UGC & Govt. Approved
Sonargaon University (SU)
সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research Monograph
on

Digital Evidence in the Trial System of Bangladesh: prevalence, challenges and expertise.

Research paper Submitted in partial fulfillment of the requirements of the degree of Master of Laws(LL.M.) under Sonargaon University

Supervised By

Sharmin Jahan Runa
Assistant Professor & Head
Department of Law
Sonargaon University

Submitted By

Md. Sirajul Islam
ID No: LLMP2301028004
Session: Fall-2025
Course Code: LAW 5408
Department of Law
Sonargaon University

Date of Submission: 5 January 2026

Letter of Transmittal In Research

Date: 5 January 2026

To
Sharmin Jahan Runa
Assistant professor & Head
Department of Law
Sonargoan University, Dhaka

Subject: letter regarding the submission of research Monograph on **"Digital Evidence in the Trial System of Bangladesh: prevalence, challenges and expertise"**

Dear Madam,

With due respect, I am hereby Pleased to submit the research report entitled **"Digital Evidence in the Trial System of Bangladesh: prevalence, challenges and expertise."** It was a great pleasure to work on such an important topic. This project was assigned to me in partial fulfillment of the requirements for the award of the degree of Master of Laws (LL.M.) Under Sonargoan University.

I belive that this project will definitely help you in evaluting my work. I would be very happy to provide any assistance in interpreting any part of the paper wherever needed.

Sincerely Yours

Md. Sirajul Islam
ID No: LLMP2301028004
Session: Fall-2025
Course Code: LAW 5408
Department of Law
Sonargaon University, Dhaka

Certification By The Research Supervisor

This is to certify that the research Monograph on **"Digital Evidence in the Trial System of Bangladesh: prevalence, challenges and expertise"** is the bonafide record of the project work done by Md. sirajul Islam, ID No-**LLMP2301028004** in partial fulfillment of the requirements for the award of the degree of Master of Laws (LL.M.) from Sonargoan University, Dhaka.

I do hereby certify that the project work has been carried out under my direct supervison and guidance.

Sharmin Jahan Runa
Assistant Professor & Head
Department of Law
Sonargaon University, Dhaka

Declaration By Student

I do hereby solemnly declare that I am the author of the dissertation **"Digital Evidence in the Trial System of Bangladesh: prevalence, challenges and expertise."** It is my original work and I acknowledge the veracity of the data used in this study. This work has not been previously submitted to any other University/College/Institution/Organization for academic qualification or professional degree and has not been published by me in any Newspaper, Journal, or Magazine.

I hereby assure that the work has been presented here does not breach any existing copyright law.

I further undertake to indemnity the University against any loss or damage arising from breach of the for going obligations.

Md. Sirajul Islam
ID No: LLMP2301028004
Session: Fall-2025
Course Code: LAW 5408
Department of Law
Sonargaon University, Dhaka

Acknowledgement

At first, I would like to thank Almighty Allah for his graciousness on me in accomplishing this research paper. I would like to express my deep sense of gratitude to my honorable and distinguished supervisor **Sharmin Jahan Runa,** Assistant Professor & Head, Department of Law, Sonargaon University, Dhaka for her individual suggestions, valuable time, important information and guidance during the study period that has grately inspired me in preparing this research monograph successfully. Without the assistance of my supervisor, I was not able to finish this report, thanks to her direction and counsel.

In addition to, I would like to thank all of the members of Department of Law Faculty who assisted me in overcoming my flaws when I was studing Law.

Finaly, I want to thank my family and friends for their support and encouragement in helping me reach my objectives.

Md. Sirajul Islam

ID No: LLMP2301028004
Session: Fall-2025
Course Code: LAW 5408
Department of Law
Sonargaon University, Dhaka

Abstract

This article introduces the concept of digital evidence and supports it with a few historical twists. Furthermore, it demonstrates how the Evidence Act and several other laws have integrated digital evidence into their corpus and thoroughly examines the legal process of admissibility of digital evidence within the current corpus juris of Bangladesh. In order to maintain the rule of law in society, it is now of utmost importance to implement innovative strategies for crime prevention. Such crimes can be avoided through the use of digital evidence. Digital evidence can use its properties to gather and examine information to reach conclusions. In a court of law, digital evidence can help ensure justice. Digital evidence can be one of the best methods used to convict and deter criminal activity in the legal system of Bangladesh. The aim of this article is to shed light on the limitations of digital evidence in Bangladesh, its potential legal relevance, and the concept of best evidence.

TABLE OF CONTENTS

Chapter One
Introductory

1.1 Introduction 01
1.2 Statement of Problems 01
1.3 Objectives of the Study 02
1.4 Research Methodology.....03
1.5 Importance of the Study 04
1.6 Limitations of the Study..... 05
1.7 Chapter Outline 05

Chapter Two

Best Evidence Rule & Digital Evidence Conceptual Understanding, Background and Significance.

2.1 Introduction: 06
2.2 Concept of Evidence in Law 06
2.3 Background and History of Best Evidence Rule 08
2.4 Origin, Concept, and Objectives of Digital Evidence 08
2.5 Potential and Importance of Digital Evidence in Bangladesh:.....09
2.6 Conclusion.....11

Chapter Three

Digital Evidence in Bangladesh: Significance and Need for Reform

3.1 Introduction. 12
3.2 Judicial Decision on the Admissibility of Digital Evidence in Bangladesh...…12
3.3 Reform in incorporating Digital Evidence in Bangladesh Legal System.....14
3.4 Guidelines regarding the Application of Digital Evidence in Bangladesh:……15
3.5 Importance of Digital Evidence and its status as Best Evidence rule……....16

3.6 Effects of Considering Digital Evidence as Primary and Direct 17
3.7 Conclusion..... 18

Chapter Four
Scope and Application of Digital Evidence in other countries

4.1 Introduction: 19
4.2 International Standard of Digital Evidence 20
4.3 Use and Application of Digital Evidence in Other Countries 21
4.4 Uniqueness of Electronic Evidence..... 23
4.5 Conclusion..... 24

Chapter Five
Finding Equation and Concluding Remarks

5.1 Findings..... 25
5.2 Recommendations and Suggestions 27

Bibliography..... 29

Chapter One
Introductory

1.1 Introduction

In the digital age, technology has become an inseparable part of everyday life, influencing communication, finance, security, and governance. As a result, crimes today often leave behind a trail of digital footprints—emails, mobile data, CCTV footage, social media activity, and online transactions. This growing dependence on digital platforms has made digital evidence a crucial component in modern criminal investigations and judicial proceedings. In Bangladesh, the incorporation of digital evidence into the trial system marks a significant step toward modernization and transparency in the justice process.

However, despite its growing importance, the use of digital evidence in Bangladeshi courts remains at an early stage. The legal system is still adapting to the rapid technological changes, and many challenges persist regarding the admissibility, authenticity, and reliability of electronic data. Law enforcement agencies often face difficulties in collecting, preserving, and presenting such evidence in a technically sound and legally valid manner. Moreover, a lack of technical expertise among investigators, prosecutors, and judges often weakens the evidential value of digital materials during trial.

Given these realities, understanding the prevalence, challenges, and expertise surrounding digital evidence in the trial system of Bangladesh is essential. This study aims to examine how digital evidence is currently used in courts, identify the major obstacles to its effective application, and explore ways to strengthen institutional capacity for ensuring fair and efficient justice in the digital era.

1.2 Statement of Problems

The rapid advancement of information and communication technology has transformed how crimes are committed, investigated, and prosecuted in Bangladesh. Digital tools and online platforms are now used for both legitimate and criminal purposes, resulting in the emergence of cybercrimes such as online fraud, hacking, identity theft, and digital harassment. As a consequence, digital evidence—including emails, call records, CCTV footage, social media

data, and computer forensics—has become increasingly vital for establishing facts in both civil and criminal cases. Despite this growing importance, the effective use of digital evidence in the trial system of Bangladesh remains limited and problematic.

One of the major challenges lies in the lack of clear legal and procedural guidelines regarding the collection, preservation, and admissibility of digital evidence. Although the Evidence Act 1872 (as amended in 2017) and the Digital Security Act 2018 recognize electronic records as valid forms of evidence, the practical implementation of these provisions is inconsistent. Many law enforcement officials, lawyers, and judges have insufficient knowledge or technical expertise to properly handle digital materials. Consequently, cases involving electronic data often face delays, evidential disputes, or outright rejection in court due to procedural lapses.

Additionally, the absence of adequate forensic facilities and trained digital experts creates serious obstacles to the proper verification and authentication of digital data. Limited technological infrastructure, poor chain of custody practices, and dependence on foreign expertise further weaken the credibility of such evidence. Moreover, the lack of awareness among legal professionals about digital forensics often results in the misuse or misinterpretation of digital materials during trials.

Therefore, there exists a critical gap between the legal recognition of digital evidence and its practical application within Bangladesh's judicial system. This study seeks to identify the root causes of these challenges, evaluate the current state of digital expertise in the justice sector, and propose effective measures to ensure that digital evidence can be used reliably and efficiently in the pursuit of justice.

1.3 Objectives of the Study

The main objective of this study is to examine the prevalence, challenges, and expertise related to digital evidence in the judicial system of Bangladesh. To achieve this broad aim, the study pursues the following specific objectives:

- To assess the current prevalence and types of digital evidence commonly presented in Bangladeshi courts.

- To analyze the existing legal framework governing the admissibility and use of digital evidence, with reference to the Evidence Act, ICT Act, and Digital Security Act.
- To identify major challenges faced by law enforcement agencies, prosecutors, and judges in collecting, preserving, and evaluating digital evidence.
- To examine the level of technical expertise and institutional capacity among the professionals involved in the criminal justice process.
- To propose recommendations and strategies for improving the handling, authenticity, and credibility of digital evidence in future judicial proceedings.

1.4 Methodology

This study on *"Digital Evidence in the Trial System of Bangladesh: Prevalence, Challenges, and Expertise"* is based on a **qualitative research approach**, supported by descriptive and analytical methods. The qualitative approach allows for an in-depth understanding of the legal framework, practical challenges, and institutional capacity involved in the use of digital evidence in Bangladesh.

❖ Data Collection

The study primarily relies on **secondary data sources**, including books, journal articles, law reports, government publications, and research papers related to digital forensics, cyber law, and the justice system. Relevant **Bangladeshi laws**, such as the Evidence Act (1872, amended 2017), the Information and Communication Technology Act (2006), and the Digital Security Act (2018), were carefully reviewed to understand the existing legal provisions on digital evidence. Additionally, online sources, case studies, and newspaper reports were analyzed to identify real-world applications and challenges in courts.

❖ Data Analysis

The collected data were **analyzed descriptively and comparatively**. The study examined how digital evidence is treated in Bangladesh's courts compared to international best practices. Legal gaps, procedural weaknesses, and institutional limitations were identified through thematic analysis.

❖ Scope and Limitation

The research focuses mainly on the **criminal justice system of Bangladesh**, with occasional reference to civil cases where relevant. Due to limited access to confidential court documents and official data, the research depends largely on secondary information and existing reports.

Nonetheless, efforts were made to ensure accuracy and reliability through the use of verified and credible sources.

Through this methodology, the study seeks to provide a clear picture of the current state of digital evidence in Bangladesh and offer practical insights for legal and institutional reforms.

1.5 Importance of the Study

The growing reliance on technology in all aspects of life has transformed the nature of crime and justice in Bangladesh. As digital communication and online transactions become more common, courts increasingly encounter evidence in electronic form. However, the justice system is still in the process of adapting to these technological realities. Therefore, this study on digital evidence in the trial system of Bangladesh holds significant importance both academically and practically.

Firstly, the study contributes to a better understanding of how digital evidence is used and interpreted within the country's legal framework. By identifying the gaps in existing laws and judicial practices, it helps policymakers and legal professionals recognize the areas that require reform or improvement. Secondly, the research highlights the technical and procedural challenges faced by investigators, prosecutors, and judges, thereby emphasizing the urgent need for capacity building and specialized training in digital forensics and evidence handling.

Moreover, the study provides insights that can help enhance transparency, accountability, and efficiency in the justice delivery system. A stronger understanding and application of digital evidence can lead to faster investigations, more accurate verdicts, and reduced manipulation of evidence. Finally, this study contributes to the broader goal of modernizing the Bangladeshi legal system to meet international standards, ensuring that justice keeps pace with the demands of the digital era.

1.6 Limitations of the Study

Although this study provides valuable insights into the use of digital evidence in the trial system of Bangladesh, it is not without limitations. The research is primarily based on secondary data sources, such as books, journal articles, law reports, and online publications. Due to limited access to official records and confidential case files, the study could not include firsthand data from ongoing or closed court proceedings involving digital evidence. This restricts the ability to analyze certain aspects of real-life judicial practices in depth.

Another limitation is the scarcity of updated and comprehensive statistics on the use of digital evidence in Bangladeshi courts. Many relevant institutions, such as the police, cybercrime units, and forensic laboratories, do not regularly publish detailed reports on digital evidence handling, which limits the availability of quantitative analysis.

Furthermore, because the study was conducted within a limited time frame and resource constraints, it could not cover every dimension of the issue, such as cross-border digital crimes or advanced forensic technologies used internationally. Despite these limitations, every effort was made to ensure the reliability, accuracy, and academic value of the findings by using verified and credible secondary sources.

1.7 Chapter outline

Chapter One introduces Introductory Chapter
Chapter Two introduces Best Evidence Rule & Digital Evidence Conceptual Understanding, Background and Significance

Chapter Three Digital introduces Evidence in Bangladesh: Significance and Need for Reform

Chapter Four introduces Scope and Application of Digital Evidence in other Countries

Chapter Five introduces Summary, Findings, and Recommendations

Chapter Two

Best Evidence Rule & Digital Evidence Conceptual Understanding, Background and Significance

2.1 Introduction

Digital evidence is a rule of electronic evidence. Digital evidence is primary evidence if it is presented from the original device or source, is not altered or distorted, is forensically verifiable and is admissible in court through proper production. An electronic record is a type of document. If it is submitted with the device on which it was created or stored, then it is a primary document. However, if it is transferred or copied to another storage or medium with the slightest interference, then it is a secondary document. Despite the difference of opinion, this view is more acceptable.[1] Suppose if a messenger chat is presented in court directly from a mobile and if it is verifiable, then it is primary evidence. But its print copy or screenshot is considered secondary evidence, unless it is submitted with a certificate of authenticity. The content of digital evidence has to be proved as per Section 65B of the Evidence Act. Electronic records will be used as evidence in court.[2]

2.2 Concept of Evidence in Law

In Bangladesh, oral and documentary evidence was mentioned in the beginning. At that time, there was no recognition of digital documents or electronic records.[3] Electronic records, electronic signatures and digital evidence were recognized in the ICT Act 5 and 84. Then, video footage was allowed in the

---

[1] *Basic Concepts on Digital Evidence: Bangladesh Case Study Lawyers Club Bangladesh Article May 5, 2025.*
[2] P. K. Basheer& others v. Anvar P.V. (2014) 10.SCC.473
[3] Hunter v. Garton (1969) 1 All ER 451 [1969] 2 QB 37

case of State vs. Md. Khaled (2008). State vs. Imran Hossain (2013) DNA and digital information were considered admissible.[4] Later, sections 2, 8, 43 of the Digital Security Act introduced a legal framework for the security of digital information and collection of evidence.

Digital evidence played an important role in the Nusrat murder case 2019 ,[5] Rifat Sharif murder case (2019), and the Parimani case.[6] Digital records and electronic records carry the same meaning, digital is a little smaller. All data that is in binary form is digital. All data or records stored or produced by electricity or electronic means or devices are electronic records. However, in the provisions of the Evidence Act, these two words have been used in the same sense. Generally, the use of the words electronic evidence in India and digital evidence in Bangladesh is observed. As I said earlier, electronic records are a type of document. If they are submitted with the device on which they are produced, created or stored, they are primary documents. They are secondary documents, nevertheless, if they are copied or moved to another medium or storage with even the smallest amount of participation.[7] This viewpoint is more acceptable in spite of the disagreements. Digital evidence is a subcategory of electronic evidence. Digital evidence will be primary evidence if it is presented from the original device or original source, it has not been changed or tampered with, it is forensically verifiable and if the court considers it to be properly admissible. Suppose a WhatsApp chat is presented in court directly from a mobile phone and if it is verifiable, it is primary evidence. But its print copy or

---

[4] Lawrence Williams, Digital Forensics, 'What is Digital Forensics? History, Process, Types, Challenges', 5th March, 2022, [10th March, 2022]

[5] "A Historical Perspective of Digital Evidence: A Forensic Scientist's View" by Carrie Morgan Whitcomb [Spring 2002, 2022] International Journal of Digital Evidence, Volume 1, Issue 1, 4

[6] Whitcomb (n-7)

[7] Whitcomb (n-7)

screenshot is considered secondary evidence, unless it is submitted with a certificate of authenticity.[8]

2.3 Background and History of Best Evidence Rule:

The "best evidence rule" is a very important legal principle in the law of evidence. This rule dates back to around 1800. This rule states that if the original evidence exists or can be found, no other evidence can be accepted in place of the best evidence. If the original is lost or damaged, a copy will be admissible. However, a witness must testify to the contents of the copy and confirm that it is an exact copy of the original. This rule first arose in 18th-century British law. It was further developed in the case of Omychund VS Barker (1780) where Lord Hardwicke commented that "there is a general rule of evidence, that which is best in the nature of the case will be admitted".However, with the introduction of electronic communications, some have questioned whether the best evidence rule is still valid. We admit all relevant evidence. Its merit or demerit depends only on weight, not on admissibility.

2.4 The concept, origin, and goals of digital evidence:

Digital evidence has its roots in the proliferation of computers and the Internet. The idea behind it is that any binary data can be presented as reliable evidence in court. Digital evidence is used to prosecute employing digital signatures and hash values to prevent electronic crimes, guarantee information security, and improve the validity of evidence. Numerous forms of digital data have been produced as a result of the extensive usage of computers, cell phones, and other electronic devices. These data can then be used as digital evidence.With the

[8] Lawrence Williams, Digital Forensics, 'What is Digital Forensics? History, Process, Types, Challenges', 5th March, 2022, [Accessed 12th March, 2022]

spread of the Internet and digital technology, child pornography, credit card fraud, and other cybercrimes or e-crimes have increased. The need for digital evidence to prove these crimes has arisen. To make the court process more modern and efficient, it is necessary to include digital evidence, so that the information in digital format is legally admissible.[9](10)

The concept of digital evidence:

Digital evidence is any type of information stored on a digital device that can be used as evidence in court. It includes text, audio, video, data, and other digital content. The main characteristic of this evidence is its digital nature, which makes it easy to change, modify, or destroy. However, it is important to maintain its originality and integrity when preserving digital evidence. This includes written documents, images, audio, video, and other files that are stored on computers, smartphones, or other digital devices. Digital evidence plays an important role in criminal investigations and trials, as it serves as evidence of the incident.[10]

2.5 Potential and Importance of Digital Evidence in Bangladesh:

The potential and importance of digital evidence in Bangladesh is immense, serving as a support in various fields including legal proceedings, investigation and cyber security. It enhances transparency and accountability in legal proceedings, helps in curbing digital crimes and is used as a modern evidence collection method. Technological aspects such as metadata, digital signature and timestamping play an important role in the proper collection and analysis of

[9]Lawrence Williams, Digital Forensics, 'What is Digital Forensics? History, Process, Types, Challenges', 5th March, 2022, [Accessed 12th March, 2022]

[10] ibid

digital evidence, which ensures its admissibility in the judicial system. Digital evidence plays an important role in the judicial process and serves as a powerful tool to prove the truth of crimes by presenting it.[11]

Using digital evidence, it is possible to easily investigate crimes such as financial irregularities, corporate fraud, and intellectual property theft. In the case of cybercrime or digital crimes, digital evidence is used as an essential medium for collecting evidence, analyzing crimes, and identifying criminals. Using digital forensic tools, information can be recovered from digital devices, which is considered important evidence for investigations.[12] The use of digital evidence makes it easier to ensure transparency and accountability in public and private disputes and cases. It plays a helpful role in establishing justice. Collecting digital evidence by following the right procedures increases the acceptability of justice and can play an important role in the judicial process. Digital evidence is an essential part of modern evidence collection, which makes the judicial system of Bangladesh more modern and effective. Digital crimes (such as hacking, cyberbullying, etc.) are easier to suppress through the collection and analysis of digital evidence. This helps in taking effective action against criminals and provides legal assistance. Technological aspects such as metadata, digital signatures, images, video images, and timestamping validate digital evidence, which increases its admissibility in court.[13]

[11] Saadat Tanbir Digital Evidence Admissibility in Bangladesh. October 30, 2021, BdJLS

[12] ibid

[13] Saadat Tanbir Digital Evidence Admissibility in Bangladesh. October 30, 2021, BdJLS

2.6 Conclusion:

Generally, case law issues related to digital evidence are rarely addressed, as it is an emerging form of evidence in international criminal courts. In an analysis of the limited case law, this paper has made specific findings and identified a number of unresolved issues. These findings are summarized and recommendations for further research are provided. Based on a review of relevant cases, it appears that international criminal courts have placed high priority on direct testimony from a few experts who can confirm the authenticity of digital evidence. Courts also accept documentary evidence, such as transcripts of audio recordings, instead of direct testimony, or in addition to it, which in certain cases is used to prove facts and to properly punish the actual perpetrator in the case.

Chapter Three

Digital Evidence in Bangladesh: Significance and Need for Reform.

3.1 Introduction:

Digital evidence is of great significance in Bangladesh, as it helps in the investigation and prosecution of modern crimes (such as cybercrime) and facilitates the task of verifying the truth. To effectively use digital evidence and ensure its validity, it is necessary to reform the existing Evidence Act and other related laws, which will give legal validity to digital evidence (such as electronic records) and allow its use as evidence. Digital evidence is currently permitted in situations including anti-terrorism tribunals, cyber-crime tribunals, speedy trial tribunals and bodies representing law, justice and parliamentary affairs.[14]Although the Information and Communication Technology Act, 2006 and the Digital Security Act, 2018 have been significantly amended, there is no clear or specific inclusion of digital evidence in Bangladesh. Some case law in the legal system of Bangladesh has revealed digital/electronic evidence and judicial interpretation is very important in such situations. Consequently, the focus of this chapter will be on the judicial decisions evaluating the leading case law of Bangladesh, as well as the best evidence in Bangladesh to strengthen the position and status of digital evidence.

3.2 Judicial Decision on the Admissibility of Digital Evidence in Bangladesh:

[14] *CJ for updating law to allow digital evidence, [Jan 14,2020], .13thMarch, 2022]*

Judicial decisions on admissibility of digital evidence are primarily governed by the Evidence Act of Bangladesh, 1872, which was significantly amended in 2022. The 2022 amendment introduced formal specific provisions, notably Sections 65A and 65B, to regulate the admissibility and conditions of digital record evidence in court proceedings.

In Bangladesh, there is no specific or direct law for the admission of digital evidence in judicial proceedings in every case. Special laws such as the Information and Communication Technology Act of 2006 and the Digital Security Act of 2018 have been enacted, but they are used in judicial proceedings only in specific cases.[15] The admissibility of evidence in the Evidence Act is said to be the reproduction of the original. It refers to an area that, if proven in the original, is considered secondary evidence. Again, there is no bar to proving digital and electronic evidence as not proven.[16] There is no clear provision in the law for the recognition or approval of digital evidence and its admissibility in judicial proceedings. They leave room for judicial interpretation, which can give recognition for judicial admissibility. In the case of digital or electronic evidence, it is stated that a party seeking to admit any statement or confession of a person recorded on a compact disc or video cassette or any statement or confession relating to any relevant information or data in an interview conducted by a television channel shall produce the original compact disc or video cassette or programmer broadcast on the television channel along with a certificate from the producer of the programme, showing the date and place of recording of the programme and the producer's signature on the

[15]The 1872 Evidence Act (I of 1872)

[16] Fundamental Clauses Act of 1897 [X OF 1897]

certificate. However, if the accused denies the statement or confession, its admissibility under the prevailing law of evidence should be examined.[17]

[17] Rajib Kumar Deb Digital evidence admissibility [August 27, 2019], The Daily Star < https://www thedailystar.net/law-our-rights/news/admissibility-digital-evidence-1790917 > [As of March 13, 2022] Ibid

3.3 Reform in incorporating Digital Evidence in Bangladesh Legal System:

There are rules and regulations for the admissibility of digital evidence in the courts of Bangladesh. Since our primary regulatory law, the Evidence Act, does not specifically mention digital evidence and is not currently adequately recognized, it can create uncertainty and ambiguity in the minds of magistrates and judges conducting cases. Not only that, but due to the lack of adequate training and rules and regulations, investigators are also struggling to collect and present digital evidence.[18] Although there is no clear provision on the admissibility of digital evidence in the context of Bangladesh, the Supreme Court of Bangladesh had to rule on the admissibility of digital evidence under the Evidence Act of 1872 and for this, the court has also laid down some conditions in this regard. The following are required for the identification and authentication of the producer and authentication of the disc/digital evidence for use as evidence in court. The biggest milestone in the incorporation of the Constitution into the administrative system is the amendment to the Evidence Act of 1872, through which digital or electronic records have been identified as documents. Major Amendments Evidence Act Amendment of 1872: In 2022, a landmark change was made in the Evidence Act. Section 3 of the Act was amended to include digital or electronic records in the definition of the word "document".[19] It has been made mandatory to follow certain technical and procedural matters to ensure the authenticity, integrity and politicality of a democratic state.

[18] Rajib Kumar Deb N-19

[19] Rajib Kumar Deb N-19 23 37 DLR (HCD), (1985) 275

So that no one can present fake or fake digitization, the court can give forensic instructions on the evidence-evidence core. For this, the country is setting up adequate forensic laboratories.

ICT and Digitary/Cyber Security: Earlier, the ICT Act was enacted to prosecute digital crimes. Later, the Digitary Act (DSA) was enacted in 2018. This act was partially amended in 2023 to initiate a new law called the Cyber Security Act (CA). These laws have consolidated the use of digital crimes and the prosecution of crimes committed through digital means.[20]

3.4 Guidelines regarding the Application of Digital Evidence in Bangladesh:

The guidelines for the application of digital evidence in Bangladesh are governed by the Digital Security Act, 2018 and the Digital Security Rules, 2020, which provide specific rules and regulations for the collection of digital data, its use as evidence and investigation of crimes. Under these, courts can summon and seize digital documents, digital forensic labs are used and technologies like digital signatures are used. There are rules and guidelines for the admissibility of digital evidence in the courts of Bangladesh. Since digital evidence is not specifically mentioned in our primary regulatory law, the Evidence Act, and is not currently adequately recognized, it can create uncertainty and ambiguity in the minds of magistrates and judges trying cases. Not only that, but investigators struggle to collect and present digital evidence due to lack of training and rules. Although there is no clear provision on the admissibility of digital evidence in the Bangladeshi context, the Supreme Court of Bangladesh had to adjudicate the admissibility of digital evidence under the

[20] Mohammad Shahjahan, Admissibility of Digital Evidence: Bangladesh Perspective, (15 January, 2022) Lawyers Club Bangladesh<http://lawyersclubbangladesh.com/en 2022/01/15/admissibility of digital evidence bangladeshperspective/ > [Accessed 14th March, 2022]

Evidence Act 1872 and for this, the court has also laid down certain conditions in this regard.[21] The following are required for identification and authentication of the maker and authenticity of the disc/digital evidence to be used as evidence in court.

If the accused does not deny any of the recorded words or confessions, the digital evidence may be admissible in court. In cases where the accused denies the statement or confession, the maker of the digital evidence has to appear in court to prove it legally. The detectives have to collect the digital evidence from the seized list.[22] In order to remove doubts about the maker and authenticity of the disc, these measures are essential. In the case of Major Bazlul Huda and Others vs. State[23], the Hon'ble Appellate Division Mr. Justice Md. Tafazzul Islam has commented on the admissibility of digital/electronic evidence. For it to be admissible, a party must produce the original compact disc or video cassette, with the certificate of the maker or author, date and place of recording.[24]

3.5 Importance of Digital Evidence and its status as Best Evidence rule:

Digital evidence is essential in modern legal proceedings. Digital evidence plays a vital role in cybercrime and digital security breaches. Following the right procedures helps in collecting, analyzing and preserving digital evidence as the best evidence in legal proceedings.[25]

If digital evidence is collected illegally, it will not be admissible in court. Maintaining the confidentiality of personal information while collecting digital evidence is a challenge. Proper training and use of technology are essential to

[21] ibid
[22] 2017(2) LNJ (HCD) 303
[23] Christine Sgarlata Chung and David J. Byer The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence [22nd September, 1998] B.U. J. SCI. & TECH
[24] ibid
[25] Bills v. Kennecott Corp. 108 F.R.D. 459, 462 (D. Utah 1985)

meet the challenges of digital evidence.[26] Digital evidence is helpful in verifying the authenticity and understanding the nature of the incident. It serves as the best evidence of the time, place and related matters of an incident. Digital evidence is essential in investigating cybercrimes such as hacking or data theft. It provides evidence of the activities and use of technology by the criminal. In a business environment, digital evidence is important for making decisions based on accurate information and data. Digital evidence helps in maintaining confidentiality and security.[27] It is important to protect the confidentiality of information and prevent unnecessary access. The status of digital evidence as the best evidence rule There are certain rules to follow while collecting digital evidence. By using digital signatures, it can be proven that the data came from the original source and has not been altered in any way.[28] According to the laws of different countries, digital evidence can be admissible in court. Like a handwritten signature, a digital signature cryptographically binds a digital identity to a digital document, which cannot be copied. It plays a crucial role in proving the authenticity and reliability of digital records.[29]

3.6 Effects of Considering Digital Evidence as Primary and Direct:

Anyone involved in the judicial process must comprehend the distinction between direct and circumstantial evidence. The testimony of an eyewitness who depicts a defendant committing a crime or tangible evidence like a video recording of an incident are examples of direct evidence, which establishes a

[26] VivekDubey, Digital Proof Acceptance: An Indian Perspective 4, FRACIJ (2017),Chung and Byer n-36 4

[27] Manes, Gavin W.; Downing, Elizabeth; Watson, Lance; and Thrutchley, Christopher, Modern Federal Law and Digital Proof (2007).

[28] Chung and Byer n-36

[29] 30 Christine Sgarlata Chung and David J. Byer, The Electronic Paper Trail: Evidentiary Barriers to Electronic Evidence Discovery and Admission [September 22, 1998], B.U. J. SCI & TECH

fact without the need for any conclusions.[30]Because it establishes a clear link between the defendant and the claimed legal infraction, this kind of evidence leaves little space for debate. In contrast, a jury or judge must draw a logical judgment from circumstantial evidence. DNA discovered at a crime scene is an example of forensic evidence that can strongly suggest the defendant was involved in the crime, even though it may not prove it. In civil litigation, both direct and circumstantial evidence are crucial, and how these types of evidence are presented and understood to ensure justice frequently determines how strong a case is.[31] The establishment of certain provisions or modifications to the legal system pertaining to digital evidence, such as Section 65B of the Evidence Act, 1872 in Bangladesh, has been prompted by this shift. This gives attorneys precise instructions on how to use digital evidence. Digital evidence is more reliable when it is treated as primary evidence, but it can also be manipulated or misused.[32]

3.7 Conclusion:

Digital devices have proven to be more beneficial for the courts by enabling them to collect more valuable information. Nowadays, digital devices are used practically everywhere. It facilitates local and global communication. As a result, electronic communication, e-commerce and data storage are becoming increasingly important. An amendment is needed in the law governing information technology and electronic evidence in civil and criminal trials. Although digital technology adds to the original evidence, it also saves time and

---

[30] In D. Utah 1985, Bills v. Kennecott Corp. 108 F.R.D. 459, 462

[31] Vivek Dubey, "Admissibility of Electronic Evidence: An Indian Perspective"4, FRACIJ (2017), 58

[32] 30 Christine Sgarlata Chung and David J. Byer, The Electronic Paper Trail: Evidentiary Barriers to Electronic Evidence Discovery and Admission [September 22, 1998], B.U. J. SCI & TECH

energy when it comes to preparing and presenting it digitally. Consequently, it is past time for our parliament to assess the development of computers, the social impact of information technology and the ability to store information in digital form and incorporate these considerations into the legal system of Bangladesh.

Chapter Four

Scope and Application of Digital Evidence in other Countries

4.1 Introduction:

Nowadays, people can rely on technology not only to communicate with each other but also to work as technology is responsible for global growth and development. This technological advancement allows for more data storage. Due to its usefulness, many countries have already adopted or incorporated digital evidence into their national laws. From the United States to the United Kingdom, India and Pakistan, all have adopted digital evidence provisions that allow digital evidence to be admitted in court. In the last decade, numerous jurisdictions have effectively moved towards digital evidence. As a result, global and national standards for the application of digital evidence will be thoroughly examined in this chapter, as well as whether digital evidence is the best evidence. Digital evidence is a relatively new tool for law enforcement investigations, with law enforcement agencies relying heavily on ‘digital evidence’ for crucial information about both victims and suspects. Due to the potential volume of digital evidence, it is more difficult to generate leads and solve cases where such evidence is lacking. Three recent investigations

highlight the ‘importance of digital evidence to the criminal justice community’– one case presents an example of how digital forensics can play a central role in closing cases and prosecuting them, another shows how mishandling digital evidence can have serious consequences, and the final case highlights the challenges for modern investigations when digital evidence is limited or non-existent.

4.2 International Standard of Digital Evidence:

There is no international treaty on electronic evidence. However, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce provides legal advice to countries at the UN level for the development of their national legislation.[33] A framework for assessing, considering and determining digital evidence has been proposed. This framework emphasizes the legal and technical prerequisites for ensuring that digital evidence is admissible in national courts.[34] A draft convention on electronic evidence has recently been prepared by a private initiative. The authentication of electronic evidence and the application of best evidence rules are among the topics covered in this draft convention.[35] This phase includes the search and recognition of relevant evidence, as well as its documentation. During this phase, evidence collection priorities are identified based on the

[33] In D. Utah 1985, Bills v. Kennecott Corp. 108 F.R.D. 459, 462

[34] Vivek Dubey, “Admissibility of Electronic Evidence: An Indian Perspective”4, FRACIJ (2017), 58

[35] Bills vs Kennecott Corp 108 F.R.D. 459, 462 (D. Utah 1985)

value and volatility of the evidence. This phase involves collecting all digital devices that could potentially contain data of evidentiary value. These devices are then returned to a forensic laboratory or other facility for digital evidence collection and analysis. This process is called static acquisition.[36]As digital evidence becomes more common, the International Criminal Court is also facing challenges. The ICC has listed four categories of evidentiary concerns unique to digital evidence: (1) authenticity; (2) hearsay; (3) chain of custody; and (4) preservation of evidence. Rule-69(4) of the ICC Rules of Procedure and Evidence instructs judges to consider the potential value of the evidence for a fair trial and its evaluation. (39) Ad hoc tribunals, on the other hand, support external verification of digital evidence.

4.3 Use and Application of Digital Evidence in Other Countries:

The laws governing the use of digital evidence in criminal cases in nine Asian beneficiary countries—the People's Republic of Bangladesh, the Kingdom of Bhutan, Brunei Darussalam, the Kingdom of Cambodia, the Republic of Maldives, Mongolia, the Federal Democratic Republic of Nepal, the Democratic Socialist Republic of Sri Lanka, and the Socialist Republic of Vietnam—were examined by the Commission of the International Criminal Police Organization of the University of Hong Kong. A claimed questioning was removed from the middle of the film footage in a ruling by the Extraordinary Chambers of the Court of Cambodia on Cybercrime Law because the evidence was repetitive and necessitated a thorough inquiry into its veracity. Despite the fact that the Maldives Evidence Act (1976) has not yet been revised, courts have permitted digital evidence when it is pertinent and compliant with the law. Parliament is now debating a new Evidence Bill that would allow digital

[36] Vivek Dubey, “Admissibility of Electronic Evidence: An Indian Perspective”4, FRACIJ (2017), 58

evidence.[37]According to the Mongolian Criminal Procedure Code (2002) Law, "facts and information relating to the circumstances of the crime" are admissible as evidence.

Electronic recordings can be used as evidence, and the Act recognizes audio and video recordings as "documents" (including images created or derived from recordings).[38] In September 2020, the National Criminal Procedure (Code) Act (2017) and Nepal's Evidence Act (1974) were modified to include specific "provisions" pertaining to digital evidence and audio-visual recordings. Information, documents, data, and other materials maintained in digital form are legally legitimate according to the Electronic Transactions Act (2008). New cybercrime offenses and enforcement authorities are established by the Information Technology Act of 2019.[39] Digital evidence, including computer-generated audio-visual recordings and statements, is admissible under Sri Lanka's Evidence (Special Provisions) Act (1995). The Electronic Transactions Act of 2006 and the Data Messages Act of 2007 both have provisions that, absent contrary evidence, permit the court to assume the veracity or correctness of information contained in electronic documents or records. The Computer Offences Act of 2007 establishes new penalties for cybercrime as well as authority to gather computer data.[40] Indian law has had to evolve as a result of the use of digital evidence in Indian courts. A legal foundation for electronic transactions was created by amending the Indian Evidence Act of 1872, the Indian Penal Code of 1860, the Information Technology Act of 2000, and the

[37] The Electronic Commerce Law was passed on May 2, 2020, and the Electronic Commerce Law of Cambodia was passed on November 6, 2019.

[38] Makulilo, Alex B. The new Evidence Act of 2018, Digital Evidence and Electronic Signature Law Review [accessed April 24, 2022] addresses the admissibility and authentication of digital evidence in Zanzibar.

[39] Acceptance of digital proof, UNODC, 2019 [last visited April 5, 2022]

[40] Digital Evidence and Electronic Signature Law Review 13 S1, Stephen Mason Draft Convention on Electronic Evidence 2016

Bankers' Book Evidence Act of 1891. The Indian Evidence Act of 1872 has been modified under Section 3.[41]

This was done due to the increasing complexity of digital evidence. The case states that the intention of the legislature is clear that if the legislature omits any word, it is 'intentional'. It is generally established that the legislature does not destroy words.[42] To address the rise of cybercrime and to address concerns regarding the admissibility of digital evidence in such cases, the Pakistani legislature has enacted the Electronic Transactions Ordinance, 2002 (ETO).[43] (46) This ordinance fundamentally changes the law of evidence in civil and criminal cases. Essentially, this ordinance makes electronic or digital evidence indispensable. It ensures that digitally stored or transmitted material is not hearsay evidence. This ordinance emphasizes that digital evidence meets the requirements of best evidence.[44]

4.4 Uniqueness of Electronic Evidence:

Physical and visual indicators of the origin and legitimacy of electronic records are absent. As a result, compared to traditional analog recordings, maintaining the content, structure, and context of electronic records is more crucial and challenging. The origin, legitimacy, purpose, and usage of electronic records can all be better understood with the help of metadata, which is simply defined as "data about data." Guidelines must be created to guarantee that electronic

[41] Nepal's National Criminal Procedure (Code) Act (2017) September 2020 and the Digital Evidence Act (1974).

[42] The Digital Evidence Special Provisions Act of Sri Lanka (1995).

[43] Sections 61 to 65 of the Indian Evidence Act of 1872.

[44] Shweta and Ahmad (n-62) 7

records maintain authenticity, correctness, integrity, and accessibility because they are so easily altered and shared.[45]

The Evidence Taking Regulation is an instrument dedicated to cooperation in the taking of evidence in cross-border proceedings, the text of this Regulation was amended in 2020 and the new provisions will apply between EU Member States (except Denmark) on 1 July 2022 (Article 35 Evidence Recast). These regulations can be relied on when it is necessary to take evidence abroad in civil and commercial court proceedings. However, their use is not mandatory and is left to the choice of the requesting court and the interested parties. So far, in practice, there has been a tendency to avoid the use of evidence taking regulations whenever possible. This is to avoid a solution that is often seen by practitioners as "difficult, bureaucratic and time-consuming". Courts conducting trials try to resort as much as possible to taking evidence in their own country, based on their own national procedural rules or through designated experts.[46]

4.5 Conclusion:

E-Governance is highlighting electronic evidence as an important means of communication, processing and recording in both public and private sectors. However, before it may be presented before the court to support a claim, a number of requirements must be met. Digital evidence is sometimes used as primary evidence, sometimes as secondary evidence and sometimes as supportive evidence. Sometimes it is given probative value, and sometimes the

---

[45] Dr. UsmanHameed, ZarfishanQaiser, and KhushbakhtQaiser, Digital Evidence Admissibility: A Pakistani Justice System Perspective [2021], PSSR, Vol. 5 No. 4 [518-530] < https://pssr.org.pk/issues/v5/4 /admissibility of digital evidence a perspective of the Pakistani legal system>

[46] Shweta and Ahmad (n-62) 7

verdict is based entirely on digital evidence. Depending on its importance and significance, digital evidence plays a crucial role. Digital evidence has been crucial in guaranteeing justice in the courts, regardless of whether it is the finest evidence..

Contact information, transactional information, cloud storage data, social media material, and web surfing data are the most prevalent kinds of digital evidence. Digital evidence must be relevant, accurate, and verified in order to be admitted in court, according to the Federal Rules of Digital Evidence. Digital evidence is frequently used in criminal cases like identity theft and cybercrime, but it is also frequently used in family and employment law trials, IP protection lawsuits, and regulatory compliance cases. Organizations might approach litigation more pro-actively with the use of data archiving.

Chapter Five

Finding Equation and Concluding Remarks:

5.1 Results:

1. The rule of best evidence ensures that evidence is correct in court. If the party providing the evidence cannot prove its correctness and validity, the court will reject it and take legal action.

2. All digital/electronic data is a ‘copy’. A copy is the original data stored in a computer of digital evidence. Since digital data is created, stored and rarely printed. Since best evidence refers to the original document, a copy obtained from an electronic device qualifies as an original.

3. Digital evidence is considered primary evidence rather than just supporting evidence. When no other evidence is available, digital evidence is accepted as primary evidence in court and has been used to render a verdict.

4. Although the results are not 100% accurate, digital evidence has proven to be efficient in detecting crimes in the modern world. Which helps in settling cases.

5. The Evidence Act of 1872 is outdated. Digital evidence has been modified and used in other countries in similar geographical areas. Not only that, digital evidence is widely considered to be the best evidence.

6. Before digital evidence can be used in court, a number of prerequisites must be fulfilled.

7. Digital evidence is given probative value only when it is presented with other evidence.

8. In the UK and the US, the requirements for digital evidence are different. Despite its flaws, digital evidence was admissible in US courts. Even copies of computer data were accepted as the best evidence.

9. India has strict requirements for digital evidence, while Pakistan is relatively lenient.

10. Digital evidence is more durable than paper. Digital equipment can be easily repaired, but documentary evidence that has been shredded or destroyed cannot be restored.

5.2 Recommendations and Suggestions:

At a time when digital evidence was not widely used, documentary evidence was considered the best evidence. When papers and images could only be copied by hand, the rule of best evidence was of utmost importance. Most evidence can now be digitized in high-resolution form and some courts have started to view digital copies as equivalent to the original. It is a promising start that digital evidence is being allowed for the purpose of adjudicating in the courtrooms of Bangladesh. On the other hand, it is unfortunate that digital evidence is not yet legally included or covered by a separate law. From the above explanation, it seems that digital evidence has the potential to be the best evidence, or can be included or considered under the rule of best evidence in Bangladesh.

The problem is not the digital evidence itself, but rather the lack of expertise in collecting and creating it. This is because digital forensic professionals need to have extensive knowledge of computer science and information security methods and tools. Therefore, continuous training of those involved in the investigation and collection of computer-related crimes is essential to strengthen and improve the admissibility of digital evidence in Bangladesh. In addition, there is a need to establish digital evidence-specific rules in Bangladesh. This will include providing a legal framework for the means, conditions and processing of electronic evidence at the stage of criminal investigation, prosecution and information gathering. In addition, harmonisation and evolution can begin with the amendment of Section 3 of the Evidence Act, 1872, which will include digital evidence in the definition of document.

This amendment can further broaden the concept and understanding of document, whereby digital evidence can be considered not only as evidence but also as the best evidence in support of the case. Ultimately, it involves both experts and the court. Experts apply skills and tools to confirm or deny evidence. However, the court considers it. Training of digital forensic professionals and provision of digital forensic tools/machines can ensure the reliability of digital evidence in Bangladesh.

Bibliography

Legislations:

1. The Evidence Act of 1872 (I of 1872)
2. The 1897 General Clauses Act (X OF 1897)
3. The 1860 Penal Code (XLV of 1860)
4. The 1995 Civil Evidence Act
5. The Indian Evidence Act of 1872
6. The 2015 Federal Rules of Evidence
7. The 1968 Civil Evidence Act
8. The 1984 Police and Criminal Evidence Act

Case Laws:

9. Omychund v. Barker [1744] Willes 538; 125 ER 1310
10. Hunter v. Garton [1969] 1 Every ER 451 [1969] 2 QB 37
11. Lorraine v. Markel, 241 F.R.D. 534 (D. Md. 2007)
12. The State v. Mrs. KhaledaAkhtar, 37 DLR, (HCD) (1985) 275
13. Qamrul Islam & others v. State 2017(2) LNJ (HCD) 303
14. The State 18 BLT (AD) v. Major Bazlul Huda & Others (2010) 7
15. Shephard v. R (1988) 86 Cr App R 47
16. Crim. L.R. 199 (C.A.Cr.D.) IN R. vs. SPIBY [1991]
17. HOBSON vs. Cambridge London Borough Council
18. CATABRANIS v. United States
19. ANVAR CASE (2014) 10 SCC 473