International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 18-04-2021, Accepted: 07-05-2021, Published: 27-05-2021
Volume 7, Issue 3, 2021, Page No. 97-101

Cyber forensic: Emerging I.T. trends

Tapan Kumar Chandola
Associate Professor, ALSL, Amity University, Lucknow, Uttar Pradesh, India

Abstract
Cyber forensic is the collection and documentation of the proves by using tools and techniques of information technology and analysis of digital evidence from electronic devices in such a manner that it can be presentable before court of law. The aim of cyber forensic is to investigate that what, where, when and how the crime had happened. The cyber forensic expert collect and store the electronic evidence from computer of electronic device and analyse the evidence. After analysing the electronic evidence the expert produce his report in the court of law so that the with the help of forensic report the judiciary can deliver a fair judgement.
The concept of digital evidences, digital signatures, encryption etc., was first introduced in India through Information and Technology Act, 2000 but the forensic tools and investigating authorities in India are not as upgraded and trained as the cyber-crimes are increasing, upgrading and flourishing. To arrest the accused and prevent the cyber-crimes, cyber forensic experts, investigating authorities need to be trained and forensic tools need to be upgraded.
This paper describes the laws and provisions relating to electronic evidence, cyber forensics nationally and internationally and its contribution in investigating the matters related to cyber-crimes by the officials. This paper explains the lacunas in present forensic tools, which are not upgraded frequently in accordance with technology by the government. The aim of this paper is to develop the cyber forensics and methods of investigation of digital evidences to provide a crime free world in digital space.

Keywords: cyber forensic, electronic evidence, cybercrimes, forensic investigations

Introduction
With the starting of the association of human beings and the construction of social societies the crimes came into existence. Earlier the crimes, committed in the societies were considered as civil wrongs but with the development the nature of the crimes started changing. Now the offenders started committing crimes of criminal nature which causes not only mental and physical damages but also financial damages to the human beings. Now, in this information technology world the face of committing crimes is totally changed. Nowadays crimes mainly with the intension to earn illegal money are spreading like anything in all over the world including India as this is very easy to make people fool online and steal their hard-earned money easily by using different I.T. tools and technology. Different crimes which were committed by offenders in digital world are hacking, spamming, online frauds, credit/debit card frauds, internet banking frauds, privacy invasion etc. and the motive to commit all these crimes are basically illegal financial gains. We all know that cyber world is borderless so its very easy for the offender to commit cybercrimes from any remote location without the fear to be recognised or arrested.

Cyber Forensic
Digital forensics and cyber forensics are the vast areas in which hacking, bank fraud and email spamming are investigated. With the proliferation of computers in our daily lives, it has become inevitable that computer content or traces must be included as part of formal evidence. In the form of laptops, desktop computers, servers, etc., computerized devices are part of our world, but there are many other storage devices that can contain forensic evidence. [1] Devices such as memory cards, personal digital assistants and video gaming systems are among many devices that can accept input, output and store data. The center of cyber forensics is this data or the use of these devices. Cyber forensics is the practice of legally acceptable collection, analysis and reporting of digital data. It can be used in crime detection and prevention and in any dispute in which evidence is stored digitally. Specialized techniques for the recovery, authentication and analysis of electronic data are used in cases involving problems related to the reconstruction of computer use, the examination of residual data and the authentication of data by means of technical analysis or explanation of technical characteristics of data and computer use. Cyber forensics requires specialized expertise that goes beyond the normal techniques of data collection and preservation available to end users or system support staff. Cyber forensics comprises the application of the law to computer science, similar to all forms of forensics. Cyber forensics deals with cyberspace evidence preservation, identification, extraction and documentation. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures to ensure the accuracy of evidence preservation and accuracy of data processing results. [2] Digital forensics, as explained "is a discipline that combines elements of law and computer science in order to collect and analyze data from computer systems, networks, and wireless communications and storage devices in a manner that is admissible as evidence in court." The word forensics refers to the use of digital forensics in law / courts as a process that is ultimately carried out to obtain evidence that can be used in a court of law. As simply stated, the objective of digital forensics is "to identify digital evidence for an

investigation." It cannot be overemphasized that digital forensics has a legal connotation. For centuries, forensic science has been used in other brotherhoods, but digital forensics still faces a number of challenges in its developmental stages. A digital forensics investigator must ensure that all aspects of the process are in accordance with the law or that the resulting evidence can face major challenges in court. [3] Digital forensics and cyber forensics are the vast areas in which hacking, bank fraud and email spamming are investigated. With the proliferation of computers in our daily lives, it has become inevitable that computer content or traces must be included as part of formal evidence. In the form of laptops, desktop computers, servers, etc., computerized devices are part of our world, but there are many other storage devices that can contain forensic evidence. [1] Devices such as memory cards, personal digital assistants and video gaming systems are among many devices that can accept input, output and store data. The center of cyber forensics is this data or the use of these devices. Cyber forensics is the practice of legally acceptable collection, analysis and reporting of digital data. It can be used in crime detection and prevention and in any dispute in which evidence is stored digitally. Specialized techniques for the recovery, authentication and analysis of electronic data are used in cases involving problems related to the reconstruction of computer use, the examination of residual data and the authentication of data by means of technical analysis or explanation of technical characteristics of data and computer use. Cyber forensics requires specialized expertise that goes beyond the normal techniques of data collection and preservation available to end users or system support staff. Cyber forensics comprises the application of the law to computer science, similar to all forms of forensics. Cyber forensics deals with cyberspace evidence preservation, identification, extraction and documentation. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures to ensure the accuracy of evidence preservation and accuracy of data processing results. [2] Digital forensics, as explained "is a discipline that combines elements of law and computer science in order to collect and analyze data from computer systems, networks, and wireless communications and storage devices in a manner that is admissible as evidence in court." The word forensics refers to the use of digital forensics in law / courts as a process that is ultimately carried out to obtain evidence that can be used in a court of law. As simply stated, the objective of digital forensics is "to identify digital evidence for an investigation." It cannot be overemphasized that digital forensics has a legal connotation. For centuries, forensic science has been used in other brotherhoods, but digital forensics still faces a number of challenges in its developmental stages. A digital forensics investigator must ensure that all aspects of the process are in accordance with the law or that the resulting evidence can face major challenges in court.[3] Digital forensics and cyber forensics are the vast areas in which hacking, bank fraud and email spamming are investigated. With the proliferation of computers in our daily lives, it has become inevitable that computer content or traces must be included as part of formal evidence. In the form of laptops, desktop computers, servers, etc., computerized devices are part of our world, but there are many other storage devices that can contain forensic evidence. [1] Devices such as memory cards, personal digital assistants and video gaming systems are among many devices that can accept input, output and store data. The center of cyber forensics is this data or the use of these devices. Cyber forensics is the practice of legally acceptable collection, analysis and reporting of digital data. It can be used in crime detection and prevention and in any dispute in which evidence is stored digitally. Specialized techniques for the recovery, authentication and analysis of electronic data are used in cases involving problems related to the reconstruction of computer use, the examination of residual data and the authentication of data by means of technical analysis or explanation of technical characteristics of data and computer use. Cyber forensics requires specialized expertise that goes beyond the normal techniques of data collection and preservation available to end users or system support staff. Cyber forensics comprises the application of the law to computer science, similar to all forms of forensics. Cyber forensics deals with cyberspace evidence preservation, identification, extraction and documentation. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures to ensure the accuracy of evidence preservation and accuracy of data processing results. [2] Digital forensics, as explained "is a discipline that combines elements of law and computer science in order to collect and analyze data from computer systems, networks, and wireless communications and storage devices in a manner that is admissible as evidence in court." The word forensics refers to the use of digital forensics in law / courts as a process that is ultimately carried out to obtain evidence that can be used in a court of law. As simply stated, the objective of digital forensics is "to identify digital evidence for an investigation." It cannot be overemphasized that digital forensics has a legal connotation. For centuries, forensic science has been used in other brotherhoods, but digital forensics still faces a number of challenges in its developmental stages. A digital forensics investigator must ensure that all aspects of the process are in accordance with the law or that the resulting evidence can face major challenges in court.[3] Cyber forensic is the collection and documentation of the proves by using tools and techniques of information technology and analysis of digital evidence from electronic devices in such a manner that it can be presentable before court of law. The aim of cyber forensic is to investigate that what, where, when and how the crime had happened. In other words, cyber forensic is the investigation process to search the method of crime and criminal. With the increasing interference of digitalization in our day-to-day life, the electronic evidence has become the part of evidence as digital evidence or electronic evidence. The work of cyber forensic is to collect the digital evidence, store them carefully as the digital evidences are fragile in nature, analysis of digital evidence and then present the report in the court of law so that the justice can be pronounced fairly by the court of law. These all procedures are completed by the cyber forensic expert who is specifically trained to handle digital evidence. Digital evidences are the set of information in digital world which are admissible in the court of law according to laws and provisions of the land. These evidences can be found in the computers and other electronic devices in the form of binary. DVD, floppies, deleted data or messages, emails, CDs and encrypted documents etc. are some example of electronic or digital evidence.

Evolution of the New Technology: Cyber Forensic

In 1980, the cyber forensic was came into existence when the personal computers were introduced. In1984, the FDI Programme was introduced and the "Computer Analysis & Response Team" (CERT) was formed to support the field officers of FDI to search and seizure of electronic/ computer evidences [1]. In 1989, the "International Association of Computer Investigative Specialists" (IACIS) [2] created a "Federal Law Enforcement Training Centre" (FLETC) to make the students literate to bring out the evidences from computers and other electronic devices that had been used by the offenders while committing the crime. This is why, a need to establish an organization was felt by the law makers so that it could synchronize the laws and norms of cyber forensic in all over the world. In 1993, the first international conference was organized by FBI on computer evidence. After two years in 1995, the "International Organization on Computer Evidence" (IOCE) [3] had been created to interchange information for the investigation technologies for cybercrimes and other issues for 'Computer Forensic' worldwide. The aim of the Conference was to improve the "Compatible Forensic Standards" of computer forensic.

Now there was a need to harmonize the methods to recover; preserve and analyse the digital evidences apart from the boundaries of one state to ensure that the digitally collected evidence could be accepted in other states too for the successful prosecution of the offenders worldwide. These motives were fulfilled in 1998 by the "Federal Crime Laboratory Directors" [4] by developing the "Scientific Working Group on Digital Evidence" (SWGDE).

In 2000, the first FBI "Regional Computer Forensic Laboratory" (RCFL) was established to evaluate the digital evidence for the investigation in the matters of different cyber-crimes including finance i.e. hacking, identity theft, computer viruses, pornography, investment fraud, phishing/spoofing, credit card fraud, online auction fraud, e-mail bombing and spamming, property crime etc [5].

In 2004, the international conference i.e. "International Conference on E-Security, Cyber Crime and Law" [6] was held in Chandigarh in India. This International conference was about the issues related to computer forensics that how to store and preserve the computer evidence and which methods should be used by the cyber forensic experts to make the evidence relevant, authentic and presentable before the court.

In 2006, there was a conference was held in Brazil namely "International Cyber Crime Conference". The subjects of discussion of the conference were cybercrimes; cyber security of data subject and cybercrimes in International context including International collaboration regarding investigation of electronic evidence and extradition of criminals.

In 2008, an "International Conference on Terrorism and Organized Crimes" [7] was conducted in U.S.A. So many problems were discussed in this conference on spreading terrorism internationally and on the increasing cybercrimes. The main issue of the discussion was cyber forensic and the method to investigate the cyber offences and also the need to recruit the computer forensic experts to process of cyber forensics.

In 2009, "The International Conference on Digital Forensics and Cyber Crime" was held in New York, U.S. and the main point of the discussion in conference was to establish a reminiscent and synchronized pattern of cyber forensic worldwide to control the increasing cybercrimes [8].

Procedure of Cyber Forensic

The procedure of the cyber forensic is to evaluate the electronic evidence collected from electronic devices. The work of the cyber forensic experts is to collect the digital evidence from electronic devices which should be relevant and scientifically approved so that to make the electronic evidence legally admissible. It was observed by the Apex Court in the case of "Tukaram S. Dighole v. Manikrao Shivaji Kokate" [9], that the new technologies are the demand of the day. Electronic or digital evidence can be transformed or changed easily this is why the rules and laws related to relevancy and authenticity of these electronic evidences should be stricter and standardized than other normal documentary evidences. The four steps are being used to process cyber forensic i.e. to store and collect electronic evidence, analysis of this evidence and then make it relevant, accurate and admissible in the judiciary. These four steps are mentioned as hereunder:-

- **Identification of an Electronic Evidence:** This is the first step to investigate the crimes related to cybercrime. The main questions arise before the expert that how a cybercrime has been committed, which electronic tool has been used, which electronic evidence can be used to prove a cybercrime and how the evidence has been stored what is the process to recover it? It is all depends on the knowledge of forensic expert.

- **Preservation of Electronic Evidence:** The second most important step of cyber forensic is to preserve the collected electronic evidence in the manner that the originality and authenticity of the evidence is not affected because the electronic evidence is fragile in nature and can be destroyed with a little negligence. Sometimes it happens that the electronic evidence cannot be preserved in the manner in which it is, then the preservation of the electronic evidence depends upon the skills of the expert that he preserves the evidence in the manner that it does not lose its authenticity and nature.

- **Analysis of Electronic Evidence:** After preserving the electronic evidence, the next important step of cyber forensic is the analysis of the electronic evidence by the cyber forensic expert so that the electronic evidence can be read by common people and presented in the court of law.

- **Presentation of Electronic Evidence:** The last step of cyber forensic is to make the electronic evidence presentable in the manner that it can be admissible in the court of law.

Cyber Forensic: Indian Prospective

The development of information technology such as electronic trade, privacy issues, electronic communication, and storage of personal information of data subject in electronic devices need stronger and uniform laws to protect all the personal information of data subject including trade and finance related information so that the cyber forensic techniques can be admissible not only in India but also in all over world. To flourish the e-trade internationally and to synchronize the laws related to cyber world, the United Nations General Assembly established the "United Nations

Commission on International Trade Laws" (UNICITRAL) [10] in 1966. Being a member of the charter, India also enacted I T Act, 2000. The motive to enact IT Act, 2000 was to flourish the e-trade as per the guidelines of UNICITRAL Model Law, protect the people from different cybercrimes and penalize the criminals to deter the cybercrimes.

While observing the increasing cybercrimes, an amendment has been done in I.T. Act, 2000, to make the laws more effective and for the admissibility of electronic evidences by inserting some special provisions in the original Act. Along with the amendment in IT Act, 2000, the other amendments have been made in the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891.

Amendments in Evidence Act: A Step Ahead to Make Cyber Forensic Stronger

The Evidence Act in India has been enacted years ago and many amendments have been made in Indian Evidence Act, 1872 time to time. In similar manner, the amendment has been made in 2008 for the admissibility of electronic evidence.

Section 3 (a) of the Evidence Act has been amended by the amendments of IT Act, 2008 and the inserted provision includes all the documents along with 'Electronic Records' for the examination by the court of law. The term "Electronic Records" is same in the mentioned in the same manner in Evidence Act as it is defined in I.T. Act, 2000, *"data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche"*.

Section 17 of the Evidence Act, 1872 has been amended and it includes the provisions related to the statements in oral, statements in documents and statements in electronic form.

Section 22A has been inserted in Evidence Act, 1872 by the amendment. It says that-"*Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.* [11]"

Indian Judicial Perspective

Cyber forensic reports are based on the analysis of the electronic evidence which is made readable and understandable in the manner that a common man can understand the crux of the conclusion. Earlier there was no provision for the admissibility of electronic evidences in India. But after the amendment in 2008 some provisions were inserted in the main Act. Alongwith the amendments the Indian judiciary also has interpreted the laws related to the admissibility of electronic evidence in India time to time. Section 65A and section 65B of the Evidence Act, 1872, describe about the admissibility of electronic evidence in the court of law. Section 65A mentioned the provisions about the relevancy of electronic records while section 65B tells about the admissibility of electronic evidence in courts.

Section 65B of the Evidence Act, 1872 has described some conditions in which it has been mentioned that the when the electronic evidence is admissible in the court without the production of original one. Although section 65B is confusing in language but in simple words it says that any evidence which is collected through computer or any other electronic device in the form of hard copy will be considered as a document. This document will be considered as an evidence in the court alongwith the certificate or if it fulfils the other mentioned conditions of section 65B. Section 65B (4) deals with the provision that it is compulsory to file certificate of authenticity before court in the support of every electronic evidence.

The Supreme Court held in the case of Parliament Attack [12] that it is on the discretion of the court that if it thinks fit that any electronic document could be admitted without the certification or authentication. The aforesaid case was related to the acceptance of telephone calls records as electronic evidence. In this case the accused stated that the prosecution did not produce the certificate of authentication before the court so that the relevancy of the telephone call records is in question and not fulfilling the provisions mentioned under section 65B(4) of Evidence Act and the record should not be admitted by the court of law. The Apex Court concluded that after considering the statement of competent witness, the call records were sufficient to admit it as electronic records.

In another case of Ratan Tata **[13]** the Supreme Court accepted the electronic evidence without following the provisions described under section 65(B) of Indian Evidence Act.

These judgements of the Supreme Court of India established that the admissibility of electronic evidence depends upon the discretion of the courts. The courts could adopt special procedure to admit the electronic evidence while ignoring the provisions mentioned under section 65B of Evidence Act.

The decision of Navjot Sandhu case [14] was overruled after nine years in the case of "Anvar P. K. vs. P.K Basheer & Ors." [15] In this case the provisions related to admissibility of electronic evidences in the courts were redefined and the sections 63, 65 and 65B of Indian Evidence Act were reinterpreted. In this case, Mr. Anvar filed an appeal after losing the Assembly election in Kerala and stated that Mr. P. K. Basheer, Member of Legislative Assembly vanished his fame by defamatory material recorded in CDs and songs. The Supreme Court had denied to accept produced electronic evidence without the certificate of authentication. It was held by the Apex Court that in the case of accepting any electronic evidence, the provisions of section 65B should be followed rigorously. The acceptance of electronic evidences as record is not accepted by the court without it.

Hon'ble Supreme Court observed that any alteration or tempering of the electronic evidence or records can be easily made. It is observed by the Kurian J. in his judgement,

"Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice". [16]

In the result, this progressive approach of Indian judiciary encouraged the compliance of the aforesaid provisions of Evidence Act related to the admissibility for electronic evidence. In the judgement of "Shafhi Mohammad Vs. The State Of Himachal Pradesh" [17], Supreme Court has interpreted and justified the provisions of admissibility of secondary or electronic evidence in the court of law under section 65(B) of the Indian Evidence act and the provisions of section 54A which describes the identification process through videography along with the provisions of section 164 Cr.P.C. which mention the confession through audio-video recording.

The Hon'ble Supreme Court also described the cases "Ram

Singh And Others vs. Col. Ram Singh" [18] and the judgements of English-law such as "R. vs. Maqsud Ali" [19] and "R vs. Robson" [20] and from American Law [21] that "*it will be wrong to deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved.*" [22]

Cyber Forensic: Investigating Process of Cyber Crimes in India

In India, the Information Technology Act, 2000 describes different types of cybercrimes, punishments and penalties. The Act also describes the process of investigation of cybercrimes by the police authority. But unfortunately I.T. Act, 2000 is not sufficient to investigate the matters of cybercrimes. Therefore, the provisions of traditional laws are also being followed in India while investigate the matters of cybercrimes. Section 78 of I.T. Act, 2000 describes the "Powers to Investigate Offences". It empowers the police officer not below the rank of inspector to investigate cyber offences. It says that,"*Notwithstanding anything contained in the Criminal Procedure Code,1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.*" [23] The provisions to investigate and search in I.T. Act are quite similar to the provisions of the traditional laws. Even the crimes which are committed online by using internet and computer or other electronic devices and are not mentioned or described in I.T. Act, 2000, they are investigated by implementing the provisions of traditional criminal laws i.e. Cr.P.C or IPC. Thus, the traditional criminal laws are exercisable accordingly upon cyber matters. The investigation of cyber offences is not easy, and it requires expertise in cyber forensic. Thus, it is required to adopt the new techniques by the investigating agencies or cyber forensic experts in place of traditional method of investigation.

Conclusion

Although there is a developed and amended cyber law in India but after considering the above mentioned circumstances it must be said that there are some lacunas in the existing cyber laws and the provisions of investigation of cybercrimes. Cyber forensic investigating officers are not as trained as they should be. Proper investigating tools are not available in cyber forensic labs. Proper staff in cyber forensic labs are missing. Lack of synchronization between the investigating officers of different states in India. Jurisdictional issues are also a big problem in the matters of cybercrimes. The I.T. laws are not appropriated and the provisions for cyber forensic are not sufficient and strong therefore the investigating process is so lengthy and time taking in India. In this regard the efforts of Indian judiciary are praiseworthy. The strictness of Indian courts to follow the provisions for the admissibility of electronic evidence in India not only has saved the time of courts but also has given a clarity in the minds of lawyers and lawmakers. In the case of "Punjab v. Amritsar Beverages Ltd." the Supreme Court held that there are so many problems which are being faced by investigating officers due to lack of scientific expertise, proper tools and the knowledge of cyber forensic techniques [24].

References

1. Federal Bureau of Investigation, https://www2.fbi.gov/hq/lab/org/cart.htm, retrieved on 19.02.2021.
2. https://www.iacis.com/about-2/
3. http://www.ioce.org/
4. https://www.ncjrs.gov/App/publications/Abstract.aspx?id=240555.
5. https://www.rcfl.gov/
6. International legal response to cyber terrorism, Chapter V, 287, http://shodhganga.inflibnet.ac.in/bitstream/10603/75367/12/12_chapter%205.pdf.
7. http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/17/17_chapter%208.pdf, p.400, last seen on 22.02.2021.
8. John R. Vacca, Computer Forensics, 2006, p. 14; See also C. Nicoll, Digital Anatomy and the Law: Tensions and Dimensions, 2003, p. 200.
9. (2010) 4 SCC 329.
10. http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html.
11. Section 22A of Indian Evidence Act, 1872.
12. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
13. Ratan Tata v. Union of India, Writ Petition (Civil) 398 of 2010 before Supreme Court of India.
14. Ibid.
15. (2014) 10 SCC 473.
16. Stephen Mason, ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012), 4.26; see also chapter 10.
17. SLP (Crl.)No.2302 of 2017, https://supremecourtofindia.nic.in/supremecourt/2017/6212/6212_2017_Judgement_30-Jan-2018.pdf
18. 1985 (Supp) SCC 611
19. (1965)2 All ER 464
20. (1972) 2 ALL ER 699
21. American Jurisprudence 2d (Vol 29) Page 494
22. https://www.sci.gov.in/supremecourt/2017/6212/6212_2017_Judgement_30-Jan-2018.pdf
23. Section 72 of Information Technology Act, 2000.
24. (2006) 7 SCC 607.