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

EVIDENCE IN DIGITAL ERA & FORENSIC SCIENCE

AUTHORED BY - RISHIKA SHRIVASTAV
STUDENT, LLM II SEM
Institute Of Law And Legal Studies Sage University Indore

GUIDED BY - DR. JAYSHREE NANDESHWAR
(Professor- Institute of Law & Legal Studies)

Abstract

The rapid advancement of digital technology has transformed the way crimes are committed, investigated, and prosecuted. Electronic devices and online platforms have become key sources of criminal evidence, from mobile data and emails to cloud storage and surveillance systems.

Digital evidence, however, is volatile, susceptible to tampering, and complex to analyze. This has led to the rise of digital forensics, focusing on the identification, extraction, preservation, and interpretation of electronic data for legal use. Challenges such as encryption, cross-border jurisdiction, and evolving cyber threats demand advanced tools, trained personnel, and policy reforms.

This study examines how forensic science is adapting to the digital era, emphasizing innovative techniques, legal frameworks, and inter-agency collaboration to ensure the integrity and admissibility of digital evidence.

Keywords: - Digital evidence, Forensic science, Indian Evidence Act, BNS2023, legal framework, Admissibility.

Introduction:-

In today's hyper-connected world, digital technology has revolutionized not only the way people communicate and transact but also how crimes are committed, detected, and prosecuted. From online banking fraud to cyber stalking and ransom ware attacks, the digital environment has given rise to sophisticated criminal behaviors that transcend geographical and legal boundaries. Consequently, digital evidence—including data from mobile phones, emails, cloud

ISSN: 2582-6433

storage, social media, surveillance systems, and even metadata—has become a cornerstone of modern criminal investigations.

However, this evidence is inherently fragile, volatile, and technically complex. Its admissibility in court depends not only on its authenticity and integrity but also on how it is identified, preserved, analyzed, and presented. This demand has catalyzed the development of digital forensics—a specialized branch of forensic science dedicated to the systematic handling of electronic data for legal purposes.

With rising encryption standards, massive data volumes, and jurisdictional complexities, investigators face unprecedented challenges. The UK's Digital Forensic Strategy 2022 emphasizes the urgent need for innovation, investment in skilled personnel, and collaborative frameworks between law enforcement, private sectors, and legal institutions. Additionally, emerging technologies like artificial intelligence, block chain, and cloud forensics are gradually transforming the forensic landscape.

This research explores how forensic science is adapting to the digital age by integrating scientific rigor, evolving legal standards, and technological advancements. It also addresses the critical balance between digital privacy and public safety, while highlighting the global efforts required to ensure the admissibility, reliability, and ethical use of digital evidence in the pursuit of justice.

Definition & characteristics of digital evidence

"Electronic evidence is any data resulting from the output of an analogue device and a digital device of potential value that is generated, processed, stored, or transmitted using any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format."

Under the ***Bhartiya Sakshya Adhiniyam,2023*** :- section 2(1)(e)-

- "Evidence means and includes- All statements including statements given electronically which the Court permits or requires to be made before it by witness in relation to matters of fact under inquiry and such statements are called **oral evidence**."
- "All documents including electronic or digital records produced for the inspection of the court and such documents are called **documentary evidence**."

ISSN: 2582-6433

***Council of Europe**:*

"Electronic evidence means any evidence obtained from data contained in or created by any device, the operation of which depends on software or data stored or transmitted through a computer system or network."

Egyptian Law No. 175 of 2018:

"Any electronic information that has a strength or proven value stored, transmitted, extracted, or acquired from computers, information networks, and the like, and that can be collected and analyzed by using special hardware, software, or technological applications."

Characteristics of Digital Evidence

1. **Scientific in Nature**:-Digital evidence is the result of scientific and technical processes. Its credibility depends on technical accuracy and logical validation.
2. **Fragile and Easily Tampered**:- It can be quickly deleted, altered, or damaged, making timely preservation essential.
3. **Diverse in Form**:- Digital evidence may include documents, images, emails, audio files, log files, GPS data, etc.
4. **Requires Expert Handling**:- Collection, preservation, and analysis need specialized skills in computer forensics and IT.
5. **Traceable**:- Contains metadata (timestamps, IP addresses, device IDs) which can help link it to suspects or events.
6. **Analytical in Nature**:- Can be used to reconstruct digital behavior, track activities, and identify motives or patterns.
7. **Legally Sensitive**:- Must be collected under proper legal authorization; else it may be ruled inadmissible in court.
8. **High Evidentiary Value**:- Once authenticated, it can serve as powerful proof in trials, often more detailed than traditional evidence.

Classification and Examples of Digital Evidence

Digital or electronic evidence can be classified according to various criteria, most notably based on the form of electronic data, method of creation, and purpose of generation.

1. **Classification by Form or Type of Electronic Data:-** Electronic evidence includes a wide range of digital formats, which are used in the investigation and prosecution of crimes committed using computer systems and the internet.

"Electronic evidence is an informative digital component that takes many forms, such as

ISSN: 2582-6433

writing, pictures, audio, and photographs, through which the crime, perpetrator, and victim can be linked."

Examples include:-

- **Written Data**: Documents created using word processors, emails, and mobile text messages.
- **Audio Recordings**: Voice messages stored on mobile phones or apps.
- **Photographs & Videos**: Digital images, CCTV footage, and other multimedia files.
- **Audiovisual Attachments**: Multimedia files embedded in or attached to emails.
- **Raw Data**: Unprocessed information such as log files, metadata, and system traces.
- **Monitoring System Data**: Data retrieved from network monitoring tools and server logs. Electronic Documents & Digital Signatures: Legally recognized files such as contracts, PDFs, and digitally signed documents.

2. ***Classification by Method of Creation:-***

As per the U.S. Department of Justice model (2002), electronic evidence can be:- Automatically Generated Records: e.g., log files, phone bills.

Processed Input Data: example:- Excel spreadsheets, using entered data. Stored Communication Records: e.g., saved chats, emails.

3. ***Classification by Purpose:-***

Intentionally Created as Evidence: Such as automated system logs or receipts. **Unintentionally Left Behind:-** Like browser history, temporary cache, or deleted files. "This type of digital evidence is unintentionally left behind by the perpetrator."

Challenges in Collecting Digital Evidence

"Extracting electronic evidence from crime scenes is considered a complex investigative work, especially considering the increase in digital criminal methods and the difficulty of tracing them. This requires specialized investigators and technical experts who can be used by the judge to uncover some clues that may remain ambiguous to him."

"Given the special nature of the electronic crime scene, the difficulties, and complex steps that the criminal investigator may face in this field, as the evidence is stored in electronic means, it can be manipulated and change the truth we seek to reach."

ISSN: 2582-6433

Preservation of Digital Evidence

- **General Digital Preservation:-**Preservation in the digital world: This requires the electronic technical expert to monitor and inspect the Internet site, or information that indicates the crime. The expert uses auxiliary software to achieve preservation, depending on the type of data.
- **Preservation Within a Computer:-** Preservation inside the computer: The process of preserving electronic evidence inside the computer is carried out in several ways, the simplest of which is represented by using the normal preservation method. Its strongest manifestations are in computer seizure operations on the evidence placed in it.
- **Preservation of Physical Media (CDs):-** Preserving compact discs (CD): Place the CD inside a plastic bag or inside a plastic box or cardboard cover. It is preferable to use nylon reinforced with air bubbles. And you must ensure that there are no scratches on it. A digital camera is used to photograph the disc, and the number of the seizure record, the name of the accused and the expert are written on it.

Analysis of Digital Evidence

To extract this evidence, the technical expert copies all the seized media, especially the hard disk, and then begins the process of searching for hidden and deleted files using special programs such as Recover Man Professional and Easy Recover. He can also uncover texts and images that are hidden from the general user's view, print them or store them on physical paper to be presented in court.

The expert also analyzes the IP address trail, the software used, and the location of the site hosting. In some cases, he may be able to identify the person who dealt with the computer and the means used in it, whether it was a telephone line, mobile phone, or modem.

1) *Expert Tools and Investigator Guidelines:-*

The expert must use a forensic station equipped with all the requirements of the work and has advanced capabilities and supported programs such as FTK and En Case, as well as programs to copy the hard disk, some of which copy the information and data at a speed of 7 gigabytes per minute. The expert must also use a write blocker, especially when he is unable to copy the disk, and must deal with cracking complex passwords using the Rainbow system. The expert may also use programs to control and detect deleted data and record all steps to maintain chain

ISSN: 2582-6433

of custody."

2) ***Securing and Storing Digital Evidence***

All electronic evidence must be stored in a safe place to prevent it from being tampered with, destroyed, or accessed by unauthorized persons. CDs and DVDs must be stored in a place free from moisture and heat, and care must be taken not to scratch them. It is preferable to store them in air bubble nylon or strong plastic boxes. Evidence must be sealed and written on with seizure details, expert name, and date of storage.

The Role and Challenges of Forensic Science

Forensic science plays a pivotal role in legal proceedings by applying scientific and technical methods for the identification, collection, analysis, and explanation of evidence. This multidisciplinary field encompasses a wide array of techniques and procedures aimed at providing empirical support to either accept or refute a hypothesis within the context of criminal justice. Over the years, forensic science has evolved with an ongoing pursuit of accuracy and reliability to uphold the principles of justice.

Role in Legal and Criminal Investigations

- **Evidence Handling:-** Forensic science is central to modern legal systems, as it supports evidence-based decision-making. It aids in the systematic identification, collection, and analysis of both physical and digital evidence for use in legal contexts. Scientific forensic methods are essential in preserving the authenticity and integrity of the evidence, which is a prerequisite for its admissibility in court.
- **Truth and Accountability:-** Forensic science has emerged as a "truth beacon," increasing transparency and accountability in the legal system. It not only aids in solving cold cases but also helps prevent wrongful convictions. The scientific validation of forensic methods enhances the reliability of criminal investigations and fosters public trust in the justice system.
- **Integration of Technology:-** In the age of digital transformation, forensic science continues to benefit from technological advances. Artificial Intelligence (AI), machine learning, and data analytics are now being integrated into forensic methodologies to overcome complexities, expedite evidence analysis, and deliver more accurate results. These innovations have significantly improved the effectiveness of forensic investigations.

ISSN: 2582-6433

Associated Challenges

- **Technological Advancement:-** While technology offers powerful tools for forensic science, it also presents new challenges. The fast-paced evolution of digital technologies necessitates continual updates in forensic tools and methodologies. This dynamism, though promising, creates gaps in standardization, tool reliability, and empirical validation.
- **Ethical Practice:-** Ethical concerns are a constant companion of forensic science. Practitioners must navigate issues related to privacy, consent, and the ethical use of sensitive information. Ensuring impartiality and objectivity in scientific testimony remains a cornerstone of the field.
- **Scientific Validation:-** Scientific validation is critical for the legal acceptance of forensic methods. Courts increasingly demand rigorous empirical support to confirm the accuracy and reliability of forensic techniques. The lack of standardized datasets and formal testing procedures limits the reproducibility of forensic findings, thereby undermining their legal credibility.
- **Adapting to New Complexities:-** The emergence of new subfields—such as cloud forensics, social media forensics, IoT forensics, and multimedia forensics—has complicated traditional practices. These domains introduce unique technical, legal, and procedural challenges, including data ownership, jurisdictional boundaries, authentication issues, and rapid data volatility.

Legal Framework and Admissibility in Court

Admissibility Standards of Expert and Scientific Evidence:-The admissibility of evidence, particularly scientific and expert testimony, is governed by structured standards in many jurisdictions. Two key legal benchmarks globally recognized are:

Frye Standard: Introduced in *Frye v. United States (1923),* this standard mandates that scientific evidence is admissible only if the method or principle on which it is based is "generally accepted" by the relevant scientific community.

Daubert Standard: Established in *Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993),* this U.S. standard expanded the criteria for admissibility.

It considers: Whether the theory or technique can be tested. Whether it has been peer-reviewed and published.

ISSN: 2582-6433

Known or potential error rates.

General acceptance in the scientific community.

In contrast to Frye, Daubert provides a more flexible, case-by-case analysis, placing the judge in the role of "gatekeeper" to assess the relevance and reliability of evidence.

Challenges in Admissibility of Digital Evidence

Modern legal systems face increasing complexities due to the growing volume of digital evidence.

- **Lack of Scientific Validation**: Digital forensic tools often lack empirical validation and standard error rates, which undermines their credibility in court.
- **Bias in Datasets**: In digital forensics, the absence of standardized datasets often leads to inconsistent outcomes, making results hard to reproduce or verify scientifically.
- **Anti-Forensic Techniques**: Offenders use techniques like data encryption, trail obfuscation, and file manipulation to evade forensic examination. This poses a serious challenge for courts in confirming the authenticity and reliability of such evidence.
- **Tool Reliability Issues:** Software bugs, lack of formal testing, and rapid tech evolution further complicate admissibility.

Indian Legal Framework: Digital Evidence and Admissibility

In India, admissibility is governed by the **Indian Evidence Act, 1872**, which was amended in 2000 to accommodate digital records via the Information Technology Act, 2000. Key sections include:

Section **65A** and **65B** of the Indian Evidence Act:

Section 65B lays down conditions for admissibility of electronic records.

To be admissible, the electronic evidence must be accompanied by a certificate under Section 65B(4) stating:-

The manner of production. Authenticity of the source. Details of the device used.

Case Law**:** ***Anwar P.V. v. P.K. Basheer (2014),*** the Supreme Court emphasized that without compliance with Section 65B, electronic records are inadmissible, regardless of their relevance.

Burden of Proof: The onus lies on the party submitting the electronic record to prove its authenticity, origin, and integrity.

ISSN: 2582-6433

Scientific Objectivity and Best Practices

Digital forensic techniques must align with objectivity, impartiality, and independence. Without empirical validation and peer review, such techniques may be rejected under both Daubert-like criteria and Indian legal expectations under **Section 45 (Expert Evidence).**

In India, expert evidence under **Section 45** of the Indian Evidence Act requires:

- Demonstration of the expert's credentials.
- Explanation of the scientific basis of the method.
- Relevance of the technique to the case.

Courts have discretion to accept or reject expert testimony if it fails to meet these conditions.

Role of Technology in Digital Evidence

In the modern era, technology plays a transformative role in criminal investigations, especially in the collection and analysis of digital evidence. As cybercrime becomes increasingly sophisticated, digital technology has become indispensable for law enforcement and legal professionals.

1. *Importance of Digital Evidence*

Digital evidence refers to any data stored or transmitted in digital form that may be used in legal proceedings. Unlike physical evidence, it exists in electronic media and requires specialized tools and methods for its extraction.

It includes:- Emails, chat logs, call records, Digital documents (Word, PDF, etc.), Multimedia content (images, videos, audios), Metadata and timestamps, Network traffic logs and user behavior.

This form of evidence can be more informative than physical traces, as it often provides a timeline and details about user activity, location, and intent.

2. *Scope and Devices Involved*

The scope of digital evidence is broad and continuously expanding. Digital forensic investigations now cover a wide range of devices and technologies:- Computers and laptops, Smart phones and tablets, USB drives, memory cards, and SSDs, Cloud platforms (Google Drive, Drop box, etc.),Social media platforms (Facebook, Instagram, Twitter) Internet of Things (IoT) devices (CCTV, smartwatches, etc.)These devices generate, store, and transmit data that can be crucial in criminal investigations.

ISSN: 2582-6433

3. ***Role of Technology at Crime Scenes***

Advanced technology is now used to:-Forensically clone hard drives without altering original data, Recover deleted or hidden files, Analyze data logs to recreate a sequence of events, Track user behavior through digital footprints, Extract data from encrypted or corrupted sources Technological tools help maintain the chain of custody, ensuring that evidence remains untampered and legally admissible.

4. ***Challenges with Emerging Technologies***

With the emergence of new technologies, digital forensics faces challenges such as:-

Cloud Forensics: Distributed storage, jurisdictional issues, and shared tenancy complicate evidence collection.

Social Media Forensics: Huge data volume, unstructured content, and difficulties in authentication.

IoT Forensics: Diverse, volatile, and decentralized data make acquisition and validation complex.

Encryption & Anti-forensics: Criminals use advanced encryption and anti-forensic tools to destroy or alter digital traces.

5. ***Scientific Validation and Admissibility***

Legal systems require digital evidence to meet scientific criteria such as: Known error rates, Peer-reviewed methodologies, General acceptance in the scientific community

Role of Digital Forensic Experts

Digital forensic experts are at the core of transforming raw electronic data into legally admissible evidence. Their expertise, tools, and investigative procedures are critical in handling cybercrimes, frauds, data breaches, and digital disputes.

1. Specialized Roles and Skills:- Digital forensic experts are trained to use specialized software to extract data without altering it retrieve deleted, encrypted, or hidden files analyze user behavior through data logs**,** authenticate and validate the integrity of digital evidence**,** maintain proper documentation and chain of custody they apply scientific methodologies to ensure the data can withstand legal scrutiny.

2. Responsibilities in Cybercrime Investigations:- Experts are involved in :-

ISSN: 2582-6433

- **Evidence Identification:** Locating relevant data across multiple devices and platforms.
- **Data Acquisition**: Imaging or extracting data using forensic tools.
- **Data Analysis**: Understanding patterns, content, and connections.
- **Legal Testimony**: Presenting findings in court as expert witnesses.

They help in linking suspects to activities such as financial fraud, online harassment, hacking, and digital impersonation.

3. Challenges in the Field:- Forensic experts encounter many challenges, such as:

- **Encrypted Devices**: Full-disk encryption blocks access to data even with court approval.
- **Anti-Forensic Techniques**: Methods that criminals use to mislead investigators or erase data.
- **Rapidly Evolving Technology**: New file systems, platforms (e.g., IoT, cloud), and devices.
- **Lack of Standards**: Absence of globally accepted SOPs or forensic validation metrics.

They also need to ensure their tools and methods meet Daubert criteria, which require the method to be testable, peer-reviewed, have known error rates, and be generally accepted.

4. Scientific and Legal Obligations:-Forensic experts must follow best practices as per ENFSI, NIST, and SWGDE guidelines be capable of clearly explaining complex digital evidence in simple terms demonstrate the scientific validity and accuracy of the tools and techniques they use maintain objectivity and neutrality, avoiding bias in interpretation.

5. Adapting to New Domains:- As fields like social media forensics, cloud investigations, multimedia authentication, and IoT analysis grow, forensic experts are expected to evolve continuously. They must update their skills and tools to manage new types of data and technologies.

Case Studies:-

Case study 1:-

Dr.Rajesh Talwar and Dr. Nupur Talwar V/s State of U.P. (2017)

(Popularly known as the Aarushi – Hemraj Murder Case)

The Aarushi–Hemraj double murder case is one of India's most high-profile investigations

ISSN: 2582-6433

where digital and forensic evidence played a crucial role. On the night of 15–16 May 2008, 14-year-old Aarushi Talwar was found murdered in her Noida home. The next day, the body of domestic help Hemraj was discovered on the terrace.

Key digital and forensic evidence included:

- Wi-Fi router logs, showing it was turned off at 3:43 a.m. and back on at 6:01 a.m., suggesting manual intervention during the suspected murder time.
- Call Detail Records (CDRs), which tracked Hemraj's missing phone to Nepal.
- Deleted photos from Aarushi's camera, later recovered by forensic experts, suggesting tampering.
- DNA analysis, which found traces of Hemraj's blood on a pillow at another staff member's home, initially overlooked due to a lab error.
- Tampered vaginal swab samples, indicating possible manipulation of biological evidence.

The investigation faced major challenges, including a compromised chain of custody, conflicting expert reports, and contamination of the crime scene. Though a CBI trial court convicted Aarushi's parents in 2013, the Allahabad High Court acquitted them in 2017, citing insufficient and unreliable evidence.

This case highlights the critical importance of digital evidence handling, proper forensic documentation, and adherence to legal standards such as Section 65B of the Indian Evidence Act. It remains a landmark example of how flawed investigation and mismanaged digital data can lead to miscarriage of justice.

Case Study 2:-

Avnish Bajaj V/s State (NCT of Delhi) 2001

(Sony Sambandh Cybercrime Case)

Title: First Indian Conviction Based on Electronic Evidence

In 2001, a female employee of Sony India Pvt. Ltd. began receiving obscene and threatening emails from a fake Yahoo! account. These messages disturbed her mental peace and damaged her professional image.

Sony filed a complaint with Delhi Police's Cyber Crime Cell. The police traced the emails to a Delhi cyber café. Although the café's register entries were incomplete, CCTV footage helped identify the suspect, Avnish Bajaj. Upon seizing his personal computer, forensic analysis confirmed that the Yahoo! account used to send the emails had been accessed from his device.

ISSN: 2582-6433

Key Digital Evidence:

- IP Address Tracking to the cyber café
- CCTV Footage for user identification
- Computer Forensics showing cached email data
- Yahoo! Logs linking account access.

This case became India's first conviction under the IT Act, 2000 based entirely on electronic evidence. It demonstrated the importance of cyber forensics and helped establish the admissibility of digital evidence in Indian courts.

Future Prospects and Innovation of Digital Evidence in Forensic Science

In an increasingly digitized world, **digital evidence** has emerged as a cornerstone in both criminal and civil investigations. The ability to trace, extract, analyze, and interpret electronic data has transformed how law enforcement approaches crimes, especially those committed or facilitated using digital means. As we look to the future, the domain of **digital forensics** faces a dual challenge: to adapt rapidly to technological advancements and to establish scientifically validated methods that ensure credibility and admissibility in court.

- **Social Media Forensics**:- Social media platforms have become treasure troves of information. Posts, images, location tags, and metadata serve as vital evidence. However, the extraction, validation, and admissibility of this evidence face technical and legal hurdles. Tools must be developed to **preserve authenticity**, maintain **chain of custody**, and handle **diverse data formats** across platforms like Facebook, Instagram, and Twitter.
- **Cloud Forensics**:- As data migrates to cloud environments, forensic investigators must grapple with the **multi-tenant, decentralized, and volatile** nature of cloud data. Traditional methods are inadequate, and new models such as **Digital Forensics- as-a-Service (DFaaS)** are proposed to provide scalable, secure forensic access to virtual storage and systems.
- **Encryption Challenges**:- Encryption ensures user privacy but poses a major obstacle to forensic access. While laws in some jurisdictions (e.g., the UK) allow authorities to demand encryption keys, others (e.g., the US) view such demands as a violation of constitutional rights. Furthermore, **default device encryption**, especially by manufacturers like Apple and Google, adds to the complexity of evidence acquisition. Innovations in **live system forensics** and **quantum computing** offer potential future

ISSN: 2582-6433

breakthroughs.

- **Internet of Things (IoT) Forensics**:- The proliferation of smart devices—from home security systems to connected vehicles—means that investigators must analyze data from **heterogeneous and continuously streaming** sources. IoT forensics raises unique concerns over **jurisdiction**, **data integrity**, and **chain of custody**, and currently lacks unified protocols for handling such evidence.
- **Multimedia Forensics**:- Images and videos are frequently used as evidence, especially from social platforms and surveillance systems. However, the **ease of manipulation** through editing software demands robust **authentication tools**. Future innovations must focus on developing **algorithms that distinguish legitimate edits from tampering**, ensuring reliability in court proceedings.

Barriers to Scientific Validation

Despite progress, **digital forensic science still struggles** with universal acceptance due to:- Lack of **standard datasets** for testing new tools. Absence of **established error rates**. Use of **anti-forensic tools** that obscure or manipulate data.

Fragmented legal and technical standards across jurisdictions.

These gaps hinder the scientific reliability and reproducibility of forensic methods, which are essential for courtroom admissibility.

Conclusion

In conclusion, digital evidence and forensic science have become indispensable pillars of the modern criminal justice system. As crimes increasingly shift to the digital domain, the demand for scientifically sound, legally admissible, and ethically handled electronic evidence continues to grow. Although digital forensics is still evolving, it plays a crucial role in defining, collecting, preserving, and presenting digital data in a manner that meets judicial scrutiny.

The future of justice in the digital era depends not only on technological tools but also on legal reform, inter-agency collaboration, and capacity building. To ensure that digital evidence maintains its relevance, authenticity, and impact in legal proceedings, it is essential to strengthen digital forensic capabilities and uphold the integrity of investigative processes. Only by integrating scientific methods with robust legal frameworks can we ensure a just and secure digital society.

ISSN: 2582-6433

References

1. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
2. Rogers, M. K. (2006). A Developmental Model for Digital Forensics. Digital Investigation, 3, 255–260. https://doi.org/10.1016/j.diin.2006.06.005
3. National Institute of Justice. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. U.S. Department of Justice.
4. Kessler, G. C. (2010). Judges' Awareness, Understanding, and Application of Digital Evidence. Digital Investigation, 7(2), 114–123. https://doi.org/10.1016/j.diin.2010.01.004
5. Casey, E., Ferraro, M., & Nguyen, L. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. Journal of Forensic Sciences, 54(6), 1353–1364. https://doi.org/10.1111/j.1556-4029.2009.01154.
6. Brenner, S. W. (2006). Cybercrime: Criminal Threats from Cyberspace. Praeger Security International.
7. NIST. (2020). NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1
8. Bharatiya Nyaya Sanhita (BNS), 2023. (2023). The Bharatiya Nyaya Sanhita, 2023. Ministry of Law and Justice, Government of India. Retrieved from https://legislative.gov.in (for latest provisions related to cyber crime, electronic evidence, and digital forensics)
9. Aarushi Murder Case: Dey, A. (2013). The Aarushi Case: The Anatomy of a Murder and the Making of a Media Trial. HarperCollins Publishers India.
   (Cited for insights on digital evidence including mobile records, emails, and computer use in forensic reconstruction of events.)
10. Sony Sambandh Digital Evidence Case:
    Sony Sambandh scam: Delhi Police unravel ₹12 crore online fraud using digital trail.