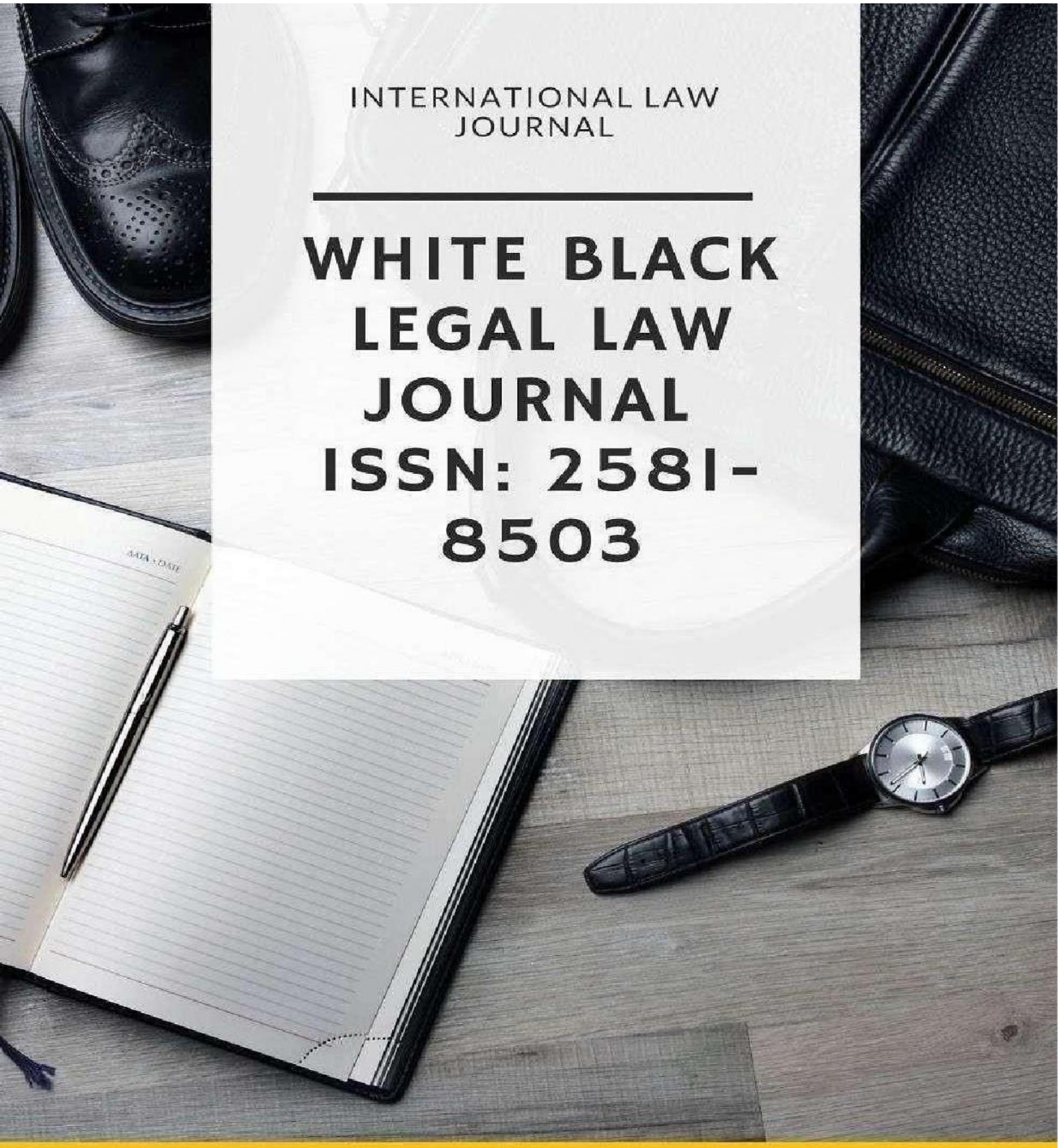


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

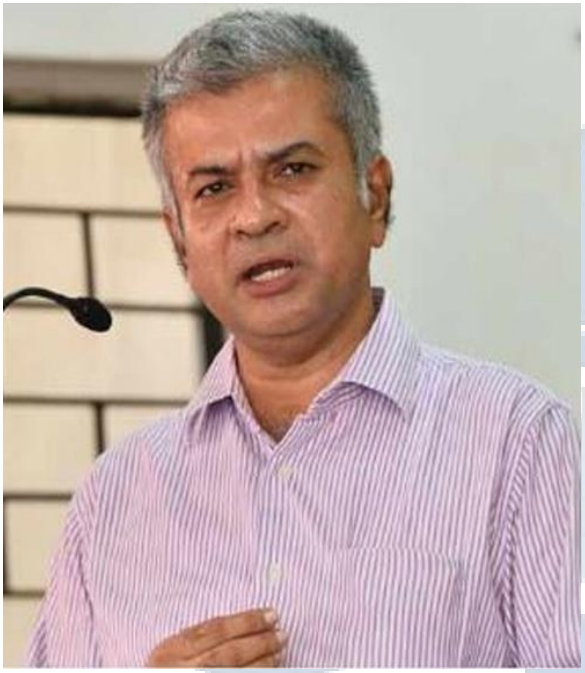
The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

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 providededicated 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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

DIGITAL FORENSICS AND CRIMINAL JUSTICE

AUTHORED BY - SWATI SWATI

Introduction

A few years ago, there wasn't much knowledge about digital forensics, which is the skill of retrieving and examining data from digital devices including desktop computers, netbooks, tablets, cell phones, etc. However, this area of forensics has recently grown significantly in importance due to the rise in cybercrime and the increased use of digital devices, supplementing what was previously thought to be limited to the recovery and examination of chemical and biological evidence during criminal investigations.[1]

Forensic science or Forensic evidence serves as the backbone of modern legal systems, providing a factual basis for the investigation and prosecution of crimes. Its emergence has revolutionized the criminal justice landscape, transitioning from a reliance on witness testimony to an evidence based approach that can objectively link suspects to crimes or exonerate the innocent.[2]

Digital forensics, also known as security forensics or computer forensics, is used to find evidence in digital data. Digital forensics is conducted for computer systems, mobile devices, storage media, electronic files, packets over the network, and so on. In particular, forensics in information security is defined as investigating digital evidence using scientific verification and restoring the original appearance of the incident through retrieval, analysis, and restoration to provide a basis for court proceedings.[3]

Digital evidence, also known as electronic evidence, is electronic information that is stored or transmitted in digital form. Digital evidence can be any electromagnetic record stored and transmitted using a computer or related electronic equipment. Messages, pictures, audio and

[1] Dr.Jeetendra Pande and Dr. Ajay Prasad, *Digital Forensics*, Uttarakhand Open University, Haldwani, available at https://uou.ac.in/sites/default/files/slm/MIT(CS)-202.pdf, accessed on 2 September, 2024 at 14:17 IST

[2] The Role And Admissibility Of Forensic Evidence In The Indian Criminal Justice System, available at https://www.mondaq.com/india/crime/1469694/the-role-and-admissibility-of-forensic-evidence-in-the-indian-criminal-justice-system, accessed on 5 September, 2024 at 09:00 IST

[3] D. Kim, S. Oh, and T. Shon: Forensic Sci. Int.: Digit. Invest. **46** (2023) 301608. https://doi.org/10.1016/j.fsidi.2023.301608

video, coordinates, symbols, or other data can be digital evidence. Any electromagnetic records that can be read by appropriate equipment can be used as digital evidence. Digital evidence is used to support or disprove crimes or can be used to express key elements such as criminal motives.[4]

Computer forensics[5] is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. It is the use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage3. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. Similar to all forms of forensic science, computer forensics is comprised of the application of the law to computer science. Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. The use of specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.

EVOLUTION

It is difficult to pinpoint the first ―computer forensic‖ examination or the beginning of the field for that matter.[6] But most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and

[4] D. Roni, N. S. Gill, and P. Gulla: J. Ind. Inf. Integr. **38** (2024) 100568. https://doi.org/10.1016/j.jii.2024.100568
[5] https://forensiccontrol.com/resources/beginners-guide-computer-forensics/
[6] *Digital evidence*. (2015, Aug. 20). Retrieved Oct. 11, 2015, from Wikipedia: https://en.wikipedia.org/wiki/Digital_evidence available under the Creative Commons Attribution-ShareAlike License.

assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field is evolving. Both Government and private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field.

The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents. In 1892, a eugenicist named Sir Francis Galton established the first system for classifying fingerprints. Sir Edward Henry, commissioner of the Metropolitan Police of London, developed his own system in 1896 based on the direction, flow, pattern and other characteristics in fingerprints. The Henry Classification System became the standard for criminal fingerprinting techniques worldwide.

In 1835, Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to the murder weapon. Bullet examination became more precise in the 1920s, when American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings. And in the 1970s, a team of scientists at the Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.

In 1836, a Scottish chemist named James Marsh developed a chemical test to detect arsenic, which was used during a murder trial. Nearly a century later, in 1930, scientist Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups. His work paved the way for the future use of blood in criminal investigations. Other tests were developed in the mid-1900s to analyze saliva, semen and other body fluids as well as to make blood tests more precise.

In 1984, FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.

In 1988, the International Association of Computer Investigative Specialists (IACIS), an international non-profit corporation composed of volunteer computer forensic professionals dedicated to training and certifying practitioners in the field of forensic computer science was formed.

It was followed by formation of International Organization on Computer Evidence (IOCE)[7] in 1995, which aims to brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

With the rise in cybercrime, the G8 nations realised the importance of computer forensic, and in 1997 declared that ―Law enforcement personnel must be trained and equipped to address high-tech crimes. In 1998, G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. In the same year INTERPOL Forensic Science Symposium was held. The First FBI Regional Computer Forensic Laboratory established in 2000 at San Diego.

Methodologies in Digital Forensics

The methodologies in digital forensics in India encompass a range of systematic approaches used for the collection, preservation, analysis, and presentation of digital evidence. As cybercrime incidents increase, the need for robust digital forensics methodologies becomes more critical for law enforcement agencies, private sector organizations, and legal practitioners. This report outlines the key methodologies employed in digital forensics, highlighting their significance, processes, and challenges in the Indian context.

The digital forensics process generally involves several stages, including data collection, preservation, examination, analysis, and presentation of evidence.[8] Each stage is crucial for ensuring that the evidence remains admissible in court, maintaining its integrity throughout the investigative process. This structured approach is designed to support investigations into a variety of cybercrime cases and facilitate legal proceedings. Data collection in digital forensics

[7] https://en.wikipedia.org/wiki/Scientific_Working_Group_on_Digital_Evidence
[8] Anuraag Singh, *Digital Forensics Software for Indian Cyber Labs*, https://www.linkedin.com/pulse/digital-forensics-software-for-indian-cyber-labs-anuraag-singh-vfpqc#:~:text=The%20steps%20involved%20in%20a%20digital%20forensic%20investigation%20include,analysis%2C%20and

involves various techniques aimed at acquiring information from different types of digital devices, such as computers, smartphones, and servers. Techniques may include creating bit-by-bit copies of hard drives, using write blockers to ensure that original data remains unaltered, and employing specialized software tools for data extraction. Selecting the appropriate technique depends on the situation, the type of device involved, and the nature of the investigation.

Evidence preservation is a critical aspect of digital forensics, ensuring that data remains intact and unaltered from the time of collection until it is presented in court. This is often achieved through secure storage and chain-of-custody documentation, which tracks the handling of evidence. Digital forensics practitioners must adhere to strict procedures to avoid any contamination or alteration of digital evidence. Data examination involves scrutinizing the collected data to identify relevant information linked to the case. Forensic experts utilize various software tools to analyze data, recovering deleted files, analyzing metadata, and identifying patterns of behavior within digital artifacts. Given the complexity of digital data, this stage often requires a multidisciplinary approach, combining knowledge from fields like computer science, cyber security, and legal studies.

Incident response is a vital component of digital forensics, particularly in cases of active breaches or cyberattacks. Organizations employ incident response protocols to quickly identify, contain, and mitigate threats to digital assets. Effective incident response often relies on swift digital investigation methodologies that enable teams to recover compromised data and assess the extent of damage.

Given the rapid increase in mobile device usage, mobile forensics has emerged as a specialized branch of digital forensics in India. This involves recovering and analyzing data from mobile devices, such as smartphones and tablets, often applying unique techniques due to the distinct data management practices used in these devices. Mobile forensics is essential for numerous investigations, including those involving criminal activities, fraud, and intellectual property disputes.

The methodologies of digital forensics in India must adhere to legal standards and ethical guidelines to maintain the integrity and admissibility of digital evidence. Practitioners must be aware of regulations governing digital evidence collection and ensure compliance with laws

related to privacy and data protection. Addressing these legal challenges is critical for maintaining public trust in the digital forensics process. As technology evolves, so too must the methodologies employed in digital forensics. The rising sophistication of cyber threats requires ongoing innovation in forensic tools and techniques. Additionally, challenges such as the need for skilled personnel, the development of standardized protocols, and addressing jurisdictional complexities in cybercrime will influence the future landscape of digital forensics in India.

The methodologies in digital forensics are vital for effective investigations in the face of rising cybercrime in India. With a structured approach that includes data collection, preservation, examination, analysis, and incident response, stakeholders must continue to refine these methodologies. Emphasizing training, resources, legal compliance, and the integration of advanced technologies will strengthen the field of digital forensics, ensuring that it can effectively address emerging challenges in the digital landscape.

Impact on Criminal Investigations

Digital forensics has emerged as a pivotal component in the criminal justice system of India, significantly influencing the manner in which criminal investigations are conducted. As cybercrime becomes increasingly sophisticated, the importance of digital forensics in collecting, analyzing, and presenting digital evidence cannot be overstated. This report outlines the impact of digital forensics on criminal investigations in India, examining its methodologies, legal implications, and the challenges that lie ahead. The supreme court held in the leading case;

"…the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85-A, 85-B, 85-C, 88-A and 90-A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence."[9]

Digital forensics plays a crucial role in modern criminal investigations by providing law enforcement agencies with the ability to recover and analyze data from various digital devices.

[9] BODALA MURALI KRISHNA VS. SMT. BODALA PRATHIMA (2007 (2) ALD 72)

The scientific methods employed in digital forensics allow investigators to gather evidence systematically, which is essential for building strong cases against suspects. This is particularly vital in cases involving cybercrimes, where traditional investigation methods may fall short due to the nature of digital evidence. The integration of digital forensics into the criminal justice process has enhanced the efficiency and transparency of investigations. Recent legal reforms, particularly the introduction of the Bhartiya Nyay Sanhita (BNS) and its provisions surrounding audio-video technology, have modernized how evidence is collected and preserved. These changes aim to streamline judicial procedures and improve the overall efficacy of law enforcement responses to crimes.

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) establishes the framework for the admissibility of electronic records in Indian legal proceedings. This section not only outlines the conditions for accepting electronic evidence but also introduces stringent requirements for certification, thereby modernizing and expanding the scope of evidence law in the digital age.

Section 63 delineates the conditions under which electronic records can be considered admissible in court. It states that an electronic record, when stored in either electronic form or printed on paper, is deemed a document if specific criteria are met5. This provision marks a significant step in aligning legal frameworks with modern technological practices.

A notable aspect of Section 63 is the requirement for a special certificate to accompany electronic records. This certificate must be provided by both the party presenting the electronic records and an expert, ensuring a higher standard of verification2. The certification process aims to bolster the credibility of electronic evidence, addressing potential issues related to data integrity.

The BSA broadens the definition of electronic records compared to previous laws. It encompasses not just traditional computers but also any communication devices, reflecting the diverse range of technologies available today. This inclusive definition is essential for adapting to the complexities of collecting digital evidence in a rapidly evolving technological landscape.

Section 63(4) introduces a standardized format for the certificate outlined in the BSA's Schedule. This consistency in documentation is expected to enhance the clarity and efficiency

of admissions of electronic evidence in courts5. Proper format and information are critical for establishing the authenticity of electronic records presented before the judiciary.

The provisions in Section 63 signify a critical evolution in evidentiary law in India. By ensuring that electronic records can hold the same legal weight as traditional documentation, the BSA seeks to improve the justice delivery system, particularly in cases involving significant digital evidence3. This evolution not only streamlines legal processes but also prepares the judicial framework to address future challenges posed by technological advancements.[10]

While the advancements in digital forensics have positively impacted criminal investigations, legal challenges remain. The admissibility of digital evidence in court has been a contentious issue, as highlighted by landmark cases that have set important precedents. For example, the requirement for certificates under Section 65B of the Indian Evidence Act emphasizes the need for digital records to meet stringent legal standards6. However, there is a continuous need for law enforcement agencies to stay updated on legal requirements related to digital evidence.

Despite its significance, the implementation of digital forensics in India faces several challenges. These include a lack of adequate digital forensic laboratories, insufficient trained personnel, and limited public awareness regarding the importance of digital evidence in criminal investigations3. Establishing a robust framework for digital forensics requires investment in training and resources to meet the growing demands of cybercrime investigations.

Digital forensics is especially significant in investigating cybercrimes, which have risen dramatically in recent years. In 2022, the Indian Computer Emergency Response Team reported approximately 1.4 million cybersecurity incidents, underscoring the urgent need for effective digital forensic methods7. By utilizing forensics, investigators can quickly identify and trace cybercriminals, thereby enhancing the ability to prosecute such crimes successfully.

Looking ahead, the future of digital forensics in India will be shaped by ongoing technological advancements and the increasing complexity of digital crimes. Collaborative efforts between law enforcement, academia, and the private sector will be crucial to foster innovation and

[10] Section 63 of the Bharatiya Sakshya Adhiniyam

address emerging threats6. As India continues to digitalize, building capabilities in digital forensics will be essential for maintaining effective law enforcement and judicial processes.

In conclusion, digital forensics has made a significant impact on criminal investigations in India by enhancing the collection and analysis of digital evidence. Ongoing investments in digital forensic capabilities, legal reforms, and public education will be vital in addressing the challenges that persist. By empowering law enforcement with the necessary tools and knowledge, India can improve its responses to digital crimes and uphold justice in the digital age.

Digital Forensics in India

Digital forensics in India is increasingly vital as cybercrime rises, yet several challenges hinder its effectiveness. These challenges include inadequate infrastructure, a lack of trained personnel, legal complexities, and the evolving nature of technology. Addressing these issues is crucial for improving the digital forensics landscape and enhancing law enforcement capabilities.

One of the primary challenges faced in digital forensics is the lack of adequate infrastructure. Many Indian states do not have sufficient resources or facilities to conduct thorough forensic examinations. This results in delayed investigations and compromises the quality of digital evidence collection and analysis. Establishing robust digital forensics laboratories equipped with modern tools and technologies is essential for overcoming this challenge and improving investigative outcomes.

The shortage of trained digital forensics professionals remains a significant barrier to effective investigations. As the field of digital forensics evolves, the demand for specialists who are well-versed in the latest techniques and technologies is growing2. However, the current workforce often lacks the necessary skills and training, causing a backlog in investigations and reducing the overall efficiency of law enforcement agencies2. Focused training programs and initiatives are required to build capacity in this domain.

The legal landscape surrounding digital forensics in India can be confusing and complicated. There are numerous regulations and requirements that govern the admissibility of digital

evidence in court, particularly under Section 65B of the Indian Evidence Act3. The necessity for a proper certificate for electronic records adds an additional layer of complexity, which can impede timely justice3. Law enforcement agencies and legal professionals must be well-informed about these legalities to ensure that digital evidence is handled appropriately.

The pace at which technology is advancing presents a significant hurdle for digital forensics. Cybercriminals continually adapt to new tools and methods, making it challenging for law enforcement to keep up. The evolving nature of digital devices and the internet complicates the search for digital evidence, as novel types of data and communication platforms emerge regularly1. Ongoing investments in research and development are essential to stay ahead in the fight against cybercrime.

Privacy Concerns

Privacy issues arise in digital forensics due to the potential for invasive investigative practices. As forensic techniques become more sophisticated, there are concerns regarding consent, data protection, and the ethical implications of data collection3. Striking a balance between thorough investigations and respecting individual privacy rights is critical to maintaining public trust and ensuring compliance with legal standards.

Effective digital forensics often requires collaboration among various law enforcement agencies at the local, state, and national levels. Coordination between these entities can be poor, leading to inefficient sharing of information and resources. Establishing clear communication channels, shared protocols, and collaborative frameworks for digital forensic investigations will enhance overall effectiveness and timeliness in dealing with cybercrime.

Finally, financial constraints play a significant role in the challenges of digital forensics in India. Many organizations struggle to allocate sufficient budgets for advanced forensic technologies and training for personnel2. Greater funding from government and private sectors is necessary to build capacity and equip law enforcement agencies with the tools needed to effectively combat cyber threats.

Addressing these challenges will require a concerted effort from the Indian government, law enforcement agencies, and the private sector. By investing in infrastructure, training, legal

clarity, and technology adaptation, India can significantly enhance its digital forensics capabilities and improve the handling of cybercrime investigations.