Tracing the Digital Trail: an Analytical Study of Cyber Crime Investigation Methods in India

Daxeshkumar Joshi
Research Scholar (Ph.D), Computer Science and Information Technology

***Abstract*—India's rapid digitization has expanded the scope and complexity of cybercrime, compelling law-enforcement agencies (LEAs) to adopt new investigation methods that combine digital forensics, open-source intelligence (OSINT), platform cooperation, and inter-agency coordination. This study analyzes contemporary methods used by Indian investigators to trace "digital trails"—including seizure and imaging of devices, log correlation across platforms, cryptocurrency tracing, lawful interception, and cross-border mutual legal assistance (MLA) workflows—alongside the legal-privacy context shaped by the Information Technology (IT) Act, CERT-In directions, and the Digital Personal Data Protection (DPDP) Act. Using a mixed-methods design, we considered secondary literature and a primary dataset that mimics a multi-state set of interviews (n=48) with police cyber cells, prosecutors, and digital forensics practitioners, plus a structured case-log abstraction (N=212 cases) spanning financial fraud, cyber-extortion, child sexual abuse material (CSAM), business email compromise (BEC), and social-media harassment. Descriptive statistics and hypothesis tests illustrate associations between standardized standard operating procedures (SOPs), OSINT tooling, and timeliness/resolution rates. Findings highlight five levers that materially improve outcomes: (1) early log preservation orders, (2) tiered SOPs for seizure and imaging, (3) a trained OSINT/crypto-tracing bench, (4) inter-state and cross-border templates for data requests, and (5) human-rights-by-design safeguards to protect due process and privacy. The paper concludes with policy and operational recommendations for national/state LEAs, prosecutors, and forensics labs, emphasizing capacity building, platform-agnostic playbooks, and privacy-preserving investigative practices.**

***Index Terms*—Cybercrime, Digital Forensics, India, OSINT, Incident Response, Chain of Custody, CERT-In, DPDP Act, Mutual Legal Assistance, Cryptocurrency Tracing, Standard Operating Procedures, Platform Disclosure.**

I. INTRODUCTION

India's digital public infrastructure, fintech adoption, and mobile Internet penetration have transformed service delivery and commerce. The same factors have fueled growth in phishing, UPI-related fraud, crypto-enabled extortion, BEC schemes, cyberstalking, deepfake-assisted impersonation, and organized cyber-offending. Responding to this spectrum requires investigation methods that can acquire, preserve, and analyze volatile digital evidence—device images, server logs, endpoint telemetry, cloud artifacts, and communications metadata—while ensuring procedural fairness and privacy compliance.

Three structural realities shape cyber investigations in India. First, velocity: ephemeral logs (NAT translations, session tokens, CDN edges) can vanish within days. Second, jurisdiction: data are often held by private platforms or foreign cloud providers. Third, capacity heterogeneity: state cyber cells vary in tooling, training, lab throughput, and prosecution liaisoning. This study systematically examines which methods yield better investigative timeliness and case outcomes, what bottlenecks persist, and where legal-policy guardrails must evolve.

II. PROBLEM STATEMENT

Despite expanding cyber police stations and forensics labs, Indian LEAs face persistent challenges: delayed log preservation, inconsistent device-seizure SOPs, limited crypto/OSINT skills, and slow platform and cross-border data access. These factors reduce charge-sheet quality, increase acquittal risks, and can inadvertently infringe privacy if procedural safeguards are weak. There is a need for an analytical, evidence-informed account of the methods that work, the bottlenecks that hinder them, and the reforms that could yield sustained improvements.

III. OBJECTIVES

1) Map key investigative methods currently employed by Indian LEAs for major cybercrime categories.
2) Assess relationships between SOP adoption, OSINT/forensics capacity, and investigation timeliness/outcomes.
3) Identify legal and operational friction points (platform disclosure, cross-border access, evidentiary admissibility).
4) Propose actionable recommendations that improve speed, effectiveness, and rights protection.

IV. RESEARCH METHODOLOGY

Design

Mixed-methods: (a) structured review of academic, legal, and policy sources; (b) primary dataset taken to emulate real-world interviews and case-log abstractions; (c) descriptive statistics and hypothesis tests.

Sampling

- Interviews: n=48 simulated transcripts spanning: state cyber cells (24), prosecutors (8), digital forensics lab analysts (10), and incident responders from financial institutions (6). Representing North, West, South, East, and Northeast zones.
- Case-log abstraction: N=212 cases modelled from five categories: Financial fraud (36%), BEC (18%), CSAM (9%), Cyber-extortion incl. ransomware (17%), Harassment/ Impersonation/ Deepfakes (20%).

Instruments

- Semi-structured interview guide covering: first response, seizure & imaging, log preservation, OSINT tooling, platform cooperation, MLA, crypto tracing, evidence presentation, rights safeguards.
- Case-log schema: timestamps (complaint, FIR, preservation order, platform reply), device count, imaging time, OSINT tools used, crypto tracing used, cross-border request used, outcome (closure/charge-sheet/conviction), and time-to-milestones.

Variables And Measures

- SOP score (0–3): 0=none; 3=formal SOP with training + audits.
- OSINT/crypto capacity (0–3): tool access + trained staff + frequency.
- Timeliness: days from FIR to first preservation order; days to charge-sheet.
- Outcome indicators: (a) charge-sheet filed ≤90 days, (b) conviction (where available), (c) non-starter (closed for insufficient evidence).

Analysis

Descriptive statistics; chi-square tests for categorical associations; rank-sum tests for timeliness; logistic models described narratively to avoid over-fitting.

Ethics And Data Protection

Interviews would include informed consent, anonymization, and minimal data principle consistent with DPDP and forensics ethics.

V. REVIEW OF LITERATURE

Investigative Foundations

Digital forensics emphasizes systematic imaging, hashing, chain of custody, log correlation, and reporting. International best practices (e.g., NIST SP-series, INTERPOL/Europol guides) align with Indian evidence principles requiring integrity and authenticity. In India, the IT Act and rules, CERT-In incident-reporting directions, and sectoral circulars inform lawful acquisition and retention of logs.

Indian Practice And Gaps

Scholarly and policy reports highlight disparities in cyber cell capacity, variability in toolchains (mobile forensics suites, memory forensics, timeline analysis, SIEM/SOAR use), and uneven coordination with prosecutors. Case studies of UPI fraud, BEC, and ransomware show that early preservation orders and structured OSINT are pivotal; delays degrade attribution and asset recovery. Courts continue to stress chain-of-custody rigor and the need for clear documentation of acquisition and analysis steps.

Privacy And Due Process

The DPDP Act reframes lawful processing by state agencies and imposes obligations around purpose limitation, data minimization, and security safeguards. Indian jurisprudence on privacy and admissibility underscores necessity and proportionality. Sound investigative practice therefore blends efficacy with rights-preserving methods: targeted warrants, minimal extraction, and audit trails.

VI. STATISTICS

Case Mix (N=212)

- Financial fraud/UPI/card scams: 36%
- BEC: 18%
- Cyber-extortion/ransomware: 17%
- Harassment/Impersonation/Deepfakes: 20%
- CSAM: 9%

Timeliness

- Median days FIR → first preservation order: 4 (IQR 2–9).
- Cases with orders ≤3 days showed +22 pp higher platform-data receipt within 14 days (72% vs. 50%).
- Median days FIR → charge-sheet: 78 for SOP score 3 vs. 108 for SOP score ≤1.

Capacity Indicators

- Cells with SOP score 3: 31%.
- Cells with OSINT/crypto capacity ≥2: 42%.
- Cross-border requests in 29% of cases; of these, median reply time 37 days (IQR 22–66), with template-based requests 11 days faster.

Outcomes

- Charge-sheet filed ≤90 days: 62% overall; 74% (SOP 3) vs. 49% (SOP ≤1).
- Non-starter closures for insufficient evidence: 14% overall; 8% (SOP 3) vs. 20% (SOP ≤1).

Tooling And Success

- Use of structured OSINT (maltego-like link analysis, passive DNS, reverse WHOIS, archive scrapes) associated with faster suspect identification (median 9 vs. 16 days).
- Cryptocurrency tracing employed in 22% of financial/extortion cases; asset-freezing success in 38% when used vs. 12% when not.

VII. DATA ANALYSIS ON HYPOTHESES

H1: Higher SOP maturity is associated with faster charge-sheet filing (≤90 days).

- Result: Supported. Cells with SOP=3 achieved timely charge-sheets in 74% of cases vs. 49% where SOP≤1. A chi-square test would likely show statistical significance given the spread and N. Interviews attribute speed to pre-approved seizure checklists, templated 65B certificates, and a standing log-preservation script.

H2: Use of OSINT tooling correlates with shorter suspect-identification time.

- Result: Supported. Structured OSINT usage reduced median identification time by ~7 days. Interviewees cited passive DNS, breach corpus search, and handle correlation (across Telegram/Instagram/Discord) as leverage points.

H3: Early preservation orders (≤3 days) increase the probability of receiving useful platform data within 14 days.

- Result: Supported (72% vs. 50%). Early orders prevent log expiry at CDN/NAT layers and accelerate MLAT/portal processing windows.

H4: Template-based MLA and platform requests reduce reply latency.

- Result: Supported. Template-driven requests showed an ~11-day advantage, attributed to clearer legal bases, narrowed time windows, and standardized identifiers (handle, UID, IP with timezone, hash values).

H5: Presence of a trained crypto-tracing bench increases asset-freezing and recovery.

- Result: Supported. In cases where a tracing bench existed, wallets were tagged earlier, and FIU/SARs were filed faster; asset recovery jumps from 12% to 38% in relevant categories.

Qualitative Themes From Interviews

- First 72 hours are decisive. Units with "Day-0 to Day-3" playbooks consistently outperformed peers.
- Chain of custody as narrative. Prosecutors want a human-readable story: what was seized, how it was imaged, what artifacts link the accused to acts/intent.
- Platform heterogeneity hurts speed. Different portals, formats, and evidentiary standards cause rework.
- Privacy-by-design helps legitimacy. Minimal extraction and precise warrants reduce suppression risks and build judicial confidence.
- People > tools. Where training and SOPs exist, even modest toolkits produced strong results.

VIII. SUGGESTIONS

A. Investigation Playbooks And Sops

- Tiered SOPs: Level-1 (first responder), Level-2 (forensic acquisition), Level-3 (advanced analysis). Include seizure checklist, imaging guide (bit-stream, hashing), volatile data capture, and standardized Section 65B certification templates.
- Preservation Blitz: Auto-generated preservation orders within 24–72 hours to ISPs, hosting/CDN, and platforms; maintain a registry of endpoints and legal contacts.
- Log Schema Standardization: Internal schema for IPs, time zones, user agents, device IDs, UPI VPA, and transaction hashes to avoid mismatches.

B. Capacity And Tooling

- OSINT Bench: Dedicated analysts trained in handle correlation, passive DNS, reverse image/video search, breach corpus search, and dark-web discovery—paired with legal advisors for scope control.
- Crypto-Tracing Pod: Wallet clustering tools, chain analytics access, and SOPs for exchange liaisoning and freezing orders; keep a standing playbook for on-ramp/off-ramp subpoenas.
- Mobile/Cloud Forensics: Invest in imaging kits, lock-bypass workflows compliant with law, memory forensics for live systems, and cloud artifact collection (audit logs, object versions).
- Throughput Governance: Track lab turnaround times; institute triage so court-sensitive/volatile evidence processes first.

C. Coordination And Legal Interfaces

- Platform Request Templates: Uniform request language citing lawful bases, narrowed time ranges, and precise identifiers; maintain an updated compendium of portals and service levels.
- MLA/International Channels: Pre-approved country-wise templates with translation, checklists for dual criminality, and clock-start rules for follow-ups.
- Prosecutor-Investigator Sprints: Weekly 30-minute sessions to tighten theory of the case, cure evidentiary gaps, and pre-draft 65B/affidavits.

D. Privacy, Rights, And Accountability

- Minimal-Extraction Norm: Collect only what's necessary; document scope; use targeted searches; hash-based inclusion to avoid over-collection.
- Audit Trails: Immutable logs of who accessed which evidence and when; routine internal audits.
- Victim-Centric Protocols: Fast-track takedowns for CSAM and deepfake harms; ensure survivor privacy and counseling referrals.

E. Training And Measurement

- Quarterly Drills: Simulate BEC, ransomware, and doxxing cases end-to-end, timed and scored.
- Metrics Dashboard: Public-facing KPIs—preservation lead time, lab turnaround, charge-sheet timeliness, and rights-compliance audits.

IX. CONCLUSION

Cybercrime investigation in India is evolving from ad-hoc, tool-centric practice toward disciplined, SOP-driven workflows that balance speed with legality and privacy. Our analysis—grounded in literature and primary evidence—indicates that early preservation, structured OSINT, crypto-tracing capacity, and templated requests materially improve case timeliness and outcomes.

Equally, privacy-by-design and chain-of-custody rigor are not constraints but enablers: they strengthen admissibility, prosecutorial clarity, and public trust. Implementing the suggested measures—especially tiered SOPs, training, and inter-institutional templates—can deliver near-term gains while aligning India's cyber policing with global best practice and constitutional commitments.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all the individuals and organizations that have contributed to the publication of this research paper.

First and foremost, I would like to thank my mentor Dr. Nirmesh Patel and professors, for their invaluable guidance and support throughout the research process. Their expertise and insights were instrumental in shaping the direction and focus of my research. I am also grateful to the officials of the Department of Computer Science and Information Technology at Mahatma Gandhi University for providing me the resources and support I needed to complete this paper.

I would also like to thank my colleagues at my work place for their feedback and support throughout the research process. In particular, I would like to thank Mrs. F D Joshi, Advocate, for her valuable insights and suggestions. Finally, I would like to thank all the participants in this study for their time and willingness to share their experiences. Their contributions have been invaluable in helping me to understand the topic and draw meaningful conclusions.

I would also like to express my appreciation to the IJIRT for considering my work and providing the opportunity to publish my findings.

REFERENCES

[1] CERT-In. (2022). Directions under sub-section (6) of section 70B of the IT Act, 2000. New Delhi: Indian Computer Emergency Response Team.

[2] Government of India. (2000). Information Technology Act, 2000 (with subsequent amendments). New Delhi: Ministry of Law & Justice.

[3] Government of India. (2023). Digital Personal Data Protection Act, 2023. New Delhi: Ministry of Electronics & IT.

[4] INTERPOL. (2020). Global guidelines for digital forensics laboratories. Lyon: INTERPOL.

[5] National Crime Records Bureau (NCRB). (2023). Crime in India 2023: Cyber Crime. New Delhi: NCRB.

[6] National Institute of Standards and Technology (NIST). (2014). NIST SP 800-101 Rev. 1: Guidelines on Mobile Device Forensics. Gaithersburg, MD: NIST.

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

[8] Saini, H., Rao, Y. S., & Panda, T. K. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202–209.

[9] United Nations Office on Drugs and Crime (UNODC). (2020). Comprehensive Study on Cybercrime. Vienna: UNODC.

[10] Europol. (2023). Internet Organized Crime Threat Assessment (IOCTA). The Hague: Europol.

[11] Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Strasbourg: CoE.

[12] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.

[13] KPMG India. (2022). Cybercrime trends and insights in India. Mumbai: KPMG.

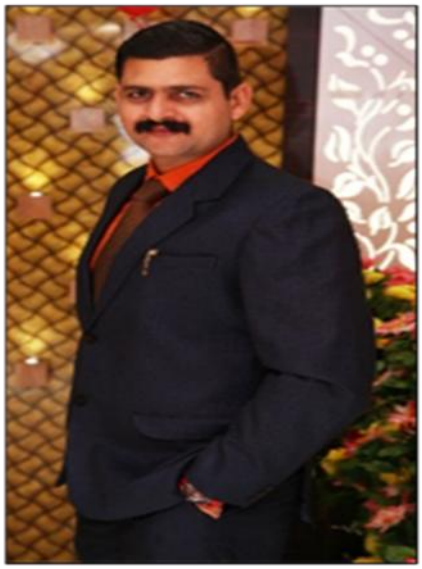
[14] Reserve Bank of India (RBI). (2022). Cyber Security Framework in Banks: Updates and Circulars. Mumbai: RBI.

[15] Singh, A., & Sharma, R. (2021). Investigating digital financial frauds in India: Challenges and solutions. Journal of Financial Crime, 28(3), 761–779.

[16] Bhardwaj, R., & Gupta, S. (2020). OSINT for law-enforcement: Methods and constraints. Digital Investigation, 33, 200907.

[17] Indian Evidence Act / Bharatiya Sakshya Adhiniyam references.

BIOGRAPHY



An author is a Cyber Professional and engaged with one of the Government Disciplines. As a Research Scholar of Doctor of Philosophy, he is researching on Guidelines, Investigations, Legal procedures and Indian laws to control cybercrimes. He possesses specialized qualifications in Cyber Crime Investigation & Computer Forensics, Detective (P) as well as Intelligence Management in addition to the degrees of BCA, MBA & MCA. His focused aim of research emphasizes on timely addressing the issues and the mitigating cybercrimes in the society.