**CHAPTER 18**

# CYBER CRIMES

**18.1** With increased use of computers in homes and offices, there has been a proliferation of computer-related crimes. These crimes include:

(i) Crimes committed by using computers as a means, including conventional crimes.

(ii) Crimes in which computers are targets.

**18.2** The investigation of such crimes is complex. The evidence is often in an intangible form. Its collection, appreciation, analysis and preservation present unique challenges to the Investigator. The increased use of networks and the growth of the Internet have added to this complexity. Using the Internet, it is possible for a person sitting in India to steal a computer resource in Brazil using a computer situated in USA as a launch pad for his attack. Distributed attacks are also not unheard of. The challenges in such cases are not only technological, but also jurisdictional.

**18.3** The Internet is the single, richest and most frequently updated information resource on Computer Crimes. With highly systematic and structured searching techniques available, it is easy to go to the specifics one has in mind. CBI Officers are advised to use the Internet as a resources for any new technological challenges.

**18.4** To combat computer-related crimes, the CBI has the following specialized structure:–

(i) Cyber Crimes Research and Development Unit (CCRDU);

(ii) Cyber Crime Investigation Cell (CCIC);

(iii) Cyber Forensics Laboratory; and

(iv) Network Monitoring Centre.

**18.5** The CCRDU is charged with the responsibility of keeping track of the developments in this ever-growing area.

**18.6** The CCRDU is primarily involved in the following tasks:–

(a) Liaison with the State Police Forces and collection of information on cases of Cyber Crime reported to them for investigation and to find out about the follow-up action in each case;

(b) Liaison with software experts to identity areas, which require attention of State Police Forces for prevention and detection of such crimes with a view to train them for the task;

(c) Collection of information on the latest cases reported in other countries and the innovations employed by Police Forces in those countries to handle such cases;

(d) Preparation of a monthly Cyber Crime Digest for the benefit of State Police Forces; and

(e) Maintenance of close rapport with the Ministry of IT, Government of India and other organizations/Institutions and Interpol Headquarters,. Lyon for achieving its objective of giving the needed thrust to collection and dissemination of information on Cyber Crimes.

**18.7** The CCIC, established in September 1999, started functioning from March 2000. It is a part of the Economic Offences Division. The Cell has all-India jurisdiction and investigates criminal offences under the Information Technology Act, 2000, besides frauds committed with the help of

computers, credit card etc. It is also a round-the-clock Nodal Point of contact for Interpol to report Cyber Crimes in India, and also a member of "Cyber Crime Technology Information Network System" of Japan.

**18.8** The Cyber Forensics Laboratory (CFL), established in November 2003, functions under the Director, Central Forensic Science Laboratory.

The responsibilities of CFL are:

(i) Provide media analysis in support of criminal investigations by CBI and other Law Enforcement Agencies.

(ii) Provide on-site assistance for computer search and seizure upon request.

(iii) Provide consultation on investigations or activities in which media analysis is probable or occurring.

(iv) Provide expert testimony.

(v) Research and Development in Cyber Forensics.

**18.9** The following principles are followed by the CFL: ─

(i) The purpose of the analysis shall be to use the evidence in the Court.

(ii) All legal formalities shall be followed.

(iii) The media should have been legally seized and chain of custody maintained.

(iv) The analysis shall be on an image of the media and not on the media itself.

(v) The laboratory shall have the best imaging tools and software tools for analysis.

**18.10** The purpose of the Network Monitoring Centre is to police the Internet. It has a Network Monitoring Tool (NMT) developed by I.I.T., Kanpur and may use similar and other tools to achieve its purpose after following the required procedure.

**Search and Seizure of Digital Evidence**

**18.11** In the conventional environment, items are stored in a tangible form that can be stored physically like information written on paper, bills, receipts, address, book, etc which are susceptible to damage by physical methods such as theft, burglary, etc., but in the information age of electronic environment, data is stored in an intangible form making it a virtual world where these limitations of conventional methods no longer apply. It also has no physical boundaries. Hence, criminals seeking information stored in network computers with dial-in-access can access that information from virtually anywhere in the world. The quantity of information that can be stolen or the amount of damage that can be caused by malicious programming code may be limited only by the speed of the network and the criminal's equipment.

**Advance Planning for Search**

**18.12** When the Investigating Officer is required to carry out search in a place where it is suspected that computer or computer networks or any other electronic memory devices are likely to be found, it is advisable to contact computer forensic scientists of a Forensic Science Laboratory to accompany the search team. In case, it is not possible, information may be collected regarding the type, make, model, operating system, network architecture, type and location of data storage, remote access possibilities etc., which can be passed on to Forensic Experts as that would help making necessary preparation to collect and preserve evidence. It must be remembered that on some occasions, it may not be possible to remove the computer system physically and data may have to be copied at the scene of crime/place of search. The Investigator

or expert must carry necessary media, software, and other specialized items as well as special packing materials which can prevent loss of data as data of magnetic media can be destroyed by dust, jerks and electrostatic environment.

## PRECAUTIONS AT THE SEARCH SITE

### Taking control of the Location

**18.13** It is extremely important to ensure that suspect or an accused is not allowed to touch any part of the computer or accessory attached to it either by physical means or through wireless. Since these days, systems could be connected through physical networks such as fibre optic, cables, telephones or on Wi-fi or Wi-max wireless networks or even through a mobile phone having a wireless communication port, the Investigator has to be extremely alert and may seek guidance from an expert, if not available on site, on telephone and take steps as per instructions. The Investigator must remember that even by pressing a key or by giving a command through a wireless mouse or keyboard or even by executing a command through an e-mail message, the entire data either could be wiped out or corrupted, making it useless for the Investigator. This is also applicable in the case of small devices or removable storage devices, which have the capacity of storing huge amount of data. Thus, it is extremely important that individuals present at the site of the search are separated from their computers and all devices are kept out of their reach. Since it is easy to tamper or destroy computer evidence, and it can be done from across a network, which could be physical, or wireless the Investigator should take all steps to secure data.

**18.14** As already mentioned, the information in a network environment need not be stored at the same site. The data could reside at a remote location even in a different country. Therefore, it may be important to find out the storage location and take action accordingly. In case, storage of data is suspected to be located outside the country, it may be necessary to alert the Interpol and take necessary follow up steps to issue letters rogatory under the provisions of Section 166 A Cr PC.

**18.15** Before conducting the search, the Investigator will need to decide whether to seize data on site, or seize hardware for examination at a Computer Forensic Laboratory. While on-site data seizure has the advantage, that one does not have to transport much hardware, one may need services of a Computer Forensic Expert to download data for analysis and preserve data for presenting it in the Court. When in doubt, make use of a Computer Forensics Specialist at the scene, if possible, to determine whether one needs to seize data or seize hardware. In case, a specialist is not available, it is recommended that one seizes everything.

### Networked Computers

**18.16** Do not disconnect the computer if networks or mainframes are involved, pulling a computer from a network may damage the network, and cause harm to the company's operations. It is generally not practical to seize a mainframe because it requires disconnecting all the computers that are attached to it. Hardware seizure with computers on a network can be very complicated, and one should definitely enlist the help of a Computer Forensics Specialist in these cases.

### Preparation for the Search

**18.17** The Investigator should carry the following items with him that will facilitate the search: ─

(1) Disks or Cartridges ─ these can be used to store copies of files from the computer for use in his investigation.

(2) Labels ─ to label cables, where they plug in, disks, the various parts of the computer and to write/protect disks.

(3) Screwdrivers and other tools used to dismantle the hardware for seizure.

(4) Gloves ─ remember that often, latent prints can be taken from disks or other storage media or hardware.

(5) Packing materials – rubber bands, tape, boxes, bubble wrap, and if he does not have access to anti-static wrap, paper bags should be used, because they have less static charge than plastic bags.

(6) Camera equipment – to videotape and photograph the scene.

(7) Chain of custody report sheets and other paper to inventories seized evidence.

**STEPS FOR THE SEARCH**

**Rely on Technical Experts**

**18.18** Be careful not to cause damage during a search as electronically stored data can be easily lost. The services of the Computer Forensic Experts must be availed, wherever possible. The experts can not only help during a search, but could also assist in interviewing the company's technical personnel because they will know what questions to ask to elicit relevant information for the investigation.

**18.19** Once on-site, the Investigator must survey the equipment and take precautionary steps as described above. Next, he will need to document the way the system is connected together and take the following steps: ─

(i) **Labelling & Photographing the Set-up**

Labelling and photographing everything prior to dismantling the system is an important first step. Take some general photographs of the search site to document its pre-search condition for legal purposes, and to serve as a reference during investigation. This documentation on how the system was configured may prove essential when the system is re-connected in the Forensic Laboratory. As the IO is taking the pictures, he should make sure to get close-ups of the front and back of all equipment and the way it is connected. He should pay special attention to DIP switches on the back of certain equipments that must be in a certain configuration. These switch settings could accidentally be moved in transport creating problems for the examiner.

(ii) **Label all Parts**

The I.O. should label each part before he starts dismantling any of the equipment. He should remember to label all the connectors and plugs at both ends, and on the computer so that re-assembly is easy and accurate. A good way to do this is to label each item its own letter. For example, a power cord may be marked 'A' on the end and a corresponding label marked 'A' on the computer port where this plug is to be inserted.

(iii) **Power System Down**

As a rule if a computer is off, it should not be turned on. Hackers can make their computers erase data if a certain disk is not in the drive when the machine is booted up or if a certain password is not entered. Likewise, if the machine is on, one should check it before turning it off otherwise it may

destroy data. Keep in mind that a computer may look powered down but actually, it may be in a "sleep" mode. Hackers can set their computers to erase data if not properly awakened from a "sleep" mode, so one may be required to pull the plug or remove the battery from a laptop in these cases. The I.O. may need to shut the machine down through the operating system rather than just "Pulling the Plug." If, however, he does need to "pull the plug," he should disconnect it from the back of the machine rather than at the wall, because if the machine is plugged into a back up power supply it may initiate a shutdown procedure that could alter files.

(iv) **Dismantle the System**

Once the system is labelled and powered down, it can be dismantled into separate components for transportation. If a computer is at a business location and a part of a network, proper procedure should be followed to properly disconnect the computer from the network.

(v) **Seize Documentation**

Seize all manuals for the computer, its peripheral devices, and especially the software and operating system. The examiners at a Forensic Laboratory need to refer to a manual to determine the kind of hardware and its technicalities. Seizing other documentation at the site like notes, passwords, and journals may prove very useful. Sticky notes, or other pieces of paper around the computer systems that may have passwords or login ID's written on them, should also be seized from the spot.

**18.20 Handling Evidence & Computer Hardware**

(i) **Protecting Data**

The I.O. should also write/protect disks or cartridges he finds at the site of search in order to protect the data. Most disks and cartridges have a small sliding tab that prevents changing the disk content when set correctly. Placing a blank disk in the hard drive of computer system will keep them from booting up from the hard drive if they are accidentally turned on.

(ii) **Packaging for Transport**

Once the I.O. or the expert has dismantled the computer, it is ready to be packaged for transportation to the Forensic Laboratory. Computers parts being sensitive are easily damaged and the hard drives that usually store data have delicate mechanisms, so they should be handled carefully. One should not wrap the computer components using Styrofoam because small particles can break off and get inside the computer causing it to malfunction. Anti-static plastic bubble/wrap is preferred.

(iii) **Keep System Components together**

Keep the components of each computer system together. This small organizational step can save lots of time when the examiners are trying to reconstruct the system.

(iv) **Single Machine, Single seizing Agent**

If one person handles the seizure of a computer, that same person can authenticate the evidence at a trial. This simple consideration can avoid confusion later.

(v) **How to transport and store the System**

Do not put the computer in the trunk of a Police vehicle. The computer system should be secured in a way that would reduce vibrations that may shake a part loose. The I.O. should store the computer in a secure, cool dry place away from any generators or other devices that emit electromagnetic signals.