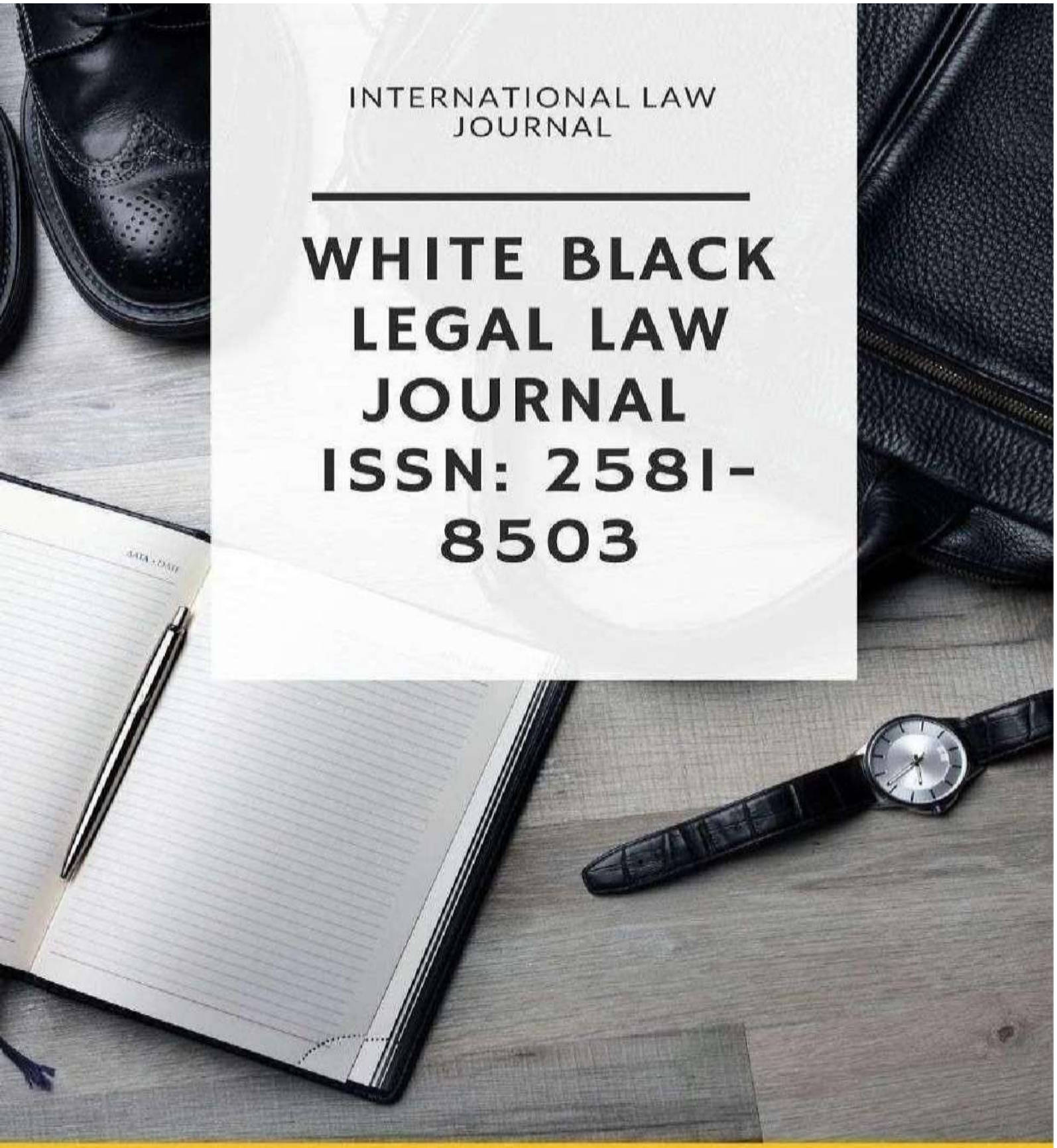

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

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

DISCLAIMER

ABOUT WHITE BLACK LEGAL

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

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

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

AIM & SCOPE

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

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

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

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

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

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

BRIDGING THE GAP: CHALLENGES AND FUTURE REFORMS IN DIGITAL FORENSIC INVESTIGATIONS

AUTHORED BY - DR KANA MUKHERJEE
Professor, Dept.of Legal Science
Techno India University, West Bengal

CO-AUTHOR - DR.DEBIKA MUKHERJEE
Assistant Professor, Dept. of Legal Science
Techno India University, West Bengal

Abstract

As digital crimes continue to rise globally, there is an urgent need to safeguard the public from such offenses and apply technological tools to effectively combat these threats. This study examines the forensic practices pertaining to digital investigations in the Indian context. Forensic science holds vital role of criminal investigations system on the basis of scientific evidence that helps law makers and the judges. This study examine the procedure and the stages of investigation which are conducted by forensic expert.The researcher highlights here some legislative enforcement and judicial interpretation how forensic science plays crucial position to solve digital investigation. However some issues are raising in question .Therefore it is suggested to set up robust legal structure, technological development, confidentiality of digital evidence, proper training of forensic officials speed up criminal trail and enhance to combat against cybercrime.

Keywords: 1. Gap 2.Challenges 3. Reforms 4. Digital 5 .Forensic Investigations

Overview

The term "science", is obtained from a Latin word that is closely refers to the scientific method of acquiring knowledge. The word forensics or "forensic science", in general term which means the application of scientific principle and methods in legal matters depending mostly on physical evidence. But nowadays a specialized branch of this forensic science focuses on digital

forensic that primarily deals with recovering and analyzing evidence from electronic systems or digital devices.

Forensic law includes application of science to law by using scientific knowledge to solve legal issues. It also includes evidence analysis like DNA, blood spatter etc to identify criminals and helping in criminal investigation.

Generally Scientists collect, preserve, and analyse data from digital devices. Digital forensics or Computer forensics has become an indispensable part of modern cybersecurity operations. Therefore it becomes necessary to gather and analyse the data.[1]

In todays world the cyber damage is so high that it affects businesses, regulatory compliance, and trust of the customers.[2] Here it becomes necessary to understand different types of digital forensics that are globally used today.

Objectives

This research has the following aims -

- to discuss the conceptual understandings of forensic science
- to highlights the digital forensic mechanism
- to analyse the forensic investigation in cyber related matters
- to show the difficulties of the investigation procedure
- to provide some proposed measures in this regard

Methodology of Research

This researchers follow d**octrinal and empirical** study with an **analytical and descriptive** method.It focusing on assessing the impact of foreign scientific technique with on Indian digital crime investigations.The researchers have gather their data from doctrinal sources like IT ACT, 2000, Indian Evidence, Bharatiya Sakshya Adhiniyam 2023,case references .In Emprical study the material are the collected from interview ,observation of forensic expert etc.

Types of digital Forensics

1. Disk Forensics:

   It involves the examination of physical or logical storage media such as hard drives,

[1] https://en.wikipedia.org/wiki/Forensic_science(last visited on 24.03.26)
[2]https://www.researchgate.net/publication/348191339_Techniques_in_Forensic_Science_and_Their_Utility_in_Criminal_Justice_System_An_Indian_Perspective(last visited on 24.03.26)

solid-state drives, and removable storage devices. Investigators analyze these storage media to recover deleted files, discover hidden data, and gather evidence related to digital crimes.

2. Network Forensics:

   Network forensics focuses on monitoring and analyzing network traffic and log data to investigate security incidents. It helps in identifying the source of cyberattacks, tracking communication between devices, and understanding the extent of network breaches.

3. Memory Forensics:

   The computer's volatile memory (RAM) provide uncover information about running processes, network connections, and malicious activities to identify live cyber threats and rootkits with this method.

4. Mobile Device Forensics:

   The analysis of smartphones, tablets, and other mobile devices to retrieve data, messages, call logs, and application usage history. Investigators use specialized tools to access locked or encrypted mobile devices.

5. Database Forensics:

   The examine of database systems to identify unauthorized access, data breaches, or data manipulation. Investigators analyze database logs and data structures to uncover evidence of wrongdoing.

6. Cloud Forensics:

   The investigation of cloud-based services and data are stored in the cloud. It includes examining cloud logs, access controls, and metadata to trace activities and assess security incidents.

7. Malware Forensics:

   This involves analysis of malicious software (malware) to understand its behaviour, origins, and impact on system.Investigators study malware code and behavior to determine the scope of an attack.

8. Email Forensics:

   It focuses on the investigation of email communications to gather evidence for legal proceedings. It includes tracking email senders, receivers, timestamps, and content.

9. Live Forensics:

   This form of forensic detect the ransonware activities. The expert has utilize this technique to protect system and retrive violative data without interrupting operation. It is pertinent here to understand the tools and techniques used to assist the investigators.

Cyber Forensics Techniques

In criminal Investigation digital forensic analyse and presenting evidence with the following method :

1. Data Capture Tool

   These tools assist with capturing and preserving digital evidence. They help in forensic imaging, data acquisition, reporting, and validation example FTK Imager, EnCase, Magnet Acquire.

2. File Viewers

   File viewers allow investigators to read file contents without modifying them, ensuring data integrity during analysis for example File Viewer Plus, Quick View Plus, Universal Viewer.

3. File Analysis Tools

   These tools help experts analyse file metadata, access patterns, and ownership information. They assist in identifying anomalies or suspicious activity. example like Autopsy, X-Ways Forensics, Sleuth Kit.

4. Internet Analysis Tools

   These tools track and analyse internet activity, browser history, cookies, cache, and download logs for example tools like Browser History Capturer, Web Historian, NetAnalysis

5. Email Analysis Tools

   Used to trace email headers, analyse attachments, and detect phishing or spoofing activities example tools like MailXaminer, Paraben Email Examiner

6. Mobile Device Forensics

   In this techniques the evidence are derived from electronic devices, messages .It can trace location via GPS, ISP. Oxygen Forensic Suite is a software to collect evidence from mobile.

7. Network Forensics Tools

   It can capture, record, and analyse network traffic LAN/WAN to detect intrusion or unauthorised access example tools like Wireshark, Network Miner.[3]

[3] https//ijettjournal.org/assets/year/2016/volume-41/number-5/IJETT-V41P249.pdf(last visited on 20.4.2026)

Steps of Forensics investigation in digital crime

Digital Forensics is used to test cyber crime by the extracting data from computer system, smartphone, drives found from crime scene. How digital Forensics helps in an Investigation?

1. Incident Response

   The first step in any forensic investigation is incident response. When organizations detect cyberattacks, they must act quickly to contain the threat and minimize damage. This involves identifying the affected systems, securing evidence, and preventing further damage e.g. to prevent malware from spreading, organizations may disconnect infected devices or networks from the larger infrastructure.As soon as they identify an incident, investigators begin recording all actions taken and evidence collected.

2. Evidence Collection

   Once the organization contains a threat, forensic investigators begin collecting digital evidence. This includes logs from firewalls, servers, endpoints, memory dumps, disk images, network traffic captures, and any other relevant data. You must collect evidence in a way that preserves its integrity, meaning that it is not altered or damaged in the process. You can use techniques like disk imaging and write blockers to create exact copies of data, ensuring that the original evidence remains untouched.

3. Data Preservation

   Data preservation is critical for ensuring the collected evidence is usable throughout the investigation. Investigators create a “snapshot” of the systems involved, which they refer back to at any point in the future. The preserved data is crucial for legal proceedings, and its authenticity and integrity are tested.

4. Analysis and Examination

   During this phase, forensic experts analyze the collected data to reconstruct the events that led to the breach. This includes identifying the initial point of compromise, the

methods used by the attackers, and the scope of the damage. You can employ techniques like log analysis (examining system logs for abnormal activity), malware reverse engineering (dissecting malware to understand its behavior), and network traffic analysis (reviewing packet captures for malicious activity).

5. Reporting and Documentation

   Finally, forensic investigators compile their findings into a detailed report. This report outlines the nature of the attack, the vulnerabilities exploited, the evidence collected, and the recommended steps for preventing future incidents. Therefore, this documentation is vital for legal purposes and the organization's internal understanding of the incident.[4]

Legislative structure of Forensic Investigation

Indian Penal Code (IPC), 1860 - The IPC does not clearly mention about forensic science. But we see in DNA profiling, ballistic analysis, and toxicology as for following example -

Offence	**Indian Penal Code (IPC), 1860**	**Bharatiya Nyaya Sanhita 2023[5]**	**Descriptions**
Murder	Section 302	Section 103	Penalty of murder, death or life imprisonment / fine.
Sexual offence	Section 376	Section 64	Punishment for rape, imprisonment upto 10 years - life sentenced and fine.
Damage caused by poisonous means	Section 328	Section 123	10 years and fine as punishment is provided.

Criminal Procedure Code (CrPC), 1973 describes Section 53 describes – Examination of the Accused at the request of police officer (now in section 51of Bharatiya Nagarik Suraksha Sanhita 2023) permits for medical examination of the accused such as DNA samples.

Section 54 says –medical examination of the arrested person .This provision is included currently section 53 of BNSS. The Crpc (Section 165) In cases urgent forensic analysis,authorized officer can seize items for without a warrant which is changed in section185

[4] ermprotect.com(last visited on 6.02.2026)
[5] Justice Khastgir,New Criminal Major Acts , Edition 2025,Kamal Law House,kolkata

of BNSS.Further Section 293 Crpc lays down the report prepared by the Govt. Scientific expert is admissible as evidence before court now included section 328 of BNSS.

Indian Evidence Act, 1872

Section 45 discuss about expert testimony which is considered as a forensic evidence in criminal trial.This provision now inserted section 39(1) of Bharatiya Sakshya Adhiniyam 2023. The function of forensic official is significant supporting the trial procedure. Section 46 deals with the power of the court to rely on expert opinions. It has opened the door for incorporating forensic evidence such as autopsy reports, DNA evidence and its corresponding section 50.

The decision in "**Anvar P.V. v. P.K. Basheer"[2014] 10 SCC 473** that a court have adopted electronic records as a evidence under section 63 of the Indian Evidence Act, now inserted in Bharatiya Sakshya Adhiniyam.The decision has overruled an previous judgment, i.e., State (NCT of Delhi) v. Navjot Sandhu [2005] 11 SCC 600 -the court has awarded an electronic records should not produced as a secondary evidence without proper certificate. [6]

Thus the judiciary has also accepted some problem faced when the genuine electronic copy is missing or certificate cannot be received. Hence it is proposed to change the statute.

Some Judicial interpretations on the digital forensic

In **Arushi Talwar and Hemraj Double Murder Case [2013] 14 SCC 456** deals with the analysis of mobile phone data and online acts and statement of the accused are eaxmeined. However, this case takes the help of forensic expert.Unfortuanately nothing proved against the accused and they were finally discharged by the Allahabad High Court during 2017.

Another landmark case is the "**Mumbai Terror Attacks Case,**" - Investigators depends on call detail records, emails, and mobile data which traced the attackers'connection with the Pakistan. Ajmal Kasab, who is a terrorist of 2008 attacks is guilty of terrorism, murder, and conspiracy. This case proof how digital forensics engaged in a crime .

(Mukesh and Anr. v. State for NCT of Delhi, (2017) 6 SCC) the use of electronic evidence is significant in this case. Forensic professionals shows mobile phone records, CCTV footage, and call lists of the accused that sets up their presence at the crime . All the evidence , medical record and eyewitness punishes the death penalty on four of them.

This case shows the advancement of forensic technology and its effectiveness to solve critical criminal investigations. Courts have rely on the credibility of digital evidence, its

[6] See foot note 4

acknowledgement and validity as laid down of Section 63 of BSA.Thus digital expert plays a important role in assisting cross-examination and contesting opposition evidence , e.g. **"Arushi Talwar Case."** But mishandling the evidence can result in unfair acquittals.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal [2020] 7 SCC 1 mention Section 65B requires the admissiblity of the digital evidence if obtaining the certificate at the time of filing is impossible then evidence will be collected later.Therefore emails or digital photographs, must also have an authentication presented in court.[7]

Sushant Singh Rajput Case 2020 -during 3 October 2020, Dr. Sudhir Gupta of AIIMS, the member of forensic medical team has told that Sushant has committed suicide as no evidence of struggle has been found.[8]

The Sheena Bora Case , the forensic expert verified different IP addressed Sheena personally used and old SMS ,email account.The DNA report showing bones were damaged so they were not easy to identify , but mitochondrial DNA helped confirm that they belong to Sheena.[9]

P. **Gopalkrishnan @ Dileep v. State of Kerala**, **AIR 2020 SC 1; AIRONLINE 2019 SC 1599; 2020 Cri LJ 1240; (2019) 16 SCALE 752** (Supreme Court, judgment dated **29 November 2019**). The display representation and document are seized by the forensic experts After watching the said videos and the petitioner has lodge the complaint before the Judicial First Class Magistrate. The Court has taken considered the seized **memory card/pen-drive** as important electronic material. It observed that the contents of the memory card were copied into a pen drive.[10]

Just Rights For Children Alliance & Anr. v. S. Harish & Ors., **2024 INSC 716** (Supreme Court, judgment dated **23 September 2024**)- This case relating to respondent no 1 has downloaded the obscene material from his phone. The court's decision based on **Computer Forensic Analysis Report** which derived from the mobile phone's internal memory with all call list. .That forensic data are crucial in determining the nature of the stored videos and in relation with **Section 15 of POCSO**. The accused is punishable under Section(s) 67B of the IT Act and 14(1) of the POCSO.[11]

State of Kerala v. Nino Mathew, **2024: KER:34028** (Kerala High Court, judgment dated **24 May 2024**). PW25 was the Assistant Director of Serology, Forensic Science Laboratory,

[7] https://ijrpr.com/uploads/V5ISSUE11/IJRPR34611.pdf(last visited on 20.04.26)
[8] https://en.wikipedia.org/wiki/Suicide_of_Sushant_Singh_Rajput(last visited on 21.04.2026)
[9] https://reflections.live/articles/25665/the-sheena-bora-case-how-digital-forensics-helped-uncover-a-forgotten-case-by-disha-kale-27568-mj6odj3d.html(last visited on 21.04.2026)
[10] https://indiankanoon.org/doc/188011203/(last visited on 19.04.2026)
[11] https://indiankanoon.org/doc/37078038/(last visited on 20.04.2026)

Thiruvananthapuram who submit the report of the material objects and evidences that human blood of group 'AB' was detected in MO1' chopper' and MO21' stick. The Assistant Director of Chemistry in the Forensic Science Laboratory, Thiruvananthapuram, is interrogated as PW26 and records that MO36 and MO18 are chilly powder .Thus The Court has decided the judgemt relied on the **-forensic report**under **Section 67A of the IT Act**. **And** WhatsApp and SMSinformation has been collected from the digital devices which are core elements of **criminal conspiracy**[12]

Munna v. State of Tamil Nadu, **Crl.A. Nos. 73 of 2017 & 106 of 2019** (Madras High Court, judgment delivered **7 December 2021**) that the accused is punished under **Sections 66B, 66E, and 67A of the IT Act with the help of forensic evidence that the** the video clip are indecent. The data are extracted from the e-devices from the accused and the report analyses 65 porn visual representation are stored on the memory card and send to the Physics Division of the Forensic Science Department for investigation.[13]

International Cases Solved with Forensic Investigation in Digital Crimes

Colonial Pipeline Ransomware Attack the Federal Bureau of Investigation used block-chain analysis to track the Bitcoin ransom payment and recovered $2.3 million in 2021. **HSE Ransomware Attack** -Since the attack on Ireland's health service, forensic investigator has analyzed the malware of the devices and modes of communication. **Waifu Hacker Arrest case** culprit has hacked 165 companie's confidential information and asked for money. Expert has traced IP location and arrest the criminal.**Silk Road Dismantling case** Ross Ulbricht's devices and call logs, chat, bakning details financial are checked by the digital investigators. These shows his linked to the illegal business.[14]

Complication in Digital Forensics investigations

Generally it has been seen that digital forensic investigation is quite complicated in nature. **There are several difficulties that forensics expert face while investigating like -**

Digital investigator still face challenges like data encoding, security concerns.Thus it is required to keep digital forensic evidence confidential of the digital evidence which is significant of a case investigation.

[12] https://indiankanoon.org/doc/145067366/(last visited on 24.04.2026)
[13] https://indiankanoon.org/doc/19739195/(last visited on 24.04.2026)
[14] https://www.cyberforensicacademy.com/blog/real-cybercrime-cases-solved-with-cyber-forensics(last visited on 23.04.2026)

Due to limited forensic labs leading pending of cases.

- The users at times feels puzzled for the emergence of software updates and digital platforms.
- Forensic analyst faces problem to gather all the evidence[15] since the New Data Protection Act 2024 provides protection and safeguards against free flow of data.
- Due to multiple jurisdictional issues, it is hard to manage the effective investigation.

Apart from lack of technical expert, procedural complexities, technological limitations gives rise to some challenges.

Suggestion and Conclusion

1. The advanced technologies development forensic investigations is needed.
2. The Indian courts, Judges, lawyers, and parties of the trial should rely and faith on the forensic science in delivering impartial judgment.
3. India requires more forensic laboratories with well equipped technology
4. Trained Digital professional are recruited. In this regard some colleges are now running with various courses in forensic science, digital forensics, and cyber security and students should be aware and given interest to study these types of education.
5. Investing in forensic research and development is vital for for modern criminal investigation.
6. There is required to change or modify the existing statutes that governs the interpretations of digital evidence, training programme with international collabortion and forensic education should also be encouraged.

Last but not the least digital forensic investigation has become a crucial component in any justice delivery system of a country in today's world. With the rapid use of online transactions, cloud computing, and social media, cybercrimes have grown in leaps and bound requiring equally modern investigative mechanisms to deal with such crimes. Though commendable progress has been made in cybercrime units in India, challenges like inadequate infrastructure, unskilled professionals, and such other issues often slow downs the investigation. In this scenario a robust and adaptive digital forensic investigative infrastructure will definitely enhance cybercrime detection, overcome the challenges and reinforce faith in India's digital transformation and justice delivery system.

[15] https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/(last visited on 6.4.2026)