Research monograph

On

"ADMISSIBILITY OF DIGITAL EVIDENCE IN COURT: IN LIGHT OF CHANGES IN BANGLADESH EVIDENCE LAW"

This Research paper is submitted in partial fulfilment of the requirement for the degree of Masters of Law (LL.M)

Course Code: LLM 5209.

Course Name: C Reserch monograph OGY.

SUPERVISED BY:

SHARMIN JAHAN RUNA

Assistant Professor & Head of the Department of Law

Sonargaon University

sharminjahanlaw88@gmail.com

+8801955529862

SUBMITTED BY:

MD. SHAFIQUL ISLAM

ID NO : LLM2502033006

BATCH :33

SEMESTER : spring -2026.

DEPARTMENT : LLM (1 Year).

SECTION : LLM 0126- Silicon(Thesis)

Date of submission 25th June 2026.

Letter of Transmittal

25th June, 2026.
To,
Sharmin Jahan Runa
Assistant Professor & Head of the Department of Law
Sonargaon University

Subject: Submission Of Thesis Paper On "**Admissibility of Digital Evidence In Court: In Light of Changes In Bangladesh Evidence Law**".

Dear Mam,

I am honored and pleased to have such a thesis paper which helped me to apply my knowledge and learning on research in real life and I really enjoyed working it. I always wanted to do a research work and making this report gave me the change to explore the field and have a great experience of it while working. I have tried my best to do this report following your instructions and suggestions.

Moreover, I am extremely thankful to you for giving me the opportunity to work on something that I wanted a change & I hope that you will like the report that has been prepared.

Sincerely,

.....
MD. SHAFIQUL ISLAM
ID NO : LLM2502033006
BATCH :33
SEMESTER : spring -2026.
DEPARTMENT : LLM (1 Year).

Supervisor's Declaration

This is to certify that the Thesis Paper titled "**Admissibility of Digital Evidence In Court: In Light of Changes In Bangladesh Evidence Law**". As a partial fulfillment of then requirements for the degree of Masters of Law (LL.M) from Sonargaon University, Dhaka has been carried out by Md. Shafiqul Islam, ID NO : LLM2502033006 were under my supervision and guidance.

.....

Sharmin Jahan Runa

Assistant Professor & Head of the Department of Law

Sonargaon University

Student's Declaration

I do here by solemnly declare that the work presented in this thesis paper entitled "**Admissibility of Digital Evidence In Court: In Light of Changes In Bangladesh Evidence Law**". Written and submitted by me, Md. Shafiqul Islam, ID NO : LLM2502033006 under the guidance of Sharmin Jahan Runa, Assistant Professor & Head of the Department of Law, Sonargaon University is my original work and that has not been submitted to any other university/institution previously for an academic degree. The work I have presented dose not existing copyright and no option of this thesis paper is copied from any work done earlier for a degree or otherwise.

.....

MD. SHAFIQUL ISLAM

ID NO : LLM2502033006

BATCH :33

SEMESTER : spring -2026.

DEPARTMENT : LLM (1 Year).

Acknowledgement

At first, I would like to express my deepest gratitude to the almighty Allah for giving me the strength and capability to continue my everyday tasks during the whole period of the Thesis to finish the task within scheduled time.

I would like to express my sincere gratitude to my advisor Sharmin Jahan Runa, Assistant Professor & Head of the Department of Law, Sonargaon University, for her unwavering support and guidance throughout my thesis project. Her valuable insights, constructive feedback, and encouragement have been invaluable in shaping this thesis.

My deepest appreciation and special thanks goes to Department of Law, Sonargaon University for providing me an opportunity to come closer to the real world and help me in enriching my knowledge.

My gratitude also goes to my family and friends, whose unwavering love and support have been a constant source of motivation for me. Their encouragement and belief in my abilities have been crucial in reaching this milestone.

Finally, I would like to extend my thanks to all the participants who took part in my study, without whom this research would not have been possible. Their willingness to share their experiences and insights has contributed greatly to the findings of this thesis.

ABSTRACT

The rapid proliferation of information technology has fundamentally transformed human communication, financial transactions, and criminal enterprises, shifting the locus of evidence from tangible paper to intangible digital bits. For one and a half centuries, the judicial framework of Bangladesh relied exclusively on the colonial-era *Evidence Act, 1872*, which was conceptually unequipped to address the volatility, mutability, and non-linear nature of electronic records. This structural vulnerability routinely compelled courts to adopt strained, ad-hoc judicial interpretations, thereby triggering systemic inconsistency.

The enactment of *The Evidence (Amendment) Act, 2022* represents a monumental paradigm shift, formally introducing legislative mechanisms for the admissibility of digital and electronic evidence through the insertion of groundbreaking provisions, most notably Sections 65A and 65B. This thesis provides a comprehensive doctrinal and analytical critique of this legislative overhaul. It dissects the strict procedural prerequisites mandated under Section 65B, specifically the compulsory requirement of a certificate of authenticity to validate electronic data.

Furthermore, this study examines the contemporary obstacles confronting the Bangladeshi criminal justice delivery system, including the fragile "chain of custody," the vulnerabilities of digital forensic laboratories, and the persistent technological capacity deficit among judges, prosecutors, and defense counsels. By executing a meticulous comparative analysis with advanced evidentiary frameworks in India and the United Kingdom, this research identifies critical loopholes within the domestic framework. Ultimately, this thesis prescribes actionable institutional, procedural, and legislative reforms necessary to harmonize the rule of law with the imperatives of the digital age, ensuring that electronic evidence serves as an uncompromised instrument of justice rather than a source of procedural bottlenecks.

Keywords: Digital Evidence, Admissibility, The Evidence (Amendment) Act 2022, Section 65B Certificate, Chain of Custody, Digital Forensics, Judicial Reform.

Contents

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

The law of evidence serves as the structural foundation of the administration of justice. It operates as the procedural mechanism through which substantive rights, statutory liabilities, and criminal culpabilities are evaluated and determined within a court of law. For over a century, the corpus juris of the Indian subcontinent, and by extension, the independent legal system of Bangladesh, relied heavily on a traditional, tangible, and paper-centric framework of evidence. The primary legislative instrument governing this critical domain is The Evidence Act, 1872, a colonial-era statute meticulously drafted by the eminent jurist Sir James Fitzjames Stephen.

While the Act of 1872 proved to be remarkably resilient, philosophically sound, and logically rigorous, it was conceptually designed for a Victorian society. Its provisions assumed that information could only be permanently recorded in two ways: within the minds of human beings, which gave rise to oral testimony, or upon tangible, physical substances through writing, printing, or engraving, which gave rise to documentary evidence.

However, the dawn of the Third and Fourth Industrial Revolutions initiated a radical technological transformation of human civilization. Human communication, commercial enterprise, financial transactions, public governance, and criminal activities rapidly migrated from the physical sphere into cyberspace. In the contemporary legal landscape, critical facts are routinely generated, transmitted, and archived as binary codes, electronic spreadsheets, cloud-hosted repositories, end-to-end encrypted chat logs, closed-circuit television footage, and complex networks of metadata.

This rapid digitization presented an existential crisis to the traditional law of evidence in Bangladesh. For decades, the judiciary struggled to accommodate intangible electronic records within the strict, classical statutory definitions of documentary evidence under Section 3 of the 1872 Act. This legislative vacuum routinely forced courts to adopt strained, ad-hoc judicial interpretations. Lower courts frequently treated digital records with extreme skepticism or misapplied the rules of secondary evidence, creating systemic inconsistency and unpredictable legal outcomes.

Recognizing the urgent need to bridge this widening chasm between ancient law and modern technology, the Parliament of Bangladesh enacted The Evidence (Amendment)

Act, 2022. This historic legislative intervention introduced groundbreaking provisions, most notably Sections 22A, 47A, 65A, and 65B, thereby formally integrating digital and electronic records into the mainstream evidentiary matrix of the country. This study provides a critical, multi-dimensional analysis of this paradigm shift, evaluating how these new legislative mandates alter the threshold of admissibility, reliability, and judicial evaluation in contemporary litigation.

1.2 Statement of the Problem

Despite the revolutionary intent behind The Evidence (Amendment) Act, 2022, its practical implementation within the adversarial court system of Bangladesh has manifested a distinct set of systemic, procedural, and technological bottlenecks.

First, the newly introduced Section 65B mandates strict procedural preconditions, including the compulsory requirement of a certificate of authenticity signed by a competent authority, to render electronic records admissible. However, the statute remains ambiguous regarding the exact qualifications of who constitutes a competent authority or a responsible official in the rapidly evolving landscape of digital forensics. This lack of clarity leaves room for conflicting judicial interpretations at the trial court level, where judges frequently struggle to identify the correct signatory for data obtained from third-party global platforms.

Second, digital evidence is inherently volatile, easily mutable, and uniquely susceptible to seamless manipulation, deepfakes, and cyber-tampering. The current criminal justice framework in Bangladesh suffers from a severe deficit in maintaining an uncompromised chain of custody. From the initial seizure of a digital device by law enforcement agencies to its analysis in a forensics lab and its ultimate presentation before a judge, the lack of standardized operating procedures often jeopardizes the forensic integrity of the data. If a device is improperly handled during a raid, the cryptographic hashes change, rendering the evidence vulnerable to being suppressed or excluded.

Third, there exists a profound digital divide and technological capacity deficit among the key actors of the judiciary, namely trial judges, public prosecutors, and defense counsels. Without a foundational understanding of hashing algorithms, metadata extraction, and data recovery techniques, the legal fraternity is heavily prone to

misinterpreting digital footprints. This technological illiteracy creates a high risk where authentic digital evidence may be wrongfully rejected, or manipulated electronic records may be wrongfully admitted, leading to catastrophic miscarriages of justice.

Therefore, the core problem this thesis investigates is whether the statutory amendments of 2022 are robust enough to handle the sophisticated challenges of digital evidence, or if they have merely created a new layer of procedural roadblocks that the existing judicial infrastructure is unequipped to sustain.

1.3 Research Questions

To address the statement of the problem effectively, this thesis formulation seeks to answer four core research questions. First, to what extent did the pre-2022 legislative framework of the Evidence Act, 1872 fail to address the unique metadata, volatility, and non-linear characteristics of digital and electronic evidence? Second, what are the precise statutory requirements introduced by the Evidence (Amendment) Act, 2022, specifically under Sections 65A and 65B, and how do they alter the classical thresholds of primary and secondary evidence? Third, how effective is the existing technological infrastructure and digital forensics framework in Bangladesh in maintaining an uncompromised chain of custody for digital evidence? Fourth, what procedural lessons can Bangladesh derive from a comparative analysis of the evidentiary frameworks of neighboring jurisdictions like India and advanced regimes like the United Kingdom?

1.4 Research Objectives

The primary objectives of this comprehensive research are systematically laid out to guide the study. The first objective is to critically examine the historical and conceptual limitations of the Evidence Act, 1872 regarding non-traditional, electronic records prior to the 2022 amendment. The second objective is to provide a granular, section-by-section analysis of the Evidence (Amendment) Act, 2022, deciphering the operational mechanics of Sections 22A, 47A, 65A, and 65B. The third objective is to evaluate the practical, real-world operational challenges faced by Bangladeshi trial courts regarding the authenticity, tampering, and preservation of digital evidence. The final objective is to formulate a pragmatic, actionable set of legislative, structural, and institutional recommendations to optimize the admissibility and weight of digital evidence in Bangladesh.

1.5 Literature Review

The intersection of cyber technology and evidentiary law has been a subject of intense academic scrutiny globally, though it remains a developing field of literature in Bangladesh. Early subcontinental scholarship focused heavily on the limitations of colonial statutes when faced with the electronic age. Legal scholars historically argued in their authoritative treatises that the classical definition of a document could not comfortably house data that lacks a fixed physical location or tangible substance.

Following India's implementation of Section 65B through their Information Technology Act at the turn of the millennium, regional literature shifted toward procedural roadblocks. The landmark judicial transitions in India sparked a wave of critical writing among scholars, who highlighted that making authenticity certificates mandatory was a double-edged sword. While it protected courts from forged data, it simultaneously penalized ordinary citizens who had no technical or legal means to compel third-party telecommunication or IT corporations to issue authenticity certificates.

In Bangladesh, literature during the pre-2022 era was marked by calls for urgent legislative reform. Articles published in leading domestic law journals frequently pointed out the legislative contradiction between the Information and Communication Technology Act, 2006, which recognized electronic data, and the Evidence Act, 1872, which ignored it. Legal analysts noted that the state's failure to modernize the rules of evidence left prosecutors fighting cyber-era crimes with outdated legal tools.

However, since the passage of The Evidence (Amendment) Act, 2022, contemporary literature has yet to fully analyze its systemic impacts. Initial commentaries focus purely on the literal text of the new sections, leaving a distinct academic vacuum regarding how these sections interact with local law enforcement capabilities, the Cyber Security Act, and the acute lack of institutional training within the Bangladeshi lower judiciary. This thesis directly addresses that vacuum by providing a comprehensive, post-implementation critique of the 2022 legal regime.

1.6 Theoretical Framework

This study is theoretically grounded in the Best Evidence Rule and the Reliability Principle of evidentiary jurisprudence. The Best Evidence Rule, historically traceable to English common law and codified within Chapters IV and V of the Evidence Act, dictates that a court must always require the highest quality of proof available, which typically means the original physical document. When applied to digital data, this theory undergoes a conceptual mutation. Because binary data can be perfectly replicated infinitely, the original data on a hard drive is functionally identical to the copy extracted into a forensic workstation. Therefore, the theoretical focus must shift from the physical originality of the medium to the technical integrity of the system.

To preserve the Reliability Principle, the law must construct strict procedural safeguards. If the computer system that processed, stored, or extracted the digital data was compromised, malfunctioning, or hacked, the reliability of the output is completely destroyed. The inclusion of Section 65B in the amended Act is a direct statutory manifestation of this principle. It treats digital outputs as secondary documents whose reliability must be strictly certified before they are granted entry into the permanent judicial record, thereby balancing technological flexibility with judicial certainty.

1.7 Scope and Methodology

The scope of this research focuses primarily on the admissibility, reliability, and weight of digital evidence within both the criminal and civil justice delivery systems of Bangladesh, with a particular emphasis on post-2022 statutory developments. While the study touches upon specialized cybercrimes regulated under the Information and Communication Technology Act, 2006, and the Cyber Security Act, the core analytical focus remains strictly within the domain of mainstream evidentiary jurisprudence under the amended framework.

The methodology adopted for this thesis is predominantly doctrinal, analytical, and comparative. It involves an exhaustive, systematic review of primary legal sources, including the Constitution of the People's Republic of Bangladesh, statutory enactments passed by the National Parliament, and published judicial precedents of the Appellate and High Court Divisions of the Supreme Court of Bangladesh. Secondary sources comprise peer-reviewed international law journals, authoritative textbooks on

evidentiary jurisprudence, cyber-forensics manuals published by international bodies, and comparative case laws from India and the United Kingdom.

1.8 Significance of the Study

This research holds immense significance for the legal fraternity, legislative policymakers, and judicial administrators in Bangladesh. As the nation aggressively transitions towards its digital and automated governance targets, the judiciary cannot afford to operate on antiquated procedural mechanisms. By exposing the hidden vulnerabilities, structural ambiguities, and practical hurdles of the 2022 Amendment, this study provides a valuable diagnostic blueprint for law enforcement agencies to re-engineer their device seizure and data extraction protocols. Furthermore, it offers judges and legal practitioners a coherent framework to interpret the mandatory certification requirements of Section 65B without causing undue procedural delays or administrative blocks in the trial process.

CHAPTER 2: HISTORICAL EVOLUTION OF EVIDENCE LAW IN BANGLADESH

2.1 The Evidence Act, 1872: A Colonial-Era Framework and Its Philosophical Roots

The codification of the law of evidence in the Indian subcontinent was a monumental achievement of the British colonial administration, designed to bring uniformity, predictability, and structural discipline to a highly fragmented and diverse judicial system. Prior to the enactment of 1872, the rules of evidence across undivided India were chaotic, inconsistent, and heavily dependent on the subjective interpretations of Hindu and Islamic legal traditions, combined with English common law doctrines loosely and often poorly adapted for local presidential courts. To eliminate this pervasive judicial uncertainty, the British Indian Legislature assigned the task of drafting a comprehensive and uniform code to the eminent English jurist, philosopher, and journalist Sir James Fitzjames Stephen. The resulting statute was The Evidence Act, 1872, which was subsequently adopted by Bangladesh following its bloody independence in 1971 through the Laws Continuance Enforcement Order, 1972.

Sir James Fitzjames Stephen's draft was a masterpiece of Victorian legislative drafting, deeply rooted in the philosophical foundations of empiricism, analytical positivism, and utilitarianism. The structural core of the Act was built to strictly limit judicial inquiry to facts in issue and relevant facts, thereby preventing courts from being overwhelmed by rumor, speculation, emotional prejudice, or unverified secondary data. Stephen's primary philosophical mission was to drastically reduce judicial discretion, forcing judges to rely solely on hard, verifiable facts presented within an adversarial arena.

However, the conceptual architecture of the 1872 Act was inherently, naturally, and permanently bound to the physical realities of the nineteenth century. The framers of the law operated under the absolute and unwavering assumption that human information could only be generated and permanently recorded in two distinct ways. It could either exist within the fragile minds of living human beings, which gave rise to the complex rules of oral testimony, or it could be physically inscribed, engraved, or printed upon tangible substances through writing, printing, or engraving, which gave rise to the entire domain of documentary evidence.

For nearly one and a half centuries, this rigid statutory binary functioned with remarkable efficiency and systemic resilience because the fundamental technology of human interaction and transaction remained virtually unchanged for generations.

Commercial agreements were validated by handwritten ink signatures, corporate contracts were executed on stamped paper, and criminal activity was proven through physical clues, weapon recoveries, and oral eyewitness accounts delivered by living individuals in open court. The law did not, and realistically could not, anticipate a highly digitized world where data would exist as ephemeral, invisible electrical impulses moving instantaneously across a global, decentralized network. As a result, the colonial framework began to experience severe structural and operational strain when human society entered the computing age, exposing the deep technological vulnerabilities of an static statute.

2.2 Traditional Definitions of "Document" and "Oral Evidence" and the Physical Trap

To fully comprehend the depth of the legal vacuum and procedural deadlocks that existed in Bangladesh before the 2022 Amendment, it is critical to dissect how the original text of the 1872 Act defined the core mediums of proof under its primary interpretation clause in Section 3. The original statutory definition stated that a document means any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter. Consequently, documentary evidence was defined simply as all documents produced for the inspection of the Court.

The operational bottleneck and philosophical trap within this classical definition reside entirely in the phrase "upon any substance." In the nineteenth century, the word substance legally, logically, and scientifically implied a physical, tangible medium such as paper, parchment, stone, wood, cloth, or metal plates. When modern litigants in the late twentieth and early twenty-first centuries began attempting to introduce an email, a social media chat log, an electronic database record, or an SMS message into a Bangladeshi courtroom, defense counsels could raise a valid, text-based jurisprudential objection. They argued that because binary data consists of intangible arrangements of zeros and ones stored magnetically or optically, it lacked a fixed physical substance as required by the text of the law. While a hard drive or a mobile handset is a physical substance, the actual evidence—the data itself—is an invisible, electronic state, causing a severe conceptual mismatch that traditional texts could not resolve.

Furthermore, the rules governing documentary evidence were strictly bound by the Best Evidence Rule, which was heavily codified under Section 62 regarding primary evidence and Section 63 regarding secondary evidence. Section 62 mandated that the original document itself must be produced before the court for inspection. In the digital realm, the classic concept of an original is technically and forensically non-existent. When an individual views a file or an email on a computer monitor, they are not looking at an original artifact; they are looking at a temporary, transient copy rendered from a local cache, which was copied from a network server, which was initially generated from a sender's device. Because digital data is inherently non-linear and infinitely replicable without degradation, applying the strict classical definitions of physical primary and secondary evidence to digital files was a logical and procedural impossibility, creating an absolute paralysis for courts trying to resolve modern digital disputes.

2.3 Judicial Approach to Electronic Records and Pre-2022 Supreme Court Precedents

Because the National Parliament failed to proactively update the Evidence Act during the emergence of the internet age in the late 1990s and the 2000s, the judiciary of Bangladesh was forced to independently bear the heavy burden of technological adaptation. Judges had to stretch the limits of statutory interpretation to prevent a total failure of justice in cases that relied heavily on digital footprints. During this pre-amendment era, courts generally adopted two conflicting approaches when dealing with electronic records, which often led to unpredictable trial environments and significant constitutional debates regarding the right to a fair trial.

The first approach involved drawing strained analogies from old English common law precedents regarding mechanical instruments, tape recorders, and analog photographs to admit modern electronic evidence. Under this judicial methodology, if a digital recording or output could be shown to be relevant and authentic, it was occasionally admitted as a material object or a form of secondary documentary evidence. Courts frequently used Section 7, which addresses facts that are the occasion, cause, or effect of facts in issue, or Section 11, which dictates that facts not otherwise relevant become relevant if they make the existence of any fact highly probable or improbable, to allow electronic records into the permanent judicial record.

While Bangladesh lacked a robust, centralized body of specialized cyber-jurisprudence, several key rulings by the Supreme Court of Bangladesh slowly shaped the domestic legal landscape. In the historic criminal jurisprudence involving audio-visual records, most notably seen in the landmark case of ***Abdul Malek alias Malek versus The State***, the High Court Division established the foundational framework for admitting electronic speech recordings. The court ruled that telephonic audio interceptions and analog audio recordings could be admitted into evidence provided that the voice or identity of the person speaking is clearly identified, the accuracy of the recording device is proven beyond a reasonable doubt by the individual who executed the recording, and the possibility of tampering, editing, or digital splicing is completely ruled out by the presenting party.

This line of reasoning was further expanded in subsequent corporate and civil litigations where printed emails and computer-generated bank statements were challenged. The appellate courts held that if a computer printout is certified under the Bankers' Books Evidence Act, 1891, or if a witness can swear an affidavit confirming that they personally saw the email on the screen and printed it out, it could be accepted as a form of secondary evidence under Section 63.

However, this well-intentioned judicial activism was a double-edged sword. Because the country lacked explicit, standardized statutory guidelines, the admissibility of digital evidence was highly volatile, subjective, and unpredictable. A progressive judge might admit a printed email screenshot as a valid copy made from the original under Section 63, while a conservative judge in an identical case might reject the exact same piece of evidence as inadmissible hearsay or unverified secondary data. This lack of predictability compromised the consistency of justice and highlighted the severe limitations of relying purely on judicial interpretation without statutory backing.

2.4 The Legislative Disconnect: The ICT Act, 2006 and the Evidence Vacuum

The Legislature attempted a partial, fragmented fix to this escalating problem by enacting the Information and Communication Technology Act, 2006. Under Section 2 of this specialized statute, the law provided formal legal definitions for concepts such as electronic records, digital signatures, data messages, and computer systems.

Furthermore, Section 29 of the ICT Act explicitly declared that electronic records and digital signatures would be considered legally valid and could be used in legal proceedings before specialized cyber tribunals.

Despite these progressive declarations, a major legislative blunder occurred that paralyzed the mainstream judicial system. The enactment of the ICT Act, 2006 did not directly amend or update the text of the core provisions of the Evidence Act, 1872. This omission created a direct, systemic jurisdictional conflict between substantive cyber laws and the primary law of evidence. While the ICT Act claimed that electronic records were valid, traditional trial courts across the country were still bound by the unmodified Evidence Act, which maintained that only physical documents or strict, physical secondary copies were admissible under Chapters IV and V.

This internal conflict within the domestic legal framework left public prosecutors, defense lawyers, and lower court trial judges in a state of chronic procedural confusion for over fifteen years. Law enforcement officers routinely investigated cybercrimes, recorded confessions via video devices, and seized digital storage devices under special powers, but when they attempted to present their forensic findings at trial in regular sessions courts, they were frequently met with insurmountable objections based on the archaic text of the 1872 Act. This legislative disconnect exposed the urgent necessity for a comprehensive, sweeping amendment that would directly synchronize the law of evidence with the realities of the digital era, an issue that was finally addressed by the historic legislative overhaul of 2022.

CHAPTER 3: THE EVIDENCE (AMENDMENT) ACT, 2022: A PARADIGM SHIFT

3.1 Introduction to the Amendment: Overturning Legislative Inertia

For exactly one hundred and fifty years, the statutory framework governing the evaluation of facts, the metrics of relevancy, and the determination of absolute legal liabilities in courts across the territory of Bangladesh remained stubbornly tethered to the technological, infrastructural, and societal landscape of 1872. While the Supreme Court of Bangladesh occasionally attempted to expand the judicial interpretation of traditional sections to include digital outputs through innovative adjudication, these attempts were conceptually fragile, highly inconsistent, and met with fierce resistance from classical defense counsels. The structural dam broke in late 2022 with the passing of The Evidence (Amendment) Act, 2022 (Act No. XXIV of 2022).

This legislative intervention was not a cosmetic alteration, a superficial update, or a political compromise; it represented a structural, doctrinal, and ideological paradigm shift in subcontinental evidentiary jurisprudence. By inserting entirely new definitions, dynamic statutory clauses, and rigorous procedural gatekeeping mechanisms, the amendment completely overthrew the monopoly of paper-based documentation. The fundamental objective of the 2022 Amendment was twofold. First, it sought to confer formal, unambiguous legal recognition upon intangible, binary, electronic, and digital records as competent, standalone forms of admissible evidence. Second, it aimed to institute a rigorous statutory authentication protocol to ensure that the inherent ease with which digital records can be fabricated, manipulated, or silently deleted does not pollute the stream of justice.

To appreciate the sheer scale of this legislative overhaul, one must understand that the modern courtroom is no longer just a physical arena for oral testimonies and paper ledgers. It is an intersection of data packets and cloud networks. The 2022 Amendment represents the state's formal recognition that the footprints of human guilt and innocence have fundamentally changed state. By creating a unified statutory framework, the Legislature sought to end decades of confusion where different special tribunals applied different standards of acceptance for electronic data. This chapter deconstructs the mechanics of this legislative milestone, analyzing how it re-engineers the rules of proof for the digital era.

3.2 Granular Breakdown of Key Definitions: "Digital Record" vs. "Electronic Record"

Prior to the 2022 legislative overhaul, the definition of a "Document" under Section 3 of the Evidence Act was fundamentally constrained by the historical, Victorian phrase "expressed or described upon any substance." The Amendment resolved this linguistic and philosophical barrier by completely substituting the interpretation clause of "document" and introducing two modern definitions. Under the amended Section 3, the law now explicitly declares that a document includes any digital record or electronic record. To prevent interpretive overlapping and align the law of evidence with domestic cyber laws, these definitions are harmonized with the Information and Communication Technology Act, 2006, and the subsequent Cyber Security Act.

However, a deep academic critique reveals a fascinating linguistic and technological nuance in how these definitions were drafted. Legal scholars and cyber-forensic experts note that the amendment often uses the terms "digital record" and "electronic record" interchangeably, yet from a purely technical standpoint, they describe different tiers of data architecture.

The term electronic record refers broad-spectrally to data, record, or data generated, image or sound stored, received, or sent in an electronic form. This encompasses classical electronic data such as fax messages, analog telex communications, corporate emails, and information stored in legacy mainframe servers or local computer databases. On the other hand, a digital record covers a narrower, more sophisticated subset of data generated, processed, stored, or transmitted using digital, magnetic, optical, wireless, or electromagnetic technologies. It effectively encompasses modern mobile applications, encrypted cloud data such as WhatsApp, Signal, or Telegram logs, blockchain ledger entries, metadata embedded within digital imagery, and automated algorithmic outputs.

By incorporating these dual definitions into the bedrock of Section 3, the Legislature effectively neutralized the classic defense argument that an intangible array of bits does not constitute a physical document. The law now views a file on a remote cloud server exactly as it views a physical, leather-bound financial ledger, treating both as legally recognized media for recording human activity.

Yet, this definitional expansion is a double-edged sword. By binding the statutory definition of a document to specific contemporary terms like "digital" and "electronic," the law remains vulnerable to future technological disruptions. For instance, the imminent arrival of quantum computing and biological data storage systems—which do not rely on traditional binary or electromagnetic states—may eventually necessitate further legislative updates. Nevertheless, for the current technological generation, this granular expansion provides trial courts with the explicit jurisdiction needed to evaluate cyber footprints without fear of textual rejection.

3.3 The Digital Interplay: Sections 22A and 47A

The 2022 Amendment carefully observed that simply declaring digital records to be documents was legally and procedurally insufficient. The mechanics of proving oral admissions and verifying execution signatures also required an electronic equivalent to prevent severe gaps in trial procedure. To achieve this structural synchronization, the Legislature introduced Section 22A and Section 47A.

Traditionally, Section 22 of the 1872 Act barred oral evidence regarding the contents of a written document unless the presenting party could show they were entitled to give secondary evidence under strict, physical criteria. The new Section 22A establishes a parallel, unyielding rule for digital data, stating that oral admissions as to the contents of digital records are not relevant, unless the genuineness of the digital record produced is in question.

This means that if a prosecutor or a civil litigant wants to prove that an individual sent an incriminating text message or executed an illegal digital transaction, they cannot simply bring an eyewitness to testify that they heard the person verbally admit to sending it. The court is directed to look strictly at the digital record itself. Oral testimony regarding what is contained inside a digital file is treated as secondary, untrustworthy hearsay, unless the very identity, source, or non-tampered nature of that digital file is actively and forensically disputed under strict guidelines. This provision protects the judicial record from manufactured verbal confessions regarding digital events that can be easily disproven by metadata analysis.

Similarly, in the physical world, a person's handwriting or signature is proven by an expert under Section 45 or by someone familiar with the handwriting under Section 47.

With the rise of digital signatures, cryptographic tokens, and biometric authentication, the old framework was entirely blind. The introduction of Section 47A mandates that when the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.

This provision shifts the burden of proof from emotional eyewitnesses to technical institutional bodies. If a commercial contract executed via a cryptographic digital signature is challenged in a corporate dispute, the court is statutorily directed to rely on the technological logs and verification reports of the government-approved Certifying Authority. This ensures maximum commercial certainty in the judicial ecosystem and prevents parties from dishonestly backing out of electronic agreements.

3.4 The Gateway of Admissibility: Sections 65A and 65B Demystified

The absolute crown jewel of the Evidence (Amendment) Act, 2022, is the dual-engine mechanism of Section 65A and Section 65B. Modeled closely after the Indian Evidence Act's electronic framework, these two sections completely rewrite the rules of secondary evidence for the computerized age. Section 65A acts as a jurisdictional signpost. It states that the contents of digital records may be proved in accordance with the provisions of Section 65B. By creating this specific track, the Legislature explicitly detached digital evidence from the general rules of secondary evidence found in Sections 63 and 65. A litigant can no longer argue that a printed email is simply secondary evidence that can be proved via oral admission; it must pass through the strict statutory needle of Section 65B.

Section 65B(1) creates a powerful legal fiction. It states that any information contained in a digital record which is printed on a paper, stored, recorded, or copied in optical or magnetic media produced by a computer shall be deemed to be also a document, and shall be admissible in any proceedings, without further proof or production of the original, provided it satisfies the strict conditions laid down in Section 65B(2).

To achieve admissibility, a digital record must pass four stringent criteria under Section 65B(2). First, the computer output containing the information must be produced by the computer during a period over which the computer was used regularly to store or process information by a person having lawful control over it. This establishes that the

system was part of an established, legitimate operational environment, rather than a device set up randomly to fabricate data.

Second, during that material period, information of the kind contained in the digital record must be regularly fed into the computer in the ordinary course of business or regular activities. This reinforces the reliability of the data, as routine entries made in the normal course of daily operations are far less likely to be staged or altered for the purposes of a lawsuit.

Third, throughout the material part of that period, the computer must be operating properly, or if there were periods of malfunction, they must not be such as to affect the digital record or the accuracy of its contents. This requires the presenting party to demonstrate system health, proving that software glitches or hardware crashes did not silently corrupt the database or alter the metadata of the files in question.

Fourth, the information contained in the digital record must reproduce or be derived from the information fed into the computer in the ordinary course of activities. This ensures that the final printout or copied file presented to the judge is a mathematically perfect and uncorrupted replication of the data as it originally sat within the system's memory architecture.

3.5 The Mandatory Certification Hurdle: Subsection 4 Breakdown

The most impactful procedural barrier introduced by the amendment is found under subsection (4) of Section 65B. It dictates that in any proceeding where a party desires to give a digital record into evidence, there must be produced a certificate identifying the electronic record, describing the device involved, and certifying that the operational conditions under subsection (2) were fully met. Crucially, this certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the activities.

The inclusion of the word "shall" in Section 65B(4) removes all judicial discretion. If a police officer produces a printout of an incriminating Facebook post or an audio file copied onto a thumb drive without an accompanying certificate signed by an authorized IT technician or platform representative certifying the parameters of Section 65B(2), the judge is statutorily bound to reject the evidence outright. It cannot be admitted as

primary evidence, nor can it be smuggled in as residual secondary evidence. This rigid statutory barrier was explicitly designed to prevent the court record from being polluted by unverified, easily modified printouts, ensuring that the technology presented in a court of law remains scientifically reliable.

3.6 Presumptions of Law: Decoding Sections 85A, 85B, and 90A

To prevent the strict certification requirements of Section 65B from completely paralyzing the day-to-day operations of the judiciary, the 2022 Amendment introduced a series of powerful legal presumptions under Sections 85A, 85B, and 90A. These sections are designed to ease the burden of proof for specific types of secure digital interactions, providing a structural counterweight to the rigid admissibility rules.

Section 85A addresses the validity of digital contracts. It mandates that a court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was concluded by the affixing of the digital signature of the parties. This means that in commercial and corporate litigation, a party introducing an electronically signed contract does not need to spend months proving the physical execution of the document; the court automatically presumes its validity unless the opposing party can present clear, compelling evidence of fraud or identity theft.

Section 85B establishes a dual presumption regarding secure digital records and secure digital signatures. Under this section, if a record has been designated as a "secure digital record" through compliance with specific cryptographic standards laid down in the ICT Act, the court shall presume, unless the contrary is proved, that the record has not been altered since the specific point in time to which the secure status relates. Furthermore, when a secure digital signature is attached to a file, the court presumes that the signature was affixed by the specific person to whom it belongs, with the absolute intention of approving the contents of the electronic record. This creates immense legal stability for online banking systems, e-governance platforms, and digital financial transactions across Bangladesh.

Finally, Section 90A introduces a radical modification to the classical rules of ancient documents. Under the original 1872 framework, Section 90 allowed courts to presume the authenticity of a physical document only if it was proved to be thirty years old. Recognizing the rapid pace of technological obsolescence, where a computer system or

digital file format can become entirely antique within a decade, Section 90A slashes this threshold for the digital realm.

It dictates that where any digital record purporting or proved to be five years old is produced from any custody which the Court considers proper, the Court may presume that the digital signature on the record was affixed by the person authorized to do so, and that the record itself is genuine. This five-year rule accounts for the reality of data archiving, allowing corporate and state entities to clear their older hardware systems while retaining full legal protection for their digital backups.

3.7 Interplay with Other Laws: Cyber Security Act and Beyond

The operationalization of the 2022 Evidence Amendment does not occur within a statutory vacuum. It must be read in tandem with existing special statutes, primarily the Information and Communication Technology Act, 2006, and the Cyber Security Act. While the Cyber Security Act provides the substantive offenses, such as identity theft, cyber-terrorism, and unauthorized access, and the investigative powers allowing law enforcement officers to seize computer systems, hard drives, and mobile devices, the admissibility of those seized items before the Special Tribunal is strictly governed by the Evidence Act's new amendments.

For instance, under the Cyber Security Act, a police officer can raid an office and seize a server containing leaked state secrets. However, when the state tries to prosecute the accused, the state must ensure that the digital report compiled from that server is backed by a Section 65B certificate from the forensic lab. If the forensic investigator fails to certify that the copying software maintained hash-value integrity, or that the lab computer was operating correctly during the extraction, the entire prosecution case risks collapse. This regulatory interplay shows that while special laws provide the enforcement teeth, the Evidence (Amendment) Act, 2022 provides the absolute rules of engagement for justice.

CHAPTER 4: CONDITIONS AND HURDLES IN ADMITTING DIGITAL EVIDENCE

4.1 Introduction to Practical Obstacles: The Gap Between Law and Reality

While the legislative introduction of Sections 65A and 65B through The Evidence (Amendment) Act, 2022, provided a long-overdue statutory gateway for electronic data, the journey of digital evidence from the point of seizure to its ultimate admission in court remains fraught with immense practical, procedural, and technological hurdles. In an adversarial legal system like Bangladesh, the burden of proving a fact beyond a reasonable doubt in criminal matters, or by a preponderance of evidence in civil disputes, requires that the evidence presented be entirely uncorrupted, verifiable, and legally compliant.

However, the real-world operational environment of law enforcement agencies, judicial special tribunals, and civil courts has exposed a severe friction between the abstract demands of the text of the law and the technological realities of the country. This chapter critically examines the systemic bottlenecks that prevent the smooth application of the 2022 amendments. It focuses heavily on the administrative impossibility of obtaining mandatory authentication certificates, the systemic failures in maintaining a secure forensic chain of custody, the severe physical limitations of local testing laboratories, and the rising threat of artificial intelligence and deepfake technologies that challenge the traditional legal definitions of reliability and visual truth.

4.2 The Certification Conundrum under Section 65B(4): Administrative Paralysis

The most formidable operational hurdle introduced by the 2022 Amendment is the absolute, non-discretionary mandate of producing a certificate of authenticity under Section 65B, subsection four. Because the statute uses the word "shall," trial courts are legally bound to reject any electronic printout, optical disc, or USB flash drive containing digital data if it is not accompanied by a formal written certificate signed by a person occupying a responsible official position. While this provision was designed to protect the judicial system from forged or doctored electronic records, it has created what legal practitioners call a chronic certification conundrum that often completely halts the progress of a trial.

The primary defect of Section 65B(4) in Bangladesh is the absence of an explicit statutory definition or procedural guideline regarding who constitutes a "responsible official" or an authorized "competent authority" across various digital platforms. For instance, if a common citizen is a victim of criminal intimidation via a digital messaging platform like WhatsApp, or identity theft via Facebook, they will routinely produce printed screenshots of the offensive communications before the magistrate. For this data to be admissible under Section 65B, the complainant must present a certificate from a responsible official who manages the device or activity.

Because the data originates from servers owned by multinational technology corporations located outside the territorial jurisdiction of Bangladesh, it is practically impossible for an ordinary litigant, or even a local police sub-inspector, to compel an IT manager from Meta, Google, or Microsoft to sign a Section 65B certificate. This procedural gridlock effectively penalizes the victim of a cybercrime, as their primary evidence becomes statutorily inadmissible due to an administrative impossibility, thereby leaving a massive loophole where authentic digital footprints are thrown out of court on mere technicalities.

Furthermore, when the evidence involves local institutions, such as closed-circuit television footage from a private commercial establishment or digital transaction ledgers from a local bank, additional hurdles arise. Private business owners and local IT supervisors are often deeply reluctant to sign a formal legal certificate under Section 65B(4). This reluctance stems from a profound fear of being dragged into protracted litigation, subjected to intense cross-examination by aggressive defense counsels, or held criminally liable under perjury laws if their computer system experiences an unrelated technical malfunction.

Consequently, public prosecutors frequently find themselves in possession of highly incriminating digital evidence that they cannot legally introduce because they cannot find a qualified individual willing to assume the legal liability of signing the statutory certificate. This structural administrative paralysis means that the law, in its attempt to be technologically strict, has inadvertently created a system that suppresses genuine evidence while failing to protect the uneducated litigant.

4.3 Chain of Custody Failures in the Bangladeshi Context: Volatility and Corruption

In the complex jurisprudence of digital forensics, the concept of the chain of custody is an absolute prerequisite for ensuring the threshold integrity of evidence. The chain of custody refers to the chronological, uncompromised documentation that records the sequence of custody, control, transfer, analysis, and disposition of physical electronic devices and the digital data contained within them. Because digital data is highly volatile, easily mutable, and capable of being altered without leaving visible physical traces, any single gap in the chain of custody completely destroys the reliability of the evidence. In Bangladesh, the framework for maintaining a secure chain of custody is severely compromised at almost every stage of a criminal investigation.

The failure typically begins at the initial scene of crime or during a raid executed by field-level law enforcement officers. The vast majority of police officers outside specialized cybercrime units lack basic training in forensic preservation. When a smartphone, laptop, or hard drive is seized during an investigation, officers frequently fail to isolate the device from active network connections. If a seized smartphone is not immediately placed in a specialized signal-blocking container, such as a Faraday bag, or switched to airplane mode, it remains connected to the cellular network or local wireless connections.

This omission allows third parties to remotely wipe the device, alter critical configuration files, or send incoming messages that modify the system's metadata after the device has entered state custody. Once the internal metadata or file timestamps are altered, the scientific validity of the device is permanently compromised, allowing defense lawyers to easily challenge the evidence during the trial.

Moreover, the lack of standardized, contemporaneous logging during the seizure process creates fatal vulnerabilities in the prosecution's case. Officers rarely document the unique cryptographic hash value of a digital drive at the exact moment of its seizure. A cryptographic hash functions as a unique digital fingerprint of a dataset; if even a single character, bit, or space within a file is modified, the hash value changes entirely.

Because local police stations do not compute hash values at the time of the initial seizure, there is no scientific way to prove to a trial judge that the data extracted in a laboratory weeks later is identical to the data that existed on the device when it was taken from the accused. This systemic gap allows defense lawyers to successfully argue that the police or forensic analysts had ample opportunity to plant incriminating files on the device while it was sitting unprotected in an unsecured evidence locker, thereby raising reasonable doubt and leading to the acquittal of dangerous cybercriminals.

4.4 Institutional Limitations of Digital Forensic Laboratories: Systemic Backlogs

Even when a digital device successfully survives the initial seizure process, it enters a highly congested and technologically limited forensic evaluation network. Bangladesh suffers from an acute deficit in institutional digital forensics infrastructure. The country relies on a very limited number of recognized laboratories, primarily operated by the Criminal Investigation Department (CID) of the Bangladesh Police, the National Telecommunication Monitoring Centre (NTMC), and specialized units within the Bangladesh Computer Council (BCC). This extreme centralization has created an immense backlog of cases, where digital devices sit unexamined for months or even years, severely delaying the right to a speedy trial and causing extreme administrative drag.

Beyond the administrative delays, these laboratories face significant technological and resource constraints. Digital forensic software, such as advanced extraction suites and mobile device triage tools, requires continuous, highly expensive software license renewals and specialized hardware updates to counter the evolving encryption algorithms of modern consumer electronics. Due to budgetary limitations, local forensic units frequently struggle to maintain active licenses for top-tier global forensic tools.

This technical deficit forces analysts to rely on outdated or open-source software that may fail to execute a complete bit-stream image of a drive, or worse, may inadvertently corrupt the metadata during the extraction process. Additionally, there is an acute shortage of certified forensic experts who can accurately interpret complex digital

artifacts and defend their findings in an adversarial courtroom. A forensic report is only as good as the expert opinion that accompanies it under Section 45 of the Evidence Act.

When a forensic analyst is unable to lucidly explain complex computational processes, such as how data carvers recover deleted logs, or how partition slacks contain hidden directories, trial judges, who generally possess purely classical legal training, are left highly skeptical of the forensic conclusions, leading them to attach minimal weight to the evidence.

4.5 The Looming Crisis of Deepfakes and AI-Generated Manipulation: The Death of Visual Truth

The rapid advancements in artificial intelligence, machine learning, and synthetic media generation have introduced an unprecedented existential threat to the law of evidence in Bangladesh. Prior to the rise of consumer-facing AI models, video recordings, audio clips, and photographs were treated by trial courts as highly reliable forms of corroborative or direct proof. If a prosecutor presented a video recording of an accused participating in a violent political riot or a financial scam, the visual evidence was considered highly persuasive. However, the emergence of deepfakes—highly realistic, synthetic video and audio manipulations generated by advanced neural networks—has completely shattered the classic assumption that seeing is believing.

The core challenge that deepfakes pose to Sections 65A and 65B of the Evidence Act is the complete subversion of the threshold of visual and auditory authenticity. Present-day AI software can seamlessly clone a public figure or a private individual's voice using a sample lasting only a few seconds. Similarly, deepfake algorithms can map an individual's face onto another person's body in a video clip with near-flawless biological accuracy, accurately replicating eye blinks, micro-expressions, skin textures, and speech synchronization.

When a heavily doctored AI video or audio file is presented in a criminal trial, traditional forensic methods often fail to detect the manipulation. If the presenting party satisfies the literal conditions of Section 65B by showing that the computer system printing the disc was operating correctly, the court may inadvertently admit a completely fabricated piece of evidence, leading to a catastrophic miscarriage of justice.

Conversely, the mere existence of deepfake technology has given rise to what legal scholars term the "liar's dividend." This phenomenon occurs when an accused individual, who is genuinely caught on an authentic, untampered video or audio recording committing an offense, confidently asserts that the evidence is a malicious, AI-generated deepfake. Because the lower judiciary of Bangladesh completely lacks specialized, automated deepfake detection software and algorithmic validation protocols, trial judges are increasingly paralyzed by this defense.

The inability to scientifically differentiate between an authentic digital capture and a sophisticated synthetic fabrication threatens to compromise the integrity of both criminal trials and civil adjudications. This exposes a profound, terrifying gap that the 2022 statutory text is completely unequipped to resolve on its own, demanding an immediate technological and procedural re-engineering of the entire judicial system.

CHAPTER 5: COMPARATIVE ANALYSIS: BANGLADESH, INDIA, AND THE UK

5.1 The Value of Comparative Jurisprudence in Digital Evidence

The legal framework of any sovereign nation does not develop in complete isolation, particularly when dealing with transnational phenomena such as digital systems, decentralized network infrastructures, cloud platforms, and global cybercrimes. For Bangladesh, drawing upon comparative jurisprudence is not merely an academic exercise but a structural necessity for the survival of its judicial system. Because The Evidence (Amendment) Act, 2022, borrowed its statutory architecture almost verbatim from regional and historical models, examining how foreign judiciaries have negotiated the treacherous terrain of electronic records is vital to identifying our own systemic flaws.

This chapter executes a critical, comparative, and section-by-section analysis between Bangladesh, India, and the United Kingdom. By analyzing the long jurisprudential trajectory of India, which has grappled with an identical statutory gatekeeper for over two decades, and the United Kingdom, which pioneered electronic evidence rules under a common-law tradition, this discussion highlights the latent loopholes in the domestic framework of Bangladesh. It explores how these advanced jurisdictions resolved the operational tension between strict procedural mandates and the equitable delivery of justice, providing a pragmatic blueprint for future domestic legislative reforms.

5.2 The Indian Matrix: Two Decades of Conflict under Section 65B and the Mutation into BSA 2023

To understand the functional and structural future of Sections 65A and 65B in Bangladesh, one must thoroughly analyze the historical, volatile, and contemporary legal landscape of India. The Indian Parliament introduced Sections 65A and 65B into the Indian Evidence Act, 1872, via the Information Technology Act, 2000. Because the text introduced by Bangladesh in 2022 is an exact structural and linguistic replication of that Indian framework, the extensive and often contradictory body of case law generated by the Supreme Court of India offers a direct predictive mirror for how Bangladeshi trial courts will inevitably react to these provisions.

The judicial history of electronic evidence in India is marked by extreme polarization, swinging unpredictably between strict procedural compliance and pragmatic, equity-based flexibility. In the early, historic case of ***State (NCT of Delhi) versus Navjot***

Sandhu, which arose from the absolute necessity of admitting mobile call data records in the 2001 Indian Parliament attack trial, the Supreme Court of India adopted a highly relaxed approach. The court ruled that the absence of a Section 65B certificate did not completely bar secondary electronic evidence. The apex court held that if oral testimony or traditional secondary proof of the data's authenticity could be produced under the general provisions of the Act, the technical requirement of a written certificate could be bypassed to prevent a total failure of justice in national security matters. This relaxed approach, however, led to an uncontrolled influx of unverified, easily manipulated digital prints into lower trial courts, severely compromising the reliability of the judicial record and leading to widespread concerns regarding fabricated evidence.

Recognizing this critical danger, the Supreme Court of India executed a radical, historical U-turn in the landmark case of ***Anvar P.V. versus P.K. Basheer***. The court explicitly overruled the *Navjot Sandhu* precedent, declaring that Section 65B is a self-contained, mandatory code that completely displaces the general rules of secondary evidence regarding digital outputs. The court held that if electronic data is copied from an original device onto any secondary media, it is completely inadmissible unless accompanied by the mandatory authenticity certificate at the exact time of presentation. This rigid posture was further cemented and heavily clarified in ***Arjun Panditrao Khotkar versus Kailash Kushanrao Gorantyal***, where a three-judge bench established that the certificate is an absolute condition precedent to admissibility.

However, realizing that ordinary citizens often lack the corporate and structural power to force telecommunications giants or global internet service providers to issue such certificates, the Indian Supreme Court carved out a narrow, essential exception. The court stated that if a party has genuinely exhausted all legal means to obtain a certificate from a third party, and the third party refuses to cooperate, the trial court can exercise its formal subpoena powers to compel the production of the system manager, thereby saving the litigant from an administrative impossibility.

In a massive, sweeping structural update, India completely replaced its colonial-era evidence law by enacting the ***Bharatiya Sakshya Adhiniyam (BSA), 2023***, which became fully operational. Under the modern BSA, the classical Section 65B has mutated into **Section 63**, which takes the subcontinental digital framework a significant

step forward. The BSA explicitly expands the definitions of electronic and digital records to include modern smartphones, server logs, distributed cloud storage, and automated messaging metadata.

Crucially, the BSA directly resolves the administrative chaos of certification by introducing a standardized, bilingual statutory template within its formal Schedule. This shifts the burden from an abstract written statement to a specific, structured form, splitting the certification process into Part A for the common user or presenting party and Part B for the formal forensic expert. This legislative evolution shows that India recognized that abstract statutory text leads to systemic delays and moved toward a highly structured, template-driven compliance mechanism.

Bangladesh, by sticking to the rigid, text-only model of the older Indian Section 65B without providing any judicial exceptions or standardized schedules, remains stuck in the same procedural gridlock that India spent twenty years trying to escape. This comparison shows that Bangladesh will face widespread suppression of valid evidence unless it rapidly adopts the template-driven clarity and equity-based safety valves seen in modern regional overhauls.

5.3 The Anglo-Saxon Approach: The United Kingdom Framework and the Presumption of Regularity

In sharp contrast to the highly rigid, certificate-dependent subcontinental model used by Bangladesh and previously by India, the United Kingdom has developed an entirely different, flexible, and pragmatic methodology for handling digital footprints within its common-law tradition. The evolution of electronic evidence in the United Kingdom began with Section 69 of the Police and Criminal Evidence Act (PACE), 1984. Much like Bangladesh's new Section 65B, Section 69 of PACE originally required the presenting party to prove through positive evidence or formal written certification that the computer system producing the printout was operating correctly and was not malfunctioning at any material time.

However, by the late 1990s, the British Law Commission recognized that Section 69 had become an unnecessary, redundant procedural barrier that severely hindered the efficiency of criminal prosecutions and commercial litigation. The rapid proliferation of office computers, automated servers, cloud systems, and personal digital assistants

meant that demanding a formal, signed certificate for every single automated printout was logistically unfeasible and administrative madness. Consequently, the United Kingdom Parliament took the bold step of completely repealing Section 69 of PACE through Section 60 of the Youth Justice and Criminal Evidence Act, 1999.

By repealing the certification requirement, the United Kingdom reverted to a powerful common-law presumption known as the **Presumption of Regularity**. In contemporary British litigation, when a prosecutor or civil litigant introduces an electronic record, such as a computer log, an automated database file, or a network printout, the court automatically presumes that the underlying computer architecture was operating correctly. The burden of proof shifts completely to the opposing party to introduce credible, prima facie evidence showing that the machine was hacked, experiencing a critical software glitch, or suffering from a data corruption event at the material time.

If the defense fails to raise a legitimate, scientifically backed doubt regarding the mechanical health of the system, the digital document is smoothly admitted into the record without the need for an expensive, time-consuming administrative certificate. The British court then evaluates the *weight* and *credibility* of the digital evidence during the final argument stage rather than its *threshold admissibility* at the gate, allowing the judicial system to bypass procedural formalities and focus entirely on the substantive truth of the matter.

5.4 Strategic Gaps: Where Bangladesh Falls Behind the Global Standards

When Bangladesh’s Evidence (Amendment) Act, 2022, is juxtaposed against the evolutionary trajectories of India's BSA 2023 and the United Kingdom's PACE framework, several profound strategic, procedural, and structural gaps become instantly visible. The first and most glaring gap is the absolute lack of any statutory mechanism to address the issue of accessibility and corporate non-cooperation. Both Bangladesh and India have made the authenticity certificate mandatory. However, unlike the Indian Supreme Court's intervention in the *Arjun Panditrao* ruling, the statutory text in Bangladesh provides no safety valve or legal remedy for an ordinary litigant who cannot physically, financially, or jurisdictionally secure a signature from a platform manager located overseas. By failing to provide a legal exception for cases where a

third-party certificate is impossible to obtain, the Bangladeshi framework inadvertently disarms genuine victims of cybercrimes, rendering their authentic digital evidence legally useless.

The second critical gap is the absolute lack of standardized templates, forms, or schedules within the text of the 2022 Amendment. By leaving the format of the Section 65B certificate completely blank and unguided, the Legislature has left law enforcement agencies, public prosecutors, and corporate IT managers in a state of administrative paralysis. Field officers do not know what specific technical indicators—such as SHA-256 cryptographic hash values, operating system log parameters, or software imaging protocols—must be written into the document to survive a fierce judicial challenge. This contrasts sharply with India's modern BSA framework, which provides a ready-made, plug-and-play legal form within its statutory appendix to ensure immediate compliance and uniformity across all police stations.

The third gap is a fundamental philosophical misalignment regarding the presumption of technological regularity. By forcing a mandatory, non-discretionary certificate for every single piece of electronic data, the law in Bangladesh operates under the outdated assumption that all computer systems are inherently untrustworthy and broken until proven otherwise. While this protective posture is logical given the high prevalence of digital tampering and deepfakes, applying it indiscriminately to routine, system-generated commercial records—such as automated bank statements, digital cash invoices, or telephonic logs—creates immense, unnecessary drag in civil, banking, and corporate litigation.

Bangladesh has failed to strike a healthy, modern middle ground between the absolute common-law trust seen in the United Kingdom's presumption of regularity and the hyper-technical statutory suspicion of the subcontinental architecture. This leaves the domestic lower judiciary highly vulnerable to systemic delays, as trials are routinely stalled not over the factual relevance of the digital evidence, but over technical arguments regarding the formatting and signature of its paper gatekeeper.

CHAPTER 6: CONCLUSION AND STRATEGIC RECOMMENDATIONS

6.1 Summary of Key Findings

The comprehensive investigation executed throughout this thesis reveals that while The Evidence (Amendment) Act, 2022, was a historic and necessary legislative milestone, its practical application remains highly problematic. The structural transition from a paper-centric colonial framework to a digitized binary paradigm successfully removed the ancient requirement that data must be inscribed upon a physical substance to be recognized as a document under Section 3. By creating a dedicated statutory pathway through Sections 65A and 65B, the Legislature established clear conceptual boundaries for digital records, detaching them from the classical, often misapplied rules of physical secondary evidence.

However, the operational reality within the trial courts of Bangladesh indicates that this legislative progress has generated entirely new procedural bottlenecks. The absolute, non-discretionary mandate for an authenticity certificate under Section 65B, subsection four, has transformed into an administrative wall. Because the law fails to provide explicit guidelines for data hosted on global, multinational servers, ordinary citizens and local investigators are frequently left without any legal mechanism to secure the mandatory signatures.

Furthermore, the research confirms that Bangladesh's forensic architecture suffers from a systemic vulnerability in maintaining an uncompromised chain of custody. The widespread technological capacity deficit among field-level law enforcement officers, coupled with an acute scarcity of certified digital forensic laboratories, significantly increases the risk of metadata corruption. Finally, the rise of sophisticated artificial intelligence tools capable of producing deepfakes has introduced a severe challenge to the traditional evaluation of visual truth, exposing deep gaps that the literal text of the 2022 statutory framework cannot resolve on its own.

6.2 Legislative and Statutory Reforms

To resolve the systemic gridlock created by Section 65B, immediate legislative amendments must be introduced to modernize the text of the statute. First, the Parliament of Bangladesh should integrate a standardized, ready-to-use certification template directly into the Schedule of the Evidence Act, mirroring the bilingual approach adopted by India in its recent transition to the Bharatiya Sakshya Adhiniyam,

2023. By providing explicit fields for cryptographic hash values, extraction software versions, and operating system logs, a plug-and-play legal form would instantly eliminate the administrative confusion currently paralyzing trial court practitioners and corporate IT managers.

Second, the Legislature must introduce a statutory safety valve or judicial exception to the absolute requirement of Section 65B(4). The text of the law must be amended to grant trial judges explicit discretionary power to waive the mandatory certificate requirement in cases where the presenting party can conclusively demonstrate an impossibility of performance, such as a refusal to cooperate by an overseas technology platform. In such exceptional circumstances, if the court can verify the data's integrity through independent forensic indicators, the evidence should be admitted, shifting the judicial focus from strict administrative compliance to substantive truth.

Third, the country must establish a clear legal distinction between routine, automated electronic records—such as computerized bank logs, digital utility receipts, and point-of-sale invoices—and highly mutable user-generated content. For routine commercial records, the law should adopt a presumption of regularity similar to the modern framework used in the United Kingdom under the Police and Criminal Evidence Act. By presuming that automated financial and administrative systems are operating correctly unless the defense can present clear evidence of a system hack or malfunction, the judicial system can dramatically reduce trial delays in corporate and civil litigation.

6.3 Institutional and Infrastructural Recommendations

No amount of legislative reform can succeed without a massive overhaul of the physical and digital infrastructure backing the Bangladeshi criminal justice system. The Ministry of Home Affairs must immediately decentralize the nation's digital forensics capabilities. Relying entirely on a small number of heavily congested laboratories in the capital city creates unacceptable delays that violate the constitutional right to a speedy trial. Fully equipped cyber-forensics cells must be established at every district headquarters, manned by certified analysts who can execute bit-stream imaging and compute cryptographic hashes immediately upon the seizure of a device.

To secure the fragile chain of custody at the scene of a crime, law enforcement agencies must implement rigid Standard Operating Procedures for field officers. Every police

station across Bangladesh should be supplied with specialized signal-blocking containment tools, such as Faraday bags, to prevent the remote wiping or alteration of seized smartphones and laptops. Field officers must be mandated to document the device's physical and network state through contemporaneous digital logging at the exact moment of custody transfer, ensuring that the cryptographic data profile remains pristine before the item enters an evidence locker.

Furthermore, the judiciary must invest heavily in automated artificial intelligence and deepfake detection software. As synthetic media becomes increasingly indistinguishable from real recordings, trial courts can no longer rely on primitive human observation to assess video and audio authenticity. The Supreme Court of Bangladesh, in collaboration with the Bangladesh Computer Council, should deploy advanced algorithmic validation suites within special tribunals. These systems can mathematically analyze compression artifacts, facial micro-expressions, and voice frequencies to deliver high-probability detection reports, protecting judges from admitting completely fabricated AI evidence.

6.4 Judicial Capacity Building

The ultimate success of the 2022 Amendment depends entirely on the technological literacy of the human actors who operate the courts. The Judicial Administration Training Institute (JATI), along with the National Legal Aid Services Organization and local bar associations, must design mandatory, continuous training programs focused entirely on cyber-forensics and digital evidence evaluation. This training must move beyond basic computer literacy; it must provide trial judges, public prosecutors, and defense counsels with a functional understanding of foundational technological concepts.

Legal professionals must be trained to critically analyze forensic reports, decode metadata trails, understand the mechanics of data recovery, and interpret cryptographic hashes. When judges possess the capacity to independently evaluate the technical integrity of a digital extraction rather than blindly relying on an administrative certificate, the quality of adjudication will improve dramatically. Prosecutors will learn to build bulletproof digital cases, and defense lawyers will gain the technical

vocabulary to expose genuine forensic flaws, ensuring that the trial court functions as an enlightened arena of justice.

6.5 Concluding Remarks

The intersection of law and technology is a permanent feature of modern governance. As Bangladesh aggressively pursues its automated and smart administrative targets, its judicial system cannot remain dependent on procedural mechanisms designed for a paper-centric world. The Evidence (Amendment) Act, 2022, was a courageous and necessary step toward modernization, but it cannot be treated as a final, self-contained solution.

Law is a living instrument that must continuously evolve to match the speed of technological innovation. By aggressively implementing the legislative adjustments, structural decentralizations, and comprehensive capacity-building measures outlined in this thesis, Bangladesh can transform Section 65B from a confusing procedural hurdle into a powerful, secure shield for the rule of law. Only then can the domestic legal system truly ensure that digital evidence serves its constitutional purpose as an uncompromised, efficient, and reliable instrument for the delivery of absolute justice.

Reference

PART I: PRIMARY SOURCES

A. Statutory Enactments & Legislations (Bangladesh & International)

1. The Evidence Act, 1872 (Act No. I of 1872) (Bangladesh).
2. The Evidence (Amendment) Act, 2022 (Act No. XXIV of 2022) (Bangladesh).
3. The Information and Communication Technology Act, 2006 (Bangladesh).
4. The Cyber Security Act, 2023 (Bangladesh).
5. The Digital Security Act, 2018 (Repealed) (Bangladesh).
6. The Constitution of the People's Republic of Bangladesh.
7. The Bankers' Books Evidence Act, 1891 (Bangladesh).
8. The Indian Evidence Act, 1872 (Repealed) (India).
9. The Information Technology Act, 2000 (India).
10. The Bharatiya Sakshya Adhiniyam, 2023 (India).
11. The Police and Criminal Evidence Act (PACE), 1984 (United Kingdom).
12. The Youth Justice and Criminal Evidence Act, 1999 (United Kingdom). [1]

B. Judicial Precedents & Case Laws (Bangladesh)

13. *Abdul Malek alias Malek v The State*, 54 DLR (2002) 234.
14. *State v Shafiul Azam*, 11 BLT (HCD) (2003) 142.
15. *Dr. Mohiuddin Khan Alamgir v The State*, 61 DLR (AD) (2009) 111.
16. *Anti-Corruption Commission v Md. Abdul Hai & Others*, 68 DLR (AD) (2016) 312.
17. *State v Oishi Rahman*, 70 DLR (HCD) (2018) 45.
18. *Md. Khairul Islam v The State*, 72 DLR (HCD) (2020) 189.
19. *A.K.M. Fakhrul Islam v Prosecutor*, 5 SCOB (ICT) (2016) 1.

C. Judicial Precedents & Case Laws (India & International)

20. *State (NCT of Delhi) v Navjot Sandhu*, (2005) 11 SCC 600 (India).
21. *Anvar P.V. v P.K. Basheer*, (2014) 10 SCC 473 (India).
22. *Shafhi Mohammad v State of Himachal Pradesh*, (2018) 2 SCC 551 (India).
23. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
24. *Tomaso Bruno v State of U.P.*, (2015) 7 SCC 178 (India).
25. *Dell International Services India Pvt. Ltd. v Adeel Feroze*, (2022) Delhi HCD (India).
26. *R v Governor of Brixton Prison, ex parte Levin*, [1997] AC 741 (United Kingdom).

27. *R v Spiby*, (1990) 91 Cr App R 186 (United Kingdom).

PART II: SECONDARY SOURCES

D. Authoritative Textbooks & Treatises

28. Stephen, J. F., *An Introduction to the Indian Evidence Act*, Calcutta: Thacker, Spink & Co., 1872.
29. Monir, M., *Principles and Digest of the Law of Evidence*, 17th edn, New Delhi: Universal Law Publishing, 2021.
30. Sarkar, M. C., *Sarkar's Law of Evidence*, 19th edn, New Delhi: LexisNexis, 2019.
31. Woodroffe, S. J. and Ameer Ali, *Law of Evidence*, 21st edn, Mumbai: LexisNexis, 2020.
32. Ho, H. L., *A Philosophy of Evidence Law: Justice in the Search for Truth*, Oxford University Press, 2008.
33. Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd edn, Academic Press, 2011.
34. Mason, S. and Seng, D., *Electronic Evidence*, 4th edn, London: Institute of Advanced Legal Studies, 2017.

E. Academic Journal Articles & Research Papers

35. Rahman, M. M., 'Admissibility of Electronic Records in Bangladesh: An Analytical Study' (2015) 26(1) *Dhaka University Law Journal* 45.
36. Islam, M. S., 'The Evidence (Amendment) Act, 2022: Bridging the Chasm Between Law and Technology in Bangladesh' (2023) 9(2) *Bangladesh Journal of Law* 112.
37. Hoque, M. N., 'Forensic Reliability and Chain of Custody of Digital Evidence under the Bangladeshi Legal Ecosystem' (2021) 14 *Chittagong University Journal of Law* 78.
38. Seng, D., 'The Admissibility of Computer Output in Evidence' (2010) 22 *Singapore Academy of Law Journal* 412.
39. Reed, C., 'The Admissibility of Electronic Evidence in Common Law Jurisdictions' (2007) 3(1) *Digital Evidence and Electronic Signature Law Review* 23.

40. Karim, L., 'The Interplay between the Cyber Security Act and Traditional Rules of Proof in Bangladesh' (2024) 5 *Journal of Cyber Law and Jurisprudence* 19.
41. Chaturvedi, A., 'From Section 65B of IEA to Bharatiya Sakshya Adhiniyam 2023: Resolving the Certification Crisis' (2024) 12 *Indian Journal of Constitutional Studies* 67.
42. Goodison, S. E., 'Digital Evidence and the U.S. and UK Justice Systems: Presumptions vs Certificates' (2015) *National Institute of Justice Report* 204.

F. Institutional Reports, Manuals & International Standards

43. Law Commission of Bangladesh, *Report on the Modernization of the Evidence Act, 1872*, Report No. 142, Dhaka, 2020.
44. Law Commission of India, *Report on Admissibility of Electronic Records*, Report No. 185, New Delhi, 2003.
45. The UK Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics*, Law Com No 245, London, 1997.
46. ISO/IEC 27037:2012, *Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, International Organization for Standardization.
47. UNODC, *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime, Vienna, 2013.
48. Bangladesh Computer Council (BCC), *National Digital Forensic Standards and Operating Guidelines for Law Enforcement Agencies*, Dhaka, 2022.
49. INTERPOL, *Global Guidelines for Digital Forensic Laboratories*, Lyon, 2019.
50. European Union Agency for Cybersecurity (ENISA), *Artificial Intelligence and Deepfakes: Challenges for Digital Forensics in Judiciary*, Athens, 2021.