INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 13 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 13 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-13-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

INTEGRATING DIGITAL FORENSICS INTO INTELLECTUAL PROPERTY RIGHTS ENFORCEMENT: A FRAMEWORK FOR CYBERCRIME INVESTIGATION

AUTHOR - MADHURIKA DE* & DR. KABITA CHAKRABORTY**

* RESEARCH SCHOLAR, FACULTY OF LAW, ICFAI UNIVERSITY, TRIPURA

** PROFESSOR, FACULTY OF LAW, ICFAI UNIVERSITY, TRIPURA

BEST CITATION - MADHURIKA DE & DR. KABITA CHAKRABORTY, INTEGRATING DIGITAL FORENSICS INTO INTELLECTUAL PROPERTY RIGHTS ENFORCEMENT: A FRAMEWORK FOR CYBERCRIME INVESTIGATION, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (13) OF 2025, PG. 423-433, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

The rapid growth of digital technologies has intensified the incidence of intellectual property (IP) violations, including copyright infringement, trade secret theft, and digital piracy. Traditional enforcement mechanisms remain inadequate in addressing these crimes due to the complex, cross-border, and technologically advanced nature of modern cybercrime. This article proposes a comprehensive framework for integrating digital forensic practices into intellectual property rights (IPR) enforcement to enhance the investigation, prosecution, and adjudication of cyber-enabled IP offences. The proposed framework operates across three interconnected layers—technical, legal, and institutional—linking forensic readiness with IP protection strategies. It emphasizes forensic evidence acquisition, chain of custody preservation, and harmonization of legal standards to ensure admissibility and reliability of digital evidence. By aligning investigative procedures with judicial processes and policy mechanisms, the integration model strengthens cooperation among law enforcement agencies, IP offices, and cybersecurity institutions. The study highlights the need for standardized protocols, capacity building, and international collaboration to ensure effective digital enforcement of IPR in the evolving cyber ecosystem. Ultimately, integrating digital forensics into IP protection systems will advance transparency, accountability, and the overall resilience of global innovation frameworks.

KEY WORDS :- Cybercrime; Digital Evidence; Digital Forensics; Intellectual Property Rights (IPR); Legal Framework

I. Introduction

The twenty-first century has seen unparalleled digitization in the creation, management, and distribution of intellectual property. Digital platforms, cloud computing, and AI-driven tools revolutionized how creative and technological innovations are designed, distributed, and monetized across global markets[649]. Yet these same technologies have created an environment in which IPR has become increasingly susceptible to cyber-enabled infringements. Digital piracy, data exfiltration, trademark counterfeiting, and trade secret theft have increased in scale and sophistication,

[649]N. A. Rakha, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, Mexican Law Review, 16(2), 23–54 (2024)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

often perpetrated via encrypted networks, anonymization technologies, and transnational cyber infrastructures[650]. The rise of intangible criminality-where offenses occur within digital ecosystems devoid of physical evidence-presents a profound challenge to existing legal and enforcement mechanisms[651].

The economic and social impact of such crimes is enormous. According to recent studies, billions of dollars are lost by the global economy every year because of digital IP violations; this seriously undermines the incentive for innovation and distorts fair competition[652]. These infringements not only affect the legitimate rights of creators and businesses but also undermine consumer trust and national innovation policies. In exploiting these technological asymmetries, cybercriminals are able to evade traditional strategies of enforcement premised on territorial jurisdiction and tangible proof[653]. The legal architecture of IP protection, designed for the industrial era, has so far failed to effectively cope with the evidentiary challenges of the digital age, in which data is volatile, decentralized, and easily manipulated.

Among the central barriers to effective enforcement, the management of digital evidence represents a principal obstacle. The process of collecting, preserving, and authenticating electronic data requires specialized technical knowledge and strict adherence to forensic protocols[654]. However, in many jurisdictions, the enforcement agencies lack adequate forensic infrastructure and legal frameworks that ensure evidentiary integrity[655]. It is common for courts to face challenges in establishing the chain of custody regarding digital artifacts, often leading to admissibility and credibility challenges[656]. The lack of uniform standards, both nationally and internationally, further exacerbates the issue of cross-border cooperation in cybercrime investigations related to intellectual property theft[657].

In such a scenario, digital forensics comes into play as the essential element needed to fill the gap between technology and law. As a discipline, it introduces the methodological rigors required to transform electronic traces into admissible legal evidence[658]. Forensic techniques enable the investigator to identify, extract, and preserve data from digital media in a way that maintains the integrity and verifiability of the data[659]. These functionalities also play multiple roles within the context of IPR enforcement: establishing ownership and authorship, tracing infringing activities to their digital origins, and verifying the authenticity of evidence before judicial authorities[660]. Moreover, the concepts of forensic readiness allow an organization to take a proactive instead of a reactive approach toward the protection of intellectual property[661].

This paper argues that the inclusion of digital forensic methodologies in intellectual property enforcement frameworks is indispensable in protecting creative and technological innovations in a digitized world. It proposes a multi-tiered model that addresses the technical, legal, and institutional dimensions to ensure that forensic procedures meet the standards of procedural fairness, as well as international legal requirements. The proposed framework establishes forensic practices at each level of the IP enforcement cycle-from detection and investigation to prosecution and adjudication-enhancing evidentiary reliability, inter-agency cooperation, and global responses to cyber-enabled IP violations.

[650] C. Hegde, C. N. Sugali & L. A. Kumar, Digital Forensics for Safeguarding Intellectual Property Rights: A Study in the Context of Indian IPR Laws, Journal of Intellectual Property Rights, 29(6), 500–506 (2024)
[651] Digital Forensics in Intellectual Property Theft and Ethical Concerns, International Journal of Legal Science and Innovation, 3(2), 45–58 (2023),
[652] World Intellectual Property Organization (WIPO), World Intellectual Property Indicators 2023,
[653] Application of Digital Forensics in Cybercrime Investigations, Knowledge International Journal, 6(1), 1–14 (2023),
[654] National Institute of Standards and Technology (NIST), Guide to Integrating Forensic Techniques into Incident Response (Special Publication 800-86, 2006)
[655] Hegde, Sugali & Kumar, supra note 2.
[656] Digital Forensic Evidence in the Courtroom: Understanding Content and Quality, U.S. District Conference Paper (2014)
[657] Rakha, supra note 1.
[658] Digital Forensics and Media Offences – Investigate Synergy in the Cyber Age, Journal of Forensic Science and Research, 9(2), 88–97 (2024),
[659] NIST, supra note 6.
[660] IJLSI, supra note 3.
[661] Hegde et al., supra note 2.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Essentially, the use of digital forensics within IPR enforcement not only ensures the veracity of evidences but also retains the spirit of justice, due process, and innovation governance in an increasingly digitalized world.

II. Research Gap

This exponential growth in cybercrime has brought into sharp focus the vulnerability of IP assets in the digital domain, from trade secrets to copyrighted content, and from patented innovations to digital trademarks. While a great number of studies have looked either at digital forensics as an investigative science or at intellectual property rights (IPR) as a legal protection mechanism, the intersection between the disciplines remains insufficiently theorized and operationalized

The existing enforcement frameworks, including those under the World Intellectual Property Organization (WIPO) and the TRIPS Agreement, do not prescribe standardized forensic protocols for IP-related cyber incidents. Similarly, forensic standards, even though technically robust, are seldom integrated with legal evidentiary rules governing IP adjudication. This causes continuing enforcement gap whereby digital evidence lacks procedural admissibility and IP violations remain unprosecuted because of technical or jurisdictional deficiencies.

Therefore, this study identifies the critical lacuna in the alignment of forensic practice and IPR enforcement—a gap this research aims to fill with the help of an Integrated Forensic–IPR Enforcement Framework (IFIEF).

III. Research Objectives

The main objective of the study will be to design and validate a unified operational framework incorporating digital forensics in enforcing intellectual property rights. This is to be realized through the following specific objectives:

A. To assess the effectiveness of current intellectual property enforcement mechanisms in tackling digitally mediated infringements and evidence management.
B. To assess the available digital forensics frameworks in view of their suitability to the investigation into IP-related cases.
C. To design an Integrated Forensic–IPR Enforcement Framework (IFIEF) that harmonizes legal, technical, and procedural standards.
D. To propose institutional and policy recommendations for the implementation of forensic-integrated IPR enforcement at national and international levels.

IV. Research Methodology

This study employs a qualitative and doctrinal research methodology based on comparative legal analysis and normative synthesis. In this respect, the doctrinal aspect involves the critical analysis of primary legal sources, including international treaties like the WIPO, TRIPS, and Budapest Convention on Cybercrime; national statutes dealing with digital forensics and IP enforcement; and relevant judicial decisions.

V. Theoretical Framework

A. Understanding Digital Forensics in Cybercrime Investigations

Digital forensics has grown from a niche technical craft into a central pillar of contemporary criminal and civil adjudication. It may be defined as "the application of scientifically derived and proved methods for the identification, preservation, collection, validation, analysis, interpretation, documentation, and presentation of digital evidence in a manner that maintains its probative value".[662] Unlike traditional evidentiary disciplines that rely on physical artefacts, digital forensics operates in an environment characterized by volatility, duplication, and rapid data transformation. Every click, transaction, or transmission leaves an electronic footprint that can become legally

[662] NIST, supra note 6

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

significant-provided it is captured and preserved through validated methodologies.[663]

This practice generally follows four interdependent phases. First, there is the phase of identification, whereby all the possible sources of relevant data are identified, such as computers, mobile phones, servers, or network logs, and their forensic value is assessed. The second phase is that of preservation: once identified, the data should be secured with write-blockers, cryptographic hashes, and forensic imaging so that no alteration takes place. The third phase involves analysis, an interpretive stage where investigators use specialized software to reconstruct the digital events, detect anomalies, or identify links between different actors and artefacts. Finally, there is the presentation phase, where the findings need to be documented and communicated in an understandable way to non-technical audiences, for instance, judges and juries.[664]

The legitimacy of the discipline is based on its guarantee of integrity, authenticity, and chain of custody.[665] Courts regularly reject digital evidence when these principles are breached, since even minor procedural shortcomings may have a significant impact on reliability.[666] In cybercrime investigations, such evidence exists in temporary forms like temporary memory, cache files, or cloud data and thus can be erased or mutate in split seconds.[667] As Rakha 2024 says, "Digital forensics is the scientific link between technology and law, transforming intangible data into credible legal proof." Therefore, forensic standards not only ensure evidentiary fairness but also strengthen public trust in judicial verdicts being rendered on electronic evidence.[668]

B. Intellectual Property Rights and the Digital Challenge

Intellectual property rights are the legal scaffolding of innovation, ensuring that creators have exclusive control over their inventions, artistic expressions, and distinctive identifiers.[669] These include copyrights, patents, trademarks, industrial designs, and trade secrets, each offering protection for different manifestations of creativity and knowledge. However, these categories have become highly porous in the digital environment, as technological convergence blurs distinctions between tangible and intangible assets.[670]

The vulnerabilities of IPR in cyberspace are multifarious. Copyrighted digital media are replicated and globally distributed through peer-to-peer networks and streaming platforms, often beyond the reach of domestic legal systems. Patented innovations are susceptible to misappropriation through cyber-espionage, while trade secrets-related source code or confidential algorithms can be exfiltrated through unauthorized access or insider threats.[671] As Hegde, Sugali, and Kumar (2024) note, such infringements occur "in a jurisdictionally amorphous environment where the source, execution, and impact of the crime are seldom confined within national boundaries."[672]

Whereas technological advancements have complicated and enriched the evidentiary process, metadata analysis, blockchain verification, and digital watermarking now serve as tools of ownership authentication and infringement tracking.[673] Yet, the same innovations require new literacies in digital interpretation to be cultivated by courts and enforcement agencies.[674] The intersection of technology, data security, and ownership verification thus forms the core of the

[663] Rakha, supra note 1
[664] Hegde et al., supra note 2
[665] Digital Forensic Evidence in the Courtroom, supra note 8
[666] Rakha, supra note 1.
[667] Hegde et al., supra note 2
[668] Rakha, supra note 1
[669] World Intellectual Property Organization (WIPO), supra note 4
[670] Ibid.
[671] IJLSI, supra note 3
[672] Hegde et al., supra note 2.
[673] Digital Forensics and Media Offences – Investigate Synergy in the Cyber Age, supra note 10
[674] IJLSI, supra note 3.

contemporary IP debate. As open-access studies on digital forensics in intellectual property theft highlight, forensic science can provide a path to establishing digital provenance, proving unauthorized modification, and authenticating original content with mathematical certainty.[675]

In this regard, the integration of digital forensics into IP enforcement is not a peripheral reform but a jurisprudential necessity. It is only with digital forensics that infringement claims can be scientifically verified, thereby substantiating the moral and economic rationale underlying IP protection: namely, the assurance of recognition and recompense to creators for their work in an era of infinite replication.[676]

C. The Enforcement Gap: Bridging The Divide Between Legal Frameworks and Forensic Realities

Despite the spread of IP protection legislative frameworks, there remains a serious enforcement gap between normative aspirations and practical capabilities. Many jurisdictions have reached an advanced level from a statutory point of view but lack technical infrastructure and human expertise to deal effectively with the investigation of cyber-enabled IP crimes.[677] This makes enforcement reactive, fragmented, and technologically obsolete.

A critical component of this gap lies in the absence of forensic preparedness. Investigative agencies very often lack standardized digital evidence protocols, resulting in procedural inconsistencies and evidentiary contamination[678]. Courts, on the other hand, face the dilemma of assessing evidence gathered through non-forensic or extra-legal means. In many instances, electronic data, while probative, becomes inadmissible because the chain of custody cannot be established or because methods of acquisition have violated privacy or data-protection laws.[679] The judicial balancing in these areas-security, privacy, and justice-is becoming increasingly fragile in cyber-IP cases.

The jurisdictional fragmentation of digital enforcement further compounds the problem. Often, cyber-IP crimes traverse multiple sovereign domains in which an infringer might operate from one jurisdiction and utilize cloud servers located in another while targeting victims across several others.[680] Mutual legal assistance treaties (MLATs) and cross-border evidence-sharing frameworks remain narrow in scope and slow in operation.[681] The result is that there is an asymmetry in enforcement capacity: cyber-criminals can act with speed and across distance, but legal responses remain locally bound and bureaucratic.[682] Furthermore, tensions between data privacy and forensic necessity will persist. Strict regimes of data protection, while crucial to protect individual rights, tend to stand in the way of forensic evidence collection and international cooperation.[683] Without a balanced policy that harmonizes these imperatives, IP enforcement risks being ineffective in a borderless digital environment. Overcoming this enforcement gap requires a twin-track approach: forensic capacity-building and harmonization of legal norms that regulate digital evidence.[684] In this light, regional forensic networks, standardized protocols, and transnational IP-forensic partnerships could provide the infrastructure required to achieve it. Ultimately, embedding forensic competence within the architecture of IPR enforcement turns enforcement from a reactive posture into a resilient system that can address the fluidity of cybercrime.[685]

[675] Ibid
[676] Hegde et al., supra note 2
[677] Application of Digital Forensics in Cybercrime Investigations, supra note 5
[678] Digital Forensic Evidence in the Courtroom, supra note 8
[679] Rakha, supra note 1
[680] IJLSI, supra note 3
[681] World Intellectual Property Organization (WIPO), Cybercrime and Cross-Border Enforcement Challenges (2023)
[682] Hegde et al., supra note 2.
[683] NIST, supra note 7.
[684] Rakha, supra note 1.
[685] Hegde et al., supra note 2

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

D. The Need for Integration: Aligning Digital Forensics With Intellectual Property Rights Enforcement

The convergence of digital technologies and IP protection requires evolving enforcement mechanisms. Traditional IPRs, developed for tangible goods and localized infringements, now face cyber-enabled infractions that take advantage of anonymization, cloud storage, peer-to-peer networks, and global supply chains.[686] The lack of systematic inclusion of digital forensic processes in IPR enforcement continues to leave it vulnerable to evidentiary failure, procedural delays, and international enforcement gaps.

1. Why Synchronization Is Imperative?

IPR enforcement and digital forensics need to be aligned for a number of inter-locking reasons. In the first place, the nature of evidence in digital IPR offences is essentially electronic: metadata, logs, network traffic, cloud snapshots, firmware for embedded systems, etc.[687] Such evidence needs to be collected, preserved, and analyzed in such a way that it follows forensic best practices-including chain of custody, hash verification, forensic imaging, and expert annotation-so it can attain admissibility and persuasive value in court or administrative proceedings.[688] Without such forensic rigour, enforcement proceedings are at risk of collapse due to challenges over authenticity, alteration, or relevance.

The second point is that forensic integration supports proactive capabilities. Instead of mere reaction upon the occurrence of infringements, an enforcement system aligned with forensic readiness can monitor, detect, and intervene much earlier in the cycle of IP violation.[689]For example, in hardware-IP theft-such as semiconductor netlists-or digital media piracy, forensic traceability like watermark detection or network traffic capture enhances the speed and strength of enforcement action.[690]

Thirdly, the global nature of digital IPR violations makes forensic-legal alignment essential to cross-border cooperation. If evidence collection practices in one jurisdiction are not transparent, other jurisdictions may decline to recognize or admit such evidence, hence creating enforcement loopholes.[691] Harmonized forensic frameworks support mutual legal assistance based on evidence sharing and harmonized admissibility criteria.

2. Structural Deficiencies Undermining Effective Ipr Enforcement

(i) Fragmented Institutional Roles.

In most jurisdictions, IP offices, cybercrime units, forensic laboratories, and the judiciary operate in silos, each with its mandate, protocols, and technical capacities.[692]This fragmentation leads to duplication, delays, and gaps in the evidentiary chain. A good example is when a forensic lab collects data, but the IP regulatory office lacks training to interpret it, or the prosecutor lacks resources to introduce expert testimony, leading to the loss of probative value.

(ii) Inconsistent Evidentiary Standards.

There is wide variation in the way courts treat digital evidence across jurisdictions and sometimes within the same jurisdiction. For example, in India, while the sem-inal judgment of Anvar P.V. v. P. K. Basheer[693] held that electronic records are admissible only if they meet the require-ments of Section 65B of the Evidence Act (as it then was), including certification by the person in charge of the computer system,[694] subsequent practice has shown inconsistent adherence to that requirement.[695] In a related area of law, the U.S. case of Pacific Century International, Ltd. v. Does

[686] ibid
[687]Digital Evidence and Cybercrime: Admissibility and Challenges in Indian Law," The Legal Quorum (2025)
[688] NIST, supra note 6.
[689] Ibid.
[690] GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection," arXiv preprint (2021)
[691] Ibid.
[692] GNN4IP, supra note 42
[693] Anvar PV v PK Basheer (2014) 10 SCC 473 (SC India).
[694] Digital Evidence and Cybercrime: Admissibility and Challenges in Indian Law," supra note 35.
[695] Ibid.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

demonstrated the challenges of joining multiple alleged infringers relying solely on IP address evidence-a specific example of how gaps in evidence frustrate the prosecution of digital IPR infringements.[696]

(iii) Limited Inter-Jurisdictional Cooperation.

Digital IPR infringements often span more than one country, with infringing content stored on servers abroad, distribution taking place through global peer-to-peer networks, or hardware supply-chain theft spanning across several countries. However, mutual legal assistance treaties (MLATs), extradition mechanisms, and digital evidence-sharing regimes usually lag behind. [697] Without forensic protocols interoperable across jurisdictions, a trail of evidence captured in one country may lose value or admissibility in another, enabling offenders to exploit jurisdictional safe-havens.

(iv) Poorly Developed Digital Evidence Frameworks.

Many jurisdictions lack properly codified forensic standards tailored for digital IPR enforcement. In the words of one open-access study: "Whereas the [Indian legal] regime has broadened the domain of cyber-crimes, most of those responsible for upholding the law … have no specialist training in technology."[698] Similarly, forensic readiness practices-such as maintaining pre-incident logs, secure imaging before alteration, and documented chain of custody-are sporadic or missing.[699] Without dedicated legislative or regulatory frameworks regarding digital evidence in IPR contexts, enforcement remains prone to procedural failure.

3 Benefits Derived from Integration

(i) Improved Evidence Integrity.

A forensicised IPR enforcement system enhances the reliability of electronic evidence to the level where devices are imaged forensically, metadata is captured, alteration is prevented, and expert reports can be anchored in validated protocols. This reduces the risk of evidentiary exclusion, judicial scepticism, or appellate reversal.

(ii) Speedier And More Effective Prosecution.

With integrated processes, investigations move faster. Early forensic capture of data allows faster analysis, quicker assessment of liability, and efficient case preparation. For example, in cases of digital counterfeiting or software theft, forensic traceability gives the enforcement agencies an opportunity to act proactively before manifest damage is caused.

(iii) Enhanced Cross-Border Cooperation

When forensic standards and workflow protocols are harmonized, evidence collected in one jurisdiction is more likely to be recognized in another. This consistency facilitates mutual assistance, data transfer, and joint investigations of transnational IPR crimes. Over time, this fosters global enforcement networks better equipped to deter offenders.

(iv) Policy And Institutional Modernization.

Integration fosters coherence across technical, legal, and institutional domains. It promotes training programs, inter-agency coordination, public-private partnerships-that is, between IP rights holders and forensic units-and the creation of national strategies that connect protection of innovation to forensic readiness.

E. The Need for an Integrated Framework: Embedding Digital Forensics Within IPR Enforcement Mechanisms

Digitally enabled infringements, from trade-secret exfiltration to AI-generated plagiarism, illicit data replication, and counterfeit e-commerce networks, today define the global IP landscape. The conventional IPR enforcement structures, born of analog transactions requiring tangible evidence, are unequal to the task of dealing with the forensic and procedural complexity of these infractions.[700] The nature of

[696] Pacific Century International, Ltd. v. Does 1-101, No. 4:11-cv-02533 (N.D. Cal. July 8, 2011)
[697] Ibid.
[698] Pacific Century, supra note 48
[699] Ibid.
[700] Hegde, Sugali & Kumar, supra note 2.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

digital evidence, basically volatile, replicable, and disseminated across jurisdictions, calls for an interplay between digital forensics and IPR enforcement.

It is to bridge this divide that the present paper proposes a normative and operational model: the Integrated Forensic-IPR Enforcement Framework (IFIEF). IFIEF attempts to integrate necessary legal, institutional, and technological processes in order to ensure that evidence generated on cyber-enabled IP infringements is scientifically verifiable and legally admissible.[701]

1. The Conceptual Basis of the IFIEF Model

Underpinning the core of IFIEF is the principle of "forensic legitimacy" that every digital investigative act must withstand both technical scrutiny and legal evaluation.[702] Such dual legitimacy transforms digital forensics from a reactive investigative tool into a proactive component of legal governance.

The framework has four interdependent pillars:

i. Legal Harmonization: Embedding the principles of digital forensics into national IP and cybercrime legislation to standardize evidentiary admissibility and due process.

ii. Institutional Coordination: Setting up interoperable structures between IP offices, cybercrime units, forensic laboratories, and judiciary branches.

iii. Institutionalization of Forensic Readiness And Procedural Standardization: This includes evidence acquisition, preservation, and reporting with adherence to international standards such as ISO/IEC 27037, 27041.

iv. Cross-Border and Multi-Stakeholder Collaboration: This involves fostering transnational cooperation through mutual recognition of forensic methodologies and shared digital evidence platforms.

2. Legal Harmonization: The Doctrinal Pillar

Legal harmonization under IFIEF requires that IPR statutes explicitly acknowledge digital-forensic procedures as part of the enforcement process. Although the Budapest Convention on Cybercrime, 2001, remains the benchmark instrument in laying down harmonized rules on securing and preserving electronic evidence across the signatory states, this has not been well applied to IP enforcement.

Similarly, the WIPO–INTERPOL IP Crime and Infringement Enforcement Guidelines of 2023 recommend integration of forensic expertise into every stage of the investigation—receipt of complaint, data capture, analysis, and prosecution—to "ensure the authenticity, accuracy and reproducibility of evidentiary materials."[703]

Recent judicial developments underline this requirement. In the case of Gates Rubber Co. v. Bando Chemical Industries, Ltd. (1996), for example, the US District Court ruled that digital evidence must be collected in a manner consistent with forensic best practices or otherwise face exclusion.[704] In the context of Indian law, Anvar P. V. v. P. K. Basheer (2014) transformed the law of evidence by requiring electronic records to be proved in accordance with Section 65B of the Indian Evidence Act, thereby making forensic compliance a statutory imperative.[705]

To operationalize harmonization, IFIEF advocates for:

i. Model legal provisions mandating digital-forensic adherence in IP investigations.
ii. Amendment of evidence statutes to incorporate chain-of-custody obligations
iii. Creation of judicial training modules on digital-forensic interpretation.

[701] Digital Forensic Evidence in the Courtroom: Understanding Content and Quality, Supra note 8
[702] I. Atrey, Cybercrime and its Legal Implications, SSRN (2023)
[703] Budapest Convention on Cybercrime (2001), Council of Europe Treaty 185
[704] WIPO & INTERPOL, IP Crime and Infringement Enforcement Guidelines (2023)
[705] Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90 (D. Colo. 1996).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

These reforms ensure that forensic evidence does not just supplement legal proceedings but acts as a co-equal pillar of enforcement.

3. Institutional Coordination: Creating Interoperability and Expertise

IFIEF's second pillar refers to fragmentation in enforcement architecture. Within most jurisdictions, the IP registry, cybercrime division, and forensic laboratory are all separate, which leads to delays and inconsistencies.

The framework therefore recommends the establishment of Forensic–IP Liaison Units (FILUs) — hybrid entities comprising:

i. IP enforcement officials trained in basic digital evidence preservation;
ii. Certified forensic examiners; and
iii. Legal analysts ensuring procedural compliance.

Each FILU serves as the central coordination node between rights holders, investigative authorities, and prosecutors. For instance, the U.S. National IPR Coordination Center integrates Homeland Security Investigations with digital forensics units for targeting counterfeit supply chains and theft of trade secrets[706]. The NCFL in India coordinates efforts with the DPIIT to support online infringement tracing and dark-web investigations.[707]

The same coordination at an institutional level offers the opportunity for shared case management systems, enabling real-time digital evidence exchange under secure encryption protocols that preserve authenticity while assuring timely judicial access.

4. Forensic Readiness and Procedural Standardization

Forensic readiness is the capacity of an organization or state to lawfully collect and preserve digital evidence at short notice. In IP contexts—where infringement may involve cloud-stored source codes or metadata-embedded artworks—readiness ensures that no evidentiary opportunity is lost.

The IFIEF therefore codifies a Standardized Digital Forensic Protocol (SDFP) comprising four procedural stages:

Stage	Description	Legal/Forensic Outcome
Identification	Detect potentially infringing digital artefacts or transmissions.	Activation of forensic readiness policy.
Preservation	Create forensically sound images and compute hash values to ensure data immutability.	Validated chain of custody.
Analysis	Examine metadata, logs, and network traces to establish ownership and access history.	Attribution of infringement.
Presentation	Prepare forensic reports in admissible format, complying with evidentiary statutes.	Judicial reliability and probative weight.

Courts globally now expect adherence to these standards. In State (NCT of Delhi) v. Mohd. Afzal & Ors. (2003), the Delhi High Court underscored the importance of "scientifically verifiable" digital chain of custody.[708] Similarly, the European Court of Human Rights in K.U. v. Finland (2008) recognized that procedural

[706] Supra note 45
[707] U.S. National IPR Coordination Center,
[708] State (NCT of Delhi) v. Mohd. Afzal & Ors., 2003 SCC OnLine Del 1082.

deficiencies in digital investigations could violate the right to an effective remedy.[709]

Thus, the SDFP transforms forensic practice from an ad hoc response into a regulatory compliance discipline, aligning national IP enforcement with international evidentiary standards (ISO/IEC 27037, 27041, 27042).

5. Cross-Border and Multi-Stakeholder Collaboration

The transnational nature of IP violations, especially digital piracy, counterfeit e-commerce, and AI-driven content replication, requires jurisdictional interoperability. The fourth pillar of IFIEF is the Global Forensic-IPR Collaboration Mechanism, GFICM, which is built around:

i. Mutual recognition of forensic reports through bilateral or regional treaties.

ii. Cross-certification of forensic experts under WIPO or INTERPOL accreditation.

iii.Implement secure evidence-exchange portals with the ability to securely transmit data across borders in encrypted form.

Success within the EUROPOL–EUIPO IP Crime Unit indicates how digital-forensic integration significantly enhances transnational enforcement, achieving faster takedowns and prosecutions[710]. Similarly, in Microsoft Corp. v. Zhang Yi (China, 2019), forensic cooperation allowed for the cross-jurisdictional tracing of pirated software servers across multiple territories[711].

The GFICM model thus enables inter-jurisdictional admissibility, a central prerequisite for handling cyber-enabled IP violations that traverse legal borders.

F. Recommendations

1. To establish a Unified Digital Forensic–IPR Enforcement Authority under the joint mandate of national IP offices and cybercrime agencies to ensure coordinated policy and enforcement actions.
2. To develop legally binding national standards for digital forensic procedures in IP-related investigations, harmonized with international norms such as ISO/IEC 27037 and 27041.
3. To create a shared forensic data platform enabling real-time collaboration and evidence exchange among enforcement agencies, forensic laboratories, and judicial bodies.
4. To institutionalize cross-border cooperation frameworks through WIPO and INTERPOL to facilitate mutual recognition of digital evidence under MLATs and international conventions.
5. To implement judicial and investigator capacity-building programs focused on forensic interpretation, evidence preservation, and cyber-enabled IP crime prosecution.
6. To leverage emerging technologies such as blockchain and AI to enhance traceability, authentication, and transparency in the management of digital evidence

G. Conclusion

The evolution of intellectual property enforcement into the digital era requires a paradigm shift from reactive prosecution to proactive, forensically driven governance.

Digital forensics now lies at the heart of credible IP protection, with its methodologies defining the authenticity, traceability, and admissibility of electronic evidence. The proposed IFIEF integrates technology, law, and policy into one coherent system that ensures evidentiary precision, procedural harmony, and institutional synergy. Ultimately, the meeting of digital forensics and intellectual property law is not a theoretical aspiration but an operational necessity. It marks the future of cybercrime

[709] K.U. v. Finland, App. No. 2872/02 (ECHR 2008).
[710] EUROPOL–EUIPO, Intellectual Property Crime Threat Assessment 2023,
[711] Microsoft Corp. v. Zhang Yi, Beijing IP Court (2019)

investigation—a future in which technological verification, legal validation, and judicial integrity function as one to protect and preserve innovation and creativity in the digital society.

VI. References

A. Books, Articles, And Journals

1. N. Allah Rakha, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, Mexican Law Review (2024), available at https://scielo.org.mx.
2. F.H. Deandra & I.M. Sherly, Advancing Digital Forensic Investigations: Addressing Challenges and Enhancing Cybercrime Solutions, World Journal of Information Technology (2025), available at https://upubscience.com.
3. C. Hegde, C.N. Sugali & L.A. Kumar, Digital Forensics for Safeguarding Intellectual Property Rights: A Study in the Context of Indian IPR Laws, Journal of Intellectual Property Rights (JIPR) (2024), available at https://niscpr.res.in.
4. I. Atrey, Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence, International Journal of Research and Analytical Reviews (2023), available at https://papers.ssrn.com.
5. A.K. Blaskovic, J.D. Rusk & V.C. Parker Jr., Cybercrime and Intellectual Property Theft: An Analysis of Modern Digital Forensics, in Proceedings of the Future Technologies Conference (Springer, 2022).
6. A.Z.A. Shami, M. Saleem & J. Ashraf, Cybercrime and Digital Evidence: Investigating the Challenges and Opportunities in Prosecuting Cybercrime and Handling Digital Evidence, Research Consortium Archive (2025), available at https://rc-archive.com.

B. Cases

7. Anvar P.V. v. P.K. Basheer & Others, (2014) 10 S.C.C. 473 (India).
8. R. v. Shearing, [2002] EWCA Crim 2273 (U.K.).
9. United States v. Bonallo, 858 F.2d 1427 (9th Cir. 1988).
10. Pacific Century International, Ltd. v. Does 1–37, 282 F.R.D. 189 (N.D. Ill. 2012).
11. Tata Sons Ltd. v. John Doe & Ors., 2019 SCC OnLine Del 11963 (India).C.

C. International Instruments and Reports

12. World Intellectual Property Organization (WIPO) & INTERPOL, Cybercrime and IP Enforcement in the Digital Age (2023).
13. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
14. Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
15. National Institute of Standards and Technology (NIST), Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800–86 (2006).
16. ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.
17. ISO/IEC 27041:2015, Information Technology—Security Techniques—Guidance on Assuring Suitability and Adequacy of Incident Investigative Methodology.