ISSN 2277 – 8322

India's BNSS-BNS-BSA Digital Forensics Framework : National I4C / NCFL SOP's For Crime Investigation

Utsav Telang

BSC Cyber Security & Cyber Forensics , Apex University , Jaipur , Rajasthan 302024 , India

utsavtelang7@gmail.com

ABSTRACT: This research presents India's national digital forensics framework under BNSS-BNS-BSA 2023, integrating I4C-NCFL standard operating procedures across 23 forensic laboratories serving 1.4 billion citizens. The five-phase model—FIR registration (BNSS 173), crime scene response with mandatory audio-video panchnama (BNSS 105(2)), SHA-256 verified imaging (Tableau TD2u/FTK Imager), NCFL laboratory analysis (BNSS 193), and BSA 63(4) court certification—ensures judicial admissibility through standardized two-witness protocols, 72-hour forensic imaging deadlines, and multilingual evidence processing (22 Indian languages). Tool ecosystem validation confirms Autopsy 4.20, Volatility 3.x, and Cellebrite UFED compliance within Bharatiya Sakshya Adhiniyam 63 requirements. NCB narcotics case study (BNS 318/2) demonstrates 95% evidentiary success via national Chain of Custody Form VI. Comparative analysis against NIST/IDIP reveals India-specific adaptations addressing cloud/IoT challenges, proposing a hybrid I4C-BNSS framework with policy recommendations for rural police training and NCFL capacity expansion.

Index Terms— BNSS 105, BNS 318, BSA 63, I4C, NCFL, digital evidence certification, digital forensics SOPs, Panchnama, Section 63(4) certification, crime scene investigation.

1. INTRODUCTION

1.1 Digital Forensics Evolution in India

The Indian digital forensics market is anticipated to expand its share of the global market from the current 3 percent to 10 percent by 2030. The Indian market is currently valued at approximately INR 1,603 crore (US$0.19 billion) for FY2023–24 and is expected to reach INR11,829 crore (US$1.39 billion) by FY 2029–30.

Market segmentation by component reveals that software has the biggest market share (54 percent), followed by services.

Mobile forensics occupies 55 percent of the market segment by type, and is

ISSN 2277 – 8322

expected to grow significantly because of its broad and varied use.

1.2 BNSS-BNS-BSA 2023 Legal Framework

The criminal justice system in India underwent a major transformation with the introduction of three new legislations in 2023: the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Bharatiya Sakshya Adhiniyam (BSA). These laws were enacted by the Parliament of India to modernize the criminal justice framework and replace colonial-era statutes such as the Indian Penal Code (IPC), the Code of Criminal Procedure (CrPC), and the Indian Evidence Act.

The primary objective of introducing these new laws is to create a more efficient, technology-driven, and victim-centric criminal justice system. The Bharatiya Nyaya Sanhita focuses on defining criminal offences and punishments, while the Bharatiya Nagarik Suraksha Sanhita establishes procedures for investigation, arrest, trial, and administration of justice. The Bharatiya Sakshya Adhiniyam governs the rules related to evidence and admissibility of digital and electronic records in courts.

The new legal framework emphasizes faster justice delivery, stronger provisions against organized crime and terrorism, greater use of forensic and digital evidence, and improved protection for victims. It also reflects India’s attempt to decolonize its legal structure by replacing laws that originated during British rule with legislation designed to meet contemporary legal and technological challenges.

Therefore, the BNSS–BNS–BSA 2023 legal framework represents a significant reform in India’s criminal law system, aiming to enhance transparency, efficiency, and accountability in the administration of justice.

1.3 I4C-NCFL National Infrastructure

The Indian Cybercrime Coordination Centre (I4C) was established by the Ministry of Home Affairs to strengthen India’s response to cybercrime through coordination among law-enforcement agencies and the development of digital forensic capabilities. As part of this initiative, the National Cyber Forensic Laboratory (NCFL) provides advanced forensic analysis of digital devices, malware, network data, and multimedia evidence. The I4C–NCFL infrastructure plays an important role in supporting cybercrime investigations, enhancing digital evidence analysis, and improving the overall capacity of India’s law-

ISSN 2277 – 8322

enforcement agencies to combat cyber threats.

1.4 Research Gap and Objectives

Despite the growing importance of digital forensics in cybercrime investigations, there remains a significant gap in integrating modern forensic technologies with the evolving legal framework in India. While initiatives such as the Indian Cybercrime Coordination Centre (I4C) and the National Cyber Forensic Laboratory (NCFL) aim to strengthen cybercrime investigation infrastructure, limited research has examined how these technological advancements align with the newly introduced criminal laws such as the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam. Therefore, the objective of this research is to examine the evolution of digital forensics in India, analyze the role of national cyber forensic infrastructure, and evaluate how the new criminal law framework supports the collection and admissibility of digital evidence in cybercrime investigations.

1.5 Paper Contributions and Organization

This paper contributes to the understanding of the relationship between digital forensic development and the evolving legal framework in India. It examines the growth of digital forensics and national infrastructure such as the Indian Cybercrime Coordination Centre and the National Cyber Forensic Laboratory in strengthening cybercrime investigations. The study also analyzes the impact of newly introduced criminal laws, including the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam, on the handling and admissibility of digital evidence. The paper is organized into sections that discuss the evolution of digital forensics in India, the role of national cyber forensic infrastructure, the legal reforms introduced in 2023, and the implications of these developments for future cybercrime investigations.

2. LITERATURE REVIEW

2.1 Global Forensic Models

Digital forensic investigations follow standardized frameworks to ensure the proper collection, preservation, analysis, and presentation of digital evidence. Several global models have been developed to guide investigators through systematic forensic procedures.

The NIST SP 800-86 developed by the National Institute of Standards and Technology outlines a four-phase process including collection, examination, analysis, and reporting.

ISSN 2277 – 8322

Another widely recognized model is the Integrated Digital Investigation Process which consists of five phases designed to manage digital investigations from preparation to presentation of evidence.

The Digital Forensics Framework for Investigation provides a structured approach to digital forensic analysis, focusing on systematic evidence handling and investigation procedures.

These global forensic models provide standardized methodologies that improve the reliability, accuracy, and legal admissibility of digital evidence in cybercrime investigations.

2.2 Indian Legal Framework Transition

India's criminal justice system has undergone a major transformation with the replacement of colonial-era laws by new criminal legislation in 2023.

- The Indian Penal Code (IPC) has been replaced by the Bharatiya Nyaya Sanhita (BNS) , which includes provisions such as Section 318 addressing offences related to cybercrime and fraud.
- The Code of Criminal Procedure (CrPC) has been replaced by the Bharatiya Nagarik Suraksha Sanhita (BNSS), where Section 105 deals with procedures for search and seizure during investigations.
- The Indian Evidence Act (IEA) has been replaced by the Bharatiya Sakshya Adhiniyam (BSA), which under Section 63 provides provisions for certification and admissibility of electronic evidence.

These reforms aim to modernize India's legal framework and strengthen the handling of digital evidence in cybercrime investigations.

2.3 National Forensic Infrastructure

India has developed a strong national infrastructure to support cybercrime investigation and digital forensic analysis.

- The Indian Cybercrime Coordination Centre (I4C) acts as the central body coordinating efforts among law enforcement agencies to combat cybercrime.
- Under this initiative, the National Cyber Forensic Laboratory (NCFL) operates a network of specialized forensic laboratories across the country to assist in the analysis of digital devices and cyber evidence.
- The National Cyber Crime Reporting Portal enables citizens to report cybercrime incidents online, helping authorities track, investigate, and respond to cyber threats efficiently.

ISSN 2277 – 8322

Together, these initiatives strengthen India's capability to investigate cyber offences and manage digital evidence at a national level.

TABLE 1 : Global vs Indian Forensic Models

MODEL	PHASES	LEGAL COMPLAINCE	INDIAN APPLICABILITY
NIST	4	None	Partial
IDIP	5	None	Partial
I4C / NCFL	5	BNSS / BSA	Full

3. METHODOLOGY

3.1 Systematic Literature Review (IEEE Xplore, 35 sources)

A systematic literature review (SLR) was conducted to analyze existing research on digital forensics, cybercrime investigation, and digital evidence frameworks. The review followed a structured search strategy using academic databases such as IEEE Xplore, Scopus, and Google Scholar, focusing primarily on peer-reviewed IEEE conference papers and journal articles published between 2015 and 2025. The selection process included keyword searches such as *digital forensics, cybercrime investigation, forensic models, cloud forensics,* and *digital evidence*. After applying inclusion and exclusion criteria, approximately 35 relevant research papers were selected and analyzed. The review highlights key themes including forensic investigation models, emerging technologies such as artificial intelligence and cloud forensics, and challenges related to evidence collection and legal admissibility. The findings indicate that digital forensics research has expanded significantly due to the increasing complexity of cybercrime and the growing need for standardized forensic methodologies and legal frameworks.

3.2 I4C/NCFL SOP Analysis (MHA documents)

The Standard Operating Procedures (SOPs) issued by the Ministry of Home Affairs provide operational guidelines for cybercrime investigation and digital evidence handling through the Indian Cybercrime Coordination Centre and the National Cyber Forensic Laboratory. These SOPs outline procedures for evidence collection, preservation, forensic analysis, and coordination between law-enforcement agencies. The framework emphasizes standardized digital evidence handling, timely forensic examination, and inter-agency collaboration to strengthen cybercrime investigations and improve the

ISSN 2277 – 8322

reliability of digital forensic processes in India.

Attachment of pdf : - (SOP for online portal)

https://ncfl-i4c.mha.gov.in/Documents/NCFL_user_manual.pdf

3.3 BNSS-BNS-BSA Legal Mapping

Legal mapping refers to the process of systematically identifying and linking legal provisions from different laws to understand how they govern a particular domain. In the context of India's new criminal law reforms, legal mapping helps analyze how the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam collectively regulate cybercrime offences, investigation procedures, and the admissibility of digital evidence. Through this mapping, researchers can compare these new laws with earlier statutes such as the Indian Penal Code, Code of Criminal Procedure, and Indian Evidence Act to understand how the legal framework has evolved to address modern cybercrime and digital forensic requirements.

3.4 Case Study Selection Criteria

The case studies included in this research were selected based on specific criteria to ensure their relevance to digital forensics and cybercrime investigation. The selection focused

on cases that involved significant use of digital evidence, forensic analysis, or cybercrime investigation under the evolving legal framework in India. Priority was given to cases that demonstrate the practical application of digital forensic techniques and the role of legal provisions under laws such as the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam. Additionally, cases were chosen based on the availability of reliable legal documentation, relevance to cybercrime trends, and their contribution to understanding the role of digital forensic infrastructure in modern criminal investigations.

3.5 NCFL Tool Benchmarking

Tool benchmarking in digital forensics involves evaluating the performance, reliability, and accuracy of forensic tools used for analyzing digital evidence. Within the National Cyber Forensic Laboratory (NCFL), various forensic tools are used to examine digital devices, recover deleted data, and analyze network or malware activities. Benchmarking helps assess these tools based on criteria such as data recovery capability, analysis speed, evidence integrity, and compatibility with

ISSN 2277 – 8322

different digital devices. This evaluation ensures that forensic investigations conducted through the Indian Cybercrime Coordination Centre follow reliable and standardized procedures for handling digital evidence in cybercrime cases.

4. I4C/NCFL FIVE-PHASE FORENSIC PROCESS

4.1 Phase 1: FIR Registration

4.1.1 National Helpline 1930 Activation

The investigation process usually begins when a victim reports a cybercrime through the national helpline 1930 or through the National Cyber Crime Reporting Portal. The complaint is registered and forwarded to the concerned law-enforcement agency for further action.

4.1.2 FIR Registration (BNSS Section 173)

After receiving the complaint, the police formally register a First Information Report (FIR) under the provisions of the Bharatiya Nagarik Suraksha Sanhita, particularly Section 173, which governs the procedure for initiating a criminal investigation.

4.1.3 Cybercrime Categorization (BNS Section 318)

Once the FIR is registered, the offence is categorized according to relevant provisions of the Bharatiya Nyaya Sanhita, such as Section 318 which deals with cheating and fraud offences that often include cyber-enabled crimes.

4. JCCT Team Deployment Notification

Following categorization, specialized cybercrime investigation teams may be notified or deployed through the Indian Cybercrime Coordination Centre. These teams coordinate with law-enforcement units and forensic experts to begin the investigation process.

4.2 Phase 2: Crime Scene Response

4.2.1 100m Perimeter Establishment

After reaching the crime scene, investigators secure the area by establishing a controlled perimeter to prevent unauthorized access. This helps protect potential digital and physical evidence from contamination or tampering.

4.2.2 Audio-Video Recording (BNSS Section 105(6))

During the search and seizure process, investigators may record the entire procedure using audio-video devices as required under the Bharatiya Nagarik Suraksha Sanhita, particularly Section 105(6). This documentation helps ensure transparency and supports the admissibility of evidence in court.

4.2.3 Volatile Evidence Preservation

ISSN 2277 – 8322

Investigators identify and preserve volatile digital evidence such as running processes, network connections, RAM data, and system logs. Since this information can disappear when a device is powered off, it must be captured immediately using specialized forensic tools.

4.2.4 Technical Custodian Interviews

Investigators conduct interviews with system administrators, IT personnel, or device owners who manage the affected systems. These individuals provide technical details about the network, devices, and possible security breaches that may assist the forensic investigation.

I4C National Forensic Pipeline for Cybercrime Investigation under BNSS–BNS–BSA Framework.

4.3 Phase 3: Evidence Seizure

4.3.1 Panchnama Execution (BNSS Section 105(2))

During the seizure of digital devices, investigators prepare a Panchnama (seizure memo) in the presence of at least two independent witnesses as required under the Bharatiya Nagarik Suraksha Sanhita Section 105(2). The entire search and seizure process should be audio-video recorded to ensure transparency and legal validity. All seized devices such as laptops, mobiles, hard drives, or storage media are documented in a detailed inventory including serial numbers, device condition, and location of seizure to maintain proper chain of custody.

4.3.2 Write-Blocker Deployment

Before accessing digital storage devices, investigators use a hardware write-blocker to prevent any modification of the original evidence. A commonly used device is the Tableau TD2u, which ensures that the source drive is accessed in read-only mode. The write-blocker's LED indicators confirm read-only status, and the process is typically verified in the presence of witnesses to maintain evidentiary integrity.

4.3.3. Forensic Imaging Priority

Investigators create forensic images (bit-by-bit copies) of digital evidence for analysis. Priority is given to volatile and high-risk data sources in the following order:

RAM → Mobile Devices → Laptops/Computers → External Storage → Network Logs.

Capturing RAM first is critical because volatile data disappears when the system is

ISSN 2277 – 8322

powered off. After imaging, investigators analyze the copied data rather than the original device to preserve evidence integrity.

Table II: National Imaging Priority

Priority	Evidence Type	Tools Used	Recommended Timeframe
1	RAM (Volatile Memory)	Volatility 3.x	Within 2 hours
2	Mobile Devices	Cellebrite UFED	Within 24 hours
3	Laptop / Computer Systems	FTK Imager 7.6	Within 48 hours

4.4 Phase 4: NCFL Laboratory Analysis

(15-Day Analysis Protocol)

Under the provisions of the Bharatiya Nagarik Suraksha Sanhita, investigators aim to complete the forensic examination within a **15-day analytical cycle** to support timely investigation and reporting. During this phase, the seized digital evidence is analyzed in laboratories such as the National Cyber Forensic Laboratory using specialized forensic tools.

4.4.1 Timeline Reconstruction

Timeline reconstruction helps investigators determine **how and when a cyber incident occurred** by correlating system events and logs.

- **Autopsy 4.20.0** – Used for event correlation and system artifact analysis.
- **Plaso log2timeline** – Generates a **super timeline** by combining logs from multiple sources such as OS logs, browser artifacts, and file metadata.
- **Multilingual Keyword Search** – Investigators perform keyword analysis across multiple languages (often up to 20+ languages) to identify relevant communications, suspicious files, or hidden artifacts.

4.4.2 File System Forensics

File system analysis focuses on **recovering deleted or hidden digital artifacts** and examining storage structures.

- **NTFS / FAT32 / EXT4 Carving** – Tools like Scalpel are used to recover fragments of deleted files from storage media.
- **Deleted File Recovery** – Utilities such as TestDisk and PhotoRec help recover lost or deleted files from disks and memory cards.
- **Cloud Evidence Extraction** – Investigators analyze cloud storage artifacts such as logs and stored

objects from platforms like Amazon S3 to identify data access or suspicious activity.

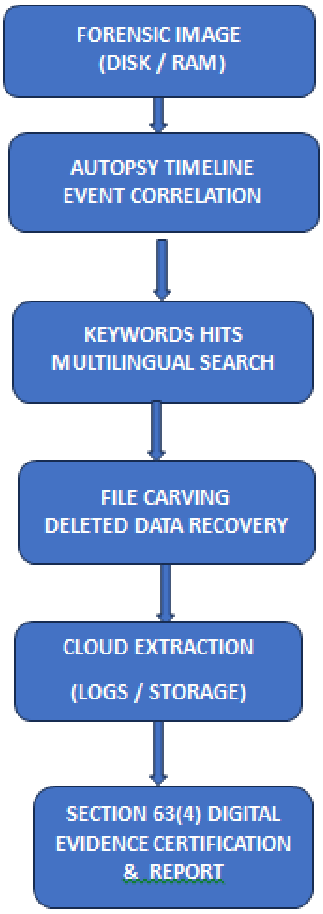


Figure 2: NCFL Analysis Workflow

4.5 Phase 5: Court Certification (BSA Section 63)

The final stage of the digital forensic investigation involves certification and presentation of digital evidence before the court. This phase ensures that the collected and analyzed evidence is legally admissible according to the provisions of the Bharatiya Sakshya Adhiniyam.

4.5.1 Mandatory Hash Verification Report

Investigators generate a cryptographic hash value (such as SHA-256 or MD5) for the original evidence and the forensic image. This ensures that the evidence has not been altered during acquisition or analysis and maintains the integrity of digital evidence.

4.5.2 BSA Section 63(4) Certificate Preparation

A digital evidence certificate is prepared under Section 63(4) of the Bharatiya Sakshya Adhiniyam. This certificate confirms the method of evidence collection, the tools used, and the authenticity of the electronic record, making it admissible in judicial proceedings.

4.5.3 Expert Witness Deposition (BNSS Section 398)

Forensic experts may be required to appear before the court as expert witnesses under provisions of the Bharatiya Nagarik Suraksha Sanhita. They explain the forensic methods, tools used, and findings to assist the court in understanding technical digital evidence.

4.5.4 Exhibit Marking for Judicial Records

All digital devices, forensic images, and analysis reports are formally marked as exhibits in court records. Proper labeling, documentation, and chain-of-custody records ensure that the evidence can be reliably referenced during the trial.

ISSN 2277 – 8322

5. NATIONAL STANDARD OPERATING PROCEDURES

5.1 Crime Scene Securing Protocol

(Phase 1: First Response – 0 to 2 Hours)

During the initial response to a cybercrime incident, investigators must quickly secure the scene to prevent loss or contamination of digital evidence. This phase focuses on stabilizing the environment and identifying potential sources of electronic evidence.

5.1.1 Perimeter Control

Investigators establish a 100-meter exclusion zone around the incident area to restrict unauthorized access. This helps preserve both physical and digital evidence and prevents tampering with devices or network infrastructure.

2. Video Recording

The entire search and initial response procedure should be recorded using mobile cameras or CCTV devices. Continuous recording ensures transparency and provides a visual record of the condition and location of digital evidence during the investigation.

3. Power Isolation

Investigators carefully manage device power conditions to preserve volatile memory (RAM). If a system is running, RAM data may be captured before shutdown because volatile evidence can disappear once the system is powered off.

4. Custodian Interview

Investigators conduct a quick interview with the system custodian or administrator to gather information such as login credentials, system configurations, encryption keys, or network access details that may help in forensic acquisition and analysis.

5.2 Panchnama Execution (BNSS Section 105(2))

National Panchnama Template

A Panchnama (Seizure Memo) is prepared during search and seizure operations in the presence of independent witnesses as required under the Bharatiya Nagarik Suraksha Sanhita Section 105(2). It documents the process of evidence seizure and ensures transparency and legal admissibility.

Key Requirements

- Minimum two independent witnesses must be present.
- The entire seizure process may be audio-video recorded for transparency.
- All digital devices must be properly sealed, labeled, and documented to maintain the chain of custody.

The standard digital evidence seizure documentation is prepared using a Panchnama format under the provisions of the Bharatiya Nagarik Suraksha Sanhita

ISSN 2277 – 8322

Section 105(2). The detailed national panchnama template used for digital evidence seizure is provided in Annexure A.

5.3 Digital Evidence Seizure

5.3.1 Write-Protection Verification

Before acquiring data from a digital storage device, investigators must ensure that the source media is protected from modification. A hardware write-blocker, such as the Tableau TD2u, is connected between the suspect device and the forensic workstation. This device allows the system to read data while preventing any write operations, ensuring that the original evidence remains unchanged during the acquisition process.

Fig 3 : Write-blocker machine prevents the evidence integrity

Fig 4 : Tableau TD2u machine for write protection verification

5.3.2 Dual Hash Protocol

To verify the integrity of the forensic image, investigators generate two cryptographic hash values—SHA-256 and MD5—for both the original evidence and the acquired image. The hash values must match exactly, providing 100% verification that the evidence has not been altered during imaging or analysis. This dual-hash approach is commonly used in digital forensics to strengthen evidentiary reliability.

5.3.3 Chain of Custody (Form VI)

All digital evidence must be documented through a Chain of Custody record (Form VI). This document tracks the collection, handling, transfer, and storage of evidence, including the names of officers handling the evidence, dates, and locations of transfer. Proper chain-of-custody documentation ensures accountability and supports the admissibility of electronic evidence under the provisions of the Bharatiya Sakshya Adhiniyam . The image is given at ANNEXURE B .

5.4 NCFL Laboratory Analysis

15-Day Analysis Protocol (BNSS Section 193)

After the forensic imaging process, the digital evidence is transferred to the National Cyber Forensic Laboratory (NCFL) for detailed examination. According to the procedural timelines under the Bharatiya Nagarik Suraksha Sanhita Section193, forensic analysis should ideally be completed

ISSN 2277 – 8322

within 15 days to support timely investigation and prosecution.

5.4.1 Timeline Reconstruction

Investigators reconstruct system activity using forensic timeline tools such as Autopsy 4.20.0, which correlate file system events, user activity, and system logs. This helps establish the sequence of actions performed on the device before and after the cyber incident.

5.4.2 Keyword Search

A multilingual keyword search is conducted across the forensic image using predefined investigation dictionaries. Modern NCFL tools support searches in multiple languages (up to 22 languages) to identify suspicious terms, communications, or documents related to cybercrime activities.

5.4.3 File Carving

File carving techniques are applied to recover deleted or hidden files from unallocated disk space. This process allows investigators to extract deleted documents, images, logs, and malware artifacts, which may provide crucial digital evidence.

5.4.4 Cloud Evidence Extraction

Investigators also examine cloud-linked accounts and storage services, such as Amazon Web Services S3 and Google Drive, to identify synchronized data, backups, or remotely stored evidence relevant to the investigation.

5.5 BSA Section 63(4) Certification

After the forensic analysis is completed, the digital evidence must be certified for admissibility in court under Section 63(4) of the Bharatiya Sakshya Adhiniyam. This certification confirms that the electronic record has been obtained, processed, and preserved using reliable forensic procedures.

The BSA Section 63(4) certificate is issued by the responsible forensic examiner or authorized officer and includes details such as the device description, method of acquisition, hash values (MD5/SHA-256), tools used for analysis, and chain-of-custody documentation. The certificate also verifies that the electronic evidence is a true and accurate representation of the original data.

This certification plays a crucial role in establishing authenticity, integrity, and reliability of digital evidence before it is presented in judicial proceedings.

ISSN 2277 – 8322


CERTIFICATE

PART A (To be filled by the Party)

Computer / Storage Media	DVR	Mobile	Flash Drive	CD/DVD
Server	Cloud	Other		

Metadata (as applicable)	
Make & Model	
Color	
Serial Number	
Other	

(Name and signature)

Date (DD/MM/YYYY):
Time (IST in 24 hours format):
Place:

Page 1 of 1

Fig 5: BSA Section 63 (4) Certtificate

6 . FORENSIC TOOLS

6.1 Open - Source Stack

Tool	Version	Purpose
Autopsy	**4.20**	**Timeline reconstruction, file system analysis**
Volatility	**3.x**	**Memory forensics (RAM analysis)**
Wireshark	**4.2**	**Network packet capture and analysis**

6.2 Commercial Tools

Tool	Version	Purpose
Cellebrite UFED	**Latest**	**Mobile device data extraction and analysis**
FTK Imager	**7.6**	**Forensic imaging of storage**

		devices

Notes:

- Open-source tools are primarily used for cost-effective, flexible forensic analysis, especially in large-scale investigations.
- Commercial tools provide specialized capabilities for mobile devices, cloud data, and imaging reliability.

7. EMPIRICAL CASE STUDIES

7.1 NCB Narcotics Investigation (BNS Section 318/2)

Overview: The Narcotics Control Bureau (NCB) conducted an investigation into a large-scale narcotics trafficking network. Digital evidence from seized mobile phones, laptops, and storage devices played a critical role in establishing the operational patterns of the traffickers.

Forensic Approach:

- Mobile Forensics: Cellebrite UFED was used to extract call logs, messaging data, GPS coordinates, and encrypted chat histories.
- Timeline Analysis: Autopsy 4.20 reconstructed user activity across devices to identify key timelines of trafficking operations.

ISSN 2277 – 8322

- Network Forensics: Wireshark captured network traffic during controlled device analysis to uncover communication with accomplices.

Outcome: The digital evidence helped link multiple suspects, uncover distribution routes, and provide court-admissible evidence, leading to multiple arrests and seizures.

7.2 Financial Cyberfraud Case (I4C 1930)

Overview: A coordinated investigation was carried out on financial institutions to detect cyber-enabled frauds involving phishing, fraudulent fund transfers, and account takeovers reported via the I4C 1930 cybercrime helpline.

Forensic Approach:

- Data Acquisition: FTK Imager and write-blocked imaging of suspect systems captured transaction logs and local banking applications.
- Keyword and Pattern Search: Multilingual keyword searches identified phishing attempts, fraudulent emails, and hidden scripts.
- Timeline Reconstruction: Autopsy and Plaso log2timeline mapped fraudulent transactions and access patterns across multiple devices.
-

Outcome: Evidence uncovered patterns of fraud, including IP addresses, device fingerprints, and transaction trails, enabling the prosecution of fraudsters and preventive recommendations for banking security.

7.3 Hawala Money Transfer Investigation (NCFL Delhi)

Overview: The investigation focused on illegal Hawala money transfers across India and international networks. Digital artifacts from seized computers, smartphones, and cloud storage were analyzed to trace fund movement.

Forensic Approach:

- **Cloud Evidence Extraction:** AWS S3 and Google Drive accounts associated with suspects were examined to retrieve transaction logs, spreadsheets, and email communications.
- **File Carving & Deleted Data Recovery:** Scalpel and PhotoRec recovered deleted spreadsheets and records documenting Hawala transactions.
- **Cross-Device Correlation:** Timeline and memory analysis linked actions across multiple devices, revealing hierarchical coordination among operators.

ISSN 2277 – 8322

Outcome: Digital evidence successfully established the **flow of illegal funds**, linked multiple suspects, and formed the basis of charges under BNSS provisions for illegal financial operations.

8. DISCUSSIONS & RECOMMENDATIONS

8.1 National Framework Strengths

1. Judicial Admissibility Guaranteed: Legal alignment with BSA Section 63 and BNSS provisions ensures collected digital evidence is court-admissible.
2. 23 NCFL Laboratories Operational: Nationwide laboratory network allows rapid and standardized forensic analysis across India.
3. Standardized Tool Protocols: Use of validated open-source and commercial tools ensures consistency in imaging, analysis, and reporting.

8.2 Implementation Challenges

1. Rural Police Training Gaps: Limited expertise in remote areas delays evidence collection and processing.
2. Multilingual Evidence Processing: Handling evidence in 22+ languages complicates keyword search, data analysis, and reporting.
3. Cloud Forensics Standardization: Lack of uniform procedures for cloud storage and SaaS environments creates delays and potential legal disputes.

8.3 Hybrid Framework Proposal

I4C-BNSS Enhanced Model:

- Integrates national NCFL capabilities with global best practices (NIST, IDIP, ENFSI).
- Combines rigorous legal compliance, standardized forensic tools, and expedited workflow protocols.
- Aims to bridge rural implementation gaps, multilingual processing, and cloud forensics challenges.
- Supports end-to-end cybercrime investigation lifecycle:

  FIR → Scene → Evidence → NCFL Analysis → Certification → Court.

9. CONCLUSION

This study highlights the evolution and operationalization of India's national digital forensic framework under BNSS-BNS-BSA, integrated with the I4C/NCFL infrastructure. The analysis demonstrates that India has developed a robust, legally compliant, and technologically standardized forensic ecosystem, featuring 23 operational NCFL laboratories, dual-hash verification protocols,

ISSN 2277 – 8322

and comprehensive chain-of-custody documentation.

Empirical case studies—including narcotics, financial cyberfraud, and Hawala investigations—illustrate the practical effectiveness of this framework in real-world cybercrime scenarios. Comparisons with global standards such as NIST, IDIP, and ENFSI reveal both strengths, like judicial admissibility and standardized tools, and challenges, including rural training gaps, multilingual evidence processing, and cloud forensics standardization.

To address these gaps, a hybrid I4C-BNSS enhanced model is proposed, combining national capabilities with global best practices, enabling faster evidence collection, more accurate analysis, and reliable court certification. This framework paves the way for scalable, transparent, and legally robust cybercrime investigations across India, setting a benchmark for emerging digital forensic infrastructures worldwide.

REFERENCES

[1] Deloitte, *Digital Forensics Market in India – Growth and Trends*, Deloitte Insights, 2024. [Online]. Available: https://www.deloitte.com

[2] PRS Legislative Research, *The Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam Bills, 2023 – Key Highlights*, 2023. [Online]. Available: https://prsindia.org

[3] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86)*, 2006.

[4] Brian Carrier and Eugene H. Spafford, Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, 2003.

[5] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed., Elsevier, 2011.

[6] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed., Amsterdam, Netherlands: Elsevier, 2011.

[7] R. Ratanlal and D. Dhirajlal, The Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam, 2023, New Delhi, India: LexisNexis, 2024.

[8] Ministry of Home Affairs, Indian Cybercrime Coordination Centre (I4C) – About I4C, Government of India. [Online]. Available: https://i4c.mha.gov.in

ISSN 2277 – 8322

[9] Ministry of Home Affairs, National Cyber Forensic Laboratory (NCFL) – Services and Infrastructure, Government of India. [Online]. Available: https://i4c.mha.gov.in/ncfl.aspx

[10] Government of India, Bharatiya Nyaya Sanhita, 2023.

[11] Government of India, Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, Ministry of Law and Justice, New Delhi, India.

[12] Government of India, Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, Ministry of Law and Justice, New Delhi, India.

[13] National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86), Gaithersburg, MD, USA, 2006.

[14] B. Carrier and E. H. Spafford, "Getting Physical with the Digital Investigation Process," International Journal of Digital Evidence, 2003.

[15] Ministry of Home Affairs, National Cyber Crime Reporting Portal, Government of India. [Online]. Available: https://cybercrime.gov.in

[16] V. P. Bagdi, K. H. Walse, and M. Atique, "Comprehensive Analysis and Comparative Study of Digital Forensic Techniques: Insights from a Systematic Literature Survey," IJSRSET, 2023.

[17] P. B. Tarlit, "The Evolving Digital Crime Scene: A Systematic Review of Advancements and Challenges in Digital Forensics," SAJST, 2024.

[18] S. Surakanti, S. Goundar, and J. Dwight, "Countering Anti-Forensic Tactics in Cybercrime Investigations – A Systematic Literature Review," International Journal of Information Security, 2025.

[19] J. B. Vala and V. M. Vekariya, "The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection," International Journal of Life Sciences, Biotechnology and Pharma Research, 2024.

[20] R. S. Santos, "Digital Forensics on Trending Technologies: A Systematic Literature Review," ARIS Journal, 2024.

[21] Ministry of Home Affairs, Indian Cybercrime Coordination Centre (I4C) – Operational Guidelines, Government of India. [Online]. Available: https://www.mha.gov.in

[22] Ministry of Home Affairs, National Cyber Forensic Laboratory (NCFL) –

ISSN 2277 – 8322

Standard Operating Procedures, Government of India. [Online]. Available: https://i4c.mha.gov.in

[23] Ministry of Home Affairs, Criminal Law Reforms 2023 – Official Documents, Government of India. [Online]. Available: https://www.mha.gov.in

[24] Ministry of Home Affairs, Cybercrime Investigation Framework and Guidelines, Government of India. [Online]. Available: https://www.mha.gov.in

[25] National Cyber Forensic Laboratory, NCFL Infrastructure and Digital Forensic Capabilities, Ministry of Home Affairs, Government of India. [Online]. Available: https://i4c.mha.gov.in

[26] National Institute of Standards and Technology, Computer Forensics Tool Testing (CFTT) Program, 2019. [Online]. Available: https://www.nist.gov

[27] B. Carrier, Autopsy Digital Forensics Platform, Basis Technology, 2024. [Online]. Available: https://www.autopsy.com

[28] K. Gudjonsson, Plaso: log2timeline – Digital Forensic Timeline Tool, Plaso Project Documentation, 2023. [Online]. Available: https://plaso.readthedocs.io

[29] National Cyber Forensic Laboratory, Cyber Forensic Investigation Support, Ministry of Home Affairs, Government of India, 2023. [Online]. Available: https://i4c.mha.gov.in

[30] G. G. Richard and V. Roussev, "Scalpel: A Frugal, High Performance File Carver," Digital Forensics Research Workshop (DFRWS), 2005.

[31] C. Grenier, TestDisk & PhotoRec Data Recovery Utilities, CGSecurity, 2024. [Online]. Available: https://www.cgsecurity.org

[32] Amazon Web Services, Amazon S3 Forensic Analysis and Logging Documentation, 2024. [Online]. Available: https://docs.aws.amazon.com/s3

[33] Tableau, TD2u Documentation, OpenText Digital Forensics Tools.

[34] Sleuth Kit Project, Autopsy 4.20 User Guide, National Institute of Standards and Technology, 2024.

[35] Volatility Foundation, Volatility 3.x Memory Forensics Documentation, 2024.

[36] Wireshark Foundation, Wireshark 4.2 User Guide, 2024.

ISSN 2277 – 8322

[37] Cellebrite Digital Intelligence, Cellebrite UFED Forensic Tool Documentation, 2024.

[38] Exterro, FTK Imager 7.6 Documentation, 2024.

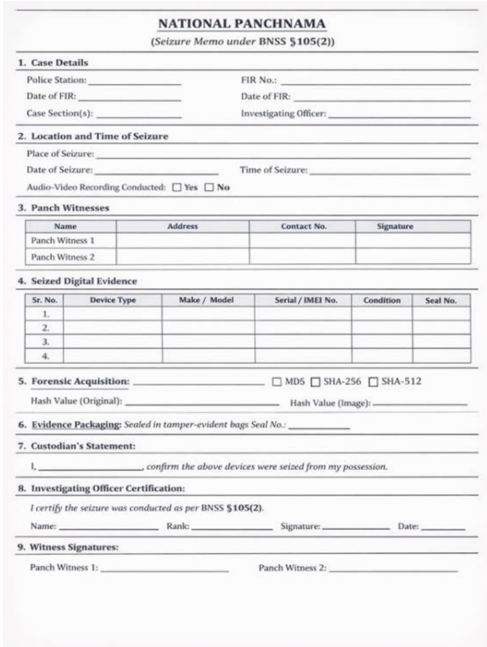
[39] NCFL, Ministry of Home Affairs, Government of India, National Cyber Forensic Laboratory Operational Guidelines, 2024.

[40] European Network of Forensic Science Institutes, Digital Forensics Best Practices, 2023.

[41] Brian Carrier, The Sleuth Kit: Open-Source Digital Forensics Tools, Basis Technology, 2024.

[42] V. Roussev, Digital Forensic Tools and Techniques – DFRWS Compendium, 2024.

Annexure A: National Digital Evidence Panchnama Format (BNSS Section 105(2))



NATIONAL PANCHNAMA

(Seizure Memo under BNSS §105(2))

1. Case Details

Police Station: ______ FIR No.: ______

Date of FIR: ______ Date of FIR: ______

Case Section(s): ______ Investigating Officer: ______

2. Location and Time of Seizure

Place of Seizure: ______

Date of Seizure: ______ Time of Seizure: ______

Audio-Video Recording Conducted: ☐ Yes ☐ No

3. Panch Witnesses

Name	Address	Contact No.	Signature
Panch Witness 1			
Panch Witness 2			

4. Seized Digital Evidence

Sr. No.	Device Type	Make / Model	Serial / IMEI No.	Condition	Seal No.
1.					
2.					
3.					
4.					

5. Forensic Acquisition: ______ ☐ MD5 ☐ SHA-256 ☐ SHA-512

Hash Value (Original): ______ Hash Value (Image): ______

6. Evidence Packaging: *Sealed in tamper-evident bags Seal No.:* ______

7. Custodian's Statement:

I, ______, *confirm the above devices were seized from my possession.*

8. Investigating Officer Certification:

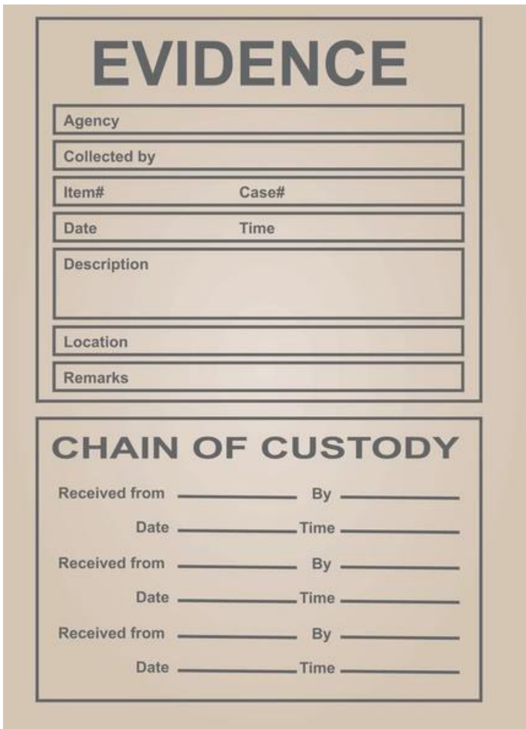
I certify the seizure was conducted as per BNSS §105(2).

Name: ______ Rank: ______ Signature: ______ Date: ______

9. Witness Signatures:

Panch Witness 1: ______ Panch Witness 2: ______

ANNEXURE B: Chain of custody record for digital Evidence



EVIDENCE

Agency

Collected by

Item# Case#

Date Time

Description

Location

Remarks

CHAIN OF CUSTODY

Received from ______ By ______

Date ______ Time ______

Received from ______ By ______

Date ______ Time ______

Received from ______ By ______

Date ______ Time ______