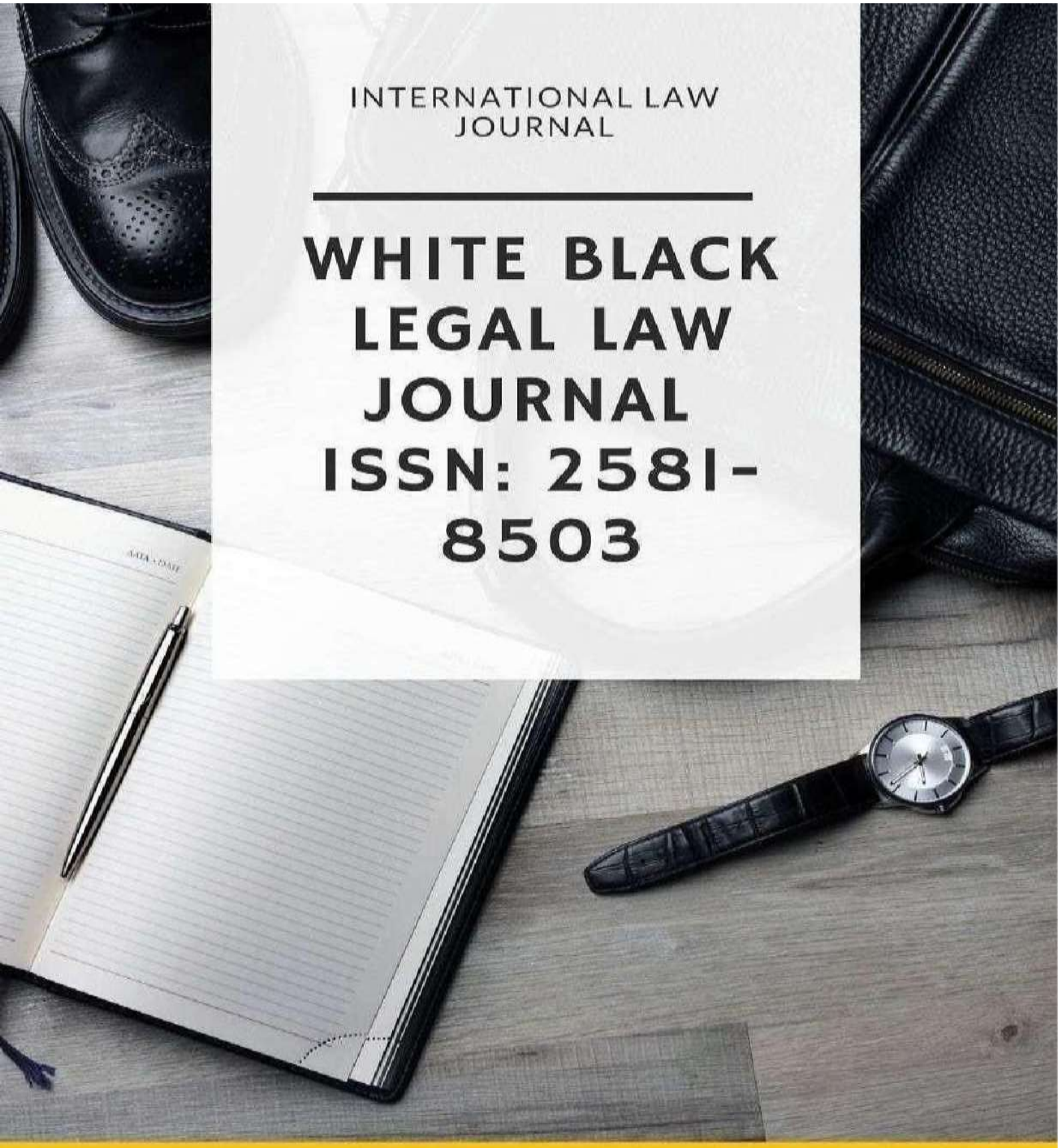

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

"TECH INFUSED COURTROOMS: REVOLUTIONISING FAIR TRIALS THROUGH FORENSICS"

AUTHORED BY - SUHANI AGARWAL
Course - BBA LLB (H)

ABSTRACT

In this 21st century, with the meteoric rise, digitalization has become the backbone of corporate communications, trade, administration, private life, etc. The ambit of law has deciphered various new fields for drafting comprehensive and effective solutions, digital platforms for conducting online hearings, and yet the quest to consider digital forensics and evidence as useful or bogus is still viewed with a blind eye and to be heard with a negligent voice. Digital and forensic evidence plays a vital role in almost every criminal investigation, provided the amount of information and evidence available and also the opportunities offered by electronic data to investigate a crime. However, these electronic pieces of evidence are often considered with the utmost suspicion and uncertainty, although, on occasions they are justifiable. Presently, the use of scientifically unproven forensic techniques are highly frowned upon in legal proceedings. It can't be denied that we have thoroughly failed to reform the laws regarding the admissibility, authentication of the digital and forensic evidence. Nonetheless, the highly unique and ever-changing nature of electronic data, in addition to the current legislation and privacy laws, remain as challenging aspects for systematically attesting evidence in a court of law. This article offers a thorough analysis of the problems that must be discussed and resolved, for the proper acceptance of evidence based on scientific grounds. If not, then digital and forensic evidence will continue to fail to prove its usefulness. Moreover, reviewing the challenges that may complicate the process of systematic authentication of electronic evidence. The study further explores various solutions previously proposed, by researchers regarding their appropriateness based on their experimental evaluation, comparative analysis of the Indian investigation process with other countries. The article explains the emerging subfields of forensics in respect of the Information Technology Act, Bhartiya Nagrik Suraksha Sanhita, Bhartiya Sakshya Adhiniyam and different International laws regarding the same. The research also discusses various theories and practices developed over the years by different academics

and reviewed them, which are debated and tested for many years before finally being implied or denied on legitimate scientific grounds and principles. It also discusses the struggle involved in demonstrating the reliability and validity of these approaches with contemporary evaluation methods. Indeed, it may not be difficult, but challenging to develop universal standards for digital and forensic evidence to meet scientific and judicial needs, due to the diversity and complex digitalisation which has clearly not only provided the opportunities to the safeguards but also to the offenders. Additionally, the development of reliable practices, tools, theories and testing methods for digital forensic techniques is the need of the hour and of immense value to increase the credibility of electronic evidence in legal proceedings. Conclusively, by preventing cybercrimes, ensuring authentication of digital and forensic evidence will pave the way of the judiciary towards fair trials and serve justice to the people.

INTRODUCTION

The rapid increase of digitalisation and technology has emerged, to completely change the human lifestyle, not only in professional or business fields but also for socialisation between people. The increasing phenomenal role of digitalisation has proved itself an efficient tool to work with and this increase has also caused the need to transform laws relating to digital evidence and its rules for authentication and admissibility in court. It has transpired to almost eradicate the conventional forms of paper work in the legal fraternity. The increased use of technology introduces various new chapters and challenges in the legal system which demands the standardization of procedures for the same.

Over the time, sine qua non amendments are done to the Indian legal system like enactment of Information Technology Act (IT Act, 2000) which introduced the concept of admissibility of digital evidence in courts of India. This enactment was followed by amendments in Indian Evidence Act, 1872, Indian Penal Code 1891, and Banker's Book evidence Act,1860. With the legal developments, the Indian Courts pronounced more reliability on digital evidence through various case laws. Forensic science applies scientific principles and techniques to the investigation of crimes. It plays a critical role in the criminal and civil justice system by providing objective evidence that can help establish guilt or innocence.[1]

Digital evidence is helpful as it introduces a multi faceted realm of cutting edge issues and

[1] Max M. Houck and Jay A. Siegel, Fundamentals of Forensic Science, (2015), Third Edition

makes distant shores emerge from the mist. Perceiving the dominance of digital evidence, it is our new reality which is equally relevant for the decision makers. It is possible to manipulate the mind, by creatively combining a complex digital evidence, including music, text, images, and videos, in a matrix. Are these complexities true, equitable, and just? Who propagates the truth and who misrepresents it? What is the process by which society can assess the distinction? Whatever it is, it must be securely preserved, protected and implemented to clear the path of fair trials. As stated by Ewald often both humans and software are challenged to have consistent analyses of the facts and "contradictions and misconceptions in judicial decisions about the facts of the crime"[2] are often observed.

STATEMENT OF WORK

This research paper aims to provide a comprehensive analysis of the evolving landscape of digital evidence and forensic science within legal systems, with a particular focus on the Indian context. It seeks to identify the inherent challenges in the admissibility and authentication of electronic evidence in an increasingly digitized world. The work will delve into existing legal frameworks, assess their efficacy, and explore the scientific and technical methodologies required to ensure the integrity and reliability of digital data in judicial proceedings. By examining contemporary issues and drawing comparisons with international practices, this paper intends to propose actionable solutions to enhance the credibility of digital evidence and support the pursuit of fair trials.

RESEARCH OBJECTIVES

- To analyze the current legal provisions and judicial interpretations concerning the admissibility and authentication of digital and forensic evidence in India.
- To identify the technical and practical challenges associated with the collection, preservation, and presentation of electronic evidence in court.
- To critically evaluate the effectiveness of existing forensic techniques and tools used for digital evidence analysis and propose improvements.
- To compare India's approach to digital evidence with international best practices and identify areas for reform and harmonization.

[2] Big Data in Criminal Justice – Few Chances and Serious Risks' <http://videolectures.net/lawandethics2017_ewald_big_data/

- To develop recommendations for standardizing procedures, defining expert qualifications, and implementing technological solutions to bolster the reliability of digital evidence in courtrooms.

RESEARCH QUESTIONS

- What are the primary challenges concerning the admissibility and authentication of digital and forensic evidence in modern legal proceedings?
- How have Indian legal frameworks, such as the Information Technology Act and Bhartiya Sakshya Adhiniyam, evolved to address digital evidence, and what are their current limitations?
- What role do scientific principles and forensic techniques play in establishing the veracity and reliability of digital evidence, especially in the face of manipulation?
- How do current international practices for handling digital evidence compare to those in India, and what lessons can be drawn?
- What are the proposed solutions and best practices to standardize procedures for the collection, examination, analysis, and reporting of digital evidence to ensure its integrity and prevent forgery?

KEY WORDS

- Digital Evidence
- Forensics
- Authentication
- Admissibility
- Hash Value
- Chain of Custody
- Self-Corrosion

FROM COMPUTER FORENSICS TO MORE INCUSIVE "DIGITAL EVIDENCE"

The landscape of Digital evidence has been increasing in many parts of the world and making its place since the 1970s. At that time a Computer Forensic Unit was established which has worked closely with the FBI for the development of computer forensic capabilities.

Simultaneously, audio and video were also moving to digital format. The concept of digital evidence, which included digital audio and digital video evidence was brought before the federal laboratory directors on March 2, 1998, at a meeting hosted by the U. S. Postal Inspection Service, Forensic and Technical Services Division, Dulles, Virginia.[3]

After its introduction, U.S. conducted several conferences and meetings with other federal governments in which many technical experts also participated and gave their views. Finally, on June 17, 1998, the Technical Working Group Digital Evidence (TWGDE) was established which later on evolved into Scientific Working Groups (SWGs) which focused on technicality and science both. In the present scenario, as far as the international arena is concerned, there are various other perspectives and provisions for dealing with digital evidence compared to Indian legislation. Though, the inception of digital evidence in Indian Law came way too after than other countries. The Indian Evidence Act 1872, was first based on only archaic form of evidence that is documents, later on they added the view of Electronic Evidence. Presently, Bhartiya Sakshya Adhiniyam, 1872, Section 2(d)[4] defines 'document' as any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records. Major chunks of the act were amended and substituted by the addition of electronic records, electronic evidence, electronics documents, etc. The video footage/clipping contained in such a memory card/pendrive being an electronic record as envisaged by Section 2(1)(t) of the 2000 Act, is a "document" and cannot be regarded as a material object.[5]

CHALLENGES AND CONTROVERSIES IN TECH INFUSED COURTROOMS

Tech includes many kinds of technologies but the focus of the current topic is digital evidence. It has provided various opportunities which served with the information or data that have quickly become an indispensable and constant necessity in our daily lives. We can use this data to follow the trail of messages, transactions and other digital media by demographic location,

[3] An Historical Perspective of Digital Evidence: A Forensic Scientist's View Carrie Morgan Whitcomb, Director, National Center for Forensic Science International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1 www.ijde.org
[4] Bhartiya Sakshya Adhiniyam, 1872, s 2(d)
[5] [2019] P. Gopalkrishnan v. State of Kerala, SCC OnLine SC 1532

or by an individual's address, bank account, passport or other identifier, among others. Investigators, especially law enforcement agencies, increasingly rely on audit trails to track a criminal's computer footprint and employ digital evidence to prosecute them. Though considered in detail in criminal proceedings, electronic evidence tends to be accepted with extreme caution and reluctance. Crucially, any item to be admissible as evidence in a court has to show its veracity and reliability. Moreover, digital evidence can be easily manipulated, it must undergo both an intensive and acceptable scientific process. It is the study of a technological innovation on the scale of millennia, a transformation that has ushered in a new age for civilization, perhaps appropriately termed the "Age of Information Complexity[6].

Electronic evidence is widely known to be inconsistent with scientific standards imposed by the Courts. The lack of a framework for evaluating digital evidence and uncertainty in the digital forensic workflow is a gift to the defense lawyers who want to dispute the, to be introduced as evidence in a court of law. They point out various deficiencies in the collecting and comparing of evidence that justifiably question the truth and accuracy of the data. Though, verifying digital evidence as an accurate and repeatable science is not an easy undertaking, and a topic open for debate.

It is important not to permit anybody, to disturb the hardware or the network, or any work on computer. It is also advisable that the police officers engaged in searching for digital evidence be properly trained[7]. It is just the tip of an iceberg as there are various stages involved in regards with digital evidence and all of them needs to be handled with standardised procedures. There are some steps that are common in all investigations related to digital evidence: (a) Collection, (b) Examination, (c) Analysis, and (d) Reporting.

There should be professionalism in handling digital forensic evidence, from the starting of seizure, by taking on site forensic pictures of the hard drives that have been seized, that can be served as a proof that it is untouched and kept securely after being seized. The difficulty of authenticity is a fundamental problem for all legal systems. Digital material is so ubiquitous and easy to forge that the world's legal systems need to develop procedures that validate, challenge and test the authenticity of digital material. No legal system can function effectively

[6] George L. Paul & Jason R. Baron, Information Inflation: Can the Legal System Adapt?, 13 Rich. J.L.& TECH., no. 3,2007 at 1,7 n3\, available at http://law.richmond.edU/jolt/v13i3/articlel0.pdf.
[7] [2005] R v Good DCR 804

without lawyers being able to tell if written things are what they say they are. This then leads to questionable things around the “integrity” of a file (has it changed over time in ways we don’t know?) and the authenticity of the "identity" which is attached to a file. It's not only a technical issue. It is extremely philosophical since it raises questions about how a lawyer could be expected to dispute digital information when there isn't enough of it to support such a claim. In this regard, there aren't yet any standardized practices across the legal systems of the world. Since evaluating authenticity is an empirical endeavor, it mostly depends on all available data, including circumstantial evidence. There is a need to realise that digital evidence has a very wide impact in the access of justice and this access is being tarnished without the realisation of the same.

There are numerous cases in which fake evidence is presented by the parties in the court and attempted to blow smoke in the eyes of law. In the case of Lenihan v. Shankar[8], court saw the increased prevalence of digital forgery in law disputes, where the mother falsified paternity tests, emails, and witness statements. It emphasizes the importance of preserving authentic digital evidence, as tampered records can undermine legal proceedings.

Simple screenshots can be scrutinized, so legal teams may verify authenticity using hash values and metadata. The manner of evidence collection and preservation is crucial, and a clear chain of custody is necessary for credibility in court otherwise tainted evidence can be produced very easily. The case serves as a warning for legal professionals to be vigilant about the authenticity of digital documents. Though, through the passage of time, with digital evolution, courts are also coping up with digitalisation due to which reliance on screenshots is also noticed. However, it lacks sufficient metadata to prove their authenticity and important context that is necessary to interpret the evidence.

The courts refused the admission of screenshots in a case due to their noncompliance with the Best Evidence Rule[9]. In the case plaintiffs were unable to provide native files with metadata that would have allowed the legitimacy of messages to be confirmed. This instance demonstrates how screenshots by themselves are frequently insufficient in the absence of adequately validated digital proof[10]. Furthermore, in the case of, Dell International Services

[8] [2021] ONSC 1537
[9] Indian Evidence Act, 1872, Sections 91 to 100
[10] Moroccanoil v. Marc Anthony Cosmetics (2014)

Private Limited V. Adeel Feroze & ors[11], the Hon'ble Delhi High Court held that no electronic evidence will be admissible unless it is accompanied by the electronic evidence certificate under Section 65B of the Evidence Act[12]. The admissibility of electronic evidence in courts is now governed by Section 63 of the Bhartiya Sakshya Adhiniyam, 2023[13]. The format of certificate under Section 63 has been modified and split into two sections, with "Part A" pertaining to the essential information to be filled by the individual submitting the evidence. Section 63(4)(c)[14] states that "an expert shall be evidence of any matter stated in the certificate," which means that "an expert" must now fill out the technical portion of Part B.

Overall, sole reliance on screenshots is prevented by the courts as there is no proper standardised procedures by which they can be verified. Under section 63 of Bhartiya Sakshya Adhiniyam, 2023, the certificate of an expert is required to be submitted for the admissibility of the evidence. The format provided under the Bhartiya Sakshya Adhiniyam, 2023 deals with the technical requirements for the admissibility of electronic evidence. The legislature has allegedly improved on its previous legislation by transposing it into the electronically sophisticated requirement. It has provided the form of the certificate but the on ground reality is way too different as people find loopholes according to them. The inclusion of "an expert" referred to in Part-B of the Certificate in Section 63 of the Bhartiya Sakshya Adhiniyam, 2023 is still an issue. This is likely to be discerned through rules to be enacted subsequently or through the judiciary as soon as possible. Section 63 of BSA has not specifically interpreted the term "expert" and people with less or no experience are submitting the same. Standard operating procedures are required to be implemented so that the people can't find an escape clause and the aim of the legislature behind the amendment can be fulfilled.

AUTHENTICITY CRISIS

There are no uniform standardized practices across the legal systems of the world and with a doubt that there ever will be any. Since testing authenticity is an empiricism exercise, it mostly depends on all available evidence, including circumstantial evidence. Forensic science refine over time the authenticity testing method also needs to evolve over the time.

[11] ([2024] SCC Online Del 4576)
[12] Indian Evidence Act, 1872, s 65B
[13] Bhartiya Sakshya Adhiniyam 2023, s63
[14] Bhartiya Sakshya Adhiniyam 2023, s 63(4)(c)

Technical topics like mathematical transformations of digital information, such as verifying "hash value" methods, are inevitably introduced in Bhartiya Sakshya Adhiniyam, 2023. Hash value explores further technical information, including network connection evidence, log and printed files, internet usage evidence, browser caches, cookies, and email and instant messaging evidence.

HASHING METHOD

A hash function value mentioned under the form Part B of the admissibility of electronic evidence certificate under Section 63 of BSA, is an outcome of a mathematical method that transforms a digital file in a single, irreversible step, producing a distinct but significantly smaller digital file. These mathematical findings might be thought of as a digital fingerprint in a certain sense. When we compare digital files to see if they are exactly the same, hash results can be helpful. When hashed, two files that change by just one bit will appear fundamentally and unpredictably different. Basically, it verifies that data under the particular record is safe and unaltered. It is advisable to retain first in time copies of any files that are to be identified in order to be able to recalculate hashes as algorithms become deprecated and new ones are introduced. For the purpose of detecting changes using digital signatures, SHA-1 and MD5 should be considered unreliable and deprecated as usage of SHA-1 began to be phased out in the technology community in 2017[15]

Since digital signatures are usually only valid for a limited time period, this is less of a problem, although even with MD5, issues have been identified since at least 2004, and they still persist[16]. The filtering technology has proved itself more useful and even used by social media platforms for the avoiding of dropping illegal content. For example it is used to prevent child images being marketed, which is done by only changing the logos. Similarly, there are many technologies that can compare content to determine how identical a file is to the content of a prior copy, rather than relying on finding an exact match (via a file hash). These filtering algorithms typically indicate, with a predetermined degree of certainty, that the content matches a copy. Instead of achieving a precise match, as file hashes do, the outcome is a percentage of

[15] Google Security Blog, 'Announcing the first SHA1 collision', 23 February 2017, https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html.

[16] Xiaoyun Wang, Denggou Feng, Xuejia Lai and Hongbo Yu, 'Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD', Cryptology ePrint Archive Report 2004/199, 16 August 2004, Institute of Software, Chinese Academy of Sciences, https://eprint.iacr.org/2004/199.pdf; Fahmida Y. Rashid, 'Oracle to Java devs: stop signing JAR files with MD5', InfoWorld, 19 January 2017, http://www.infoworld.com/article/3159186/security/oracle-to-java-devs-stop-signing-jar-files-with-md5.htm.

likeness. For this reason, numerous technologies exist that do not rely on establishing an exact match (by way of a file hash), but rather are capable of comparing content to establish the proximity of a file to the content of a known previous copy[17]. These filtering algorithms usually provide an indication at a preset level of certainty, of the fact that material matches a previously observed copy. The result is a percentage of likeness, rather than an exact match.

CONTINUING CUSTODY

Furthermore, recent advancements in data storage techniques could lead to issues along the road. Evidence kept on contemporary internal primary storage systems may undergo a process we call "self-corrosion," as shown by Graeme B. Bell and Richard Boddington[18]. This means that a contemporary solid-state storage device can permanently delete evidence to a very amazing degree in a short span of time, even in the absence of computer instructions, in a way that a magnetic hard drive would not. Experiments employing actual consumer hardware in a replicable laboratory setting demonstrate the existence of the Solid State Drive (SSD) self-corrosion phenomenon[19]. Experimental findings demonstrate that solid-state drives (SSDs) have the capacity to destroy evidence catastrophically under their own volition, in the absence of specific instructions to do so from a computer[20]. It is more confusing for the layman with little or no technical understanding of the nature of the evidence. The recovery of data is quite not possible in many scenarios as it leads to self corrosion over a period of time. In India, the cases stretch for years and the digital evidence stored in these drives get corrupted leading to the loss of evidence. Proper storage guidelines must be introduced to avoid these kind of discrepancies.

There is very little room for positive assumptions in the way SSDs operate today; the only assumptions that can be made is that the investigator can access the data that is stored on the disk. Data would disappear forever within minutes; that is being attempted to be destroyed, such as by formatting the disk in a quick format mode, even if the computer is shut down immediately after issuing a destruction command (such as quick format) there is no way yet to

[17] Well-known technologies include Microsoft's Photo DNA, used for identifying altered image material, and the Sift algorithm, used, for example, through technology applied by Facebook to filter illegal uploads.
[18] Graeme B. Bell and Richard Boddingto Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Journal of Digital Forensics, Security and Law, Vol. 5(3)
[19] 'Solid state drives'; Ravi Kant Chaurasia and Priyanka Sharma, 'Solid state drive (SSD) forensics analysis: a new challenge' (2017)
[20] Graeme B. Bell and Richard Boddingto, Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Journal of Digital Forensics, Security and Law, Vol. 5(3) http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf

prevent the disk from erasing the data once the power is turned on. This situation is similar to Schrodinger's cat, which said, "Until the box is opened, no one knows if the cat is alive"[21] With the speed at which controller and SSD memory technology is developing and growing, it is unlikely that the new grey area in the forensic and legal sphere can ever be eliminated or reduced. "The golden age for forensic recovery and analysis of deleted data and deleted metadata may now be coming to an end," according to Australian scientists[22].

Electronic evidence should be handled with extra caution since it can be easily altered. The integrity of the evidence must be proven, with the fact that it was not altered after being taken or copied. In the case of multiple pieces of hardware and multiple computers, it will be necessary to make sure that there is a clear connection between the hardware and the electronic evidence that was copied from the hardware. This is another reason to be careful about making sure that the continuity of electronic evidence is maintained and that its custody is accurately documented. In this regard, a record is maintained to cover things like who gathered the evidence, how and where it was gathered, who took possession of it, how and where it was stored, the protection provided to the evidence during storage, and the identities of those who took the evidence out of storage, along with the justifications for doing so[23].

The ACPO Guide[24] focuses on the collection phase and outlines the four primary stages of managing electronic evidence: collection, examination, analysis and reporting . A professional who works with digital evidence should think about implementing the procedures for the four stages of his investigations. A first "assessment" or "triage selection" phase may be added to these four processes with the development of forensic triage procedures which has received considerable attention within the forensic practitioner and law enforcement communities.

Assessing the collected evidence is the core part of investigation as its failure can lead to unreliable and false assumptions. In the case of Liser v Smith[25], the time stamp shown in ATM and the time of video footage had a gap of about 20 minutes as told by the bank manager, according to which a person was held liable for the murder. Later on, it was discovered that the

[21] (Schrodinger's cat, http://en.wikipedia.org/wiki/Schr%C3%B6dinger's_cat).
[22] Ibid 20
[23] Warren G. Kruse II and Jay G. Heiser, Computer Forensics Incident Response Essentials (AddisonWesley 2002), 6–11
[24] ACPO Good Practice Guide for Digital Evidence, Version 5 (October 2011)
[25] [2003] 254 F.Supp.2d 89 (D.D.C.)

time gap was more than 20 minutes and assessment of digital evidence went wrong. It also shows the reliance of investigating authorities on digital evidence and inefficient assessment of the same.

CASE LAW ANALYSIS

There are various cases like Mansfield murder case[26], DPP v McKeown (Sharon), DPP v Jones (Christopher)[27], Woodward v Abbey National plc (No 2), J P Garrett Electrical Limited v Cotton[28] in which judges held that digital evidence should be assessed sensibly and must be viewed in a special light to draw proper conclusions.

In the case of R v. Ross Magoulias[29], the appellant's identity was based on surveillance camera and ATM records, the judge in this case provided a more realistic assessment of clock accuracy. In this case, both the victim and the appellant were at the service station on 7 July 2001, with video footage showing the victim there between 18:37:18 and 18:40:25. The appellant withdrew $50 from an ATM at 18:40:59, according to the ATM's timing. However, there's no evidence proving the clocks were synchronized, and the video doesn't show the appellant near the ATM at that exact moment, which raises doubt about the timing. The clocks and timing devices can show slightly different times, and this can lead to small errors, especially when synchronization is required for precise events. Thus there was no room for any presumption to operate in any useful way[30].

On the other side of the coin, a clock can also help in solving a case and identifying a fake evidence. In an attempt to clear his name after being caught speeding on June 1, 2009, Shaun Richards tried to manipulate evidence by driving the same route (without speeding) in January 2010 and then altering the timestamp on his satellite navigation data to match the original date. However, he overlooked one crucial detail: the time change between British Summer Time and Greenwich Mean Time, which resulted in a one-hour discrepancy. Once this mistake was

[26] People v. Mansfield, Case No. E077064 (Cal. Ct. App. Mar. 14, 2022), Ruben Castaneda, 'Mistaken arrests leave Pr. George's murder unsolved', washingtonpost.com, 22 June 2003, https://www.washingtonpost.com/archive/politics/2003/06/22/mistaken-arrests-leavepr-georges-murder-unsolved/8e6257de-22c6-4e73-894f-0e71f7ad9b2c/.
[27] [1997] 1 WLR 295, [1997] 1 All ER 737, [1997] 2 WLUK 386, [1997] 2 Cr App R 155 (HL), (1997) 161 JP 356, [1997] RTR 162, [1997] Crim LR 522, (1997) 161 JPN 482, (1997) 147 NLJ 289, Times, 21 February 1997, Independent, 7 March 1997, [1997] CLY 1093.
[28] [2005] 4 All ER 1346, [2005] 7 WLUK 814, [2005] ICR 1702, [2005] IRLR 782, [2005] CLY 1244.
[29] [2003] NSWCCA 143, 2003 WL 21208345.
[30] [2003] NSWCCA 143 at [41].

uncovered, Richards was sentenced to four months in prison for trying to deceive the justice system[31].

FUTURE CONSIDERATIONS OF SAFEGUARDS

The legal profession, as the guardian of the truth seeking process, must devise more schemes for governing the digital evidence. In Khodorkovskiy and Lebedev v Russia[32], a case before the European Court of Human Rights, the defence raised a number of important issues challenging the electronic evidence sought to be admitted that related to the volatile and mutable nature of such evidence. The court held that, possible discrepancies in the documents describing the amount of data contained on the hard drives, inaccuracies as to the exact location of the computer servers, and other defects complained of may have various explanations. The Court cannot detect any manifest flaw in the process of seizing and examining the hard drives which would make the information obtained from them unfit for use at the trial[33].

As in an Australian case of Roads and Traffic Authority of New South Wales v. Timothy Adam Michell[34] a security indicator will be worth implementing on photographic evidence as given under Section 47 (2)(c) of the Road Transport (Safety and Traffic Management) Act of 1999. It asserts that the question of integrity in this new avalanche where the ease of alteration is a serious question and reality of today's legal system. It is illuminating to read about other legal systems and learn how they deal with the new digitized era.

There are various softwares, technologies that exist to verify the authentication of different digital documents like for emails DKIM facility which prevents email spoofing. Such authentication shall be made compulsory before heavily relying on these digital documents. As we are entering in the era where use of AI is increasing, where it is very convenient to produce a forged email, certificates by experts will not alone prevent it from happening. There should be a whole other regulation to verify every single digital document mentioning the procedure to conduct it.

A forensic tool named FTK imager is used for creating an image of the disk and FTK Toolkit

[31] 'Devon driving instructor jailed for sat-nav speed fraud' BBC News Devon, 13 January 2011.
[32] 11082/06 and 13772/05 – [2013] ECHR 747 (25 July 2013)
[33] 11082/06 and 13772/05 – [2013] ECHR 747 (25 July 2013) at [702]
[34] [2006] NSWSC 194 (Austl.)

or Field Testing Kit for solving this case by finding the key evidence. The results obtained from HDD (Hard Disk Drive) are set as a hypothesis for the study. The same process is followed in a solid-state drive. The results obtained in these two cases are compared statistically and it will help us understand the challenges that are being faced by forensic investigators for cracking the evidence in solid state drives.

It is amusing to learn that the best evidence rule is being used in many countries such as Australia, England, India and elsewhere. This principle comes with a vague and frequently misinterpreted "right to confront," and has historically served as the basis for a regulation at best, and has become somewhat obsolete and, at worst, has lost some of its effectiveness.

The Section 15 Information Technology Act, 2000 uses the word secure for digital signature and defines it as "secure electronic signature."[35] According to this technique, a document's signatory has a special "key" connected to his verified identity. Then, this key is utilized in combination with cryptographic procedures, and a digital file is hashed and encrypted in other ways using "asymmetrical cryptography." If the system verifies the record, it has been established that the digital file has not been altered since it was encrypted and that it is linked to the owner of the encrypting "key" in question. This in addition determines whether the digital file has been altered or not, since it was encrypted[36]. It is seen that we are living in such a immersive virtual environment technology world that no courts have ever checked the validity of digital signatures but ironically they have mandated this kind of signatures in some sectors[37]. The playfield of the technological world is changing very fast. What is true today may no longer exist tomorrow. So, it is necessary to keep an eye on what is happening in the industry.

CONCLUSION

There must be conducted necessary inquiries and policies for testing future mind control that may exist. As in the past, the lawyers are responsible for protecting society since they are the scientists and high priests of knowledge in this new arena. There must be uniform and practically applicable principles to all areas of digital evidence, which meets the end of the justice system. Professional certification is a global issue by definition. It will be challenging

[35] Information Technology Act 2000, s15
[36] ELECTRONIC EVIDENCE, (THIRD EDITION), Stephen Mason, General Editor, LexisNexis Butterworths
[37] See Karia & Karia, supra note 30, at 562; Ministry of Company Affairs, Notification, Part II, Sec 3(ii) The Gazette of India: Extraordinary 15 (2006)

to proceed in a systematic and efficient way until we have a universal indicator of individual ability and knowledge. Standards and norms will be pushed by technology, which will also drive education and training, to support certification procedures. The final user will be the legal system, which will set rules and regulations. The community needs to be set up with procedures that can handle these numerous obstacles and be more clear and accurate about the process.

With technology advancing at a rapid pace, the challenge is to successfully guide the numerous experts along a systematic and efficient path to address the various difficulties pertaining to digital evidence. We need to set up a system that can respond to change and generate a vastly skilled workforce in terms of technical proficiency. Can an international certification body operated by a consortium of National and International organizations be the answer to the current problems related to digital evidence? Representatives from a wide range of current organizations and groups will engage in a debate on worldwide professional certification challenges led by the National Center for Forensic Science.

We should be prepared for professional certification between such a chaotic structure regarding the digital evidence. Especially in India, where in many parts basic technical equipment have not reached to create a path of justice through it, in those areas implementation of more complex technicalities can prove to be more harmful than being useful.

The computer generated visualisations tend to be handled more cautiously as it is very persuasive in nature due to the "seeing and believing effect"[38]. This could lead the trials into some other directions from where they are meant to be. It is important to keep in mind that a digital evidence professional or we can call it an expert in digital evidence is required for many tasks like for obtaining and copying electronic evidence with high probative value and also for analyzing such evidence. Examining the data's properties and substance will be part of the evidence analysis process. This exercise could also involve, but not be restricted to, searching for and retrieving erased files and other data that might be concealed on the disk, monitoring activity logs, and looking for residual data in unallocated and slack space.

Due to the extensive use of computers, smartphones, mobile phones, and the Internet, the

[38] Damian Schofield & Stephen Mason, Using Graphical Technology to Present Evidence, in ELECTRONIC Evidence 217, 218 (Stephen Mason gen. ed., 2012).

majority of lawyers now deal with electronic evidence[39]. Only in basic circumstances the value of the evidence can be understood easily but in other cases when the other parties contest the data or the evidence it cannot. The court has to frequently rely on experts in digital evidence in these situations. This suggests that each piece of evidence must have its merits carefully examined.

Although this paper offers a number of guidelines and standards for managing and evaluating electronic evidence, future developments in technology will surely bring up new difficulties and conflicts for the procedure of gathering, assessing, and examining electronic evidence in a court of law soon. We have to deal with the present situation and be prepared for the future.

REFERENCES

Books, journals and articles

- Schafer, Burkhard, and Stephen Mason. "The Characteristics of Electronic Evidence." Electronic Evidence, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 18–35. JSTOR, http://www.jstor.org/stable/j.ctv512x65.9. Accessed 5 Jan. 2025.
- Monika Rathore, 'Admissibility of Evidence in India' (2023) 6 Int'l JL Mgmt & Human 2739
- Mason, Stephen, and Allison Stanfield. "Authenticating Electronic Evidence." Electronic Evidence, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 193–260. JSTOR, http://www.jstor.org/stable/j.ctv512x65.14. Accessed 28 Dec. 2024.
- Weir, George R. S., and Stephen Mason. "The Sources of Electronic Evidence." Electronic Evidence, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 1–17. JSTOR, http://www.jstor.org/stable/j.ctv512x65.8. Accessed 18 Jan. 2025.
- Wilson, Nigel, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." Electronic Evidence and Electronic Signatures, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 429–87. JSTOR, http://www.jstor.org/stable/j.ctv1vbd28p.16. Accessed 15 Jan. 2025.

[39] Graeme Horsman and Lynne R. Conniss, 'Investigating evidence of mobile phone usage by drivers in road traffic accidents' (2015) 12 Digital Investigation s30

- Chandni Ghatak, Leaving My Legacy Online - Weighing the Viability of Recognising Digital Wills in India, 7 NIRMA U. L.J. 87 (January 2018).
- Bozidar Banovic, 'Electronic Evidence' (2006) 44 J Crimin & Crim L 223
- Tejas Karia, Akhil Anand & Bahaar Dhawan, 'The Supreme Court of India Re-Defines Admissibility of Electronic Evidence in India' (2015) 12 Digital Evidence & Electronic Signature L Rev 33.

Websites

- https://www.jstor.org
- https://www.scconline.com/
- www.manupatrafast.com
- https://heinonline.org/