DE JURE NEXUS LAW JOURNAL

Author:

Sharon Kerketta

Reva University, Bengaluru

Student, BA, LL.B.

A STUDY ON THE CHALLENGES OF DIGITAL FORENSIC INVESTIGATION IN INDIA: A LEGAL PERSPECIVE

INTRODUCTION

The upgradation with respect to technological advancement in today's modern era has shown its immense contribution to the criminal investigation. Technology has reinforced forensic science especially in digital forensic investigation. Digital forensic investigation is the gathering of evidence acquired by computer artifacts, storage devices, and digital media. It extends its application from computer-oriented crimes such as cyberattacks to the findings of data reposit in the electronic medium like mobile phones[1], servers, or networks. Digital forensic operates from collecting evidence to furnish the final report on the findings of the examination. Thus, digital forensics is carried out for a legal purpose involving the analysis of digital evidence[2]. Information contained in electronic media can be used as evidence in a court of law[3]. The steps encompassed in the process of investigation are classification, conservation, compilation, inspection, analysis, production, and conclusion

The core agenda behind this research paper is to inspect the proceedings of investigation in particular and mention the unique challenges faced by the team of forensics. Investigation process should be prioritized as it serves its efficacy in the declaration of the judgement. It will foster the target of less adjournment for the cases pending before the court of law. The cause-and-effect relationship between a well-structured digital investigation and the speedy trial of cases is construed to analyse the adverse implication and in due furtherance its significance will be highlighted.

This research is proposed to identify the major lacunas and to provide suggestions for its refinement. The strong and effective investigation is of paramount importance so that its judicial purpose is served predominantly.

HISTORY AND EVOLUTION OF DIGITAL FORENSIC INVESTIGATION

Until the late 1990s digital forensics was not introduced and it was only computer forensics which prevailed at that time. Investigators and operatives of technical support realised that there is a requirement of standard techniques, protocols and procedures. A paper was written

[1] In State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600
[2] Kannagi vs K. Kandasamy (2016)
[3] Information technology act 2000 & 65B, No. 21, Act of Parliament, 2000 (India).

by Collier and Spaul focusing on the new discipline to the world of forensic science[4]. The explanation made didn't cover any training or standardization guideline on digital forensics.

'Digital Forensics' and the informal guidelines need to be developed. Conferences were held at the Police Staff College at Bramshill in 1994 and 1995 initiated by the Serious Fraud Office and thereafter modern British digital forensic methodology was established. In 1998 UK the Association of Chief Police Officers (ACPO) released its first version of its *Good Practice Guide for Digital Evidence* in virtue of main principles applicable to all digital forensics for law enforcement in the UK.

Enforcement agencies and heads of divisions worked together on laws collaborating with other several laws and organised meeting on a regular basis. As a result, it had foreseen a substantial growth in 1990s. Federal Bureau of Investigation (FBI) in 1993 held a conference known as the *International Law Enforcement Conference on Computer Evidence*, to determine the need for formal standards and procedures with digital forensics.

Series of conferences had driven the formation of bodies dealing with digital forensics standards in its best practice. One such example was the SWGDE which was formed by the *Federal Crime Laboratory Directors* in 1998. The organization was responsible for exhibiting the most adopted practices for computer evidence. The SWGDE extended its collaboration with other organizations, such as *American Society of Crime Laboratory Directors **(ASCLDs)*** established in 1973 and it has been prominent in the efficient development of the best practice and training in relation to forensic science.

FBI established a formal *Regional Computer Forensic Laboratory **(RCFL)*** in 2000. In 2002, *National Program Office **(NPO),*** a central body was established to coordinate and guide RCFL's law enforcement. Many agencies such as the FBI, CIA, NSA, and GCHQ was established focusing on the operation of digital forensics.

It was just computer device that was widely discussed but at the end of 1990s dependence on mobile phones grown immensely and the technological advancement made the device serve its utility in the investigation process[5].

[4] Wilding, E." Computer Evidence: A Forensic Investigation Handbook. London: Sweet& Maxwell". P.236.(1997). ISBN0-421-57990-0

[5] S.G Punja. "Mobile Device Analysis". Small Scale Digital Device Forensic Journal. (2008). http://www.ssddfj.org/paper/SSDDFJ_v2_1_Punja_ Mislan.pdf.

STAGES OF INVESTIGATION

Richard H. Ward defines the work of a criminal investigator as the one who is responsible for gathering information, determining the validity of information, identifying and locating the perpetrators of the crime and to provide evidence of his guilt for a court of law and his responsibility is to protect the innocent.

An investigator follows six stages of investigation namely Identification, Preparation, Collection, Examination, Analysis, and Reporting

1. Identification: Identification is the preliminary step in the process of investigation where the investigator finds answers to the possible question like who, what, when, where, and how and therefore sets the direction to proceed with the case. It elucidates the availability of potential evidence stored in electronic storage media such as personal computers, mobile phones, and PDA's.
2. Preparation: Preparation involves arrangement of equipment, techniques and search warrants. Second stage of the investigation includes preservation of evidence where the investigator freezes or secures the crime scene to prevent any activity that can alter or delete information stored in a digital device. Preservation is required to maintain the authenticity of data as it creates a sense of trustworthiness and eliminates the chance of misguidance.
3. Collection: It consists of gathering relevant information by collecting the device or through the recording of information. This process involves seizure of personal computers from the incident scene, copying or printing files from the server and recording of network traffic with standardised and accepted procedure. Every possible information that can be extracted from electronic media, equipment and are covered in this stage of investigation[6]. Mobile phones are not only constrained to technology which connects two people but also assist in revealing facts and contribute to the case being a great source of information. It is interesting that the megapixel of camera is of great importance that due to its high resolution, the image or the video can be zoomed to find hidden clues and can be produced as a form of evidence.
4. Examination: The information once collected from potential sources are studied systematically. An in-depth research is carried out to examine data files. Examination

[6] Dr. Bhagyashree A. Despande, textbook on cyber law, 214 (1st ed.) 2019)

is the process wherein potential source, origin, creation, alteration or destruction of evidence will be reviewed and documented. This documentation process assures preservation of that both inculpatory and exculpatory information. There lies an important procedure that a well-defined plan is required to select unerring choice of forensic software tools.

5. Analysis: Analysis means to draw conclusions based on evidence found. The information obtained needs to be assessed to assure that it can act as a substantial evidence. In this stage reconstruction of crime scene is exhibited to draw relation of one event to another and interpret the conclusion in form of digital evidence. Analysis of evidence is the most challenging and time-consuming stage as large amount of data is assessed.
6. Reporting: In the last stage a report is drafted to give an outline of examination process with the data recovered and summary of the actions taken by the investigator. Every detail is recorded in the report and maintained in all prior forensic stages A good report is the one containing solid documentation, notes, photos and tool generated content. The final report, includes physical evidence, interrogation records and other relevant data gathered throughout the case. The prosecutor in court of law to tries to convict a suspect with the help of this report.

CHALLENGES OF DIGITAL FORENSIC INVESTIGATION

Digital Forensic Investigation encounters various inconsistencies in its system. The reason is mentioned below

1. Insufficient cyber laboratories

   There is an alarming rate of cybercrime against women and children. The effective mechanisms of Cyber Crime Prevention Against Women and Children (CCPWC) scheme handles such cybercrimes by enforcing laws in consonance with Indian Penal Code and the Information Technology Act,2000. The Data Security Council of India (DSCI) submitted a draft on the programme report to the ministry of home affairs on handling of cybercrime investigation and proposed to establish cyber forensic labs to all states and union territories[7]. It has now become a prime importance for the country to initiate the project at its earliest. The report expresses the need of Cyber

[7] DSCI, https://www.dsci.in

Crime Police Stations (CCPS), Cyber Crime Investigation & Forensic Training Facilities and Centres of Excellence in Cyber Forensic in all major cities.

2. Lack of expertise

   The criminal activity in cyberspace is increasing day by day and it ask for digital forensic professionals. Specialized equipment and training are needed to investigate cybercrime and also e-commerce crime. It's time to overhaul the practice of digital forensics by emphasising more on training programs and updating the laboratories with modern tools and techniques. In State of Punjab v. Amritsar Beverages Ltd[8]., the Supreme Court recognized there investigating officers face difficulties due to lack of scientific expertise and insight into digital evidences techniques. The court also noted that IT Act does not cover all aspect and hence the agencies are seriously handicapped in some respects. Modern digital forensics is now a multidisciplinary effort that several fields, including law, computer science, finance, networking, data mining, and criminal justice. Professionals will face difficulties regarding the efficiency of digital evidence processing.

3. Absence of universally accepted guidelines for the best practice of digital forensics

   There is a lack of availability of proper guideline for collection and acquisition of digital evidence. Every country has its own guideline for best practices in digital forensics and few are masters in it but there is a need of universally accepted guideline. By this way countries will follow common protocol and can transcend in digital forensics.

4. Legal scenarios in the process of investigation

   a) Jurisdiction: Cyber jurisdiction or cyberspace jurisdiction is covered under section 75[9] of Information technology Act ,2000[10], Section 3[11] and 4[12] of Indian Penal

[8] (2006) 7 SCC 607

[9] Section 75 of ITA 2000-Act to apply for offence or contravention committed outside India.(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

[10] Information technology act 2000, No. 21, Act of Parliament, 2000 (India)

[11] Section 3 of Indian Penal Code -Any person liable, by any Indian law to be tried for an offence committed beyond India shall be dealt with according to the provisions of this Code for any act committed beyond India in the same manner as if such act had been committed within India.

[12] Section 4 of Indian Penal Code -Extension of Code to extra-territorial offences (1) any citizen of India in any place without and beyond India(2) any person on any ship or aircraft registered in India wherever it may be(3) any person in any place without and beyond India committing offence targeting a computer resource located in India

Code, 1860 and Section 188[13] of Code of Criminal Procedure, 1973 including section 178[14] and 179[15]. In SIL Import V. Exim Aides Silk Importers[16] The Supreme Court felt recognized that judiciary need to interpret a statute by providing allowance for technological change until there lies specific legislation for jurisdiction of Indian courts hearing internet disputes.

There are issues of jurisdiction of cyberspace

1. Complexity in deciding the territorial jurisdiction of cyberspace as the user can access website at any place in the world[17].
2. No legislation determines whether the cyberspace event is controlled by laws of country where website is located or the laws of the place where internet service provider is located[18].

b) Stages of investigation

1. Collection: The Indian Evidence Act, 1872 does not entails the method of collection of e-evidence and it only emphasize on the presentation of electronic evidence in the court of law by producing a certificate as per section 65B (4)[19].

[13] Section 188 of CR.PC -Whoever, knowing that, by an order promulgated by a public servant lawfully empowered to promulgate such order, he is directed to abstain from a certain act, or to take certain order with certain property in his possession or under his management, disobeys such direction, shall, if such disobedience causes or tends to cause obstruction, annoyance or injury, or risk of obstruction, annoyance or injury, to any person lawfully employed, be punished with simple imprisonment for a term which may extend to one month or with fine which may extend to two hundred rupees, or with both; and if such disobedience causes or trends to cause danger to human life, health or safety, or causes or tends to cause a riot or affray, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

[14] Section 178 of Cr. PC- Place of inquiry or trial. (a) When it is uncertain in which of several local areas an offence was committed, or (b) where an offence is committed, partly in one local area and partly in another, or (c) where an offence, is a continuing one, and continues to be committed in more local areas than one, or (d) where it consists of several acts done in different local areas, it may be inquired into or tried by a Court having jurisdiction over any of such local areas.

[15] Section 179 of Cr. PC- Offence triable where act is done or consequence ensues. When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a Court within whose local jurisdiction such thing has been done or such consequence has ensued

[16] (1994) 4 SCC 567

[17] Asahi metal industry co. v. supreme court 480 U.S 102(107 S.Ct. 026) (1987)7

[18] www.legalserviceindia.com

[19] Section 65B(4) of Indian Evidence Act 1872 -In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say—(a) identifying the electronic record containing the statement and describing the manner in which it was produced (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this

2. Analysis: The role of forensic examiners is to do both extractions as well as the analysis, with the help of forensic analysts. There are bundle of cases and increased evidence volume that it becomes difficult for examiners and analysts to manage time. Thus, forensic investigators are pressurized to not only be in to assess all the digital evidence that the respective cases generate. The involvement of the forensic investigators in the analysis process is also deemed beneficial, since the investigators have a superior understanding of the case.

5. Technical Challenges: DFI is engineering in nature which ask for development of new software and hardware to enable the collection, retention and examination of potential digital evidence.
6. Admissibility of Digital Evidence: In Shafi Mohammad v. The State of Himachal Pradesh[20] a comprehensive guideline was laid down by Supreme Court of India on the admissibility of electronic Evidence. The court has considered admissibility of electronic evidence in context of Section 65B[21] of Indian Evidence Act. Section 54A of Cr. P.C[22] and provisions to section 164(1) Cr. P.C[23].

   Supreme court clarified about legal position on admissibility of electronic evidence that if a party is not in the possession of device from which the document is produced, the party is not required to produce certificate under section 65B (4)[24] of Evidence Act. Special measure should be taken in account of cyber forensics investigation. The agency undergoes a strict test of admissibility of evidence Hence they are required to co-relate the sequence of events to substantiate the innocence of the accused.

sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

[20] SLP (crl). No 2302 of 2017

[21] Section 65B of Indian Evidence Act 1872- Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

[22] Section 54 A of Cr. PC- If the person identifying the person arrested is mentally or physically disabled, the identification process shall be video graphed

[23] Any Metropolitan Magistrate or Judicial Magistrate may, whether or not he has jurisdiction in the case, record any confession or statement made to him in the course of an investigation under this Chapter or under any other law for the time being in force, or at any time afterwards before the commencement of the inquiry or trial Provided that any confession or statement made under this sub-section may also be recorded by audio-video electronic means in the presence of the advocate of the person accused of an offence;

[24] Section 64B (4), supra note 19.

CONCLUSIONS AND SUGGESTION

1. Law enforcement assistance must be available in both physical and virtual for help during the investigation.
2. With the advancement of technology, the tools should be regularly updated and techniques needs to be improvised with time to cater readiness for challenges that fall in digital forensics.
3. The rapid changes in forensic tools, techniques and standards also require on-going education and best training should be provided.
4. There should exist a universal accepted guideline for digital forensic investigation.
5. A much comprehensive legislation is required to deal with all the aspect of DFI and clearly mention the methods of investigation in details.