# AN IGNORED ASPECT: THE STATUS OF DIGITAL EVIDENCE IN INDIA

Pooja Ghosh* & Poonam Bera**

*"In cyber -crimes, India is still in infancy. ATM frauds are increasing. Effective forensic investigation at the scene of crime can bring criminals to book. The importance of the knowledge of forensic evidences specially traces of hair, fibers etc. found at the site, have to be ingrained in the Officials dealing with cyber- crimes."*[1]

Use often leads to popularity. And ultimately, popularity becomes a necessity to sustain in society. The cyber-space which is pacing in its reach to the most marginalized areas in 21st century is one of the major examples of popularity transforming into one of the most significant means of human sustenance. Humans have found ways of helping themselves with the use of the cyber-space. We use it for economic transactions, imparting social services like medical aid as well as education. We are so innovative with this particular means that we have even devised a way of committing theft through it, stalking someone on the net and even creating terror via it! This 'innovation' is rising at an alarming rate! The National Crime Records Bureau recorded a 350% leap of cyber-crimes in India in the last three years. The age- group which is apparently the workforce of India, (18-30) account for the highest percentage of these crimes!! With such increase, it is important that the issue is addressed at the earliest. And this exigency can only be met with effective use of digital evidence. It was further added by *Dr. JR Gaur that the lawyers and the police fail to adduce the digital evidence in such crimes due to lack of knowledge and expertise in this field*. The importance of digital evidence and the current issue of ineffective use of digital evidence by the cyber cells in India have been highlighted ending with suggestions to improve cyber-forensics in India. As it is not only cyber-crime which is in its infancy, it is also cyber-investigation.

## Why digital evidence?

*Following is an excerpt of importance of digital evidence in India as highlighted by Shubha Mangala Sunil, Founder Chairperson, Cyber Security Response Team*[2]*:*[3]

**** Could you give us a few examples where social media proof was used in the court of law?***

*'In many cases this year, we have seen people using digital evidence and magistrates have accepted this proof as secondary evidence…Divorce was granted in that case. In another case, when the Facebook account of a prominent celebrity was deleted immediately after her death, it was revealed that her boyfriend had deleted the account, lest her husband find out the comments they had been posting on each other's walls.'*

* Army Institute of Law, Mohali, (0)9915018094, poojaddun2011@gmail.com
** Army Institute of Law, Mohali

[1] Dr. J R Gaur, Principal Scientific Officer (Life Sciences), Bureau of Police Research and Development.
[2] http://csrt.org.in/about/about-me-extended/ <as accessed on 21.02.2014>
[3] http://www.newindianexpress.com/cities/bengaluru/article599037.ece <as accessed on 21.02.2014>

**** Do legal professionals depend a lot on digital evidence?***

*'Many a time, legal professionals rely solely on digital evidence and it does help crack cases. Further, what works in their favor if they have managed to get their hands on digital evidence is the fact that they've studied the criminal even before they have tracked them down.'*

Cyber forensics is an emerging field in India. Owing to this, the nature of investigation involved is synthesized poorly in India. Cyber forensics in simple words is application of computer science to aid the law regarding cyber-crimes and bringing the criminals to book. As forensics includes scientific application to the investigation of crimes, the analysis of evidence is the most important element of forensics. The same applies to cyber-forensics. For a successful investigation, the correct synthesis of electronic or digital evidence is significant. *Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places.*[4] Hence, for enabling efficiency in cyber-investigation digital evidence plays a significant role. To cope with the unique complexities with which cyber-crimes are increasing in India, it is important that the role of digital evidence should not be ignored and be relied upon only after credible authenticity of such evidence. It may come into play where serious crimes like extortion, fraud, child pornography or terrorism is committed by just a click of button. Not only this, but it should be kept in mind that particular crimes can only be committed online like identity theft and phishing which makes the role of digital evidence even more important. The main purpose of the computer forensics is to produce evidence in the court that can lead to the punishment of the actual. The forensic science is actually the process of utilizing the scientific knowledge for the purpose of collection, analysis, and most importantly the presentation of the evidence in the court of law. The word forensic itself means to bring to the court. Computer forensics has been efficiently used to track down the terrorists from the various parts of the world. The terrorists using the internet as the medium of communication can be tracked down and their plans can be known. For these reasons it can be said that the enforcement bodies should choose digital evidence and rely while dealing with the cases of such nature. It can make the investigation ***speedier*** and the observations of the investigation ***more accurate***. Hence, the importance of digital evidence and cyber-forensics can be encapsulated as below:

- Produces evidence in court that is professional and easy to understand.
- Saves time of both the police and the Court when they have to deal with cyber-crimes

**Scenario of Digital Evidence in India**

The main purpose of the cyber-forensics is to search, preserve and analyze information on computer systems to find potential evidence for a trial. In a way, the role of cyber-forensics is

[4] "Electronic Devices: Types, Description and Potential Evidence Electronic" in Crime Scene Investigation: A Guide for First Responders, Second Edition.

to present the evidence in such a manner that it aids the case and the court of law as much as possible.

These pieces of important evidence can be found in no. forms. Some of which are listed as follows (It may include more.): 1) Calendar, 2) Browser, 3) E-mails, 4) Databases, 5) Cookies, 6) Compressed archives including encrypted archives, 7) SMS, 8) System files, 9) IP Address of user and 10) Log files. The no. of evidence is immense, what matters, is the manner which the evidence is handled by the investigator. The nature of digital evidence is highly volatile and can be manipulated easily. Hence, cyber-forensic teams have to emphasize ***more on the preservation of the evidence.*** Every law enforcement agency has a manner in updating its system to deal with the way the evidence is to be collected and analyzed. In India, the Intelligence Bureau and the CBI are two agencies which not only are responsible for evidence handling but also suggest ways in which such handling is updated with the latest technology.

The CBI Command Centre plays an integral role in the management of the technology used to analyze the electronic evidence and coordinating all such activities of CBI branches and units in various parts of the country. A major part of the Command Centre is the Cyber Forensics and Digital Analysis Centre. This is a joint venture between CBI and CFSL. Other three branches of the Command Centre are: 1) Network Monitoring Centre, 2) Computer Centre and 3) The Strategic Communication Centre. These branches of the Command Centre coordinate in the investigations with the law. The Cyber Forensics and Digital Analysis Centre is responsible for the collection and the analysis of digital forensics. The Centre uses the following tools available for disc forensics and digital image analysis:

- ENCASE
- DIBS
- DRAC
- Password Recovery Kit
- Other Forensic Supporting Software

*The other tools which are important for investigation used in India include disk forensics, network forensics, mobile device forensics, live forensics, memory forensics, multimedia forensics and internet forensics.*[5] The Centre also provides assistance to Investigating Officers in investigation of Cybercrime cases and video/ audio identification. The facility is being used by the Scientists of CFSL for gathering/ providing the evidence in the seized discs/digital evidence. This Centre also provides technical support as well as manpower to the Investigating Officers of CBI in seizing and analyzing the discs and digital evidence.[6]

The Network Monitoring Committee monitors the internet with the help of the tools as present on their site. The Computer Committee manages the software modules used by the CBI and even generates reports every month like crime report, cases under investigation etc.

[5] http://www.cyberforensics.in/ <as accessed on 21.02.2014>
[6] http://cbi.nic.in/aboutus/manuals/Chapter_26.pdf <as accessed on 23.02.2014>

The Command Centre also coordinates with outside private IT Companies and even NIC, IIT's for developing and updating the software.

Though, internet users in India has burgeoned enormously still due to the stagnant reluctance of officials to resort to cyber-experts and lack of awareness cyber-forensic is still not in a very good state in India. Failure in promoting training schemes for the law enforcement agencies and dearth of cyber-forensic experts in the country there has been a non-uniform development of in this field.

**Legal position in India**

In India, there was ***sort of progress in digital evidence by the amendment brought by the Information Technology Act, 2000. This added Sec. 65-A[7] and Sec.65-B to the Indian Evidence Act, 1872.*** The second schedule of The Information Technology Act 2000 is India's only act dealing with computer crime, with an intension to introduce the concept of electronic evidence has added to the provisions of Indian Evidence Act, 1872 which had been drafted earlier keeping in mind only the physical world.[8] Some of the important ones are:

**Section 3(a) of the Indian Evidence Act** added to the definition of ***"Evidence",*** for the words, "all documents produced for the inspection of the Court", the **words** ***"all documents including electronic records produced for the inspection of the Court" have been substituted****;*

Electronic evidence/electronic record[9] now, is covered under documentary evidence[10] under the Indian statute. **Sec. 65-A** states that electronic record is admissible and no further proof is required for its authenticity if the provisions under Sec. 65-B is complied with.

**Sec-65-B** of the Indian Evidence Act, explains at length how electronic records can be admitted in the Court of Law.

Sec. 65-B (2) of the Act highlights the conditions which have to be satisfied**.** The bare provision has been provided as below:

***(2)*** *The conditions referred to in the Sub-section (1) in respect to the computer output shall be following, namely:*

*(a) The computer output containing the information was produced by computer during the period over which computer was used regularly to store or process information for the*

[7] ***65A. of Indian Evidence Act, 1872: Special provisions as to evidence relating to electronic record:***
*The contents of electronic records may be proved in accordance with the provisions of section 65B.*

[8] http://www.legalservicesindia.com/article/article/cyber-forensics-&-electronic-evidences-challenges-in-enforcement-&-their-admissibility-975-1.html <as accessed on 21.02.2014>

[9] The term ***'electronic record'*** as used in the above Section has been further defined by the Information Technology Act, 2000 as: ***'Data, record or data generated, image or sound stored, received or sent in an electronic film or computer generated micro-fiche.'***

[10] ***Sec. 3 of Indian Evidence Act, 1872: Documentary evidence defined as:***
*Document means any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording the matter.*

*purposes of any activities regularly carried on over that period by the person having lawful control over the use of computer.*

*(b) During the said period the information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities.*

*(c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation for that part of the period, was not such to affect the electronic record or the accuracy of its contents.*

*(d) The information contained in the electronic record reproduces or is derived from such information fed into computer in ordinary course of said activities.*

After section 22, **section 22A** of the Act has been inserted which 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**."*

Other sections that were added to the Act are ***Sections 17, 34, 35, 39, 47A, 67A and 73A which deal with proof and verification of digital signature, 81A, 88A and 90A which deal with the presumption of the evidence and 131.*** Such changes were added to the Indian Evidence Act by the IT Act to pave the way for use of digital evidence in cyber-forensics. These Amendments in a manner elaborated the procedure and the presumption to be followed by the Courts while adjudging such cases.

These amendments is just a reflection of the UNCITRAL Model Law of E-commerce which makes the law flexible when dealing with digital evidence and not exclude them just on the basis of the evidence being data or different from traditional evidence. Art. 9 of the Model Law states:

***Article 9: Admissibility and evidential weight of data messages:***

*(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:*

*(a) On **the sole ground that it is a data message**; or,*

*(b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that **it is not in its original form**.*

*(2) **Information in the form of a data message shall be given due evidential weight**. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.*

**Judiciary of India and digital evidence: An overview**

Without a uniform interpretation of the situation in the legislation, the law assumes no importance due to overlapping explanations and loopholes. The Supreme Court has always been on the forefront to give binding interpretations which are not only followed by implementing authorities but even the society. Hence, the role of Supreme Court in India is momentous. It does not let the letter of the law remain mere letters rather the Supreme Court helps reserve the spirit of that letter in reality.

In the light of its role, the Supreme Court has been active in the interpretation of the use of digital evidence in the courts. The Supreme Court for the first time analyzed the issue of physical presence of person in Court and held that adducing evidence could even be done through video conferencing. For the first time, the Supreme Court analyzed the Sec.65-A and 65-B in the case and allowed video-conferencing to be used as a medium.[11]

The breakthrough judgment given by the Apex Court was in the ***State v. Navjot Sandhu*** [12](Afzal Guru's case) where the Court held that irrespective of the compliance with the requirements of Section 65B, which is a special provision dealing with admissibility of the electronic record, there is no bar in adducing secondary evidence, under Sections 63 and 65 of the Evidence Act, of an electronic record.[13] This meant that compliance with Sec. 65-A and Sec. 65-B in the case of digital evidence (which is a copy of the original hence, secondary evidence) was not required. This judgment in some manner diverged from the set procedure in the same Act regarding digital evidence.

The Supreme Court recently overruled this judgment in ***Anvar v. Basheer***[14] by ***applying the principle of generalia specialibus non derogant (special law will always prevail over the general law),*** held that the evidence relating to electronic record being a special provision, the general law on secondary evidence under Section 63 read with Section 65 of the Evidence. Act shall yield to the same.[15] In the light of this case, the Supreme Court once again has preserved the spirit of the law by giving out a uniform way in which both primary and secondary evidence shall be adduced before admissibility. Indirectly, Sec. 65-B has been made mandatory in each and every digital evidence irrespective of their nature i.e. primary evidence or secondary evidence. It even shows that the Supreme Court has responsibly dealt with the question of authenticity of evidence being submitted before the court and still is concerned with the same. Certificate in terms of Sec.65-B is a must and should thus, accompany the evidence. It can thus be concluded that both the law and the judiciary in India are successfully dealing with the promotion of usage of digital evidence in the country. Still, with the increasing complexities in the nature of crimes and the given fact that digital evidence can be manipulated easily, the law, enforcement bodies and the judiciary are required to remain updated which is a difficult task in a country like India where digital divide and ignorance towards usage of technology is widespread. India still needs better

[11] State of Maharashtra vs. Dr. Praful B Desai AIR 2003 SC 2053, Amitabh Bagchi vs. Ena Bagchi AIR 2005 Cal 11
[12] (2005) 11 SCC 600
[13] http://blog.scconline.com/post/2014/09/20/ruling-of-navjot-sandhu-case-to-the-extent-of-admissibility-of-electronic-evidence-as-secondary-evidence-overruled.aspx <as accessed on 22.02.2014>
[14] Anvar v. Basheer, Civil Appeal No. 4226 of 2012, decided on 18.09.2014
[15] Ibid

cyber-forensics and better law-enforcement only then is the use of digital evidence would become meaningful.

**What limits digital evidence in India?**

Even though the importance of use of digital evidence and the mandatory application of the Information Technology Act has been elaborated by the Supreme Court in the recent cases, it has been silent about the current status of digital evidence in India. The laws and the judgment are not enough to provide a strategic improvement in the field of digital evidence. India is in a dwindling state of affairs considering the fact that the technological development in India is slow. With the alarming rise in the incidence of cyber-crimes it is important to address the current problems which limit digital evidence and its usage in India. The major problems in this field are:

- Lack of education in the field of cyber-technology limits the use and the extraction of digital evidence by the police and also the prosecution. Hence, the Courts and the enforcement bodies are not able to use it to their advantage.
- Outdated techniques for collection of evidence and lack of training about cyber-forensics to police officials.
- The method and content of data on crime collected and recorded varies from State to State. With cross border crime occurring frequently, tracing criminals is a challenge for any State police, in the absence of criminal data sharing and cooperation. The data collected and recorded by the National Crime Records Bureau (NCRB) is basic and data access at all levels is limited.
- Though the Supreme Court has emphasized time and again that digital evidence should be subject to an accurate and stringent test still, no clear test has been laid down as such to prove the authenticity of evidence being admitted in the Court. Courts still in India grapple with the problem of authentication of evidence. This requires to be addressed immediately as manipulation of evidence is quite easy. A framework laying down the procedure of the test is the necessity of the hour.
- There is no integrated approach of criminal investigation as there is no particular federal structure that governs a standardized investigation in India.
- Technology is not only limited to the investigation agencies but also corporate Inc. of India. Indian enterprises as such do not have the required IT skills and tools to deal with the increase in IT fraud. Hence, the problem of not having the awareness and the skills is multi-dimensional and even is a threat to the Indian trade and commerce.

**Where do we go from here?- Immediate address required!**

Over-dependence of people, big corporates and even governments on use of technology, cyber-threat is on the rise and has become easier. ASSOCHAM in accordance with the study that it conducted in 2014 predicted that the reporting of cyber-crimes would double up in the country in 2015. Hence, the immediate solution required is that the Police enforcements and the Courts are well-equipped to able to handle investigations and the digital evidence which

needs to be adduced correctly by the Courts. In keeping with the current scenario certain immediate changes and improvements are required to be opted by India.

**International framework:** Though India has signed Mutual Legal Assistance Treaty and is even a signatory to UN Convention against Transnational Organized Crime. Still, it is important that a harmonious framework is made between the national laws of India and the international law as cyber-crimes are generally trans-border. A Convention of Cyber- Crimes at least would provide a harmonious structure to the seizure, confiscation and production of electronic evidence in Courts and also cooperation between legal enforcement bodies of India and other countries while evidence is being handled. A Convention signed would at least bind all the signatory countries to cooperate and bring uniformity in the investigation framework.

**The Indian Law:** The current amendment in the Indian Evidence Act lays down a rather lengthy procedure which only restricts itself to the evidence as adduced from '*computer',* the term '*computer'* seems to be rather a narrow conjecture of the source of digital evidence. This term at least should be given a wider perspective as there are various sources of digital evidence. Hence, this term should be replaced.

It would even be appropriate if the admissibility of evidence is dealt not only by a general Act i.e. the Indian Evidence Act but, a specific Act which includes not only the procedure but also the jurisdiction, filing of complaint in the Tribunals etc. This specific Act can give a concise explanation to cyber-legal experts and even students. The Act can be complementary to the Indian Evidence Act. The Act should also provide for the minimum standards of the tools used during the investigations as manipulation of digital evidence is very easy. The system of authentication would only be sufficed if it meets the necessary standards.

**The Indian enforcement bodies and court:** Indian enforcements are grappling with the problem of lack of training to handle digital evidence. It is important that the field of cyber-forensics and better use of technology be given more importance by the Government. Regular workshops organized by State Governments to train the police, legal prosecution and even the students. It is also important that the judges as well as the police enforcements adopt and welcome technology in their work rather than flinching from it. This notion can only be changed with the rapid implementation of E-government and E-courts.

A specialized cell that specifically deals with cyber investigations should be constituted in corporate offices which can provide an immediate platform to report such cyber-crime incidences like fraud and phishing.

**Due importance to digital evidence handling**

Conclusively, it can be said that though India has laws to tackle cyber-crimes but it still struggles to deal with the admissibility of digital evidence in the Courts. Cyber-crimes can only be abated and prevented if due importance is given to the handling and management of digital evidence by not only the police but by the judiciary itself. With the Anvar v. Basheer[16] judgment, the burden of adducing digital evidence has increased even more. In the wake of

[16] *Supra 13*

digitalization in India, it is time that digital evidence is given more importance rather than just making laws on it.

## REFERENCES

Websites:


1. http://www.cyberlawsindia.net/computer-forensics.html
2. http://perry4law.org/cfii/
3. *BhairavAcharya, Anvar v. Basheer and the New (Old) Law of Electronic Evidence*, http://cis-india.org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence
4. *Adv. Prashant Mali, Electronic evidence and cyber law*, http://www.csi-india.org/c/document_library/get_file
5. http://www.chmag.in/article/apr2013/indian-evidence-act-and-digital-evidence
6. http://www.lawyersclubindia.com/forum/Digital-evidence-section-45A-How-to-utilise-this-section--40314.asp
7. http://www.hcmadras.tn.nic.in/jacademy/article/Electronic%20Evidence%20PSJ.pdf
8. http://www.hcmadras.tn.nic.in/jacademy/article/Electronic%20Evidence%20PSJ.pdf