Application of Cyber Forensics in Crime Investigation

Urvashi Sharma Mishra
Assistant Professor in Computer Science,
Hans Raj Mahila Maha Vidyalaya, Jalandhar.

Received: May 09, 2018 Accepted: June 21, 2018

ABSTRACT *Use of computers in the domain of law is recent and confined to the surface levels only. But the new techniques and types of crimes, known as cyber-crimes going to the extreme levels of terrorism through the channels of economic offences at both national and international levels prove the existing interface of law and cyber forensics inadequate and lagging both in theory as well as in practice. Such areas may be of crime investigation and trial in the courts of law, thereby making humble advances in this field as enactment of Information Technology Act and amendments in this law as well as in the Code of Criminal Procedure and Indian Evidence proving to be largely insufficient and inadequate to address to the present needs. Such needs are achieving over 80% convictions like in the developed world, scientific investigations and proof of evidence in the courts through cyber forensics techniques and technology. For the purpose, the co-operation of law and cyber forensics must become very intimate to be coupled together appearing to one discipline.*

Keywords: *Cyber Forensics, cyber-crime, crime investigation, Information Technology Act.*

INTRODUCTION

Technology has caused a bearing on practically every aspect of our lives. Law and criminal administration of justice are no exception to it and accordingly, forensic devices have entered in areas of Criminology. These devices are being used by courts, Advocates, crime investigation agencies and institutions imparting legal education. Computers have facilitated our work and made things easier. It has led to development of e-commerce, e-banking etc. Today commercial transactions, commercial contracts and banking transactions are carried out with the help of computer devices and internet. But these advancements have other aspects as well. They have not only facilitated commission of traditional crimes but have also given birth to cybercrimes causing their increase at a rapid pace [14]. On the other hand, the unscientific investigation of crimes is resulting in acquittals of crimes on a shockingly high scale. The forensic tools fail to match with the knowledge and techniques of criminals. Unless the forensic tools are upgraded and efficient systems are developed, the menace of increasing acquittals may cause havoc in our society shattering its socio-economic fabric. The need for it is urgent and instant compelling the research institutions to come forward to meet this pressing need of criminal judicature.

Crimes and Cyber Crimes

Though punishment is the normal consequence of a crime but the standard requirements of proving the criminal commission lead to the situation where acquittal of the criminal is visibly more rampant than the infliction of punishment. In India, the conviction rate i.e. the proportion of accused persons found guilty of the offences by the courts is about 46.9% [34], meaning thereby that majority of the criminals go scotfree. So far as cybercrimes are concerned, the conviction rate is more poor at 23.9% [1]. This trend of criminal jurisprudence in India is not a healthy one because the responsible and honest citizens lose faith in the legal system. It encourages the potential criminals to enter the criminal world and also the criminals escaping punishment getting encouraged to perpetrate more heinous crimes. If not dealt firmly and effectively, this malady may cause disruptions and upheavals in the society. For this reason it is essential and urgent that causes of acquittals are remedied.

Globalization and digitalization of information in the present day information society has effected all of us and it has brought to the fore various legal, ethical and social issues. A relatively newer category of offences viz., cyber offences have hit the crime scene with great force. Advancements in technology have not only resulted in creating categories of new offences but it has also brought with it new dimensions in crime detection and investigation.

Legal Upgradation

Law cannot remain aloof from technological advancements. Rather it usually follows them though it may be slow in reacting to the technological advancements. Accordingly, to cope up with cyber crimes various legal measures have been adopted including amendments in Indian Penal Code, Evidence Act and

Bankers Books Evidence Act etc. and the enactment of Information Technology Act, 2000 which is a mother legislation dealing with cyber crimes. The increasing advent and dynamics of cyber crimes compelled the Indian legislature to update the Information Technology Act. With this object in mind and to bring the IT law in tune with Model Law on Electronic Signatures adopted by the United Nations Commission on International Trade Law, the Information Technology (Amendment) Act, 2008 has been enacted. Indian Evidence Act has been amended to make electronic evidence relevant and admissible in Indian Courts.

However, there is still a vast area uncovered where interface between law and computers can bring about large scale improvements. The most important area of this uncovered field is investigation of crime and use of digital evidence in courts. The need for this has been felt and underscored. Justice V.S. Malimath Committee Report (2003), 185th Report of the Law Commission of India and Justice J.S. Verma Committee (2013) have suggested for making efforts in the direction of scientific criminal investigation and Computer Forensics.

Our reference to the literature on the subject has revealed that lack of scientific investigation is the major reason for large scale acquittals by the courts in India. Availability of scientific investigation tools and techniques makes the conviction rate of crimes in UK and USA going to the extent of 80 to 90%. Therefore, Indian legal system has also made some progress in the field of scientific investigation of crime and is looking forward for much more research and efforts in this direction. The progress made is embraced by the term Forensics.

Cyber Forensics

Cyber Forensics is the process of using scientific knowledge for collecting, analyzing and presenting evidence to the courts. Basically cyber forensics is the combination of computer forensics and network forensics. The aim of cyber forensic examinations is to recover the evidence to support or oppose a criminal activity. It requires the investigators to collect and analyse the electronic evidence.

It exists in forms, such as fingerprints reading, blood analysis, toxicology, DNA mapping, facial reconstruction, handwriting, paternity issues, ballistics, chemical analysis, autopsy, disputed document analysis, Brain Electrical Activation Profile, Narco, Polygraph, Sound Spectograph/Voice Print Studies, Signature verification, Cyber Forensics etc. All these are being used to prove crimes and prosecuting the accused.

Looking Forward

Cyber forensic techniques are used in the detection, investigation and trial of traditional offences. Accordingly, the law is in the process of adaptation to the new changes in techniques and tools. And to widen its ambit for extension to other categories of crime, C-DAC and some other agencies like CFSL Chandigarh, CFSL Hyderabad, SFSL Shimla, etc. are on the job but the scope of the uncovered areas is so vast and the demands are so urgent that many more research efforts are needed to be made.

The amount of success in computer forensics will require approval and acceptance of the law enforcement and interpretation agencies i.e. the police, advocates, doctors and judges. Therefore, the research in cyber forensics is possible only under the guidance of both computer and law experts.

LITERATURE REVIEW

According the author of [30], Cyber forensic evidence collected in one country is not admissible in foreign courts. Government policies and cyber laws from different regions should make efforts to resolve conflicts and issues arising due to multi-jurisdiction investigations. There is a requirement for training of investigation agencies and judicial members. There exists a need to develop investigation procedures like Cyber Forensic Examinations to collect digital evidence and to amend Indian Cyber laws to match up the speed of technological progress.

As per the data of National Crime Record Bureau, given by the author of [46], during past 5 years, the registered cases under IT Act are 3682 and the conviction rate is 7% i.e. the registered cases are increasing and the conviction rate is declining. The increase in reported cases is 8 times. According to Advocate Pawan Duggal, a cyber-crime expert and senior advocate of Supreme Court, most of the time electronic evidence is neither captured in the right way nor is it retained and preserved in the manner required to be useful in law.

As per the data released by National Crimes Records Bureau of India, in 2014, mentioned by the author of [5], the reported cases were 7201 and convictions were just 65 and in 2015 reported cases were 8045, arrested 5102 and convicted 250. According to the NCRB data, a total of 11,789 cases are pending during investigation stage. 60.1% of the cybercrime cases with the police are pending, while the courts have an even higher pendency rate of 90.3%. The courts are reported to have 6,435 pending trials. The high rate of pending cases leads to the very low rate of convictions because of evidence getting lost during the time lapse. The problem of lacked cooperation exists while conducting investigations in both intra-country and inter-country crimes.

As per the NCRB report of 2015-16, the cybercrimes in India are continuously increasing, but because of ineffective investigation, the percentage of solved cases is low. The author in [24] claims the lack of sophisticated tools as the main responsible cause. Gap between the knowledge of criminals and investigating agencies leads to high acquittal rate. Criminals use more specialized tools for committing crime than can be tracked by police. The proper storage of evidences is required. There is the non-availability of sophisticated tools or software required for collection of information from volatile memory.

The author of [33] claims that the Investigating Officers are required to be properly trained regarding the technology. Suitable systems should be developed for the collection and preservation of evidence and making proper use of such evidence in conviction. He advises making necessary amendments of laws for giving recognition to such evidence.

Narcoanalysis as a test and its affects on violation of Right to Life and Personal Liberty given under Article 21 of the Constitution are mentioned in [2]. The authenticity of Narcoanalysis is required in criminal convictions. Narcoanalysis tests undermine the right against self-incrimination and have the potential to adversely affect the fairness of a trial. The legal system should imbibe developments and advances that take place in science as long as they do not violate fundamental legal principles and are for the good of the society.

The author in paper [11] examines criminal justice responses to cyber-crime under the common law model. The Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013) has been done and it focuses on core issues of concern. The paper discusses various barriers to cybercrime investigations, prosecutions and digital forensic interrogations like ineffectiveness in tracing criminal activity when data anonymization and obfuscation techniques have been employed. Availability of data sanitization and device wiping software for consumer devices may lead to destruction of evidence. There exists inability to obtain authorization for conducting online inspection and collection of remotely stored data particularly if the base station is outside the jurisdiction of the local authorities and inability to acquire data due to advancements in consumer security on commodity devices like strong encryption, open source privacy tools and anti-forensic technologies. Emerging data protection and privacy laws worldwide are putting electronic information beyond the reach of investigating authorities.

In [47] the author underscores the legal issue to define the privacy policies for computer forensics for making investigation process more lawful in terms of privacy preservation. Current policies and processes are inadequate. A number of policies that cover all computer forensic investigation steps viz. imaging, analysis and presentation should be used.

In [17], four Digital Forensic tools have been discussed i.e. iSafe, USBDeview, Recuva and WinHex. To avoid being a victim of Cyber-crimes, the use of different Digital Forensic tools should be adapted to minimize system vulnerability.

According to author in [38], there are no formal standards, procedures nor models for digital forensics to which courts can refer. The existing models focus on one aspect of process. It should describe the entire lifecycle of a digital forensic investigation.

In [18], the expansion in the number of cybercriminal actors and opportunities to engage in highly profitable illegal activities is the main cause which has given rise to the development of new cybercrime tools in areas such as ATM fraud and mobile malware. A large part of the problem relates to poor digital security standards and practice by businesses and individuals.

RESEARCHABLE AREA

From the above scanning of literature, it surfaces that the available tools and techniques of cyber forensics are not put to use in investigation of crimes for the reason of inadequate knowledge of agencies involved in investigation and other areas of criminal administration of justice. For the reason of non-recognition of some techniques in law are also responsible for this gap. The result is unscientific investigation and by untrained people leading to poor achievement of convictions and sentences to the criminals.

The knowledge of criminals is more sound and updated than those involved in preventing them from committing crimes by inflicting punishments. Therefore, Indian techniques, tools and standards are required to match with those of the developed world. Cybercrimes need no boundaries of the nations and ask for common standards and cooperation between nations.

As far as the use of forensic tools in the investigation of crimes in general and the cybercrimes in particular on the touch stone of their efficiency is concerned, there is hopefully no research work available.

The focus should be on identifying the use of forensic tools in crimes in general and cybercrimes in particular. The international practices in this field should be analyzed so as to learn lessons for improving the Indian investigation system.

There is a strong need to understand the applicability of computer forensic tools to detection, investigation and trial of crimes covered under the Indian Penal Code, 1860 and Information Technology Act 2000. It should also be in conformity with methodology of investigation prescribed under the Code of Criminal Procedure, 1973 and the evidence rules under the Indian Evidence Act, 1872. The following are:

- Analysis of tools used in cybercrime investigation in terms of their potency.
- Analysis of legal protection for such tools and the samples collected thereby (IT Act, CrPC and Evidence Act)
- Studying the working of agencies involved in developing the tools for cybercrime investigation like CDAC, the Forensic labs actually doing the testing part like CFSL, SFSL, Police Academy and IT Police Centre etc.
- Use of Forensics by the courts for conviction to be analyzed.
- Comparative study of Indian positions with that of USA and UK to be made.

CURRENT AND FUTURE NEEDS

Criminals are extensively using technology to commit both traditional crimes and cybercrimes. Cyber-terrorism has become a global menace. Similarly, the economic offences committed through the use of computers, internet, mobiles and other computer devices are on the increase. Cybercrime has international dimensions and is the most serious form of crime related to the drugs and cyber terrorism, etc. If we have a look at the rate of cybercrimes in India, we find that they have increased more than 800% during past five years whereas the conviction rate is moving on the lower side. Therefore, there is an increase both in traditional crime as well as in cybercrimes, however, the conviction rate is lower in both the cases and the obvious reason is the failure of the investigation and prosecution agencies to tender adequate evidence in court. It evidences the fact that the investigation agencies are not well versed with the use of cyber forensic tools in crime investigation. Further, there is dearth of interface between cyber forensic tool research institutions, Forensic Laboratories, Investigation agencies and prosecution agencies. Therefore, there is a need of interdisciplinary research to bridge the gap because if a satisfactory conviction rate is not achieved it may have cascading effect causing a disorder in society and a threat to our lives, liberties and property. The advancements in technology and their increasing use in our lives multiples the chances of increased crime in equal proportions, if not more.

CONCLUSION

The scenario of cyber forensics in law can be portrayed as under:

- Cyber forensic tools have a large scope in crime investigation and achieving better conviction rates.
- Electronic/digital evidence collected using cyber forensic tools is useful in trial of offences and is admissible as evidence under the present law.
- Law is slow to react to technological advancements and the present law needs to be synchronized and updated with the technological advancements in the field of cyber forensics to ensure that the criminals are brought to book.
- Law enforcement agencies lack adequate training in collection and use of evidence using cyber forensics.

Thus, there is a need for the following:

- To understand the use of cyber forensics in administration of justice.
- To examine tools used in crime investigation and studying their efficiency levels.
- To propose new system (not already recognized) used in crime investigation.
- To scientifically experimenting with the system proposed for testing its efficiency.

As such, there is a need to analyze the existing legal regime relating to use and admissibility of cyber forensics in crime investigation and trial. For the purpose, various tools and techniques used for disc and device forensics should be analyzed. These tools and techniques can be made more useful in criminal investigation and trial. The analysis of the provisions of law where under these Cyber Forensic tools can be used by the investigation agencies and the courts in law enforcement should also be done. The present relation of cyber forensics and law is of new friends, which needs to be furthered and achieved to the level of a wedded couple.

REFERENCES

1. ‘Crime in India 2014 Compendium’, National Crime Records Bureau, Ministry of Home Affairs
2. ‘New Tools of Criminal Investigation’ Law Teacher Journal
3. Ahmad, Farooq, Cyber Law in India (Law on Internet), Pioneer Books
4. André Årnes, ‘ Cybercrime Law’, Published Online: 23 MAY 2017, DOI: 10.1002/9781119262442.ch3, Available at: http://onlinelibrary.wiley.com/doi/10.1002/9781119262442.ch3/
5. Asheeta Ragidi, ‘With Only 250 convictions, India’s cybercrime conviction rate remains abysmally low’, Nov. 22, 2016, http://www.firstpost.com/tech/news-analysis/with-only-250-convictions-indias-cybercrime-conviction-rate-remains-abysmally-low-3692665.html
6. Ashok KM, ‘What NCRB statistics says about Criminal Justice system in India?’ NOVEMBER 13, 2015 ,http://www.livelaw.in/what-ncrb-statistics-says-about-criminal-justice-system-in-india/
7. Barbara Guttman; James R. Lyle; Richard Ayers, Ten Years of Computer Forensic Tool Testing, 8 Digital Evidence & Elec. Signature L. Rev. 139, 147 (2011)
8. Bill Laberis, ’20 Eye-Opening Cybrecrime Statistics’, Security Intelligence, IBM, CISCO, November 2016.
9. Caloyannides, Michael A., (2001), Computer Forensics and Privacy, Artech House (www.artechhouse.com).
10. Caloyannides, Michael A., (2nd Ed. 2004), Privacy Protection and Computer Forensics, Artech House
11. Cameron S. D. Brown1, ‘Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice Cameron S. D. Brown1 Australian National University, Australia’, International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015
12. Casey, Eoghan (3rd Ed.), Digital Evidence(Forensic Science, Computers & the Internet Computer Crime), Academic Press
13. Casey, Eoghan (Ed. 2001), Handbook of Computer Crime Investigation: Forensic Tools and Technology, Academic Press.
14. Chethan Kumari TNN, ‘One Cybercrime in India every 10 minutes’, The Times of India, July 22, 2017
15. Cyber Hunt for Evidence: Tales from the Trenches
Hennepin Lawyer, Vol. 80, Issue 3 (March 2011), pp. 8-9
Schaub,BrookT.80 Hennepin Law. 8 (2011)
16. Daniel B. Garrie, Digital Forensic Evidence in the Courtroom: Understanding Content and Quality, 12 Nw. J. Tech. & Intell. Prop. [i], 128 (2014)
17. Dhwaniket Ramesh Kamble , Nilakshi Jain , Swati Deshpande, ‘Cybercrimes Solutions using Digital Forensic Tools’, I.J. Wireless and Microwave Technologies, 2015, 6, 11-18 Published Online November 2015 in MECS(http://www.mecs-press.net) DOI: 10.5815/ijwmt.2015.06.02
18. Europol News Item, ‘The Relentless Growth of Cybercrime’, 27 September, 2016
19. Farmer, D., & Venema, W. (2000), Forensic Computer Analysis: an Introduction.
20. Halboob, Mahmod, Udzir, Abdullah, ‘Privacy Levels for Computer Forensics: Towards a More Efficient Privacy-preserving Investigation’, International Workshop on Cyber Security and Digital Investigation, Procedia Computer Science, Elsevier 2015.
21. Halil Ibrahim Bulbul, Yavuzcan, Mesut Ozel, ‘Digital Forensics: An Analytical Crime Scene Procedure Model’, Forensic Science International, Elsevier, 2013.
22. Justice Singh, Yatindra (2nd Ed.), Cyber Laws, Universal Law Publishing Co. Pvt. Ltd.
23. Kamath, Nandan, (2nd Ed.), Law Relating to Computers,Internet and E-Commerce, Universal Law Publishing Co. Pvt. Ltd.
24. Kiran Kumar Akate Patil, ‘Hurdles in Cyber Forensic Investigation in India’, IOSR Journal of Computer Engineering
25. M. Al. Fahdi, Clarke, Furnell, ‘A suspect-oriented intelligent and automated computer forensic analysis’, Digital Investigation, Elsevier, 2016.
26. M.M. Kohn, M.M. Eloff, J.H.P Eloff, ‘Integrated Digital Forensic Process Model’, Computers and Security, Elsevier 2013.
27. Maneela, ‘Cyber Crimes: The Indian Legal Scenario’, 11 US-China L. Rev. 570, 586 (2014)
28. NIIT (2005), Understanding Forensics in IT, Prentice Hall of India Private Limited, New Delhi-110001
29. NIIT (Ed. 2004), Hacking Tools and Techniques & Incident Handling, PHI Pvt. Ltd.
30. Nishesh Sharma, ‘Cyber Forensics in India – A Legal perspective’, Universal Law Publishing
31. Paul Curran, ‘Cyber Terrorism – How Real is the Threat?’ Checkmarx, May 2016.
32. Paul H. Luehr, Real Evidence, Virtual Crimes - The Role of Computer Forensic Experts, 20 Crim. Just. 14, 25 (2005)
33. Peter D. Keisler Attorney General, ‘Investigative Uses of Technology: Devices, Tools and Techniques’, US Dept. of Justice, Office of Justice Programs, Washington D.C.
34. Rakesh Dubbudu, ‘Conviction Rate of Sec 498-A cases is among the lowest of all IPC Crimes’, Report ‘Crime in India’, National Crime Records Bureau, July 2017

35. Raymond Lutui, 'A Multidisciplinary digital Forensic Investigation Process Model', Elsevier, Available online at:www.sciencedirect.com
36. Reckless, Walter C., Crime Problem in India
37. Reed, Chris & Angel, John (4th Ed.), Computer Law, Universal Law Publishing Co. Pvt. Ltd.
38. Reza Montasari, Pekka Peltola, David Evans, 'Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations', Available at: https://link.springer.com/chapter/10.1007/978-3-319-23276-8_8
39. Ricci S.C. Leong, 'FORZA – Digital Forensics Investigation Framework that Incorporate Legal Issues', Digital Investigation, Elsevier 2006
40. Robbins, Judd, (2001), An Explanation of Computer Forensics, National Forensics Center.
41. Shahzad Saleem, Oliver Popov, Ibrahim, 'Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles', Procedia Computer Science, Elsevier, 2014
42. Sommer, Peter (2001), Computer Forensics: An Introduction, Virtual City Associates, London, United Kingdom (http// csrc.lse.ac.uk)
43. Sood, Vivek (Ed. 2002), Cyber Law Simplified, Tata Mc Graw Hill Publishing Company Ltd., New Delhi
44. Sutherland, Criminology
45. Vacca, John R.,(2002), Computer Forensics – Computer Crime Scene Investigation, Firewall Media (An imprint of Laxmi Publications Pvt. Ltd.), Daryaganj, New Delhi-110002.
46. Vicky Nanjappa, 'Cyber Crime – 1600 arrested, only 7 convicted', Rediff Business News, http://www.rediff.com/money/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm
47. Waleed Halboob, Ramlan Mahmod Nur IzuraUdzirMohd TaufikAbdullah, 'Privacy policies for Computer Forenics', Computer Fraud & Security, Computer Fraud and Security, Elsevier, Vol. 2015, Issue 8, August 2015, Pages 9-13