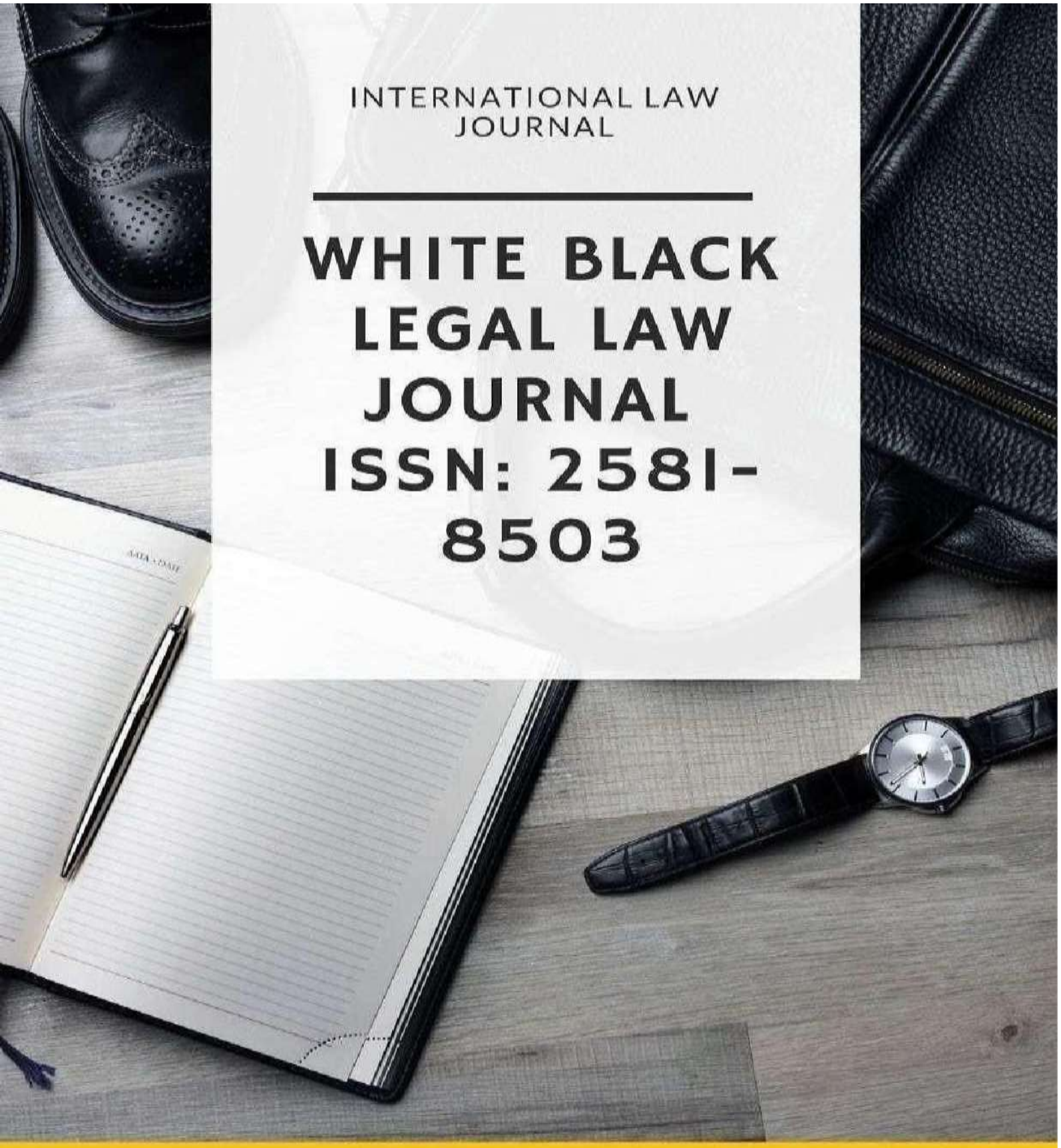

INTERNATIONAL LAW JOURNAL

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

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK LEGAL

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

INDIA'S CHALLENGES WITH DIGITAL EVIDENCE PRESERVATION AND INTEGRITY

AUTHORED BY: SANJANAA A M
2250562
5 BBA LLB B

ABSTRACT:

Digital evidence is getting prime importance in the Indian legal structure. However, the various challenges associated with the preservation of digital evidence and its integrity make such utilization of digital evidence in judicial proceedings a challenge. This paper addresses the problems related to digital evidence in India in respect of preservation and integrity of such evidence and suggests potential solutions to such issues. This discussion commences with the assertion that digital evidence per se is volatile in nature, which automatically means that it can easily be tampered with or destroyed. Additionally, it postulates that the amount of digital evidence produced and its complexity raise tremendous challenges in its safe and reliable preservation and management. Next, it explores the different risks to digital evidence integrity which cut across intentional manipulation by perpetrators, accidental alteration based on human error or malfunctioning of software/hardware, and no integrated system of managing digital evidence. The paper concludes by proposing strategies to address the problems associated with the integrity of preserving digital evidence. These include the development of a clear and comprehensive digital evidence preservation policy, the deployment of appropriate preservation tools and techniques, education of staff in the right collection, preservation, and analysis of digital evidence, and effective management of digital evidence.

I. Introduction

Digital evidence plays a crucial role in modern Indian legal jurisprudence. With the rise in crimes committed through digital devices and technologies, the necessity for collecting, preserving, and analyzing digital evidence has increased. However, its admissibility in court is challenged by issues related to its preservation and integrity. Digital evidence differs from traditional forms of evidence because it is highly volatile, susceptible to tampering, and can be manipulated remotely.

The rapid advancement of technology has made digital evidence an essential component in criminal and civil cases, ranging from cybercrimes and financial fraud to intellectual property disputes and terrorism investigations. As digital evidence can originate from multiple sources, such as emails, social media, surveillance footage, and encrypted communications, its management requires expertise in digital forensics. The effectiveness of digital evidence depends on its authenticity, proper documentation, and compliance with legal standards. However, due to the lack of a standardized framework and sufficient forensic infrastructure in India, law enforcement agencies face multiple challenges in ensuring its credibility.

Another significant concern in India is the legal and procedural complexity surrounding digital evidence. The legal system must adapt to the growing number of digital crimes while ensuring that evidence is collected, preserved, and presented in a legally sound manner. The absence of dedicated digital evidence management laws and a lack of awareness among legal professionals further complicate the situation. Additionally, cybercriminals continuously evolve their techniques to bypass security measures, making it difficult for investigators to keep up with emerging threats.

Law enforcement agencies in India often struggle with accessing digital evidence stored on servers located in foreign jurisdictions. Due to data protection laws in other countries, obtaining critical evidence requires international cooperation and time-consuming legal procedures, which can lead to delays in criminal investigations. Moreover, the lack of trained forensic professionals and advanced forensic tools further exacerbates the challenges faced in handling digital evidence efficiently.

The importance of digital evidence preservation cannot be overstated. Ensuring that digital evidence remains untampered and reliable is critical for upholding justice. A failure to preserve digital evidence adequately can lead to wrongful convictions or the acquittal of guilty individuals. Therefore, India must adopt global best practices in digital forensics, invest in technological advancements, and create a specialized workforce dedicated to handling digital evidence effectively.

Given these challenges, this paper aims to analyze the factors restricting proper digital evidence preservation in India and explore solutions to strengthen digital forensic practices. By addressing technological, legal, and human-related challenges, this study provides

recommendations for necessary reforms to enhance the digital evidence management system in India.

II. Challenges Of Digital Evidence Preservation

This often makes digital evidence a great challenge to preserve since it has an intrinsic propensity to become changed or lost due to evil or accidental circumstances. For instance, if a digital device is shut down or disconnected, unsaved data may be lost forever. Digital evidence may also become corrupted due to malware or other software malfunction. Another crucial concern in preserving digital evidence is the sheer volume of data. The mass production and storage of digital information compound this complicated task of maintaining evidence securely and reliably. Lastly, preserving digital evidence is complex and labor-intensive, involving a great deal of knowledge about digital technology as well as the ability to apply specific forensic tools and techniques.[1]

III. Challenges Of Digital Evidence Integrity

Digital evidence integrity means that no digital evidence is compromised or altered in any manner. The integrity of digital evidence assumes great importance since any compromise on the integrity of digital evidence may automatically rule it out for its use in court. Integrity of digital evidence is subjected to numerous challenges among which are alteration of digital evidence by criminals to destroy evidence of their crimes by either intentional change or addition to the evidence. Digital evidence can also become corrupted unintentionally due to human error or failure of software or hardware. It must be acknowledged here that the preservational and integrity challenges in digital evidence are not unique to India. However, there are specific challenges being faced in the Indian context. Digital evidence integrity faces threats such as:

1. Intentional alteration by criminals to destroy or manipulate evidence.
2. Accidental corruption due to human error or software/hardware failure.
3. The lack of uniform digital evidence standards across India, given its vast and diverse population.
4. Limited resources and expertise in India's relatively immature digital forensics ecosystem.

[1] Chawla, S. (2020). Digital Forensics in India: Challenges and Opportunities. Indian Journal of Law and Technology, 11(2), 11-22.

5. Advances in encryption techniques and anonymization tools make digital evidence difficult to access and verify.

For example, the case of India shows a very heterogeneous and broad population. In some situations, uniform digital evidence preservation and integrity standards may be very difficult to develop and enforce within such a vast population. The digital forensics ecosystem in India is still relatively immature in comparison to others, hence accessing necessary resources and expertise becomes very challenging.[2]

IV. Technological Challenges in Digital Evidence Preservation

When digital evidence is presented, the technological challenges involved are continually changing too. Some of the technological challenges include:

a. **Volatility:** Digital evidence is most times volatile as it would be very easy to modify or even destroy. This is brought about by many causes, such as power outages, system crashes, or malware infections.
b. **Volume:** Digital evidence is usually large, thus challenging to store and handle. For example, in cases involving more than one device or several video or audio recordings, this is problematic.
c. **Complexity**: Digital evidence can be very complex and difficult for anyone to understand, even the best forensic investigators. It results from the wide variety of digital devices and technologies available.
d. **Data Encryption**: The widespread use of encryption makes it difficult for forensic experts to extract and verify critical information without proper decryption methods.
e. **Cloud Storage and Remote Access**: The reliance on cloud services means evidence may be stored across multiple jurisdictions, complicating retrieval and legal access procedures.

V. Legal and Procedural Challenges in Digital Evidence Preservation:

Apart from these technical challenges, the preservation of digital evidence also faces a number of other legal and procedural challenges. Some of these include the following:

[2] Gupta, M. (2021). Challenges of Digital Evidence Preservation in India. Journal of Digital Forensics, Security, and Law, 16(2), 79-90.

1. Jurisdiction: Jurisdictional issues further complicate digital evidence preservation. As digital evidence is often stored on servers located in different countries or regions, law enforcement agencies may encounter significant delays in obtaining the necessary warrants or legal permissions to retrieve data from foreign jurisdictions. International legal cooperation and mutual agreements, such as those outlined in conventions like the Budapest Convention, are vital but time-consuming, and they introduce additional hurdles to investigations.
2. Privacy: Privacy concerns also pose a significant challenge when it comes to digital evidence. Since digital evidence often involves private or sensitive information, law enforcement must balance the need to preserve evidence with the rights of individuals to maintain their privacy. The challenge lies in ensuring that the collection and handling of digital evidence comply with privacy regulations without compromising the integrity of the evidence itself.
3. Admissibility: Electronically collected evidence should be collected and preserved in a proper manner within the court environment. The problem lies therein that the evidence is voluminous or assumes a very complex form.

VI. Human Factors in Digital Evidence Preservation

Human error remains one of the most significant threats to the integrity of digital evidence. Law enforcement personnel and forensic investigators may unintentionally alter, destroy, or mishandle digital evidence due to a lack of training or unfamiliarity with the necessary procedures. The absence of standardized protocols for handling digital evidence further increases the risk of mistakes. Inadequate awareness about the importance of maintaining an unbroken chain of custody can also lead to the contamination of evidence. Some significant human-related factors responsible for such mistakes are as follows:

a. **Lack of training**: The preservation process of digital evidence requires a specific skill set and expertise. In the absence of proper training, investigators may commit some unintended errors to compromise the integrity of the evidence themselves.
b. **Ineffective procedure:** Through the lack of proper and well-identified procedures, investigators may make error in collecting, preserving, or even in analyzing digital evidence.

c. **Neglect oversight:** Neglect oversight refers to a failure to preserve digital evidence due to acts or omissions, for example, lack of resources, time constraints, among others may cause one not to preserve digital evidence through negligence of the investigators.

As such, digital evidence integrity is very important since digital evidence cannot be accepted in court as well as relied upon for conviction unless it is maintained in integrity. Digital evidence integrity ensures that the evidence remains unchanged and not tampered with in any manner.

Authentication and Chain of Custody: Among the most integral elements in ensuring the quality of digital evidence is authentication and chain of custody. Authentication is the verification process undertaken to establish the validity of the digital evidence and guarantees that it is accurately defined as it seems. Chain of custody refers to a comprehensive record of handling the evidence from when it was gathered up to the time it is brought to court.

Vulnerability to Tampering and Admissibility Issues: Digital evidence is susceptible to both intentional as well as accidental changes. A criminal may intentionally change the evidence to cover up his or her activities, whereas accidental changes can be caused due to human errors, software malfunctions, and hardware malfunctions. If evidence is suspected of tampering, it risks being dismissed in the court of law as it might prove unreliable.[3]

VII. Real-Life Examples of Effective Digital Evidence Preservation In India

In India, several real-life cases have highlighted how digital evidence preservation techniques have been effectively used by law enforcement agencies to ensure justice. These cases exemplify the importance of proper evidence handling, the use of modern forensic tools, and adherence to best practices in preserving digital evidence for judicial use. Some of the practical cases that illustrate digital evidence preservation in India are given below:

a. **The Mumbai terror attacks of 2010:** During the 2010 Mumbai terror attacks, digital evidence was central to identifying and prosecuting the perpetrators. In response, the National Investigation Agency (NIA) was formed to handle terrorism-related offenses. The NIA used advanced digital forensic methods to preserve and analyze data from devices such as mobile phones, laptops, and intercepted communications. These tools ensured that vital evidence, such as emails and phone records, was recovered from

[3] Forensic Science Association of India (FSAI). (2019). Digital Forensics Standards and Guidelines. FSAI.

encrypted or damaged devices. This digital evidence was instrumental in linking the attackers to the plot, leading to successful convictions. The NIA's use of digital forensics set a precedent in counter-terrorism investigations in India.

b. **The ISRO espionage case:** In 2013, a case involving the Indian Space Research Organisation (ISRO) became another prominent example of the use of digital evidence preservation in India. Several scientists and engineers from ISRO were arrested by the Central Bureau of Investigation (CBI) on charges of espionage. The accused were allegedly involved in leaking sensitive information related to India's space technology to foreign entities. The CBI's investigation into the espionage ring required meticulous handling of digital evidence. The agency used a variety of digital forensic methods to gather evidence from the personal computers and mobile devices of the accused. This evidence included emails, chat logs, encrypted files, and digital traces that confirmed the illicit sharing of classified information. Specialized software tools were employed to extract data from the devices while ensuring that the integrity of the evidence remained intact. In particular, the CBI utilized data recovery techniques that could access hidden or deleted files on the devices, further strengthening the case against the accused. The preservation of this digital evidence was crucial in linking the scientists to the espionage activities and led to the successful prosecution of the defendants.This case underscored the importance of using robust digital evidence preservation methods, as the reliance on digital forensics provided the hard evidence necessary to secure convictions in a high-stakes espionage case.

c. **2018 Kerala Floods**: During the 2018 Kerala floods, the Kerala Police used digital evidence preservation techniques to investigate crimes like looting and fraud. CCTV footage, mobile phone records, and digital devices were essential in documenting criminal activities. Despite challenges posed by flood damage to infrastructure, the police collaborated with forensic experts to ensure the integrity of collected data. Digital evidence helped identify and convict perpetrators, demonstrating how crucial proper preservation techniques are in post-disaster investigations.

VIII. Learnings from Successful Cases

The study of successful digital evidence preservation cases in India provides crucial insights into best practices and potential areas of improvement. Several high-profile cases have demonstrated how effective digital evidence management can significantly impact the outcome

of legal proceedings. From counter-terrorism to espionage and post-disaster crime solving, preserving digital evidence with integrity is essential for justice. By refining digital forensics protocols, investing in advanced tools, and training law enforcement, India can continue to strengthen its ability to handle digital evidence effectively in an increasingly digital world.

One such case is the Mumbai terror attacks of 2008, where digital evidence played a key role in identifying and prosecuting the perpetrators. The National Investigation Agency (NIA) utilized digital forensic techniques to recover data from mobile phones, emails, and surveillance footage, ensuring that all evidence was authenticated and properly preserved.

Similarly, in the ISRO espionage case, the Central Bureau of Investigation (CBI) leveraged digital forensic tools to extract evidence from computers and mobile devices, leading to successful prosecution. Another example is the Kerala floods of 2018, where law enforcement agencies used digital preservation techniques to document and investigate criminal activities such as looting and fraud during the disaster response. The following are some key learnings drawn from some of the successful cases in India related to digital evidence preservation:

A clear definition of digital evidence preservation policy: Either a basic one or a detailed policy is very much necessary to ensure that digital evidence is continuously collected, preserved, and analyzed in a valid manner.

Selection of appropriate tools and techniques of preserving digital evidence is important because different circumstances may require different tools and techniques in the process of digital evidence preservation.

Training investigators to Collect, Preserve, and Analyze Digital Evidence A knowledge of preservation techniques must be learned by an investigator in order to handle evidence such as digital evidence reliably and in a manner that is admissible in court.

There may be a need for collaboration by various agencies; some digital preservation is often successful by coordination between the law enforcement agencies, forensic labs, and sometimes others. Clearly outline communication and collaboration among all parties.

These insights will enable the organizations to preserve their digital evidence well, thus making

sure that any digital evidence that may be brought to the courts is admissible.

IX. Overcoming The Challenges:

There could be a wide range of actions taken to address the problems created by digital evidence preservation and integrity. Such a digital evidence preservation policy must clearly and comprehensively define the procedures undertaken in collecting, preserving, and analyzing digital evidence. It should identify the roles and responsibilities of different personnel involved in the lifecycle of the digital evidence. digital evidence preservation tools and techniques appropriate to the case. Tools and techniques in using these may ensure that digital evidence is collected and preserved in a secure manner. Thirdly, training personnel on proper collection, preservation, and analysis of digital evidence must be ensured. It should be done including digital forensic basics, use of digital preservation evidence tools and techniques, chain of custody, and so on. In the last, there should be a sound digital evidence management system. Such a system will provide an avenue for ensuring appropriate, secure, and reliable storage and management of digital evidence.[4]

X. Conclusion:

Addressing the challenges associated with digital evidence preservation and integrity is critical for ensuring the credibility of electronic evidence in judicial proceedings. The increasing reliance on digital evidence demands a robust legal and technological framework that guarantees its authenticity, reliability, and admissibility in court. The key obstacles, including technological vulnerabilities, jurisdictional complexities, human errors, and lack of standardized procedures, require a multi-pronged approach to resolution.

The successful preservation of digital evidence hinges on comprehensive policies that define best practices for data collection, storage, and analysis. Implementing advanced forensic tools and techniques helps mitigate risks related to tampering and data corruption. Furthermore, continuous training and education for law enforcement personnel, forensic experts, and legal professionals are crucial for enhancing digital evidence handling capabilities.

Collaboration among various agencies, including law enforcement bodies, forensic laboratories, and judiciary institutions, will facilitate the seamless integration of digital forensic

[4] Indian Law Institute. (2022). Digital Evidence Law in India: A Compendium. Indian Law Institute.

practices into the legal system. Additionally, adopting international best practices and developing a standardized framework for digital evidence management will strengthen India's forensic capabilities.

Despite the existing challenges, India's legal and forensic ecosystem is evolving to address digital evidence preservation concerns. Increased investments in technology, research, and training will be instrumental in overcoming current limitations. By implementing these measures, India can ensure that digital evidence remains a reliable and admissible source of information in legal proceedings, thereby strengthening the justice system in the digital age.

XI. References:

Chawla, S. (2020). Digital Forensics in India: Challenges and Opportunities. Indian Journal of Law and Technology, 11(2), 11-22.

Forensic Science Association of India (FSAI). (2019). Digital Forensics Standards and Guidelines. FSAI.

Gupta, M. (2021). Challenges of Digital Evidence Preservation in India. Journal of Digital Forensics, Security, and Law, 16(2), 79-90.

Indian Law Institute. (2022). Digital Evidence Law in India: A Compendium. Indian Law Institute.

WHITE BLACK LEGAL