FORENSICS AND THE 'e-world': HOW FAR INDIA REACHED

Adv. Ratna Sisodiya - Practicing advocate at District and Session Court, Udaipur, Rajasthan, India.
Email - ratnasurendrasingh@gmail.com

Abstract: The latest trends of internet provide ample fastest services but certainly provide a web of crime to deal with. The technology dealing with such criminal activities and to secure measures to deal with, is termed as computer forensics/ cyber forensics or IT forensics. To find the scene behind crime, conducted with the help of a computer resource and involving numerous guilty minds from different part of the world. In India the digital conduct and IT functioning is governed by Information Technology Act, 2000 and also some sections of Indian Penal Code (IPC). The accuracy of analysis is maintained by the knowledge and experiences of experts. Somtimes also by repeated analysis involving other experts for confirmation and second opinion.

Key words : Cyber Forensics, e-discovery, Physical Forensics, Jurisdictional Issues, Computer Evidences, Domain Specific.

Introduction:

"In simplest words, an art of applying computer science to aid the legal process is known as Computer forensics"

- **Chris LT Brown**
(Computer evidence
Collection and preservation, 2006)

It is rightly said that the revolution of internet came along with a new revolution of crime. The cyber or computer crime which embraces activities like hacking, online frauds, illegal downloading, child pornography, scams, cyber terrorism, creation and distribution of viruses or spam's and so on. Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that it is suitable for presentation in a court of law. In other words it is the process which facilitates a link as to curb a check on such activities and to reach out the real culprit behind the screen is referred as cyber forensics.Though, a finely drafted piece of legislation "The information technology act,2000" provides legal ways to combat problem related to computers and also gives a legal framework so that information is not denied its legal effects, validity or enforceability, solely on the basis that it is in the form of electronic record. The goal of computer forensics is to perform a structured investigation while maintaining a document chain of evidence to find out exactly what happened on a computer device and who was responsible for it.
Global Position System (GPS) software embedded in smartphones and satellite navigation (satnav) systems can also aid prosecutors by tracking the whereabouts of a suspect. Since companies that develop software for computer forensics also develop products for satellite navigators, they are well-equipped with the tools and technology necessary for acquiring GPS evidence.

Experts:

In court computer forensic evidence is subject to the usual requirements for digital evidence; requiring information to be authentic, reliably obtained and admissible. A Cyber expert is the person who is expected to know all aspects and legal implications related to this field. Expert investigates and coveys his analysis and output through a report that is considered his opinion legally. It is to be taken care of that the investigation and analysis is done following a legal prescribed way preserving all evidences for future reference. As in case of every field digital devices and IT Networks also follow basic principles of functioning and digital laws. Accuracy of analysis is maintained by the knowledge and experience of expert sometimes also by repeated analysis involving other experts for conformation and second opinions.

COMPUTER FORENSICS AND E-DISCOVERY:

Although the terms tend to be used interchangeably, and there is a degree of overlap, there are clear differences between computer forensics and e-discovery. The e-discovery process usually deals with data from multiple desktop systems in an enterprise, or from servers with that may contain lots of user accounts and their associated information. The discovery method tends to use proven software and hardware combinations and is often pre-planned at the start of an investigation.

Computer forensic goes deeper and may be a logical next step to the e-discovery process. It may deal with single or multiple systems or devices; it is also more often dealing with missing or incomplete data and, crucially its findings may be presented and challenged in Court.

COMPUTER FORENSICS VS. PHYSICAL FORENSICS:

Cyber forensics is distinguished from physical forensics as there are many core differences between the both. Where, the physical forensics focus on identification and individualization, computer forensic science on other hand focus on finding the evidence and analyzing it in reference with 'e-crime'. Cyber forensics requires specialized expertise and tools that goes beyond the normal data collection and preservation techniques. Thus, cyber forensics is more than the technological, systematic inspection of computer system and its contents for evidence of civil wrong or a criminal act.

JURISDICTIONAL ISSUES:

By its nature, however, the internet is international: it disrespects local and national jurisdiction. The challenges, therefore, are to create rules that work across local, national and international boundaries. Though, Information Technology Act, 2000 does have extra territorial jurisdiction but he implementation is still facing few difficulties. In case of *Casio India Co. Ltd. Vs.Ashita tele systems Pvt Ltd.,* Delhi high court held that once a website can be accessed from Delhi, it is enough to invoke the territorial jurisdiction of court. But, later in case of *India T.V. Independent News services Pvt. Ltd. VS. India Broadcast Live LLC* held that mere a fact that a website is accessible in a particular place may not itself be sufficient for courts of that place to exercise personal jurisdiction. Furthermore, as methods for encryption and anonymity grow more advanced, technology may be abused by helping criminals hide their actions. Ultimately, the role of technology in computer forensics may not reach its full potential due to legal boundaries and potential malicious intentions.

RESOURCE CENTRE FOR CYBER FORENSICS (RCCF):

RCCF was established at C-DAC (T), i.e., Centre for Development of Advanced Computing, Thiruvananthapuram. As state- of -the -art research centre for cyber forensic, by The Department of Electronic and Information Technology, Government of India to pursue research and development, training and technical services in cyber forensics. RCCF is a pioneering institute, pursuing research activities in the area of cyber forensics in India and was set up with following objectives:

1. Developing indigenous cyber forensic tools.
2. Provide training on cyber forensic to Law Enforcement Agencies (LEAs).
3. Providing technical support to LEAs for cyber crime investigation and analysis.
4. Supporting LEAs for setting up of cyber forensic laboratories.

Another leading name in this field is **Perry4law.** It is the 'first & exclusive' techno-legal and cyber forensic firm of India and one of the best in world. Its professional services are not only unique but also matchless. Being the only cyber forensic firm of India, it has developed 'Domain Specific' cyber forensic capabilities and expertise. Perry4law has also played a crucial role in strengthening the Information Technology Act, 2000, by suggesting useful provisions regarding cyber terrorism in India, obscenity and pornography provisions etc. At the same time it has also advised government of India not to violate "civil liberties" of Indian citizens by unreasonable and unconstitutional provisions in Information Technology Act, 2000.

This shows that India is developing its IT skills from public as well private sector. It is definitely a huge step towards globalisation and much needed to stand with other developed nations.

CONCLUSION:

No doubt that the country has reached MARS of success, yet many miles to go more. The fastest growing technology demand more caution and legal check to assure safety. Laws so formulated cannot operate properly until a proper procedure is prescribed. We need to develop cyber forensics investigation solution in India to encourage digital and scientific evidences in India. The regulations and guidelines must also be drafted as soon as possible. For computer forensics to progress, the law must keep pace with technological advancements. Clear and consistent legal procedures regarding computer system searches must be developed so that police and investigators can be properly trained. An International Code of Ethics for Cyber Crime and Cyber Terrorism should also be established to develop protocols for "obtaining and preserving evidence, maintaining the chain of custody of that evidence across borders," and "clear[ing] up any difference in language issues." Following these measures may be the first steps to resolving the technological and legal limitations afflicting computer forensics. Interpol, the International Criminal Police Organization, has developed a Computer Crime Manual with "training courses" and "a rapid information exchange system" that serves as a foundation for international cooperation. Lastly, the criminal abuse of technology can be limited by equipping the police department with state-of-the-art training and equipment for forensic analysis. Only then is the world safely prepared to face the future of technology. As one author predicts,

"the next world war will be fought with bits and bytes, not bullets and bombs".

REFERENCES:

1. Cyber forensics@ CYBERLAWSINDIA.net
2. Elvidence Pty Limited, *"Computer forensics and e-discovery, are they the same thing?"* (December 6, 2014).
3. Jeremy Kirk, IDG News, April 12, 2011 *"Study – police increasingly peeping facebook, e-mails and insta messages".*
4. Aaron Philip; David Cowen ;Chris Davis (2009) *"Hacking exposed : computer forensics".*
5. Amit M. Sachdeva, *"International jurisdiction in cyberspace: A Comparative Perspective".(2007).C.T.L.R. Pp245-258.*
6. Dartmouth Undergraduate Journal of science- *"Computer Forensics in criminal investigation"*, by Barry Chen/ Applied sciences, uncategorized, winter 2013/ march 13, 2013.

WEBSITES:

1. Computerforensicsindia.blogspot.com
2. www.cyberforensics.in
3. www.cyberlawsindia.net
4. www.indiaforensic.org

Author's Biography:

Adv. Ratna Sisodiya a Bachelor in Commerce, possess another Bachelor Degree in Law, a Post graduate Diploma in Taxation and also a Master Degree in Law from MLS University, Udaipur.