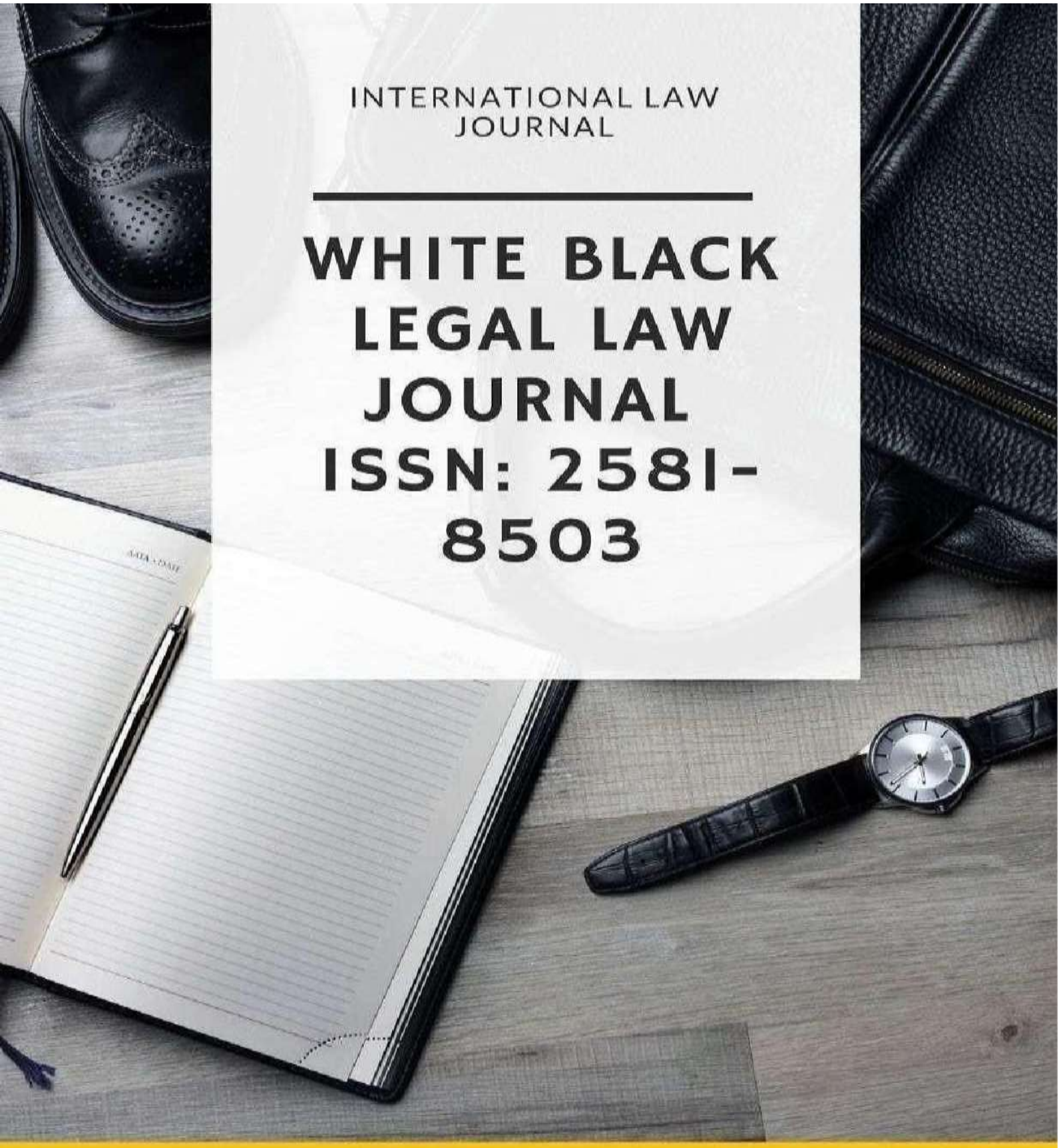

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

"DIGITAL FORENSICS IN CYBERCRIME INVESTIGATION: LEGAL PROCEDURES AND CHALLENGES"

AUTHORED BY - SIMRAN KAUR
Faculty of Law, SRM University Delhi Ncr, Sonepat

Under the Supervision of - Dr. Anjali Dixit
(Associate Professor)

1.1 Introduction

Digital forensics is no longer just a small technical support side function; it has become the main engine of modern policing and prosecution based on India. It is clear that the aforesaid factors: networked payments, cloud platforms, end to end encrypted messaging, and algorithmic content curation have resulted in the most common case files being filled with logs, hashes, device images, metadata trails, and platform responses which need to be collected, preserved, and proven in compliance with procedure and the law. The procedural discipline is derived out of the reformed criminal process and evidence law, whereby the production, search, and seizure of digital materials must be carried out under formal authorizations and recording mandates, including audio video documentation of the searches. The legal sensitivity, on the other hand, is derived from the constitutional right to life and personal liberty as well as a modern privacy law, which, among other things, provides for the purpose, notice, and consent and imposes certain obligations in respect of children's data. The statutory framework, however, is not a single block. The substantive computer related crimes and the powers of inquiry are placed in the Information Technology Act, 2000 with its system of interception, blocking, monitoring, and incident response rules. Meanwhile, the Bharatiya Sakshya Adhiniyam, 2023, which updated the Indian law of evidence to be more compatible with the ew era, is the location where the issues of electronic or digital records' admissibility and the certification regime are dealt with. The Bharatiya Nagarik Suraksha Sanhita, 2023, which not only repurposes summons to produce and letters of request with giving explicit digital evidence references but also prescribes audio video recording for search and seizure, is the place where production of devices and electronic communications, search scope, and reciprocal assistance channels are dealt with. The sectoral directions of CERT In, RBI, DoT, and other regulators shape the availability, retention, and format of logs and subscriber data, and most of the time, they also set very concrete timelines for reporting and preservation that investigators and

defenders must be well acquainted with. The Digital Personal Data Protection Act, 2023, on top of this, imposes compliance and accountability obligations on all actors who are involved in the processing of personal data, even when the processing is for the prevention, detection, investigation, or prosecution of offences. When combined, these instruments depict the state of digital forensics in India as being a practice of lawful collection and preservation with four foundational principles. First, production, search, or preservation orders that are lawfully triggered, and are time bound, recorded, tailored. Secondly, acquisition and hashing that are technically sound, that do not compromise integrity and that maintain a clear audit trail. Thirdly, certification and expert disclosure through which a judge is enabled to link a seized exhibit to an unbroken chain and a trustworthy toolset. Lastly, privacy safeguards which not only describe lawful purpose, necessity, and proportionality but also regulate collateral exposure, in particular, for sensitive and children's data.

1.2 Conceptual Foundations

A well-structured explanation of digital forensics is essentially a journey from method to legitimacy. The method refers to the internationally recognized procedural steps for handling potential digital evidence following the incident timeline, thus involving identification and isolation to collection, acquisition, preservation, analysis, and reporting. Legitimacy, on the other hand, refers to the legal principles that limit intrusion and regulate the use of personal data downstream. Worldwide standards, especially ISO IEC 27037, detail the initial stages of identification, collection, acquisition, and preservation with a strong emphasis on integrity, repeatability, and clarity of roles between first responders and specialists. National evidence laws consider electronic or digital records as documentary evidence and create a framework for admissibility and certification that can be achieved if the proponent demonstrates authenticity and integrity along with proper certification and tool validation records. The data protection law introduces the ideas of lawful purpose, data minimization, purpose limitation, accountability, and special safeguards for children. By bridging these levels, a scientifically defensible and legally sustainable practice across investigation, trial, and appellate review is created.[1]

[1] ISO/IEC 27037:2012 Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, *available at:* https://www.iso.org/standard/44381.html (last visited on October 28, 2025).

1.2.1 What Are Digital Forensics

Essentially, digital forensics is the intentional recovery and review of data from computers, mobile devices, removable discs, networks, and cloud services that is done in a manner that is consistent with the integrity of the data and which allows for the same results to be obtained again by a different person. The purposes of such operations are three main ones. Firstly, to find the most relevant digital traces that prove or disprove the occurrence of an event and the guilty mind of the perpetrator, or, alternatively, confirm the witness's version of the events. Secondly, to ensure the preservation and thorough documentation of those traces in the formats that would meet the requirements of verification of authenticity and chain of custody coming from the court. Thirdly, to make the reports of the discoveries in an understandable way along with the tool versions, hash values, and validation references. The phases are in line with the widely accepted recommendations. After Identification and isolation come the stages that avoid alteration. Those which are Collection and acquisition employ write blockers and validated tools to create bit stream or logical images and at the same time compute cryptographic hashes. Preservation is the stage when the original media and evidence copies are maintained in a safe place together with access logs. Analysis is done by using validated workflows to retrieve the relevant data such as registry keys, chat histories, geolocation traces, and application caches. Reporting is the stage when the utilized methods, the faced limitations, and the drawn conclusions are presented without speculation.[2]

1.2.2 Cybercrime Typologies

The value of digital forensic investigations is most obvious in categories where the modus operandi is technically, remotely, or distributivity. Financial frauds use phishing kits, mule accounts, and social engineering scripts, and thus fingerprints can be found in device artefacts, payment rails, and platform logs. Identity theft and cheating by personation through computer resources are the most straightforward ways of tracking offences that cover credential misuse and deceptive online conduct. Cyber harassment cases revolve around account activity, IP address allocation, device usage patterns, and content provenance. Ransomware investigations zoom in on encryption artefacts, dropped executables, command and control beacons, and cryptocurrency transaction trails. Threats against protected systems and critical infrastructure refer to provisions on protected systems, incident reporting, and the national nodal agencies.

[2] Best Practices for Computer Forensic Acquisitions, *available at:* https://www.swgde.org/wp-content/uploads/2024/03/2023-06-15-SWGDE-Best-Practices-for-Computer-Forensic-Acquisitions-17-F-002-2.0.pdf (last visited on October 27, 2025).

Platform content harms bring in safe harbor and due diligence questions for intermediaries besides takedown timelines and preservation duties. Cross border spam and botnet activity cannot do without extraterritorial reach and mutual legal assistance routes. These typologies, on the other hand, are rooted in law, which defines offences, compels assistance, and creates process routes for obtaining data and disrupting harm.[3]

1.2.3 Types of Digital Evidence

Device based materials are the likes of disk images, mobile extractions, removable media, and embedded systems. Network based materials are the flow records, firewall and proxy logs, DHCP leases, and ISP subscriber assignment records. Cloud based materials are the mailboxes, object storage keys, platform event logs, content moderation logs, and authentication histories. Metadata and logs consist of timestamps, geolocation tags, EXIF headers, registry entries, and application specific artefacts. OSINT artefacts are public posts, domains, WHOIS history, and cached pages. The law considers these categories as documentary evidence when they are produced for inspection and explicitly recognize electronic or digital records, so the evidentiary test mainly revolves around authenticity, integrity, and linkage to a relevant fact in issue. The definitional anchor in information technology law, which governs electronic records, essentially, frames them as data and images stored, received, or sent in electronic form. This makes it easier for courts to accept artefacts that are common in networked systems but are unfamiliar to the traditional evidentiary taxonomies.[4]

1.2.4 Privacy and Data Protection Principles

Privacy controls in digital investigations should not be viewed as an abstract add on. They have an impact on the scope, method, duration, and disclosure of the investigation. The data protection law outlines two main points for handling personal data consent and some legitimate uses and defines a lawful purpose as any purpose that is not prohibited by law. The obligations of a data fiduciary involve limiting the purpose, minimizing the data, providing reasonable security safeguards, notifying the Board of a breach, and following the retention controls set by the regulator, while significant data fiduciaries have additional obligations. The collection of children's data requires obtaining verifiable consent, and there are class-based prohibitions

[3] The Information Technology Act, 2000, *available at:* https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited on October 26, 2025).
[4] The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf (last visited on October 25, 2025).

on tracking and targeted advertising. Besides that, rulemaking enables the government to define classes and establish conditions for the processing of children's data. The rights of access, correction, and erasure cooperate with criminal law exceptions that come into force when a competent authority requests data for the prevention, detection, or investigation of offences or cyber incidents. A forensic plan that specifies the lawful purpose, limits the scope to what is necessary, and keeps a record of the decisions made regarding sensitive and children's data will have a stronger legal basis and will be able to protect admissibility later on.

1.3 Legal Framework in India

Various laws govern digital forensics, starting from constitutional guarantees, technology laws that are sector neutral, procedure and evidence codes, as well as sectoral and regulatory standards. The Constitution, while guaranteeing personal liberty and free speech, allows for reasonable restrictions and thus, sets the standard against which any intrusions are evaluated. The statute on information technology outlines the definition of electronic records, establishes crimes related to identity theft, impersonation by use of computer resources, obscenity through electronic publishing, protected systems, interception and decryption powers, blocking powers, and a national incident response apparatus. The procedure code changes production, search, and assistance to show communications electronically by reference and also requires audio video recording of search and seizure. The contemporary evidence statute acknowledges electronic or digital records as documentary evidence, offers special provisions for their admissibility, and establishes a certification system that applies when parties rely on electronic or digital records. Sectoral rules and directions, among other things, describe incident reporting timelines, data retention, and intermediaries' due diligence, who often decide what investigators can lawfully obtain and how quickly. The data protection law, therefore, puts in place a compliance and accountability framework that interacts with the investigative exceptions.[5]

1.3.1 Constitutional Basis

The right to life and personal liberty should be used as a basis for the consideration of any interference with devices, accounts, and communications. Any taking of these rights must be in accordance with a procedure established by law. Freedom of speech extends to online

[5] The Constitution of India, *available at:* https://www.indiacode.nic.in/bitstream/123456789/16124/1/the_constitution_of_india.pdf (last visited on October 24, 2025).

expression but allows Parliament to set reasonable limitations for the maintenance of the sovereignty and integrity, security of the State, public order, decency or morality, contempt of court, defamation, or incitement to an offence. This equilibrium does not imply that there are no constitutional limits for digital evidence. It implies that searches, seizures, and forced disclosures should be based on a valid statutory authority, be required for a legitimate aim, and be designed to avoid unnecessary collection. Privacy provisions in the data protection law are consistent with these standards in that they require a lawful purpose and recognize the need for investigation within the framework of the statute. When the investigators obtain authorizations, limit their scope, and state their purpose, courts are then able to determine whether the intrusion respects the balance between freedom and order in a tangible way.[6]

1.3.2 Information Technology Regime

The technology law provides the enforcement toolkit that is generally at the cybercrime investigation's base. It specifies the term "electronic record", and accords legal status to electronic records and electronic signatures, and also, sets the retention period for records in electronic form. The law provides for identity theft to be made a criminal offence and the use of false identity by means of computer resources as a punishable offence, stipulates penalties for the production of obscene content in electronic media, and creates new obligations for the preservation of and furnishing of information. It gives the government the power to issue lawful interception, monitoring, and decryption instructions subject to procedural safeguards, and to prevent access to information by the public through a specified process. The law establishes the Indian Computer Emergency Response Team, defines its functions in incident response, and facilitates directions including reporting obligations. The Intermediary due diligence and safe harbor are through the Act and the Intermediary Guidelines that provide for takedown timelines, grievance redressal, and data retention norms. CERT directions on incident reporting timelines and log retention mandates that go along with these duties and have become essential for the timely preservation and facilitation of attribution.[7]

1.3.3 Criminal Procedure and Evidence Rules

The procedure code on process, among other things, allows a summons to produce documents or other things and, importantly, extends this to electronic communication and communication

[6] *Supra* note 5.
[7] *Supra* note 3.

devices likely to contain digital evidence. It requires the recording of audio and video for search and seizure and keeps the court's authority to impound documents produced. It provides reciprocal provisions for the execution of processes in different locations. As the modern evidence statute, the combined effect is a way where correct authorizations, written searches, complete imaging with hash validation, and proper certification can bring electronic records from the field to the court with clear provenance and integrity. It recognizes electronic or digital records as documentary evidence and makes special provisions for their admissibility. It also offers a certification method that is in line with the previous jurisprudence but is more explicit in terms of the terminology and examples.

1.3.4 Sectoral and Regulatory Standards

Sectoral regulators have an impact on digital forensic workflows as they determine the type of logs that exist, the duration for which they are kept, and the format in which they can be accessed. CERT In's directions call for incident reporting within six hours of the time of detection and impose a requirement on service providers to keep logs in India for one hundred eighty days, with data centers, cloud providers, VPNs, and virtual asset participants having specific obligations. The Intermediary Guidelines provide for due diligence, takedown timelines, and the preservation of removed content and related records for one hundred eighty days. Banking and telecom regulators establish KYC, CDR retention, and cybersecurity norms which essentially govern the possibilities of subscriber identification and availability of network and transaction logs for timely correlation. These norms turn into the actual framework for preservation orders, platform queries, and expert analysis, and they very often determine whether the sequence of events can be traced.[8]

1.3.5 International Cooperation Interfaces

Such investigations across the borders require formal channels that not only uphold the sovereignty but also ensure admissibility. The procedure code essentially serves as the instrument that formalizes requests made to foreign authorities for examination of persons and production of documents and things. It also envisages the receiving of such requests for investigation in India. Besides that, it lays down a chapter of reciprocal arrangements for

[8] Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 23, 2025).

assistance in attachment and forfeiture as well as the management of property, with a separate provision on reciprocal arrangements regarding processes. At the layer of treaty and policy, the Ministry of Home Affairs is the Central Authority for mutual legal assistance in criminal matters. It issues detailed guidelines for outgoing and incoming requests and, along with the Ministry of External Affairs and Indian missions, carries out the coordination. The Department of Legal Affairs is the custodian of the treaty texts. These provisions serve as a complement to platform channels for preservation and disclosure and provide a court with the assurance that foreign evidence has been obtained through lawful routes.

1.4 Initiation and Authorisation of Investigation

A forensic exercise that can be defended should be based on a lawfully triggered process and documented permissions. The triggers for such cyber contexts may be, among other things, a first information report made through the conventional channels, complaints filed through national portals and helplines, immediate calls from banks or payment aggregators, and suo motu cognizance based on the credible information from sectoral agencies. Problems related to jurisdiction arise when the behavior, servers, or victims span different states or countries. The reformed procedure code removes some of the disagreements by electronic communication being recognized at several stages and by prescribing reciprocal routes for cross border acts. Initiation from a privacy point of view must be in line with a lawful purpose and the early documentation should reflect that the necessity and proportionality were considered before devices were imaged or accounts were accessed. The steps of preservation should be there implicitly soon after the log retention windows can be short, and CERT In and Intermediary Guidelines introduce hard timelines that are on the opposite side if there is a delay in the investigators The early cooperation with the sectoral custodians provides more opportunities that volatile and perishable artefacts can be frozen in time without the over collection.

1.4.1 Complaint and Fir Pathways

Some of the most practical and easy to access initiation points for filing a complaint are cyber police stations, general police stations having cyber cells, the national reporting portal, and the national helpline for financial frauds. The portal allows for detailed complaints and keeps track of the sequence and the artefacts that help later forensic steps. The helpline gets financial intermediaries involved in the “golden hour” when stop payment and wallet freezing operations may work, a factor that often decides whether the evidentiary trail ends in attribution and

recovery or gets scattered into unrecoverable networks. Signing up should refer to the territorial and subject matter areas with the necessary detail so as not to encounter jurisdictional disputes. Platform and service provider preservation notices that are immediate should indicate the statutory provisions for retention and request the specific logs, subscriber records, and content pointers. If it is necessary, the time bound follow up with the summons to produce or search warrants should also be documented and scoped to the alleged conduct.[9]

1.4.2 Search and Seizure of Digital Devices

Usually, a court authorized warrant is needed if police want to conduct an intrusive search of homes, offices, or server rooms. The difference between a legitimate search and a fishing expedition is the control of the scope. The code of procedure explicitly includes electronic communication and communication devices within the scope of a summons to produce documents or other things and imposes audio video recording of the search and seizure. As a result, investigators are required to prepare for on-site imaging, live capture decisions, and encryption handling, and they must record every step with timestamps, device identifiers, hash values, and role assignments. Judges still have the authority to physically take the produced documents and supervise the destruction and storage of the property. Encryption can be dealt with by giving the password under the technology provision, along with procedural safeguards that allocate the responsibilities to the competent authorities and require the approval to be documented. This is the route that is especially applicable if the devices or platforms that have been seized contain encrypted material that is responsive to the warrant.

1.4.3 Preservation and Production Orders

Speedy conservation is the link between the start and the full takeover. The law foundation extends from a summons to produce documents or other things that may include electronic communication and communication devices, intermediaries' obligations to preserve removed content and associated records for one hundred eighty days, and CERT In directions requiring logs to be retained in India for one hundred eighty days and reporting within six hours. Investigators need to define specific accounts, time windows, and artefact classes to lessen privacy impact and increase compliance probability. Production orders should indicate export formats and hash algorithms, specify whether subscriber records, IP assignment logs, access logs, or content artefacts are being sought, and request preservation if mutual legal assistance

[9] Cyber Crime Portal, *available at:* https://cybercrime.gov.in/ (last visited on October 22, 2025).

is needed for extraterritorial data. This stage should result in a paper trail linking subsequent forensic images to the first lawful instruction that was in accordance with retention and notification rules.

1.4.4 Role of Intermediaries and Service Providers

Platforms and service providers have become procedural actors as a result of changes in the law. The safe harbor framework imposes obligations related to due diligence, handling of grievances, and takedown. Sectoral incident response rules establish reporting windows and impose logging duties. The technology statute establishes a national incident response team and gives it the authority to issue directions, including those that set log retention and synchronization requirements. The Intermediary Guidelines provide for the preservation of disabled content and associated records for one hundred eighty days and specify certain assistance duties, while recent clarifications have emphasized accountability expectations and refinement of unlawful content specifications. From a forensic standpoint, this is all reflected in timelines, data dictionaries, export formats, and confidentiality undertakings. Lawful orders that are clear in terms of scope and format and that take into account the provider's statutory timelines and constraints will generally be executed more quickly and be less vulnerable to contestation at a later stage, particularly if privacy principles from the data protection statute are upheld in the wording and execution of the request.[10]

1.5 Forensic Acquisition and Preservation

In order for an operation to maintain credibility, the process of acquisition and preservation must be handled very carefully and in a proper manner from the moment the first interaction with the evidence until the final courtroom exhibit. Various international guidelines highlight identification, collection, acquisition, and preservation as the main aspects and also strongly emphasize that integrity controls should be implemented and there should be clear definitions of roles for first responders, specialists, and laboratory managers. Those teams that are out in the field have to make a choice between a live and a dead acquisition, have to disconnect the devices from networks, and have to make plans for the safety of the scene as well as for the capture of volatile data. On the other hand, those teams that are working in a laboratory have to decide whether to do a physical or a logical imaging, have to calculate and write down the

[10] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 English, *available at:* https://mib.gov.in/sites/default/files/2024-02/IT%28Intermediary Guidelines and Digital Media Ethics Code%29 Rules%2C 2021 English.pdf (last visited on October 21, 2025).

hashes, have to retain the write block discipline, and have to make sure that the originals are kept closed while the analysis is being done on the copies that have been verified. Audit trails should be very detailed and they should reflect the information about the person who, when, and what was accessed including the tool versions and the details of the configuration. The Indian evidence code stipulates that the aspects of authenticity and integrity have to be demonstrated by means of certification and records that provide for independent verification. Any documentation that follows international best practices and at the same time is in compliance with the national requirements for admissibility will be able to withstand the scrutiny of an adversary.[11]

1.5.1 On Scene Protocols

A scene plan needs to start with safety and isolation. Wireless isolation is used to avoid remote wiping and the execution of a command. Power decisions and live response triage largely depend on the volatility of data and the risk of encryption locks. Seizure lists definitely have to note the capture of the device along with its make, model, serial number, storage capacity, SIM, or ICCID identifiers, and visible state, together with pictures of the connections and the screen. The procedure code anticipates the audio video recording of the search as well as the seizure, which is one of the means of improving the transparency. First responders documenting should also include the people who found each item, the people who bagged and sealed it, and the time stamps throughout the sequence. In case there is a need for on-site imaging, write blockers, validated tools, and contemporaneous hash computation should be used to create an evidentiary spine that will be able to carry forward into the lab. If only seizure is possible, then rapid preservation notices to platforms and service providers will be the ones to protect perishable logs while devices are being taken for controlled imaging.

1.5.2 Imaging and Hashing

Bit by bit imaging captures all addressable sectors of a disk, which includes slack and unallocated spaces where deleted artefacts are often stored. Logical imaging may be used for certain mobile device extractions or cloud data exports where a full physical access is not possible or is too much. In both cases, hashing at the time of acquisition and for every subsequent copy is absolutely necessary as it establishes an integrity ‘anchor’ which can be

[11] ISO/IEC 27037:2012 Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, *available at:* https://amnafzar.net/files/1/ISO 27000/ISO IEC 27037-2012.pdf (last visited on October 20, 2025).

checked again at any time. Writing blocks, certified software, and contemporaneous logs recording device identifiers, tool versions, hash algorithms, and values are considered best practice. More than one hashing algorithm can be used to lessen worries about collisions while not allowing the process to become too complicated. First of all, the originals have to be sealed and kept safe, and the working copies must be properly labelled and separated. These measures help to change a technical copy into a courtroom ready exhibit with a verifiable provenance that is in line with the requirements for certification and authenticity of national evidence law.[12]

1.5.3 Volatile Data and Live Capture

RAM contents, running processes, network connections, and ephemeral keys are examples of volatile artefacts that can determine attribution and intent, but they also have the risk that the collection may change the state. Instruction for mobile and endpoint forensics is that the triage should be done carefully, the commands executed should be clearly documented, and the tools used should be validated and of minimal footprint. If a device is live and encryption or self-destruct behavior is suspected, a controlled live capture with memory dumps and process listings may be the only option followed by a shutdown and full imaging. If a device is turned off or can be safely separated, dead acquisition is a way of maintaining the device's integrity but at the cost of losing the volatile state. Courts look into whether the live actions taken were necessary and proportionate, and also whether the logs show the commands executed, and the hashes done later confirm that the image was intact. This is the reason why the decision to go live should be an explicit one, it should be recorded and justified against the investigative aim and the risk of irreversible loss.[13]

1.5.4 Cloud and Remote Data

Cloud artefacts are a challenge in terms of jurisdiction and control. Enterprise tenants can use consent, credentials, and provider portals to enable lawful exports or voluntary disclosures by account holders. In the case of public platforms and cross tenant data, legal requisitions should detail account identifiers, time windows, and artefact classes, and should also request preservation while mutual legal assistance is exchanged where the data is located abroad. Decryption and content blocking steps have to depend on the powers given by the technology statute and their safeguard rules. Investigators should also be familiar with the provider's data

[12] *Supra* note 2.
[13] Guidelines on Mobile Device Forensics, *available at:* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf (last visited on October 19, 2025).

dictionaries and export formats to be on the safe side regarding the admissibility of the evidence in court. The concepts of lawful purpose and legitimate uses, as defined by the data protection statute, are still important in this case, particularly when dealing with personal data on a large scale. The aim is to have the necessary and specific artefacts, not to create dragnet collections that a court may later consider as disproportionate. The existence of clear, scoped orders and being provider facing specific helps to shorten the timelines and cut down on the unnecessary exposure of third-party data.[14]

1.6 Chain of Custody and Admissibility

The trip from seizure to the witness stand is very much dependent on documentation and technical integrity. The evidence code considers electronic or digital records as documentary evidence and lays down the special provisions for their admissibility which depend on authenticity, integrity, and correct certification. Chain of custody is initiated at the scene and records all transfer events, storage locations, seals, and access logs. Hash values associate the pictures and exports with the source and enable any subsequent copy to be compared with the acquisition state. Tool calibration records and laboratory accreditation certificates are the reliability indicators Courts will be looking for a story that links the initial lawful authorization, the on-site actions, the imaging and hashing records, the preservation of originals, the audited access to working copies, and the certification that goes with the electronic or digital record. The closer that story follows law and standard, the stronger the evidentiary base will be.[15]

1.6.1 Documentation and Audit Trails

At the same time, documentation is one of the main proof instruments and should not be considered as a mere afterthought. Seizure memos need to explain the items in a detailed manner, should record serial numbers as well as identifiers, and be linked to the photographs. Evidence bags ought to have unique numbers, seals, and signatures along with time stamps. Access logs are supposed to indicate the personnel who opened a particular container or repository and the reason for that. Change control records are supposed to reflect the capturing, verification, and any analytical transformations. The procedure code's requirement for audio video recording of search and seizure, as far as possible, is a transparency layer that can

[14] Section 67C Preservation and Retention of Information by Intermediaries, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=86 (last visited on October 24, 2025).
[15] *Supra* note 4.

alleviate defense doubts about planting or alteration. The goal is to show that the exhibit that is submitted to the court is the same exhibit that was seized or exported, not changed except for the clearly documented and validated steps that were necessary for analysis and reporting.

1.6.2 Authenticity and Integrity Tests

Provenance together with technical markers is what keeps hash validation is the main thing that demonstrates a forensic image or an export has not been changed since the time of acquisition. Tool validation records, also including references to published best practices, show that acquisition and analysis were done in a proper way. Certification under the evidence statute connects the record to its production method and the system that created or stored it, thus letting the judge evaluate the reliability without the judge having to review the whole technical chain in the oral testimony. If there are any doubts about alteration, the presence of stable, sealed originals and re verifiable hashes provides the court with a real way to settle the disagreements. The more detailed the logs about used algorithms, tool versions, and verification events, the less there is a possibility of a guess that the data was tampered with.[16]

1.6.3 Expert Evidence

An expert digital forensics opinion is convincing when the expert thoroughly explains the method, the check, the limitations, and the possible mistakes and at the same time, gives enough detail for another person to get the same result. The expert's qualifications are important, but usually, the courts concentrate on whether the report demonstrates what was done and why those steps were suitable for the artefacts at hand. The court should be informed about the error rates of parsing tools, the extraction coverage for a particular device model, and the known issues with application artefacts instead of these being glossed over. Laboratory accreditation to ISO IEC 17025 standards is a sign of process discipline, documented quality control, and proficiency testing, and a number of public laboratories and private facilities in India are now accredited to this standard, in particular, in the divisions of electronic evidence. A disclosure that combines method, validation references, hashes, and accreditation context enables the judge to follow and trust the journey from the raw data to the courtroom conclusion.[17]

[16] *Supra* note 2.
[17] ISO/IEC 17025 Testing and Calibration Laboratories, *available at:* https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html (last visited on October 22, 2025).

1.6.4 Judicial Assessment Trends

Courts are increasingly understanding the language of electronic records and the processes of hashing, imaging, and certification. They search for authorizations based on law, scope considered proportionate, proper recording of searches, trustworthy imaging, and understandable certification under the evidence statute. Often, exclusion is found where there is a collapse in the chain of custody, where imaging records are absent or inconsistent, where certification is faulty, or where the search seems to be separated from a lawful purpose. Generally, acceptance is found where a clear procedural pathway is apparent and where defense doubts can be resolved by re verification of hashes and inspection of sealed originals. The overall result is that more importance is placed on a disciplined process. It also serves as a reminder that handling in a manner sensitive to privacy is not only principled but also instrumental for admissibility because an overbroad or indiscriminate collection increases the likelihood of judicial discomfort at a later stage.[18]

1.7 Conclusion

Digital forensics in Indian cybercrime investigations is most effective when the scientific method and the legal process complement each other. Laws and regulations now talk directly to electronic communications, device searches, certification, and cross border requests, and sectoral directions provide concrete timelines for reporting and retention. The data protection law sets privacy as a discipline, not a veto, and thus, it invites investigators to articulate lawful purpose, necessity, and proportionality and to demonstrate minimization and accountability. International standards provide the common language for identification, collection, acquisition, and preservation and local practice is in line with global expectations. The institutional network of cyber police, incident responders, critical infrastructure protectors, and accredited laboratories is the dependable backbone that gives the investigations strength. The subsequent stage is about consistency and depth. Consistency refers to SOPs that each unit can implement and judges can identify. Depth denotes validation records, proficiency tests, and honest expert disclosures. This is the way digital evidence moves from seizure to conviction or acquittal with legitimacy intact.[19]

[18] *Supra* note 4.
[19] *Supra* note 1.

Bibliography

- Best Practices for Computer Forensic Acquisitions, *available at:* https://www.swgde.org/wp-content/uploads/2024/03/2023-06-15-SWGDE-Best-Practices-for-Computer-Forensic-Acquisitions-17-F-002-2.0.pdf (last visited on March 27, 2026).
- Cyber Crime Portal, *available at:* https://cybercrime.gov.in/ (last visited on March 22, 2026).
- Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on March 23, 2026).
- Guidelines on Mobile Device Forensics, *available at:* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf (last visited on March 19, 2026).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 English, *available at:* https://mib.gov.in/sites/default/files/2024-02/IT%28Intermediary Guidelines and Digital Media Ethics Code%29 Rules%2C 2021 English.pdf (last visited on March 21, 2026).
- ISO/IEC 17025 Testing and Calibration Laboratories, *available at:* https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html (last visited on March 22, 2026).
- ISO/IEC 27037:2012 Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, *available at:* https://amnafzar.net/files/1/ISO 27000/ISO IEC 27037-2012.pdf (last visited on March 20, 2026).
- ISO/IEC 27037:2012 Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, *available at:* https://www.iso.org/standard/44381.html (last visited on March 28, 2026).
- Section 67C Preservation and Retention of Information by Intermediaries, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=86 (last visited on March 24, 2026).
- The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf (last visited on March 25, 2026).

- The Constitution of India, *available at:* https://www.indiacode.nic.in/bitstream/123456789/16124/1/the_constitution_of_india.pdf (last visited on March 24, 2026).
- The Information Technology Act, 2000, *available at:* https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited on March 26, 2026).