GNU GROUP · LAW & TECHNOLOGY FIELD GUIDES

FREE SAMPLE

# Section 63 in Practice

## Proving Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

A field guide for lawyers, investigators and forensic experts: the certificate, the hash value, Part A and Part B, chain of custody, and what the courts have said so far.




Law stated as on 14 November 2026

Covers *Pune Bar Association v. Union of India* (Supreme Court, 2026)

**GNU Group**

Written by the GNU Group legal team

**Free sample**

**gnugroup.org/books**

# Section 63 in Practice

## Proving Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

A field guide for lawyers, investigators and forensic experts

**GNU Group**

Written by the GNU Group legal team

Free sample: Chapters 1 and 7 · Law stated as on 14 November 2026
gnugroup.org

**Section 63 in Practice: Proving Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023**

Free sample of the first edition, November 2026. Digital edition (PDF).

Published by GNU Group, a brand of Gnu IT Solutions & Services Pvt. Ltd., Mumbai, India. https://gnugroup.org

Written by the GNU Group legal team.

**Copyright.** © 2026 Gnu IT Solutions & Services Pvt. Ltd. All rights reserved under the Copyright Act, 1957. The text of statutes, rules, notifications and judgments referred to in this book belongs to the Government of India and the respective courts; this book claims no copyright in them.

**This sample.** This free sample contains the front matter, Chapter 1 and Chapter 7 of the book, unabridged. You may read it, keep it and share it with others, provided it is passed on complete and unaltered and is not sold. All other rights are reserved. The full book, 122 pages, is available at gnugroup.org/books. References in these pages to other chapters and appendices are to the full book.

**Not legal advice.** This book is general information for practitioners. It is not legal advice and does not create a lawyer-client relationship. Evidence law is applied by courts to the facts of each case; whether a record is admitted, and what weight it receives, is decided by the court. Before relying on any statement in this book in a proceeding, read the current official text of the statute and the full text of the judgment cited, and take advice from an advocate in your jurisdiction.

**Law stated as on 14 November 2026.** The law on Section 63 is developing. In particular, the question of who may sign Part B of the certificate was expressly left open by the Supreme Court in May 2026 and may be decided differently in future. Chapter 6 lists the open questions. Check for later decisions and amendments before you rely on this edition.

**No guarantee.** The publisher has taken care to check the contents against the sources listed in "Sources and verification" but gives no warranty that the book is free of error, and accepts no liability for loss arising from its use, to the fullest extent the law permits. No tool, template, certificate format or procedure described here can guarantee that a court will admit a record.

**Specimens are fictional.** All names, parties, devices, identifiers, file names and facts in the worked examples are invented for illustration. Any resemblance to real persons, organisations or cases is coincidental. Hash values printed in the specimens were computed from sample files created for this book.

**Evidence Custodian.** Chapter 20 describes Evidence Custodian (evidence.gnugroup.org), a product of the publisher, as one worked example of a certification platform. Every procedure in the book can be carried out without it.

**Trade marks.** WhatsApp, Windows, PowerShell, macOS, Android, iOS, Google, Gmail, Outlook and other product names are trade marks of their respective owners and are used only to identify the products. This book is not affiliated with or endorsed by any court, government body or vendor.

Corrections and suggestions: support@gnugroup.org

# Contents

How to use this book . . . . . iv
What is in the full book . . . . . vi

**I The Law**

1 Why electronic evidence got its own rule . . . . . 2
1.1 Three properties that paper does not have . . . . . 2
1.2 What the court is really being asked to accept . . . . . 2
1.3 Why the rule was tightened in 2023 . . . . . 3
1.4 What changed and what did not . . . . . 3

**II The Technology**

7 Hash values without the mathematics . . . . . 6
7.1 What a hash value is . . . . . 6
7.2 What a hash value proves, and what it does not . . . . . 6
7.3 MD5, SHA-1 and SHA-256 . . . . . 7
7.4 Computing a hash value . . . . . 8
7.5 The hash report . . . . . 10
7.6 Answering objections about the hash . . . . . 10
Continue with the full book . . . . . 12

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

# How to use this book

Since 1 July 2024, anyone who wants an Indian court to look at a WhatsApp chat, a CCTV clip, an email, a bank statement printout or a call recording has had to deal with Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The section replaced Section 65B of the Indian Evidence Act, 1872, and it added two things that practitioners had never had to produce before: a hash value for the record, and the signature of an expert.

This book is a working guide to that requirement. It explains the law in the order a practitioner needs it, explains the technology without assuming a technical background, and then shows, field by field, how the certificate is completed and where it goes wrong.

## Three readers, one book

The book is written for three groups who meet in the same courtroom and usually do not share a vocabulary.

| If you are | You most need | Read first | Then |
|---|---|---|---|
| A lawyer or litigator | To file a certificate that survives objection, and to attack one that should not | Chapters 3, 5, 6, 11 to 15 | Chapter 7 for the hash value; the rest as reference |
| A police officer or investigator | To seize, hash, preserve and document so that the record is usable at trial | Chapters 7 to 10, 16 | Chapters 3, 11, 12 and 14 |
| A forensic or IT expert | To know what you are certifying in Part B and how to defend it in the witness box | Chapters 5, 6, 12, 17 | Chapters 3, 4 and 10 |
| An organisation that produces records (bank, hospital, company) | To be ready to certify your own records on request | Chapters 11, 18 | Chapters 7 and 10 |

Chapters 1 to 6 are the law. Chapters 7 to 10 are the technology. Chapters 11 to 14 are the certificate itself. Chapters 15 to 18 are role playbooks. Chapters 19 and 20 are complete workflows, first by hand and then with a platform. The appendices hold the worksheets, checklists, glossary and tables.

## Conventions

Every chapter ends with two boxes. **In practice** gives the three to five actions to take. **If challenged** gives the objection you are most likely to meet and the answer to it. Other boxes are used as follows.

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

**Key point: what this box is for**

A rule or idea that the rest of the chapter depends on.

**Unsettled: what this box is for**

A point on which the law is not settled as on the date of this edition. These are collected in Chapter 6.

**Caution: what this box is for**

A mistake that damages evidence or a certificate and is hard to undo.

References to "the Act" or "the BSA" are to the Bharatiya Sakshya Adhiniyam, 2023. "IEA" is the Indian Evidence Act, 1872. "BNSS" is the Bharatiya Nagarik Suraksha Sanhita, 2023. "BNS" is the Bharatiya Nyaya Sanhita, 2023. "IT Act" is the Information Technology Act, 2000. "The Schedule" is the Schedule to the BSA, which sets out the certificate. "The certificate" is the certificate under Section 63(4).

Commands are shown in a monospaced box. Text you type is shown as written; output is shown beneath it. Hash values are long, so they are printed in small type and may wrap onto a second line. A wrapped hash is still one value with no spaces.

## What this book does not do

It does not reproduce the Act. Provisions are described in the book's own words, clause by clause, with the section number, so that you can read them beside the official text on India Code (indiacode.nic.in). Where exact wording matters, and in a certificate it always does, take the wording from the official text and not from this or any other commentary.

It does not teach digital forensics as a discipline. It teaches the part of it that a certificate depends on: identifying the source, taking a faithful copy, hashing it, and keeping an unbroken record of who held it.

It does not promise outcomes. A correct certificate gets a record through the door. What the court makes of the record after that is a separate question, and Chapter 6 explains why.

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

# What is in the full book

This sample contains the two chapters marked with an arrow. The full book has 20 chapters and 10 appendices in 122 pages.

| Part | Chapters |
|---|---|
| **I. The Law** | **1. Why electronic evidence got its own rule** ← in this sample |
| | 2. From Section 65B to Section 63: the case-law road |
| | 3. Section 63 read clause by clause |
| | 4. The neighbouring provisions |
| | 5. Pune Bar Association v. Union of India (2026) |
| | 6. Open and contested questions |
| **II. The Technology** | **7. Hash values without the mathematics** ← in this sample |
| | 8. Where the record lives: device, file, image and cloud |
| | 9. Metadata and timestamps |
| | 10. Chain of custody and the audit trail |
| **III. The Certificate** | 11. Part A, field by field |
| | 12. Part B, field by field |
| | 13. Worked examples: six specimen certificates |
| | 14. Twelve defects that sink certificates |
| **IV. Role Playbooks** | 15. For lawyers: filing, objecting, curing |
| | 16. For police and investigators |
| | 17. For forensic and IT experts |
| | 18. For organisations: being evidence-ready |
| **V. Tools and Workflow** | 19. Doing it by hand |
| | 20. Doing it with a platform: Evidence Custodian as an example |
| **Appendices** | A. Section 63 at a glance |
| | B. Certificate data worksheet |
| | C. Hash report specimen |
| | D. Custody log specimen |
| | E. Checklists, including a certificate verification table |
| | F. Notified Examiners of Electronic Evidence |
| | G. Glossary |
| | H. Table of cases and statutes, with links to the principal sources |
| | I. Model drafts: preservation request and two applications |
| | J. Frequently asked questions |

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

PART I

# The Law

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

CHAPTER 1

# Why electronic evidence got its own rule

A paper document has a body. It can be held, its ink can be tested, its paper can be dated, and an alteration usually leaves a mark. For more than a century the law of documentary evidence in India rested on that fact. The best evidence of a document was the document itself, produced in court, and a copy was allowed only when there was a good reason why the original could not be brought.

Electronic records broke that model in three ways, and each of the three explains a part of Section 63.

## 1.1 Three properties that paper does not have

**Copies are perfect.** A photocopy is visibly a copy. A copied file is bit-for-bit the same as the file it was copied from. There is nothing in the copy that marks it as second-generation. So the old question, "is this the original or a copy?", often has no physical answer. The law had to decide what "original" means for a record that lives on a server in another city and is seen only through printouts and exports.

**Alteration is silent.** A chat export is a text file. Anyone can open it and change "4,50,000" to "4,60,000" and save it. No erasure mark is left. The same is true, with more effort, of images, audio and video, and the effort required has fallen sharply with generative tools. A court looking at a printout cannot tell from the paper whether the underlying file was changed before it was printed.

**The record is surrounded by data about itself.** A photograph carries the make of the camera, the time, sometimes the place. An email carries the path it travelled. A file system records when a file was created and last modified. This metadata can support a record or contradict it, and it is easily lost or changed by ordinary handling, such as forwarding a picture through a messaging app.

The law's response to the first property is the deeming rule in Section 63(1): a computer output that meets stated conditions is treated as a document and is admissible without the original. Its response to the second is the certificate, and since 2024, the hash value inside the certificate. Its response to the third is indirect. Metadata is not mentioned in Section 63, but the disciplines that protect it are the same disciplines that keep a hash value stable, and they are the subject of Part II of this book.

## 1.2 What the court is really being asked to accept

When a party tenders a printout of a bank statement, the court is asked to accept a chain of four propositions.

1. A computer system held certain information.
2. The system was working properly and was being used in the ordinary way when it held that information.

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

3. What is now before the court is a faithful output of that information.
4. Nothing has changed between the moment of output and the moment of tender.

Section 63(2) is about propositions 1 and 2. The certificate under Section 63(4) is a statement, by a person with responsibility for the system, that propositions 1 to 3 are true. The hash value is the tool for proposition 4. Read in this way, the certificate is not a formality added to the evidence. It is the evidence of reliability, given in a compact form so that the person who runs a server does not have to be called in every case to say so orally.

> **Key point: admissibility is not proof**
>
> Section 63 answers one question: may the court look at this record as a document? It does not answer the next questions: is the record genuine, who authored it, and what does it prove? Those are decided on all the evidence. A certificate gets a record admitted. It does not make the record true.

## 1.3 Why the rule was tightened in 2023

The Statement of Objects and Reasons of the BSA says that the new law provides for the admissibility of electronic or digital records as evidence and widens secondary evidence to include matching hash values. When the Supreme Court upheld Section 63(4) in May 2026 it tied the stricter certificate to a present-day concern. The order observes that electronic records are easily altered and that artificial intelligence and deepfakes complicate their admissibility, and it treats the hash value and the expert's signature as safeguards against that risk (Chapter 5).

Two practical facts lie behind the change.

First, the volume. Family disputes are argued on chat screenshots. Commercial suits are argued on email and ledgers. Criminal trials turn on call detail records, CCTV and phone extractions. A rule that was once a specialist's concern now touches most contested cases.

Second, the experience under Section 65B. For years the certificate was often a short paragraph, differently worded in every case, signed by whoever was available, and sometimes produced after the trial had begun. Courts spent much of the period from 2005 to 2020 deciding whether it was needed at all. The BSA answers with a fixed form, set out in a Schedule, so that the same particulars are given in every case and a court can check them quickly.

## 1.4 What changed and what did not

The core of the old Section 65B survives. The four conditions in sub-section (2) are substantially the same. The idea that the certificate is the route to admitting a copy is the same. What is new is summarised below and explained in Chapter 3.

| Point | Section 65B, Indian Evidence Act | Section 63, BSA |
|---|---|---|
| Devices covered | Computer | Computer or any communication device; output "otherwise stored, recorded or copied in any electronic form" is included |
| Media named | Paper, optical or magnetic media | Adds semiconductor memory |
| Form of certificate | No prescribed form | Form set out in the Schedule: Part A and Part B |

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

| Point | Section 65B, Indian Evidence Act | Section 63, BSA |
|---|---|---|
| Who signs | A person in a responsible official position | The person in charge of the device or of the management of the relevant activities, and an expert |
| Hash value | Not mentioned | To be stated in both parts, with the algorithm, and a hash report enclosed |
| When submitted | Not stated in the section | With the electronic record, at each instance where it is submitted for admission |
| Electronic records as primary evidence | Developed by case law | Explanations 4 to 7 to Section 57 |

**In practice**

- Treat the certificate as the reliability evidence for the record, and prepare it with the same care as an affidavit.
- Separate two tasks in your mind and in your file: getting the record admitted (Section 63), and proving that it is genuine and what it shows (everything else).
- Use the Schedule format for every matter governed by the BSA. A Section 65B-style paragraph is not a Section 63 certificate.

**If challenged**

*"The certificate is a technicality; the document speaks for itself."* The answer is that an electronic copy cannot speak for itself, because nothing on its face shows whether it matches its source. The certificate and the hash value are how that is shown, and the Supreme Court has held the requirement to be a rational safeguard and not an arbitrary burden.

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

PART II

# The Technology

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

CHAPTER 7

# Hash values without the mathematics

The Schedule asks for one technical thing that lawyers and police officers did not have to produce before 2024: the hash value of the record, the algorithm used, and a hash report. This chapter explains what a hash value is, what it proves, how to compute one on any common computer, and how to answer the objections you will meet. No mathematics is needed.

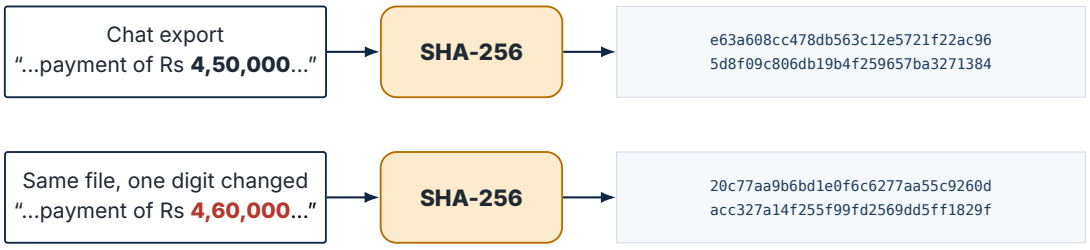
## 7.1 What a hash value is

A hash function is a fixed procedure that reads a file from its first byte to its last and produces a short string of characters. For the SHA-256 function the result is always 64 characters long, using the digits 0 to 9 and the letters a to f. That string is the hash value, also called the digest or checksum.

Four properties make it useful as evidence.

1. **Same input, same output.** The same file gives the same hash value on any computer, with any correct tool, today or in ten years.
2. **A change almost certainly produces a different output.** Change one character, one pixel or one bit, and the hash value changes completely and unpredictably. In strict theory two different files can share a value, because there are more possible files than possible values. For SHA-256 the chance is so remote that no such pair has ever been found.
3. **One-way.** The file cannot be reconstructed from its hash value, so disclosing the hash does not reveal the contents. One caution: where the content is short or guessable, such as a phone number or one of a handful of known documents, a person can hash each candidate and see which one matches.
4. **Collisions are computationally infeasible to find.** With a sound hash function, no practical method exists for finding two different files with the same hash value.

The Explanation to Section 3(2) of the IT Act describes a hash function in these terms, and the Supreme Court in 2026 called the hash value an electronic fingerprint.




The two values in the figure are real. They were computed from a two-line sample chat file and from the same file with a single digit altered.

## 7.2 What a hash value proves, and what it does not

A matching hash value is, for every practical purpose, proof that **the file examined now is identical, bit for bit, to the file that was hashed then**. That holds only if the reference value is itself reliable: correctly computed, correctly recorded, and kept where it could not be quietly

replaced. That is all a hash shows, and it is a great deal. It lets a court confirm in a few seconds that the pen drive on the record holds exactly what the certificate describes.

A hash value does **not** prove:

- that the file was genuine when it was hashed;
- who created the file, or on what device;
- that the events shown in the file happened;
- that the file is the same as some *other* file that was never hashed, such as the original message on the sender's phone.

This is why the moment of hashing matters. A hash taken at seizure, on the spot, covers everything that happens afterwards. A hash taken on the day of filing covers nothing before that day.

> **Key point: the hash depends only on the contents**
>
> The hash value of a file depends on its contents and nothing else. Renaming a file does not change its hash. Copying it to another disk does not change its hash. Changing its "date modified" does not change its hash. Opening and re-saving it in an application usually **does**, because the application rewrites the contents.

The sample chat file was copied and renamed for this book, and the hash was unchanged:

```
$ sha256sum "WhatsApp Chat with Vikram Shah.txt" /tmp/renamed-exhibit-P3.txt
e63a608cc478db563c12e5721f22ac965d8f09c806db19b4f259657ba3271384  WhatsApp Chat with Vikram Shah.txt
e63a608cc478db563c12e5721f22ac965d8f09c806db19b4f259657ba3271384  /tmp/renamed-exhibit-P3.txt
```

## 7.3 MD5, SHA-1 and SHA-256

The Schedule offers four choices of algorithm: SHA1, SHA256, MD5, and "Other", which must be a legally acceptable standard. They differ in length and in strength.

| Algorithm | Length of value | Status | Use in a certificate |
|---|---|---|---|
| MD5 | 32 characters | Collisions have been constructed since 2004. Two different files with the same MD5 value can be manufactured deliberately | Permitted by the Schedule. Avoid as the only algorithm |
| SHA-1 | 40 characters | A practical collision was published in 2017. Standards bodies are retiring it | Permitted by the Schedule. Avoid as the only algorithm |
| SHA-256 | 64 characters | Part of the SHA-2 family in the United States federal standard FIPS 180-4. No practical attack is known | Recommended |

The same sample file gives three different values under the three algorithms:

```
$ md5sum    "WhatsApp Chat with Vikram Shah.txt"
1abeab8e70be295d55874bf16c56c9ee  WhatsApp Chat with Vikram Shah.txt
$ sha1sum   "WhatsApp Chat with Vikram Shah.txt"
5f6335a921eba2be5740996ee6ea1226c4af0b2c  WhatsApp Chat with Vikram Shah.txt
```

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

```
$ sha256sum "WhatsApp Chat with Vikram Shah.txt"
e63a608cc478db563c12e5721f22ac965d8f09c806db19b4f259657ba3271384  WhatsApp Chat with Vikram Shah.txt
```

**Use SHA-256.** It is on the Schedule's list, every operating system can compute it without extra software, and no practical collision attack on it is known, which is the strongest answer available to a collision objection. No hash function carries an absolute mathematical guarantee; the claim is practical infeasibility.

**Why MD5 and SHA-1 are still seen.** Older forensic tools and many laboratory reports print MD5 or SHA-1 by default, often both. A report showing an MD5 value is not worthless. The known weaknesses allow someone to *construct two files in advance* that share a value. They do not allow someone to take an existing file and produce a different file with the same value; no practical method of doing that is known for either algorithm. But a certificate should not invite the argument. Where an existing report uses MD5 or SHA-1, compute SHA-256 as well and give both.

**"Other (legally acceptable standard)".** SHA-384, SHA-512 and the SHA-3 family are sound. If you use one, tick "Other", name it exactly, and be ready to explain why. There is rarely a reason to depart from SHA-256.

## 7.4 Computing a hash value

The commands below are built into the operating system. Nothing has to be installed.

### Windows

Open Command Prompt and use `certutil`:

```
certutil -hashfile "C:\Evidence\WhatsApp Chat with Vikram Shah.txt" SHA256
```

The tool prints a line naming the algorithm and the file, the hash value on the next line, and a completion message. Or open PowerShell and use `Get-FileHash`, which defaults to SHA-256:

```
Get-FileHash -Algorithm SHA256 "C:\Evidence\WhatsApp Chat with Vikram Shah.txt" | Format-List
```

PowerShell prints the algorithm, the hash in capital letters, and the path. Capital and small letters are equivalent in a hash value; `E63A...` and `e63a...` are the same value. To hash every file in a folder and save the result:

```
Get-ChildItem "C:\Evidence" -File -Recurse | Get-FileHash -Algorithm SHA256 |
  Export-Csv "C:\Evidence-hashes.csv" -NoTypeInformation
```

### macOS

Open Terminal:

```
shasum -a 256 "WhatsApp Chat with Vikram Shah.txt"
```

### Linux

```
$ sha256sum "WhatsApp Chat with Vikram Shah.txt"
e63a608cc478db563c12e5721f22ac965d8f09c806db19b4f259657ba3271384  WhatsApp Chat with Vikram Shah.txt
```

To hash a set of files into a manifest, and later verify every file against it:

```
$ sha256sum IMG_20260118_0*.jpg > photos.sha256
$ cat photos.sha256
f27d1ff548d21a4da2b56a4ba01e5a4f8dcbca02847cbdebcd35c0d9be923980  IMG_20260118_01.jpg
4648b34d852068f93547735e416ff2ffaa9c3949ba76b08951f13fc5066ffbcb  IMG_20260118_02.jpg
bd7b0e157c3e218f371b88f77c9b7e916521f8c11d4084c76b0007a5be366951  IMG_20260118_03.jpg
$ sha256sum -c photos.sha256
IMG_20260118_01.jpg: OK
IMG_20260118_02.jpg: OK
IMG_20260118_03.jpg: OK
```

If a single byte is added to one photograph, verification reports exactly which file changed:

```
$ sha256sum -c photos.sha256
IMG_20260118_01.jpg: OK
IMG_20260118_02.jpg: FAILED
IMG_20260118_03.jpg: OK
sha256sum: WARNING: 1 computed checksum did NOT match
```

> **Note: what a hash command does and does not tell you**
>
> **You need:** read access to the file, ideally on a copy, and a computer whose clock is correct, since you will record the time. **You get:** one value per file. **It tells you:** the value of that file at that moment, for later comparison. **It does not tell you:** where the file came from, whether it is complete, or whether it was altered before the command was run.

## Mobile phones

Android and iOS have no built-in command for this that an ordinary user can reach. There are three sound approaches.

- Transfer the file to a computer by cable, without passing it through a messaging app, and hash it there. Record that you did so.
- Use a file-hashing app on the phone. Record the app's name and version in the hash report, and confirm the value on a computer when you can.
- For a full extraction, the forensic tool that performs it computes the hashes and prints them in its report.

## Cross-checking with a second tool

A careful practitioner computes the value with two independent tools and confirms that they agree. On Linux, for example, `sha256sum`, `openssl` and a two-line Python script gave the same value for the sample bank-statement file:

```
$ sha256sum statement_0126.csv
c95c1e33907ad746e5eb437bc78a8c002b2848a9f829a5dbe7476a08077c395f  statement_0126.csv
$ openssl dgst -sha256 statement_0126.csv
SHA2-256(statement_0126.csv)= c95c1e33907ad746e5eb437bc78a8c002b2848a9f829a5dbe7476a08077c395f
```

Agreement between tools is the simplest answer to a suggestion that the tool was faulty.

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

> **Caution: do not use online hash calculators**
>
> Websites that offer to compute a hash require you to upload the file, or run code you cannot inspect. Uploading evidence to a third-party site breaks confidentiality, may breach data-protection duties, and gives the other side a custody argument. Use the built-in tools.

## 7.5 The hash report

The Schedule says a hash report is to be enclosed. It does not prescribe its form. A report that answers every question a court is likely to ask contains the following.

| Item | Example |
|---|---|
| Matter and exhibit reference | Commercial Suit No. 412 of 2026; Document P-7 |
| File name, as tendered | `WhatsApp Chat with Vikram Shah.txt` |
| File size in bytes | 181 |
| Algorithm | SHA-256 |
| Hash value | the full value, typed and not handwritten |
| Tool and version | `sha256sum` (GNU coreutils) 9.4 |
| Computer used | Make, model and operating system |
| Date and time, IST, 24-hour | 12/03/2026 19:05 |
| Person who computed it | Name, designation, signature |
| Source | Exported from the WhatsApp application on the declarant's phone described in Part A |
| Verification | Re-computed on 14/03/2026 10:20 by the Part B expert; values match |

For many files, the report is a table with one row per file, or a printed manifest such as the `photos.sha256` listing above, signed on each page. Appendix C gives a specimen.

## 7.6 Answering objections about the hash

| Objection | Answer |
|---|---|
| "The hash value in the certificate does not match the file on record." | This is serious and usually fatal to that file until explained. First check for clerical error: a mistyped character, the hash of a different file, or a file re-saved after hashing. If the file really differs, it is not the file that was certified |
| "The hash only shows the file has not changed since the certificate; it could have been fabricated before." | Correct, and it should be conceded. Answer with evidence of origin: the device, the extraction, the witness, metadata and corroboration |
| "MD5 is broken." | If SHA-256 was also given, the point falls away. If not, explain the difference between constructing a colliding pair in advance and forging a match to an existing file, and offer a fresh SHA-256 of the same file |
| "Part A and Part B show different values." | They must be identical. If they differ, the two signatories examined different files, or one made a copying error. Correct by a fresh certificate; do not alter the old one |

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

| Objection | Answer |
|---|---|
| “The hash was computed by the advocate’s office, not by the party.” | Nothing in the Schedule says who must operate the tool. The declarant states the value and encloses the report. The report should name the person who computed it, and that person can be called |
| “The tool is unreliable.” | Show the same value from a second tool, or compute it in court |

### In practice

- Use SHA-256, and tick only that box unless you are also giving a legacy value.
- Hash at the earliest possible moment, and record the date and time in IST.
- Type hash values or paste them; never copy them by hand. Then have a second person read the value back against the screen.
- Re-compute the hash immediately before every filing and compare it with the certificate.
- Keep the hash report as a signed document in its own right.

### If challenged

*“A hash value is technical opinion and needs an expert to prove it.”* Computing a hash is a mechanical operation that any person can repeat with a built-in command and that always gives the same answer. The Schedule requires the party to state it in Part A and the expert to state it in Part B. If its correctness is doubted, the simplest course is to re-compute it before the court.

© 2026 Gnu IT Solutions & Services Pvt. Ltd. · Free sample · Full book at gnugroup.org/books

# Continue with the full book

You have read why the certificate exists and how the hash value at its centre works. The full book takes you through the rest of the job.

| If you need to | The full book gives you |
|---|---|
| Know exactly what Section 63 requires | A clause-by-clause reading of the section and the Schedule, and the provisions around it |
| Understand the 2026 Supreme Court order | A chapter on *Pune Bar Association v. Union of India*: what it decides and what it leaves open |
| Decide what to do where the law is unsettled | Twelve open questions, each with the competing views and a safe practice |
| Complete the certificate | Part A and Part B field by field, and six worked specimens with real hash values |
| Avoid the common mistakes | Twelve defects that sink certificates, and a one-page pre-filing check |
| Do your own part well | Separate playbooks for lawyers, police and investigators, forensic experts, and organisations |
| Get it done tomorrow | A complete manual workflow with free tools, worksheets, checklists and three model drafts |

**Section 63 in Practice: Proving Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023**
122 pages · PDF · Law stated as on 14 November 2026

Available at **gnugroup.org/books**

Free practice-based learning on electronic evidence: legal.gnugroup.org