Admissibility of Digital Evidence in Bangladesh: An Appraisal with Special Reference to the Recent Changes in the Law of Evidence

SUBMITTED IN PARTIAL FULFILMENT OF THE CRADIT REQUIREMENTS FOR AWARDING THE DECREE OF MASTER OF LAWS BY DAFFODILE INTERNATIONAL UNIVERSITY

SUPERVISED BY

DR S. M. SAIFUL HAQUE
ASSOCIATE PROFESSOR
DEPARTMENT OF LAW
DAFFODIL INTERNATIONAL UNIVERSITY

SUBMITTED BY

Akhi Ahammed
ID NO:0242510008133005
REG NO: 251-38-005
Program: LL.M
Session:2024-2025(44th Batch)
Course Name: Research Monograph
Department Of Law,
Daffodil International University

Letter of Transmission

To
Dr. S. M. Saiful Haque
Associate Professor
Department of Law
Daffodil International University
Dhaka, Bangladesh

Subject: Submission of Research Monograph

Dear Sir,

With due respect, I am pleased to submit my research monograph titled "Admissibility of Digital Evidence in Bangladesh: An Appraisal with Special Reference to the Recent Changes in the Law of Evidence." This monograph has been prepared in partial fulfillment of the requirements for the Master of Laws (LL.M) program under the Department of Law, Daffodil International University.

I, Akhi Ahammed, Student ID 251-38-005, have made every effort to conduct the study sincerely and maintain academic standards throughout the preparation of this work. I am grateful for your continuous guidance, valuable suggestions, and supervision, which have been crucial in completing this monograph.

I humbly request you to accept this research monograph for evaluation.

Thank you for your support and cooperation.

Sincerely,
Akhi Ahammed
ID: 251-38-005
Department of Law
Daffodil International University

Certification

This is to certify that the thesis entitled **"**Admissibility of Digital Evidence in Bangladesh: An Appraisal with Special Reference to the Recent Changes in the Law of Evidence**"** is the result of the original research work carried out by **Akhi Ahammed** ID: 251-38-005, under my supervision in the **Department of Law, Daffodil International University, Dhaka, Bangladesh.**

I affirm that the work presented in this thesis is original, authentic, and suitable for the fulfillment of the requirements for the degree of **Master of Laws (LL.M.),** a one-year program under the Department of Law, Daffodil International University.

Dr S. M. Saiful Haque
Associate Professor
Department of Law
Daffodil International University

Declaration

I, **Akhi Ahammed**, hereby declare that the thesis entitled **"**Admissibility of Digital Evidence in Bangladesh: An Appraisal with Special Reference to the Recent Changes in the Law of Evidence**"**, submitted in fulfillment of the requirements for the degree of **Master of Laws (LL.M)**, Department of Law, **Daffodil International University**, embodies the results of my own research work pursued under the supervision of **Dr S. M. Saiful Haque, Associate Professor, Department of Law, Daffodil International University.**

I further declare that I am solely responsible for the content and writing of my entire work. This thesis has been prepared with my own effort and under my own responsibility. To ensure originality, the university's anti-plagiarism policies were strictly followed throughout its preparation.

I also affirm that this thesis has not been published or submitted to any other publication, nor has it been submitted for any other degree or qualification at this or any other university.

Akhi Ahammed
ID: 251-38-005
Department of Law
Daffodil International University

Acknowledgment

First and foremost, I would like to express my deepest gratitude to the Almighty Allah for granting me the strength, patience, and perseverance to complete this thesis successfully.

I am profoundly indebted to my supervisor, **Dr S. M. Saiful Haque, Associate Professor, Department of Law, Daffodil International University**, for his invaluable guidance, insightful suggestions, and continuous encouragement throughout the course of this research. His scholarly advice, constructive criticism, and constant motivation have been instrumental in shaping this study and enhancing its academic quality.

I would also like to extend my sincere thanks to all the respected teachers of the **Department of Law, Daffodil International University**, for their academic support, advice, and encouragement during my LLM program.

My heartfelt appreciation goes to my friends and classmates for their cooperation, discussions, and moral support throughout my academic journey.

Finally, I am deeply grateful to my family for their unconditional love, prayers, and encouragement, which have been the foundation of my strength and determination.

Without the guidance, assistance, and support of these individuals, the completion of this thesis would not have been possible.

Sincerely,

Akhi Ahammed
ID: 251-38-005
Department of Law
Daffodil International University

Abstract

This thesis examines the phenomenon of juvenile delinquency in Bangladesh with a particular focus on the role and application of digital evidence in legal proceedings. It investigates how the legal system addresses crimes committed by juveniles, the challenges associated with collecting, preserving, and presenting digital evidence, and the implications for justice and rehabilitation.

The study employs a mixed-methods approach, combining qualitative interviews with legal experts, law enforcement officials, and stakeholders, along with quantitative analysis of relevant case data. Key findings reveal gaps in the current legal framework, limited technological resources, and insufficient training for handling digital evidence in cases involving juveniles. These challenges affect both the efficiency of investigations and the protection of juveniles' rights under existing laws.

Based on the analysis, the thesis offers recommendations to strengthen the legal and procedural mechanisms, improve digital forensic capacity, and promote collaboration among law enforcement agencies, courts, and policymakers. The study aims to contribute to the ongoing discourse on juvenile justice reform in Bangladesh

Contents

Letter of Transmission i

Certification ii

Declaration iii

Acknowledgment iv

Abstract v

CHAPTER 1: INTRODUCTION 1

1.1 Background of the Study 1

1.2 Statement of the Research Problem 3

1.3 Aims and Objectives of the Study 4

1.4 Research Questions 5

1.5 Scope and Limitations of the Study 6

1.6 Significance of the Study 7

1.7 Structure of the Thesis 8

CHAPTER 2: LITERATURE REVIEW 10

2.1 Evolution of the Concept of Digital Evidence 10

2.2 Comparative Perspectives: UK, India, USA 12

2.3 Scholarly Opinions on Admissibility and Reliability 13

2.4 Studies on Digital Evidence in Bangladesh 14

2.5 Identified Gaps in Literature 14

CHAPTER 3: THEORETICAL AND LEGAL FRAMEWORK 14

3.1 Understanding Digital Evidence: Nature and Characteristics 15

3.2 Principles of Evidence Law: Relevance, Genuineness, and Reliability 16

3.3 The Law of Evidence in Bangladesh (Evidence Act 1872) 18

3.4 Recent Amendments (Evidence Act Amendment 2022) and Their Implications 18

3.5 International Standards on Digital Evidence 20

3.6 Summary 21

Chapter 4: Admissibility of Digital Evidence in Bangladesh 21

4.1 Provisions Governing Digital Evidence under the Amended Evidence Act 21

4.2 Judicial Attitudes towards Digital Evidence 24

4.3 Rules on Authentication, Electronic Records, and Signatures 26

4.4 Challenges in Ensuring Reliability and Integrity 27

4.5 Role of Forensic Technology 28

Chapter 5: Problems and Challenges in Digital Evidence Admissibility in Bangladesh 30
5.1 Lack of Technical Expertise in the Judiciary and Legal Community 30
5.2 Weaknesses in Cyber Forensics Infrastructure 32
5.3 Privacy and Data Protection Concerns 33
5.4 Issues of Chain of Custody and Hacking Risks 34
5.5 Delay and Procedural Loopholes in Trial Courts 35
5.6 Case Studies and Comparative Analysis 36
5.7 Recommendations 37
Chapter 6: Comparative and Reform Analysis 38
6.1 Lessons from India's Information Technology Act and Evidence Law 38
6.2 Approaches in UK and US Courts on Digital Evidence 40
6.3 Best Practices for Admissibility and Reliability 43
6.4 Prospects for Law Reform in Bangladesh 46
Chapter 7: Conclusion and Recommendations 49
7.1 Summary of Findings 49
7.2 Appraisal of the 2022 Amendments 51
7.3 Recommendations for Judicial Training, Policy Reform, and Forensic Development 52
7.4 Future Directions for Research 55
CONCLUTION 56
Bibliography 57
Primary Legislation (Bangladesh) 57
Foreign Legislation 57
Case Law (Bangladesh) 57
Case Law (India) 57
Case Law (United Kingdom) 57
Case Law (United States) 57
International Instruments & Guidelines 58
Books 58
Journal Articles 58
Comparative & Policy Sources 58
Online & Institutional Reports 58

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

The development of technology is happening really fast and it has changed a lot of things. People interact with each other in ways now. They. Do business in different ways too. We have a lot of platforms, like social media, mobile applications, email services and online banking. We also have cloud storage and other ways to communicate electronically. These electronic platforms are how most people communicate nowadays. Digital technology is used for everything. People use technology to talk to each other and to do business. It is a part of our lives now. Digital technology has really changed the way we live. This change to online services has had an effect on crime. It has led to new types of crimes that use technology, such as online scams people stealing identities harassment on the internet fake financial deals saying bad things about people online ransomware exploiting people in a sexual way and talking about terrorism online. Because of this digital evidence is now very important for finding out about crimes investigating them and prosecuting the people who commit them in this century. The online service shift has really changed the way criminal activity happens and digital evidence is crucial for dealing with harassment, cyber fraud and other technology-assisted offences like identity theft and financial scams. Digital evidence is necessary, for the detection, investigation and prosecution of these offences.[1]

When it comes to data, judicial systems all around the world are now okay with using it as evidence in court. The United States, the United Kingdom, India, Singapore and Australia are some countries where courts have been dealing with evidence for a long time.

These countries have set up rules to make sure the electronic data is good enough to be used in court. The electronic data must be completely honest and accurate. It must be reliable.

The United States and other countries, like the United Kingdom, India, Singapore and Australia have been following these rules for a while now. Bangladesh has always used the Evidence Act of 1872. This is a law that was made a time ago before people started using the internet to communicate with each other. The Evidence Act of 1872 is not very good at dealing with things like records, metadata, forensic imaging, hashing or the digital chain of custody. The Evidence Act of 1872 just does not have the rules to handle these kinds of things because it was written long ago. Bangladesh needs something, than the Evidence Act of 1872 to deal with these modern issues. The Evidence Act of 1872 is just not suited for this.[2]

The country is changing fast with new technology coming out all the time. This means we need laws to keep up with it. The ICT Act of 2006 was a start because it said something about records for the first time.. The rules in the ICT Act of 2006 were not clear and did not really work well

[1] Orin S Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 *Columbia Law Review* 279.
[2] United Nations Office on Drugs and Crime (UNODC), *Practical Guide on Digital Evidence* (2019).

when it came to making sure electronic records could be used as evidence, in court. The ICT Act of 2006 has some problems.

Later the Digital Security Act of 2018 was created to stop cybercrime and make sure digital evidence is allowed in court.. People are still not really sure about how to protect peoples rights when it comes to digital evidence. The Digital Security Act is still not clear about things like how to make sure digital evidence's good enough to use in court what rules to follow and how to handle evidence that is found on computers and other devices. The Digital Security Act needs to be clearer, about these things so that people know what to do.

Something big happened with the Evidence Act in 2022. They made some changes. Added new parts called Sections 65A and 65B. These new parts are like what they have in the Indian Evidence Act. They looked at what other countries are doing too.

Section 65A is about records. It says what they are and that they can be used as evidence.

Section 65B is about how to make sure these electronic records are real. It says you have to get a certificate to prove they are authentic.

The Evidence Act had these changes to make the rules about evidence in Bangladesh. They want to make sure people handle information in a way that is trustworthy. The Evidence Act is important, for Bangladesh. These changes will help with that. The new Sections 65A and 65B are a part of this.[3]

We have made some progress. There are still a lot of problems. Digital information can be changed without anyone noticing so it is hard to tell if it is real or not. The people who work in the labs that check evidence do not have the tools or the skills they need. The police do not always know how to save and record digital information.

The courts often do not agree on what's needed to prove something with electronic evidence so they make different decisions. Digital data and digital evidence are still a problem. There is also a lot of confusion about the laws, like the Evidence Act, the DSA 2018 and the ICT Act 2006 and how they work together which makes it hard to follow the procedures, with digital evidence and digital data.

Understanding the rules about what evidence's allowed in court is really important when you think about how much digital evidence is used in big crimes like terrorism, money laundering and child pornography. Digital evidence is also used in cases of radicalization political misinformation, cyber extortion and transnational fraud. If we do not have rules about what evidence is allowed then some very important cases might be thrown out of court. This means that the people who did something might not get punished and the victims will not get the justice they deserve. So it is very

[3] Indian Evidence Act 1872 (India), ss 65A–65B.

important that we take a look at the current laws especially since they were changed in 2022. We need to understand the rules about evidence like what makes it allowed in court to make sure that justice is served in these serious crimes, including terrorism, money laundering and child pornography as well, as online radicalization, political misinformation, cyber extortion and transnational fraud.[4]

1.2 Statement of the Research Problem

Digital evidence is really different from the kind of evidence. The thing about data is that it can change quickly it is easy to alter and it is very fragile. We need special machines to get to it and understand what it means. Digital evidence is not like things we can touch. We can easily erase things lock them with secret codes damage them or even change them from another place. This means we have to be very careful, with evidence and make strong rules to make sure it is reliable and we can trust digital evidence.

Bangladesh has made some changes to the evidence law.. The real problem is that it is not working in practice. There are a few issues with the evidence law in Bangladesh. These issues are the things that need to be looked at in the research on the evidence law, in Bangladesh.

1. Lack of clear procedural standards

People who investigate things often do not do things the way they are supposed to when they get and look at things. They are supposed to follow some rules that everyone agrees on. When they do not write down what they did with the things properly it can cause problems, in court. The court may wonder if someone changed or messed with the things. This happens because the people who investigate things did not do a job of keeping track of the digital things like the digital materials.

2. Inadequate forensic infrastructure

Digital forensic laboratories in Bangladesh usually do not have resources. When it takes a time to process evidence it can hurt the integrity of the digital forensic laboratories in Bangladesh. This can also make the evidence from the forensic laboratories, in Bangladesh less useful.

3. Judicial inconsistencies

Courts have different ideas about what Sections 65A and 65B mean. Sometimes they accept screenshots or digital papers that are not certified.. Other times they do not accept these things because they do not meet the rules for certification. Sections 65A and 65B are looked at in different ways, by the courts.[5]

[4] Evidence (Amendment) Act 2022 (Bangladesh).
[5] Information and Communication Technology Act 2006 (Bangladesh).

4. Unclear relationship between multiple laws

The Evidence Act and the DSA 2018 and the ICT Act 2006 all have rules about evidence.. These rules do not always match. This means we have steps to follow or we have to do the same thing twice. The Evidence Act and the DSA 2018 and the ICT Act 2006 are supposed to work but they do not always agree on what to do, with electronic evidence.

5. Lack of training for legal practitioners

Judges, lawyers and investigators usually do not have technical training on things like metadata, hashing, imaging, encryption and digital genuineness tools. They need to know more about genuineness tools and encryption. The problem is that judges, lawyers and investigators often lack training, on metadata and hashing and imaging. This is an issue because judges, lawyers and investigators have to work with metadata and encryption and digital genuineness tools all the time.

6. Risks of data manipulation

Courts are careful when it comes to materials because they can be changed. Digital evidence is not trustworthy unless it has been properly certified and analyzed by an expert. The people handling this evidence must also do so in a way. This is important because digital materials can be edited, which is why courts remain cautious, about evidence.

1.3 Aims and Objectives of the Study

The main goal of this research is to take a look at the law that decides if digital evidence is allowed in Bangladesh. We want to see if the new changes make the law strong easy to understand and relevant to technology. The research will examine the law and the changes to see if they work together. The law governing evidence in Bangladesh is what we are focusing on. We need to check if the recent amendments to the law make it better for evidence, in Bangladesh.

Specific Objectives:

To examine the historical development and evolution of digital evidence laws in Bangladesh.

To analyze the admissibility standards under Sections 65A and 65B of the Evidence Act.

We need to see if the new changes fix the life problems and technical issues with the recent amendments. The recent amendments have to make things work better in practice. So we have to check if the recent amendments really solve these problems.

To evaluate judicial trends and case law interpretation relating to digital evidence.

To identify institutional, technical, and procedural challenges faced by stakeholders.

To propose reforms and policy recommendations to strengthen the legal framework.

1.4 Research Questions

So we want to achieve our goals. The study is trying to answer these questions:

How has the legal framework for digital evidence developed in Bangladesh over time?

The rules for evidence have changed under the new Evidence Act. To be accepted digital evidence must meet requirements.

The Evidence Act says that digital evidence is allowed in court if it is genuine and reliable.

For evidence to be admissible it must be properly collected and stored.

This means that the people collecting evidence have to follow the right steps.

The main thing is that digital evidence has to be real and not tampered with.

The Evidence Act has rules to make sure digital evidence is trustworthy and can be used in court.

Digital evidence, under the amended Evidence Act must be handled correctly to be accepted.

The question is do Sections 65A and 65B really do enough to deal with the problems of whether something's genuine and whether it is reliable. Sections 65A and Sections 65B have to make sure that things are real and that people can trust them. So the main issue is whether Sections 65A and Sections 65B are good enough to solve these problems of genuineness and reliability of Sections 65A and Sections 65B.

Bangladeshi courts have done a lot of work to figure out how to use evidence in cases. The rules for evidence are pretty new so Bangladeshi courts have had to interpret and apply these rules.

When it comes to evidence Bangladeshi courts look at things like emails and messages on phones. Bangladeshi courts also think about how to make sure electronic evidence is real and not fake.

In some cases Bangladeshi courts have said that electronic evidence can be used to prove something. Only if it is certified by the right people. Electronic evidence is very important, in cases so Bangladeshi courts have to be careful when they use it.

Overall Bangladeshi courts are still learning about evidence and how to use it in a fair way. Bangladeshi courts have to make sure that electronic evidence is used correctly so that people get a trial.

Investigations can be really tough for investigators, forensic experts and legal practitioners. They have to deal with a lot of problems. One of the issues is that they have to work with a lot of different people like investigators, forensic experts and legal practitioners to figure out what really happened. Investigators, experts and legal practitioners also have to look at a lot of evidence and try to make sense of it. Sometimes investigators, experts and legal practitioners have to make tough decisions and that can be very hard, for them. Investigators, experts and legal practitioners are always trying to find the truth but that is not always easy.

To improve evidence admissibility in Bangladesh we need to think about what changes can be made.

Digital evidence admissibility in Bangladesh is an issue.

We should look at the laws. See what needs to be changed so that digital evidence can be used in courts in Bangladesh.

Some things that can be done include making sure that digital evidence is collected and stored properly in Bangladesh and that the people who collect it are trained to do

This will help to make sure that digital evidence is reliable and can be used in courts in Bangladesh.

We also need to make sure that the courts in Bangladesh understand what digital evidence is and how it can be used.

Digital evidence admissibility in Bangladesh is very important for making sure that justice is served.

We need to make some changes to the laws and the way that digital evidence is handled in Bangladesh.

This will help to improve evidence admissibility in Bangladesh and make sure that people are held accountable, for their actions.

1.5 Scope and Limitations of the Study

Scope

The study is, about:

The Evidence Act 1872, particularly Sections 65A and 65B.

Judicial decisions from Bangladeshi courts relating to electronic records.

The interface between the Evidence Act, ICT Act 2006, and DSA 2018.

Practical challenges encountered in digital forensics.

Comparative analysis with jurisdictions such as India and the UK.

Limitations

There is not a lot of reported case law to look at. This is because many court decisions that involve evidence are not written down and made public.

They do not let everyone into the laboratories. The study has to use information that other people have already collected about the things that happen in these laboratories. This is because the study is based on what other people have found out about forensic procedures.

Things are changing fast. The laws we have today may become news soon because technology is moving forward so quickly. This means that the laws may not be able to keep up with all the technological changes that are happening all the time and that is a problem because laws about technology are really important and the laws we have now may quickly become outdated due, to constant technological innovation and rapid emerging changes.

There are things that the police do that we cannot know about because they are secret. Some of the things the police do like the way they investigate crimes using information are not available to the public. Confidentiality barriers are in place to keep these police procedures and intelligence-based investigations secret. This means that people, outside of the police department cannot access this information because of these confidentiality barriers.

1.6 Significance of the Study

This research is significant for several reasons:

1. Strengthening Criminal Justice

Rules for evidence are really important. They help the police and the court when they are trying to solve crimes that involve technology. Digital evidence rules make it more likely that the people who commit these crimes will be found guilty. This is because digital evidence rules help to make sure that the evidence is handled correctly and that it is used in a way that's fair. Digital evidence is a part of many crimes, like hacking and online fraud so having good rules is crucial.

2. Modernizing Legal Framework

The study gives us a look at the changes made to the Evidence Act in 2022. It checks if the 2022 amendments, to the Evidence Act are enough or if the Evidence Act needs changes.

3. Protecting Victims of Cybercrime

Women and children and vulnerable groups are often targeted on the internet and social media.

We need rules to figure out what really happened so we can get justice for women and children and vulnerable groups when it comes to cyber harassment and exploitation and financial crimes.

Women and children and vulnerable groups should be protected from cyber harassment and exploitation and financial crimes.

4. Supporting Judicial Consistency

The study looks at what the courts have said in the past to help people understand Sections 65A and 65B in the way. This is really important for Sections 65A and Sections 65B because it helps make sure everyone is, on the page when it comes to Sections 65A and Sections 65B.

5. Enhancing Forensic and Investigative Capacity

The findings can help the people who make policies to make the digital forensic infrastructure better. These findings are very useful for policymakers to improve the forensic infrastructure.

6. Contribution to Academic Research

This study is very important because it looks at the rules for using evidence in court in Bangladesh. The study gives an detailed review of how digital evidence is allowed in Bangladesh. It helps to answer some questions that people did not have answers to before about digital evidence, in Bangladesh.

1.7 Structure of the Thesis

This thesis is divided into seven chapters. Each chapter looks at a part of the study. The goal is to give an organized look at whether digital evidence is allowed in court in Bangladesh. The thesis examines the admissibility of evidence in Bangladesh in a thorough and systematic way. The study of evidence, in Bangladesh is the main focus of this thesis.

Chapter 1: Introduction

This part of the book is, about the background of the study. It tells us what the research problem is. The aims and objectives of the study are also talked about here. We find out what questions the study is trying to answer. The study has its limits. This part also explains what it can and cannot

do. It also says why the study is important. At the end it shows us how the rest of the thesis is organized.

Chapter 2: Literature Review

This chapter looks at what other people have written about evidence. It talks about how digital evidence has changed over time. The chapter also compares how the UK, India and the USA handle evidence. We see what scholars think about whether digital evidence's acceptable in court and if it is reliable. There are also studies that focus on evidence, in Bangladesh. The chapter finds out what is missing from what people have written about digital evidence.

Chapter 3: Theoretical and Legal Framework

This chapter is about evidence. It talks about what digital evidence's what it looks like. The principles of evidence law are also covered, including how relevant something's if it is real and if it is reliable. We will look at the Evidence Act 1872. See how it works. We will also talk about the changes made to this act in 2022. Digital evidence has rules that everyone should follow, like the Budapest Convention and the guidelines from the United Nations Office on Drugs and Crime which are often called the UNODC guidelines. These international standards are important, for evidence.

Chapter 4: Admissibility of Digital Evidence in Bangladesh

This chapter looks at the rules about evidence in the updated Evidence Act. It checks what judges think about evidence and what courts have said in the past. The chapter also talks about the rules for making sure digital evidence is real and, about signatures. It finds the problems that make it hard to trust evidence and keep it safe. The chapter also shows how forensic technology helps with evidence.[6]

Chapter 5: Problems and Challenges

This chapter is about the problems that people face when dealing with crimes. For example, many judges and lawyers do not have the technical skills to handle these cases. The cyber forensic infrastructure is also not very strong. There are concerns about privacy and how to protect people’s information. Sometimes it is hard to keep track of evidence which is a problem. The courts also take a time to hear these cases and there are many loopholes in the system that cause delays. The judiciary and legal professionals need to work on these issues to make the system better. The lack of expertise among the judiciary and legal professionals is a major issue. The weaknesses in forensic infrastructure are also a big concern. People are worried about their privacy and data

[6] Evidence (Amendment) Act 2022 (Bangladesh).

protection. The chain of custody issues is very important. The delays and procedural loopholes, in trial courts need to be fixed.

Chapter 6: Comparative and Reform Analysis

This chapter looks at how Bangladesh handles things and compares it to what India, the UK and the USA do. It tries to find the ways to make sure digital evidence is acceptable and trustworthy. The chapter also thinks about how the law in Bangladesh can be changed and how institutions can be made better specifically when it comes to evidence, in Bangladesh.

Chapter 7: Conclusion and Recommendations

This last part of the book talks about the things we found out. It looks at the changes made in 2022. Says what it thinks about them. The chapter also gives ideas for training judges, changing policies and making science better. It tells us what we should do next to learn more, about the 2022 amendments and forensic development and what we should research in the future about training and policy reform.

CHAPTER 2: LITERATURE REVIEW

2.1 Evolution of the Concept of Digital Evidence

The idea of evidence has changed a lot over time as digital technologies and information systems have grown really fast all over the world.

At first legal systems were set up to deal with evidence like papers what people say they saw and things you can touch.

When computers came along in the 1960s and the internet arrived in the 1990s digital evidence like emails and files became really important in court cases whether they were about crimes or disagreements, between people.[7]

Digital evidence is now a big part of both civil cases and digital evidence is used to figure out what really happened.

Digital evidence is basically any information that is stored or sent in form and can be used in court. This can be things like emails, digital pictures, videos, audio recordings and other types of data. We are talking about evidence from mobile devices, cloud storage and social media platforms.

[7] Information and Communication Technology Act 2006 (Bangladesh).

Digital evidence is different from types of evidence because it can be easily changed or destroyed. This means we need ways to collect, preserve and look at digital evidence. We have to be careful with evidence because it can be altered, copied or destroyed which is why we need to use special forensic techniques to handle it. Digital evidence is used to prove or disprove facts, in court. It is very important that we handle it correctly.

People who made laws had a time with electronic evidence because you cannot touch it. At first they wanted to make sure that the evidence they looked at in court was really what it said it was. They needed to know it was the thing. In the United States they changed the rules about what you can use as evidence in the 1990s. They made sure electronic records were reliable and honest. The United Kingdom and Australia did something. They made rules about what kind of evidence you can use from computers. They tried to balance what is possible with technology and what is fair in court. Electronic evidence is still a deal. The rules, for evidence are important.

The internet and mobile phones are everywhere now. This means that digital evidence is a bigger deal. Cybercrime is a problem all, around the world. Courts are seeing more cases of people stealing identities fake financial stuff bothering people online and even cyberterrorism. All of this shows that we really need some rules to make sure electronic evidence is real not messed with and handled properly. Digital evidence is a thing now and we need to deal with it.

The way digital evidence is changing is marked by three trends:

Expansion of digital sources: From simple computer files to cloud storage, social media, and IoT devices.

When it comes to technology things can get really complicated. The use of encryption, remote storage and distributed networks makes it necessary to have forensic methods for Technology. This is because Technology has become so sophisticated that it is hard to keep track of what's going on. The use of encryption in Technology requires methods to figure out what is happening. Also remote storage and distributed networks, in Technology need forensic methods to understand them.

Legal adaptation: Judicial recognition, statutory amendments, and international conventions to standardize admissibility.

Bangladesh has had to make a lot of changes to its laws. This is because of the way things are changing. The country has had to adjust its system. Recently in 2022 Bangladesh made some changes to the Evidence Act. These changes tell people how to prove that electronic evidence is real. They also say how to certify and present evidence in a court of law. The Evidence Act now has rules, for evidence.[8]

[8] Evidence (Amendment) Act 2022 (Bangladesh).

2.2 Comparative Perspectives: UK, India, USA

We need to look at evidence frameworks from different places to see what works best. This will help us understand what other countries are doing and find ways for Bangladesh to handle digital evidence too. Looking at what otherers doing will teach us a lot and help Bangladesh make good decisions, about digital evidence frameworks.

2.2.1 United Kingdom

The United Kingdom recognizes evidence because of laws and what the courts have decided. The Civil Evidence Act 1995 and the Police and Criminal Evidence Act 1984 are the laws that say what is allowed in court. These laws say that digital materials have to be real and not changed.

When it comes to computer records the courts want to make sure they are genuine. They need to know who had the records and where they came from. The courts also want to hear from experts who know about computers.

The United Kingdom courts always say that electronic evidence has to be reliable. They do not want any evidence that has been manipulated or is not real. The United Kingdom courts are very careful about what evidence they allow in court. Electronic evidence is very important, in the United Kingdom courts.[9]

2.2.2 India

The Information Technology Act 2000 in India along with some changes to the Indian Evidence Act 1872 gives us a set of laws for electronic evidence. These laws explain what electronic records and certificates are and how they should be checked to make sure they are real. This means that digital evidence can be used in court if everything is done correctly.[10]

The courts in India have looked at these laws closely and have made some important decisions about them. They have said that it is very important to have the certificates and to keep all the information about the electronic records, like who made them and when. They have also said that expert opinions are necessary to make sure the evidence is reliable and can be trusted. The Information Technology Act 2000 and the Indian Evidence Act 1872 are very important for evidence, in India.[11]

2.2.3 United States of America

In the United States of America the rules that courts follow to decide if they can use records as evidence are pretty important. These rules are called the Federal Rules of Evidence. There are also

[9] Civil Evidence Act 1995 (UK).
[10] Indian Evidence Act 1872 (India), ss 65A–65B.
[11] Information Technology Act 2000 (India).

laws in each state that say what can be used as evidence. When it comes to records the courts want to know if they are real if they are relevant, to the case and if they are reliable. This means that the people presenting the evidence have to show that the electronic records have not been changed or messed with in any way. The judges really care about getting opinions using the right methods to collect the evidence and keeping track of who has handled the evidence and when. The Daubert standard is also a deal because it helps the judges figure out if the methods used to collect and analyze the electronic evidence are reliable. The Federal Rules of Evidence and the Daubert standard are both crucial when it comes to evidence.

When we look at things from angles, we can see that everywhere in the world digital evidence is really important. Digital evidence must be completely trustworthy and honest. This means it has to meet high standards.

Bangladesh has made some changes recently. These changes are based on what other countries are doing. However, Bangladesh still has some problems to solve when it comes to putting these changes into practice. Digital evidence is still really important, in Bangladesh and other countries.

2.3 Scholarly Opinions on Admissibility and Reliability

When we talk about using evidence in court it is really complicated. Scholars point out that digital evidence is allowed in court not because of the laws that say it is okay but also because of how it was collected, preserved and checked by forensic experts. Digital evidence is only allowed if all these things are done correctly. Scholars say that the rules, for evidence are not the only thing that matters digital evidence also needs to be collected and preserved properly and then verified by forensic experts to make sure it is real.

Kerr says that digital data can be really unstable and that is why we need to be very careful about how we handle it. We have to keep a record of everything that happens to the data to make sure nobody messes with it. Casey thinks that making a copy of the data and using something called hashing is important to keep the data safe. He believes that judges need to understand how all this technical stuff works so they can make decisions about digital data. Kerr and Casey both talk about data and how we need to be careful, with it.

Some people who study the law think that the laws in Bangladesh were not good enough before they were changed in 2022. They think this because the judges did not always make the decisions and there were no clear rules to follow. Hoque and Akter say that the Bangladesh courts had a problem because they did not have the training and equipment to look at electronic evidence. This meant that the courts could not make decisions in cases that involved electronic evidence, like emails or text messages. The laws of Bangladesh and the way the courts work with evidence are still a problem.[12]

[12] *State v Md Rafiqul Islam* (unreported, Cyber Tribunal, Dhaka).

International scholarship also points out that it is really important to make digital evidence standards the same everywhere like they do in countries. This is especially true because cybercrime often happens across borders so digital evidence standards should be the same, as the practices that everyone follows especially when it comes to cybercrime.[13]

2.4 Studies on Digital Evidence in Bangladesh

Bangladesh has not had studies on this topic but that is changing. Rahman did a study in 2018 that looked at how the ICT Act affects the way we collect evidence. He found that there are some problems with the way we handle evidence in science. Ahmed wrote a paper in 2020 that said the courts in Bangladesh are not consistent when it comes to evidence. Sometimes the courts will accept prints without making sure they are real and other times they will reject evidence that is actually good because they do not understand the technology, behind Bangladesh digital evidence. Bangladesh digital evidence is an issue that needs to be studied more.

The Digital Security Act 2018 brought problems and chances for people. It made cyber crimes illegal. It also made electronic evidence official. The Evidence Act 2022 was changed recently to fix some issues.. Studies that look at real life situations show that there are still problems. The Digital Security Act 2018 and the Evidence Act 2022 are facing challenges. These challenges are, about having the technical skills, the right infrastructure and training judges properly. The Digital Security Act 2018 is still a part of this.

2.5 Identified Gaps in Literature

There are still some gaps even though a lot of research is being done on the subject of scholarship. Significant gaps exist:

Limited empirical studies in Bangladesh on the practical application of digital evidence in courts.

Scant analysis of judicial interpretation of Sections 65A and 65B since the 2022 amendments.

Insufficient comparative research linking Bangladeshi practices with global standards.

There are still a lot of problems with how forensic things handled that people have not looked into much in books and studies. Forensic handling has technical and procedural challenges that are not well understood. People do not talk about the challenges in forensic handling or the procedural challenges, in forensic handling as much as they should.

CHAPTER 3: THEORETICAL AND LEGAL FRAMEWORK

[13] *State v Unknown Accused* (Cyber Tribunal, Dhaka, 2023).

3.1 Understanding Digital Evidence: Nature and Characteristics

Digital evidence, which is also called evidence is information that is stored or sent in digital form. This information is important, for cases and can be used to prove or disprove things. Digital evidence is really important now because people use computers and mobile devices all the time. We also use cloud storage, social media and other digital platforms every day. Sometimes these are even used for criminal activity. Digital evidence is a part of legal systems today. The kinds of evidence are things, like emails, digital photographs and videos metadata, system logs, instant messaging and chat records, social media content, financial transactions, mobile GPS data and cloud storage files. Digital evidence can be photographs and videos it can be emails it can be metadata it can be system logs it can be instant messaging and chat records it can be social media content it can be financial transactions it can be mobile GPS data and it can be cloud storage files. Digital evidence includes these things.

The thing about evidence is that it is really different, from the usual papers or physical things we find. These differences are very important when it comes to using evidence in court keeping it safe and examining it closely with digital evidence. Digital evidence has its set of rules and digital evidence needs to be handled in a special way.

Volatility is a problem with digital data. This kind of information can be. Erased really easily. Sometimes this happens by accident when we update our systems or when we get a virus. It is not like a paper document that just stays the same. Digital evidence is different. We have to be very careful, with it so it does not get messed up. We need to handle it in a way to make sure it stays okay. Volatility of data is something we have to think about all the time.

The thing about evidence is that you cannot see it or look at it closely without using special tools. People who investigate and the courts have to use methods like making copies of the data using hashes or looking at the software to get to the digital evidence. This is because digital evidence, like evidence is not something that you can touch or see easily. Investigators have to rely on these methods to work with the digital evidence.

When we talk about replicability digital data is something that can be copied over and again without losing any of its quality. This is really helpful when we need to make backups or analyze the data. However it also makes it hard to figure out what the original digital data is and whether it is real or not. Digital data is easy to copy so we have to be careful when we are working with data to make sure we know what is real and what is not. The thing, about data is that it can be copied and this is a problem when we are trying to find out if the digital data is genuine.

We really need technology to work with evidence. This means we have to collect it store it and check it to make sure it is real. We need hardware, software and people who know what they are doing. If someone does not understand how the technology works it can cause problems with using the digital evidence in a case. Dependence on technology is an issue because collection, storage and verification of digital evidence are dependent on functioning hardware, software and technical

expertise. Dependence on technology can compromise the evidence if there is a lapse, in technological understanding.

Metadata is really important. The information that is embedded in files like when something was made and where it came from is very useful. This information includes things like the time something was made where it was made what device was used to make it and who made it. All of this information about metadata helps us figure out if something is real who actually made it and when it was made. Metadata provides evidence, about these things.

Digital evidence has some qualities that make it hard to deal with. If you do not collect or store evidence properly it may not be allowed in court because someone might have messed with it or accessed it without permission. So it is really important to follow the rules for handling evidence like keeping track of who has had it and using special codes to verify it to make sure digital evidence is reliable and trustworthy and that is why following these rules is crucial, for digital evidence.

Digital evidence is really important in cases. When the police investigate cybercrimes, they need to look at emails chat logs and the IP address to find out who did it. For example, when someone commits fraud, the police have to look at the digital records of transactions or the accounting records that are stored in the cloud. Mobile phones can give us a lot of information like where someone was who they called and what apps they used. This information can help prove if someone was really where they said they were or if they were planning something. What people post on media can also be used as evidence in cases of harassment, defamation and terrorism. Digital evidence like this is used in different types of cases including cybercrime investigations and financial fraud cases and it can be really helpful, in solving these digital evidence cases.

The way digital evidence is changing is also affected by the fact that the world is becoming more connected. When crimes happen in countries police from different places have to work together. This means that digital evidence has to be accepted by courts in countries, which is very important for police to do their jobs, around the world. Digital evidence is really important for police to solve crimes that happen in countries.

3.2 Principles of Evidence Law: Relevance, Genuineness, and Reliability

The rules for using evidence in a court of law are based on some basic ideas. These ideas are that the digital evidence has to be relevant, to the case it has to be real. It has to be reliable. Digital evidence must be relevant it must be genuine. It must be reliable to be used in a court of law. The core principles of evidence law that govern the admissibility of evidence are relevance, genuineness and reliability of digital evidence.[14]

3.2.1 Relevance

[14] Constitution of the People's Republic of Bangladesh, art 43.

Relevance is important because it helps evidence show something is true. Digital evidence is relevant if it helps prove something is true or not true about a claim. For example emails or chat logs can show what someone was thinking. If they agreed to something and this can be used in cases about contracts or crimes. Courts look at if the evidence is really helpful in figuring out the truth and if it is more helpful than it is hurtful and they do this with evidence too like digital evidence, from computers or phones. Digital evidence is relevant. It is used to help figure out the truth.

3.2.2 Genuineness

The digital evidence needs to be real. What it says it is. Courts want to know that the information has not been changed and that it comes from a source. To prove that the digital evidence is genuine we need to show where it came from make sure it has been handled properly and sometimes get an expert to talk about the systems used. There are rules like Section 65B of Indias Evidence Act and Bangladeshs Evidence Act that was updated in 2022 that make sure all of this is done correctly.

3.2.3 Reliability

The thing that makes evidence trustworthy is reliability. Courts want to know if the evidence was handled and looked at in the way. They check if it was kept safe collected properly and examined using methods that are widely accepted. You can tell if evidence is reliable by making a copy of it checking it with tools keeping track of what you do with it and having an expert say it is okay. For example, in the United States of America there is the Daubert standard that helps courts figure out if scientific evidence like evidence is reliable. Reliability of evidence is very important, in courts.

3.2.4 Doctrinal Perspectives

People who study this stuff say that digital evidence has to be handled in a specific way. This is so we can be sure that it is real and actually means something. Casey says that the way we collect and look at evidence is very important. If we do not do it correctly then the digital evidence is not really evidence all. We cannot be sure that it is genuine or that it can even be used in court. Kerr agrees with this. Says that we need to keep very good records of what happens to the digital evidence. This is because digital evidence can be changed on purpose or, by accident. Digital evidence is what we are talking about here. It is crucial that we get it right when it comes to digital evidence.

3.2.5 Challenges in Practice

The rules are simple. Courts have a lot of trouble using them. This is because digital evidence is often very complicated. Judges and lawyers do not always understand it. They can get things wrong when it comes to things, like metadata, encryption or cloud storage. This can mean that important

digital evidence is not used or that bad information is accepted. Digital evidence is a problem because it is so complicated. Courts have to deal with evidence all the time.

3.3 The Law of Evidence in Bangladesh (Evidence Act 1872)

The Evidence Act 1872 is still the law that deals with evidence in Bangladesh. This law was made a time ago before we had computers and the internet. It mostly talks about evidence that is written down on paper and what people say in court. The parts of the Evidence Act 1872 that are important, for evidence are:

Section 3–4: Definitions of relevant facts.

Sections 62–66: Secondary evidence and certified copies.

Section 67: Documents produced in evidence.

Before 2022 the courts in Bangladesh usually used examples of papers to decide if they could use digital records. This caused problems because the law did not clearly say how to make sure digital records were real who had them or if they were official. The digital records were a problem for the courts, in Bangladesh.[15]

3.3.1 Judicial Practice Pre 2022

Judges sometimes accepted things like screenshots and emails. Chat logs as proof.. They often needed other people to say it was true or for an expert to explain it. The problem was that there were no rules about what was allowed. This made it really unclear about things like signatures and information about when something was made and data that people stored online with services, like Google Drive or Dropbox. Judges had a time figuring out what to do with this kind of information.[16]

3.3.2 Complementary Legislation

The ICT Act 2006 and the Digital Security Act 2018 say that electronic records and cyber offences are things.. These laws do not clearly say how electronic evidence should be used in court. So lawyers often have to use reports, from experts or depend on what the judge thinks at the time to present evidence in court. The ICT Act 2006 and the Digital Security Act 2018 are still the laws that people look at when they talk about records and cyber offences.

3.4 Recent Amendments (Evidence Act Amendment 2022) and Their Implications

[15] Evidence Act 1872 (Bangladesh).
[16] Indian Evidence Act 1872 (India), ss 65A–65B.

The 2022 amendments made some changes, to the Evidence Act so it now clearly deals with evidence. The Evidence Act was updated by the 2022 amendments to include evidence.

3.4.1 Key Provisions

Section 65A: Defines electronic records and confirms their admissibility if produced according to prescribed procedures.

Section 65B: Introduces certification requirements to establish genuineness, requiring responsible officers to verify the origin, integrity, and accuracy of digital records.

3.4.2 Implications for Legal Practice

The courts have an understanding of what to do now because they have clear rules to follow. This means they do not have to compare things to documents as much as they used to. Judicial Clarity is really helping the courts make sense of things. They can just look at the Judicial Clarity rules. That makes it easier for them to make decisions.

Enhanced Reliability: Certification and expert verification safeguard against tampering.

When it comes to solving crimes investigators have to do things in a specific way. They need to follow the rules, for collecting evidence storing it and then presenting it. This is what we call Standardization. So investigators must follow these procedures for the collection of evidence the storage of evidence and the presentation of evidence.

3.4.3 Comparative Perspective

The new rules in Bangladesh are based on the IT Act from India in the year 2000. What is done in the UK.

The Indian law has sections called 65A and 65B.

These sections provide a foundation for deciding what evidence is allowed in court.

They say that people need to get a certificate and show that the evidence has not been changed.

In the UK people have to examine the evidence carefully and keep good records of who handled it and when.

Bangladesh made some changes in 2022 that are similar to what other countries do.

This shows that Bangladesh is following the rules as other countries.

Bangladesh's 2022 amendments are really, about following the principles that India and the UK follow, which is good because it means Bangladesh is doing things the way other countries do.

3.4.4 Remaining Challenges

It is really hard to put things into practice because judges and lawyers and law enforcement people do not have technical knowledge. We also have problems with our laboratories and the way we enforce the rules is not the same which makes it even harder to actually do things the way we are supposed to. The law enforcement and judges and lawyers are all having a time with this because of these issues, with the laboratories and the rules.

3.5 International Standards on Digital Evidence

3.5.1 Budapest Convention (2001)

The Council of Europe's Convention on Cybercrime is really important because it makes sure that people collect and store evidence in a lawful way. The Council of Europe's Convention on Cybercrime also says that countries should work together when it comes to evidence.

The Council of Europe's Convention on Cybercrime has rules for when countries need to work to investigate something that happened in another country. The Council of Europe's Convention, on Cybercrime wants to make sure that electronic evidence is real and not fake so it sets some standards for this.

3.5.2 UNODC Guidelines

The United Nations Office on Drugs and Crime Practical Guide on Digital Evidence tells us what we need to do to keep evidence safe and reliable. We have to follow steps and write down what we do with the digital evidence every time we touch it. The United Nations Office on Drugs and Crime Practical Guide on Digital Evidence also says we have to check the evidence very carefully to make sure it is real and can be used in court. This way the digital evidence from the United Nations Office, on Drugs and Crime will be good enough to use.

3.5.3 Interpol Recommendations

Interpol issues guidance for seizure, imaging, and storage of digital devices to maintain evidentiary value in multinational investigations.

3.5.4 Implications for Bangladesh

These standards are really important for Bangladesh. They helped shape the changes made in 2022. They give us an idea of how to improve the courts and the way things are done. If we follow what other countries are doing well it will make our system more trustworthy. It will also help us deal

with problems that come up when we need to get evidence from countries.. It will make our laws on cybercrime match up with what the rest of the world is doing which is a good thing, for Bangladesh and its cybercrime laws.

3.6 Summary

This chapter is about evidence in Bangladesh. It talks about what digital evidence's what it looks like. The chapter also looks at the rules of evidence law. It checks the laws of Bangladesh and what the courts are doing. The chapter sees how the changes made in 2022 are affecting things. It also looks at how Bangladesh's doing compared to other countries when it comes to digital evidence. Digital evidence, in Bangladesh is the focus of this chapter.

This framework is really important because it sets the stage for the rest of the book. The next chapters, like the one on if digital evidence is allowed in court (Chapter 4) the problems people face when trying to use evidence (Chapter 5) and how other countries handle digital evidence (Chapter 6) all rely on the framework developed here.

The digital evidence in the Bangladeshi system is looked at in a very detailed way in this chapter. It does this by looking at what the laws and rules say. Also what other countries are doing. This helps us understand evidence, in the Bangladeshi legal system in a complete way.

Chapter 4: Admissibility of Digital Evidence in Bangladesh

4.1 Provisions Governing Digital Evidence under the Amended Evidence Act

4.1.1 Historical Context and Need for Reform

The Evidence Act of Bangladesh was made a time ago before we had computers and other digital stuff. At first the Act said that only papers and things that were printed or written could be used as evidence. This included letters and other things that were written down. But now we have a lot of problems with cybercrime and people doing things online so the courts have to figure out if they can use things like emails from people records from phones, pictures from CCTV cameras, messages from social media and records from online banking as evidence. The Evidence Act of Bangladesh is still used today. It has to deal with things, like emails and social media messages.

When it comes to material courts usually used the basic rules of the Evidence Act to decide what to accept. For instance judges would sometimes look at printed emails or screenshots. Call them "documents" as stated in Section 3 of the original Act.. This way of doing things had its problems. There were issues with figuring out if something was real if it had been changed and who had control of it from start to finish especially when the original information was stored on a computer and could be altered. The digital material, like emails had to be genuine. The courts had to make sure of that.

The need for recognition became really important when we think about laws related to cybercrime like the Digital Security Act, 2018. This Digital Security Act, 2018 made things like hacking, identity theft and spreading digital content illegal. If we do not have rules under the Evidence Act then the evidence we collect in these cybercrime cases might not be allowed in court or could be questioned. This would not be good, for justice and the Digital Security Act, 2018 because it would make it hard to prove that someone did something.

4.1.2 Key Provisions of the Evidence (Amendment) Act, 2022

The Evidence Amendment Act, 2022 did something, about these problems. It made sure that digital evidence is part of the system. The main things it covers are:

4.1.2.1 Definition of Digital Record

Section 3 now says that a document is any kind of record. This means it includes all the data that is generated sent, received or stored on a computer. The digital record can be anything that's electronic. So the document is really any record that people use electronically.

The amendment is talking about things like footage from security cameras, information from phones emails that people send recordings of audio and video pictures taken by drones messages, on social media and other kinds of digital information. The amendment specifically mentions these things, including CCTV footage, mobile phone data, emails, audio video recordings, drone images, social media messages and other digital data.

The law says that forensic evidence like DNA and fingerprints and iris scans can be used in court. Forensic evidence is really important. Things, like DNA and fingerprints and iris scans are all types of evidence.

4.1.2.2 Sections 65A and 65B: Computer Generated Records

Section 65A says that digital records can be used as evidence if they follow the rules of Section 65B. This means that digital records are allowed to be proved in court long as they meet the requirements of Section 65B. The digital records have to be in line, with what Section 65B says in order to be considered valid.

Section 65B has some rules, for when Section 65B evidence's allowed in court. These rules do not need the thing to be shown. Section 65B says that some things must be done for Section 65B evidence to be okay. These things are:

The record has to be made available, from the people who are legally allowed to have it. The record must come from the people who have custody of the record.

The. System that is making the record has to be used all the time. The device or system must be something that people use every day. This is important, for the device or system that is generating the record.

The record should stay the way it is. We must not change the record or mess with it. The record is what it is. That is it. We have to keep the record the same. The record must not be. Manipulated.

This framework helps to cut down on arguments about whether something's real or not. It does this while still making sure that the right steps are taken. The framework is good because it reduces disputes, over the genuineness of things.

4.1.2.3 Digital Signatures and Authentication

When we talk about signatures, Sections 67A and 73A are really important. These sections say that the person using the signature has to be verified. If a court needs to check something they can ask for a Digital Signature Certificate, from a Certifying Authority. This is how digital signatures work. The Digital Signature Certificates are issued by Certifying Authorities. They help verify the user of the digital signatures.

Section 73B is a rule that lets people compare evidence and digital evidence to figure out who someone is. This means that physical evidence and digital evidence can be looked at together to establish the identity of a person. The main goal of Section 73B is to help investigators use evidence and digital evidence to solve cases.

4.1.2.4 Presumptions

Section 88A says that the message is what it says it is but it does not say who actually sent the Section 88A message.

Section 89A says that forensic evidence is thought to belong to the person it was taken from unless someone can prove that it does not belong to that person. This means that forensic evidence is linked to the person it was collected from unless there is proof that shows it is not theirs.

Section 90A says that digital records that are old are probably real if they have been kept properly. Section 90A is, about records that have been stored in a good way. If digital records are old and have been taken care of Section 90A assumes they are genuine. This is what Section 90A does for digital records.[17]

4.1.2.5 Expert Opinions

[17] Interpol, *Guidelines for Digital Forensics First Responders* (2020).

When it comes to the law opinions, from Certifying Authorities and forensic experts are really important now. These opinions are seen as facts that courts can trust. This means courts can use expert verification from Certifying Authorities to help them make decisions. Courts are now relying on the verification of Certifying Authorities and forensic experts to figure things out.

4.2 Judicial Attitudes towards Digital Evidence

4.2.1 Early Judicial Approaches in Bangladesh

Before the 2022 Amendment the Bangladeshi courts were really careful when it came to evidence. The judges usually stuck to what they knew which was the way of doing things with papers and documents. They would look at the situation. Listen to what experts had to say to figure out what was true. The Bangladeshi courts would do this by looking at the details, around the evidence. Some examples include:

CCTV footage: Admitted as corroborative evidence in property crime cases.

Mobile call logs: Used to establish an alibi or presence at a location.

Social media evidence: Accepted cautiously, with focus on verification of origin.

The court had some problems. One of the challenges was that there was no way to make sure judges were qualified to do their jobs. The judges also did not have technical knowledge. So the court often just decided what evidence to accept on its own. This meant that the court made decisions in similar cases. The challenges with the court included a lack of certification procedures for judges and limited technical expertise, among the judges.

4.2.2 Comparative Perspective: India

Indian courts provide examples that we can learn from:

The case of Anvar P.V. Versus P.K. Basheer in 2014 is very important. It says that only digital records that come with a certificate, under Section 65B(4) can be used as evidence without showing the original document. This means we do not need the original if we have the record and this certificate. The digital records of Anvar P.V. Versus P.K. Basheer are an example of this rule.

The court case of Arjun Panditrao Khotkar versus Kailash Gorantyal that happened in the year 2020 is an example. In this case the court said it is very important to produce the device or certificate. This is to make sure that everything is genuine. The court wants to see the thing, which is the original device or certificate to ensure that Arjun Panditrao Khotkar, versus Kailash Gorantyal case is dealt with properly.[18]

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

Bangladesh can do things to prevent arguments about whether something's real or not. They can make sure that things are done quickly and easily. Bangladesh needs to take steps like this to stop people from disagreeing about the authenticity of things. This will help Bangladesh to make things run smoothly like other countries do and this will be good for Bangladesh. Bangladesh will be able to make sure that everything is done properly and that there are no problems with the genuineness of things, in Bangladesh.

4.2.3 Comparative Perspective: United Kingdom

The courts, in the United Kingdom really depend on what experts have to say. They also use their own discretion. The UK courts need experts to tell them what they think about a case. This is how the UK courts work. They listen to the experts. Then they make a decision based on that and their own judgement. The experts give their testimony and the UK courts take that into account when they are deciding what to do.

Public Prosecution Service v Elliott & McKee [2013] UKSC 32: Expert verification of digital fingerprints and device data was sufficient for admissibility, even without statutory certification.

This way of doing things is about being flexible so courts can use evidence that is trustworthy without having to follow a lot of strict rules. The approach is really focused on flexibility, which helps courts to use evidence like the evidence from the case without having to deal with rigid technical formalities and this approach, with its flexibility is what makes it work.

4.2.4 Analysis

Bangladesh has to find a ground. Bangladesh needs to make sure that Bangladesh does not go far in one direction. This is really important for Bangladesh. Bangladesh must do what is best for the people of Bangladesh. Bangladesh has to think about what will happen if Bangladesh does not strike a balance. The people of Bangladesh are counting on Bangladesh to make decisions. Bangladesh is a country with a lot of potential. Bangladesh must use this potential to help the people of Bangladesh.

* Bangladesh has a lot of work to do

* Bangladesh must work hard to achieve its goals

Bangladesh will be a country if Bangladesh can strike a balance and make good decisions for the people of Bangladesh. Bangladesh is the key to a future, for the people of Bangladesh.

Ensure strict genuineness verification.

We should not be too strict about following rules when it comes to justice. The rules are there to help people get a deal so we must be flexible with them if that is what justice needs. Justice is what matters most not just doing things by the book. We have to make sure that justice is served even if that means bending the rules a bit. Justice is the thing we are trying to achieve here so we must do what is best, for justice.

Incorporate expert testimony and certification to enhance reliability.

4.3 Rules on Authentication, Electronic Records, and Signatures

4.3.1 Authentication of Digital Evidence

So authentication is really important because it makes sure that the evidence is real it has not been. We know who it belongs to. Key rules, for authentication are:

The police have to get evidence from someone who is allowed to have it. This means that digital evidence must come from someone who has the right to have it like the owner of a computer or phone. Digital evidence is very important. It must be produced from lawful custody.

Metadata and timestamps and device logs are really important to prove that something is real. We need metadata and timestamps and device logs to show that something actually happened. These things help us figure out if something is genuine or not. Metadata and timestamps and device logs are essential to verify the authenticity of something.

Courts can use analysis to make sure that the evidence is real and not fake. The forensic analysis helps courts confirm that the evidence has not been changed or tampered with. This is important, for the courts because they need to know that the evidence they are looking at is the thing and that is where forensic analysis of the evidence comes in to confirm the evidence integrity.

4.3.2 Electronic Records and Signatures

So when we talk about signatures we need to make sure they are real, under Sections 67A and 73A. To do that electronic signatures have to be checked by Certifying Authorities. This is how we validate signatures.

Section 73B is a rule that lets forensic experts connect signatures to the people who made them, which is the individuals. This means that digital signatures can be used to identify the individuals who signed something online. The forensic experts use Section 73B to figure out who made a signature and they can link it to the individuals.

Certificates that we get from the people who give these certificates are very important. They make things more believable. Certificates from these certifying authorities make the evidence stronger.

When we have a certificate from a certifying authority it means that the evidence is more reliable and trustworthy and that is why certificates, from certifying authorities are very useful.

4.3.3 Expert Testimony

Expert opinions are critical in the technical verification of evidence.

Courts are using forensic labs more and more to make sure things are true. They really need digital forensic labs to validate things. Digital forensic labs are very important, for courts.

4.4 Challenges in Ensuring Reliability and Integrity

4.4.1 Chain of Custody Issues

Maintaining evidence integrity is challenging:

Using lots of devices and platforms can be a problem. The more. Platforms you use, the more chance there is that someone will try to tamper with them. This is because multiple devices and platforms make it easier for people to mess with your stuff. So you have to be careful when you use devices and platforms.

When it comes to evidence we do not have a set way of handling it. This is a problem because it can make disputes even worse. The lack of procedures, for digital evidence handling is really the issue here. Digital evidence handling is something that needs to be done in a way.

4.4.2 Limited Forensic Infrastructure

Bangladesh does not have digital forensic labs that are accredited. The number of forensic labs, in Bangladesh that are accredited is really small. Bangladesh has a few accredited digital forensic labs.

We do not have trained people to do the analysis properly. This is a problem because the people we have are not able to do the job correctly. The shortage of trained personnel is what limits our ability to do an analysis of the situation.

4.4.3 Technological Complexity

Advanced technologies like encryption, deepfakes, and blockchain complicate authentication.

The courts have to depend on experts to explain things. This is because the courts need expert interpretation to make sense of issues. The courts must rely on expert interpretation to get it right.

4.4.4 Legal and Privacy Concerns

The Digital Security Act of 2018 and the fact that we do not have any laws to protect peoples information make it really tough to collect evidence. When we talk about the Digital Security Act of 2018 it is clear that it affects how we gather evidence. The Digital Security Act of 2018 has an impact, on this process.

The courts have to make sure they are fair to peoples privacy rights and the need for evidence, in a case. Courts need to balance the privacy rights of individuals and the evidentiary needs of the system. This means that courts have to think about how to protect peoples private information while also making sure that the legal system has the evidence it needs to work properly. The courts must get this balance right so that peoples privacy rights are respected and the legal system can do its job.

4.4.5 Presumption Limitations

People who do not understand technology can be taken advantage of under Sections 88A–90A because they do not know how things work. Sections 88A–90A are rules that can be misused if someone is not good, with technology. This is a problem because people who are not technical can get into trouble under Sections 88A–90A.

Judges and lawyers really need to learn how to understand presumptions. This is very important for Judges and lawyers to get it right when it comes to presumptions. They have to be trained so they can make decisions, about presumptions. Judges and lawyers must know what presumptions mean so they can do their jobs properly with presumptions.

4.5 Role of Forensic Technology

4.5.1 Evidence Preservation

Use of write blockers and forensic imaging to prevent alteration.

Documentation of the chain of custody is mandatory.

4.5.2 Analysis Techniques

So we have things like metadata extraction and hash verification that help make sure our evidence is real. These things along with checks are important, for keeping our evidence safe and making sure it is not changed. Metadata extraction and hash verification and these cryptographic checks all work together to ensure the integrity of the evidence.

Recovering deleted or damaged files is really helpful. This is because it makes the files more useful as evidence. Reconstruction of deleted or corrupted files makes them more valuable, to us. We can

learn a lot from these files when we recover them. Reconstruction of deleted or corrupted files is very important.

4.5.3 Expert Reporting

The reports that are detailed have a lot of information. They tell you about the methodology that was used. They also tell you about the steps that were taken to verify things.. They have integrity checks too. These detailed reports really give you a lot of details about what was done. The methodology in these reports is important. So are the verification steps and integrity checks, in the reports.

People who know a lot about something, like experts help explain things that're hard to understand, such as complex technical processes and these experts testify to make complex technical processes clearer. Experts are good, at explaining technical processes.

4.5.4 Capacity Building

Training for law enforcement, prosecutors, and judges is essential.

The development of labs and standard operating procedures makes sure that everything is consistent. This is because accredited labs and standard operating procedures help to keep things the same. Accredited labs and standard operating procedures are very important, for this reason.

4.5.5 Technological Innovation

The use of blockchain based logging can help make sure that digital records are real. Blockchain based logging is a way to verify the genuineness of digital records. This is because blockchain based logging keeps a record of all the changes made to records.

AI tools can find out when someone is trying to manipulate things, which makes the court feel more confident in the decisions they make. The court has faith in the decisions because AI tools help detect manipulation of evidence and other things. This is important, for AI tools to detect manipulation so that the court can trust the information they are given.

The Evidence Act that was changed in 2022 is a deal, for Bangladesh. It makes the countrys laws work better with the world. To really make the most of this law:

We need to make sure the laws are clear. At the time the judges have to really understand the laws. This is very important, for the laws and the judges because legislative clarity and judicial understanding go hand in hand. We are talking about clarity and judicial understanding. They have to work for things to make sense.

You can really trust the analysis because it is done by experts. The experts make sure that the forensic analysis is reliable.

We can learn a lot from India and the United Kingdom. The lessons from India and the United Kingdom give us a step by step guide, on how to do things. India and the United Kingdom have a lot to teach us about how to get things done.

Training, infrastructure, and technological adoption are essential for the sustainable use of digital evidence.

Chapter 5: Problems and Challenges in Digital Evidence Admissibility in Bangladesh

5.1 Lack of Technical Expertise in the Judiciary and Legal Community

5.1.1 Judicial Knowledge Gaps

The criminal justice system in Bangladesh is facing a problem. This problem is that the judges in Bangladesh do not have the technical knowledge. The Evidence Amendment Act of 2022 says that digital evidence is allowed in court. However the judges in Bangladesh often have a time understanding the forensic reports, digital signatures, metadata and device logs from digital evidence. The judges need to know more about evidence to do their job properly. The criminal justice system, in Bangladesh needs to find a way to give the judges the knowledge they need to understand digital evidence.

Judges have to deal with CCTV videos and mobile phone data. The thing is, they may not know enough to figure out if a CCTV video has been messed with or not. They also may not know if a mobile phone log is correct when it shows where a suspect was. This is a problem because Judges need to know if the CCTV video and mobile phone data are real or not. Judges have to make decisions based on this kind of information so they need to be sure it is correct. The CCTV videos and mobile phone data are important. Judges may not have the knowledge to understand them properly.

Encryption challenges are a problem. In cases of fraud and cybercrime encryption makes it really tough to understand what is going on. This is because people use encrypted communications or secure messaging apps to talk to each other. These encryption things make it hard to figure out what people are saying without having some skills. Encryption challenges, like these are very tricky to deal with.

Here is a case that happened in a court. It was the Dhaka Cybercrime Court. It took place in the year 2023. The judge had some doubts, about WhatsApp chat logs being used as evidence. The judge did not really understand what metadata is. This caused some problems. The case got delayed. The court had to postpone the case times. The WhatsApp chat logs were the thing the judge was questioning. The judge was not sure if WhatsApp chat logs were reliable because of the metadata issue.

5.1.2 Limitations of Legal Practitioners

Lawyers have a time dealing with digital evidence. They need to know if the evidence is real or not. For this they have to ask the questions. Lawyers need to understand things like computers and phones to do this. They need to know about methods and how to check if something is real like a hash verification or device authentication. This is important for lawyers to do their job, which's to question the other side or what we call cross examination, when it comes to digital evidence like emails or messages on a phone. Lawyers need to be good, at this to figure out what is going on with the evidence.

When we do not ask the questions to forensic experts it can cause problems. We might misunderstand what they are saying. We might rely too much on the certificates they give us. This is not good because forensic experts are talking about the experts. The forensic experts and their certificates are very important. We need to ask the experts the right questions so we can understand what the forensic experts are saying.

The defense or the prosecution may lose an advantage if they are unable to challenge the data that has been manipulated or the data that is not reliable. The defense or the prosecution need to be able to challenge this kind of data because it can be very bad, for their case. If the defense or the prosecution cannot challenge the manipulated data or the unreliable data they may not win the case.

In India the Supreme Court says that people need to verify certificates under Section 65B of the Indian Evidence Act.. The thing is, even lawyers in India do not always ask the right questions about technical reports. This shows that Indian lawyers need to keep learning and training all the time. The Supreme Court and the Indian Evidence Act are very important so Indian lawyers need to understand them well. This is especially true when it comes to reports and certificate verification, under Section 65B of the Indian Evidence Act.

5.1.3 Proposed Solutions

Mandatory technical workshops and certification programs for judges and lawyers.

Collaborative programs with universities and cybersecurity institutes.

Development of guidelines for technical cross examination and evaluation of digital evidence.

5.2 Weaknesses in Cyber Forensics Infrastructure

5.2.1 Limited Accredited Forensic Labs

Bangladesh does not have a system for cyber forensics. This is an area for them. Now there are only a few labs that the government says are okay to do digital forensic work. These labs are very important for Bangladeshs forensic infrastructure, which is still, in its early stages. Bangladeshs cyber forensic infrastructure is not strong because it is still growing.

Backlogs in processing evidence delay trials.

Some labs use software or they have to check things by hand which makes them less reliable. This means the labs that use software or manual verification processes are not as trustworthy as they should be. The thing is these labs are using software or they are checking things manually and that is what reduces their reliability.

Sometimes cases are sent to countries, which increases the costs and makes people wonder if everything is really legitimate. Cases like these can be a problem because they are sent abroad and that raises questions, about the genuineness of cases.

Case Example: Something big happened in Dhaka in 2022. There was a cyber fraud case. The police had some bank records that were encrypted. This means they were secret and could not be read. These records had to be sent to a lab in India. The people at the lab could read the records.. It took a long time to get the records to India and to get the results back. This caused a delay of six months in the court case. The trial had to wait for the results from India before it could move forward. The cyber fraud case, in Dhaka was delayed because of the encrypted bank records.

5.2.2 Equipment and Technological Deficits

Forensic labs usually have things, like write blockers that're up to date tools that help them make copies of computer data and systems that use blockchain to verify things are real. These forensic labs also use blockchain based verification systems to make sure everything is correct. They have write blockers and forensic imaging tools that help them do their job.

Cloud storage and encrypted communications these things are really hard to check without tools. We need equipment to make sure cloud storage and encrypted communications are working like they should. Cloud storage and encrypted communications are very tricky to figure out on our own.

5.2.3 Staffing and Training Challenges

There is a shortage of trained experts. This means that the people who are doing this job have a lot of work to do. The workload is not balanced. That is why it takes a long time to get the results. The forensic experts are very important. We need more of them to do the job quickly. The shortage of trained experts is a big problem that causes delays.

Investigators do not have experience with new technologies. This makes it hard for them to find evidence keep it safe. Make sure it is real. The investigators need to know about emerging technologies, like these so they can do their job better and work with evidence from emerging technologies.

5.2.4 Comparative Insights

In India the people who investigate cybercrimes get help from the Cyber Crime Coordination Centre. This centre does an important job. It looks at the evidence from cybercrimes in a detailed way and gives expert technical advice to the investigators. The Cyber Crime Coordination Centre is like a place where all the cybercrime investigation units can go to get the help they need. The Cyber Crime Coordination Centre provides this help to the cybercrime investigation units, in India.

The United Kingdom has a team called the National Cyber Crime Unit. This team has people who're really good at figuring out crimes that happen on computers. They are very skilled at looking at evidence and solving problems. Bangladesh could do something like this too. If Bangladesh had a team, like the National Cyber Crime Unit it would be really helpful. The National Cyber Crime Unit would help Bangladesh get better at dealing with computer crimes and working together with teams.

5.3 Privacy and Data Protection Concerns

5.3.1 Legal Gaps in Data Protection

Bangladesh does not have laws to protect peoples personal information like the European Union has with their GDPR law or like India has with their Personal Data Protection Bill. Bangladesh really needs laws like these to keep peoples information safe. The laws that Bangladesh has now are not enough to protect peoples data, like the GDPR law or the Personal Data Protection Bill do. Bangladesh needs data protection laws to keep peoples information safe.

When we collect evidence like phone records, emails and things we post on social media it can be a problem if we do it the wrong way. Digital evidence collection can be bad if it is not done correctly. This is because digital evidence collection can affect our right to privacy. So we have to be careful, with evidence collection to make sure it does not violate our privacy rights.

The Constitution has rules that protect our privacy like Article 43. This means we have the right to privacy.. The problem is that there are not enough specific rules to explain how this works. So people are not really sure what is legal and what is not when it comes to privacy. This is because

of the lack of regulations. The Constitution and Article 43 are supposed to guarantee our privacy. Without clear rules there is a lot of confusion, about what this really means for our privacy.

5.3.2 Risks of Abuse

When the government spies on people without permission or collects much information about them it can make people lose faith in the legal system. This is a problem because people need to feel safe and know that their personal information is protected. Unauthorized surveillance and the, over collection of data are serious issues that can undermine trust in the legal system and make people question its fairness.

When people are looking into something they might see information that's not really related to what they are trying to find out. This can cause problems with the law because Investigators may have seen things they should not have and that can lead to challenges, for the Investigators and the investigation itself.

This is a case where something went wrong. In 2021 people in Bangladesh started a project to watch what was happening on media.. Then they collected personal information about people that had nothing to do with any crime. This is a problem because it is not right to collect information about people without a good reason. It also raises questions about privacy. The social media monitoring project in Bangladesh is an example of this. The people in charge of the social media monitoring project in Bangladesh collected data that was not related to any criminal case and this caused ethical and privacy concerns about the social media monitoring project, in Bangladesh.

5.3.3 Proposed Solutions

Enact comprehensive data protection legislation with clear rules on collection, retention, and destruction.

We need to make sure that the courts are watching to see that the police collect evidence in a way and follow the law. The police should only collect evidence that's really necessary and they should do it by the book. This is what judicial oversight mechanisms are, for to ensure that evidence is collected proportionally and lawfully so that the judicial system can work properly with the evidence that the police collect in an proportional way.

Adoption of privacy by design principles in forensic investigations.

5.4 Issues of Chain of Custody and Hacking Risks

5.4.1 Maintaining Integrity

The chain of custody is really important because it makes sure that digital evidence is kept safe and remains the same as when it was found. However Bangladesh has a lot of problems to deal

with such, as the chain of custody and these problems are making it hard for the chain of custody to work properly in Bangladesh.

Lack of standardized documentation for handling digital devices.

When evidence goes from one person to another like from investigators to labs and then to courts it is easier for someone to mess with the evidence. This is because the evidence is being handled by many people it is harder to keep track of what is happening to it. The times the evidence is transferred the more chance there is that someone will tamper with it. This is a problem because evidence is very important in courts and labs and it needs to be kept safe so that it can be trusted. Transfers of evidence, between investigators and labs and courts need to be done to prevent tampering.

Here is a case that really shows the problem. In a cybercrime case in Dhaka the police had an issue with the logs from a device. These logs did not match up. That caused a big problem. The court did not accept some important evidence because of this issue. This meant the trial had to be delayed for months. The cybercrime case, in Dhaka is an example of what can go wrong when device logs are confusing.

5.4.2 Hacking and Cybersecurity Threats

Digital evidence is vulnerable to unauthorized access, malware, or remote hacking.

Law enforcement agencies have cybersecurity protocols that're not strong enough. This can be a problem because it can hurt the integrity of forensic evidence. The integrity of evidence is very important, in law enforcement agencies. When law enforcement agencies have cybersecurity protocols it can compromise forensic integrity.

5.4.3 Proposed Solutions

We need to use blockchain to keep a record of how thingsre handled. This way we can make sure that the record is secure and nobody can change it. We will use blockchain based logging to document everything that happens. This means that blockchain will be used to keep a record of all the handling that takes place.

Use encrypted storage, multi factor authentication, and access control.

Regular audits and certification of labs and investigators.

5.5 Delay and Procedural Loopholes in Trial Courts

5.5.1 Judicial Delays

Court backlogs are a problem because they make digital evidence less useful. The digital evidence is not as good when it is old. Court backlogs really hurt the value of evidence.

When trials are delayed it is more likely that the information we need will not be good anymore. This can happen because the people who were going to be witnesses might not be available anymore. Also the technology we are using for the trial might be old. Not work properly by the time we get to court. Delayed trials can cause a lot of problems, like data degradation, witness unavailability or technical obsolescence. That is why delayed trials are a big issue.

5.5.2 Procedural Loopholes

Lack of standardized procedures for submitting, authenticating, and cross examining digital evidence results in inconsistent rulings.

Lawyers take advantage of loopholes, in the system to question whether something is real or to hide evidence. They do this by finding weaknesses in the way things are done and using those weaknesses to challenge the truth of something or to keep evidence from being seen. Lawyers use these loopholes to their advantage when they want to challenge the genuineness of something or suppress evidence that could be used against them.

5.5.3 Proposed Solutions

Specialized cybercrime courts with trained judges and staff.

Standardized rules of procedure for digital evidence handling and submission.

Integration of alternative dispute resolution for minor cyber disputes.

5.6 Case Studies and Comparative Analysis

5.6.1 Bangladesh Cybercrime Case Studies

Dhaka Bank Fraud Case (2022): Delays in forensic analysis due to inadequate labs.

In the year 2023 there was a problem with WhatsApp Evidence Dispute. The judges had a time understanding the WhatsApp metadata. They really struggled to figure out what the WhatsApp metadata meant. This was an issue, for the judges and the WhatsApp Evidence Dispute.

Lessons: Need for technical training, lab infrastructure, and procedural clarity.[19]

5.6.2 Comparative Perspectives

[19] *State v Md Rafiqul Islam* (unreported, Cyber Tribunal, Dhaka).

In India they have something called Section 65B certificates. These certificates are really helpful when it comes to evidence in court cases. They also have centralized cyber labs which make it easier for evidence to be accepted in court. This is a deal for India because it means that evidence from computers and other electronic devices can be used to prove things in court. Section 65B certificates are important, for this process.

In the United Kingdom the National Cyber Crime Unit makes sure that evidence is looked at carefully by experts. The National Cyber Crime Unit is really good, at analyzing evidence because they have experts who know what they are doing. The National Cyber Crime Unit and their experts work together to make sure the evidence is correct.

The European Union has a law called the General Data Protection Regulation or the GDPR for short. This law, the GDPR gives people in the European Union rules about how their personal information is protected. At the time the GDPR allows the police and other authorities to use digital evidence in a lawful way when they need to. This means that the GDPR is very good, at balancing the need to protect peoples information with the need to allow the police to use digital evidence when they are investigating a crime all while following the rules of the GDPR.

5.7 Recommendations

Capacity Building: Technical training for judges, lawyers, and investigators.

Infrastructure Development: Modern forensic labs with certified experts.

Legal Reform: Comprehensive data protection laws and procedural rules.

Chain of Custody Improvements: Blockchain, encryption, and auditing.

We need Specialized Courts that have Cybercrime benches. These Cybercrime benches can handle evidence in a faster and more expert way. This will help with Cybercrime cases because Cybercrime is a problem that requires special attention from the courts. Having Cybercrime benches will make it easier to deal with evidence, in Cybercrime cases.

Bangladesh has a lot of problems when it comes to using evidence in court. The main issues are that people do not have the skills the systems in place are not good enough there are concerns about privacy there is a risk of hacking and things take a long time to happen.

To fix these problems Bangladesh needs to make changes to its laws train its judges improve its equipment for looking at evidence and start using new technology. It can learn from what India, the United Kingdom and the European Union're doing.

If Bangladesh makes these changes digital evidence will be believable, more reliable and more effective in court. Digital evidence will become a valuable tool, for Bangladesh. Bangladesh will be able to use evidence in a better way.

Chapter 6: Comparative and Reform Analysis

6.1 Lessons from India's Information Technology Act and Evidence Law

The law for evidence in South Asia has been shaped by what happened in India. This is because the legal systems of India and Bangladesh have a lot of similarities. India started to update its rules for evidence before Bangladesh did. India made changes to its laws with the Information Technology Act 2000. Updates to the Indian Evidence Act 1872. This gives Bangladesh some lessons. Bangladesh can learn how changes to laws court involvement and technical expertise can all work together. This helps to make sure that digital evidence is accepted and trustworthy in Bangladesh just like it is in India, with the Indian Evidence Act 1872 and the Information Technology Act 2000.

6.1.1 Section 65B of the Indian Evidence Act: A Foundational Framework

India has made a contribution, to digital evidence rules. One of the important things India has done is add Section 65B to the Indian Evidence Act. This was done by changing the IT Act 2000.

Section 65B says:

The admissibility criteria for electronic records;

Certification requirements; and

The presumption of integrity and genuineness of electronic documents produced in court.

The section says that electronic records can be used as evidence. These electronic records may be allowed in court if certain conditions are met. One of these conditions is that there must be a certificate issued under Section 65B(4). This certificate is important because it confirms that the electronic record was made properly. It also confirms that the device used to make the electronic record is working correctly and that the copy of the record is accurate. The electronic records are very important in this case. The certificate helps to prove that they are real. The certificate is, like a guarantee that the electronic recordsre genuine and that they can be trusted.[20]

Bangladesh has just started to make rules through the Evidence Act that was changed in 2022.. Indias court system shows us what is good and what is bad about having strict rules for certifying

[20] Indian Evidence Act 1872 (India), ss 65A–65B.

things. The Indian Supreme Court made an important decision in the case of Anvar P.V. Versus P.K. Basheer in 2014. They said that digital evidence is only allowed in court if it has a Section 65B certificate. This decision changed the way digital evidence is used in courts over India. It made getting this certificate a step that everyone has to follow. The Evidence Act is still being used in India and Bangladesh is following the path, with the Evidence Amendment Act 2022.

6.1.2 Judicial Evolution: From Anvar to Arjun Panditrao

The Indian courts had a time with Section 65B at first. This law was very strict. The Anvar ruling helped clear things up. It also made things difficult in practice. This was especially true for people who could not get a certificate from companies like media platforms or telecom operators.

In the case of Shafhi Mohammad v. State of Himachal Pradesh in 2018 the Supreme Court tried to make things easier. They said that people who did not have control, over a device did not need to get a certificate. This was the Supreme Courts way of relaxing the rules of Section 65B. The Indian courts and Section 65B are still being figured out.

In the case of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal that happened in 2020 a bigger group of judges went back to the interpretation of Anvar. They said that the rules for certificates are really important and must be followed, unless the original device is shown in court. This case made it clear again that there are steps in place to make sure things are real and trustworthy these steps are like safeguards for the procedure the Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal case is an example of this. The judges in Arjun Panditrao Khotkar, v. Kailash Kushanrao Gorantyal made sure that the rules are clear and that everyone knows what to do.[21]

6.1.3 Relevance for Bangladesh

Indias experience with evidence is a good example. The law alone does not guarantee that digital evidence will be used successfully. The courts have to interpret the law. The institutions have to be capable of handling digital evidence. This is very important.

Bangladesh made some changes to its Evidence Act in 2022. This amendment allows electronic records to be used as evidence. However the rules are not very clear. They do not have procedures, like Indias Section 65B. Digital evidence is a thing and digital evidence is something that needs to be handled carefully. Indias digital evidence and Bangladeshs digital evidence rules are not the same.

Indian law says that Bangladesh should:

Provide precise evidentiary guidelines, including certification mechanisms;

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

We need to teach train judges and prosecutors about chains of custody so they can understand it. This is important for train judges and prosecutors to know about chains of custody. Train judges and prosecutors have to learn what digital chains of custody are.

Establish cooperation frameworks with telecommunications and digital service providers.

India is an example of what can go wrong when we make rules that are too strict. Bangladesh needs to make sure it finds a balance between being honest and realistic especially when it comes to things like Facebook or WhatsApp from countries. Bangladesh has to think about how to deal with platforms, like Facebook or WhatsApp in a way that is fair and works well for everyone.

6.2 Approaches in UK and US Courts on Digital Evidence

The United Kingdom and the United States have been really important in figuring out what digital evidence is about.

They have some ideas, about making sure digital evidence is real and trustworthy.

The United Kingdom and the United States also have rules to make sure everything is done fairly.

These things can help Bangladesh make some changes to their own systems for dealing with digital evidence.[22]

6.2.1 The UK Approach: Focus on Reliability and Judicial Discretion

The United Kingdom does not depend on one law that covers all digital evidence. Instead the rules for what can be used as evidence are decided by looking at lots of different things, such, as:

The Police and Criminal Evidence Act (PACE) 1984,

The rules of law say that evidence has to be real and relevant. Common law rules are very specific about this. For example common law rules require that evidence be genuine and have something to do with the case. The common law rules are, in place to make sure that real and relevant evidence is used.

Judicial discretion guided by case law.

Under PACE we think that documents made by computers are correct unless someone can prove they are not. This means that if someone wants to challenge these documents they have to show that the computer system made a mistake. The courts, in the UK want the person who is using

[22] *Public Prosecution Service v Elliott and McKee* [2013] UKSC 32.

evidence to prove that the computer system that made the record was working the way it should. They have to show that the PACE system was working properly when the documents were made by the computer.

There are cases like R v. Shephard from 1993 that helped figure out how to make sure digital records are real.

What is important is that the computer system was working right and that there were safeguards in place.

The main thing is that the process is reliable not that it has some kind of certification. R v. Shephard is an example of this it shows that R v. Shephard is, about making sure digital records are trustworthy.

This way of doing things is good, for lawyers because it is flexible and does not have a lot of rules but it still checks digital evidence very carefully. For Bangladesh this means that judges need to be able to make decisions and consider what is reasonable when it comes to digital evidence because technology is changing very quickly.

6.2.2 The US Approach: Flexible Standards with Strong Procedural Infrastructure

The United States does things a bit differently. They follow the Federal Rules of Evidence. The rules that are important here are Rules 401 which's about relevance Rule 901 which is about making sure something is real and Rule 803 which is about when someone can talk about what they heard from someone else. The United States uses these rules to figure out what evidence is allowed in court. The Federal Rules of Evidence are like a guide, for the United States. They help the United States decide what is relevant and what is not.

When it comes to evidence it has to be real. Under Rule 901 digital evidence can be used in court when there is proof to show that the item is really what the person who is presenting it says it is. So US courts use different methods to make sure digital evidence is authentic including:

Metadata analysis;

Expert testimony;

Hash value comparison;

Witness testimony from operators of digital systems;

There are exceptions to business records. These exceptions can affect business records. Business records are not always the same because of these exceptions. The exceptions, to business records can be different. Business records have to deal with these exceptions.

The case of Lorraine v. Markel American Insurance Co. That happened in 2007 is an example. This case gives us a lot of information about what courts think about evidence. It tells us how to figure out if digital evidence's real and if we can trust it. The case also talks about things like hearsay. If the original writing is needed. It even explains how to balance things according to Rule 403. The Lorraine, v. Markel American Insurance Co. Case is very helpful when it comes to evidence.

The United States experience shows that digital forensics laboratories are really important. This is because many states in the United States need evidence that has been checked by forensic examiners. These examiners follow the rules set by the Scientific Working Group on Digital Evidence also known as SWGDE. The digital forensics laboratories and the certified forensic examiners play a role in this process. They help make sure that the digital evidence is handled correctly and that it is reliable. The United States experience with forensics laboratories and certified forensic examiners is a good example of this. Digital forensics laboratories are essential, for checking evidence.

6.2.3 Comparative Insights for Bangladesh

The United Kingdom and United States models show that:

The law, about evidence needs to be able to change easily. Digital evidence law has to stay flexible so it can keep up with things. Digital evidence law must remain flexible because it is always changing.

We need to make sure the process is reliable. This is more important, than getting a certification that says everything is okay. The reliability of the process is what really matters, not just having a piece of paper that says it is certified.

Courts really need to understand technology. This is very important, for the courts. The people who work in the courts need to know about things. Courts need literacy so they can make good decisions about technology.

Strong forensic infrastructure is essential;

Having guidelines for what to do really helps to stop lawsuits from taking a long time. Clear procedural guidelines make it so that lawsuits do not get held up for a time. This is because clear procedural guidelines are very important, for the lawsuit process.

Bangladesh can learn from these examples. They can make a system that takes the things from India, where the laws are clear and the good things from the United Kingdom and the United States, where the processes are flexible. Bangladesh can build a model that combines these two things, which is clarity of laws and flexibility of processes to make something that works well for

Bangladesh. Bangladesh needs to find a way to make a system that has laws like India and flexible processes, like the United Kingdom and the United States. This hybrid model can help Bangladesh.

6.3 Best Practices for Admissibility and Reliability

To make sure that digital evidence is acceptable and trustworthy we need to balance the technical and institutional aspects.

When we look at what other countriesre doing we find some good ways that Bangladesh should think about.

These are the things that many people, around the world consider to be the ways to handle digital evidence. Bangladesh should consider these evidence practices.

6.3.1 Clear statutory definitions

Digital evidence laws must have definitions of digital evidence. The laws need to say what digital evidence is. Digital evidence laws have to make sure everyone understands what digital evidence means. This is important for evidence laws.

* Digital evidence

* The rules for evidence

* How to handle digital evidence

These are all things that digital evidence laws have to be clear, about. Digital evidence laws need to be simple so people can understand them. Digital evidence is a part of digital evidence laws.

Electronic record;

Computer output;

Digital signature;

Hash values;

Metadata.

The IT Act of India has some examples that we can look at.. The definitions that Bangladesh is using right now are not detailed enough. The definitions of Bangladesh need to be more detailed. The IT Act of India is a reference point, for this.

6.3.2 Chain of custody and integrity preservation

A reliable chain of custody includes things like making sure that evidence is handled correctly.

This means that the people who are in charge of the evidence they have to be very careful, with it.

A reliable chain of custody includes:

* Keeping track of who has the evidence at all times

* Making sure that the evidence is stored in a place

A reliable chain of custody is very important because it helps to prove that the evidence is real and that it has not been tampered with.

A reliable chain of custody includes being able to say where the evidence was and who had it from the time it was found to the time it is used in court.

This is what a reliable chain of custody includes.

Proper seizure procedures;

Forensic imaging;

Secure storage;

Hash value verification;

Documentation of handling.

The United States and some other countries have strict rules about handling evidence. If these rules are not followed the evidence may not be allowed in court. Bangladesh does not have the rules everywhere in the country, which is a problem. The United States and other countries, like it have to follow these rules but Bangladesh still has a lot of work to do to get its rules in order especially when it comes to the chain of custody of evidence.

6.3.3 Certification or authentication pathways

Good ideas for security include giving people a few ways to confirm who they are with authentication. This means people can use methods, for authentication. Authentication is a part of keeping things safe and secure. So companies should really think about using types of authentication.

Certificates (India style);

System operator testimony (UK style);

Forensic examiner verification (US style).

Bangladesh does not have a system that can adapt to situations. This means that it takes a time to get certificates from other countries. Bangladesh needs a system to make this process faster. The current system of Bangladesh is not flexible. It is hard to get certificates from foreign platforms, which causes a lot of delays, for Bangladesh.

6.3.4 Judicial training and special cyber benches

Judges need to keep learning things in:

Metadata interpretation;

Device forensics;

Cloud storage systems;

Social media evidence.

India has set up schools to teach people about cyber things. The UKs Judicial College has classes that teach about evidence. In Bangladesh judges usually only look at the reports that the police make using computers. This is a problem because it can lead to decisions in court. The judges in Bangladesh are using these police reports from computers, which's not a good way to get accurate information and this can cause problems with the judicial findings, in Bangladesh, where the judges are relying on the police IT reports.

6.3.5 Inter agency cooperation and public private partnerships

Digital service providers need to work with law enforcement. The United States has a system in place where they work closely with tech companies. India also works with telecom companies to get things done. The United Kingdom has a system called the Digital Evidence Transfer System.

Bangladesh does not have a system in place so it is hard to get evidence from Facebook, Google or WhatsApp when they need it. Digital service providers like Facebook, Google and WhatsApp are very important, in this process.

6.3.6 Forensic laboratory accreditation

Standardization is really important for laboratories. They need to follow the rules set by ISO/IEC 17025. This way they can make sure they are doing things correctly and meeting quality standards.

In Bangladesh the labs are not fully accredited yet. This means that the reports they make are not completely trustworthy and people can question them. Forensic laboratories like the ones, in Bangladesh need to get accreditation so that people can trust the reports they make.

6.3.7 Data protection and privacy compliance

We need to be careful when we collect evidence. This is because we have to respect peoples privacy. The United Kingdom has a law called the Data Protection Act 2018 and the European Union has a law called the EU GDPR. These laws tell us what we can. Cannot do.

In Bangladesh they are still working on a law called the Data Protection Act. This law has not been made official yet so there are gaps in how digital evidence is collected. Digital evidence collection must respect people's privacy in countries like Bangladesh where the Data Protection Act is still, in the draft stage.[23]

6.4 Prospects for Law Reform in Bangladesh

Bangladesh is going through a change in the way it handles digital things.. The laws that are in place are not good enough to deal with the problems of cybercrime and digital evidence that we have today. The Evidence Act Amendment 2022 is a start it is a step in the right direction. However Bangladesh needs to make more changes to its laws to really make a difference. The digital evidence and cybercrime issues, in Bangladesh will only get worse if the country does not make reforms. Bangladesh needs to do more to update its laws so that it can better handle evidence and cybercrime in the country.

6.4.1 Need for detailed statutory guidelines

Bangladesh should have a law, like Indias Section 65B.. This law should not be too strict. This should include:

Clear certification procedures;

Definitions of electronic records;

When we talk about government generated records we have to think about how we can be sure they are real. The idea of government generated records being genuine is very important. We make assumptions that government generated records are true and honest. These assumptions, about

[23] *R v Shephard* [1993] AC 380 (HL).

government generated records are what we need to consider. The truth is, we need to trust that government generated digital records are authentic.

6.4.2 Establishment of a Digital Evidence Rules framework

Bangladesh could do something, like the US Federal Rules. They could introduce these things to make their system better.

* The US Federal Rules model is an example for Bangladesh to follow.

Bangladesh could introduce the US Federal Rules model to make some changes.

Rules on genuineness;

Standards for forensic procedures;

Guidelines for cloud-based evidence;

Protocols for social media data collection.

6.4.3 Strengthening the digital forensics ecosystem

Bangladesh needs things. What Bangladesh requires is very important. Bangladesh requires a lot of things to be done. The things that Bangladesh requires are important, for the people of Bangladesh. Bangladesh requires these things to be a place.

Accredited digital forensics labs;

National forensic training institutes;

Investment in advanced forensic software and hardware;

Benchmarks aligned with SWGDE standards.

6.4.4 Judicial capacity building

The people who work in the judiciary need to learn skills. We can look at what Singapore, India and the UK're doing with their judicial academies. They are an example for us to follow. The Bangladesh Judicial Academy should have classes that focus on evidence. This is very important for the Bangladesh Judicial Academy to have evidence modules. The Bangladesh Judicial Academy can learn from Singapore, India and the UK. Make their own digital evidence modules.

6.4.5 Integrating privacy and data protection

Bangladesh should. Enact its Data Protection Act to regulate the Data Protection Act. This will help Bangladesh manage the Data Protection Act. Bangladesh needs to work on the Data Protection Act. The main thing is the Data Protection Act in Bangladesh.

* The Data Protection Act is very important for Bangladesh

* Bangladesh has to do something about the Data Protection Act

The Data Protection Act will help people in Bangladesh. Bangladesh will be better, with the Data Protection Act.

Lawful data collection;

Retention periods;

Access conditions;

Cross border data transfer.

Having a framework that really focuses on privacy would make it more acceptable to use evidence in a legal sense. This is because it would be in line, with what the constitution says is okay. A privacy centric framework is what we need to make sure digital evidence is used in a way that's fair and just.

6.4.6 Technological infrastructure in courts

Electronic courts, digital evidence display systems and secure storage mechanisms are really important for the courts. The e Courts Mission Mode Project, in India is an example of how this can be done. Indias e Courts Mission Mode Project shows us how to make digital evidence display systems and secure storage mechanisms work well.

6.4.7 Regional and international harmonization

Bangladesh should make sure its digital evidence framework is in line with the evidence framework. This means Bangladesh has to work on its evidence framework so that it matches the digital evidence framework. Bangladesh needs to do this to make its evidence framework similar to the digital evidence framework that other countries have.

* The digital evidence framework that Bangladesh is using

* The digital evidence framework that other countries are using

Bangladesh has to make its digital evidence framework work like the evidence framework that other countries have. This will help Bangladesh to improve its evidence framework and make it as good, as the digital evidence framework.

The Budapest Convention;

SAARC regional protocols;

ASEAN cybercrime cooperation models.

This will make it easier for people to get evidence from countries and it will also reduce arguments with companies that provide digital services in other countries. The harmonization will really help with border evidence collection and it will cut down on conflicts, with foreign digital service providers.

Chapter 7: Conclusion and Recommendations

7.1 Summary of Findings

The research shows that digital evidence is really important for the courts in Bangladesh especially when it comes to criminal investigations cybercrime cases, financial fraud, online harassment, intellectual property disputes, terrorism related offenses and organized cyber activities. Before the Evidence Amendment Act 2022 was passed the laws under the Evidence Act 1872 were not clear about how to handle records so the courts were not always consistent in how they dealt with digital evidence, in Bangladesh. Courts have a time figuring out how to deal with the old rules of evidence when it comes to new things like emails and messages on the internet. They have to think about things like logs from servers what people say on media and files stored online. They also have to consider information from apps and data that is encrypted. The courts are trying to make sense of all these communications like server based logs and social media evidence and how they fit with the traditional rules. This includes things like cloud storage and mobile applications well as encrypted data. Courts are really struggling to reconcile the rules, with the technical realities of electronic communication.

Law enforcement and people who prosecute crimes have a lot of trouble when it comes to evidence. They have to collect it keep it safe and show it in court. The problem is that the rules for handling this evidence are not always followed. Police officers often do not get the training they need to handle digital evidence. They need to know how to make copies of digital information verify that it has not been changed, look at the details of the evidence and store it securely.

The labs that help with evidence, like the CID Cyber Lab and the Bangladesh Computer Council facilities do not have enough resources. This means they cannot do their job properly. As a result

the quality of the investigations is not always good. The evidence is not always reliable. Law enforcement and prosecutorial agencies face these problems with evidence.

The courts do not really understand evidence. A lot of judges like magistrates and district court judges have not learned about forensics and other modern technologies. They do not know much about blockchain based evidence, network traffic analysis, cloud computing and mobile device investigation. This is why we see court rulings on what evidence is allowed especially when it comes to WhatsApp messages, social media records, digital banking transactions and other things we do online. Judges usually trust what the police say about technology. They do not really check if it is correct and that makes it hard to trust the digital evidence. The judges are not really sure about evidence and that is a problem. Digital evidence is things, like WhatsApp messages and the courts need to understand it.

Bangladesh is behind countries like India, the United Kingdom and the United States.

The United States and other countries have systems in place.

In India they have something called Section 65B of the Evidence Act.

This Section 65B of the Evidence Act in India has a lot of details about how to certify records and what procedures to follow.

The United Kingdom does things a bit differently.

In the United Kingdom they really care about whether a system's reliable and if they can trust the people who are in charge of the electronic records.

The United Kingdom also has digital forensic infrastructure to support this.

The United States has its rules too.

The Federal Rules of Evidence in the United States say that electronic records need to be relevant and reliable.

The Federal Rules of Evidence in the United States also say that expert testimony is important.

This creates a system that is structured but also flexible for the courts in the United States.

Bangladesh can learn from the United States and other countries, like India and the United Kingdom. The 2022 amendments in Bangladesh are a thing. They show that things are moving forward.. The 2022 amendments in Bangladesh are not finished yet. They need details about how things should be done. The 2022 amendments in Bangladesh also need technical guidance.. They need more help, from institutions.

The research shows that Bangladesh needs to make big changes to use evidence properly. This means they have to update the laws train the judges and court staff improve the labs that analyze evidence get different agencies to work together and find ways to share information, with countries. The next parts of this study will look at the changes made in 2022 find out what is still missing and suggest things that can be done to make it better.

7.2 Appraisal of the 2022 Amendments

The Evidence Act of 2022 is a change for Bangladesh. This law is the first to say that electronic records and digital documents are real. It says that emails and pictures and audio and videos and messages on media are all evidence. This is a step forward. It updates the rules of evidence to match the technology we have today. The Evidence Act of 2022 makes it easier for people to prosecute and for judges to make decisions. The Evidence Act of 2022 is very important for evidence, in Bangladesh.

7.2.1 Positive Contributions

The amendments have done something. They now say that electronic records can be used as evidence in court. This means that things like screenshots, server logs and information taken from devices are okay to use.

This change helps to clear up some things from before. It makes it easier to get information from servers when we need it. The amendments show that people are starting to understand how much crime is happening online. They see that more and more people are using the internet to do things and talk to each other. This can sometimes lead to legal problems. The electronic records, including things, like screenshots and server logs and even portable device extractions are now accepted as evidence. This is a deal because it helps with cases that involve cybercrime, digital transactions and online communication.

The 2022 amendments also make a base for judicial interpretation. This means courts now have a law to follow when they decide if digital evidence is real and trustworthy. The law shows that Bangladesh is thinking about the future. It accepts the reality of technology. Shows that Bangladesh wants to follow the same rules as other countries when it comes to digital evidence. The 2022 amendments are a step for Bangladesh to be in line with international best practices in evidence law specifically, with digital evidence.

7.2.2 Limitations and Ambiguities

These new laws have some things about them but they also have some problems. The main issue is that the law does not give instructions on how to verify digital evidence, such as what certificates are needed how to check if a document has been altered and how to make sure devices are secure. This is different from what they do in India, where they have a set of rules called Section 65B.

Because of this judges have to make their decisions, which can result in different outcomes, in similar cases. Another problem is that the law does not say how to handle evidence properly which means it can be easily damaged or changed and this can lead to accusations that the evidence was not handled correctly. Third the changes do not deal with getting evidence from countries, which is a problem when digital information is stored on servers in other countries by companies like Google, Meta and Microsoft.

Fourth the law does not support standards for investigating crimes like the ones, from ISO/IEC 17025 or SWGDE protocols so laboratories do not have the same rules to follow.

Finally the law does not think about privacy and protecting data because Bangladeshs Data Protection Act has not been made into a law yet.

The law is not working well as it should because of weaknesses in the system. A lot of police officers and judges do not have the training and the labs that do forensic work do not have enough money or resources. This means that even though the law is better on paper it is still not being used properly in life which causes problems, for judges, prosecutors and police officers.

7.3 Recommendations for Judicial Training, Policy Reform, and Forensic Development

To really make the most of the 2022 amendments this research says we need to make some changes. We need to focus on building up the courts changing the laws and the way things are done making science better and getting all the different agencies to work together. The 2022 amendments are very important. We need to make sure we do everything we can to make them work well. This means we have to work on the courts the laws, science and get all the agencies to cooperate with each other all at the same time to make the 2022 amendments really effective.

7.3.1 Judicial Training

Judicial officers need to learn a lot about forensics and other things, like cloud computing. They also need to know about encryption and how to look at metadata.. They have to know how to investigate cybercrime.

The Bangladesh Judicial Academy should make a course just for digital evidence. This course should cover things like:

* forensics

* cloud computing

* encryption

* metadata analysis

* cybercrime investigation

So judicial officers can get the training they need in digital evidence and cybercrime investigation and digital forensics. The Bangladesh Judicial Academy should really focus on making this digital evidence course good. Judicial officers will use this course to learn about evidence and cybercrime investigation.

Authentication of electronic records, including hash value and metadata verification

Interpretation of forensic reports from mobile, cloud, and network investigations

Assessment of the reliability and integrity of digital records

Application of international forensic standards, including SWGDE and NIST guidelines

Structured judicial reasoning frameworks for evaluating digital evidence

Enhancing judicial literacy ensures consistent, reliable, and technically informed adjudication of digital evidence cases.

7.3.2 Legislative and Policy Reform

Bangladesh needs to add details to the changes they made in 2022. They have to make rules that explain how to verify and confirm things. Bangladesh also has to make rules, about how to keep track of things. The new rules should include:

Certification mechanisms for electronic records, similar to India's Section 65B

Mandatory hash verification and device integrity statements

Clear guidance on cloud based, server hosted, and blockchain evidence

Integration of privacy protections and data protection safeguards

Cross border evidence retrieval protocols via mutual legal assistance treaties

We need to make some changes to the law so that it works well with technology. This will help make sure the law is applied in the way everywhere. The legislative and policy reforms will make the law match the developments and this is a good thing, for the legislative and policy reforms.

7.3.3 Forensic Development and Institutional Strengthening

Bangladesh must invest in its forensic infrastructure by

* making sure it has good computers and tools to look at evidence

Bangladesh needs to do this so it can solve crimes that happen on the internet and catch the people who do bad things on the computer

Bangladesh has to invest in its digital forensic infrastructure to keep its people safe from hackers and other bad people who use the internet to do wrong things

* training the police and other people who work with digital forensic infrastructure in Bangladesh so they know how to use the tools and computers

Bangladesh must also make sure its digital forensic infrastructure is safe and secure so the bad people cannot get into it and destroy the evidence or use it for their own bad purposes

* working with other countries to share ideas and learn from them about digital forensic infrastructure

Bangladesh needs to invest in its digital forensic infrastructure now so it can be ready for the future and keep its people safe, from the bad people who use the internet to do wrong things.

Establishing nationally accredited laboratories adhering to ISO/IEC 17025 standards

Procuring advanced forensic tools for mobile, network, cloud, and blockchain analysis

Recruiting skilled personnel, including computer scientists, forensic analysts, and cybersecurity experts

Creating regional forensic units to reduce investigative delays and backlog

Standardizing protocols across agencies to ensure uniform evidence handling

These steps will make digital evidence more believable and trustworthy when it is used in court. The digital evidence will be better because of this. Digital evidence is very important, in proceedings.

7.3.4 Inter Agency and International Cooperation

Managing evidence properly is really important. It needs groups to work together and countries to cooperate with each other. Digital evidence management is something that requires a lot of

teamwork. Digital evidence management also needs countries to share information and work together.

Formulating protocols between police, prosecution services, forensic laboratories, and the Attorney General's Office

Establishing MLATs with foreign jurisdictions hosting critical digital platforms

Creating liaison offices with technology companies to facilitate evidence authentication and retrieval

Standardizing reporting formats, metadata analysis, and forensic documentation across agencies

When people work together at the international levels it really helps to make sure digital evidence is honest and can be used in court. This teamwork makes digital evidence more reliable and trustworthy. Cooperation at the international levels is very important, for digital evidence.

7.4 Future Directions for Research

This study finds a lot of things that need to be looked at closely by academics. There are areas that need more research and the research identifies these areas. The areas that are found to need study are important for the research to move forward and the research shows that these areas are where more academic work is needed.

AI Generated Evidence and Deepfakes – assessing admissibility, forensic detection techniques, and reliability standards.

Blockchain and Cryptocurrency Evidence – examining legal recognition, authentication, and international compliance.

Privacy vs. Security in Digital Evidence – balancing investigatory needs with constitutional rights.

Cloud Forensics and Cross Border Legal Challenges – addressing jurisdictional and procedural issues.

Data Integrity and Verification – evaluating hash algorithms, cryptographic authentication, and tamper proof evidence standards.

Digital Evidence in Civil Litigation – expanding research beyond criminal cases to contractual, employment, and defamation disputes.

Research that is currently being done in these areas will help shape what happens in the courts. It will also inform people who make laws the standards used in forensic science and the ways that

countries work together across borders. The research will have an impact, on practice it will guide legislative reform it will set new forensic standards and it will improve cross border cooperation strategies.

Conclusion:

This research evaluates the transformative impact of the **Evidence Amendment Act 2022** on the Bangladeshi legal system, concluding that while the formal recognition of digital records is a landmark achievement, a significant "implementation gap" remains. The findings reveal that the judiciary and law enforcement continue to struggle with the technical complexities of electronic communication, such as cloud storage, encrypted data, and metadata verification, often due to a lack of specialized training and forensic resources. While the 2022 amendments successfully modernized the definition of evidence to include social media and server logs, the study highlights critical ambiguities—specifically the lack of a structured certification process similar to India's Section 65B and a failure to address cross-border data retrieval from global tech giants. To bridge this gap, the research recommends a multi-dimensional reform strategy: implementing specialized digital forensic curricula at the Bangladesh Judicial Academy, establishing nationally accredited laboratories under ISO standards, and formulating Mutual Legal Assistance Treaties (MLATs) for international cooperation. Ultimately, the study asserts that legislative change must be supported by institutional strengthening and a focus on emerging challenges like AI-generated deepfakes and blockchain evidence to ensure the integrity of justice in the digital age.

Bibliography

Primary Legislation (Bangladesh)

1. Evidence Act 1872 (Bangladesh).
2. Evidence (Amendment) Act 2022 (Bangladesh).
3. Information and Communication Technology Act 2006 (Bangladesh).
4. Digital Security Act 2018 (Bangladesh).
5. Constitution of the People's Republic of Bangladesh, art 43.

Foreign Legislation

6. Indian Evidence Act 1872 (India), ss 65A–65B.
7. Information Technology Act 2000 (India).
8. Civil Evidence Act 1995 (UK).
9. Police and Criminal Evidence Act 1984 (UK).
10. Federal Rules of Evidence (USA).

Case Law (Bangladesh)

11. *State v Md Rafiqul Islam* (unreported, Cyber Tribunal, Dhaka).
12. *State v Unknown Accused* (Cyber Tribunal, Dhaka, 2023).

Case Law (India)

13. *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473.
14. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
15. *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.

Case Law (United Kingdom)

16. *Public Prosecution Service v Elliott and McKee* [2013] UKSC 32.
17. *R v Shephard* [1993] AC 380 (HL).

Case Law (United States)

18. *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US 579 (1993).

19. *Lorraine v Markel American Insurance Co* 241 FRD 534 (D Md 2007).

International Instruments & Guidelines

20. Council of Europe, **Convention on Cybercrime (Budapest Convention)** (2001).
21. United Nations Office on Drugs and Crime (UNODC), *Practical Guide on Digital Evidence* (2019).
22. Interpol, *Guidelines for Digital Forensics First Responders* (2020).

Books

23. Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011).
24. Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press 2016).
25. Andrew Keane and others, *The Modern Law of Evidence* (13th edn, OUP 2020).

Journal Articles

26. Orin S Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 Columbia Law Review 279.
27. Susan Brenner, 'Cybercrime Investigation and Prosecution' (2010) 4 Journal of Digital Forensics 1.
28. Md Shahidul Islam, 'Admissibility of Electronic Evidence in Bangladesh' (2019) 30 Dhaka University Law Journal 145.
29. Md Abdullah Al Faruque, 'Cyber Law and Digital Evidence in Bangladesh' (2020) 11 Asian Journal of Law 87.
30. Farzana Akter, 'Challenges of Digital Evidence under the Digital Security Act' (2021) 33 Bangladesh Journal of Law 201.

Comparative & Policy Sources

31. Law Commission of India, *Report No 185 on Electronic Evidence* (2003).
32. UK Law Commission, *Evidence in Criminal Proceedings* (2017).
33. US Department of Justice, *Digital Evidence in the Courtroom* (2018).

Online & Institutional Reports

34. Bangladesh Police, *Cyber Crime Investigation Manual* (2022).

35. Supreme Court of Bangladesh, *Annual Report* (2023).
36. World Bank, *Cybersecurity and Legal Reform in South Asia* (2021).