NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

NAVIGATING DIGITAL ARREST UNDER INDIA'S CYBER-FORENSICS FRAMEWORK: COMPLEXITIES, LEGAL GAPS, AND PATHWAYS FORWARD

Shailesh Kumar Pandey, Ansh Parashar

Abstract: *This research explores the emerging threat of digital arrest scams in India and the evolving cyber-forensics framework used to combat them. It examines the operational mechanisms of such scams, where cybercriminals impersonate law enforcement officials to extort money from victims, and highlights the jurisdictional, technological, and evidentiary challenges faced by Indian law enforcement agencies. The study delves into the role of mule accounts in laundering illicit funds, the application of advanced forensic tools like Cellebrite UFED, FTK, and EnCase, and the integration of AI-driven models such as the Mule Hunter. It also evaluates the legal responsibilities of intermediaries under the IT Act and the complexities of electronic evidence admissibility. Through a comprehensive analysis of investigative practices, legal frameworks, and inter-agency coordination, the paper proposes strategic pathways to strengthen India's response to digital arrest fraud and enhance the integrity of cybercrime investigations.*

Keywords: *Digital Arrest, Cyber Forensics, Mule Accounts, Intermediary Liability, Electronic Evidence.*

1. INTRODUCTION: OVERVIEW OF DIGITAL ARREST AND CYBER FORENSICS IN INDIA

The present research outlines the utilisation of cyber forensics tools by various law enforcement agencies in India to deal with cases of digital arrest. It has been observed that multiple world-class tools are used, including Cellebrite UFED, Forensic Toolkit (FTK), EnCase, and the indigenously developed C-DAC CyberCheck Suite. These tools are not just globally accepted but are also very capable, as they facilitate the digital forensics mechanism through effective data extraction, in-depth analysis of the extracted evidence, and then outlining the key findings in the form of a report. Multiple law enforcement agencies have relied upon these tools to ensure that the Indian digital forensics framework can deal with emerging challenges in Indian cyberspace. The digital arrest fraud is a novel technique applied by cybercriminals to intimidate and extort money from innocent civilians by deterring them in the name of law enforcement authorities. Recently, India has experienced an increase in such offenses, and due to excessive intimidation and manipulation, a teacher in Madhya Pradesh tragically committed suicide after falling victim to the digital arrest scam.

As per the report of the World Cybercrime Index, India is ranked 10th among nations facing alarming cyberattacks and cybercrime-related cases; India needs to develop a robust strategy and counter-crime mechanism, including strengthening the framework of digital forensics and cyber forensics management to be done by the law enforcement agencies. A nationwide policy on investigating methods and technologies is necessary to enhance the investigation, examination, and presentation of evidence in court, ensuring its integrity and admissibility beyond a reasonable doubt.

According to a report published by The Times of India in 2023, innocent Indians targeted by cybercriminals lost ₹17,000 crore in wealth. Around 4,50,000 bank accounts were identified as being involved in the rotation and circulation of cybercrime proceeds, transferring funds from victims' bank accounts to overseas accounts. In 2024 alone, approximately 29,000 cyber fraud cases were reported in India. Alarmingly, less than 10% of the total fraud amount was recovered by law enforcement agencies.

These statistics clearly highlight a significant gap between legislative requirements, the need for advanced technical equipment, and the on-ground response of law enforcement authorities in investigating and tracking money involved in frauds like digital arrest. Due to the absence of a standard operating procedure for dealing with digital arrest-related offenses and transaction traces, it is becoming increasingly difficult for the prosecution to secure convictions and ensure justice in court.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

A large chunk of criminals committing fraud, like digital arrests, are using fake SIM cards or mule bank accounts, and due to the overseas operations by the cybercriminals, even the IP addresses are not traceable. Hence, the perpetrators of the crime are mostly out of the reach of law enforcement agencies, and the only way to bring them to justice is through a robust digital forensics mechanism that could establish their identity, involvement, and participation in the fraud of digital arrest by effectively tracing their bank accounts, computer networks, and cellular identities. The government is constantly attempting to block fake SIM cards and cell phones. So far, cybercrime proceeds amounting to 3431 crore rupees have been duly protected from cybercriminals in around 994,000 cases filed. However, the data regarding how many cybercriminals have been arrested, prosecuted, and successfully convicted is not available on public platforms.

2. UNMASKING THE SHADOWS: ANALYSING MECHANISMS EMPLOYED BY THE INDIAN POLICE IN COMBATING DIGITAL ARRESTS

The phenomenon of digital arrest scams has emerged as one of the most pernicious and rapidly proliferating forms of cyber extortion in the digital landscape of India. An appropriate nomenclature for digital arrests can be sophisticated frauds, wherein criminals meticulously impersonate law enforcement officials to deceive and defraud some unsuspecting individuals, presenting several formidable challenges to public security as well as financial wellbeing. Recent data from the government reveals an alarming trajectory upon this issue – digital arrest scams and related cybercrimes have nearly been tripled between 2022 and 2024, with defrauded amounts skyrocketing by an unprecedented twenty-one times during this period. This section examines the multifaceted mechanisms deployed by Indian police departments so far in order to investigate these intricate crimes, apprehend perpetrators, and mitigate the impact of this ever-evolving threat. The police response, characterized by a synthesis of traditional investigative tenets and advanced cyber forensic techniques, underscores a concerted effort to dismantle these criminal enterprises, albeit against significant systemic and operational challenges.

A. The Genesis of Action: Victim Reporting and Mobilization of Specialized Units

The investigative trajectory in digital arrest cases almost invariably commences when a victim, having endured significant psychological distress and often substantial financial loss, lodges a formal complaint. These reports are typically filed at local police stations, or now increasingly specialized cyber police stations, or through national reporting channels such as the cybercrime helpline number 1930 and the National Cyber Crime Reporting Portal (www.cybercrime.gov.in). The critical nature of timely reporting is being constantly emphasized by law enforcement agencies, as evidenced by Kolkata Police's advice to contact the financial helpline 1930 within 15-20 minutes of a fraudulent transaction to attempt at potentially freezing the transfer.

B. Specialized Investigative Units

The gravity and technical complexity of digital arrest scams have now rather necessitated the formation of specialized units within the police departments. Many states have even established dedicated cybercrime cells or Special Task Forces (STFs) to spearhead these investigations. For instance, in a Dehradun case where a retired teacher was duped of ₹2.27 crores, a special team was constituted which had leveraged data from banks, telecom providers, and technology companies to trace the accused. Similarly, the Criminal Investigation Department (CID) has been noted to register and investigate such cases, as seen in Ranchi where a retired CCL employee had lost ₹2 crores to fraudsters who kept him on a virtual video call. The establishment of multiple cyber police stations, as in Faridabad, further signifies the institutional response to the rising tide of such crimes.

3. THE INVESTIGATIVE ARSENAL: DECRYPTING DIGITAL DECEPTION AND FINANCIAL MAZES

The very core of the police's counter-offensive policy lies in the meticulous deconstruction of the digital and financial labyrinth constructed by the fraudsters. This involves several key investigative prongs:

A. Financial Trail Analysis

This is arguably one of the most crucial and challenging aspects of the investigation. Scammers employ a complex network of mule bank accounts-often opened using stolen or fraudulently obtained KYC documents-to layer transactions and obscure the ultimate destination of the extorted funds. Police tend to engage in extensive correspondence with the

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

banking institutions to obtain detailed transaction histories, account holder information (which often leads to further investigations into identity theft), and CCTV footage from ATMs where illicit cash withdrawals might have occurred.

For example, the investigation into the ₹2.27 crore Dehradun scam involved scrutinizing bank data to identify the perpetrator, Neeraj Bhatt, and also revealed that the same fraudulent bank account was implicated in complaints from other states. Victims are often coerced into making large transfers via RTGS and NEFT to multiple accounts and, in some instances, are even forced to liquidate assets like gold and property or take out substantial loans to meet the fraudsters' demands. While police make concerted efforts to freeze funds in fraudulent accounts, the success rate of full recovery can be limited, as highlighted by one victim who recovered only a fraction of their loss, though any recovery is significant.

B. Technical Data Collection and Digital Forensics

Cyber police units depend heavily on the acquisition and forensic analysis of electronic data. This includes obtaining Call Data Records (CDRs) and subscriber details from telecom service providers to map communication networks. Collaboration with technology giants like Meta and Google is often sought to garner information on online accounts (such as Skype and WhatsApp, which are frequently used by scammers), IP addresses, and other digital footprints left by the perpetrators. A significant breakthrough by Kolkata Police involved seizing a large cache of evidence including 104 passbooks/chequebooks, 61 mobile phones, 33 debit cards, and 140 SIM cards, which underscores the scale of these operations. The forensic examination of seized electronic gadgets, such as mobile phones and laptops from arrested suspects, is paramount for unearthing direct evidence, communication logs, and links to the broader criminal conspiracy.

C. Uncovering Organized Criminal Networks

Investigations are increasingly revealing that digital arrest scams are not merely opportunistic acts by isolated individuals but are often orchestrated by sophisticated, organized criminal syndicates. The Kolkata Police's crackdown that led to the arrest of 11 individuals, including a Bengaluru-based software engineer identified as the mastermind, Chirag Kapoor, is a case in point. This operation exposed a syndicate involved in creating and supplying fraudulent bank accounts to scammers across India.

This points to a disturbing ecosystem supporting these frauds, which also includes the illicit procurement and sale of citizens' personal data, including Aadhaar and PAN details, used to open these mule accounts and lend credibility to the impersonations. The scale of these operations is reflected in government data presented to Parliament, which revealed that in 2024 alone, 123,672 digital arrest cases were reported with a staggering defrauded amount of ₹1,935.51 crore.

Despite the digital nature of the crime, traditional policing methods involving human intelligence and coordinated field operations remain indispensable. Large-scale crackdowns, such as the one by Faridabad police resulting in 27 arrests across multiple states within a week, and the Kolkata Police's multi-state operation to nab the mastermind, demonstrate the extensive reach and operational capabilities of law enforcement when dismantling these networks. These operations often involve complex surveillance, informant networks, and swift, synchronized raids on identified hideouts.

4. THE IMPERATIVE OF COORDINATION: A UNIFIED FRONT AGAINST A BORDERLESS CRIME

The pervasive and often inter-state, and at times international, nature of digital arrest scams demands an exceptionally high degree of coordination among various law enforcement agencies and other relevant stakeholders. These scams often involve sophisticated tactics that span multiple jurisdictions, making it imperative for local, state, and federal authorities to work collaboratively. Effective communication and information sharing are critical in tracking down perpetrators who exploit technological advancements to deceive victims. Additionally, private entities, consumer protection organizations, and international law enforcement partners must also join forces. This collective effort aims to enhance prevention strategies, improve response times, and ultimately safeguard the public from these malicious schemes.

A. Inter-State Police Collaboration

The very structure of these scams-with perpetrators, victims, money trails, and operational bases frequently scattered across different states-makes seamless cooperation between state police forces paramount. The arrest of Neeraj Bhatt in Jaipur by Uttarakhand Police for a crime committed in Dehradun, with links to cases in Maharashtra and Arunachal

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Pradesh, exemplifies this need. Similarly, the Kolkata Police investigation involved apprehending the mastermind from Bengaluru and an associate from Delhi. Faridabad police also reported arresting individuals involved in digital fraud from diverse states including Delhi, Rajasthan, Madhya Pradesh, Uttar Pradesh, and Gujarat.

B. Role of Central Agencies and National Helplines

The Indian Cybercrime Coordination Centre (I4C), under the Ministry of Home Affairs, plays a pivotal role in bolstering the fight against cybercrime by providing a national framework, intelligence sharing mechanisms, and analytical support to state police forces. The national helpline 1930 serves as a critical first-response mechanism, facilitating rapid reporting and, crucially, enabling swift action to trace and potentially freeze illicitly transferred funds.

Engagement with Financial Institutions and Regulators

Effective tackling of these financial crimes requires close collaboration with banks and financial regulators. This extends beyond merely requesting transaction data to actively working with banks to freeze accounts and prevent further financial haemorrhage. Judicial interventions, such as the Rajasthan High Court directing the Reserve Bank of India to implement measures to halt payments to fraudsters, also signify a broader systemic approach to supporting law enforcement efforts.

Despite these concerted efforts and notable successes, Indian police face a battery of significant challenges in their campaign against digital arrest scams. The sophisticated modus operandi of fraudsters, who expertly employ psychological manipulation, impersonate officials with alarming authenticity using fake IDs and documents, and leverage technology like spoofed calls and encrypted messaging, makes detection and evidence gathering arduous. Victims are often kept in prolonged states of fear and isolation, sometimes confined to hotel rooms or engaged in continuous video calls for days, making them highly susceptible to coercion.

The cross-border dimension, with reports of scam operations being run from countries like Dubai, Pakistan, and China, introduces complex jurisdictional hurdles that impede investigation and prosecution. Furthermore, delays in victim reporting, often due to shame, fear of reprisal, or confusion, can significantly hamper the timely collection of evidence and the chances of financial recovery. Even extensive public awareness campaigns, including those mentioned by the Prime Minister, face challenges in universally inoculating the populace against these evolving tactics, as lamented by a senior police officer. The low overall rate of fund recovery also remains a major point of distress for victims.

The alarming escalation of this criminal phenomenon is evident in the parliamentary disclosure that within just the first two months of 2025, 17,718 cases with a defrauded amount of ₹210.21 crore have already been reported. This represents an intensification of the trend observed in preceding years, where the number of cases increased from 39,925 in 2022 to 123,672 in 2024, and the financial impact surged from ₹91.14 crore to ₹1,935.51 crore.

5. LIABILITY OF INTERMEDIARIES IN COOPERATING WITH LAW ENFORCEMENT AUTHORITIES

Law enforcement authorities require assistance from intermediaries in case of digital arrest and its forensics investigation. A case of digital arrest is where traditional form of investigation meets its end. However, it has been a concurrent issue whether the social intermediaries are liable in the process of digital arrest, specially as they are the platform on which it occurs, and to what extent it is supposed to cooperate with the legal authorities. To address the liability of intermediaries in cooperating with law enforcement authorities during digital arrests, it is essential to analyse the legal framework governing intermediary responsibilities, the extent of their obligation to assist, and the potential liabilities arising from non-compliance or over-compliance. Intermediaries, by virtue of their role as platforms facilitating communication and data exchange, occupy a unique position where their cooperation can have a significant impact on investigations, yet they also face challenges related to privacy, user rights, and legal limits. A comprehensive examination involves understanding statutory provisions such Sections 79 and 85 of the IT Act, 2000, which provide safe harbour protections, and recent amendments or guidelines that specify the scope of cooperation. Furthermore, cases like Shreya Singhal v. Union of India and the Supreme Court's directives on intermediary liability offer insights into the boundaries of their responsibilities.

The debate also extends to the extent of proactive cooperation whether intermediaries are mandated to actively monitor and report

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

content or merely respond to lawful requests and the implications of such obligations on user privacy and freedom of expression. Challenges such as the risk of overreach, the potential for misuse of legal powers, and the technical limitations of intermediaries in tracking encrypted communications complicate this landscape. Balancing the need for effective law enforcement with safeguarding fundamental rights requires a nuanced legal approach, which must be reflected in the evolving jurisprudence and regulatory policies. Ultimately, the liability of intermediaries' hinges on a combination of statutory mandates, judicial interpretations, and the technical feasibility of compliance, making it a complex yet critical aspect of digital forensics and law enforcement in the digital age.

A. Legal Framework Governing Intermediary Liability in India

The primary legal framework governing intermediary liability in India is Section 79 of the IT Act, 2000, which provides "safe harbor" protections to intermediaries. These protections, however, are contingent upon intermediaries following certain due diligence requirements and cooperating with law enforcement agencies when required. The implementation of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereafter "IT Rules 2021") has significantly reshaped the landscape of intermediary liability in India, creating more stringent obligations for digital platforms to assist law enforcement authorities.

Under the IT Rules 2021, "significant social media intermediaries" (those with more than 5 million registered users) face enhanced compliance requirements, including appointing India-based compliance officers, implementing automated content filtering, and maintaining user identification records. These requirements reflect India's shift toward a co-regulatory model that relies on both statutory frameworks and self-regulation by platforms.

B. Traceability Mandate and the Encryption Dilemma

Perhaps the most contentious aspect of the IT Rules 2021 is Rule 4(2), which mandates that messaging platforms enable "the identification of the first originator of the information" upon government or court order. This traceability requirement has sparked significant legal challenges, most notably from WhatsApp, which filed a petition before the Delhi High Court arguing that this mandate would fundamentally undermine end-to-end encryption and violate users' privacy rights.

WhatsApp's petition contended that Rule 4(2) fails the three-part test established in the landmark K. S. Puttaswamy judgment: legality, necessity, and proportionality. The platform argues that breaking end-to-end encryption would not only compromise user privacy but could also chill free speech, potentially endangering journalists, political activists, and attorney-client communications.

The government had countered that no fundamental right is absolute, asserting that the traceability requirement is narrowly tailored to serious offenses related to sovereignty, security, public order, or sexual abuse material. In its press response to the challenge laid by WhatsApp, the government emphasized that it values the Right to Privacy and does not intend to infringe upon it when WhatsApp is asked to reveal the source of a specific message.

C. Admissibility of Electronic Evidence from Intermediaries

The cooperation between intermediaries and law enforcement is further complicated by evidentiary requirements under the Indian law. The Delhi High Court recently held in Dell International India Private Limited v. Adeel Feroze and Ors. that WhatsApp conversations cannot be read as evidence without there being a proper certificate as mandated under the Indian Evidence Act. This ruling underscore the procedural hurdles in translating digital communications into admissible courtroom evidence.

Section 65B of the Indian Evidence Act (now Section 63 of the BSA, 2023) establishes specific certificate requirements for electronic evidence admissibility. These requirements create a framework for authenticating electronic records but have also led to uncertainty and irregularity in judicial pronouncements. Landmark rulings such as Shafhi Muhammad (2018) and Arjun Khotkar (2020) have attempted to clarify these requirements, but challenges persist in the practical implementation of these standards.

The complexities of the Section 65B certificate create a paradox, where a paper document (the certificate) ironically serves as the gatekeeper for digital evidence. For intermediaries, this creates additional compliance burdens when responding to law enforcement requests for user data that may eventually be presented as evidence in court.

D. Balancing Security Imperatives with Privacy Protections

At the heart of intermediary liability debates lies the fundamental tension between law enforcement's legitimate need for information

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

and users' privacy rights. The Supreme Court's recognition of privacy as a fundamental right in the K S Puttaswamy judgment established a constitutional standard against which all surveillance and data collection practices must be measured.

The proportionality test established in Puttaswamy requires that privacy intrusions must: (1) be sanctioned by law; (2) serve a legitimate state aim; and (3) be proportionate to the objective being pursued. When applied to intermediary obligations like the traceability requirement, this test demands careful scrutiny of whether alternative, less intrusive means could achieve the same law enforcement objectives.

It is often argued that mandates like Rule 4(2) fail this proportionality test by imposing systemic weaknesses in security architectures rather than pursuing targeted solutions. The 2021 IT Rules have been characterized as elements potentially weaponizing private sector content moderation powers for government control without traditional constitutional safeguards.

The Indian government has pointed to international precedents to justify its approach, noting that "the governments of the United Kingdom, United States, Australia, New Zealand and Canada issued a communique – that tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can gain access to data". The government further asserts that the demands posed by India are significantly negligible compared to what has been posed by other nations.

However, privacy advocates and intermediaries contend that India's approach differs significantly from these countries in both scope and implementation. While other jurisdictions may request specific data points like IP addresses or customer information, the traceability mandate of India requires a fundamental redesign of messaging services' technical architecture.

As digital technologies continue to evolve, striking the appropriate balance between intermediary cooperation with law enforcement and protecting fundamental rights remains an ongoing challenge that requires thoughtful legal frameworks, technical innovation, and continuing dialogue among all stakeholders.

6. ROLE OF MULE ACCOUNTS IN LAUNDERING DIGITAL ARREST PROCEEDS

In India, as a step for initiating a big crackdown on cyber fraud by the Indian Cybercrime Coordination Centre established under the Ministry of Home Affairs Government of India, the major achievement in this segment is that, to date, 600,000 data points have been detected and over 1.9 million mule accounts have been identified by the agencies that carried out transactions worth 2038 crore that were prevented after the introduction of the artificial intelligence-based system for the detection of mule accounts. A mule account is a bank account used by criminals to move stolen money. To effectively investigate and track down the account holders who act as facilitators of cybercrime by providing mule accounts, the Jammu and Kashmir police utilised modern technology to seek their bank accounts. They used to fluctuate, manipulate, and transfer the cybercrime proceeds from one account to another to ensure that the proceeds of cybercrime stayed untraceable, but this mode of money laundering is usually tracked down by law enforcement agencies through digital forensic methodology of tracking down the financial trails. The law enforcement agency stated that during the course of the investigation, it was observed that the amount is then transferred to an overseas bank account and also converted into cryptocurrency for easy mobility and backing by the blockchain network, which is secure and highly untraceable.

To mitigate Digital Arrest crimes, so far 450,000 'mule' accounts frozen, mainly at public sector banks. In digital arrest cases, police investigations target the money mule when such events are reported; since their accounts are involved, the real offenders stay invisible. A mule account, which is a bank account, is used by cyber criminals for laundering proceeds of digital arrest fraud. Ordinarily, a mule account is either acquired in exchange for a commission or fraudulently utilised by individuals who are often low-income or have little technical knowledge. The related phrase "money mule" refers to the bona fide innocent victims that criminals use to launder stolen or illicit money through their bank accounts.

A report by BioCatch highlights a surge in mule accounts and third-party account takeover fraud, which now accounts for 55% of all banking fraud in India. Mule accounts—used to

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

launder stolen money—are often accessed from abroad, with VPNs masking locations. Devices involved in mule activity accessed an average of 35 accounts each. Bhubaneswar saw the highest mule activity, followed by cities like Lucknow, Navi Mumbai, and Mumbai. Alarmingly, 90% of mule accounts at one bank went undetected. The RBI has recommended moving away from OTP-based authentication, which experts say is ineffective against modern fraud. Stronger fraud detection technologies are urgently needed.

7. EMERGING TECHNOLOGIES IN CYBERCRIME DETECTION

The role of generative AI in tackling new accounts and cyber fraud is being actively discussed. It has been suggested that, with the help of quantum computing capabilities, large-scale data can be analysed in real time. This provides ample scope to quickly track down victims' defrauded money by identifying suspicious transaction patterns and flagging activities that lead to the transfer of funds overseas, particularly in cases of digital arrest fraud.

A. AI-driven Initiatives: The Mule Hunter Model

The Indian regulatory authorities, with the help of the RBI, have started using artificial intelligence tools to identify and close mule accounts associated with cyber fraud. This action tackles the increasing difficulty of monitoring illegal money in digital transactions, which are more difficult to track than physical assets. AI will enable quicker intervention and recovery of stolen funds by helping to identify suspicious patterns in real time. As per India's cybercrime coordination centre in India in total two million view accounts exist in various banks, hence, effective detection of new account by verifying the mobile number given to banking agency and sim verification documents for obtaining that mobile number shall be matched with mobile number utilised for banking purpose to ensure that there is a complete water tight authentication system that could detect new accounts and ultimately control growing financial frauds.

The Mule Hunter is an artificial intelligence-based model developed to meet the needs of Indian law enforcement agencies and banking regulators. Its primary goal is to ensure that most new mule accounts can be effectively tracked and neutralized through advanced detection mechanisms. Even though using AI and machine learning is a new and creative approach, it's still unclear how to find out who is behind these accounts and how to keep digital evidence of their actions for use in court.

Simply closing these accounts may not be sufficient, as perpetrators can continue creating new mule accounts, leaving the core problem unresolved. So, it's vital to not only find and shut down such accounts but also to punish the offenders. This requires a robust digital forensics framework integrated into the system for tracking mule accounts so that both instances of cybercrime and the modus operandi can be dismantled permanently.

8. GLOBAL EVOLUTION OF CYBER FORENSICS AND ITS INFLUENCE ON INDIA

With the advancement of information technology and communication networks, the legislation slowly started evolving. In the pre-forensic or ad hoc phase, computer forensics started developing worldwide, and the evidence was examined directly by law enforcement authorities, like they used to examine ordinary evidence. The rationale behind using the word ad hoc simply means that due to rapid change in technology and communication regimes, the forensics standard of practices and rules were outdated. The fundamental notions or rules of thumb of ordinary forensic science were not being followed by professionals in pre-forensic times, and eventually, the court dismissed most of the cases based on sole reliance on such digital forensic evidence due to a lack of clarity and chain of custody requirements not being fulfilled. This absence of a standard protocol led to hardships and the dismissal of most of the criminal prosecutions. Therefore, in the late 1980s, the computer forensics regime experienced significant legislative interventions and policy changes. In this phase, computer technology and software were developed to ensure that the evidence collected through digital forensics methods would be preserved and its integrity would be proved in the court of law for securing the ends of justice.

Social media platforms contributed to the growth and expansion of various industries into billion-dollar enterprises, which eventually led to their misuse by cybercriminals who exploited these platforms for illegal activities. Leading corporations such as Facebook, which owns WhatsApp and Instagram, started utilizing end-to-end encryption to ensure data privacy and preclude external data breaches. The end-to-end encryption in social media networks and cloud-based operational software is making it extremely difficult for law enforcement

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

authorities to present digital evidence in court for effective prosecution. The standard procedure for investigating and managing digital evidence begins with identifying the digital evidence and ensuring its integrity is maintained throughout the process. This involves the acquisition of evidence using popular software, hardware, and tools while ensuring that evidence does not lose its validity. The evidence collected is replicated, with the original kept safe, and examination is done on replicated records. The third stage of digital forensics entails a critical investigation and examination of the digital data as per the case's requirements. Leading law enforcement agencies worldwide utilize numerous open-source and paid software for this purpose. The final stage involves preparing the forensic expert's report or the report from the forensic laboratory for presentation before the court.

One major challenge in digital evidence management and examination is that the evolving nature of technology is rendering forensic examination technologies redundant. There is a pressing need to rapidly modify and modernize digital forensics investigation tools and techniques. Effective utilization of digital forensics has proven its worth in multiple countries, including the USA, where effective frameworks have led to successful prosecutions. The rapid advancement of technology and end-to-end encryption-based software facilitates crime. Due to self-erasure and encryption, gathering useful digital evidence for prosecuting criminals is challenging.

In digital forensics, two main steps are data preservation and imaging and processing data. Traditional tools like write blockers were used to extract data, but complex end-to-end encryption complicates reliable evidence collection. Verification often relies on hash algorithms to ensure tampering hasn't occurred. Various digital forensic tools are available globally, with EnCase and FTK widely used in the USA. In India, EnCase was used in the Parliament terror attack case. The most significant challenge remains end-to-end encryption, necessitating that law enforcement agencies break this encryption to effectively investigate crimes.

9. CHALLENGES AND STRATEGIES IN INVESTIGATING DIGITAL ARREST SCAMS

One of the most prominent challenges in investigating digital arrest-related crimes is that, even if criminals are apprehended, the limited availability of evidence traced through investigations based on digital activities or financial transactions is often insufficient for prosecution. Therefore, vigilance and awareness must be promoted among citizens so that, if they encounter any attempt at digital arrest, they can collect evidence themselves. This includes actions such as screen recording the incident and making voice recordings, which can eventually be used against the perpetrators.

Digital forensics is an umbrella term that encompasses various subtypes of forensic investigation techniques, including cyber forensics and network forensics, that have emerged in Western countries but are now very relevant to Indian cyberspace jurisdiction. Law enforcement agencies worldwide utilise a variety of cyber forensic software, such as EnCase, Forensic Toolkit (FTK), and Oxygen Forensic Suite. Such platforms are not only helping in extracting important data from software and hardware but are also advantageous in extracting cyber forensic data from complex sets of networks. The Kerala POLICE is utilizing cyber forensics tools for extracting important evidence, and then they are utilising the hash algorithm to preserve sanctity, integrity, and chain of custody. With the advancement of technology, law enforcement agencies need to get equipped with the most advanced and capable cybercrime investigation tools to ensure that the investigation of critical cybercrimes, including cybercrimes of digital arrest, shall be dealt with accordingly in an effective manner.

Various methodologies are adopted for tracking down the cybercriminals behind digital error scams in India; in one such instance, the Karnataka police tracked down a syndicate of cybercriminals based on their SIM procurement. The investigation revealed that multiple SIM procurements in a dubious manner enabled cybercriminals to utilize those SIMs from the foreign territory of Dubai to defraud Indians, and the proceeds of cybercrime, namely digital arrest, were transferred in the form of gold bullion, and the money, instead of getting recovered, was channelized through Hawala networks, ultimately reaching the hands of the perpetrator.

Certain cyber forensics toolkits utilised in India are as follows

Cellebrite UFED - Among many state police agencies, including those in Maharashtra, Andhra Pradesh, Uttar Pradesh, Kerala, Delhi, Punjab, etc., Cellebrite UFED is a particularly popular mobile forensic tool. It is mostly used to extract mobile forensic data and cellular data

from cloud-based systems. This tool is equally useful for computer networks, including cloud platforms, and mobile phones. Its most notable quality is that it offers both logical and physical extraction. Thereafter, it assists in decrypting vital data and circumventing safety standards and protocols, including passwords.

A. Development and Use of Indigenous Cyber Forensic Tools by C-DAC

India has also made significant strides in developing its own cyber forensic capabilities through the Centre for Development of Advanced Computing (C-DAC).

C-DAC has created a set of homegrown cyber forensic tools, including the CyberCheck Suite, which consists of EmailTracer for email analysis, CyberCheck for data recovery and analysis, and TrueBack for disk imaging. C-DAC has also created other tools such as Win-LiFT for live forensics, SIMXtractor for SIM card analysis, MobileCheck for mobile forensics, Network Session Analyser, Advik CDR Analyser for call detail record analysis, TrueTraveller as a portable forensic kit, TrueImager for high-speed disk imaging, and CyberInvestigator for log analysis.

Various Law Enforcement Agencies around across the nation, including the CBI and several state police departments, have used these tools. C-DAC is also quite important in training law enforcement officers on cyber forensics, therefore improving their ability to use these tools properly. C-DAC's creation and use of a set of homegrown tools shows a deliberate attempt at self-reliance in this vital field, maybe providing customized solutions that fit the particular requirements and environment of cybercrime in India.

B. Application of Forensic Toolkit (FTK) in Indian Investigations

Forensic Toolkit (FTK), Developed by Exterro, Forensic Toolkit (FTK) is a highly regarded disk forensic tool used by Indian police forces including the Hyderabad and Uttar Pradesh Police. Hyderabad Police uses FTK for disk imaging and hardware forensics, including the recovery of deleted data. Comprising various products—FTK Forensic Toolkit, FTK Lab, and FTK Imager—the Exterro FTK suite is meant to simplify the process of probing digital crime. For repeatable, defensible full-disk image collection, processing, and review, FTK Forensic Toolkit is preferred. With distributed processing and multi-user review, FTK Lab enables large-scale investigations.

Capabilities of EnCase in Digital Evidence Analysis

It is Developed by OpenText, EnCase is another internationally known forensic tool used by Indian law enforcement. It provides thorough capabilities for the acquisition, analysis, and reporting of digital evidence from a wide range of devices, including computers, mobile devices, network devices, and cloud services. It supports a broad range of operating and file systems and incorporates AI and ML for advanced image analysis, including the identification of specific content like nudity or weapons.

It is important that for the cyber forensics framework's reliability and admissibility, certain notions of preserving evidence integrity, maintaining chain of custody, lawful evidence collection and transfer, etc., are important.

TABLE 1: MERITS AND SHORTCOMINGS OF KEY CYBER FORENSIC PLATFORMS IN INDIA

Platform	Merits	Shortcomings
Cellebrite UFED	Broad device compatibility, multiple extraction methods, bypasses lock, recovers passwords, decryption, application data analysis, cloud data extraction, user-friendly	Privacy concerns, software vulnerabilities, limitations against advanced security, potential data integrity issues
Forensic Toolkit (FTK)	Industry preference, repeatable imaging, fast processing, handles large datasets, comprehensive analysis, supports various file systems, integrated case management	Performance issues with large datasets, lack of recursive export, file naming issues, potentially weaker file carving, requires specialized training
EnCase	Industry standard, court-proven, comprehensive artifact support, extensive device support, AI/ML for image analysis, OCR, strong email analysis, good keyword searching	Difficult user interface, slow analysis with large files, complexity, potential version incompatibility, proprietary format, high cost
C-DAC CyberCheck	Indigenous tool, used by Indian LEAs, supports various image formats, data recovery, powerful search, browser analysis, anti-forensic detection, timeline analysis, reporting, Unicode support	Explicit shortcomings not detailed in snippets; general limitations of forensic tools (deleted data, encryption) may apply; requires further comparative analysis with international tools

10. CONCLUSION

Indian law enforcement agencies have made notable progress in using cyber forensic tools.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Using tools like the native C-DAC CyberCheck Suite, EnCase, Forensic Toolkit, and Cellebrite UFED shows a dedication to using technology in probes. The study, therefore, shows that even with these developments, notable obstacles still exist in achieving the best efficacy. The low cybercrime conviction rates highlight the need of a more holistic approach that goes beyond mere technology adoption. Unlike the USA, where the Constitutional Amendment IV and V curtails the power of law enforcement agencies to extract the data from the personal device of individuals, in India, the choice is available in hands of law enforcement authorities to extract the data relating to omission of the crime and the Indian cybercrime prevention and digital forensics framework in past few decades has been shifted towards much more autonomy to the law enforcement agencies while investigating cybercrimes and other violations involving digital forensics framework, however, there is a need to introduce sufficient changes in Indian legal system to adequately address the cybercrime of digital arrest, as it is not just the one crime but a combined whole of multiple other crimes as mentioned under the Bhartiya Nyaya Sahitha, 2023. Furthermore, the rigid and complex conditions prescribed by the judicial pronouncement needs to be revisited to allow greater flexibility to the investigators in collecting preserving examining and then presenting the digital forensic evidences for emerging and modern cybercrime. Multiple law enforcement agencies and state police departments must issue a standard operating procedure to create a unified and comprehensive approach for investigating the cybercrime connected to digital arrest so that with consistency the code can also create specific framework and set of digital evidence preservation protocols to guarantee admissibility of the digital evidence. Around the world, a multi-faceted approach is essential for efficient cybercrime investigation.

Acquiring the newest cyber forensic tools and technologies including those using AI-powered analytics and big data processing capabilities requires more investment. With an eye toward guaranteeing these tools are comparable in functionality and performance to international standards, ongoing support for the development and adoption of indigenous cyber forensic tools by organizations like C-DAC is absolutely vital. Building well-equipped specialized cyber forensic laboratories at both state and national levels, with the required hardware and software resources, will give investigators the infrastructure they need for efficient digital investigations.