The law enforcement community is facing a new challenge today, in the form of information technology age in the wired world. Asking a computer wizard to upgrade our computers or the reporting of computer crimes may be easy but combating this crime and getting successful convictions still remains an uphill task for the present law regimes around the world. Countries are depending more every day on innovative information technology in administering almost every aspect of daily life, ranging from ID cards, credit cards to health records or the security and defense of its borders. Yet, nations are now also concerned about taking specific steps in protecting themselves from losses caused by cyber criminals who act anonymously and may not even be within the national borders.

How big is this “high-tech crime” problem? No one can really answer this question. But in terms of financial losses it has cost billions of dollars to the industries annually. In 1998, a loss of US$ 11 billion in revenue was suffered in United States of America alone. Last year, 89% of businesses were the target of cyber crimes in the United Kingdom, which resulted in a loss of GBP 2.4 billion. If left unchecked, cyber crime can potentially hijack all expansion of electronic commerce and Governance.

The Internet has provided a lot of benefits to the society and businesses; likewise, it also provides new opportunities from criminal conduct.

Generally cyber crimes fall into three categories:

---

1 US Deputy Attorney General Eric H Holder Jr, 2000
2 Research by National Hitch Crime Unit (NHTCU), UK
1. **Crimes where a computer is the target, e.g. hacking.**

2. **Crimes where computers are the medium by which criminal enterprises are executed e.g. software piracy, internet frauds.**

3. **Crimes where the use of a computer is incidental to criminal acts e.g. storing information on a computer about drug trafficking, white collar crimes etc.**

The major challenges that cyber crimes pose are that they do not recognize and are therefore not limited by any boundaries. An individual armed with nothing but a PC can target businesses or air traffic controls anywhere in the world without ever stepping a foot outside his room. Anonymity is a major issue of this area of crime. But law enforcement is confined to state borders and the sovereignty of nations has to be respected. If international co-operation or a mutual legal assistance agreement is not in place, many criminals go unpunished. Laws are also not comprehensive to tackle crime or the criminal. The reason why the “LOVE BUG” criminal could not be punished in the Philippines was that there was no law to criminalize the actions of the boy and he could not be convicted under the traditional penal law. There is also a dearth of experts handling computer crimes in the world; even the few that are in the field have a lot of disparity in their work. Emerging issues of privacy and civil liberties have also strongly emerged in post-9/11 computers tapping in USA, which may possibly slow down the process of litigation and prosecuting of cyber criminals. But even if we put all these problems aside, collection of evidence and its admission in a court of law for successful prosecution in a cyber crime case is a very difficult technical job, which requires huge funds and expertise. So much so that sometimes the criminals themselves are the only experts who can help the law enforcement agencies in collecting forensics of the computer on or through which the actual crime took place. It can therefore be imagined what will be the ratio of successful cases for the police and law enforcement agencies.

It is easy to steal, leak, manipulate or destroy electronic data. But just as in the physical world, cyber criminals too leave their electronic fingerprints and footprints at a digital crime scene^{3}. Now businesses spend huge funds on IT Security to protect their

---
^{3} “The effective response to computer crime”; by Jane Simon, Computer Weekly, 21.03.2006.
networks and software from the external threats of hackers, viruses, fraudsters etc. Often when a company is faced with a cyber attack or crime, it does not know where to start, what to do or even whom to turn to. About 93% cyber crimes go unreported because companies don’t want bad publicity or disruption of business, as that could be more damaging to the company than the crime itself\(^4\). But the best line of defense is to make right policies, procedures and communications in place otherwise the time bomb is ticking. Laptops, digital cameras, mobile phones provide a mountain of data and proof that can solve a case. Email has also become indispensable in prosecuting organized crime\(^5\).

What can be the best tool to collect evidence of a cyber crime and present it in a court of law to successfully convict a cyber criminal? Traditional methods have not proved useful in this area thus far and therefore a different technique would need to be adopted. Here are some of the necessary steps which one should remember in collecting computer forensic evidence.

**REPORTING:**

Planning the response is important. One should not panic, and the person should not touch any button on the computer.

It is important that the crime is reported immediately because time is of essence in cyber forensic evidence collection. Usually unaltered digital evidence is available only within the span of a few hours. Sometimes even 24 hours proves to be too late to recover non-tampered digital evidence. In this step the company should be clear as to whom it has to report to so that an investigative team is formed, because the investigators may access sensitive data. There should be a clear privacy policy in place.

**INVESTIGATION:**

Only a skilled computer forensic investigator should undertake investigation. Otherwise collection of evidence will almost end up in a failure of an investigation and ultimately a failed prosecution.

---

\(^4\) Jane Simon; Computer Weekly 2006.

\(^5\) Jeffery Toobin; Senior Legal Analyst for the International media.
It is also very important for the investigator to understand the level of sophistication of the suspected criminals. They must be considered to be experts in any case and ancillary counter-measures must be adopted to guard against the destruction of any digital evidence. If this is neglected, it may modify the data on the computer. Some computers have automatic wiping programmes in case a new person touches the wrong key on the keyboard. It then becomes time-consuming and expensive to recover such data, if at all possible.

SECURING MACHINE AND DATA:

Electronic evidence is fragile. It can be damaged or altered by improper handling or examination. Special precautions should be taken to document, collect, preserve and examine this type of evidence. This will ensure the integrity of the electronic evidence at a later stage. When a cyber crime is committed, the room and computer of occurrence should be considered to be a crime scene and sealed off to ensure evidence is not tampered with. Even the victim’s computer should be sealed off. It is critical that in early stages nothing is changed in the immediate surroundings of the device. If the computer is off, it may be left off, if it is on, it should be left on. Care is necessary so that standards of admissible evidence can be followed. If the computer is mishandled at that time, the data collected can be challenged later and may not be valid before a court of law e.g. legal warrants of search and seizure is required just like any other search, only quicker action is needed. As a forensic expert, one should have legal authority to seize and read the data from the device. Otherwise the consequence may be that not only the case is thrown out but also that the investigator may find himself being sued for breach of privacy and damages.

Other useful tips are to take photographs of the surroundings, seizing and securing any papers, printouts, disks, MP3 players etc lying around in the vicinity of the cyber crime. Likewise, interviewing and recording the statements of people at that place can prove to be helpful. These people can later be potential witnesses in the lawsuit. This can also help in discovering passwords or email addresses of the suspect.

7 Jane Simon; Computer Weekly, 2006.
This basically means duplication of the hard drives. This is a crucial stage of digital evidence collection. It is to duplicate the entire hard drive. One has to make a bit-stream copy of every part of user accessible areas, which can store data. The original drives should then be moved to secure storage to prevent tampering. Some softwares such as “Encase” or “Sleuth Kit” are available, to duplicate the drives for digital evidence collection. It is important to use some kind of hardware write protection to ensure no writes will be made to the original drive. Even if the operating system, such as Linux, can itself be configured to prevent this, it is a better and safer practice to separately use a hardware write blocker. It is possible to image to another hard disk drive, a tape or other media. Tape is a preferred media to store images since it is less susceptible to damage and can be stored for a longer time.

It should be ensured that the image is: (i) Complete (i.e. contains all information); and (ii) Accurate (i.e. copied correctly).

The SHA-1 message Digest algorithm or other such algorithms can be used to verify the imaging process. To make forensically sound images, it is advisable to make two reads that result in the same output. Generally the drive should be hashed in at least two algorithms to help ensure authenticity. Imaging should be made within the crucial timeframe for collecting electronic evidence, since thereafter its credibility would become questionable and not valid for legal purposes.

Every bit of information should be copied. Deleted or even damaged files are actually never deleted or gone and can be recovered by the imaging process, though it may takes days or even weeks to recover them. One tip given by experts is to keep one master copy in some safe place of agency to be used as a back up, and to use the second one as working copy for the investigation and analysis. In imaging:

---

9 Encase Forensic By Guidance software, Sleuth Kit-open source disk and file system analysis software.
10 It is Possible to restore a deleted file even if it is seven times over written.
1. Everyday computers or media should not be used. New media should be used, e.g. the computer should be taken to a technical lab for imaging. Now many law enforcing agencies have their own labs for imaging and analysis of digital evidence whose reports are used in legal cases.

2. Imaging software should be forensically sound so that no changes occur during imaging. Such software is commercially available, though expensive and often costing millions of dollars\(^{11}\).

3. All investigation material should be backed up.

It is therefore necessary that the persons involved in evidence collection relating to cyber crimes are specially trained personnel. Investment should be made now in such training, which are available worldwide.

Court rooms and universities are welcoming more lawyers and agents to specialize in electronic crime issues, thereby setting stage for evolution of cyber law while the debate over digital evidence and what limits may be put on it is still raging\(^ {12}\).

**FORENSIC ANALYSIS AND DRAWING A CONCLUSION.**

The expert then examines the digital evidence and gives a final report about the act complained of as a crime. This report is a determination of whether an act on a computer was a breach of any penal law or not. Therefore it should be made very carefully. It must be objective, based on indisputable facts, because law enforcers will connect the suspect to the act of the computer performed by a human. This connection therefore has to be beyond reasonable doubt. It is advisable to obtain and rely on professional legal advice at this stage. But above all, the existence of a regulatory framework and laws catering for cyber crimes in the country are the sine qua non.

\(^{11}\) Pakistan has got Encase software installed at FIA Cyber Crime Unit.

\(^{12}\) Professor Brenner, University of Dayton reported by CNN - 07.07.2006.
The above discussion is only one part of cyber crime evidence collection. The second equally important phase is presenting all that digital evidence in a court of law as evidence against a suspected cyber criminal to successfully convict.

In Pakistan\textsuperscript{13}, it is allowed to use any modern devices through which evidence can be presented in the court. Under the Electronic Transactions Ordinance, 2002\textsuperscript{14}, electronic evidence via emails etc. has also been made admissible as evidence in courts. But the real question is how far the digital evidence collected by a computer expert fulfills the criteria set by the general law of evidence to prove guilt of a criminal. The lack of continuity and completeness of evidence can compromise the legal position. It is also required that the court be satisfied that the evidence has not been modified and is absolutely reliable. For this, hi-tech technical facilities, production of access control measures, or other supporting evidence should be used to justify integrity of digital evidence. It is necessary that legal advice be sought before relying upon logs, files or other electronic data in a court of law. Scientifically, the results of the computer analysis should be able to withstand legal scrutiny. Details of imaging will play a crucial role in establishing the credibility of digital evidence in a cyber crime case. If a country’s law enforcing agencies have no system in place or procedures to collect or store the electronic evidence, cyber crimes will go unpunished and expert’s work of investigation will also go wasted and inadmissible. While collecting electronic evidence it is good to consider (i) rules of evidence to support an action against a cyber criminal; (ii) admissibility of evidence and complying with any existing standards for the admissibility of evidence; and (iii) quality of evidence for which a strong evidence trail is necessary.

The changing world of technology presents a challenge for the courts to keep pace with new laws in addressing evidence and other legal issues involved. USA Police Officials are already complaining that since 9/11 there is a shortage of digital analysts at the local law enforcement level because the Government has engaged their services to track terrorism around the world.

\textsuperscript{13} Article 164 of Qanun-e-Shahadat Order, 1984.

\textsuperscript{14} See Schedule of the Ordinance amending Article 2,30,46, 59,73,85 of Qanun-e-Shahdat Order, 1984. A new article is also introduced as Article 78-A.
Also, there are very few legal precedents to guide the Judges on the conviction or otherwise of cyber criminals. Even in the developed world Judges often have little experience of digital technology, so we can expect far less from Pakistan. But a hot issue on digital evidence is the right of privacy of the suspect. During evidence collection, every file has to be read by the expert to know which part is relevant to the crime, and as a result he may unintentionally read or peruse some private files, which were not be read by any one. Privacy and credibility of evidence are two thorny issues to be tackled by law enforcement departments all over the world. Laws are to be revised; procedures of warrants to be changed and many computer forensic labs need to be established at state level to handle both these questions.
Reference:

(2). Research by National Hitch Crime Unit (NHTCU), UK
(5). Jeffery Toobin; Senior Legal Analyst for the International media.
(10).Encase Forensic By Guidance software, Sleuth Kit-open source disk and file system analysis software.
(11).It is Possible to restore a deleted file even if it is seven times over written.
(12). Pakistan has got Encase software installed at FIA Cyber Crime Unit.
(13).Professor Brenner, University of Dayton reported by CNN - 07.07.2006.
(15). See Schedule of the Ordinance amending Article 2,30,46, 59,73,85 of Qanun-e-Shahdat Order, 1984. A new article is also introduced as Article 78-A.