Cyber Crimes and Cyber Forensics

Lecture delivered in the National Institute of Technology Calicut on 9th Jan., 2013

Dr. P. Vinod Bhattathiripad Ph. D. (Software Piracy Forensics)

Any technology is prone to be abused and computer technology is no exception. In the modern world of information and communication technology, criminals are expanding their horizons into the electronic space. As a result, the ethical, legal and practical issues related to abuse through or of this technology are also gaining importance. Any crime related to this technology, in general, and computers, in particular, is a cyber crime, be it cyber financial fraud, identity theft (unauthorized disclosure of names, telephone numbers, email id etc.), hacking, slacking, threat through email, vulgar messages, misuse of telephone technology, use of computers for anti-national activities, virus, use of computers for personal gain, violation of company acceptable policies, launching of denial of service attacks on computer network servers, software piracy or supply of low-quality Information Technology (IT) products. Also, criminal activities like misuse of telephone technology, pornography, unauthorized disclosure of internal and confidential information, theft or trade of intellectual property etc., when realized through cyber space, can also fall under cyber crime. Any criminal activity where a computer or a computer network is the source, tool, target, or place of the crime is generally termed as a cyber crime.

Computers can assume a variety of roles in the commitment of a crime and each of these roles can raise novel investigative and prosecution-related issues because of the unique attributes of computers and of the electronic evidence they hold. Based on these roles, there are perhaps several ways of looking at and categorizing cyber crimes, and for this, one could use different taxonomic approaches too like the nature of the crime, its intent, tool that it uses or the analyst's purpose of classification. Cyber criminal activities could also be looked at in terms of their intentionality (for intellectual gratification, for destructive purposes etc.) or the technology involved (network crimes, software crimes etc.). A computer can be (1) the subject of a crime (by being stolen or damaged); (2) the site of a crime (such as when a child is solicited for sex in a chat room) or (3) the instrument of a crime (such as when it is used to store information illegally). The categories may or need not be exclusive and the criminal activities can overlap. For instance, spreading virus, even though destructive, has been found to provide (perverse) gratification for the criminal.

Cyber criminal activities leave electronic evidence which is in the form of data and information, stored in the computer disks or other peripheral storage devices. In order to establish a cyber crime, collecting digital (or electronic) evidence, with the help of cyber forensic experts, is mandatory.

Forensics of digital equipment is digital (or cyber) forensics. Digital Forensics is the gathering and analysis of digital information in an authentic, accurate and complete form for presentation as evidence in a civil proceeding or a court of law. It can also be defined as the employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity. It uses scientifically derived and proven methods for preserving, collecting, validating, identifying, analyzing, interpreting and presenting digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations. Digital forensics is highly technical, and therefore grounded in science. It is also a discipline that often requires knowledge of engineering, particularly electrical, mechanical and computer engineering with deep insight in mathematics and law. Applying the science and engineering in specific investigations is a complex process

that requires professional judgment that is sometimes more art and common sense than science. The technical requirements of computer forensics are certainly rigorous and the forensic specialists should know a great deal about the normal functions of the operating system in question. Finally, cyber forensic specialists draw on an array of methods, procedures and tests for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information. Using these methods, procedures and tests, digital forensic investigation is generally done on digital data to produce (legally accepted) digital evidence.

Cyber forensic (or a technical) expert before the court of law is generally the person who is designated by the judge or any other law enforcement authorities to look into the technical aspects of a case and prepares a report that is legally convincing and binding. A technical expert thus needs to assist the judicial system to establish culpability and help the judicial system in convincingly validating the legal process of resolving the situation. An attorney too can seek the help of an expert to perform a limited investigation with limited objectives.

From the cyber forensic experts, the legal domain and judiciary demand (or solicit) only digital forensic evidence that is relevant, derived by the scientific method and supported by appropriate validation. The American judiciary has suggested several factors to be considered to determine whether digital evidence possesses the requisite scientific validity. These are: (a) whether the theories and techniques employed by the scientific expert have been tested; (b) whether they have been subjected to peer review and publication; (c) whether the techniques employed by the expert have a known error rate; (d) whether they are subject to standards governing their application; and (e) whether the theories and techniques employed by the expert enjoy widespread acceptance and these are together called the Daubert conditions.

In order to bring cyber criminals in the court of law, almost all countries have formulated cyber laws. In India, most Cyber criminals are booked under various sections of Information Technology Act-2000 and Indian Penal Code. The Indian Evidence Act also has been amended to legalize digital evidence. The IT Act 2000 was amended in 2008 to include more sections to cover other cyber crimes. These days, police across the world, depend on digital evidence in order to establish not only cyber crimes but also non-cyber crimes like murder, rape etc.

About the speaker: Dr. P. Vinod Bhattathiripad is cyber forensic consultant to police, judiciary, income tax department and banks in India and abroad on civil / criminal cases concerning software piracy and digital data recovery issues, since 2007. His doctoral thesis is on "Judiciary-friendly forensics of software copyright infringement" and he is the first Asian and one among the very few in the world with a doctorate in this forensic area. He has been (and is still) a technical committee member of the ICST International Conference on Digital Forensics and Cyber Crime in Abu Dhabi (2010), in Dublin (2011) and in Purdue University, USA (2012). He has been the acting chairman of the Workshop on "Computer Forensics in Software Engineering" as part of the 36th IEEE World Conference on Computer Science, held in Turkey, in 2012. He has published locally and internationally on software piracy / copyright infringement forensics. He serves as a reviewer of several international journals including the 3 prestigious American journals namely Journal of Digital Forensic Practice, Computers and Security Journal, and Journal of Digital Forensics, Security and Law. His paper on the forensic importance of programming blunders was one among the five papers short listed for the best paper award in the Conference of Digital Forensics, Security, & Law (2012, Richmond, VA, USA). Earlier, as software professional, he has been part of 148 software development projects spanning 18 years between 1989 and 2007. He has extensively traveled in Asia, Europe and the US. He is available at vinodpolpaya@gmail.com or can be contacted in +91-94470-60066 or +91-94474-81234.