INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

ELECTRONIC EVIDENCE, CYBER FORENSIC, AND INVESTIGATION PROCEDURE: A STUDY

AUTHORED BY - MANISHA & DR. POOJA SOOD

Abstract

The rise of cybercrime has necessitated the integration of electronic evidence into legal and investigative frameworks. This article explores the role of electronic evidence in cyber forensics and its critical contribution to modern investigation procedures. It examines the collection, preservation, and analysis of digital data, emphasizing its admissibility in court. Key challenges, including data integrity, chain of custody, and evolving technological complexities, are discussed to highlight the importance of adhering to robust protocols and standards. Additionally, the article evaluates the role of specialized tools and expertise in uncovering cybercrimes, such as hacking, identity theft, and data breaches. By aligning technological advancements with legal principles, the study underscores the significance of cyber forensics in ensuring justice in the digital age. Recommendations for improving investigation procedures and addressing future challenges are also provided.

Keywords: electronic evidence, cyber forensics, investigation procedure, digital evidence, chain of custody, data integrity, cybercrime investigation

INTRODUCTION

The social, economic, and political lives of people have changed dramatically in the twenty-first century due to digital technology and new communication technologies, which has resulted in a constant growth in welfare and state monitoring. Cyberspace information is being misused through computer-related and computer-focused crimes as a result of society's growing reliance on interactive computer services. Older crimes have vanished, while the most recent wave of cybercrime has limited the legal scope of the entire world to include things like drug sales, sexual abuse, and anonymity,[1] sale of bitcoin/ cryptocurrency, sale of forged

[1] Anonymity describes situations where the acting is a person be non-identifiable, unreachable, or untrackable. It is seen as a technique, or a way of realizing, a certain other values, such as privacy, or liberty.

 ISSN: 2582-6433

documents and counterfeit currency, sale of unlicensed firearms, hiring hit man[2], child pornography, gambling, hacking, hosting , mail, blogs, books, chat, directory, money laundering4 , insider trading, trade secrets, government secrets, celebrity sex pictures, corruption, proprietary source code, Industrial design like medicine or defense, zero day exploits, stolen database proof of tax evasion and military limited etc. . It is very important that the investigating agencies must comply with the legal procedure while collecting, preserving and analyzing evidence from computer, computer system and computer resources in order to ensure admissibility before the Court because of most of the documents, today, are either stored on or generated by computers, among which a variety of electronic data have been admitted in the Courtroom as evidence.[3] This includes contents of websites, e-mails, text messages, instant messages, digital photos, and enhanced images etc. On many occasions, the judiciary has been sceptical in admitting such evidence, expressing that there is a need of new standards to deal with the new evidence revolving such evidence. Under such circumstances, it would be appropriate to address the commonly raised issues by the Courts with regard to electronic evidence, such as, authentication, hearsay, and rule of best evidence etc. Unfortunately, the laws prior to the emergence of computer forensics are inadequate to assess the techniques used in computer systems.[4]

Therefore, the lack of adequate mechanism to appreciate the computer based evidence has resulted in poor admissibility of such evidence in the Court. The probative value of electronic evidence is a significant challenge in criminal investigation proceedings, from collection to production.[5] Electronic documents carry metadata, which is essential information about data, which may not be visible on the face or may be lost when converted to paper form. This metadata can be defined as information regarding document creation and modification or information created by the operating system or application about a file that allows it to be stored and retrieved at a later date. The transnational admissibility of electronic evidence is complicated by different positions of law on matters of evidence in different domestic jurisdictions. Electronic documents can be used as evidence to prove the truth of their contents or as real evidence to show the existence of the data or who had possession of the data. The

[2] A person (the accused) wants to kill another person and is looking for another person (the 'hitman') to murder the target in exchange for payment or reward.
[3] Dwyer, D.,"The Judicial Assessment of Expert Evidence," Cambridge University Press, 2008.
[4] Britz, M., "Computer Forensics and Cyber Crime: An Introduction, 2/e," Pearson Education India, 2009.
[5] Galves, F., & Galves, C., "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial," Crim. Just., 19, 37, 2004.

 ISSN: 2582-6433

cardinal rule of admissibility applies to both paper and electronic documents, requiring proof of relevance,[6] authenticity, and reliability. The issue of cybercrime is a global concern, with various online services such as Dropbox, Gmail, Google spreadsheet, AWS, and Flexi scale being used.[7] Outsourcing these services can lead to unauthorized access to data and third-party access, as well as the volatility of electronic data that can be altered, moved, or deleted within a short period. The major problems may be related to accessing computers and computer networks remotely, where criminal activity could be initiated in another country and result in consequences in some other countries. The Council of Europe Convention[8] provides measures for countries to empower their competent authorities to collect or record content data through technical means on their territory and compel service providers to do the same within their existing technical capability. The Strasbourg Convention aims to facilitate international cooperation and mutual assistance in investigating crime and tracking down, seizing, and confiscating proceeds from it.

G-7 members of the G7 countries emphasize the need for international cooperation and coordination to curb high-tech crimes and improve collaboration to increase the effectiveness of investigations and prosecutions of cybercrime. The G-8 conference in 2004 declared a unifying commitment to strengthen domestic laws to build up globally capacity to combat terrorist and criminal uses of the internet. A recent G-20 conference titled "Crime and Security in the Age of the Non-Fungible Token (NFT), Artificial Intelligence (AI) and Metaverse"[9] stated that no country or organization can combat cyber threats in isolation and that cooperation in the investigation of cross-border cyber crimes through joint efforts to build a "peaceful, secure, deterrent, and open" information and communication technology environment is extremely necessary today. In line with the United Nations Convention on the Criminal Use of Information and Communication Technology, speedy preservation, investigation, and co-ordination of evidences is essential. This chapter addresses the legal issues related to investigation, collection, preservation, and analysis of electronic evidence, as well as laws towards better institutional arrangements for effectively dealing with justice for those who are victimized in national and international jurisdictions.

[6] Ahmad, T., & Shweta, S., "Relevancy and Admissibility of Digital Evidence: A Comparative Study," International Journal of Law Management & Humanities, 2018.
[7] The issue of cybercrime is a global concern, with various online services such as Dropbox, Gmail, Google spreadsheet, AWS, and Flexi scale being used.
[8] Assembly, P., "Council of Europe. Financing of Political Parties," Recommendation, 1516, 2001.
[9] Jabotinsky, H. Y., "The Network Effects of International Crypto and DLT Regulation," Vanderbilt Journal of Transnational Law, 57(5), 2024.

 ISSN: 2582-6433

CYBER FORENCIC: MEANING AND CONCEPT

The term forensics roots from the Latin word, '*forensis*' which generally means 'forum for discussion' or find out the truth.[10] In modern days Forensic investigation uses various facets of Science coupled with Technology in the process of establishing facts in civil or criminal Courts of law. Forensic Science is the science that deals with analysis of physical evidence collected from all possible sources in which criminal and victim are associated with. The latest entrant in this field is cyber forensics. Cyber forensic, in narrow sense is a process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability. It deals with analysis of electronic evidence that is distributed across the large computer, computer network, computer system and other electronic devices. Cyber forensic in broadest sense is the scientific examination and analysis of data held on computer storage media for the purposes of presentation in a Court of law, together with the study of the legal aspects of computer use and misuse. Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence. Cyber forensics is a scientifically derived and proven method for preserving, collecting, validating, identifying, analyzing, interpreting, documenting, and presenting electronic evidence from digital sources.[11] It is used to facilitate or further the reconstruction of events found to be criminal or to anticipate unauthorized actions disruptive to planned operations. Cyber forensics involves the use of apt forensic tools and technical knowledge to recover electronic evidence within the contours of the rules of evidence, for it to be admissible before the Court of law. It is an electronic discovery technique used to determine and reveal technical criminal evidence, often involving electronic data storage extraction for legal purposes. In essence, cyber forensics is an archeological dig designed to uncover what happened on a specific hard drive, within a specific computer, during a specific period of time. It is the combination of law and science (computer science), focusing on real-time, online evidence gathering. Cyber forensics includes maintaining the integrity of data, continuity of data, secure collection of computer data, examination of data to determine details such as origin and content, collection and presentation of information about computer data and computer systems to courts of law, protection of computer data, and application of a country's laws to computer practice.

[10] Cooper, J. E., & Cooper, M. E., "Application of Forensic Science to Wildlife Investigations," Wildlife Forensic Investigation, 142-155, 2013.
[11] Marcella Jr, A., & Menendez, D. (2010). *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications.

 ISSN: 2582-6433

INVESTIGATION OF COMPUTER-RELATED CRIMES

In the digital age, computer-related crimes have become a growing concern, necessitating the development of advanced techniques and tools to investigate and handle electronic evidence effectively. Law enforcement agencies and digital forensic experts play a crucial role in tackling these crimes. Digital forensics involves the collection, analysis, and preservation of electronic evidence to support criminal investigations. Strict protocols are followed to ensure the integrity and admissibility of digital evidence in a court of law. Law enforcement agencies rely on skilled professionals specializing in computer forensics to extract valuable information from devices, trace online activities, and identify potential cybercriminals.

Cyber Forensics and Electronic Evidence: Cyber forensics is the systematic process of recovering, storing, analyzing, and presenting digital information. Electronic evidence, a product of this process[12], is crucial in criminal investigations due to the involvement of electronic devices and systems. It is generally admissible in many jurisdictions and is rooted in classic forensic principles. Cyber forensics is applied in both pure cybercrime cases and cyber facilitated incidents, as it is nearly impossible to encounter a crime without a digital dimension in today's information-technology-driven society. Electronic evidence is highly volatile and can be altered rapidly through computing-related activities. To ensure admissibility, courts must ensure the evidence conforms to established legal rules, is scientifically relevant, authentic, and reliable, and has been obtained legally. However, the fragility of electronic evidence, including the rapidly changing nature of technology, the fragility of the media on which data is stored, and the intangible nature of electronic data, make it vulnerable to claims of errors, accidental alteration, prejudicial interference, and fabrication. **The Role of Cyber Forensics in Cybercrime Investigation:** Cybercrime is increasing, leading to a need for cyber forensic experts in various industries and law enforcement agencies. These experts investigate encrypted data using various software and tools, using techniques based on the type of cybercrime. Tasks include recovering deleted files, cracking passwords, and identifying the source of security breaches[13]. The evidence is stored and translated for court or police examination. The aim is to preserve evidence in its original form for structured investigations. With the sophistication of crime, the judiciary has referred to the application of scientific

[12] Arshad, H., Jantan, A. B., & Abiodun, O. I., "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," Journal of Information Processing Systems, KIPS, 2018.
[13] Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L.,... & Bursztein, E., "Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2017.

 ISSN: 2582-6433

techniques in crime investigations, as traditional physical evidence may not be sufficient to prove facts beyond reasonable doubt. . In ***Tomaso Bruno and Anr.*** v**. *State of Uttar Pradesh***[14] , the Court observed that advancement of information technology and scientific temper must pervade the method of investigation. Electronic evidence was relevant to establish facts. Scientific and electronic evidence can be a great help to an investigating agency. In the case of ***Darshan T S*** v. ***State of Karnataka***[15] while highlighting on crucial issues relating to police reforms, the High Court of Karnataka held as follows: "Investigating a criminal case is not an easy or an ordinary work. It requires thorough professionalism and professionalism can be achieved only through effective training. Many offences have become Hi-tech, in the sense that mobile phones and electronic devices are used to hatch conspiracy and messages are sent through SMS and e-mail[16]. Electronic evidence plays a vital role in many cases. Seizure of hard discs, collection of call details and such other digital materials require thorough knowledge of Digital Forensic Science. Proof of such digital evidence requires stricter evidence as per Sections 65A and 65B of The Indian Evidence Act, 1872[17], now section 62 and 63 of The Bhartiya Sakshya Adhiniyam 2023.[18]

LAW RELATING TO INVESTIGATION IN INDIA

Investigation has been defined as, "includes all proceedings under this code for the collection of evidence conducted by police officer or by any person (other than magistrate) who is authorized by a magistrate in this behalf." Section 78 of the Information Technology Act, 2000 provides that: "Notwithstanding anything contained in The Bhartiya Nagrik Suraksha Sanhita, a police officer not below the rank of Inspector shall investigate any offence under this Act. Clause (3) of Section 80 of the Information Technology Act 2000[19]" clearly states that the provisions of the Code of Criminal Procedure, 1973 (2 of 1947),now The Bhartiya Nagrik Suraksha Sanhita shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry. search or arrest, made under this Section. Section 4(2) of Criminal Procedure Code, 1973,now in Bhartiya Nagrik Suraksha Sanhita, provides that offences under any other law shall also be investigated, inquired into tried or otherwise dealt according to the B.N.S.S. subject to any provisions applicable under special law. Now, the Information

[14] (2015) 7 SCC 178
[15] (2015). SCC 7706
[16] Minnaar, A. (2008). 'You've received a greeting e-card from...': the changing face of cybercrime e-mail spam scams. Acta Criminologica: African Journal of Criminology & Victimology, 2008(sed-2), 92-116.
[17] The Indian Evidence Act, 1872
[18] The Bhartiya Sakshya Adhiniyam 2023.
[19] Information Technology Act 2000

 ISSN: 2582-6433

Technology Act, 2000 which is the special law provides that notwithstanding anything contained in the B.N.S.S, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable. Cognizable offences are that which a Police Officer can investigate without warrant. A Police Officer also has authority to arrest the suspect of any such offence without warrant. It is distinct from non-cognizable offence as investigation of which can take place only after a warrant from a Magistrate. A Police Officer can arrest to suspect of only after obtaining a warrant from a Magistrate. Similarly, bailable offence means any offence which is shown in First Schedule of B.N.S.S. which is bailable by any other law for the time being enforced. While a bail can be claimed as a matter of right in case of bailable offence, grant of bail in case of non bailable offence depends upon the discretion of the Court.

CBI (Crime) Manual, 2005:

The Central Bureau of Investigation (hereinafter referred as CBI), established in 1963 by the Ministry of Home Affairs, Government of India as a prime investigating agency of the country dealing with investigation of crimes in India, and assist the State Police Forces in carrying out investigation. As far as cybercrime is concerned, the CBI has the following specialized structure to handle crimes:

- Cyber Crimes Research and Development Unit (CCRDU);
- Cyber Crime Investigation Cell (CCIC);
- Central Forensic Science Laboratory (CFSL); and
- Network Monitoring Centre.

Apart from search and seizure, the Manual has given an elaborate procedure for investigation of cybercrime in terms of handling of electronic evidence and computer hardware.

a) Cartridges or disk can be used for storage of copies of files from Computer, useful for investigation
b) Labeling of Evidence- Label cables, where they are plug in, disks, the various other parts of computer and to write /protect disks
c) Dismantle the hardware with screwdrivers other tools for the purpose of seizure
d) Use of Gloves- Often latest prints can be taken from disks or other storage hardware or media
e) Material needs for packing- Tapes, boxes, rubber bands, bubble wrap and if he does not have access to anti-static wrap then papers, bags can be used.
f) Recording Equipment- to video graph and taking photographs of the crime scene

 ISSN: 2582-6433

g) Custody of report sheets and other paper for inventories and seize evidence.

Cyber-crimes Investigation Cell (CCIC): The Cyber-crimes Investigation Cell (hereinafter referred as CCIC) was established in The CCIC was established in Sep. 1999, started functioning w.e.f. 3.3.2000. The CCIC has jurisdiction in all over the India. It acts as a part of division of economic offence. But it is also empowered to investigate all the cybercrimes under IT Act, 2000. CCIC also acts round the clock as Nodal point of contact Interpol to report cybercrimes in India.

Cybercrimes Research and Development Unit (CCRDU): It's the responsibility of Cybercrimes Research and Development Unit (hereinafter referred as CCRDU) to track the development and changes, which take place in ever changing area. It has the following functions:

a. To ensure cooperation and coordination with State Police forces.
b. To collect and compile the data of reported cybercrime cases to Police for investigation.
c. To coordinate with software experts in identification of areas, which require attention of State Police
d. To obtain the information of cybercrime cases reported in other countries and prepare a monthly cybercrime digest.

The Central Forensic Science Laboratory (CFSL): The Cyber Forensic Laboratories (hereinafter referred to as the CFSL) are one of the primary wings to provide cyber investigation services in India. It is an autonomous institution of the Ministry of Home Affairs, Government of India. It was established in 1968 to provide scientific support to law enforcement agencies in criminal investigations and to deliver expert opinion on various matters related to forensicscience including cyber forensics, forensic data revival, and electronic evidence detection. CFL could analyze the forensic data and recover electronic evidence while maintaining the veracity of the electronic evidence for detection and trial. The basic functions of the CFL are

- To find out and Scientific analysis of Digital Foot Print.
- To provide scientific analysis in support of the Crimes Investigation by Law enforcement Agencies and CBI.
- To assist on site for Computer seizure and search on request.

 ISSN: 2582-6433

- To provide consultation services for activities or investigations, where media analysis is probable as occurring.
- To provide expert testimony.
- Providing adequate Research and Development in Cyber Forensics.

To provide adequate research and development in cyber forensics. The information and analysis so collected can be used as evidence in Court of law.

Network Monitoring Centre of Cybercrime: The Network Monitoring Centre of cybercrime (hereinafter referred as NCCC) is an e-surveillance and cyber security project of Government of India. It has been classified to be a project of Indian government without a legal framework, which may be counterproductive as it may violate civil liberties and human rights.[20]

There were concerns that National Cyber Coordination Centre (NCCC) could possibly be abused for indulging in mass surveillance in India, privacy violation and civil liberty violations as agencies like NTRO (National Technical Research Organisation) and organisations like the National Security Council Secretariat are exempted from the applicability of any transparency law like Right to Information Act, 2000 Mass surveillance in India is not new as India already has e-surveillance projects like Central Monitoring System, NATGRID[21], and DRDO NETRA. Many, including legal experts, in India believe those intelligence agencies and their e surveillance projects require parliamentary oversight.

LEGAL REQUIREMENTS AND ASSESSMENT

Most jurisdictions have legal requirements that provide the grounds for admissibility of electronic evidence in legal proceedings.

(i) Legal Authorization: Assessing electronic evidence often requires legal authorization. Human rights, data protection and privacy impacts on accused parties and victims must be respected. Although there may be exceptions, the law generally provides safeguards for protecting the rights of individuals. Obtaining a legal authorization grants judicial legitimacy to the evidence in question; indeed, this may be the most important step in obtaining and handling electronic evidence. Search warrants are normally required to

[20] India's cyber protection body pushes ahead". *Hindustan Times*. January 29, 2019
[21]National Intelligence Grid (NATGRID) is the integrated intelligence master database structure for counterterrorism purpose connecting databases of various core security agencies under Government of India collecting comprehensive patterns procured from 21 different organizations that can be readily accessed by security agencies round the clock.

 ISSN: 2582-6433

seize electronic devices and electronic evidence. Failure to obtain a legal authorization may undermine the best evidence rule and jeopardize the case.

(ii) Electronic evidence Relevance: Relevance is an important determinant of electronic evidence admissibility. In order for evidence to be admissible, it must be "sufficiently relevant" to the facts at issue. Evidence cannot be admissible if it is not deemed to be relevant. For a piece of evidence to be deemed relevant in legal proceedings, it must tend to prove or disprove a fact in the proceedings. Evidence that has probative value must prove the fact in question to be more or less probable than it would be without the evidence.

(iii) Electronic evidence Authenticity: Authenticity is another important criterion that impacts the reliability of evidence. Electronic evidence to be admitted in a Court of law, there must be adduced evidence that the evidence in question is indeed what it is purported to be. For example, for a digital record to be admissible, the Court would have to be convinced that the record was indeed generated by the individual who is purported to have authored the record.

(iv) Electronic evidence Integrity: Integrity refers to the 'wholeness and soundness' of electronic evidence. Integrity also implies that the evidence is complete, unaltered and unmodified. An assessment of evidence integrity is a primary requirement for electronic evidence admissibility and serves as the basis for determining the weight of evidence. Electronic evidence integrity is not an absolute condition but a state of relationships.

(v) Electronic evidence Reliability: In order for evidence to be admissible in Court, the evidence must establish that no aspect of the evidence is suspected. There must be nothing that casts doubt about how the evidence was collected and subsequently handled. In particular, this celebrated case specifies five criteria for evaluating the reliability and by extension, the admissibility of electronic evidence:

a) whether the technique has been tested;
b) whether the technique has undergone peer review;
c) whether there is a known error rate associated with the technique;
d) whether standards controlling its operations exist and were maintained; and
e) whether the technique is generally accepted by the scientific community.

 ISSN: 2582-6433

(vi) Hash value: A 'hash value' is an electronic fingerprint. The data within a file is represented through the cryptographic algorithm as that hash value". Digital forensics professionals use hashing algorithms to generate hash values of the original files they use in the investigation. This ensures that the information isn't altered during the course of the investigation since various tools and techniques are involved in data analysis and evidence collection that can affect the data's integrity.

JUDICIAL STAND ON ADMISSIBILITY OF ELECTRONIC EVIDENCE

With the advancement of technology, the judiciary has also felt the need for giving recognition to use of tools and technology in the investigation of crimes. Through various pronouncements, the Courts have insisted on making the best use of technology in proving a case in accordance with The Indian Evidence Act, 1872. Upholding the importance of a proper investigation of computer related crimes, the judiciary has also recognized that a protocol in compliance with rules of evidence must be maintained by the law enforcement agencies throughout the process of identification, collection and preservation in order to avoid improper handling and collection of electronic evidence. Some of the judicial decisions relating to investigation of such crimes are discussed below to understand the challenges

In **CBI v. Ashok Pal Panwar**[22], the Delhi High Court emphasized that scientific evidence should not be overlooked casually and must be treated as correct and genuine unless contradicted by defense with convincing evidence. The court refused to accept electronic evidence due to its inappropriate handling and prejudicial nature. The court held that technology has advanced significantly, making it virtually a child's play to edit any electronic clip. It was therefore necessary to send such CD to a forensic laboratory to exclude any possibility of tampering. Electronic evidence is required to be handled with utmost care and caution, and there should not be any chance of prejudice to the accused due to inept handling of electronic evidence.

In **Vijesh v. The State of Kerala**[23], the Hon'ble Supreme Court provided clarity on the changing approach of the judiciary after notification. The court held that an examiner of electronic evidence need not prove their expertise in the said field in the Court of law. Once

[22] 2013 CriLJ4832.
[23] (2015) SCC 543

 ISSN: 2582-6433

notified, the expertise of the institution is recognized and established. However, in other cases, the expert who had examined the electronic evidence will have to prove his expertise in the Court of law. Such interpretation leaves a question mark on the credibility of the evidence, even if it is made by an examiner of electronic evidence. The court observed that maintaining the evidential continuity and integrity of the evidence that is copied is of paramount importance. The process of copying and handling such evidence should be carried out to the highest possible standards. In **Abdul Rahaman Kunji v. State of West Bengal**[24], the court observed the need for competent officers in cyber police stations. With the rise in crimes involving electronic communications, a competent officer from the Cyber Police Station must be inducted mandatorily into the investigating team immediately such a case arises. This would ensure that the originator of the electronic communication is nabbed swiftly and appropriate evidence is collected and led to prove the e-mails, telephone calls, or electronic messages during the trial of the case.

CONCLUSION AND SUGGESTIONS

In conclusion, electronic evidence plays an essential role in modern investigations, especially in the field of cyber forensics. As cybercrime continues to evolve, effective handling of digital evidence is crucial to ensuring justice. The challenges faced in maintaining the integrity of electronic evidence, preserving the chain of custody, and addressing privacy concerns require a consistent, thorough approach to forensic investigations. The adoption of specialized tools and continuous advancements in technology are necessary to keep pace with sophisticated cybercrimes. To improve the effectiveness of cyber forensic investigations, it is suggested that international standards for evidence collection and analysis be established, ensuring uniformity across borders. Additionally, ongoing training for forensic experts is essential to stay updated on emerging technologies and methods. Legal frameworks should be revisited regularly to accommodate new technological developments and safeguard the admissibility of digital evidence in court. Finally, greater collaboration between law enforcement, legal authorities, and cybersecurity experts will strengthen investigative procedures and ensure more effective responses to cybercrime. By addressing these aspects, the reliability and efficiency of cyber forensics can be enhanced, contributing to a more secure and just digital environment

[24] (2015) 1 Cal LT 318.

 ISSN: 2582-6433

BIBLIOGRAPHY

BOOKS AND RESEARCH PAPERS

1) Ahmad, T., & Shweta, S., "Relevancy and Admissibility of Digital Evidence: A Comparative Study," International Journal of Law Management & Humanities, 2018.
2) Arshad, H., Jantan, A. B., & Abiodun, O. I., "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," Journal of Information Processing Systems, KIPS, 2018.
3) Assembly, P., "Council of Europe. Financing of Political Parties," Recommendation, 1516, 2001.[1] Jabotinsky, H. Y., "The Network Effects of International Crypto and DLT Regulation," Vanderbilt Journal of Transnational Law, 57(5), 2024.
4) Britz, M., "Computer Forensics and Cyber Crime: An Introduction, 2/e," Pearson Education India, 2009.
5) Cooper, J. E., & Cooper, M. E., "Application of Forensic Science to Wildlife Investigations," Wildlife Forensic Investigation, 142-155, 2013.
6) Dwyer, D.,"The Judicial Assessment of Expert Evidence," Cambridge University Press, 2008.
7) Galves, F., & Galves, C., "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial," Crim. Just., 19, 37, 2004.
8) Marcella Jr, A., & Menendez, D. (2010). *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications.
9) Minnaar, A. (2008). 'You've received a greeting e-card from...': the changing face of cybercrime e-mail spam scams. Acta Criminologica: African Journal of Criminology & Victimology, 2008(sed-2), 92-116.
10) Mughal, A. A., "A Comprehensive Study of Practical Techniques and Methodologies in Incident-Based Approaches for Cyber Forensics," Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, 2(1), 1-18, 2019.
11) Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Bursztein, E., "Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2017.

 ISSN: 2582-6433

STATUTES

1) Information Technology Act 2000
2) The Bhartiya Nagrik Suraksha Sanhita
3) The Bhartiya Sakshya Adhiniyam 2023
4) The Indian Evidence Act, 1872