Research Monograph

On

"Admissibility and reliability of digital evidence in criminal trails: Challenges in the modern criminal procedure system."

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of L.L.B (Hon's), Department of Law, Sonargaon University (SU)

Submitted By

Md. Jahangir Alam

ID No: LLB2203027026

Department of Law

Faculty of Arts and Humanities

Sonargaon University (SU)

Supervised By

Sunzida Akter

Lecturer

Department of Law

Faculty of Arts and Humanities

Sonargaon University (SU)

Date of Submission: 25th June 2026

Letter of Transmittal

To,
Sunzida Akhter,
Lecturer,
Department of Law,
Faculty of Arts and Humanities,
Sonargaon University (SU).

Subject: **Submission of Research Monograph "Admissibility and reliability of digital evidence in criminal trails: Challenges in the modern criminal procedure system''.**

I am happy to submit my research monograph titled "admissibility and reliability of evidence in criminal trials: Challenges in the modern criminal procedure system". I worked hard to complete this research monograph with information that I collected from various primary and secondary sources. My goal was to achieve the objectives of the work. I hope it will serve its intended purpose. I will be grateful if you accept my thesis and evaluate it.

Sincerely,

Md. Jahangir Alam
ID No: LLB2203027026,
Department of Law,
Faculty of Arts and Humanities,
Sonargaon University (SU).

Declaration

I hereby do solemnly declare that the work presented in this research monograph titled "Admissibility and reliability of evidence in criminal trials: Challenges in the modern criminal procedure system" was done by me under the supervision of Sunzida Akhter, Lecturer, Department of Law, Faculty of Arts and Humanities, Sonargaon University and has not been previously submitted to any other institution. The work I, presented does not breach any copyright.

I further undertake to indemnify the university against any loss or damage arising from breach of the foregoing obligations.

Best regards

Md. Jahangir Alam,
ID No: LLB2203027026,
Department of Law,
Faculty of Arts and Humanities,
Sonargaon University (SU).

Certificate of the Thesis Supervisor

This is to certify that the research monograph on "admissibility and reliability of evidence in criminal trials: Challenges in the modern criminal procedure system" was done by Md. Jahangir Alam in partial fulfillment of the requirements for the degree of Bachelor of Laws (Hons) from Sonargaon University. The research monograph has been carried out under my guidance. Is a record of the bona fide work carried out successfully.

Sunzida Akhter,
Lecturer,
Department of Law,
Faculty of Arts and Humanities,
Sonargaon University (SU).

Acknowledgement

Firstly, I want to thank Almighty Allah for guiding me on the path. I am grateful to my supervisor Sunzida Akhter, Lecturer, Department of Law, Faculty of Arts and Humanities, Sonargaon University for her guidance, encouragement and cooperation that helped me to complete this research monograph.

I also want to thank those people who gave me information to proceed with my research report and to my friends whose cooperation helped me greatly. I extend my thanks to all the authors and writers whose works aided me in completing this work.

Thank You.

Md. Jahangir Alam,
ID No: LLB2203027026,
Department of Law,
Faculty of Arts and Humanities,
Sonargaon University (SU).

Dedication

This Research is dedicated to my Father, Mother and Barrister Muhammad Rafiul Islam.

Abstract

The way people interact with each other has changed a lot because of technology. This has really changed how crimes are prosecuted in Bangladesh. We used to rely on things we could see and touch and what people said but now we are looking more at digital information like text messages phone call records things people say on social media and secret online logs. This project takes a look at the rules and laws that decide if digital information can be used in court in Bangladesh. For a time more than a hundred years we had a big problem with using electronic information in court because of old laws from the time when Bangladesh was a colony the Evidence Act from 1872 which did not say anything about information that is not physical. This problem was finally fixed with the Evidence Amendment Act in 2022 which added some new sections, 65A and 65B to make it clear how digital information can be used in court.

By looking at what the courts have said in cases in reports like the Dhaka Law Reports, Bangladesh Law Reports, Criminal Law Reports and All India Reporter this study found a big problem with the system: people are getting mixed up about what makes digital information acceptable in court and what makes it reliable. The new laws from 2022 helped with the part making it clear what digital information can be used in court but the system is still not good at making sure the information is correct and has not been changed. There are problems like software that only the people who made it can understand, fake videos and pictures made by artificial intelligence police officers not following the right steps when they collect information and information being stored in many different places online. All these things make it hard to make sure everyone's rights are protected. The project ends with some suggestions, for how to make sure digital information's good and reliable while also making sure people who are accused of crimes are treated fairly.

Keywords: *digital evidence, admissibility, criminal procedure, chain of custody, authentication, digital forensics, electronic evidence, cybercrime, reliability.*

TABLE OF CONTENTS

CHAPTER ONE:

Introduction

CHAPTER TWO:

Literature Review

CHAPTER THREE:

Concept and Nature of Digital Evidence

CHAPTER FOUR:

Legal Framework Governing Digital Evidence

CHAPTER FIVE:

Admissibility of Digital Evidence

CHAPTER SIX:

Reliability of Digital Evidence

CHAPTER SEVEN:

Systemic Challenges and Limitations in the Trial Judiciary

CHAPTER EIGHT:

Comparative Analysis

CHAPTER NENE:

Recommendations and Reforms

CHAPTER TEN:

Conclusion

CHAPTER ONE

Introduction

1.1 Background of the Study

The way people interact with each other has changed a lot because of the internet, mobile phones and other technologies. This has also changed the way crimes are committed in Bangladesh. In the past the police used things like paper trails, weapons and eyewitness accounts to figure out what happened during a crime[1]. Now they use evidence like text messages call records and videos from security cameras [1].

However, using evidence in court can be tricky. The laws about evidence were made a time ago when everything was written on paper. Digital evidence is different because it is easy to change or delete. This means that the courts need to update their rules so that digital evidence can be used fairly[2].

1.2 Statement of the Problem

The problem with digital evidence in Bangladesh is that the courts do not have a good system for checking if it is real or not. Even though there are laws that allow digital evidence to be used in court the courts are still not sure how to handle it. They do not have a way to check if the evidence has been changed or if it is real.

This can cause problems because it means that fake evidence could be used to convict someone or that real evidence could be thrown out because it was not collected properly. The police and the courts need to find a way to make sure that digital evidence is handled correctly[3].

1.3 Objectives of the Study

The main goals of this study are:

1. To understand what digital evidence is and how it is used in investigations.
2. To look at the laws about evidence in Bangladesh and see if they are working well.
3. To compare the laws about evidence in Bangladesh to the laws in other countries like India, the United Kingdom and the United States.
4. To find out what the problems are with collecting and using evidence in Bangladesh.

---

[1] See generally, *The Code of Criminal Procedure, 1898* (Act No. V of 1898), which historically structured investigations around physical searches and manual inspections prior to modern digitization.

[2] See Reza, K. L. (2022). Challenges of the Digital Evidence in Bangladesh: The Evidence (Amendment) Act-2022. *RPSU Research Journal*, 1(2), 45-58.

[3] Ahmed, F. (2024). The Future of Cybersecurity and Data Privacy in Bangladesh: Identifying the Legislative Gaps. *American Journal of Social Sciences and Legal Studies*, 3(1), 12-29.

5. To come up with a plan to improve the way digital evidence is handled in Bangladesh.

1.4 Research Questions

To answer these questions this study will look at:

1. How does digital evidence challenge the way of thinking about evidence in Bangladesh?
2. Do the new laws about digital evidence really prevent fake or changed evidence from being used in court?
3. How do the tools used to collect evidence affect the ability of the defense to question the evidence?
4. What can Bangladesh learn from countries about how to handle digital evidence?

1.5 Methodology

This study will use an approach looking at the laws and court cases about digital evidence in Bangladesh. It will also look at how other countries handle evidence and compare their approaches to the one used in Bangladesh[4].

1.6 Scope and Limitations

This study will only look at the laws and court cases about digital evidence in criminal investigations in Bangladesh. It will not look at cases or other types of evidence. One of the limitations of this study is that there are not court cases about digital evidence in Bangladesh so it will have to rely on cases from other countries as well.

1.7 Structure of the Thesis

This study is divided into nine chapters:

1. Chapter 1 introduces the topic and explains the goals of the study.
2. Chapter 2 Literature Review
3. Chapter 3 looks at what digital evidence's how it is used.
4. Chapter 4 examines the laws about evidence in Bangladesh.
5. Chapter 5 looks at how digital evidences collected and used in court.
6. Chapter 6 examines the issues with digital evidence, like how to keep it from being changed or deleted.
7. Chapter 7 looks at the problems with using evidence in court like how to make sure it is real.
8. Chapter 8 compares the approach to evidence in Bangladesh to the approach in other countries.
9. Chapter 9 makes recommendations for how to improve the way digital evidence is handled in Bangladesh.

[4] For a broader analysis of Global South judicial digitization methodologies applied here, see Сохел, P. M. (2024). *Reforming criminal justice in Bangladesh through technology*. Research Repository of National Aviation University.

CHAPTER TWO:

LITERATURE REVIEW

2.1 Introduction

The use of computers and technology is becoming very common in Bangladesh. This has led to a big increase in crimes that happen on computers. Because of this digital evidence is now an important part of how we deal with crime in Bangladesh. In the past the laws that say what can be used as evidence in court were not very clear about things like emails and other electronic information[5].

This writing looks at what people have said in the past and what they are saying now about evidence in Bangladesh. It looks at the laws what the courts have said and the problems with the systems we use. The goal is to understand how things are changing because of laws and to find the gaps that this study wants to fix. Digital evidence in Bangladesh is an issue and this study is trying to learn more about it[6].

The laws and systems for evidence in Bangladesh are still not perfect and this study is trying to figure out what is missing. By studying the laws, the courts and the systems we can get an understanding of digital evidence in Bangladesh and how it is used. Digital evidence is very important, in Bangladesh. We need to make sure we are using it correctly.

2.2 Early Scholarly Views: Absence of Legal Recognition

The law in Bangladesh did not really say what to do with records. This was a problem. The Evidence Act of 1872 was made a time ago when everything was on paper. People who study law like Khandker Tanbir said that even though the law does not directly say electronic records are okay a court can still use them if they think it is relevant to the case[7]. Other law people said this is not a good way to do things because it is not fair. It is not fair because it depends on what the judge thinks. To get around this problem courts often said electronic records are like papers even though they are really different[8]. They did this with things like emails and video recordings. They treated these things like documents even though they are not the same as paper. The Evidence Act of 1872 has a section that talks about what a document but electronic records, like emails are not really the same thing.

---

[5] M. S. Rana, "Criminal Investigation in the Digital Era: Lessons for Bangladesh from Colombia, India and Beyond," Journal of Conhecimento & Diversidade vol. 16, No. 41 (2024) Pp. 112–115. This study looks at how digital technology's changing crime investigations in Bangladesh.

[6] R. M. Сохел, "Reforming Criminal Justice in Bangladesh Through Technology " National Academy of Internal Affairs Review, vol. 28 No. 2 (2025) Pp. 45–48. The author, R. M. Сохел talks about using tech to improve Bangladeshs justice system.

[7] M. S. Uddin "Utilization of Modern Technology Can Reduce Delay in Civil Litigation " CyberLeninka Academic Journal, (2023) p. 53. M. S. Uddin thinks modern tech can help speed up civil court cases.

[8] Khandker Tanbir, The Admissibility of Electronic Evidence in the Courts of Bangladesh: An Analytical Critique, (Dhaka: Law Review Publications, 2018) pp. 89–94. Khandker Tanbir wrote a book on evidence in Bangladesh courts.

2.3 Judicial Interpretation and Case-Based Development

The courts had to figure out how to use data in legal cases because the lawmakers were not doing their job. At first the judges were not sure about using data. They were worried that it could be fake or changed in some way. They also did not have any rules to follow.

As time went on the courts started to accept media, like CCTV footage and audio recordings. They would often use this kind of evidence in cases where nobody was arguing about whether it was real or not. When someone did question the digital evidence, the courts had a hard time deciding what to do. They did not have a way of checking if the evidence was genuine. The judges were making decisions on a case-by-case basis than following a set of rules. This meant that the decisions were not always consistent and it was hard to know what to expect. The digital data was being used in cases but the judges were still figuring out how to use it properly[9].

2.4 Role of Special Laws in Shaping Digital Evidence

The Evidence Act of 1872 had some limitations so the legislature made some changes to laws. They added some rules to these laws. For example:

1. **The Anti-Terrorism Act of 2009:** This law said that digital communications and electronic trails could be used as evidence in terrorism cases.
2. **The Pornography Control Act of 2012**: This law said that digital images and videos could be used as evidence.

These new laws helped for a while but some people who study law did not like this way of doing things. They thought it was an idea to put rules about evidence in different laws for different crimes. The Evidence Act of 1872 and these new laws, like the Anti-Terrorism Act and the Pornography Control Act had rules for what could be used as evidence. This meant that the same digital data could be used as evidence in one case but not in another just because the crimes were different. The Evidence Act of 1872 and these special laws did not have a standard of evidence which was a problem. The Anti-Terrorism Act and the Pornography Control Act were supposed to help. They did not fix the main issue, with the Evidence Act of 1872[10].

2.5 The Evidence (Amendment) Act, 2022: A Turning Point

The Evidence (Amendment) Act, 2022 brings a change to how Bangladesh handles evidence in courts[11]. This new law helps modernize the system by treating electronic records just like paper documents. Some important changes include:

---

[9] B. G. S. M. R. Ali, "Digital Evidence – An Approach to Safeguard from Cybercrime in Bangladesh " NDC Journal, vol. 21 No. 1 (2022) Pp. 24–28. B. G. S. M. R. Ali discusses evidence to prevent cybercrime.

[10] B. G. S. M. R. Ali p. 29. The author further explains the concept.

[11] K. L. Reza, "Challenges of the Digital Evidence in Bangladesh: The Evidence (Amendment) Act-2022," RPSU Research Journal, vol. 4 No. 1 (2024) Pp. 12–15. K. L. Reza writes about the challenges of evidence.

1. **Formal Recognition**: The law now clearly says that digital and electronic records are considered evidence.
2. **Authentication Mechanisms**: There are rules for checking if electronic signatures and digital messages are real.
3. **Expert Testimony**: The law allows experts to examine evidence and share their opinions in court.

The amendment also expands what is considered digital data to include things like:

1. Audio and video recordings;
2. CCTV footage;
3. Information from devices;
4. Computer logs;

This change helps Bangladesh's laws match international standards like the UNCITRAL Model Law on Electronic Commerce. The Evidence (Amendment) Act, 2022 and digital evidence are really important, for Bangladesh's court system[12].

2.6 Reliability Concerns in the Bangladeshi Context

Even though the law changed in 2022 people who study law are still worried about how reliable digital evidences in Bangladesh's courts[13]. They think there are some problems:

1. **Susceptibility to Alteration:** Digital evidence can be easily changed, deleted or made up which is a big threat to its authenticity.

2. **Capacity Gaps among Legal Actors:** Many investigators, prosecutors, defense lawyers and judges do not know enough about forensics and how electronic data works.

3. **Improper Handling:** People who are not tech savvy often handle storage devices the wrong way when they first take them which can change important information and make the evidence unreliable.

4. **Absence of Standard Operating Procedures:** There are no rules for how to find, collect keep and analyze digital evidence.

So, people who study law say that just because digital evidence is allowed in court it does not mean it is reliable. If digital evidence is not carefully checked and its history is not well documented it can be easily challenged**.**

2.7 Forensic Infrastructure and Institutional Challenges

[12] Tlou Maggie. Ntengenyane Khunjulwa, "The Management of Digital Court Records for Justice Delivery " Mousaion: South African Journal of Information Studies vol. 40 No. 3 (2023) Pp. 49–51. They discuss managing court records.

[13] E. Yunianto, "The Contribution of Forensic Science Experts Policies to Criminal Case Resolution " Journal of Doctrinal and Empirical Research vol. 2, No. 1 (2024) Pp. 201–204. E. Yunianto looks at science in solving crimes.

Recently people have noticed that Bangladesh has made some progress in forensics. The country has set up labs uses expert witnesses more often and the government is trying to improve how cybercrime is investigated[14].

However, researchers think that these efforts are not enough and are mostly focused in cities leaving areas without enough resources. The new law requires forensic exams, which has shown that the country's institutions are not capable of handling this. There is a difference between what the law wants to achieve and what the country can actually do and this is a big problem for digital evidence in Bangladesh's legal system specifically, for digital evidence.

2.8 Interaction Between Law and Technology

A big issue in the field is how laws and technology do not work well together. Laws take a time to change but technology moves really fast. This causes problems in three areas:

1. **The Time Gap:** Laws and court decisions change slowly. Technology, like on our phones and computers and ways to keep data safe change very quickly.

2. **Unclear Ideas:** Courts often have trouble understanding technology ideas, like where data is stored online digital records or messaging apps that disappear using old law ideas.

3. **Lack of Expertise:** In Bangladesh, law schools and training programs, for lawyers have not focused on how law, computers and data investigation work.

Experts think that for the law system to work well we need to understand technology and use help from experts who know about it. Laws should not just follow rules but also consider what technology experts say. The law and technology need to work better. This way laws can stay useful and fair.

2.9 Emerging Challenges: AI and Digital Fabrication

The newest level of study is looking at the big problems that artificial intelligence and advanced digital manipulation tools are causing. We are seeing a lot of realistic "deepfake" videos and audio recordings documents made by artificial intelligence and tools that can make up data automatically. This is a danger to how justice is given[15]. People are saying that the old ways of checking something is real by looking or listening are not good enough anymore. They are warning that Bangladesh's laws are not ready to deal with the ways of checking something is real that are needed to find out if something was made up by artificial intelligence. Artificial intelligence is making it hard to know what is real. What is not. Artificial intelligence is

[14] R. M. Сохел, "Reforming Criminal Justice in Bangladesh Through Technology " p. 50. R. M. Сохел provides insights.

[15] A. Yusuf, "Blockchain-Based Evidence Chains: Challenges to Authenticity, Admissibility and Judicial Trust " Legal Studies, in the Digital Age vol. 3, No. 1 (2023) Pp. 110–114. A. Yusuf discusses blockchain technology in evidence chains.

changing things. We need to be careful. The use of intelligence is a big problem for the legal system, in Bangladesh.

2.10 Relevance to the Present Study

The existing literature shows that Bangladesh is changing from a system that uses paper and analog methods for evidence to a legal system. The Evidence (Amendment) Act, 2022 has helped fill a gap in the law but there is still a large gap between what the law says and how it is actually implemented in a reliable way.

This study looks at the problems that still exist. It provides an analysis of the legal situation in Bangladesh after 2022. The study checks if digital data can be relied on in practice. It also looks at if the country's forensic infrastructure is good enough.

The study also considers the threat of fake information made by artificial intelligence. This research wants to suggest changes to the law and the system. These changes should be suitable, for Bangladesh's economic situation.

2.11 Conclusion

In conclusion the literature shows how Bangladesh's legal system has changed its view on evidence over time. It started with not recognizing evidence and making comparisons to old laws. Then it moved to having laws for digital evidence. The Evidence (Amendment) Act, 2022 is a step forward. However just having the law is not enough. The success of this legal framework depends on several things. These include making sure digital evidence is reliable creating rules, for forensic investigations combining law and technology and improving the infrastructure of institutions. This study uses these ideas to look into how Bangladesh can create a strong safe and modern digital evidence system. The study aims to help Bangladesh build on its laws the Evidence (Amendment) Act, 2022 and create a better digital evidentiary ecosystem.

CHAPTER THREE:

Concept and Nature of Digital Evidence

3.1 Definition of Digital Evidence

Digital evidence is any information that is stored or sent in a format. This can include things like text messages, emails and videos. Digital evidence is different from evidence because it is not something that you can touch or see directly[16].

3.2 Evolution of Digital Evidence

The way digital evidence is collected and used has changed over time. In the past digital evidence was mostly just things like printed out emails or documents. Now it can include things like text messages, social media posts and videos from security cameras.

3.3 Characteristics of Digital Evidence

Digital evidence has some characteristics that make it different, from physical evidence. These include:

- It is intangible meaning you cannot touch it or see it directly.
- It is highly volatile meaning it can be easily changed or deleted.
- It is easy to modify or replicate meaning it can be changed or copied without being detected.
- It can be persistent meaning it can still exist even after it has been deleted.

1.4 Types of Digital Evidence

To assist judicial analysis, digital evidence can be grouped into three operational classes:

Evidence Class	Source Mechanisms	Primary Investigative Value
Active Data	User-generated files like emails Word documents, WhatsApp chats and JPEG photos.	These files show a person's intent, like what they meant to do. They also show communication and planning. * Emails * MS Word documents * WhatsApp chat logs * JPEG photos

[16] In legal frameworks inherited from common-law traditions, electronic records were initially squeezed into the category of "Documentary Evidence" under Section 3 of the *Evidence Act, 1872*.

		help prove intent or men's rea. They show people talking and planning, on purpose.
System/Metadata	Things like registry entries and EXIF data in photos are important. We also look at log files and timestamps. There are Windows Prefetch files	These things help us find out what is really going on with the system. They show us what actually happened and when. We can see what changes the user made to the system. This is helpful for understanding what the user did. When they did it. The registry entries and other files like log files and timestamps are all useful, for tracking user modifications and discovering system interactions
Network/Volatile Data	Here are the things that can be used to track what a computer is doing: • IP routing tables • cell-site location logs • RAM dumps[17] • firewall traffic packets. .	This information can be used to figure out where a device is physically located it can identify what devices are connected to it and it can show the paths that information takes when it is being sent and received by the device.

3.5 Importance in Criminal Trials

In Bangladesh digital evidence is really important in trials these days. It often helps decide the outcome of a case[18]. When it comes to cases like corporate fraud, money laundering, cyber-

[17] See Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press, outlining the fundamental thermodynamic limits of electronic storage volatility.

[18] Alam, S. (2020). Offensive Statements on Social Networking Platforms with Special Reference to Cyber Defamation: A Comparative Analysis between Malaysia and Bangladesh. *Journal of Asian and African Social Science and Humanities*, 6(2), 89-104.

terrorism or targeted political violence we cannot always rely on what people saw with their own eyes. Digital evidence is a good way to know what really happened when it is collected in the right way.

For example, a single cell-site location log can show that someone is lying about where they were. Encrypted email records can also reveal plans that people made together over a time.

The superior courts of Bangladesh have said that people who witness something may not tell the truth or they may forget things when they are asked questions in court. Digital evidence that is stored properly gives us a true picture of what happened. Digital evidence is, like a record of events that does not change[19].

[19] See the observation of the High Court Division in *State v. Oli @ Oliur Rahman* (2016), reinforcing that human witnesses may lie or fail, but properly stored electronic records maintain chronological fidelity.

CHAPTER FOUR:

Legal Framework Governing Digital Evidence

4.1 Legal Framework in Bangladesh

The laws that govern evidence in Bangladesh have changed a lot. For a time, the system was a mix of old laws from the colonial era and new cyber laws that were very strict. Then the government changed the laws and got rid of the old Information and Communication Technology Act from 2006 the Digital Security Act from 2018 and the Cyber Security Act from 2023. Now the laws that govern evidence are based on the new Cyber Security Act from 2026 and the old Evidence Act from 1872[20].

1.2 Evidence Act, 1872 and Digital Evidence

The Evidence Act from 1872 was used for 150 years without any changes. It did not mention records so courts had a hard time figuring out how to use them as evidence. Then the government passed a new law in 2022 that changed the Evidence Act. The new law added two sections, 65A and 65B[21] which explain how to use digital records as evidence. Section 65A says that digital records need to be checked to make sure they are real. Section 65B says that if a digital record is printed or copied it can be used as evidence in court.

4.3 Old Laws

In the past the government used laws like the ICT Act from 2006 and the Digital Security Act from 2018 to control digital spaces. These laws gave the police a lot of power to search and seize devices without a warrant. These laws were not fair and did not protect people's rights. So, the government got rid of these laws. Created a new system based on the Cyber Security Act from 2026[22].

[20] The *Cyber Security Act, 2026* officially repealed and replaced the highly criticized *Cyber Security Act, 2023*, shifting the focus of the state from speech criminalization to data protection.

[21] *The Evidence (Amendment) Act, 2022* (Act No. XX of 2022), published in the Bangladesh Gazette, Extraordinary, on November 23, 2022.

[22] See Amnesty International Report (2023), *Braking Dissent: The Misuse of the Digital Security Act in Bangladesh*, which documented systemic abuses under the old Section 57 mechanisms.

4.4 The Cyber Security Act, 2026

The Cyber Security Act from 2026 is a law that focuses on keeping digital spaces safe. It moves away from punishing people for what they say and focuses on keeping data safe. The law explains how to use technologies like cloud networks, artificial intelligence and algorithms. It also creates an agency called the National Cyber Security Agency to oversee digital security. The law says that reports from analysts can be used as evidence in court. It also says that the police need to get approval from a court before they can block or delete digital content. However, some people still have concerns about the law, like the fact that it allows the police to search devices without a warrant[23].

4.5 Comparative Legal Framework

4.5.1 India

The laws in India are really important to Bangladesh because they started from the place. India changed its approach with Section 65B of the Indian Information Technology Act, 2000.

The Indian Supreme Court took a time to figure out what this provision meant. In the case of State versus Navjot Sandhu in 2005 the court first said that people could give testimony instead of getting a technical certificate. Then the court realized this was not a good idea because it made evidence easy to manipulate. So, in the case of Anvar P.V. Versus P.K. Basheer the court said that a Section 65B certificate is necessary to admit evidence that is not original.

This rule was made clearer in the case of Arjun Panditrao Khotkar versus Kailash Kushanrao Gorantyal, which said that if someone tries to get a certificate from a party like a phone company and they say no the court can make them give it. This way the rules do not get in the way of justice.

[23]Ahmed, F. (2024). Loc. cit., noting that structural enforcement mechanisms within the newly deployed 2026 frameworks still risk overlapping with Article 43 privacy guarantees if left unchecked.

4.5.2 United Kingdom

The United Kingdom changed its law that assumed computer systems always work properly. They got rid of Section 69 of the Police and Criminal Evidence Act from 1984. Now digital evidence in the United Kingdom is treated like any evidence.

The law in the United Kingdom assumes that complex electronic systems work correctly unless someone proves they do not. If the defense says the system might be corrupted the other side has to prove it is working properly.

4.5.3 United States

In the United States digital evidence has to follow the Federal Rules of Evidence. To make sure something is real Rule 901 says someone has to give evidence to prove it is what they say it is.

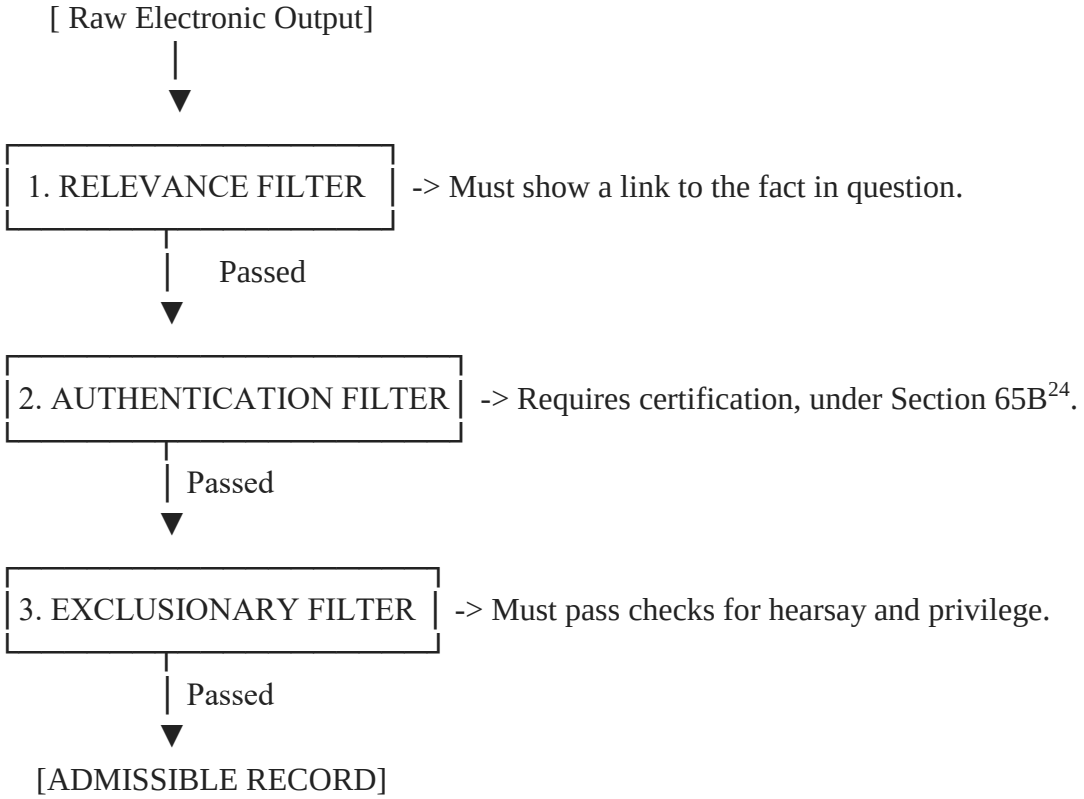
The United States made some rules, like Rules 902(13) and 902(14) to make it easier to deal with standard digital data. These rules let electronic records be used as evidence if they have a code, like an MD5 or SHA-256 that shows they have not been changed. This way a forensic expert does not have to testify in court if someone who is qualified says the evidence has not been tampered with.

CHAPTER FIVE:

Admissibility of Digital Evidence

5.1 Principles of Admissibility

In Bangladesh the law strictly controls what digital evidence is allowed in court. To be included in a case electronic records must meet certain requirements. There are three steps that digital evidence must go through to be accepted. The rules of admissibility for evidence are very clear. Digital evidence has to pass through a three-tier filter as per the law. This filter ensures that only valid digital evidence is used in a file. The admissibility of evidence is an important part of the law in Bangladesh. It is crucial that electronic records are handled properly. The three-tier statutory filter is a part of this process. Digital evidence must be treated with care to ensure it is admissible. The law in Bangladesh provides guidelines, on digital evidence. These guidelines help ensure that digital evidence is used fairly in court.



[24]Section 65B was directly modeled after Section 65B of the Indian *Information Technology Act, 2000*, attempting to import its statutory logic to mitigate data manipulation.

5.2 Relevance and Materiality

The Evidence Act of 1872 says that in any court case evidence can only be given about the facts that are being questioned and other facts that are related to the case. When it comes to cybercrimes digital data is important if it shows a conversation between people who are working together to commit a crime or if it shows the IP address that was used to launch a cyber-attack.

The digital evidence must be important to the case. Not just extra information that can confuse the issue. It must help prove a part of the crime.

5.3 Authentication Requirements

To prove that a digital file is real and has not been changed it must be authenticated. The Evidence Amendment Act of 2022 says that electronic data cannot be used as evidence on its own. If the court wants to use a copy of an email or a chat conversation it must have a certificate.

This certificate must be signed by someone who's in charge of the computer system or the activity that is being questioned[25]. The certificate must say what the electronic record is, how it was made and that the computer system was working properly when it was made.

5.4 Best Evidence Rule

The Best Evidence Rule is a law that says that the original document must be used in court, not a copy. This can be a problem with evidence because what is the original version of an email or a database entry?

The law says that if certain conditions are met a copy of the evidence can be used in court. This means that the court can accept the evidence without having to get the computer system or network[26].

[25]See *Evidence (Amendment) Act, 2022*, Section 65B (4), which defines the strict parameters of the accompanying administrator's certificate.

[26]See the foundational common-law doctrine established in *King v. Watson* (1788) regarding primary vs. secondary evidence, now updated for binary systems.

5.5 Hearsay Rule and Exceptions

In Bangladesh oral evidence must be direct. Statements from other people that have not been verified are not allowed. Digital evidence can be a problem because it may be considered hearsay. For example. a WhatsApp message that says someone else committed a crime is hearsay. Cannot be used as evidence unless it is an exception, such as a spontaneous statement or a dying declaration.

On the hand automated system logs, such as server error records or GPS pings are not considered hearsay because they are made by machines and not people[27].

5.6 Admissibility of Illegally Obtained Evidence

In Bangladesh there is a problem with evidence that is obtained illegally. If the evidence is very important to the case it can still be used, even if it was obtained without a warrant or by breaking the rules. The court can decide whether to use the evidence or not even if it was obtained illegally[28].

[27]For a discussion on machine vs. human communications under the hearsay rule, see Reed, C. (2011). *Digital Evidence*. In *Computer Law* (7th ed.). Oxford University Press.

[28]This follows the settled principle in *Kuruma v. The Queen* [1955] AC 197, where the method of obtaining evidence does not affect its admissibility if it remains logically relevant to the facts of the case.

CHAPTER SIX:

Reliability of Digital Evidence

6.1 Concept of Reliability

While it is important to decide if evidence can be used in court it is also important to make sure that the digital evidence is reliable. This means that the evidence must be accurate and not changed or manipulated.

The Supreme Court of Bangladesh has said that for evidence to be reliable it must be shown that it is accurate and has not been changed. This is very important in cases where digital evidence is being used[29].

6.2 Data Integrity Issues

Digital evidence can be compromised at any stage of an investigation. If it is not handled properly the metadata, such as the date and time it was modified can be changed.

For example, if a police officer starts up a seized laptop normally of using a special device to prevent changes the computers operating system will make changes to the system, which can destroy important evidence. This can make it hard to use the evidence, in court.5.3 Chain of Custody[30].

6.3 The Chain of Custody

The chain of custody is like a list that shows who had a piece of evidence and what they did with it. This list is very important in forensics. If the list is not complete it can hurt the case.

When evidence is found it gets a code called a hash value. This code is like a fingerprint that's unique to that piece of evidence. The evidence is then put in a bag to keep it safe.

[29] The High Court Division made a point in the case of State v. MD. Sharif in 2021 which is found in 73 DLR (HCD) 341. They said that electronic records are only given weight if we can prove they have not been changed or tampered with. This is very important when it comes to records.

[30] A book by Carrier, B. Called File System Forensic Analysis, published in 2005 by Addison-Wesley explains how the operating system can affect system files. The operating system interactions can change system files, which's a big problem.

[Seizure at Scene] ⟶ Make a Hash Value Right Away ($SHA-256$). Put in a Special Bag

[Transit & Storage] ⟶ Lock it Up; Only Let Authorized People Access it

[Forensic Lab] ⟶ Use a Special Tool to Look at it; Only Look at a Copy; Check if the Hash Value is the Same

If the hash value from the scene does not match the one from the lab it means the evidence was changed. This makes the evidence not reliable.

6.4 The Role of Digital Forensics

Digital forensics is when we use computers to help solve crimes. We collect evidence from computers and other devices. We use tools to make exact copies of the evidence. In Bangladesh there are labs that help with this. They look at the evidence. Tell the court what they found[31].

6.5 Risks of Manipulation and Tampering

Digital evidence can be changed easily. This is a problem. We need to make sure the evidence is handled correctly. If we do not check the evidence carefully it can be fake. We need to look at all the information about the evidence to make sure it is real.

6.6 AI, Deepfakes and Emerging Threats

Now we have tools that can make videos and audio. This makes it hard to tell what is real and what is not. We use codes to make sure the evidence has not been changed. These codes cannot tell us if the evidence was fake from the start[32].

[31] The Evidence Act of 1872 has a section, Section 45 that talks about when expert opinions can be used in court. This section says that expert opinions on law, science, art or identity are allowed in court.

[32] Another study by Salpekar, R. In 2020 published in the VIPS Student Law Review looks at how we can use cryptography to make sure evidence has not been manipulated. This study explores the challenges of using science in investigations. How we can use cryptographic validation to prevent algorithmic manipulation. The study of records and cryptographic validation is very important in court cases like State, v. MD. Sharif

CHAPTER SEVEN:

Systemic Challenges and Limitations in the Trial Judiciary

7.1 Lack of Technical Expertise

The main problem in the Bangladeshi trial judiciary is that judges, prosecutors and defense advocates do not have knowledge about technology. Technology is changing fast. The training given to them is still based on old legal systems. In trials with evidence courts usually rely on reports from government forensic experts. This makes the trial unfair. If the defense does not have the know-how to question the reports method the trial can become just about accepting what the experts say rather than looking at the facts. The lack of expertise is a big issue. Judges, prosecutors and defense advocates need to understand technology to make trials fair. They need training to deal with evidence. The trial judiciary needs to update its approach to keep up with technology. Lack of expertise affects the trial process. It is essential to address this issue to ensure fairness, in trials[33].

7.2 Inadequate Legal Provisions

The Evidence (Amendment) Act, 2022 did bring in some updates. There are still some big gaps in the laws. The Code of Criminal Procedure, 1898 (CrPC) does not have rules, on how to handle digital devices at a crime scene. This law is still old. There are no punishments if a police officer does not follow the right steps when searching a device.

For example, if they do not use a tool called a write-blocker or do not create a secret code to check the device nothing happens. This means that police officers have to make decisions on their own. As a result, different police stations handle evidence in different ways. The police need rules to make sure they handle digital evidence correctly. This will help make sure that evidence is not damaged or changed. The law needs to be updated to include these rules. The Code of Criminal Procedure, 1898 (CrPC) needs to be changed. Police officers need to follow

[33] Law, L. (2021). Application of Cyber Laws in Developing Legal Landscapes. *Amity Law Review*, 15(4), 201-218, highlighting the systemic legal dependency on un-vetted forensic declarations in South Asia.

the steps when handling digital devices. This will help make sure that justice is fair. The Evidence (Amendment) Act, 2022 is a start. More needs to be done[34].

7.3 Cross-border Data and Jurisdiction Issues

The internet does not have borders, which causes problems for laws in countries like Bangladesh. In Bangladesh under Section 96 of the Criminal Procedure Code (CrPC) search warrants can only be used in areas. Nowadays user data is often stored in cloud systems that are spread across many countries. If there is a case of cyber-terrorism and the data is stored on encrypted servers in Western Europe by a company based in North America the police here cannot simply get a warrant. They have to go through a process of asking for help from other countries using Mutual Legal Assistance Treaty (MLAT) or formal requests. This takes a lot of time and often the important data gets deleted or removed before they can get it. The data and server traffic logs get automatically overwritten or purged because of the delay. This makes it hard for the police to investigate cyber-terrorism cases. The main issue here is the -border data and jurisdiction. Cross-border data issues make it difficult for law enforcement to get the data they need. Jurisdiction issues also arise when the data is stored in another country. So, border data and jurisdiction issues are a big challenge for law enforcement in cases, like cyber-terrorism.

7.4 Privacy vs Investigation

The constant gathering of evidence often causes a problem with the right to privacy that is guaranteed by the constitution. Article 43 of the Constitution of Bangladesh clearly says that citizens have the right to keep their letters and other communications private[35].

The Cyber Security Act 2026 has rules that let law enforcement agencies look at electronic devices and watch network traffic if they think it is necessary to keep the public safe or secure the state. The big issue here is that the system does not have rules to protect people. For example, investigators do not need to get a paper signed by a judge before they can look at everything on a person's smartphone.

[34]Сохел, Р. М. (2024). Loc. cit., outlining how institutional disconnects between local policing sectors and international cloud network frameworks paralyze domestic cyber inquiries.

[35]For an in-depth exploration of this tension, see Riaduzzaman, M. (2025). *Constitutional Right to Privacy and Data Protection in Bangladesh: A Living Originalist Interpretation* (Doctoral dissertation, University of Dhaka).

This means that investigators can easily do things that violate people's right to privacy because there is not oversight from judges. To prevent mistakes from happening because of technology the Cyber Security Act, 2026 and the Constitution need to work together to make sure that people's personal information is protected while still allowing for fair investigations that can be checked. The Cyber Security Act, 2026 and the Constitution must find a balance to protect the information of citizens like the people of Bangladesh while still letting the police do their job and investigate crimes, in a fair way.

The cost of doing forensics is a big problem for the justice system in Bangladesh. It is very expensive to buy the software that is needed to look at the information on devices. This software needs to be paid for every year. It is a lot of money.

7.5 Financial Constraints and Forensic Backlogs

The Digital Forensic Lab in Dhaka also needs machines to check the devices and these machines are hard to get. The lab does not have enough of these machines. This means that the lab gets behind on its work.

As a result, the Digital Forensic Lab in Dhaka has a lot of devices waiting to be looked at. This causes a delay in the trials. The people who are accused of a crime have to wait a time in jail before they can have a trial. They have to wait for months just to get a report about what's on their mobile phone. The Digital Forensic Lab in Dhaka is taking a time to do its job and this is causing problems for the justice system in Bangladesh and for the Digital Forensic Lab in Dhaka. The cost and the delay are problems for the Digital Forensic Lab in Dhaka and for the justice system, in Bangladesh[36]

[36] Ahmed, F. (2024). Loc. cit., assessing the systemic infrastructure deficits of the central forensic facility located in Dhaka.

CHAPTER EIGHT:

Comparative Analysis

8.1 Developed vs Developing Legal Systems

When we compare legal systems, we can see a big difference between countries with well-established laws and good digital systems and countries, like Bangladesh, where the legal system is still getting used to the changes that come with digital evidence:

Evaluation Vector	**Developed Systems (US / UK)**	**Developing Systems (Bangladesh)**
Statutory Maturity	Unified digital evidence codes with clear rules for self-authentication (e.g., FRE 902).	Fragmented provisions; reliance on a 150-year-old Evidence Act modified by periodic amendments.
Forensic Infrastructure	Decentralized, highly certified forensic labs operating under strict international standards (ISO/IEC 17025).	Highly centralized forensic infrastructure facing significant case backlogs and budget constraints.
Procedural Safeguards	Strict enforcement of warrants and privacy protections to exclude unlawfully collected data.	Broad search and seizure authority under specialized acts (CSA 2023) with limited pre-extraction review.
Judicial Capacity	Regular, mandatory technology training for judicial officers and trial advocates.	Variable technical literacy; heavy reliance on expert witness testimony.

8.2. Strengths and Weaknesses

Strengths

The Evidence Amendment Act 2022 was a success because it finally decided how digital data should be treated by law and stopped people from handling electronic records like they were old paper documents that were not standardized. The Evidence Amendment Act 2022 did a job in figuring out the basic legal status of digital data. This law helped to end the way of treating

electronic records. The law says that there has to be a checklist that the prosecuting agencies have to follow and this checklist is like a guide that makes sure they check the source system to see if it is working properly. The statutory certification framework is very important because it helps the prosecuting agencies to confirm the status of the source system. The Cyber Security Act is also very important because it helped to establish forensic teams that make sure the courts get forensic reports that are standardized. The specialized forensic teams under the Cyber Security Act are doing a job in providing standardized forensic reports.

Weaknesses

The framework is about deciding if digital evidence can be used in court but it does not have many tools to check if the evidence is reliable or if it has been changed using advanced artificial intelligence techniques. The framework has some problems because it focuses primarily on the admissibility phase and it does not have tools to evaluate the technical reliability of digital evidence. There are no rules about using cryptographic hash tracking under the CrPC and this means that there can be mistakes when collecting evidence at a crime scene. The lack of rules under the CrPC regarding cryptographic hash tracking is a big problem because it leaves room for procedural errors at the crime scene. The fact that all the forensic facilities are in one place can cause delays, in trials and a lot of backlogs. The centralized nature of facilities is a major weakness because it leads to prolonged trial delays and backlogs[37].

8.3 Lessons for Bangladesh

Bangladesh can draw valuable procedural insights from foreign common-law frameworks:

1. **From India:** The evolution of Section 65B jurisprudence highlights that while statutory certificates are mandatory, courts must remain flexible. If a party cannot secure a certificate from a telecom controller, the judiciary should use its subpoena powers to protect due process, as established in *Arjun Panditrao*[38].
2. **From the United States:** Bangladesh should consider adopting a self-authentication framework for standard digital files based on verified forensic hash matches (MD5 or SHA-256). This step would significantly reduce trial delays by removing the

[37] Reza, K. L. (2022). Loc. cit., criticizing the legislative oversight regarding post-admissibility reliability criteria.

[38] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) Civil Appeal Nos. 10-11 of 2020 (Supreme Court of India), which definitively settled the mandatory nature of Section 65B certificates in India while carving out exceptions for non-cooperative third parties. See also *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.

requirement for expert witnesses to provide live testimony for routine, unmanipulated data extractions[39].

3. **From the United Kingdom:** Shifting the burden of proof regarding system operational health once the defense presents a plausible challenge would prevent courts from blindly assuming that automated software systems are always operating perfectly[40].

[39].See *Federal Rules of Evidence*, Rule 902(13) and 902(14), which permit certified data extractions authenticated via hash functions (MD5 or SHA-256) without live expert presence

[40] Section 69 of PACE was repealed by Section 60 of the *Youth Justice and Criminal Evidence Act, 1999*, returning the UK to the common law presumption that a computer is working correctly unless evidence to the contrary is introduced.

CHAPTER NENE:

Recommendations and Reforms

9.1 Legal Reforms

1. **Digital Evidence Rules Act**

   Bangladesh needs to make a law called the Digital Evidence Rules Act. This law should have rules for handling evidence. When the police take someone's computer or phone they have to make sure it does not get changed. They need to use a tool to stop anyone from changing the information on the device. They also need to make a copy of the information on the device with other people watching so everyone knows it is the original[41].

2. **Amendment of the CrPC**

   The Code of Criminal Procedure from 1898 needs to be updated. This update should explain what a digital search is. The police should have to get a permit that says exactly what they are looking for on a computer or phone. They should not be able to take the whole device without knowing what they are looking for. The Digital Evidence Rules Act and these changes, to the Code of Criminal Procedure will help with reforms.

9.2 Institutional Development

3. **Decentralization of Forensic Labs:**

   The government should set up facilities in different parts of Bangladesh. This means they will have labs in every division of Bangladesh. If they do this it will help because now everything is done in Dhaka and that causes delays. When there are labs in every division it will be faster to get the results of tests and this will help with trials.

4. **Independent Software Auditing Board:**

   The government should make a group that is independent and can check the software that the police use. This group will make sure that the software is good and works properly. They will check the software that the police use to get information from computers and phones and they will make sure that it is fair and accurate. This is important because some software is, like a box and nobody knows how it works so this group will help make sure it is okay.

[41]This mirrors the procedural recommendations outlined by Reza, K. L. (2022). Loc. cit.

9.3 Capacity Building

1. **Judicial Training:**

   The Judicial Administration Training Institute, which is also known as JATI needs to make some changes. JATI should make sure all session judges and magistrates learn about forensics and other technical things. They should have to get certified in things like metadata analysis and cybercrime evaluation[42].

2. **Tech-Equipped Legal Aid:**

   The National Legal Aid Services Organization should get some help. They need to have people who're experts in technology to assist them. This way people who cannot afford lawyers will have someone to help them understand evidence and challenge it in court if they need to. This will help make sure that people who do not have a lot of money have the access to good legal help, as everyone else. Capacity Building is important for this to happen.

9.4 Technological Integration

A. Cryptographic Blockchain Tracking:

We need to use a kind of computer system called Cryptographic Blockchain Tracking in Bangladesh. This system will help the police keep track of evidence. It will be like a diary that writes down every time someone looks at the evidence from the moment it is found.

Bangladesh should also get some tools that use Artificial Intelligence to detect fake videos and pictures.

B. AI Detection Tools:

These tools will help the people in the labs figure out if something is real or not. This is important because some people can use computers to make things that look real and we do not want these fake things to be used in court. The Artificial Intelligence Detection Tools will help us find out if something is fake before it is used in court. The police and the

[42]See guidelines from the Judicial Administration Training Institute (JATI) regarding curriculum adjustments for e-judiciary adaptation.

courts, in Bangladesh need to use these Artificial Intelligence Detection Tools to keep everything fair[43].

9.5 International Cooperation

Reforming the way, we work with countries to get information from big technology companies like Facebook and Google should be a priority for Bangladesh. We need to make agreements with these companies so we can get the information we need from them quickly without having to go through the usual slow process of working with other countries.

Bangladesh should also look at the rules and laws of countries and international agreements like the Budapest Convention on Cybercrime to see if our own laws are in line with them. This will help us work better with countries to stop cybercrime and make the internet a safer place for everyone. International Cooperation is very important for Bangladesh. We should make sure our laws are in line, with international laws to make this work.

[43]For systemic structures of decentralized custody architectures, see generally, Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*, which popularized the underlying cryptographic append-only architecture used in modern forensic ledgers.

CHAPTER TEN:

Conclusion

10.1 Summary of Findings.

This study shows that the Evidence Amendment Act 2022 was able to bring records into Bangladesh's legal system through Sections 65A and 65B. There is still a big problem with technical reliability. The Evidence Amendment Act 2022 is not being used properly because trial courts often accept data that is not very reliable. They do this because the people who give them the data just say it is okay without checking it. This means that the data can be wrong or changed and people may not know who had the data before. Also, the special programs used to look at the data can make mistakes.

The main problem is that the law that says how courts should work the CrPC does not have rules for using digital evidence. The judges do not know as much about digital evidence as they should. This means that the people involved in a trial the Evidence Amendment Act 2022 is still, about evidence cannot really question the digital evidence in a fair way. The Evidence Amendment Act 2022 and digital evidence are not being used well as they could be.

10.2 Final Observations.

Digital evidence is a powerful tool for discovering the truth, but it is not inherently self-authenticating or immune to manipulation. As Bangladesh deepens its digital infrastructure, its legal systems must evolve accordingly. Relying on basic documentary rules to evaluate volatile binary data risks producing technologically advanced miscarriages of justice. True procedural integrity requires an evidence framework where every digital submission can be independently audited, verified, and contested in an open court of law.

10.3 Future Scope of Research.

We need to do research on the future of law. This research should look at the problems that come up when we use web applications, automated smart contracts and encrypted edge computing in court. We should also study how courts in parts of Bangladesh are using the new rules from the 2022 Evidence Act. This will help us see if people are getting a trial

everywhere in Bangladesh. Future legal research should investigate the problems, with evidence that come from using decentralized web applications and automated smart contracts. Future legal research should also look at encrypted edge computing.

Bibliography

I. **Primary Sources**

1. The Constitution of the Peoples Republic of Bangladesh 1972 is a document that has Article 43.
2. We also have The Evidence Act, 1872 which's Act No. I of 1872.
3. The Code of Criminal Procedure, 1898 is another one it is Act No. V of 1898.
4. The Penal Code, 1860 is Act No. XLV of 1860.
5. The Evidence Act was amended in 2022 this amendment is called the Evidence Amendment Act, 2022. It is Act No. XX of 2022.
6. The Cyber Security Act, 2026 is a law in Bangladesh.
7. In the United Kingdom they have The Police and Criminal Evidence Act, which is also known as PACE and it was made in 1984.
8. India has The Information Technology Act, 2000.
9. The United States has Federal Rules of Evidence and these rules include rules 901, 902(13) and 902(14).
10. There are also court cases like State versus Navjot Sandhu, which happened in 2005 in India and the case number is 11 SCC 600.
11. In Bangladesh we have Malek Shariff versus State which happened in 2006. The case number is 14 BLR (AD).
12. In India there was Anvar P.V. Versus P.K. Basheer and this happened in 2015 with the case number AIR 2015 SC 180.
13. Another case in India is Arjun Panditrao Khotkar versus Kailash Kushanrao Gorantyal, which happened in 2020 with the case number AIR 2020 SC 3402.

II. Secondary Sources

1. Carrier wrote a book called File System Forensic Analysis in 2005. It was published by Addison-Wesley Professional.
2. Casey wrote a book called Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. This was published in 2011 by Academic Press.

3. Monir wrote a book called Principles and Digest of the Law of Evidence in 2023. It was published by Universal Law Publishing.
4. Hoque wrote an article called Admissibility of Electronic Evidence in Bangladesh: A Critical Analysis of the Statutory Loopholes and this was published in 2021 in the Dhaka University Law Journal.
5. Mason also wrote an article called The Presumption that Computers Reliable and this was published in 2016 in the Institute of Advanced Legal Studies Review.
6. The National Cyber Security Agency made a document called Standard Operating Procedures, for Digital Evidence Collection and Chain of Custody Management in 2026. This was published by the Ministry of ICT, Government of Bangladesh.