International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cryptographic Integrity and Admissibility of Electronic Evidence: A Critical Appraisal of Hash Value Mandates under Section 63 of the Bharatiya Sakshya Adhiniyam

Robin Singh[1], Dr. Devinder Singh Anand[2]

[1]Scholar, Master of Laws, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Associate Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

ABSTRACT
The growing dependence of criminal and civil proceedings on electronic records has made the integrity of digital evidence a central concern of the law of evidence. Emails, CCTV footage, call detail records, mobile-phone extractions, messaging applications, server logs, cloud data and social-media material can be copied and transmitted without visible changes, but may also be altered, selectively edited, manipulated or generated artificially. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on 1 July 2024, retains a special regime for electronic records under Sections 61 to 63 and introduces a more elaborate certificate framework through Section 63(4) and its Schedule. The Schedule requires disclosure of the hash value of the electronic or digital record and identifies algorithms including SHA-1, SHA-256 and MD5, while Part B provides for expert certification. This paper critically examines the legal and technical significance of hash values, their relationship with authenticity and integrity, and the extent to which they can support admissibility. It argues that a hash value is a valuable integrity-verification mechanism but is not, by itself, proof of authorship, source reliability, lawful acquisition, completeness or truthfulness. It concludes that Section 63 should be implemented through standardised, proportionate and transparent forensic protocols that preserve both evidentiary reliability and fair-trial rights.

Keywords: Electronic evidence; cryptographic hash; Section 63; Bharatiya Sakshya Adhiniyam; admissibility; digital forensics; chain of custody; expert certification.

1. INTRODUCTION

The digital transformation of everyday communication and commercial activity has fundamentally altered the evidentiary landscape. A substantial part of contemporary human activity is recorded electronically, whether through smartphones, computers, CCTV systems, GPS-enabled devices, banking platforms, social-media accounts, cloud services or network infrastructure. Consequently, electronic records are increasingly relied upon to establish identity, location, communication, financial transactions, intention and the sequence of events. Their evidentiary importance is accompanied by a distinctive vulnerability: digital information can be duplicated, modified, deleted, recombined or generated with limited visible indication of interference.

Traditional documentary evidence generally carries physical characteristics that may assist in detecting alteration. Digital records, by contrast, may be copied perfectly and manipulated without leaving obvious traces in the displayed content. A screenshot may not disclose the device or account from which it originated; an exported chat may omit contextual messages; a video file may be transcoded; and metadata may be modified. The court therefore requires reliable methods to establish not only what a record appears to show but also whether the record tendered is the same as the record preserved or examined during investigation.

The BSA recognises electronic and digital records as documents and provides a specialised evidentiary framework. Section 61 affirms that an electronic or digital record cannot be denied admissibility merely because it is electronic, subject to Section 63. Section 62 directs that the contents of electronic records may be proved in accordance with Section 63. Section 63, in turn, prescribes conditions for computer outputs and requires a certificate when a statement is tendered through that provision. The Schedule to Section 63(4)(c) introduces a prescribed certificate containing details of the source device and the hash value, together with the relevant algorithm and an expert component.[1]

This development makes cryptographic integrity a formal part of the statutory process. Yet, the presence of a hash value should not be mistaken for a complete guarantee of evidentiary reliability. A hash function can indicate whether a particular digital bitstream has changed after the hash was generated; it cannot independently establish whether the original data was genuine, whether it was collected lawfully, whether the device clock was accurate, or whether the file represents the event truthfully. The central question is therefore how the law should understand and apply hash value requirements without overstating their technical capacity or creating disproportionate procedural barriers.

2. RESEARCH PROBLEM, OBJECTIVES AND METHODOLOGY

2.1 Research Problem

The statutory inclusion of hash-value disclosure under the Schedule to Section 63 is intended to strengthen the authenticity and integrity of electronic evidence. However, the BSA does not itself provide a detailed operational protocol explaining when hashing must occur, which algorithm should be preferred in different circumstances, how a hash report should be preserved, or how courts should respond to a mismatch or an incomplete certificate. The absence of detailed uniform procedures may result in inconsistent practices among investigating agencies, forensic laboratories, litigants and courts. A further difficulty is the risk of treating a matching hash as conclusive proof of the entire evidentiary chain.

2.2 Objectives

1. To examine the statutory framework governing electronic records under Sections 61, 62 and 63 of the BSA.
2. To explain the technical nature and evidentiary function of cryptographic hash values.
3. To analyse the relationship between hash verification, authenticity, integrity, admissibility and probative value.
4. To examine relevant judicial precedents under the former Section 65B framework and the Supreme Court's interpretation of Section 63(4). [4]
5. To identify procedural and technological challenges in implementing hash-value mandates and suggest safeguards for reliable and fair use of electronic evidence.

[1] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63(4)(a)–(c).

2.3 Research Questions

1. How does Section 63 of the BSA regulate the admissibility of electronic records and what role does the Schedule assign to hash values?
2. To what extent can a cryptographic hash establish the integrity and authenticity of an electronic record?
3. Does compliance with the hash-value requirement necessarily establish the reliability or truthfulness of the contents of a digital record?
4. What principles emerge from judicial decisions concerning certification and electronic evidence?
5. What procedural and institutional reforms are required to ensure consistent, technically sound and fair implementation of Section 63?

2.4 Hypothesis

The paper proceeds on the hypothesis that the statutory requirement to disclose hash values strengthens the integrity-verification process for electronic evidence, but hash disclosure alone is insufficient to establish complete authenticity and reliability unless supported by documented acquisition procedures, chain-of-custody records, competent expert examination and an effective opportunity for challenge.

2.5 Methodology

The study adopts a doctrinal and analytical methodology. It examines the BSA, the Information Technology Act, 2000, relevant judicial decisions, statutory materials and selected academic commentary on digital forensics and electronic evidence. The paper uses technical concepts from cryptography only to the extent necessary to evaluate their evidentiary function. It does not claim to conduct empirical testing of forensic laboratories or hash algorithms.

3. STATUTORY FRAMEWORK UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

The BSA was enacted as Act 47 of 2023 and came into force on 1 July 2024. It replaced the Indian Evidence Act, 1872, while retaining a dedicated framework for electronic records. Section 2(1)(d) expressly includes electronic and digital records within the definition of a document. Section 61 provides that an electronic or digital record shall not be denied admissibility on the ground that it is electronic, and that it has the same legal effect, validity and enforceability as other documents, subject to Section 63. Section 62 directs that the contents of electronic records may be proved in accordance with Section 63.[2]

Section 63(1) deals with information contained in an electronic record that is printed, stored, recorded or copied in optical or magnetic media, semiconductor memory or another electronic form and produced by a computer or communication device. Such computer output is treated as a document if the statutory conditions are fulfilled. Section 63(2) sets out conditions concerning the regular use of the device, ordinary-course supply of information, proper operation and reproduction of the information. Section 63(3) recognises that information may be processed through multiple computers, devices, networks, computer systems, computer resources or intermediaries, treating them as a single computer or communication device for the statutory purpose.[3]

Section 63(4) requires a certificate to be submitted along with the electronic record at each instance where it is submitted for admission. The certificate must identify the electronic record and describe the manner of its production; provide appropriate particulars of the device involved; and address the conditions in Section 63(2). The statutory language contemplates signatures by the person in charge of the computer or

[2] *Supra* note 3, ss. 1(3), 2(1)(d), 61–63 and the Schedule.
[3] *Supra* note 3, ss. 61 and 62.

communication device or the management of the relevant activities, as appropriate, and by an expert. The Schedule supplies a prescribed format divided into Part A, to be filled by the party, and Part B, to be completed by the expert.[4]

Part A requires identification of the source, such as a computer, storage media, DVR, mobile, flash drive, CD/DVD, server, cloud or other source. It also seeks device particulars, including make, model, serial number and relevant identifiers such as IMEI, UIN, UID, MAC or Cloud ID. It contains a statement concerning lawful control and regular use of the device or source, and requires the hash value or values of the electronic or digital record together with the algorithm used. The Schedule lists SHA-1, SHA-256 and MD5 and also accommodates another legally acceptable standard algorithm. Part B provides the expert certification component.

The statutory design is significant because it connects the record tendered in court with information about its source, production and integrity. It also reflects a move from a certificate focused principally on the conditions of computer output under the former Section 65B to a more structured certificate that expressly incorporates hash-value information and expert certification. The statutory requirement should, however, be understood in its proper scope: it is a procedural and evidentiary safeguard, not a declaration that every electronic record accompanied by a certificate is necessarily genuine or conclusive.

4. CRYPTOGRAPHIC HASH VALUES: CONCEPT AND EVIDENTIARY FUNCTION

4.1 Meaning and Operation of a Hash Function

A cryptographic hash function is an algorithm that takes digital input of varying length and produces a fixed-length output, commonly described as a digest or hash value. The digest functions as a compact digital fingerprint of the particular data processed by the algorithm. When the same data is processed using the same algorithm, the expected output is the same. If even a small part of the data changes, the output will ordinarily be different. This property makes hashing useful for checking whether a file has remained unchanged between two points of comparison.[5]

In digital forensic practice, an investigator may calculate a hash value for a source image or file at the time of acquisition and calculate it again when the evidence is transferred, examined or presented. Matching values support the conclusion that the data compared is identical at the bit level. A mismatch indicates that the compared data is not identical and requires investigation. It does not, without more, reveal when the alteration occurred, who caused it or whether the alteration was deliberate.[6]

4.2 Hashing and Integrity

Integrity concerns whether the digital record has remained complete and unaltered during preservation, transfer and examination. Hashing is particularly useful for this purpose because it enables repeatable comparison of digital data. A hash report may therefore strengthen the chain of custody by recording the identity of the data at defined stages. It can also help forensic experts demonstrate that the working copy examined is consistent with the acquired forensic image.

[4] *Supra* note 3, s. 63(1)– (3).

[5] National Institute of Standards and Technology, *Recommendation for Applications Using Approved Hash Algorithms*, NIST Special Publication 800-107 Revision 1 (August 2012).

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

4.3 Hashing Does Not Prove the Truth of Content

The evidentiary function of a hash value is limited. If a fabricated video is created and its hash is calculated immediately, the hash will faithfully identify that fabricated file. If an edited screenshot is presented as an original and hashed after editing, a matching hash at later stages will show only that the edited screenshot remained unchanged after that point. A hash value does not independently establish who created the file, whether the recording device was correctly configured, whether the account was controlled by the alleged author, whether the content is complete, or whether the event depicted actually occurred.

Accordingly, courts should distinguish at least four questions: first, whether the record is relevant; secondly, whether it satisfies the statutory conditions for admissibility; thirdly, whether its source and integrity have been sufficiently established; and fourthly, what weight should be assigned to its contents. Hash verification principally assists with the third question, while Section 63 addresses the statutory route to admissibility. Neither replaces judicial evaluation of probative value.

4.4 Algorithm Selection and the Schedule

The Schedule refers to SHA-1, SHA-256 and MD5, while allowing another legally acceptable standard algorithm. These algorithms do not provide identical security assurances. MD5 and SHA-1 have known collision vulnerabilities, meaning that specially constructed different inputs can be made to produce the same digest. SHA-256, from the SHA-2 family, is generally preferred for contemporary integrity verification. The express listing of multiple algorithms in the Schedule should not be read as a technical finding that they are equally secure for every forensic purpose. A sound protocol should favour currently accepted algorithms, record the algorithm and tool version, and preserve sufficient information to permit independent verification.[7]

The statute's reference to a legally acceptable standard algorithm offers flexibility as cryptographic standards evolve. Yet, flexibility without practical guidance can lead to inconsistent selection. A uniform technical protocol should explain the circumstances in which an algorithm may be used, how multiple hashes may be recorded, and how older records bearing legacy hash values should be handled. The legal inquiry should remain focused on whether the method used is appropriate, transparent and reproducible in the circumstances.

5. ADMISSIBILITY, AUTHENTICITY AND THE CHAIN OF CUSTODY

The chain of custody is the documented history of the collection, possession, transfer, storage, examination and production of evidence. For electronic records, it should identify the person who collected the data, the device or source, the date and time of acquisition, the method and tools used, the original and forensic copies, each transfer, storage conditions and every examination performed. Hash values can reinforce this history by enabling comparison of the data at different stages. They cannot replace the history itself.[8]

A hash value calculated only after a record has passed through several undocumented hands cannot establish what happened before hashing. Similarly, if the original device is accessed in a manner that changes system data, metadata or logs, the subsequent hash may preserve the altered state rather than the state existing at the time of seizure. This is why forensic acquisition should ordinarily use documented

[7] Z. E. Rasjid, B. Soewito, G. Witjaksono and E. Abdurachman, "A Review of Collisions in Cryptographic Hash Function Used in Digital Forensic Tools," 116 *Procedia Computer Science* 381–392 (2017), https://doi.org/10.1016/j.procs.2017.10.072.

[8] National Institute of Standards and Technology, Digital Evidence Preservation: Considerations for Evidence Handlers, *NISTIR* 8387 (2022).

procedures, write-blocking where appropriate, validated tools and forensic imaging. The exact method will depend on the device, operating system, encryption status, cloud architecture and investigative circumstances.

Cloud and platform-based evidence creates additional complications. The source may be a remote server controlled by a service provider rather than a device physically seized by investigators. Data may be distributed across servers, automatically synchronised, compressed, re-encoded or subject to retention policies. In such cases, the certificate should identify the actual source and method of extraction as precisely as reasonably possible. Investigators should preserve provider responses, extraction logs, timestamps, account identifiers and available integrity information. A generic reference to a mobile phone or cloud account may not sufficiently explain how the tendered output was produced.

The distinction between an original electronic record and a computer output also remains important. Section 63 provides a route for computer outputs where the statutory conditions are satisfied. The production of a device itself, or a source record in a form recognised as primary evidence, may raise different questions from the production of a copied or exported record. Courts should avoid mechanical application of a certificate requirement without first identifying the evidentiary form being tendered and the applicable statutory route. The certificate should be evaluated in relation to the record actually produced.

6. JUDICIAL DEVELOPMENT: FROM SECTION 65B TO SECTION 63

6.1 Anvar P.V. v. P.K. Basheer

In *Anvar P.V. v. P.K. Basheer*, the Supreme Court interpreted Section 65B of the Indian Evidence Act, 1872 as a special provision governing proof of electronic records by way of computer output. The Court held that the statutory certificate was required for secondary electronic evidence and that the general rules of secondary evidence could not be used to bypass the special procedure. The decision established the centrality of certification in the admissibility of computer outputs.[9]

6.2 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

The three-Judge Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* reaffirmed Anvar and clarified the certificate requirement under Section 65B. It held that the certificate is a condition precedent to admissibility of secondary electronic evidence, while recognising that the requirement does not apply in the same way where the original electronic record itself is produced by its owner or operator and proved through the appropriate witness. The Court also recognised the court's power to assist a party in obtaining a certificate where the relevant device or system is controlled by a third party.[10]

These decisions were delivered under the former Evidence Act and did not interpret Section 63 of the BSA. Nevertheless, they remain important to the extent that the BSA retains a special statutory certificate mechanism. Their principles must be applied with attention to the textual changes introduced by Section 63(4) and the Schedule, particularly the express hash-value and expert-certification components.

6.3 Pune Bar Association v. Union of India (2026)

A significant development arose in *Pune Bar Association v. Union of India*, 2026 SCC OnLine SC 1297, decided on 22 May 2026. The Supreme Court considered a challenge to the constitutional validity of Section 63(4) of the BSA read with the Schedule, including the requirements relating to disclosure of hash

[9] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

[10] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

values and expert certification. The Court upheld the provision against the challenge of manifest arbitrariness. It reasoned that a hash value functions as an electronic fingerprint and that its disclosure has a rational connection with verifying the authenticity and integrity of digital data. The expert component was regarded as an additional safeguard for secondary electronic evidence.[11]

The Court also considered whether Part B of the certificate could be signed only by an Examiner of Electronic Evidence notified under Section 79A of the Information Technology Act, 2000. It clarified that the Madras High Court's view in R. v. B., (2024) 1 HCC (Mad) 531, that Part B must necessarily be signed by such a notified examiner, would not operate as a binding precedent. The Court discussed the interaction between Section 39(1) and Section 39(2) of the BSA and indicated that persons possessing special skill in computer science and cyber forensics may potentially qualify as experts, subject to judicial satisfaction. However, it kept the precise scope of expert certification open for consideration in an appropriate case.

The decision is important for two reasons. First, it confirms the constitutional validity of the statutory hash and expert-certificate requirements. Secondly, it does not finally settle every operational question concerning who may sign Part B or what qualifications and materials are sufficient to establish expertise. The judgment should therefore be cited carefully: it upholds the statutory framework but leaves the precise contours of expert eligibility open.

6.4 Emerging Trial-Court Practice

Recent trial-court decisions illustrate the practical consequences of incomplete certificates, including omission of hash values or the expert component. Such decisions indicate that courts may treat the requirements of Section 63(4) as material conditions for admitting computer outputs. However, individual trial-court decisions should not be treated as a substitute for authoritative Supreme Court interpretation. Their value lies in demonstrating the kinds of compliance disputes likely to arise during implementation.[4]

7. CRITICAL APPRAISAL OF THE HASH-VALUE MANDATE

7.1 Strengthening Reliability

The principal strength of the statutory mandate is that it encourages parties and investigating agencies to identify electronic records with greater precision. A hash value provides a reproducible reference point and can expose changes between acquisition and production. By requiring the value to be recorded in the certificate, the Schedule makes integrity verification visible to the court and the opposing party. The expert component can further explain the method of extraction, the tools used and the significance of the hash report.

7.2 Risk of Treating Hash as Conclusive Authentication

A major risk is that the legal process may overstate what a hash proves. A matching hash establishes identity between the data sets compared, assuming the algorithm and procedure are correctly applied. It does not establish the reliability of the source device, the identity of the person who generated the content, or the truth of the recorded event. A court should therefore ask when the hash was first calculated, what exact object was hashed, whether the source was a device, file or forensic image, whether the process was documented and whether independent verification is possible.

7.3 Algorithmic and Technical Ambiguity

The Schedule lists algorithms but does not prescribe a single preferred algorithm or provide a detailed standard operating procedure. The continued listing of MD5 and SHA-1 may create confusion for non-

[11] *Pune Bar Association v. Union of India*, 2026 SCC OnLine SC 1297 (decided on 22 May 2026).

specialists, particularly if the presence of a listed algorithm is treated as sufficient without considering known weaknesses. The law should not freeze technical standards in statutory text; instead, rules or authoritative forensic guidelines should provide a regularly updated list of acceptable algorithms and explain how legacy hashes should be treated.[12]

7.4 Accessibility and Institutional Capacity

Mandatory expert certification may create difficulties for individuals, small litigants and parties who rely on records controlled by service providers or third parties. Forensic laboratories may face backlogs, uneven geographical distribution and limited technical capacity. A requirement that is intended to improve reliability may become a barrier if there is no accessible process for obtaining a certificate or for seeking judicial assistance. The Supreme Court's 2026 clarification that the Madras High Court's restrictive view on exclusive Section 79A certification is not binding is relevant to this concern, although the precise eligibility criteria remain open.

7.5 Fair-Trial and Disclosure Concerns

The accused must be able to test the electronic material relied upon by the prosecution. Disclosure should, where relevant and legally permissible, include the certificate, hash reports, acquisition logs, forensic image details, tool names and versions, extraction methodology, relevant metadata and expert findings. A bare certificate may not provide a meaningful opportunity to challenge the evidence if the underlying technical basis is withheld. At the same time, disclosure must be managed consistently with privacy, privilege, data protection and legitimate investigative interests.

7.6 AI-Generated and Manipulated Evidence

The growing availability of synthetic audio, deepfake video, generative image tools and automated editing applications makes the distinction between integrity and authenticity particularly important. A deepfake may be hashed immediately after creation and remain unchanged throughout the chain of custody. Hash verification will confirm the stability of the file, not whether it depicts a genuine event. Courts may therefore need additional evidence concerning provenance, device characteristics, metadata, editing traces, source acquisition, expert analysis and corroborating circumstances. The hash value is one part of a broader authentication inquiry, not a substitute for it.

8. COMPARATIVE AND TECHNICAL PERSPECTIVE

International digital-forensic practice commonly treats hashing as one component of evidence preservation and verification. Technical standards and forensic guidance emphasise documented acquisition, repeatability, preservation of original data, validation of tools and recording of actions taken by investigators. The value of such guidance is not that it creates a universal rule of admissibility, but that it helps courts assess whether a forensic process was reliable and reproducible.

The United States Federal Rules of Evidence, particularly Rule 902(14), provide a mechanism for self-authentication of data copied from an electronic device, storage medium or file through a process of digital identification. The rule does not make every hashed file automatically admissible; it requires certification by a qualified person and remains subject to other evidentiary objections. This offers a useful comparison because it demonstrates how technical certification can simplify proof while preserving the court's ability to assess relevance, hearsay, unfair prejudice and reliability.

[12] Nicky Mouha, M. S. Raunak, Richard Kuhn and Raghu Kacker, "Finding Bugs in Cryptographic Hash Function Implementations," 67(3) *IEEE Transactions on Reliability* 870–884 (2018), https://doi.org/10.1109/TR.2018.2847247.

India may draw from such approaches by developing clear technical protocols while retaining flexibility for different forms of digital evidence. The framework should distinguish between a routine integrity check and a complex forensic examination. It should also recognise that a single protocol may not be appropriate for all evidence types, including live CCTV systems, encrypted mobile devices, volatile memory, cloud records and platform-generated exports.

9. RECOMMENDATIONS AND REFORM PROPOSALS

The technical guidance should ordinarily recommend the use of standard/stronger currently accepted cryptographic algorithms like SHA-256 and explain the minimal use of legacy algorithms like MD5 and SHA-1.

1. Indicate time and object hashing applied to: The certificate and the forensic report should contain the type of hashing applied to a particular object (original source, forensic image, extracted file, exported output or later working copy) and the time of the hash.
2. Standardise chain of custody documentation – Investigating agencies should document chain of custody in a way that is tamper evident with dates, times, persons responsible, and reasons column.
3. Preserve original data and forensic copies: Where reasonably practicable, preserve original source and make a verified forensic copy for examination. If any changes have been made during acquisition that cannot be avoided, they should be noted and explained.
4. Clarify the definition of relevant expertise: Rules or guidance from experts should define the competency that is relevant to the practice of digital forensics, computer science, cybersecurity and forensic acquisition, but not unnecessarily limit certification to a narrow institutional category.
5. Establish a judicial assistance process: Courts should provide for appropriate production or certification, where one cannot be obtained because of control of the device or the system by a third party, in accordance with fair-trial standards.
6. Make disclosure meaningful: Provide adequate technical information to the opposing party to defend integrity claim, such as the certificate, hash report, acquisition methods and the relevant forensic logs, subject to the Lawful Protection.
7. Evidence-type specific protocols: There should be evidence-specific guidance developed for CCTV, mobile devices, messaging applications, cloud records, social-media content, server logs and AI generated and manipulated media.
8. Train judges, lawyers and investigators: Continuing education should describe what the hash value demonstrates and what it does not demonstrate, and how to assess the expert report without relying on technical jargon rather than legal reasoning.
9. Use hash verification as an additional element in the judicial review: Courts should take into account source provenance, authorship, completeness, legality of acquisition, metadata, corroboration and possibility of manipulation together with hash values.

10. CONCLUSION

Section 63 of Bharatiya Sakshya Adhiniyam is a crucial provision in the electronic evidence law. The legislature has attempted to enhance the integrity and traceability of electronic records presented to courts by making them subject to hash-value disclosure and expert certification in the Schedule. The Supreme Court in the case of Pune Bar Association v. Union of India has again affirmed the constitutionality of this framework and the "rational relationship" that exists between hash disclosure and the goals of authenticity

and integrity. However, a hash value is not a full proof of authenticity. It can prove that the data compared has not been changed since the time the relevant hash was created and it cannot prove or stand alone as proof for the source, authorship, completeness, or lawful acquisition or factual accuracy of the record. A record that was fabricated or manipulated can also have a stable hash. Therefore, cryptographic verification needs to be considered in conjunction with the chain of custody, forensic acquisition, the metadata analysis, expert evidence and the possibility of challenging material presented by the opposing party. The ability of Section 63 to work effectively in the future will depend not only on compliance with the certificate but on the process that led to it being provided. To ensure that the hash-value mandate does not become a formality or an overly burdensome procedural hurdle, the uniform technical protocols, modern algorithm guidance, available expert services, disclosure and judicial training must be provided. The right balance is thus obtained: hash values are a meaningful integrity control measure, but their evidentiary value has to be commensurate with the potential of cryptographic technology. This would further the BSA's goal of fair trial, and also minimize the risks that digital evidence would be accepted without proper evidence or technical issues could prevent evidence from being admissible.