CHAPTER 27
CYBER CRIME AND POLICE

526-1. In this age of Information Technology Revolution, computers and computer networks are now within the reach of citizens, businessmen and public authorities. Computer networks and stand alone computers, which have wide applications at home, in business, in industry and commercial establishments, in public offices, are being used for data processing and storing vital information. In other words, the information technology encompasses the entire gamut of human activity. While on one hand the computer and computer networks have opened new vistas for various segments of the society and business, they are also being used as tools by criminals who use them as other devices such as firearms, explosives etc. Since the extensive use of computers has made some areas of our life increasingly dependent on them, the need to protect these areas from crime has become extremely important. The financial system, transportation systems, public records, manufacturing processes and the information infrastructure is amenable to attack by cyber criminals. The number, economic cost and sophistication of such attacks at the hands of well-educated criminals will be increasing in days to come. The international communication networks and omnipresent Internet have erased the national boundaries and the computer crime is increasing becoming international both in its scope and ramifications. This poses a new challenge for the police and other law enforcement authorities that are being called upon to ensure that users of computer and computer networks do not become victims of computer/cyber crime and also to take up investigation of this new generation of offences.

2. In dealing with criminal activity an also computer related crime, it is essential for the police to have the basic knowledge of computers. In the paragraphs that follow, the functions of the computers and computer networks have been briefly explained for the benefit of police officers.

3. A computer is a machine that carries out logical instructions in a predetermined manner. It is programmed to perform certain operations and store large amount of information depending upon its capacity. The computer networks consist of number of computers connected with each other by various means and are capable of sharing and transferring information between each other. The information or data stored in a computer can be retrieved or transferred, or used in an output form in number of ways.

4. A typical computer consists of 'input device', 'output device' 'central processing unit' and 'memory'. The input devices are used to feed the data or instructions in a computer from the user or from another computer system. The following are some of the **input devices:**

- a keyboard
- a mouse
- a magnetic tape drive
- a disk derive such as floppy disk derive, CD drive, DVD drive
- any kind of electric sensor
- a digital camera
- a microphone

- a bar coding reading machine
- scanners etc.

5. The output devices receive processed data for the user or another computer system. The following are some of the **output devices**:

   - a visual display unit also known as monitor
   - a printer which produces 'hard copies' of the output
   - magnetic tapes, cassettes, disks such as floppy disks, CDs, DVDs etc.

   However, certain hardware devices such as 'touch screens' and communication devices which connect one computer to another in a network such as modems etc. perform both input and output functions.

6. The **central processing unit (CPU)** can be described as heart of the computer. It carries out the instructions that have been pre-programmed into it either by the user or by software. In a typical personal computer, the central processing units may consist of one or more microprocessors – also called chips. It generally has a memory store which is measured in units known as Kilobytes (Kb), Megabytes (Mb), Gigabytes, (Gb) and Terabyte (Tb). It also has unit which processes the information. Central processing systems use "operating systems", which govern the way the computer operates. Some of the popular operating systems are MS DOS, Windows, UNIX, Linux etc.

7. The memory is important component to the investigator- for this

is where evidence is likely to be obtained. The memory is generally classified as temporary memory and permanent memory. Temporary memory is known as Random Access Memory (RAM) OR read/write memory, which can be altered or erased. The information contained in RAM is not saved or transferred to other storage media and it is lost the moment power source in disconnected. The permanent memory, known as Read Only Memory (ROM) cannot be altered or erased.

Computer Hardware

8. The mechanical devices that constitute the computer are called hardware. The hardware can be seen and felt. The hardware consists of various inter-connected electronic devices such as processors, video screens, printers and several other peripherals such as disk drives, CD writers etc.

Computer Software

9. The hardware by itself cannot do any data processing. It requires electronic instructions that drive a computer or any other hardware component to perform specific tasks. Any computer software, information / data are organised in a structure of files, software in programme files and information in data files. Though there are number of software programme, these can be broadly categorized into 'system software' and 'application software'

10. As mentioned above, one major type of system software, known as the operating system tells the computer, how to use its on

components. The application software, instructs the computer, how to accomplish specific tasks such as word processing, data analysis, computer games etc.

11. Information / data may be loaded onto a computer by using any of the input devices mentioned above. The data may normally be referred by names like records or files.

12. The descriptions of various types of computers is given in the following paragraphs:

A. **Super Computers:** Super Computers are generally the largest and most powerful computers made to process huge amount of data and carry out large number of calculations per second. The scientists and engineers generally use the Super Computers. Due to their size and cost, Super Computers are very rare and only used by large corporations, universities and government agencies.

B. **Main Frame Computers:** The largest of a computer, which is commonly used for processing huge volume of data are called Main Frame Computers. These are normally used in large organizations like insurance companies, banks and airlines, where same data need to be accessed by several people. Main Frame Computers are also used for providing services on the internet. Retrieving evidence from a Main Frame Computer may require a high degree of expertise.

C. **Mini Computers:** Mini Computer systems are smaller computers but have large capacity for processing the data. These are normally used as servers and provide network to

number of users and are capable of data sharing with the linked computer systems.

D. **Work Stations:** Work Stations are normally used for specialized purpose by single user. These normally have processing power of a mini computer and are used by scientists, engineers, graphic artists, programmers etc.

E. **Microcomputers / Personal Computers:** These are generally used by individuals for various applications. These days, with advanced technology, processing power of microcomputers often drives that of workstations or mini computers. These computers may also be used with network interface card to connect to the network of an organization or to the Internet.

F. **Note Book / Laptop computers:** Note Book / Laptop computers, as the name suggests, are smaller portable versions of micro computers and can perform any function of a micro computer. These computers can be carried anywhere and can be connected to the network through physical or wireless interface.

G. **Hand held computers:** The past few years have seen introduction of many hand held personal computers, which are also called on Palmtop Computers or Personal Digital Assistants (PDAs). These are small portable computers less powerful than microcomputers providing services on the internet.

13. **Network Computing:** A network of computers can be defined as several computers connected with each other through cables or wireless, so as to capable of sharing various kinds of

information / data. Generally, two main types of networks i.e. Local Area Network (LAN) and Wind Area Network (WAN) are in use these days.

A. **A Local Area Network (LAN)** can be defined as a network of computers located in vicinity. These are normally connected by cable, an lntra red link or through a radio transmitter. The data is normally shared by these computers through certain software protocols, which are a set of rules and forms for sending and receiving data. TCP / IB is one of the most popular protocol, which is in use these days for exchange of data.

B. **Wide Area Network (WAN)** can be defined as network of two or more LANs connected together covering a wide geographical area. A WAN may link computers situated in one country or across various countries. The computers in WAN may be connected through high speed telephone lines, fibre optics, under sea cables or through satellites.

14. **Storage Devices:** The data / information is often stored on what is known as storage media. The hardware component, on which, data can be written and read from it, is also known as storage device. There are two main categories of storage technology, which exist today i.e. magnetic storage and optical storage. Certain storage devices / media may employ both kind of technology. For detailed description, any standard book on storage devices may be referred to.

A. The primary type of magnetic storage devices are as follows:

- Diskette
- Hard Disk (could be fixed or removable)
- High capacity floppy disks
- Disk cartridges
- Magnetic tape
- Cards (credit and debit cards etc.)

B. The various types of Optical Storage devices are as follows:

- Compact Disk Read-Only Memory (CD-ROM)
- Digital Video Disk Read-Only Memory (DVD-ROM)
- CD-Re-cordable (CD-R)
- CD-Re-Writable (CD-RW)
- Photo CD

Computer Crime

527-1. Given the dynamic nature of information technology, communication infrastructure and ever changing legal measures towards better effort to prevent computer / cyber offences the paragraphs that follow are not a comprehensive description of computer crime.

2. There is no universal accepted definition of computer / cyber crime but broadly in general parlance, the computer crime is any illegal or unauthorized activity involving computers. The crime can be against an individual or organization or against the nation endangering or threatening to endanger its integrity and security. Such an illegal or unauthorized act may manifest in, preventing the computer to perform its duties as designed, or slow down its operations, or corrupting or copying

the data or software. A computer crime can thus broadly define as commission, or attempt or abetment to the commission of any one or any combination of the following illegal/unauthorized activities.

A. unauthorized access , alteration, addition, deletion or hiding data;
B. unauthorized access, alteration, addition, deletion or hiding programme or information;
C. stealing of data, programme in any manner;
D. unauthorized (physical/logical) entry into computer work environment;
E. change or alter the defined system.
F. Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
G. Disrupting or causing disruption of any computer, computer system or computer network;
H. Denial or causing denial of access to an authorized person, to any computer, system or computer network by any means;
I. Providing assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of Information Technology Act, 2000 or the rules or regulations made there-under;
J. Charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network;
K. Destroying or deleting or altering any information contained in a computer resource, or diminishing its value or utility, or affecting it injuriously by any means;
L. Stealing, concealing, destroying, altering or causing any person

to steal, conceal, destroy or alter any computer source code used for a computer resource with the intention of causing damage.

Modus Operandi of the Computer Crime

3. Digital or electronic tress passing requires very few tools such as home computer, or a note book computer or a desk top personal computer, a modem and a telephone line. The criminal first identifies and breaks into the communication channel to which the computer is connected. This may be a dial up line connected to telephone line or a leased line connected to a telephone line or to the public data system network. He then tries to log into the system by trying out various passwords or stolen password. For an insider to gain unauthorized access to the system becomes all the easier. In the case of stand-alone systems, his job becomes easy once he gets physical access to the system.

3. **Tools and Techniques used to Commit Cyber Crimes**

Cyber Crimes make use of various tools and techniques and many of these tools are used for the commission of the cyber crimes and are installed on the victim's systems which may include physical access or by making use of the intermediary systems or be deceiving the victim to allow access to his system or by gathering the victim information.

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

overwriting the valid data held in them.

.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Other type of Computer Crimes

2. Software Piracy and other Copyright Violations, Cyber Pornography, Cyber Terrorism and introducing deliberately the virus etc. are the other type of Computer Crimes. This list will keep on growing with the growth of the computers and the Information Technology. Virus is the latest and the most destructive type of identified computer crime. It has the capacity of instantaneously multiplying and attaching themselves to programme under certain circumstances. They can damage computer systems, programs and data. A programmer writes a virus which is nothing more than a few lines of numbers or letters that instruct the computer to change or destroy information inside another computer. The virus instructions are hidden inside a legitimate program – one that might contain a spreadsheet or a word processing programme. It can in fact be through a disc or even through phone lines. The computer reads the virus along with the real software program. The computer reacts to the hidden virus instruction. It might tell the computer to destroy information on a certain date or simply flash a harmless message on screen. It might also tell computer to put a copy of the infected software on every other disc inserted into the machine. A virus can spread from computer to computer system over a telephone line and electronic bulletin boards and floppies / discs. It can damage the computer memory and knock out the total system.

Crimes targeting Computer systems

a. Hacking

3. Hacking is a broader term and can be defined as gaining entry into a computer system without the permission, with an intention to cause loss, steal, or destroy the data contained in it. It is often done by people who are well versed with computer technologies by exploiting some of the vulnerabilities that are present in the computer system. This involves various methods of acquiring

sensitive information like usernames, passwords, Internet Protocol (IP) addresses and using them to access the computer system.

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

5. **Hacking** is defined under section 66 of I.T Act, 2000 as destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means, with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person. In cracking, normally the perpetrator makes minor changes in the programme, in violation of the copyright restrictions with the objective of extracting information, illegally.

6.

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

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

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

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

11. **c. Spreading viruses and malware**

12. Spreading viruses and malware is the biggest crime that is happening today and most of the Internet users are affected by it. These can be generic or targeted to a specific computer system. Injecting and spreading malicious code also can come in the form of viruses, worms, Trojans, spyware, adware, and rootkits. These get installed secretly in the victim's computer system and

can be used to access and transmit sensitive information about the system, and in some instances, the infected systems can be used as tools to commit other types of cyber crime.

13. **Website defacement**

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

Investigation of Computer Crime

6. In the following paras, brief instructions are given, which will be useful to the investigators. But these, by no means are exhaustive in nature especially as the technology and the nature of the computer crime keeps on changing and therefore the investigators are advised to refer to computer/cyber crime manual prepared and updated by Crime Investigating Department (CID) from time to time.

7. Unlike collection of evidence in normal crime, the collection of computer evidence on any scene of crime required specialist care. Serious problems could arise if the computer evidence is not collected properly and with necessary specialist care. Therefore, the investigators are advised that they may call for specialist NIC, specialist of computer crime unit of Crime Investigating Department or computer forensic scientist from the Forensic Science Laboratory.

8. Whenever the investigators comes across a computer during investigation of any crime, he should remember that it could be a valuable piece of equipment and could contain quantity of

data, which could lead to valuable evidence for the crime being investigated. Therefore, preservation of the same becomes important from the point of view of evidence. Any mistake in preserving the evidence could result in loss of valuable evidence. On the other hand, any mishandling could also result in huge economic loss to the owner of such computer, which must be avoided at every cost. The investigator must remember that computers could frequently be connected in a network and the vital necessary evidence might have been transmitted or stored at a location different from the site of the search. The information could be stored even across the boundaries of the country. The investigating officer must therefore be extremely careful whenever he comes across a network of computers. It may also be necessary to involve a computer expert at the earliest as investigator may not be equipped to collect various kinds of data storage on magnetic or optical media.

Pre-Investigation Assessment

4.1. Doing the Basics Right

It is very important for every Investigating Officer (IO) to do a pre-investigation assessment for each cyber crime/incident that is reported. It should be generally remembered that, before the complainant approaches the police officer or any agency for addressing their problems, they may have made attempts to set the things right all by themselves or with the help of their friends or some other persons. However these very acts may result in destruction of crucial digital evidence(s). Similarly, sometimes the criminal act may be a crime in progress, which can potentially cause further damage. All these factors will have an impact on the outcomes of the investigations.

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

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

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

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

The ITAA 2008, contains explicit penal provisions for certain offences (66 A to F). However, Section 66 stands on a different footing, in relation to other penal provisions. Section 66 of the IT Act makes it amply clear that only when a person, dishonestly, or fraudulently, does any act(s) referred to in Section 43 of the IT Act, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees, or with both.

Thus, for an act to be investigated under Section 66 of the ITAA 2008 as a Cyber Crime, it needs to satisfy two conditions.

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

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

Thus, to an IO, if the complaint reveals acts as defined under Section 43 of ITAA2008 only but does not reveal commission of these acts with dishonest and fraudulent intentions, then it cannot be investigated as a Crime under IT Act. Under these circumstances, these reports of the acts under section 43 need to be resolved before the adjudicating officers, who were notified under Section 46 of the ITAA2008..

It is suggested to consult Cyber crime cell team or any other expert in this field before issuing and FIR to determine the right section of law, especially under ITAA2008.

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

- elicit the information regarding the act under report in details and, ensure that the details of the offences are captured in the complaint, in full.
- Indicate the nature/modus operandi of the cyber crime in detail (include the e-mail address, systems, time zones etc).
- Indicate all the details that can be identified from the complaint like,

IP address in case of e-mail and Internet.

Profile name or user name in case of social networking abuse.

Bank details/Internet banking branch, etc., in case of online fraud.

Credit card details and nature of purchase, etc., in case of card fraud, etc.

- include the time and date in the exact format the complainant mentioned or noted in any of the documentation attached with the complaint (such as e-mails) and, Time zone conversion will have to be taken care during the course of investigation.

4.3 Preliminary Review of the Scene of the Offence

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

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

At the scence of offence (irrespective of the type of the scene of offence), the IO should carefully survey the scene, observe and assess the situation and decide on the steps for proceeding further. The pre-investigation assessment will help the IO to understand the local situation, circumstances and technical details of the systems/network at the scene of the crime before proceeding to seize/preservation of evidences. As mentioned earlier, the digital evidence is highly fragile and volatile. It will be available in a number of devices, locations and in various formats. For example, the copiers, fax machines, routers, hubs etc., apart from the standard storage/compute devices can also contain vital information relevant to the case /incident. Hence, it is utmost important for the IO to do a preliminary review of the entire scene of offence and also take some additional steps before identifying the evidence and conduct search and seizure. It is very important to include

such observations/preliminary review notes in the questionnaire that needs to be sent to FSL for expert opinion.

4.3.1. Evaluating the Scene of Offence

- After identifying the scene of offence, IO should secure it and, take note of every individual physically present at the scene of offence and, their role at the time of securing the scene of offence.
- From the information gathered and based on visual inspection of the scene of offence, IO should identify all the potential evidences. These physical evidences may include conventional physical evidences like the manuals, user guides and, other items left behind like passwords on slips, bank account numbers etc. it is also important to note the position of the various equipment and items at the scene of offence. For example, a mouse on the left hand side of the desktop possibly indicates the person operating the computer is a left-handed user.
- While identifying the digital evidence, IO should make sure that, the potentially perishable evidence is identified and, all the precautions are put in place for its preservation. At the time of review, disturbing or altering the condition of electronic evidences should be avoided.
- If the systems are OFF, they should not be turned ON for the inspection. If systems are on, it is advised to leave them ON.
- If systems are ON at the scene of offence, IO should take appropriate steps to photograph it, plan for the seizure of the evidences at the earliest and document it. IO should notify appropriate technical personnel to support during the seizure process, so that the perishable evidences (volatile data) are appropriately recovered without loss.
- IO should make note of the attached network cables and power lines to the systems. With the help of the complainant or the technical personnel at the agency, make a note of all the network connections, modems, telephone lines and, mark them both the equipment connection end and, from the source in the walls.

4.3.2 Preliminary Interviews at the Scene of Offence

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

- What steps were taken to contain the issue? (Physical access denied for suspected persons, disconnecting the suspected computers from network, suspending the employee access and so on) along with list of all suspected names, address, etc.
- Where there any logs (system access, etc.) present that cover the issue? Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?
- Did you observe any similar instance before?

- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give a detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred. (Request a letter of confirmation from complaint)
- Do they have similar systems in any of the branch/other officers?
- Whether log register of the Internet users/other users is maintained? (it is very crucial to fix the responsibility. In case of cyber café, it is a must to maintain log register of users for specific period as per the rules framed by state government.
- Are there any questions about the issue that have not been answered? (Affected system list, number of people involved, etc.)
- What are the further plans for analysis of the issue?

At the scene of offence, IO should

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

4.4. Pre-Investigation Technical Assessment

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

Scene of Offence: Cyber Café

- Identify number of computer systems present in the cyber café.
- Identify number of computer systems connected to Internet.
- Obtain details about the network topology and architecture (client-Server)

- Obtain the CCTV/Web camera clipping, if any.
- Whether any user management software is used by the cyber café owner?
- Obtain the log register of Internet users for the relevant period.
- Check the formatting of storage devices policy adopted by the cyber café owner.
- Check the hardware replacements done by the cyber café owner.
- Check the policy regarding removal media usage on the cyber café systems.

Scene of Offence: Home

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

Scene of Offence: Corporate Environment

- **Questionnaire for crime in which computers are used as instrument/means OR repository:** This questionnaire helps the investigating officer to gather the basic information where crime is committed using the computer systems.
- **Questionnaire for crime targeting computer system:** This questionnaire helps the investigation office to gather the relevant information where crime committed is targeted to destroy or affect the services, etc., of a computer system/server using the Internet or any other network. The above format(s) for pre-investigation assessment will help the IO(s) to understand the incident in totality. At the end of the pre-investigation assessment the IO will be able to decide on the issuance of preservation notices for the designated/authorized persons (in case of a company or large establishment with number of systems) or individuals who are owners of the systems and victims. Similarly it will allow the IO to decide on the kind of technical support to be requisitioned, to proceed with the acquisition of evidences. Above all, the Investigating officer decides how to proceed with investigations.

4.5. Issuance of preservation notice

- Based on the information gathered, the IO should come out with issues to be complied immediately by issuing specific do's and don'ts to the complainant/company/agency-e.g. stopping the access, taking backups, or preserving log information, etc. till further orders. For example, continuing access

to the e-mail by the accused can enable him to delete the mails which are incriminating in nature.

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

4.6. Containment of the incident/Offence

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

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

- In case of financial frauds, the IO should immediately contact the concerned branches of the banks to freeze the beneficiary/suspect/accused person’s bank accounts in case of fraudulent money transfers.
- The IO should request the Service Providers to block/remove and at the same time preserve the access details the fake/defamatory profiles in social networking/community Web sites. The IO should also notify the Service Providers to preserve the access details of the defamatory/obscene contents.

- If the targeted system is to be restored by the affected party immediately for commercial reasons or in public interest, the IO should obtain the services of technical personnel from the Cyber Forensics divisions and, obtain the image copy of the affected system and permit restoration of the system, only after that. These actions need to be documented with enough justification and should be used under rarest of the rare circumstances. Normally, the restoration is done after the seizure of the evidences and not at the immediate stage of the reporting of the crime.

Avoiding alteration of evidence

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

Preparation for collecting evidence at the scene of crime and search

9. The following precautions are advised to an investigator, if he comes across to a computer or computer network suspected to be involved in computer crime.

A. If the investigator has prior knowledge that the scene of crime which is going to be searched would have computer systems or computer network in place, it is advisable to contact the specialist computer crime unit of Crime Investigation Department or computer forensic scientist of Forensic Science Laboratory. In case it is possible, advanced information may be collected regarding the make, model, operating system, network connections etc. being used by the organization or individual, whose premises is being searched, as this information could prove valuable. The information so collected

must be passed on to the expert, who can make necessary preparation that may be required to collect evidence. This is necessary, as many a times, it may not be possible to remove the computer systems physically and the data or programme may have to be copied as per provision of Indian Evidence Act on the crime scene itself. The investigator or the expert, who may accompany the police personnel going for search should carry necessary media in the form of disk, floppy disks, optical disks, tapes, tools, software, labels and other specialized items and should carry necessary packing material, which can prevent loss of evidence collected as offered on such media as data on magnetic media can be destroyed by media, dust and electrostatic environment.

B. In case computer equipment is to be removed, necessary care would have to be taken to pack it properly and if necessary the material which will prevent any damage, as sometimes read-write heads could malfunction if subjected to sudden jerk or force, should be arrange for packing. If the computer system at crime scene happens to be large, special attention may be required for proper transport and storage arrangements, so that, data contained therein is preserved for the purpose of evidence. If necessary and possible, the place which contains such computers could be sealed and guarded properly till arrangement is made to collect the evidence.

C. During the course of the search, the investigator must not, under any circumstances, allow a suspect or accused to touch any part of the computer system. It must be remembered that even a press of a key could erase the entire data. These days, it is even possible to enter or delete data with the help of

remote keyboards and mouse. Hence care should be taken that suspect or accused does not have possibility of passing any instructions to the computer through any of such devices. Sometimes, it may be desirable / necessary for suspect or accused to be present during the search to collect valuable information especially if data is protected by user identities or passwords. In such situations, the investigator must be careful to keep the suspect / accused out of reach of computer system and must not try to recover data by using the identities or passwords told by such person. He should invariably take help of an expert under such circumstances.

D. Now-a-days, most of the computers are part of the network, which may be connected through cables, radio links, telephone, fibre optics etc. In a network, individual computer systems may function as stand alone machines also and may contain significant data / programmes. On the other hand, the information could be found elsewhere – in a physically remote area – as server connected in the network. Therefore, it is important that help of an expert is taken to identify where the storage is located. The type of storage arrangement in use in a network would determine the search and seizure procedures. It is, therefore, necessary that when a network environment is to be searched, adequate technical personnel along with general investigator must be assigned for the job. In case, it is found that the server or data storage is located outside the boundaries of India, prompt necessary action has to be taken through a competent court to issue a "*letters rogatory*" under the provisions of section 166(A) CrPC. The assistance of National Crime Bureau (N.C.B.) represented by Central Bureau of Investigation, may be taken in this regard.

E. It may therefore be necessary to ensure that the suspect / accused is not able to temper with the information contained in the computers at the time of the search. The investigator is well advised to take help of an expert to ensure that all such connections are removed and data communication facilities disabled at the earliest.

Procedure to be adopted during search and seizure of evidence contained in computer systems

10. The actual collection / seizure of evidence should take place after all steps mentioned in previous paragraphs have been taken. As mentioned above, it may be necessary to associate an expert or a forensic specialist before carrying out the search and seizure procedure. However, in the following paragraphs, few of precautions and steps taken during the search have been detailed.

11. The system should be observed carefully and the name and the model number of the system should be noted. It is necessary to prevent loss or corruption of evidence and to ensure preservation of quality of evidence.

12. Under no circumstances, crime suspect / accused should be allowed to touch a computer system or use remote control devices, which can manipulate the data / programmes contained in the computer systems.

13. The suspect / accused or anybody else must not be allowed to remove anything from the scene or carry out any activities on

the computers. It must be remembered the computers, video screens, printers and other peripheral devices may also contain valuable evidence, which could be destroyed, if anybody is permitted to handle these equipments. In case, no technical / expert assistance is available, and the investigator is not trained to handle such computer systems, it may be advisable to leave computers on the scene as it is, till technical assistance arrives.

14. In case, computer systems are found working, it may be necessary to power down these with the help of experts depending upon the operating system in use. Care should be taken to use the shut down system of the operating system and not shut off power as that could result in loss of data / programme, which may make recovery of evidence extremely difficult and even impossible.

15. Before disconnecting and dismantling any computer component, everything must be labeled, initiated with date along with the signatures of witnesses as per provisions of law. Special care should be taken to label and document all the cables. The corresponding labels must be placed on the devices, which are connected with particular cables and if necessary a descriptive labeling system i.e. LPT1, Serial Port etc. may be used.

16. It may be extremely useful and necessary to take close up photography – both still and video – of all the individual pieces of hardware and connections. The investigator may also draw a diagram of the location of the various computer systems.

17. The equipment available at the scene, must not be dismantled by the investigator and the job shall be best left to a specialist, who may disable a network/remove the peripherals first and then the computer system.

18. Any documentation or notes or scratch paper etc. found at the scene must be scrutinized properly and seized. Many a times, these could give important clues regarding passwords and other information.

19. In case, the scene of crime contains multiple computer systems, care must be taken to keep one system separate from the other and the peripherals attached to such system must be marked and packed separately, so that they do not get mixed-up.

20. The investigator is cautioned that when no expert is available, he should not try to handle the system as due to any improper handling, there is a risk of tempering the evidence available therein. Switching or disconnection of power may result in loss of temporary memory (RAM), which will create difficulties in re-gaining access to the system and collection of evidence by the expert. Even if the investigator is conversant with computer, keying in instructions could overwrite data and can be construed as interfering with the evidence. Therefore, care should be taken to have expert assistance available also for preserving the evidence.

21. The investigator should remember that sometimes the computer may appear not to be working but actually it could be in hibernation / sleep mode and it might not have been turned off. Some computer especially laptops work with the help of

batteries and therefore care should be taken for handling such systems for collecting the evidence.

Analysis of computer evidence

22. The evidence collected from scene of a crime from computer system/s must be sent to forensic laboratory for examination by computer forensic experts or any other designated expert as per the provisions of Indian Evidence Act. The Forensic laboratory may make a copy of the data seized for the purpose of analysis and should not work on the original as the data on the media seized is required to be produced in the court as evidence, and it may get destroyed or altered if the process of analysis is done on the original stored data.

23. The investigator must ensure that all equipment – tapes, disks, peripherals etc. must be stored in a dust free environment under regulated temperature. The investigator is well advised to consult an expert for properly storing the equipment and other seized material.

24. The investigation into computer crimes should be done by police officers who have the necessary experience and training in the field. A training programme for investigating officers in this form of crime should be organized in the Police Headquarter by the CID.

Computer Crime and legal penal provisions

526. The various type of computer crimes as mention in Order may fall within the ambit of existing provisions of Indian Penal Code or **Chapter-XI** of **Information Technology Act, 2000**. These offences and their nature are not being discussed here and the investigators may consult some of the books

published on the subject and manual on Computer Crime published by International Criminal Police Organizations (Interpol).

A comprehensive list of various crimes and different sections of laws for easy reference are given below:

Sl.No	Nature of Complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
1	Mobile phone lost/stolen		Section 379 IPC upto 3 years imprisonment or fine or both
2	Receiving stolen computer/mobile phone/(data or computer or mobile phone owned by you is found in the hands of someone else.)	Section 66 of ITAA 2008 – upto 3 years imprisonment or fine up to rupees one lakh or both	Section 411 IPC - upto 3 years imprisonment or fine or both
3	Data owned by you or your company in any form is stolen	Section 66 of ITAA 2008 – upto 3 years imprisonment or fine up to rupees five lakh or both	Section 379 IPC - upto 3 years imprisonment or fine or both
4	A password is stolen and used by someone else for fraudulent purpose	Section 66C of ITAA 2008 – upto 3 years imprisonment and fine upto rupees one lakh. Section 66D ITAA 2008 – upto 3 years imprisonment and fine up to rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine. Section 420 IPC - upto 7 years imprisonment and fine

5	An e-mail is read by someone else by fraudulently making use of password	Section 66 of ITAA 2008 – upto 3 years imprisonment or fine upto rupees five lakh or both. Section 66C of ITAA 2008 – upto 3 years imprisonment and fine upto rupees one lakh	
6	A biometric thumb impression is misused	Section 66 of ITAA 2008 – upto 3 years imprisonment and fine upto rupees one lakh	
7	An electronic signature or digital signature is misused	Section 66C of ITAA 2008 – upto 3 years imprisonment and fine upto rupees one lakh	
8	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66D of ITAA 2008 – upto 3 years imprisonment and fine upto rupees one lakh	Section 419 – upto 3 years imprisonment or fine or both
Sl.No	**Nature of Complaint**	**Applicable section(s) and punishments under ITAA 2008**	**Applicable section(s) under other laws and punishment**

9	Capturing, publishing, or transmitting the image of the private are without any persons consent or knowledge	Section 66E of ITAA 2008 – upto 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC – upto 2 years imprisonment and fine rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
10	Tampering with computer source Documents	Section 65 of ITAA 2008 – upto 3 years imprisonment or fine not exceeding Rupees two lakh or both. Section 66 of ITAA 2008 – upto 3 years imprisonment or fine upto rupees five lakh or both	
11	Data Modification	Section 66 of ITAA 2008 – upto 3 years imprisonment or fine upto rupees five lakh or both	
12	Sending offensive messages through communication service, etc.	Section 66A of ITAA 2008 – upto 3 years imprisonment and fine	Section 500 IPC - upto 2 years or fine or both. Section 504 IPC - upto 2 years or fine or both. Section 506 IPC - upto 2 years or fine or both- if threat be to cause death or grievous hurt, etc-upto 7 years or fine or both.

			Section 507 IPC - upto 2 years along with punishment under section 506 IPC with punishment under section 506 IPC. Section 508 IPC - upto 1 year of fine or both. Section 509 IPC- upto 1 years or fine or both of IPC as applicable
13	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA2008 first conviction upto 3 years and 5 lakh Second or subsequent conviction- upto 5 years and upto 10 lakh	Section 292 IPC- upto 2 years imprisonment and fine rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction.
14	Publishing or transmitting of material containing sexually explicit act, etc, in electronic form	Section 67A of ITAA 2008 first conviction- upto 5 years and upto 10 lakh Second or subsequent conviction- upto 7 years and upto 10 lakh	Section 292 IPC- upto 2 years imprisonment and fine rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction.
15	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in	Section 67B of ITAA 2008 first conviction- upto 5 years and upto 10 lakh Second or subsequent conviction - upto 7 years and upto	Section 292 IP – upto 2 years imprisonment and fine rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction

	electronic form	10 lakh	
16	Misusing a Wi-Fi connection if done, against the state	Section 66 of ITAA 2008- upto 3 years imprisonment or fine upto rupees 5 lakh or both. Section 66F- life imprisonment	
Sl.No	**Nature of Complaint**	**Applicable section(s) and punishments under ITAA 2008**	**Applicable section(s) under other laws and punishment**
17	Planting a computer virus if done, against the state	Section 66- 3 years imprisonment or fine upto rupees 5 lakh or both 66F- life imprisonment	
18	Conducting a denial of service attack against a government computer	Section 66 of ITAA 2008- upto 3 years imprisonment or fine upto rupees 5 lakh or both Section 66F- of ITAA 2008- life imprisonment	
19	Stealing data from a government computer that has significance from national security perspective	Section 66 of ITAA 2008 – upto 3 years imprisonment or fine upto rupees 5 lakh or both,	

		66F- life imprisonment	
20	Not allowing the authorities to decrypt all communication that passes through computer or network	Section 69 of ITAA 2008- imprisonment upto 7 years and fine	
21	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69 of ITAA 2008- imprisonment upto 7 years and fine	
22	Failure to Block Web sites, when ordered	Section 69A of ITAA 2008- imprisonment upto 7 years and fine	
23	Sending threatening messages by d-mail	Section 66A of ITAA 2008- upto 3 years imprisonment and fine	Section504- upto 2 years or fine or both
24	Word, gesture or act intended to insult the modesty of a woman		Section509 IPC- upto 1 year or fine or both – IPC as applicable
25	Sending defamatory messages by e-mail	Section 66A of ITAA 2008- upto 3 years imprisonment and fine	Section500 IPC- upto 2 years or fine or both
26	Bogus Web sites, cyber frauds	Section 66D of ITAA 2008- upto 3 years	Section 419- upto 2 years or fine or both Section 420 IPC- upto 7 years

		imprisonment and fine upto rupees 1 lakh	imprisonment and fine
28	Making a false document	Section 66D of IIT 2008- upto 3 years imprisonment and fine upto rupees 1 lakh	Section 465- upto 2 years or fine or both
Sl.No	**Nature of Complaint**	**Applicable section(s) and punishments under ITAA 2008**	**Applicable section(s) under other laws and punishment**
29	Forgery for purpose of cheating	Section 66D of ITAA 2008- upto 3 years imprisonment and fine upto rupees 1 lakh	Section 468 IPC- upto 7 years imprisonment and fine
30	Forgery for purpose of harming reputation	Section 66D of ITAA 2008- upto 3 years imprisonment and fine upto rupees one lakh	Section 469 IPC- upto 3 years and fine
31	E-mail Abuse	Section 66A of ITAA-2008 upto 3 years imprisonment and fine	Section 500 IPC- upto 2 years or fine or both
32	Punishment for criminal intimidation	Section 66A of ITAA-2008 - upto 3 years imprisonment and fine	Section 506 IPC- upto 2 years or fine or both- if threat be to cause death or grievous hurt ,etc- upto 7 years fine or both
33	Criminal intimidation by an anonymous communication	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Section 507 IPC- upto 2 years along with punishment under Section 506 IPC

34	Copyright infringement	Section 66 of ITAA 2008- upto 3 years imprisonment or fine upto rupees 5 lakh or both	Section 63, 63B Copyrights Act 1957
35	Theft or Computer Hardware		Section 379 IPC- upto 3 years imprisonment or both
36	Online Sale of Drugs		NDPS Act
37	Online Sale of Arms		Arms Act

Sikkim Information Technology Rules, 2009

1. Under Section 90 of Information Technology Act, 2000 State Government has framed Sikkim Information Technology Rules, 2009 to regulate the licenses and functioning of Cyber Cafés in the State.

2. Cyber Cafes shall be a place of public amusement and public entertainment under clause (i) of sub-section (1) of section 2 of the Sikkim Police Act, 2008.

3. Under Rule 4 of Sikkim Information Technology Rule, 2009 a person or Firm, before applying for a trade license for Cyber Café shall have to obtain a No Objection Certificate from Crime Branch.

4. Rule 5 of Sikkim Information Technology Rules, 2009 stipulates various responsibilities of Cyber Café owners. Broadly these are as follows:

(i) All the computers in the Café shall be serially numbered and the number shall be displayed on the computer/cubicle;

(ii) Each computer shall have a log register which shall be preserved in the café for a minimum period for three years from the date of last enter in the register;

(iii) A customer shall not be allowed access to internet unless he establishes his identity by producing an authentic photo identity card; and the cyber café shall keep a photocopy of such identity document. This shall be preserved for a period of three years from the date of browsing by the customer. In the case of regular customers they need not produce the identity card or photocopy thereof so long as the photocopy once produced is on the record of the café. In case a customer does not have a photo identity card, the cyber café shall keep on the hard disk of a computer, a web-camera photograph of the customer;

(iv) Children browsers not possessing photo identity card will have to be accompanied by an adult guardian whose photo identity card copy or web-photograph shall be kept on record as described above;

(v) All the clocks in the cyber café shall show Indian Standard Time;

(vi) The cyber café owner shall take all precautions to ensure that the computers are not used for illegal or criminal activities.

(vii) All the computers have safety software to block access to web sites relating to obscenity, terrorism, organized crimes, anti-national and other illegal or objectionable material;

(viii) The cyber café shall prominently display various documents namely copies of trade license; No Objection Certificate from the Crime Branch and clearance certificate from Internet Service Provider; number of computers, internet protocol address and total bandwidth, information about various services provided

through internet (video conferencing, internet protocol telephony, etc.) and information about the identity or the hardware or storage media of each computer.

(ix) The cyber cafes are required to store back-ups of logs and internet records (internet cookies, modem logs, proxy and other logs created by network software) of all computers for a minimum period of 180 days.

(x) At least two computers in a cyber café shall be kept in the open place in such a way that their screen shall face the common place. Cubicles, if provided, shall not have partition more than 60 centimeters above the top edge of the monitor. Children browsers below the age of 18 years shall not be allowed to use cubicles.

Powers of the Police under Sikkim Information Technology Rules, 2009

1. Rule 6 empowers the Superintendent of Police in charge of the Cyber Cell, or an officer not below the rank of Inspector of Police duly authorized by him to enter any cyber café with the assistance of such technical officials as may be deemed necessary and download any software to any computer kept in the cyber café for the purpose of blocking, monitoring or retrieving any content or material of web sites in consonance with the provisions of the said rules.

2. Rule 7 empowers the Superintendent of Police in charge of the Cyber Cell or an officer not below the rank of Inspector of Police duly authorized by him to inspect at any time any cyber café its documents, computers or network established there and the owners of the café shall on demand produce before such officer all the related documents information, computers or network system for inspection.

3. Rule 11 provides for establishment of an advisory committee consisting of an officer each from the

Information Technology department, Govt. of Sikkim, the National Informatics Centre, Gangtok and the Bharat Sanchar Nigam Limited, Gangtok for rendering technical advice and assistance to the Cyber Cell, Crime Branch and the Adjudicator appointed under the said Rules.