

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

THE STUDY OF COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE IN CRIMINAL INVESTIGATION

AUTHORED BY - KRISHNA VENI.D

Final year student LL.M (Criminal Law),

Crescent School of Law B.S Abdur Rahman Crescent Institute of Science and Technology,
Tamil Nadu.

ABSTRACT

The quick development of technological devices for communication and information has made digital evidence a crucial part of contemporary criminal investigations. Mobile phones, computers, CCTV cameras, emails, social media platforms, cloud storage, and GPS systems are examples of modern electronic devices that produce useful data that can help identify and prove criminal offenses. Investigating agencies can use digital data to reconstruct crime scenes, identify suspects, create timelines, and support court processes. However, due to its extreme fragility and ease of alteration, deletion, or damage, electronic data must be properly collected and preserved in order to guaranty its authenticity and admissibility in court.

The concept, significance, gathering, and storage of digital evidence in criminal investigations within the Indian judicial system are all examined in this paper. It examines the legal recognition and procedural protections for electronic evidence found in the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023. The study also emphasizes how important it is to uphold the chain of custody, employ forensic methods, and adhere to established protocols while conducting an investigation.

Both conceptual and empirical approaches are used in the study. While secondary data was gathered from books, legal journals, court rulings, government papers, and research articles, primary data was gathered from 102 respondents, including advocates and government workers, using a standardized Google Forms questionnaire. The findings indicate that although digital evidence has significantly improved the efficiency of criminal investigations,

challenges such as inadequate forensic infrastructure, the efficient use of electronic gadgets is nevertheless hampered by a lack of technical know-how and careless handling. The study comes to the conclusion that maintaining the integrity, dependability, and admissibility of digital evidence in the criminal justice system requires bolstering cyber forensic capabilities, improving investigator training, and guaranteeing strict adherence to legal procedures.

INTRODUCTION

Every element of human existence has been transformed by the quick development of information and communication technology, including how crimes are committed and investigated. Electronic gadgets including cell phones, computers, laptops, CCTV cameras, cloud storage, emails, social networking platforms, and GPS-enabled systems have become essential components of everyday life in the current digital era. As a result, practically every criminal offense leaves behind some kind of digital imprint that can help investigating agencies identify perpetrators, reconstruct events, and establish facts in court. Consequently, one of the most important types of evidence in modern criminal investigations is digital evidence.

Any information created, transferred, or kept in an electronic format that may be used as proof in court is referred to as digital evidence. Emails, text messages, call logs, CCTV footage, digital photos, audio and video recordings, internet browser histories, financial transaction information, and social media correspondence are all included. In contrast to conventional kinds of evidence, digital evidence is extremely brittle and, if improperly handled, may be readily changed, erased, or ruined. In order to preserve its integrity and validity, its gathering and preservation necessitate the use of specialized forensic techniques, accurate documentation, and rigorous adherence to legal regulations.

Significant legal advancements have resulted from India's increasing dependence on digital evidence. The legal basis for the admission and handling of electronic documents in criminal proceedings is provided by the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023. Law enforcement organizations have been motivated to use cutting-edge technology techniques by the growing significance of cyber forensics and digital investigations. This research looks at how digital evidence is gathered and stored, the laws that control its use, the difficulties investigators encounter, and the steps necessary to guaranty its accuracy and admissibility in the criminal justice system.

RESEARCHED QUESTIONS

1. How familiar are you with digital evidence?
2. Which digital source is most difficult to collect as evidence in criminal investigations?
3. Do encryption, passwords and locked devices create major difficulties in collecting digital evidence?
4. Do you think AI-generated deepfakes and manipulated videos make it difficult to identify genuine digital evidence?
5. How important is maintaining the “chain of custody” of digital evidence?
6. Which one should be given the highest priority to improve digital evidence handling?
7. In your opinion, what is the single biggest challenge in the collection and preservation of digital evidence in criminal investigations?
8. What is the biggest challenge in collecting digital evidence?
9. How concerned are you about the possibility of digital evidence being tampered with during investigation?
10. What do you think is the biggest problem in preserving digital evidence?

OBJECTIVES OF THE STUDY

Examining the idea, importance, and use of digital evidence in contemporary criminal investigations is the main goal of this study. Digital communication and electronic gadgets have become crucial sources of evidence in criminal proceedings due to the quick development of technology. In order to maintain justice and openness in the criminal justice system, the study aims to comprehend how digital evidence helps detect, investigate, and prosecute crimes.

Analyzing the different approaches used for the gathering, storing, and analysis of digital evidence is another goal of the study. The study focuses on how investigative agencies apply appropriate forensic methods and chain of custody to preserve the trustworthiness, authenticity, and integrity of electronic information.

This study evaluates recent technological advancements and legislative reforms that enhance the role of digital evidence in criminal investigations. To assess real-world awareness and practical experiences regarding digital evidence collection and preservation, an empirical survey was administered via Google Forms to 102 legal professionals and government officials. Grounded in these findings, the research highlights key operational challenges faced by

investigators and proposes targeted legal and technical reforms specifically, upgrading cyber forensic infrastructure, providing specialized training for law enforcement, and streamlining legal procedures to improve the reliability and efficiency of digital evidence.

RESEARCH METHODOLOGY

This research adopts a descriptive and analytical methodology. Both primary and secondary sources were used. Primary data was collected through a structured Google Forms questionnaire shared with advocates and government employees to understand their awareness, practical experiences, and opinions regarding collection and preservation of digital evidence. Secondary data was collected from books, journal articles, statutes, government publications, judicial decisions, and reliable online legal resources. The study uses qualitative analysis of legal provisions together with survey observations to draw conclusions.

This research adopts a descriptive and analytical methodology. Both primary and secondary sources were used. Primary data was collected through a structured Google Forms questionnaire shared with advocates and government employees to understand their awareness, practical experiences, and opinions regarding collection and preservation of digital evidence. Secondary data was collected from books, journal articles, statutes, government publications, judicial decisions, and reliable online legal resources. The study uses qualitative analysis of legal provisions together with survey observations to draw conclusions.

LEGAL FRAMEWORK GOVERNING DIGITAL EVIDENCE

The legal framework governing digital evidence in India has developed significantly with the rapid growth of technology and the increasing use of electronic devices in criminal activities. Digital evidence refers to any information stored, transmitted, or generated in electronic form that can be used as evidence in legal proceedings. To ensure its authenticity and admissibility, India has enacted several laws that regulate the collection, preservation, and use of electronic evidence during criminal investigations.

The Information Technology Act, 2000 is the primary legislation governing electronic records and cyber offences. It grants legal recognition to electronic records and digital signatures while providing provisions to address cybercrimes such as hacking, identity theft, and data breaches. The Act also empowers the Government to appoint Examiners of Electronic Evidence to

provide expert opinions in legal proceedings.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) recognises electronic records as admissible evidence before courts. It provides legal validity to emails, digital documents, CCTV footage, audio and video recordings, mobile phone data, and other electronic records, provided they are collected and preserved according to legal procedures. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) further strengthens criminal investigations by encouraging the use of technology in search, seizure, documentation, and trial proceedings.

In addition, Article 21 of the Constitution of India protects the right to privacy, requiring investigating agencies to collect digital evidence through lawful procedures. Landmark judgments such as *Anvar P.V. v. P.K. Basheer*, *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, and *Justice K.S. Puttaswamy v. Union of India* have also clarified the admissibility and protection of electronic evidence. Together, these laws and judicial decisions provide a comprehensive legal framework for ensuring the reliability, integrity, and admissibility of digital evidence in India's criminal justice system.

RECENT DEVELOPMENT

Recent technological advancements have significantly transformed the process of criminal investigation in India, particularly in the collection and preservation of digital evidence. With the implementation of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), greater emphasis has been placed on the use of electronic records, digital documentation, and forensic science in criminal investigations. These reforms have strengthened the legal recognition of digital evidence and promoted the use of technology to improve transparency, efficiency, and accuracy in the criminal justice system.

One of the major developments is the introduction of the e-Sakshya application, which enables investigating officers to collect, document, and securely store digital evidence through electronic means. The expansion of Crime and Criminal Tracking Network & Systems (CCTNS) and the Inter-Operable Criminal Justice System (ICJS) has also improved coordination among police, courts, prisons, prosecution agencies, and forensic laboratories. These digital platforms facilitate faster sharing of information and enhance the efficiency of investigations.

At the same time, emerging technologies such as artificial intelligence (AI), cloud computing, blockchain, encrypted communication applications, and deepfake technology have created new challenges for law enforcement agencies. Criminals increasingly use sophisticated digital tools to conceal evidence, making investigations more complex. As a result, investigating officers require specialised training, advanced forensic tools, and updated technical knowledge to effectively handle digital evidence.

Overall, recent developments demonstrate India's commitment to modernising its criminal justice system through technology. Continuous investment in cyber forensic infrastructure, legal reforms, and capacity building is essential to ensure the secure collection, preservation, and admissibility of digital evidence while protecting individual rights and maintaining public confidence in the justice system.

FINDINGS

1. **Growing Importance of Digital Evidence** The majority of respondents agreed that digital evidence has become an essential component of modern criminal investigations and plays a significant role in solving criminal cases.
2. **Common Sources of Digital Evidence** Most respondents identified mobile phones, CCTV footage, emails, social media platforms, computers, and cloud storage as the most frequently used sources of electronic evidence.
3. **Challenges in Collection and Preservation** Many respondents believed that inadequate cyber forensic laboratories, delays in forensic examination, and improper handling of electronic devices adversely affect the quality and admissibility of digital evidence.
4. **Need for Technical Expertise** A considerable number of participants expressed that investigating officers require specialised training in cyber forensics and digital evidence handling to ensure proper investigation.
5. **Legal Awareness** The survey indicated that awareness regarding the legal procedures governing the collection and preservation of digital evidence is still limited among some investigators, highlighting the need for continuous legal and technical education.

SUGGESTIONS

1. **Strengthen Cyber Forensic Infrastructure** The Government should establish additional cyber forensic laboratories equipped with modern technology and qualified experts to

ensure timely examination of digital evidence.

2. **Specialised Training** Regular training programmes should be conducted for police officers, prosecutors, judicial officers, and forensic experts to improve their knowledge of digital investigation techniques and legal procedures.
3. **Uniform Standard Operating Procedures (SOPs)** Investigating agencies should strictly follow uniform SOPs for the seizure, collection, preservation, documentation, and chain of custody of electronic evidence.
4. **Enhance Cybersecurity Measures** Investment in advanced forensic tools, cybersecurity infrastructure, and secure digital storage systems should be increased to protect electronic evidence from tampering or unauthorized access.
5. **Awareness and Capacity Building** Awareness programmes and workshops should be organised for legal professionals and the general public to promote understanding of digital evidence, cybercrime reporting, and the importance of preserving electronic records.

CONCLUSION

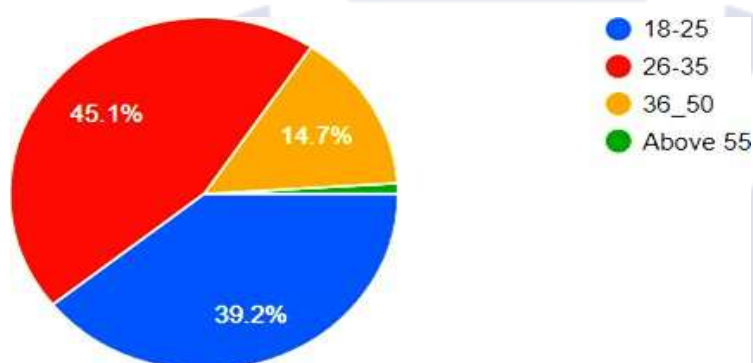
The collection and preservation of digital evidence have become indispensable in modern criminal investigations due to the rapid growth of digital technology and the increasing use of electronic devices in everyday life. As most criminal activities now involve some form of digital communication or electronic transaction, digital evidence plays a crucial role in identifying offenders, establishing facts, and ensuring the successful prosecution of criminal cases. However, because digital evidence is highly fragile and susceptible to alteration, deletion, or unauthorized access, it must be collected, preserved, and examined using scientifically accepted forensic methods and in accordance with the law.

India has made significant progress in strengthening the legal framework governing digital evidence through the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023. These legislative reforms have recognised the importance of electronic records and promoted the use of technology in criminal investigations. The empirical survey conducted among 102 advocates and government employees further highlights the growing acceptance of digital evidence while also identifying challenges such as inadequate forensic infrastructure, lack of specialised training, delays in forensic examination, and limited awareness of legal procedures.

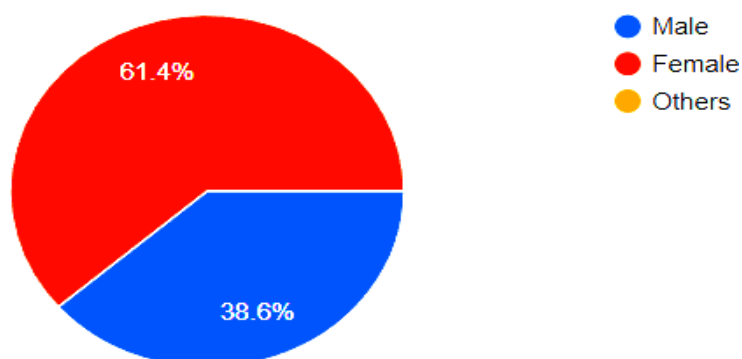
The study concludes that the effective use of digital evidence requires a coordinated effort among investigating officers, forensic experts, prosecutors, advocates, and the judiciary. Continuous training, improved cyber forensic laboratories, strict compliance with standard operating procedures, and investment in advanced investigative technologies are essential to ensure the authenticity and admissibility of electronic evidence. By adopting these measures, India can strengthen its criminal justice system, enhance the quality of investigations, protect the rights of individuals, and ensure the fair and efficient administration of justice in the digital age.

ANEXURE

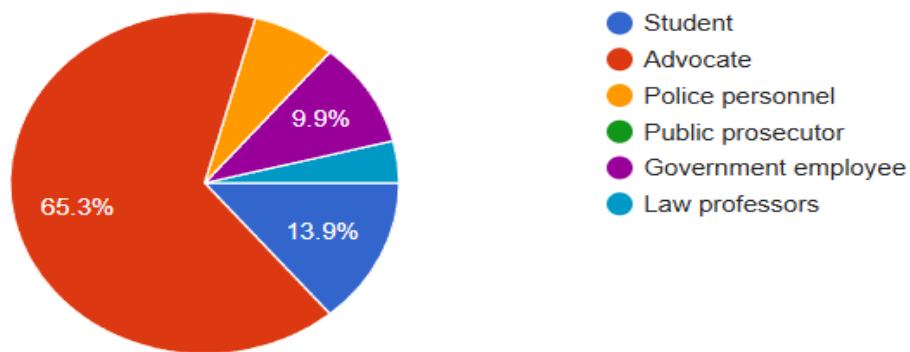
1. What is your age group?



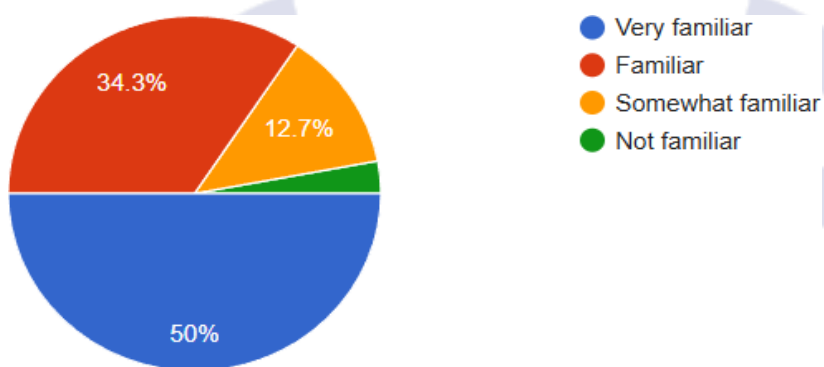
2. What is your gender?



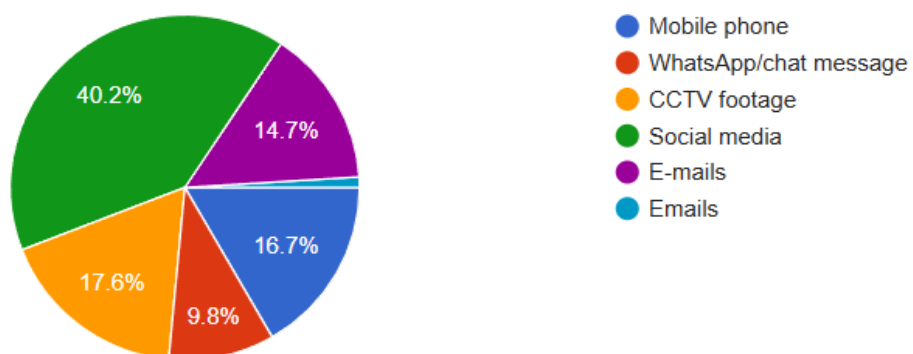
3. What is your occupation?



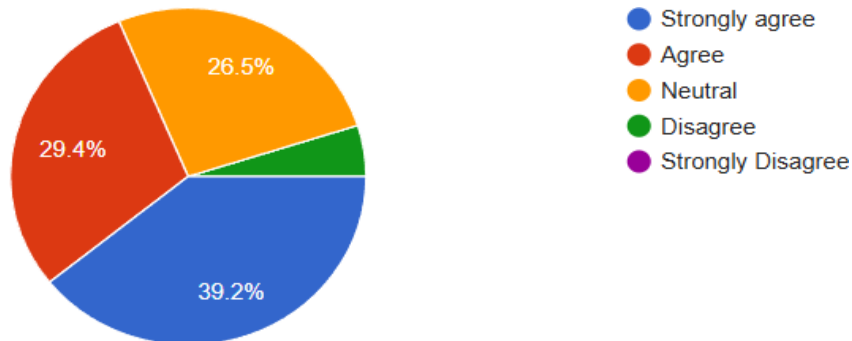
4. How familiar are you with digital evidence?



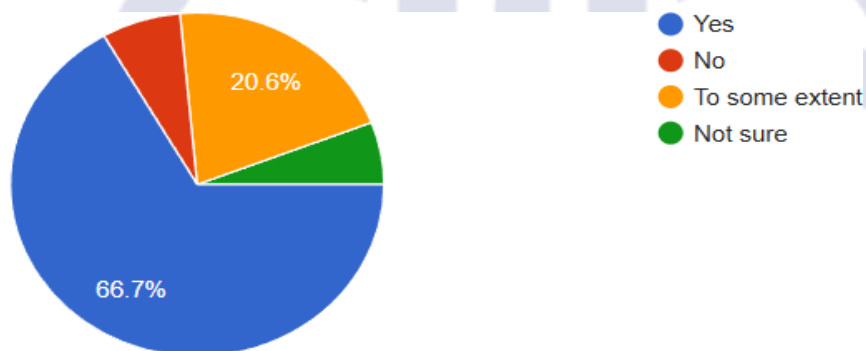
5. Which digital source is most difficult to collect as evidence in criminal investigations?



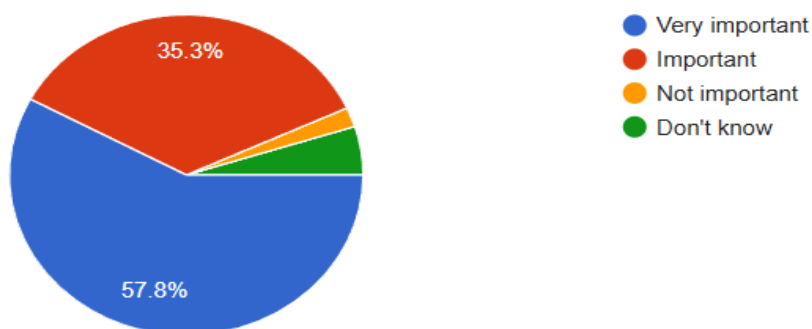
6. Do encryption, passwords and locked devices create major difficulties in collecting digital evidence?



7. Do you think AI-generated deepfakes and manipulated videos make it difficult to identify genuine digital evidence?



8. How important is maintaining the “chain of custody” of digital evidence?



9. Which one should be given the highest priority to improve digital evidence handling?

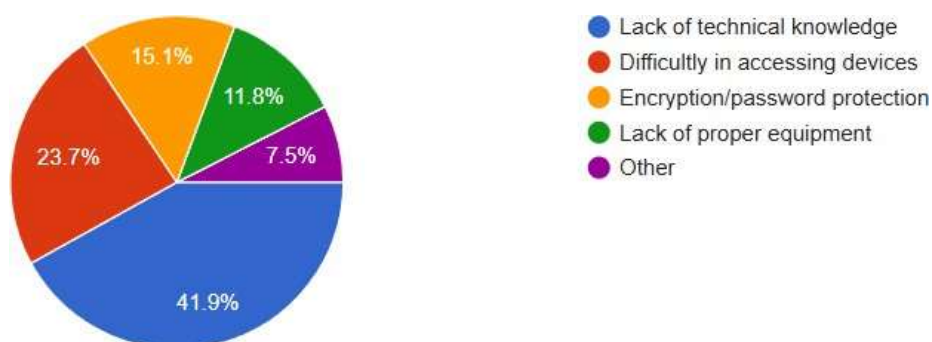


10. In your opinion, what is the single biggest challenge in the collection and preservation of digital evidence in criminal investigations?

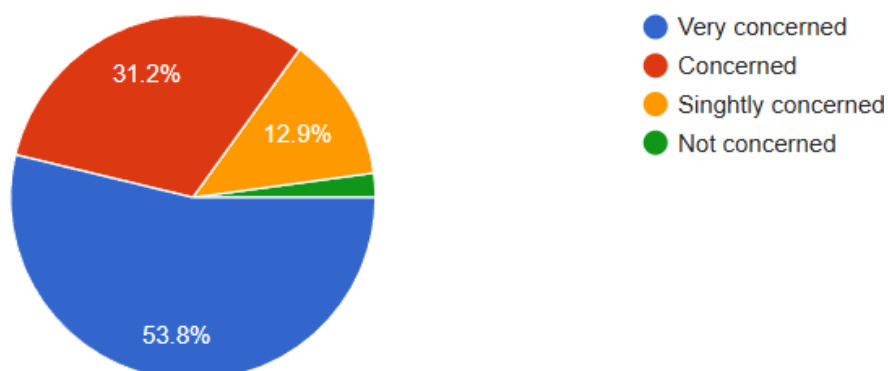
Sl. No.	Major Challenge Identified	Approximate Frequency	Interpretation
1	Maintaining integrity and authenticity of digital evidence	24	The majority of respondents believed that digital evidence is vulnerable to alteration, deletion, or tampering, making proper preservation essential.
2	Lack of technical knowledge and trained personnel	12	Many respondents felt that insufficient technical expertise among investigators affects the proper collection and handling of digital evidence.
3	Volatility and risk of data loss	10	Respondents highlighted that digital evidence can disappear quickly due to deletion, overwriting, or device shutdown, requiring immediate preservation.
4	AI-generated content and deepfakes	6	Several respondents expressed concern that AI-generated images, videos, and deepfakes make identifying genuine digital evidence more difficult.
5	Cloud storage, encryption, and	8	Evidence stored in cloud platforms or protected by encryption presents challenges

	access restrictions		in collection and examination.
6	Large volume of digital data and multiple devices	10	Respondents noted that managing data from mobile phones, computers, CCTV, and other devices is complex and time-consuming.
7	Lack of standard procedures and	11	Many respondents emphasized the need for proper forensic laboratories, standard
	Forensic infrastructure		operating procedures, documentation, and modern equipment.
8	Legal, administrative, and jurisdictional issues	5	Some respondents identified delays in approvals, cross-border investigations, and legal compliance as barriers to evidence collection.
9	High cost and limited resources	3	A few respondents considered the cost of forensic examination and limited technological resources as significant challenges.
Total	Responses Analysed	102	The findings indicate that preserving the integrity of digital evidence, improving technical expertise, strengthening forensic infrastructure, and addressing emerging technological challenges are the primary concerns in digital evidence collection and preservation.

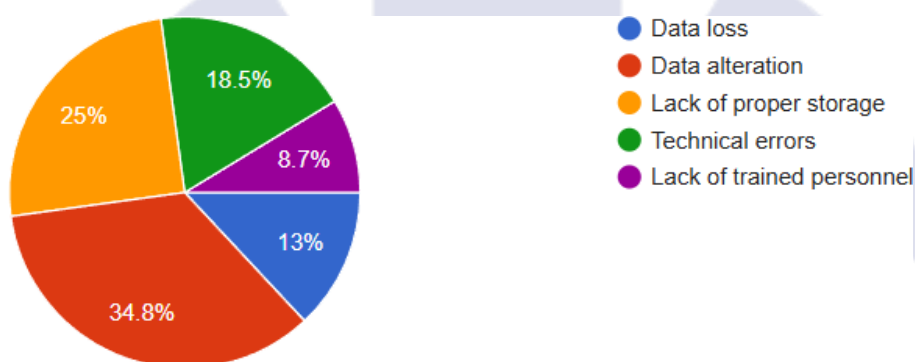
11. What is the biggest challenge in collecting digital evidence?



12. How concerned are you about the possibility of digital evidence being tampered with during investigation?



13. What do you think is the biggest problem in preserving digital evidence?



Bibliography

Books

1. Duggal, Pavan. *Cyber Law in India*.
2. Takwani, C.K. *Law of Evidence*.
3. Ratanlal & Dhirajlal. *The Law of Evidence*.

Statutes

1. Information Technology Act, 2000.
2. Bharatiya Sakshya Adhiniyam, 2023.
3. Bharatiya Nagarik Suraksha Sanhita, 2023.

Case Laws

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
3. *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.

Websites

1. Ministry of Home Affairs – <https://www.mha.gov.in>
2. National Crime Records Bureau – <https://www.ncrb.gov.in>
3. India Code – <https://www.indiacode.nic.in>

