes. Over and above, the initiatives taken by the Central Bureau of Investigations (CBI) in coordinating with international agencies like FBI of US of America and arranging training for personal of various state police forces have been widely appreciated.