INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

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

CLOUD FORENSICS – TECHNICAL METHODOLOGIES AND LEGAL CHALLENGES IN CLOUD ENVIRONMENT

AUTHORED BY - NARRI AASHRITHA & VARTICA SINHA

I. Introduction

1.1 Premise

The expansion of digital data has transformed the methods of **committing, investigating, and prosecuting crimes**, rendering digital forensics importance in criminal justice system especially in light of India **ranking 4** amongst the most targeted for cybercrimes. **Cloud forensics—a combination of digital forensics and cloud computing—**enables evidence collecting and verification across different and scattered storage sites. Despite the challenges of large-scale data management, optimised cloud forensic methods can improve security and system performance.[1]

1.2 Background

Cloud computing has transformed business operations by improving scalability, performance, and resource availability through shared infrastructure, flexibility, and fast networks. Its cost-efficiency and operational advantages have led to widespread adoption across industries, but unscrupulous actors have used them to exploit vulnerabilities for unauthorised access, data breaches, and other illegal acts leading to **security, privacy, cross border concerns** etc.[2] Frameworks for the same must be strengthened considering these risks.

1.3 The Alarming Need And Implicating Relevance – Overcome Challenges

The challenges faced in cloud forensics are categorised as follows:

- Technological difficulties: Cloud computing presents technical challenges for data extraction, safeguarding digital data, particularly in preventing unauthorised modifications.
- Legal Concerns: Privacy, Security, cross-border, confiscation, integrity etc., issues

[1] Cohen F, Ruan K. Challenges to digital forensic evidences in the cloud. Cybercrime and cloud Forensics Application for Investigation Process; 2012 Jan. p. 2–7.
[2] Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal, (2020) 7 SCC 322.

ISSN: 2582-6433

provide a significant obstacle for investigators. Consequently, investigators must meticulously and lawfully preserve acquired data.

To deter the alarming cyber threats, post key incidents – The **2014 Apple iCloud breach** revealed celebrity photos, raising concerns about cloud forensics and third-party data ownership; a **2017 Amazon S3** misconfiguration showed vulnerabilities from improper data placement and settings; the **2012 Dropbox** incident compromised 68 million passwords due to infrastructure issues; and a **2019 Microsoft Office** 365 breach that affected over 300,000 users' personal data, makes crucial to overcome these challenges in cloud forensics.

II. Research Question

1. How can solutions such as **hypervisor snapshots, API-based acquisition, and unified log formats** contribute to protecting **data integrity** in volatile, multi-tenant environments? What additional challenges does cloud computing pose for **traditional forensic procedures** of identification, acquisition, preservation, and analysis?
2. How do the Indian legal statutes under the Bharatiya Sakshya Adhiniyam, IT Act, and case laws, compare regarding admissibility, authentication, and cross-border jurisdiction?
3. Can scalability, automation, and AI-based detection be integrated with privacy and legal protections within a CSP-neutral framework?

III. Methodology

3.1 Research Methodology

Doctrinal and non-doctrinal research methodologies have been employed. The **doctrinal method** critiques India's digital forensics and cloud evidence laws, precedents, and practices. Admission, authentication, and jurisdictional concerns are explored in the *Bharatiya Sakshya Adhiniyam*[3], *Information Technology Act, 2000*[4], and major case laws.

The **non-doctrinal method** incorporates global cloud forensic techniques and empirical findings. Reports, breach case studies, hypervisor snapshots, API-based acquisitions, and standardised log frameworks in volatile, multi-tenant cloud infrastructures are examined.

The paper uses **secondary data** from journals, books, government studies, white papers,

[3] Bharatiya Sakshya Adhiniyam, 2023 (India).
[4] Information Technology Act, 2000 (India).

ISSN: 2582-6433

reliable websites, and cybercrime and forensic statistics. This method balances both techno-legal perspectives on cloud forensics' theoretical and practical foundations.

3.2 Literature Review

Challenges of Digital Forensics in Cloud Computing Environment[5]

Addresses cloud forensics concerns such volatile data, poor system management, and multi-tenancy in identification, evidence gathering and preservation, analysis, and presentation. It evaluates standardised logging frameworks, encryption, TPM-based preservation, and early forensic tools like FROST, then proposes a Eucalyptus-based framework for persistently storing suspicious VM snapshots to balance evidence integrity and resource efficiency. It excels at systematic problem identification, practical execution, and reproducibility using open-source tools. In a private Eucalyptus environment without performance indicators, legal and jurisdictional inquiry is limited. References to outdated tools and poor coverage of modern architectures (*e.g., serverless, containerised systems*) limit applicability.

The absence of a standardised, ***CSP-independent forensic framework****, along with the necessity for scalability and cost assessments for extensive evidence storage, automated* ***AI-driven detection, legal admissibility integration, and validation in public and hybrid clouds, constitutes critical research requirements.*** *A comprehensive,* ***cross-platform forensic*** *process that encompasses both technological and legal dimensions of cloud investigations may be established on this technical foundation.*

Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation[6]

Aligns Cloud Security Alliance's "*Top Threats*"—data breaches, denial of service, insider misuse, and unsecured APIs—with attack vectors and mitigation measures. The conceptual clarity, incorporation of real-world breach case studies, articulation of the burgeoning "*crime-as-a-service*" economy, and awareness of forensic issues such volatile log preservation make this taxonomy strong. However, empirical validation, legal analysis, and the procedural subtleties of its forensic framework are lacking, and some dangers elude STRIDE classification. Secondary literature dominates the analysis, which lacks quantitative validation. *Significant research gaps exist due to the lack of standardised, CSP-neutral forensic protocols;*

[5] Deevi Radharani, SK. Nazma Sultana, Pasala Lourudu Sravani, Challenges of Digital Forensics in Cloud Computing Environment, 9(17) IJST ,1-7 (2016).
[6] Gayatri S Pandi, Saurabh Shah, K.H. Wandra, Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation,167 ICCIDS, 163-172 (2019).

ISSN: 2582-6433

*the absence of **empirically tested security and forensic controls**; the need for enforceable, legally **sound SLA clauses that allocate security responsibilities**; inadequate **cross-jurisdictional evidence-handling mechanisms**; insufficient regulation of **criminal cloud-service markets**; and unclear evidentiary standards for probabilistic log-integrity techniques. Addressing these gaps would enhance both the **technical effectiveness and the legal admissibility of cloud forensic investigation**s, thereby reinforcing accountability in distributed computing environments.*

Emphasizing on Various Security Issues in Cloud Forensic Framework[7]

Analyses technical-legal issues in cloud forensics at each stage of the evidence lifecycle—identification/collection, acquisition, preservation, and analysis/reporting. Understanding integrity and chain-of-custody issues in distributed systems, VM volatility, and remote acquisition overhead, and that non-standardized logs reduce evidential value and jurisdictional clarity, including cross-border verification, are strengths. Their recommendations—stronger hashing, live-evidence preservation, data-centre mapping, and a "*uni-log*" format—are sound and engage frameworks However, mostly prescriptive, not empirical; core prescriptions (*"use a strong algorithm," "unify logs"*) lack technical specification, governance pathways, and validation; The MD5 critique falls short of admissibility standards; and SLA audit rights, cooperation duties, retention, and privacy are not developed.

*The techno-legal interface has research gaps in (i) a **standardised logging schema** (format, secure time-stamping, source authentication); (ii) legally **robust live-forensics protocols** reconciling preservation with privacy; (iii) contractual and cross-border architectures—choice-of-law, retention, and **CSP cooperation duties**—to mitigate provider dependence; and (iv) validated multi-factor integrity schemes. These demonstrate that forensic readiness must be engineered, **not assumed.***

Technical Challenges In Cloud Forensics and suggested Solutions[8]

Presents a methodical examination of forensic challenges in cloud computing, organised according to the stages of digital forensics. A significant strength is its extensive taxonomy of issues, encompassing jurisdictional conflicts and data volatility, along with the associated technical solutions, such snapshot analysis and secure provenance. The article effectively

[7] Pranay Chauhan, Pratosh Bansal, Emphasizing on Various Security Issues in Cloud Forensic Framework,10(18) IJST,1-7 (2017).
[8] Md Yasir Arafat, Sreeti Rani,Technical Challenges In Cloud Forensics and suggested Solutions, 8 IJSER, 1142-1149 (2017).

ISSN: 2582-6433

aligns classic forensic ideas with contemporary cloud environments, ultimately improving evidence dependability. Nonetheless, its deficiencies are apparent in the primarily technological focus, which affords minimal consideration to the procedural admissibility of cloud-derived evidence across various legal systems. Moreover, its suggested solutions are still theoretical, lacking adequate empirical validation or comparative assessment across other jurisdictions.

The main research need pertains to the amalgamation of technical forensic methodologies with implementable transnational legal structures. Future scholarship must engage in doctrinal analysis and multidisciplinary modelling to ***align technology feasibility with legal acceptability.***

Review on Challenges in Cloud Forensics[9]

Synthesises organisational, technical, and legal barriers to identification, acquisition, analysis, and reporting, focussing on IaaS–PaaS–SaaS, multi-tenancy, log volatility/access, encryption opacity, and global data replication, which destabilise chain of custody and evidentiary integrity. Strengths include structured taxonomy (*challenge/solution tables; tool mapping*), mobile-cloud focus, and forward-thinking proposals (*standardised frameworks, AI/ML tools, CSP–LEA collaboration*). The account is primarily descriptive and does not operationalise logging standards (*secure time-stamping, source authentication*), volatile-data acquisition methods, evidentiary reliability/admissibility tests (*method validation, auditability*), or forensic-readiness contract design. MLAT practice, suppression outcomes, and case law provide minimal evidence for breach scenarios.

The absence of a ***cross-border evidence models*** *reconciling provider replication with lawful access and* ***conflicts rules, privacy-by-design; admissibility of evidence, mobile-cloud chain-of-custody.***

Legal challenges and lacunas in the digital forensics jurisprudence in India[10]

This article comprehensively reviews India's digital-forensics jurisprudence, including statutory provisions, Supreme Court and High Court precedents, administrative guidelines, and policy recommendations, providing a valuable primer for legal scholars and practitioners. Its extensive case law synthesis (*Anvar, Khotkar, Puttaswamy*), attention to procedural

[9] Vinit Nikuj Parmar, Dr. U. Rana, Dr. RavirajSingh, Review on Challenges in Cloud Forensics, 13(6) IJSR,113-118 (2024).
[10] Srinivas Katkuri, Legal challenges and lacunas in the digital forensics jurisprudence in India,10 IJL,23-29 (2024).

ISSN: 2582-6433

vulnerabilities (*chain-of-custody, admissibility*), and pragmatic policy solutions (*standards, accreditation, capacity building*) are strengths. However, the paper's legal analysis is mostly descriptive, lacking comparative doctrinal critique, empirical data on forensic laboratory practices and case outcomes, and technical engagement with evidentiary validation methods.

*The study does not resolve **privacy, encryption, and legitimate access issues or propose a statutory draughting paradigm**. Empirical, interdisciplinary research is needed to evaluate existing **MeitY guidelines**, develop validated, **court-ready protocols** for evidence acquisition and tool verification, and draft model legislation harmonising privacy safeguards with lawful access in cross-border contexts. Filling these gaps would move the conversation from diagnosis to action. These improvements would boost national judicial and investigative trust.*

IV. Critical Analysis

Cloud forensics, at the intersection of distributed computing and digital inquiry, is marked by notable contradictions between legal admissibility and technical feasibility. Research enquiries are structured along three dimensions: (i) technology limitations of existing forensic methodologies; (ii) competence of Indian legal frameworks; and (iii) viability of an unified, cross-jurisdictional forensic model.

4.1 Cloud v. Traditional Forensic

Traditional forensics assumes **physical control** over storage media, allowing investigators to seize hardware, create bit-for-bit duplicates, and maintain custody. Cloud forensics depends on the cooperation of **cloud service providers** (*CSPs*), given that users lack physical control over the servers. This reliance undermines **chain-of-custody** assumptions and complicates live data capture. Literature suggests that **API-based** acquisition technology offers convenience and efficiency, but may overlook **RAM-based volatile data**. In contrast, hypervisor snapshots ensure completeness, though they require privileged access, which is often not readily granted by CSPs. **Forensic trade-offs** are inherent: completeness versus feasibility, independence versus reliance.

4.2 Technical Challenges

The technical challenges of cloud forensics are multifaceted.

1. Evidence Volatility: Virtual machine evidence is obliterated upon shutdown, resulting in the loss of critical information, including passwords and encryption keys.
2. Data Integrity: The integrity of distributed, replicated servers necessitates strong

ISSN: 2582-6433

hashing, provenance, and immutable logging mechanisms. The absence of CSP-independent, standardized logging frameworks undermines evidentiary trust.

3. Instance Isolation & Provenance: Ensuring the integrity of evidence requires safe instance isolation; however, effective solutions are still in their infancy. Provenance mechanisms exist but have not yet received legal endorsement.
4. Cross-border Storage: As highlighted in systematic reviews multi-jurisdictional storage presents a sovereignty challenge, since Indian authorities would need to access servers in foreign nations governed by local data protection and privacy laws that limit admissibility.[11]

Investigators often feel obligated to utilise traditional network forensics or disc forensics technologies; however, these tools are ineffective against the distributed, dynamic, and volatile data structures prevalent in cloud environments.

4.3 In Context: Indian Legal Jurisprudence

Indian jurisprudence has endeavoured to remain current; yet, significant gaps persist. ***Section 63, Bharatiya Sakshya Adhiniyam***[12] requires rigorous certification for the admissibility of electronic evidence. In ***Anvar P.V. v. P.K. Basheer***[13], and confirmed in ***Arjun Panditrao Khotkar***[14], the Supreme Court mandated adherence to certification protocols. However, in cloud environments, obtaining such certificates is almost unfeasible without the assistance of a Cloud Service Provider (*CSP*). ***The Information Technology Act, 2000***,[15] recognises electronic records; however, its stipulations do not encompass ephemeral, scattered, or transnational evidence. **Post-Puttaswamy privacy** issues and conflicting international legislation regarding data sovereignty create a legal impasse for evidence collection. India's absence of standardised forensic practices results in disparate standards among forensic laboratories and examiners. The ***Ministry of Electronics and Information Technology (MeitY)*** has released rules that are neither enforceable nor binding.

4.4 A Delve Into Research Gaps: Examination

1. Standardized Frameworks: Contemporary forensic methods are disjointed, specific to

[11] Ameer Pichan, Mihai Lazarescu, Sie Teng Soh, Cloud forensics: Technical challenges, solutions and comparative analysis,13 ELSEVIER,38-57 (2015).
[12] Bharatiya Sakshya Adhiniyam, § 63.
[13] Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.
[14] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
[15] IT Act, 2000 (India).

ISSN: 2582-6433

cloud service providers, and lack authorization across public, private, and hybrid cloud environments. A CSP-neutral system based on a universal "*uni-log*" format would improve consistency and admissibility.

2. AI/ML Automation: The magnitude and velocity of cloud data render manual forensic analysis unfeasible. The subjects of machine-based evidence verification and anomaly detection utilizing AI are inadequately explored.
3. Legal Integration: There is a necessity to amalgamate technology procedures with enforceable legal safeguards. This encompasses model SLA provisions mandating CSP collaboration, cross-border mutual assistance agreements (*surpassing current MLAT inefficiencies*), and judicially determined forensic preparedness criteria.
4. Privacy and Investigation: A balanced legal framework must be established to reconcile the Puttaswamy-enforced right to privacy with the state's interest in addressing cybercrime. The statutory codification of proportionality tests regarding access to cloud evidence may serve as a solution.

4.5 Towards A Techno-Legal Framework

The path forward is dismantling the barriers between technology and law. Cloud design must incorporate forensic readiness through immutable **logging, provenance automation, and snapshotting**. India must **update** its *Bharatiya Sakshya Adhiniyam*[16] and *IT Act*[17] to include clear provisions regarding cloud evidence, while simultaneously establishing **cross-border data-sharing agreements.** Courts face the danger of inconsistent rulings as judicial precedents establish admissibility concerns without **statutory direction.**

V. Conclusion

Cloud forensics shows a fundamental inconsistency between evidence admissibility and technology feasibility. In cloud contexts, when investigators use service providers and evidence is volatile, distributed, and cross-jurisdictional, custody doctrines fail. Indian law allows electronic records but does not cover **transient and foreign-stored data, leaving courts ambiguous.**

Integrating forensic readiness into cloud architecture via immutable logs and AI-driven verification and changing evidential and IT statutes to ensure **proportionality, privacy, and**

[16] BSA, 2023 (India).
[17] IT Act, 2000 (India).

ISSN: 2582-6433

cross-border cooperation requires a consistent techno-legal framework. Integration is necessary for evidence reliability and constitutional legitimacy.

Recommendations

1. Create a **CSP-agnostic forensic model** with shared logs, encryption, and provenance mechanisms for platform consistency and admissibility.
2. Create **forensic-ready cloud architecture** by integrating immutable logs, auto-snapshots, and AI-facilitated anomaly detection to secure ephemeral data.
3. India's **legislation reform**, IT Act reform, treaty negotiation beyond MLATs, and privacy-by-design principles aim to harmonise investigation and basic rights.

VI. References

Articles & Journals

1. Cohen F, Ruan K. Challenges to digital forensic evidences in the cloud. Cybercrime and cloud Forensics Application for Investigation Process; 2012 Jan. p. 2–7.
2. Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal, (2020) 7 SCC 322.
3. Deevi Radharani, SK. Nazma Sultana, Pasala Lourudu Sravani, Challenges of Digital Forensics in Cloud Computing Environment, 9(17) IJST ,1-7 (2016).
4. Pranay Chauhan, Pratosh Bansal, Emphasizing on Various Security Issues in Cloud Forensic Framework,10(18) IJST,1-7 (2017).
5. Vinit Nikuj Parmar, Dr. U. Rana, Dr. RavirajSingh, Review on Challenges in Cloud Forensics, 13(6) IJSR,113-118 (2024).
6. Srinivas Katkuri, Legal challenges and lacunas in the digital forensics' jurisprudence in India,10 IJL,23-29 (2024).
7. Ameer Pichan, Mihai Lazarescu, Sie Teng Soh, Cloud forensics: Technical challenges, solutions and comparative analysis,13 ELSEVIER,38-57 (2015).
8. Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age, IP and Legal Filings (visited Aug. 17, 2025), https://www.ipandlegalfilings.com/digital-forensics-in-india-bridging-technology-law-and-justice-in-the-cyber-age/.
9. Gayatri S. Pandi (Jain), Saurabh Shah & K.H. Wandra, Exploration of Vulnerabilities, Threats and Forensic Issues and Its Impact on the Distributed Environment of Cloud and Its Mitigation, in 2019 Int'l Conf. on Computational Intelligence & Data Sci. (ICCIDS 2019), Procedia Computer Science (Elsevier B.V. 2019), https://doi.org/10.1016/j.procs.2019.12.185.

ISSN: 2582-6433

Case Laws

1. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

Online Sources

1. Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age, IP and Legal Filings (visited Aug. 17, 2025), https://www.ipandlegalfilings.com/digital-forensics-in-india-bridging-technology-law-and-justice-in-the-cyber-age/.
2. 5 Legal Challenges in Digital Forensic Investigations, (visited Aug. 17, 2025), 5 Legal Challenges in Digital Forensic Investigations - Eclipse Forensics.