# Sonargaon University (SU)

## Research Monograph

## On

## "Admissibility and Reliability of Digital Evidence in Criminals Trials: Challenges in the Modern Criminal Procedure System"

**Research Monograph Submitted for the partial fulfillment of the award of the degree in**

**LL.B (Hon's)**

**Department of Law**

**Sonargaon University (SU)**

## Submitted To


**Sunzida Akter**

Lecturer

Department of Law

Sonargaon University (SU)


## Submitted by


**Md. Mahmodul Hasan Habib**

ID No. LL.B 2203027023

Program: LL.B (Hon's)

Department of Law

Sonargaon University (SU)


## Date of Submission: 25th June, 2026

# Letter of Transmittal

To

**Sunzida Akter**

Lecturer

Department of Law

Sonargaon University (SU)

Subject: Submission of Research Monograph on "**Admissibility and Reliability of Digital Evidence in Criminals Trials: Challenges in the Modern Criminal Procedure System"**

Dear Sir,

This is a great pleasure to submit the Research Monograph on **"Admissibility and Reliability of Digital Evidence in Criminals Trials: Challenges in the Modern Criminal Procedure System"** as a partial requirement for the fulfillment of my LL.B course under the Department of Law of the Sonargaon University (SU).

I have given due efforts to make this Research Monograph as fruitful one and to make it as informative as possible. I hope that this paper will not be the formality of academic course completion rather it will be a source of information for other purpose on this topic.

Yours sincerely

.....

**Md. Mahmodul Hasan Habib**

ID No. LL.B 2203027023

Program: LL.B (Hon's)

Department of Law

Sonargaon University (SU)

# Declaration

I do hereby declare that the Research Monograph Title **"Admissibility and Reliability of Digital Evidence in Criminals Trials: Challenges in the Modern Criminal Procedure System"** prepared solely by me and which has been submitted to the department of Law, Sonargaon University (SU) for achieving the LL.B (Hon's) Degree. This is an original work of nine. No part of this research, in any way of or in from, has been submitted to any University or Institution for any Degree, Diploma or for other similar purposes.

.....

**Md. Mahmodul Hasan Habib**
ID No. LL.B 2203027023
Program: LL.B (Hon's)
Department of Law
Sonargaon University (SU)

# Supervisor Certificate

This is to certify that the work presented in this dissertation is based on the work, carried out by the author herself under my supervision in Department of Law, Sonargaon University (SU).

It is also certifying that the work presented here is original and suitable for submission as the style and contents, for fulfillment of LL.B. program.

.....

**Sunzida Akter**
Lecturer
Department of Law
Sonargaon University (SU)

# Acknowledgement

I am deeply gratitude to Almighty Allah for providing me everything that required for completing my research work. I am thankful to my supervisor **Sunzida Akter** for instructing me how to prepare a Research Monograph and his famous Books lectures on this subject help me to complete my task sincerely.

For giving me the opportunity and support to complete this research on **"Admissibility and Reliability of Digital Evidence in Criminals Trials: Challenges in the Modern Criminal Procedure System"**. I am very grateful to him for his proper guidance, helpful discussions, constructive criticism, valuable editorial assistance and advice during the preparation of this research paper. Without his help, it was almost impossible for me to complete the research work. I would like to convey my heartiest respect and special thanks to him. I am also thankful to him for helping me in terms of methodology procedure of the research paper.I would like to express my gratefulness to my friends as well as wishers to me for their motivation from the beginning of my research work.

Thank you

**Md. Mahmodul Hasan Habib**

# ABSTRACT

The implementation of Admissibility and Reliability of Digital Evidence in Criminals Trials: Challenges in the Modern Criminal Procedure System . *It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education.* With the advent of Information Technology (IT), Internet and Information and Communication Technology (ICT), the world civilization is facing new dimension of criminal offence. *This chapter firstly identifies the definition and then focuses on history and background of Digital Evidences Act crime, nature of Digital Evidences Act crime,* Classification of Digital Evidences Act Crime. Crime' is more or less known to each individual on his own stand point, while 'Digital Evidences Act' is almost vague in meaning to the same. Digital Evidences Act crime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Digital Evidences Act crime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

# Contents

**Chapter- 5: General Conclusion**

# CHAPTER 1
# INTRODUCTION

## 1.1. STATEMENT OF THE PROBLEM

Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes within the ambit of Digital Evidences Act crime.[1] or Any unlawful acts wherein the computer is either a tool or target or both.[2] are called Digital Evidences Act crime. It is the newest member of crime world. Digital Evidences Act crime is very different from the use of computers for a traditional activity. Its multi-million problems by using computer to commit Digital Evidences Act terrorism, financial cheating, by giving attractive advertising in the website or enticement by email, credit card frauds, IPR violation, harassments, fraud, hackers, pornography, virus introduction, stalking, surveillance, theft, disabling computer data, software and hardware, theft of valuable information, international money laundering through internet and online gambling are the most using way to cheating Bangladeshi people.

Late enacted Information and Communication Technology Act, 2006 has defined Digital Evidences Act crime and brought this crime under our criminal jurisprudence. However, there are many other things need to be included in the Act and we have to enact and implement appropriate laws to address the problem of Digital Evidences Act crime.[3] In Bangladesh there are no sufficient laws or other instruments to prevent Digital Evidences Act crime mentioned above. Bangladesh is a developing country. Its technology is also being developed day by day. The problems I sorted out in this regard are as follows-

- The problem of Digital Evidences Act crime in Bangladesh is burning question. Now-a-days we observe that different sectors, such as education, bank and multinational company are affected by Digital Evidences Act crime.
- The punishment provided in the case of Digital Evidences Act law is not enough.
- There is no authority to monitor the misuses of Digital Evidences Act law.

So, considering above mentioned in this research I am going to deal with these problems.

[1] <http://jabalpurpolice.org/cyber_crime.php> Accessed on 02.03.2025
[2] <http://jabalpurpolice.org/cyber_crime.php> Accessed on 02.03.2025
[3] <http://www.thedailystar.net/law/2009/06/03/watch.htm> Accessed on 02.03.2025

## 1.2. IMPORTANCE OF THE STUDY

Research is an important element of modern system of legal education. It performs several related functions: attaining theoretical knowledge, practical training & a general education contributing to proper legal reasoning, effective communication & ethical responsibility. Research methodology is important for researchers in a number of ways. A student should learn about research so that he can critically analyze information on a variety issues. Legal research is also important for lawyer, who as a real-life problem solver should be familiar with those areas of law in which he claims to have expertise. Research is critically important for initiating reform & change in a society. Research can initiate a new theory of variety issues, challenge old one or help in clarifying existing theory. The findings of research may be helpful to bring about deserve changes in existing institutions.[4]

With the advent of Information Technology (IT), Internet and Information and Communication Technology (ICT), the world civilization is facing new dimension of criminal offence. Digital Evidences Act law is a new phenomenon of modern technological development. This is also a new concept in our country. About Digital Evidences Act crime in Bangladesh there is no available books, journals or effective research or work is made on it. For this reason I have chosen to work on *"Digital Evidences Act Crime in Bangladesh"*. In my research I will focus on the concept of Digital Evidences Act crime and many other related things so that students, teachers, lawyers, policy makers and overall our country will be benefitted by the findings of my research.

## 1.3. OBJECTIVES OF THE RESEARCH

The main objectives of this research are:

1) To explore the nature of contemporary Digital Evidences Act crimes and its consequences in Information and Communication Technology (ICT).
2) To analyze the related Digital Evidences Act Laws of Bangladesh.
3) To examine the legal measure against the Digital Evidences Act Crimes in Bangladesh.

## 1.4. RESEARCH METHODOLOGY

To prepare the research paper some secondary data have been collected and analyzed from the various sources. Such as, most of the information has been furnished through internet, books, journals, article's, various papers as well as others field. Although the research

[4] Abdullah Al Faruque, *Essentials of Legal Research,* (2nd ed., Dhaka: Palal prokashoni, 2010), pp. 14-15.

methodology consisted of both a quantitative and qualitative approach, in this research mainly qualitative method have been followed. Moreover to make this research paper effective, I have collected materials from the oral sources and other related sources.

**1.5. SOURCES AND MATERIALS**

To prepare this research paper some secondary data has been collected and analyzed from the various sources. Such as: Most of the information has been furnished through internet, books, journals, article's, and various papers as well as others field.

**1.6. REVIEW OF LITERATURE**

A few numbers of writers have written books on the Digital Evidences Act Law in Bangladesh perspective. They have expressed their concept in deferent ways. Some of the books are reviewed below:

**(1)** Prof. Md. Borhan Uddin. (1st Edition: January, 2008 & February, 2010), Principles of Digital Evidences Act Law, Shams Publications, Dhaka.

This book contains different aspects. The author this book had divided into thirty one chapters. The new enacted laws are included in this book. The subject has been approached in a legal perspective with emphasis on recent development in the field of Digital Evidences Act law and Digital Evidences Act crime. The author has endeavored to achieve the objects of Digital Evidences Act law and Digital Evidences Act crime. To know about Digital Evidences Act crime and its nature this book may help in number of different ways. Enough topics are written down and the author also has mentioned some Digital Evidences Act Crime Cases. But this book is not sufficient to know deeply about the topic and did not mention about the history of digital computer, internet and the genesis object and scope of the IT. There is no any significant suggestion about the future of Information and Communication Technology (ICT) sector of Bangladesh.

**(2)** Dr. Zulfiquar Ahmed (1st Edition: March, 2009), A Text Book on Digital Evidences Act Law in Bangladesh, National Law Book Company, Dhaka-1205.

This book contains different aspects. The main objective of this book is to serve the mission to spread Digital Evidences Act Law literacy. In this book the writer has been stressed mainly on the Information and Communication Technology Act, 2006. And he mentioned the topic broadly and discussed Digital Evidences Act Law of Bangladesh perspective. The author has discussed many important topics on Chapter Eight such as:

- Its Crime, Investigation, Judgment and Punishment.
- The Establishment of Digital Evidences Act Tribunal, Enquiry, Trial and Appeal of Crimes etc.

- Establishment of Digital Evidences Act Appeal Tribunal etc.

The history and definition of this book it is supposed to be discussed in the first chapter but the writer has mentioned it on chapter Eight.

I think that, this is the new concept in Bangladesh. So, my suggestion is the definition and history of the Information and Communication Technology (ICT) sector of Bangladesh should have mentioned at the first.

**(3)** Dr. Farooq Ahmad (2nd Edition: 2005), Digital Evidences Act Law in India (Law on Internet), New Era Law Publications, Law Book Publishers, 1159, Outram Lines, Near Kingsway Camp, Delhi 110009.

This book contains different aspects. To know about Digital Evidences Act crime and its classification this book may help in number of different ways. But this book is not enough to know more about the topic and did not mention the definition of the Digital Evidences Act Law, Digital Evidences Act Crime and its concept. It would be clearer if the definition of the Digital Evidences Act Law, Digital Evidences Act Crime and its concept broadly discussed. There is no any significant suggestion about the future of Information and Communication Technology (ICT) sector of today's and future world.

**(4)** Justice Yatindra Sign (2nd Edition: 2005), Digital Evidences Act Laws, Universal Law Publishing co. Pvt. Ltd. C-FF-1A, Ansal's Dilkhush Industrial Estate, G.T. Karnal Road, Delhi- 110033.

This book contains different aspects. The author has included cases decided since then, chapter 1 of the book which deal with the IT act has been arranged so as to broadly refer to the chapters and sections of the IT act.

This book is not sufficient to know deeply about the topic and it has not mentioned the history of digital computer, internet and the genesis object and scope of the IT. This book has not mentioned the definition of the Digital Evidences Act Law, Digital Evidences Act Crime and its concept and the entire topic are very short form. There is no any significant suggestion about the future of Information and Communication Technology (ICT) sector.

**(5)** Dr**.** R. K. Chaubey (1st Edition: 2009), An Introduction to Digital Evidences Act Crime and Digital Evidences Act Laws, Kamal Law House, Kolkata.

This book contains different aspects. To know about Digital Evidences Act crime and its definition, History and Background of Digital Evidences Act Crime, Nature of Digital Evidences Act Crime, Classification of Digital Evidences Act Crime, Characteristics of Digital Evidences Act Crime and kinds of Digital Evidences Act crime this book may help in

number of different ways. I think the kinds of Digital Evidences Act crime in this book discussed broadly. So, I think in my research paper mentioned above topics will be helpful.

### 1.7. SCOPE AND LIMITATION OF THE STUDY

The term Digital Evidences Act crime is not brief but it is vaster. This research will deal with the different aspects of Digital Evidences Act crime in Bangladesh. Particularly, it will analyze the concept and consequences of Digital Evidences Act crime. However this research will not concentrate on all the issues relating to Digital Evidences Act crime. International perspective will not be included in my research broadly. Because my topic is limited only in Bangladesh for this reason I tried my best to focus Digital Evidences Act crime in Bangladesh.

# CHAPTER 2
# THEORETICAL FRAMEWORK

## 2.1. INTRODUCTION

We are living in a digital world where computers are not just an ordinary thing anymore but a "necessity" to our everyday life. The internet in Bangladesh is growing rapidly. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. With the advent of Information Technology (IT), Internet and Information and Communication Technology (ICT), the world civilization is facing new dimension of criminal offence. This chapter firstly identifies the definition and then focuses on history and background of Digital Evidences Act crime, nature of Digital Evidences Act crime, Classification of Digital Evidences Act Crime. Finally the chapter analyses the Challenge of Digital Evidences Act Crimes, Characteristics, and victims of Digital Evidences Act Crime.

## 2.2. DEFINITION OF DIGITAL EVIDENCES ACT CRIME

Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes within the ambit of Digital Evidences Act crime. or Any unlawful acts wherein the computer is either a tool or target or both. are called Digital Evidences Act crime.

The term *'Digital Evidences Act crime'* has been evolved from two words *'Digital Evidences Act'* and *'crime'*. 'Crime' is more or less known to each individual on his own stand point, while 'Digital Evidences Act' is almost vague in meaning to the same. So if any time anybody uses the prefix 'Digital Evidences Act', we simply mean, he is talking about something is doing online or there has certain networking system. Actually anything related to Internet falls under the Digital Evidences Act category.[5]

Computer crime or Digital Evidences Act crime is a form of crime where the Internet or computers are used as a medium to commit crime. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement Child pornography, and child grooming.[6]

Digital Evidences Act crime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Digital Evidences Act crime also includes non-monetary offenses, such

[5] M. Abul Hasanat, *'Cyber Crime: An Ill-going Techno - Culture'*, Journal of Law, Vol. 1, no.1 (June 2003), p.15.

[6] <http://en.wikipedia.org/wiki/Cyber_crime> Accessed on: 21.03.2025

as creating and distributing viruses on other computers or posting confidential business information on the Internet.[7]

## 2.3. HISTORY AND BACKGROUND OF DIGITAL EVIDENCES ACT CRIME

The internet has revolutionized how individuals interact with each other. After four years of the Internet, fifty million people are connected to this global network. It took the radio thirty-eight years to reach fifty million users, and a mere sixteen years for the computer to reach fifty million users. The popularity of the Internet is growing exponentially.[8] The first recorded Digital Evidences Act crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. This is the first recorded Digital Evidences Act crime.[9] Interpol was the first international organization dealing with computer crime and penal legislation. In conjunction with an Interpol Conference in 1981, a survey of Interpol member countries on computer crime and penal legislation identified several problems in the application of existing penal legislation. The OECD in Paris appointed in 1983 an expert committee to discuss computer-related crime and the need for changes in the penal Codes. This committee made a proposal that could constitute as a common denominator between the different approaches taken by the member countries. The Council of Europe appointed in 1985 another expert committees in order to discuss the legal issues of computer-related crime. A summary of the guidelines for national legislatures with liability for international acts only, was presented in the Recommendation of 1989. The UN adopted a resolution on computer crime legislation at 8$^{th}$ U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba, in 1990. The United Nations Manual on the Prevention and Control of Computer-related Crime was published in 1994. The last part of this historic presentation is the Wurzburg conferences organized by the University of Wurzburg in 1992. These conferences led to 29 national reports, and recommendations for the development of computer crime legislations. Most countries in Europe adopted new penal laws according to the recommendation in the 1980s and 90s. Similar development occurred in the U.S.A. Canada and Mexico also in Asia, where Japan, Singapore, Korea and Malaysia were the leading countries. In Australia, the Commonwealth added computer crime laws to *the Crimes Act* in 1989. Today computers have come a long way, with neutral networks and

[7] < http://www.techterms.com/definition/cybercrime> Accessed on: 21.03.2025

[8] <http://www.associatedcontent.com/article/44605/cybercrime_a_revolution_in_terrorism.html?cat=37> Accessed on: 21.03.2025

[9] R. K. Chaubey, *An Introduction to Cyber Crime and Cyber Laws*, (1$^{st}$ ed., Kolkata: Kamal Law House, 2009), p.137.

nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.[10]

## 2.4. NATURE OF DIGITAL EVIDENCES ACT CRIME

A Digital Evidences Act criminal can destroy websites and portals by hacking and planting viruses, carry out online frauds by transferring funds from one corner of the globe to another, gain access to highly confidential and sensitive information, cause harassment by e-mail threats or obscene material, play tax frauds, indulge in Digital Evidences Act pornography involving children and commit innumerable other crimes on the Internet. It is said that none is secure in the Digital Evidences Act world. The security is only for the present moment when we are actually secure. With the growing use of the Internet, Digital Evidences Act crime would affect us all, either directly or indirectly.[11]

## 2.5. TOOLS AND METHODS OF DIGITAL EVIDENCES ACT CRIME

Digital Evidences Actcriminals are using numerous illegal tools: *keylogging*—using software or devices to secretly monitor and record keystrokes, enabling espionage activities or the harvesting of personal data; *distributed denial of service* (DDoS)—inundating computer system resources with tasks sufficient to render them unavailable to authorized users; *pharming*—directing traffic from a legitimate Web site to a site controlled by a criminal hacker; *phishing*—illegally accessing an individual's financial data to capture online banking and financial information; and, most recently, *botnets*—networks of infected machines, usually managed by a single command center, that are capable of causing serious damage to networked systems and enabling large-scale identity theft. Hackers obtain botnets commercially, using them to access bank accounts.[12]

## 2.6. CLASSIFICATION OF DIGITAL EVIDENCES ACT CRIME

Digital Evidences Act Crimes can be mainly classified as: Traditional crimes committed on or through the new medium of the Internet. For example, cheating, fraud, misrepresentation, defamation, pornography thefts etc. committed on or through or with the help of the internet would fall under this category. New crimes created with the Internet itself, such as hacking and spreading viruses etc. New crimes used for commission of old crimes for example, where hacking is committed to carry out Digital Evidences Act frauds.

Digital Evidences Act crimes have been classified on the basis of the nature and purpose of the offence and have been broadly grouped into three categorized depending upon the target

[10] Ibid, pp.139-140.
[11] Ibid, p.141.
[12] <www.ncjrs.gov/pdffiles1/nij/231832.pdf> Accessed on: 05.04.2025

of the crime. It may be against person, property or Government. The Digital Evidences Act crimes against person include crimes like hate message, stalking, defamation and transmission of programmes and unauthorized possession of computerized information. The third category of Digital Evidences Act crimes targets the Governments. This category of Digital Evidences Act crime is more popularly called as Digital Evidences Act terrorism.

The most comprehensive classification of computer crimes has been given by David L. Carter who classified computer- related crimes into three broad categories. Those are given below:

(a) Where computer is the target of the crime;
(b) Where computer facilitates the commission of crime;
(c) Where computer is incidental to the crime.

Three categories of computer- related crimes are describing below:

**Computer as target of the Crime**

This category of computer crimes aims at damaging computer system or stealing valuable information stored on the system and includes:

1. Sabotage of computer and computer systems or computer networks;
2. Theft of data/information;
3. Theft of intellectual property such as computer software;
4. Theft of marketable information;
5. Blackmail based on information gained from computerized files, such as medical information, personal history, sexual preferences, financial data etc.
6. Unlawful access to criminal justice and the Government records.

**Computer as an instrument of Crime**

The computer crimes falling under this category use computer as a medium for commission of offences. The computer programmes are manipulated to defraud others. Those are given below:

1. Fraudulent use of Automated Teller Machine (ATM) cards and accounts;
2. Credit card frauds;
3. Frauds involving electronic fund transfers;
4. Frauds involving stock transfers;
5. Frauds relating to e-commerce;
6. Telecommunication frauds

**Computer as incidental to the Crime**

The diverse application of internet made it incidental to the crimes that may be classified into two broad categories.

(A) Internet crime;

(B) Web based crime.

**(A) Internet crime**

The internet crimes include that group of crimes that makes criminal use of the internet infrastructure. These are:

(i) Hacking –

(a) Theft of information;

(b) Theft of passwords;

(c) Theft of credit card numbers.

(ii) Launch of malicious programmes;

(iii) Espionage;

(iv) Spamming.

**(B) Web based Crimes**

Web based crimes have been categorized separately and have been further classified into four subcategories.

(a) Web site related crime –

(i) Cheating and frauds;

(ii) Insurance frauds;

(iii) Gambling;

(iv) Distribution of pornography;

(v) Sale of pirated software.

(b) Crimes through e-mail –

(i) Threats;

(ii) Extortion;

(iii) E-mail bombing;

(iv) Defamation;

(v) Launching of malicious programmes

(c) Usenet related crimes –

(i) Distribution/sale of pornography material;

(ii) Distribution/sale of pirated software;

(iii) Discussion on methods of hacking;

(iv) Sale of stolen credit card numbers;

(v) Sale of stolen data.

(d) Internet relay chat crime –

(i) Digital Evidences Act stalking;

(ii) Fraudsters use chat rooms for developing relations with unsuspecting victims;

(iii) Criminal use it for meeting conspirators;

(iv) Hackers use it for discussing their expertise of showing the techniques;

(v) Pedophiles use chat rooms to allure small children.[13]

## 2.7. CHALLENGE OF DIGITAL EVIDENCES ACT CRIMES

Digital Evidences Actspace does not recognize geographical boundaries. This has proved a boon to the delinquents who perform illegal activities on the internet without any fear of being identified or located. Lack of knowledge of actual working of internet on the part of law enforcement agencies further complicates the matter. The challenges posed by Digital Evidences Act crimes are classified as:

(i) Legal challenges which are dependent on the statutory provisions to be used as a tool investigate and control the Digital Evidences Act crimes.

(ii) Operational challenges require a cohesive well trained and well equipped force of investigators operating and coordinating at national and international level.

(iii) Technical challenges thwarting the efforts of law enforcement agencies ability to catch and prosecute the online offenders.

Digital Evidences Act crimes are often committed beyond the national borders. The national standards of criminal behavior vary. Furthermore it is very difficult to identify the perpetrator of wrong because internet facilitates anonymity. Thus Digital Evidences Act crimes pose challenges that are unique in character unlike traditional crimes. These crimes cannot be effectively dealt with by simply passing national legislation. The IT act has extra territorial jurisdiction and applies to any offence or contravention thereunder committed outside Bangladesh by any person. This feature of the IT is not unusual. Similar provision is found in the IT legislations of other jurisdictions also. However, this provision can be effective only when there is mutual cooperation at the international level amongst enforcement authorities and Governments.[14]

---

[13] Farooq Ahmad, *Cyber Law in India (Law on Internet)*, (2nd ed., Delhi: New Era Law Publications, 2005), pp. 302-305.

[14] Ibid, pp.305-306.

## 2.8. CHARACTERISTICS OF DIGITAL EVIDENCES ACT CRIME

After the classification of Digital Evidences Act crime and before examining the legal strategies to check Digital Evidences Act crime, it is necessary to examine the peculiar characteristics of Digital Evidences Act crime. The weapon with which Digital Evidences Act crime are committed is technology. Digital Evidences Act crimes are the work of technology and thus Digital Evidences Act criminals are technocrats who have deep understanding of the Internet and computers. Digital Evidences Act crime is extremely efficient, i.e. it takes place in real time. It may take seconds or a few minutes to hack websites or do Digital Evidences Act frauds. Digital Evidences Act crime knows no geographical limitations, boundaries or distances. A Digital Evidences Act criminal in the one corner of the world can commit hacking on a system in the other corner of the world for example a hacker in the US can in real time hack in the system placed in Japan. The act of Digital Evidences Act crime takes place in Digital Evidences Actspace which makes the Digital Evidences Act criminal being physically outside Digital Evidences Actspace. All the components of Digital Evidences Act criminality from preparation to execution, take place in the Digital Evidences Actspace. Digital Evidences Act crime has the potential of causing harm and injury which is of an unimaginable magnitude. It can easily destroy websites created and maintained with huge investments or hack into website of Banks and the defense department's websites. The amount of loss which may cause is easy to be imagined. It is extremely difficult to collect evidence of Digital Evidences Act crime and prove the same in the Court of law, due to the anonymity and invisibility of Digital Evidences Act criminal and its potential to affect in several countries at the same time, which are different from the place of operation of the Digital Evidences Act criminal.[15]

## 2.9. VICTIMS OF THE DIGITAL EVIDENCES ACT CRIME

**Digital Evidences Act crime basically occurs against:**

**Person:** Digital Evidences Act crime committed against persons includes various crimes like transmission of child-pornography of any one with use of computer such as e-mail and Digital Evidences Act-stalking etc.

1. **Government:** The second category of Digital Evidences Act crime related to Digital Evidences Act crime against Government. Digital Evidences Act terrorism is one distinct kind of crime in this category. The growth of Internet has shown that individual and groups to

[15] R. K. Chaubey, Ibid, pp.141-142.

threaten the international Governments as also to terrorize the citizen of a country are using the medium of Digital Evidences Act space. The crime manifests itself into terrorism when individual 'racks' into a government or military maintained website.

**2. Property:** the third category of Digital Evidences Act crime is that of Digital Evidences Act crime against all forms of property. These Digital Evidences Act crimes include unauthorized computer trespassing through Digital Evidences Actspace embezzlement computer vandalism transmission of harmful programs and unauthorized possession of computerized information.

**65% of Web Users Are Victims of Digital Evidences Actcrime:**

Nearly two thirds (65 percent) of web users across the world have been the victim of Digital Evidences Actcrime, says Symantec. According to the security firm's "Norton Digital Evidences Actcrime Report: The Human Impact," 58 percent of victims of Digital Evidences Actcrime, which includes viruses and online credit card fraud, feel angry, while 51 percent said they were annoyed and 40 percent admitted to feeling cheated. Furthermore, 80 percent of web users don't believe the Digital Evidences Actcriminals will be caught while only three percent believe they won't fall victim to crime online.[16]

**Over 1 Million Digital Evidences Act Crime Victims a Day in 2010:**

The 2011 Norton Digital Evidences Act Crime Report was released yesterday which is based on the company's analysis of an online survey of 19,636 respondents from 24 countries. The survey was conducted between 06 February and 14 March 2011.

Given the survey an answer, Norton says that it calculates that a total of 431 million adults living in the surveyed 24 countries have been Digital Evidences Act crime victims within the past 12 months. This equates, it says, to 14 Digital Evidences Act crime victims every second; 820 Digital Evidences Act crime victims every minute; or almost 50,000 per hour. Some 74 million US residents were Digital Evidences Act crime victims last year, the report states.

The Norton report also says that the direct cost of this Digital Evidences Act crime activity was approximately $114 billion - with another $274 billion in indirect costs related to lost time/productivity. This total of $388 billion "...costs the world significantly more than the global black market in marijuana, cocaine and heroin combined ($288 billion)."

[16] <http://www.pcworld.com/article/205309/65_of_web_users_are_victims_of_cybercrime.html> Accessed on: 13.04.2025

In another Digital Evidences Act security statistic released this week, the Digital Forensics Association says that it has analyzed 3,765 data loss incidents from 33 countries over the past six years in which 806.2 million records have been known to have been improperly disclosed in one way or another. On average, its press release states, "... organizations lost over 388,000 people's records per day/15,000 records per hour every single day for the past six years."[17]

**2.10. CONCLUSION**

The term Digital Evidences Act crime has nowhere been defined in any statute /Act passed or enacted by the Bangladesh Parliament. Digital Evidences Act crime is an evil activities occurred by computers in modern life. One statistics shows that nearly two thirds (65 percent) of web users across the world have been the victim of Digital Evidences Actcrime, says Symantec and over 1 Million Digital Evidences Act crime victims a day in 2010**.** Where information and communication technology gives us a lot of advantages and our work is being easier than before and we can communicate each other from one side to another side in the world. Now a days when everything from microwave ovens, refrigerators, nuclear power plants, entertainment, business, sports, medical, education, weather update, and so many things are being operated by computers. But besides these advantages also is being misused.

[17] <http://spectrum.ieee.org/riskfactor/telecom/security/over-1-million-cyber-crime-victims-a-day-in-2010-> Accessed on: 13.04.2025

## CHAPTER 3
## KINDS OF DIGITAL EVIDENCES ACT CRIME

### 3.1. INTRODUCTION

In Bangladesh most of us only knew a little about computer security threats**,** the most common were "*virus*" and "*worm*". Let me examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Here is the list of the prevalent Digital Evidences Act Crimes, some of which are more widely spread and harmful. There are two sides of a coin. Internet also has its own disadvantages. One of the major disadvantages is Digital Evidences Act crime – illegal activity committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like hacking, virus, trojans and worms, Digital Evidences Act pornography, Digital Evidences Act stalking, Digital Evidences Act terrorism, Digital Evidences Act crime related to finance, Digital Evidences Act crime with mobile and wireless technology, phishing, denial of service attack (Dos Attack), e-mail bombing and so on, which invade our privacy and offend our senses.

### 3.2. HACKING

'Hacking' means unauthorized access to a computer system. It is the most common type of Digital Evidences Act crime being committed across the world. The word 'hacking' has been defined in *section 56 of the Information & Communication Technology Act 2006,* as follows: Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any Act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects in injuriously by any means; harm any computer, server, computer network or any other electronic system by accessing it unlawfully and in which that person has no legal authority; he commits the offence of "hacking".[18] Whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to taka one crore or with both.[19]

The person who commits an offence of hacking is called hacker. Hacker is a person who intends to gain unauthorized access to a computer system. Jargon Dictionary traces the origin

[18] Zulfiquar Ahmed, *A Text Book on Cyber Law in Bangladesh,* (1st ed., Dhaka: National Law Book Company, 2009), pp.63 – 64.
[19] The Information and Communication Technology Act, 2006, s. 56(2).

of the term 'hacker' to someone who makes furniture with an axe and the term has been used for the first time in 1960's as a badge by hacker culture surrounding the Tech Model Railroad Club (TMRC) at Massachusetts Institute Technology when its members began to work with computers.[20]

Webster's Dictionary defines the term 'hacker' as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance.[21]

The word 'hacker' represents now any person-

(a) Who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
(b) Who programmes enthusiastically.
(c) Who enjoys programming rather than just theorizing about programming.
(d) Capable of appreciating hack value, which is defined as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a particular programme or one who frequently does work using it or on it.[22]

**Examples of Hackings in Bangladesh:**

Some Examples of Hacking in Bangladesh are given below:

Recently Indian hacker groups will be destroyed by Digital Evidences Act space as it was announced. Government of Bangladesh has already made an attack by the Indian hacker group – large or small 50 websites. 300 to 400, as well as private organizations and websites have already been attacked. On the other hand, there are hundreds of Indian websites hacked by Bangladeshi hackers. The websites of the government and commercial organizations. Bangladesh started on Thursday. And not only have this but also frequently we are facing liked this problem from last few years.[23]

### 3.3. VIRUS, TROJANS AND WORMS

A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programmes like word processor or spreadsheets or they attach themselves to the boot sector of a disk. A computer worm is a self-contained program that is able to spread functional copies of itself or its segments to other computer systems. Unlike viruses, worms do not need

[20] Farooq Ahmad, Ibid, p. 329
[21] Ibid, p. 329
[22] Ibid, p. 329
[23] < http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-02-2025&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5> Accessed on: 13.02.2025

to attach themselves to a host program.[24] A computer virus is a small software program that spreads from one computer to another computer and that interferes with computer operation. A computer virus may corrupt or delete data on a computer, use an e-mail program to spread the virus to other computers, or even delete everything on the hard disk. Computer viruses are most easily spread by attachments in e-mail messages or by instant messaging messages. Therefore, you must never open an e-mail attachment unless you know who sent the message or unless you are expecting the e-mail attachment. Computer viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Computer viruses also spread by using downloads on the Internet. Computer viruses can be hidden in pirated software or in other files or programs that you may download.[25]

### 3.4. DIGITAL EVIDENCES ACT PORNOGRAPHY

The growth of technology has flip side to it causing multiple problems in everyday life. Internet has provided a medium for the facilitation of crimes like pornography. Digital Evidences Act porn as it is popularly called is widespread. Almost 50% of the web sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs... Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the Internet.[26]

### 3.5. DIGITAL EVIDENCES ACT STALKING

Although there is no universally accepted definition of Digital Evidences Act stalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.[27] Digital Evidences Act Stalking can be defined as the repeated acts harassment or threatening behavior of the Digital Evidences Act criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victim's property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. These problems occur on

[24] R. K. Chaubey, Ibid, p.143.
[25] <http://support.microsoft.com/kb/129972> Accessed on: 12.04.2025
[26] R. K. Chaubey, Ibid, p.144.
[27] <http://www.cyberguards.com/CyberStalking.html> Accessed on: 12.04.2025

the Internet as well, in what has become known as Digital Evidences Act stalking or on line harassment.[28]

**Definition of Digital Evidences Act Stalking:**

Stalking is a continuous process, consisting of a series of actions, each of which may be entirely legal in itself. Technology ethics professor Lambèr Royakkers writes that:

"Stalking is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect)."

Digital Evidences ActAngels has written about how to identify Digital Evidences Act stalking:

When identifying Digital Evidences Act stalking "in the field," and particularly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation: malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, harassment, and threats.[29]

**Types of Digital Evidences Act Stalking:**

**Of women**

Harassment and stalking of women online is common, and can include rape threats and other threats of violence, as well as the posting of women's personal information. It is blamed for limiting victims' activities online or driving them offline entirely, thereby impeding their participation in online life and undermining their autonomy, dignity, identity and opportunities.

**Of intimate partners**

Digital Evidences Act stalking of intimate partners is the online harassment of a current or former romantic partner. It is a form of domestic violence, and experts say its purpose is to control the victim in order to encourage social isolation and create dependency. Harassers may send repeated insulting or threatening e-mails to their victims, monitor or disrupt their victims' e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim doesn't want. They may also use the internet to research and compile personal information about the victim, to use in order to harass her.

---

[28] R. K. Chaubey, Ibid, p.144.

[29] <http://en.wikipedia.org/wiki/Cyberstalking> Accessed on: 12.04.2025

**By anonymous online mobs**

Web 2.0 technologies have enabled online groups of anonymous people to self-organize to target individuals with online defamation, threats of violence and technology-based attacks. These include publishing lies and doctored photographs, threats of rape and other violence, posting sensitive personal information about victims, e-mailing damaging statements about victims to their employers, and manipulating search engines to make damaging material about the victim more prominent. Victims are often women and minorities. They frequently respond by adopting pseudonyms or going offline entirely.[10] A notable example of online mob harassment was the experience of American software developer and blogger Kathy Sierra. In 2007, a group of anonymous individuals attacked Sierra, threatening her with rape and strangulation, publishing her home address and Social Security number, and posting doctored photographs of her. Frightened, Sierra cancelled her speaking engagements and shut down her blog, writing "I will never feel the same. I will never be the same."

Experts attribute the destructive nature of anonymous online mobs to group dynamics, saying that groups with homogeneous views tend to become more extreme as members reinforce each other's beliefs, they fail to see themselves as individuals, so they lose a sense of personal responsibility for their destructive acts, they dehumanize their victims, which makes them more willing to behave destructively, and they become more aggressive when they believe they are supported by authority figures. Internet service providers and website owners are sometimes blamed for not speaking out against this type of harassment.

**Corporate Digital Evidences Act stalking**

Corporate Digital Evidences Act stalking is when a company harasses an individual online, or an individual or group of individuals harasses an organization. Motives for corporate Digital Evidences Act stalking are ideological, or include a desire for financial gain or revenge.[30]

**3.6. DIGITAL EVIDENCES ACT TERRORISM**

Digital Evidences Act terrorism may be defined to be "the premeditated use of disruptive activities, or the threat thereof, in Digital Evidences Act space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." The role of computer with respect to terrorism is that of modern thief who can steal more with a computer than with a gun.. No doubt, the great fears

[30] <http://en.wikipedia.org/wiki/Cyberstalking> Accessed on: 12.04.2025

are combined in terrorism; the fear of random, violent, victimization segues well with the distrust and out-rights fear of computer technology.[31]

### 3.7. DIGITAL EVIDENCES ACT CRIME RELATED TO FINANCE

There are various types of Digital Evidences Act Crimes which are directly related to financial or monetary gains by illegal means, to achieve this end, the persons in the Digital Evidences Act world who could be suitably called as fraudsters uses different techniques and schemes to be fooled other peoples on the internet. Online fraud and cheating is one of the most lucrative businesses that are growing today in the Digital Evidences Act space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, online auction frauds, online investment schemes, offering jobs, etc.[32]

### 3.8. DIGITAL EVIDENCES ACT CRIME WITH MOBILE & WIRELESS TECHNOLOGY

At present the mobile is so developed that its becomes somewhat equivalent to personal computer, as we can do a lot of work on our mobile phones which were earlier possible on the computers only, such as surfing, sending e-mails etc. There is also increase in the services which were available on the mobile phones such as Mobile Banking which is also prone to Digital Evidences Act crimes on the mobile as it is on the Internet. Due to the development in the mobile and wireless technology day by day, the day is not far away when the commission of Digital Evidences Act crimes on the mobile will become a major threat along with other Digital Evidences Act crimes on the net.[33]

### 3.9. PHISHING

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message.[34] U.S. businesses lose an estimated $2 billion USD a year as their clients become victims, The United Kingdom also suffers from the immense increase in phishing. In March 2005, the amount of money lost in the UK was approximately £12 million Pound Sterling.[35]

---

[31] Ibid, p.145.
[32] Ibid, p.145.
[33] Ibid, p.145.
[34] Ibid, p.146.
[35] Ibid, p.148.

### 3.10. DENIAL OF SERVICE ATTACK (DOS ATTACK)

This is an act by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer's, exceeding the limit that the victim's servers can support and making the server's crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay.[36]

### 3.11. E-MAIL BOMBING

In Internet usage, all e-mail bombs is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server. Mail bombing is the act of sending an e-mail bomb, a term shared with the act of sending actual exploding devices (see mail bomb). Mail bombing is sometimes accomplished by giving the victim's e-mail address to multiple spammers. Such a file compresses into a relatively small archive, but being unpacked by early versions of mail servers might waste the free space on its disks and cause denial of service. Also known as a zip bomb.[37]

### 3.12. CONCLUSION

Computer crime is a multi-billion dollar problem. Technological changes will enable more perpetrators to ply their trade from remote locations. Managers must plan for this reality and devote resources to deal with the computer crime problem. New on the horizon is the potential for Digital Evidences Act terrorism. Although in its infancy, the internet is a vehicle for terrorist attacks by foreign and domestic antagonist wishing to inflict damage to a company with little chance of being caught. One problem is tracking a Digital Evidences Act terrorist. It is hard to determine if a Digital Evidences Act attack has been launched by a terrorist or by a hacker as a prank.

[36] Ibid, pp.149-150.
[37] Ibid, p.152.

## CHAPTER 4

## Digital Evidences Under the Evidence Act, 1972

### 4.1. INTRODUCTION

In today's world information communication system and network security has become a right issues for the reason that rights to information has become more and more important to everyone as information protects and develops human life everyday. Internet has grown in our country, the need has been felt to enact the appropriate Digital Evidences Act laws, which are indispensable to legalize and regulate internet in Bangladesh.

### 4.2. NEED FOR DIGITAL EVIDENCES ACT LAW IN BANGLADESH

Computer has become integral parts of the modern day homes and workplaces. Countries around the world continue to exhibit an encouraging trend of computer usage. Most academic institution has invested in the best technology to keep their students equipped and informed. As for the workplace, there is a gradual trend towards a possible future brimming with 'paperless and selfless offices'. The dependence on computer is increasing by the day as we are faced with better and faster machines geared up to fulfill operations that were not even imagined a few years back.[38] For the past several years, many countries have been concentrating on the awareness on questions of about the governance of Digital Evidences Actspace. The question of who controls the Internet is directly related to the question who wants to control the Internet. From the moment that the Internet was opened up to commercial activity many different groups wanted to dominate, such as user, communication companies, ISPs, and the government. Of them all, the most objected was the government intervention, yet it is governments that have managed to exert the most control. However as Internet has grown in our country, the need has been felt to enact the appropriate Digital Evidences Act laws, which are indispensable to legalize and regulate Internet in Bangladesh. The need for Digital Evidences Act laws was propelled by numerous factors. The arrival of Internet signaled the commencement of the rise of new and intricate legal issues. Despite the brilliant acumen of our master draftsman, the requirement of Digital Evidences Actspace could hardly ever be anticipated. As such, the coming of the internet led to the emergence of numerous ticklish legal issues and problem which necessitated the enactment of Digital Evidences Act laws. The existing laws of Bangladesh, even with the most generous and moderate interpretation, could not be interpreted in the light of the promising Digital Evidences Actspace, to consist of all aspect relating to different activities in Digital

[38] Zulfiquar Ahmed, Ibid, pp.49 – 52.

Evidences Actspace. There are no existing laws that assigned any legal validity or sanction to the activities in Digital Evidences Actspace, as such, before passing Digital Evidences Act Law, email was not "legal" in our country and courts and judiciary in our country had been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the parliament. The Government of Bangladesh responded by coming up with the first Digital Evidences Act law of Bangladesh Digital Evidences Under the Evidence Act, 1972.

## 4.3 HISTORICAL BACKGROUND OF THE INFORMATION AND COMMUNICATION TECHNOLOGY ACT (ICT) OR DIGITAL EVIDENCES ACT LAW

Bangladesh Government has recently enacted *Digital Evidences Under the Evidence Act, 1972* The law has been made in the shape of *the United Nations Commission on International Trade Law (UNCITRAL) of 1996*, which is called *UNCITRAL Model Law* on economic commerce. The *Model Law* does not have any force but merely serves as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of communication involving the use of computerized or other modern techniques, and for the establishment of relevant legislation where none exists. The law is sometimes called Digital Evidences Act law and sometimes the law of "Internet" or "Computer". Bangladesh is the 32nd nations in the world that has Digital Evidences Act legislation apart from countries like India, Singapore, France, Malaysia and Japan.[39]

## 4.4 CONCLUSION

Understanding the essential need of security all developed countries have taken steps to address the problem. On the other hand developing countries are far away from being able to guarantee these rights. Threats to the information technology were emerging on the content level as well as on the network level and on the physical level. Information security could however not be achieved by technology alone. In order to respond to network threats and create a secure information technology, both comprehensive prevention measures and enforcement measures are necessary.

[39] Ibid, p.52.

# CHAPTER 5
# GENERAL CONCLUSION

## 5.1. INTRODUCTION

The subject of Digital Evidences Act crime is high on the international concern today, not only because of its numerous significance, but also because of its impact on international peace, security and stability. In Bangladesh, Digital Evidences Act crime has to be voluntary and willful, an act or omission that adversely affects a person property. This chapter deals with a summary of findings of this research and recommendation. It firstly discusses the summary of findings of this research. Secondly, this chapter deals about the recommendation of mine which I found from this research.

## 5.2. SUMMARY OF FINDINGS

In my research to make it better I have divided it into five chapters on "Digital Evidences Act Crime in Bangladesh". The summary of findings from my research is given below:

**Chapter 1: Introduction**

Chapter1 is an introductory chapter this chapter deal about research proposal that assigned by my supervisor. In the chapter at first I sorted out statement of the problems, means what is the problem of this topic in our country in this regard I tried to find out the problems. Then importance of the study of this topic, Bangladesh is a developing country its technology is being developed day by day and internet is a new concept in our country. So its importance is potential for us.

Legal research is also important for lawyer, who as a real-life problem solver should be familiar with those areas of law in which he claims to have expertise. Research is critically important for initiating reform & change in a society. Research can initiate a new theory of variety issues, challenge old one or help in clarifying existing theory. The findings of research may be helpful to bring about deserve changes in existing institutions. Digital Evidences Act law is a new phenomenon of modern technological development. About Digital Evidences Act crime in Bangladesh there is no available books, journals or effective research or work is made on it. For this reason I have chosen to work on *"Digital Evidences Act Crime in Bangladesh"*. In my research I will focus on the concept of Digital Evidences Act crime and many other related things so that students, teachers, lawyers, policy makers and overall our country will be benefitted by the findings of my research. The main objectives of this research are:

4) To explore the nature of contemporary Digital Evidences Act crimes and its consequences in Information and Communication Technology (ICT).

5) To analyze the related Digital Evidences Act Laws of Bangladesh.
6) To examine the legal measure against the Digital Evidences Act Crimes in Bangladesh.

To prepare the research paper some secondary data have been collected and analyzed from the various sources. To prepare the research paper some secondary data have been collected and analyzed from the various sources. Such as, most of the information has been furnished through internet, books, journals, article's, various papers as well as others field. Although the research methodology consisted of both a quantitative and qualitative approach, in this research mainly qualitative method will be followed. In my research paper I showed some review of literature so that it be more clear to us whose books are using to prepare this research. The term Digital Evidences Act crime is not brief but it is vaster. This research will deal with the different aspects of Digital Evidences Act crime in Bangladesh. Particularly, it will analyze the concept and consequences of Digital Evidences Act crime. However this research will not concentrate on all the issues relating to Digital Evidences Act crime. At the last of chapter one I mentioned tentative structure outline of the study and I have divided my research into five chapters.

**Chapter 2: Theoretical Framework**

In present world we cannot think anything without computer with internet where computers are not just an ordinary thing but a "necessity" to our everyday life. The internet in Bangladesh is growing rapidly. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. With the advent of Information Technology, Internet and Information and Communication Technology, the world civilization is facing new dimension of criminal offence. This chapter firstly identifies the definition and then focuses on history and background of Digital Evidences Act crime, nature of Digital Evidences Act crime, Classification of Digital Evidences Act Crime. Finally the chapter analyses the Challenge of Digital Evidences Act Crimes, Characteristics, and victims of Digital Evidences Act Crime.

Victims of the Digital Evidences Act crime: Digital Evidences Act crime basically occurs against person, govt. and property. Digital Evidences Act crime is an evil activities occurred by computers in modern life. One statistics shows that nearly two thirds (65 percent) of web users across the world have been the victim of Digital Evidences Actcrime, says Symantec and over 1 Million Digital Evidences Act crime victims a day in 2010**.** Where information and communication technology gives us a lot of advantages and our work is being easier than before and we can communicate each other from one side to another side in the world. Now a days when everything from microwave ovens, refrigerators, nuclear power plants,

entertainment, business, sports, medical, education, weather update, and so many things are being operated by computers. But besides these advantages also is being misused.

## Chapter 3: Kinds of Digital Evidences Act Crime

In Bangladesh most of us only knew a little about computer security threats**,** the most common were "*virus*" and "*worm*". Let me examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Here is the list of the prevalent Digital Evidences Act Crimes, some of which are more widely spread and harmful. There are two sides of a coin. Internet also has its own disadvantages. One of the major disadvantages is Digital Evidences Act crime – illegal activity committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like hacking, virus, trojans and worms, Digital Evidences Act pornography, Digital Evidences Act stalking, Digital Evidences Act terrorism, Digital Evidences Act crime related to finance, Digital Evidences Act crime with mobile and wireless technology, phishing, denial of service attack (Dos Attack), e-mail bombing and so on, which invade our privacy and offend our senses.

Computer crime is a multi-billion dollar problem. Technological changes will enable more perpetrators to ply their trade from remote locations. Although in its infancy, the internet is a vehicle for terrorist attacks by foreign and domestic antagonist wishing to inflict damage to a company with little chance of being caught. One problem is tracking a Digital Evidences Act terrorist. It is hard to determine if a Digital Evidences Act attack has been launched by a terrorist or by a hacker as a prank.

## Chapter 4: Digital Evidences Act Law in Bangladesh

In today's world information communication system and network security has become a right issues for the reason that rights to information has become more and more important to everyone as information protects and develops human life everyday. Internet has grown in our country, the need has been felt to enact the appropriate Digital Evidences Act laws, which are indispensable to legalize and regulate internet in Bangladesh. This chapter firstly identifies the Need for Digital Evidences Act Law in Bangladesh and then focuses on Historical Background of the Information and Communication Technology Act (ICT) or Digital Evidences Act Law, Sides of Digital Evidences Act Law or ICT Act of Bangladesh, Objective of the ICT Act, 2006, Establishment & Jurisdiction of Digital Evidences Act Tribunal in Bangladesh, Establishment & Jurisdiction of Digital Evidences Act Appellate

Tribunal in Bangladesh. Finally the chapter analyses the Digital Evidences Act law and its weakness and Criticisms of the ICT Act, 2006.

Understanding the essential need of security all developed countries have taken steps to address the problem. On the other hand developing countries are far away from being able to guarantee these rights. Threats to the information technology were emerging on the content level as well as on the network level and on the physical level. Information security could however not be achieved by technology alone. In order to respond to network threats and create a secure information technology, both comprehensive prevention measures and enforcement measures are necessary.

Bangladesh is a developing country. Its technology is also being developed day by day. The problems I sorted out in this regard are as follows-

- Though such crimes are available in our country but the respective authority is not enriched with expert persons to deal with.
- We are updated with the latest information technology but have not yet updated or developed the security measure or system.
- The problem of Digital Evidences Act crime in Bangladesh is burning question. Now a days we observed that every sectors is corrupted with different Digital Evidences Act crime such as- Education, Bank, and Multinational company sectors.
- The punishment provided in the case of Digital Evidences Act law is not enough.
- There is no authority to monitor the misuses of Digital Evidences Act law.

**Chapter 5: General Conclusion**

Chapter five is a general conclusion chapter. In this chapter at first I have given introduction then recommended some significant steps for the problem of my research topic by reviewing the previous chapter in conclusion and at last conclusion.

## 5.3. RECOMMENDATION

The ICT Act, 2006 demands amendments of certain Acts for the first step for incorporation of the internet into Bangladesh's legal framework. There is still a long way to go before the Bangladeshi legal system incorporates and accepts the internet fully. *The Evidence Act, 1872, the Bankers' books Evidence Act, 1891 and the Bangladesh Bank order, 1972* shall be amended in the manner specified in the second schedule, third schedule and fourth schedule of this act.[40]

The subject of Digital Evidences Act crime is high on the international concern today, not only because of its numerous significance, but also because of its impact on international peace, security and stability. In Bangladesh, Digital Evidences Act crime has to be voluntary and willful, an act or omission that adversely affects a person property. *The ICT Act, 2006* provides the backbone for e-commerce and Bangladesh's approach has been to look at e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take into consideration the security aspects. In the present global situation where Digital Evidences Act control mechanisms are important we need to push Digital Evidences Act laws. Digital Evidences Act Crimes are a new class of crimes to Bangladesh rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a Digital Evidences Act crime. The pace of the investigation however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT Institutions can also play a role in this area. We need to sensitize our investigators and judges to the nuances of the system. Most Digital Evidences Act criminals have a counter part in the real world. A lengthy and intensive process of learning is required. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals. The real issue is how to prevent Digital Evidences Act crime. For this, there is need to raise the probability of apprehension and conviction. Bangladesh has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenge in Digital Evidences Act crime cases includes getting evidence that will stand scrutiny in a foreign court. For this Bangladesh needs total international cooperation with specialized agencies of different countries. Police has to ensure that they have seized exactly

[40] Ibid, p.61.

what was there at the scene of crime, is the same that has been analyzed and report presented in court is based on this evidence. It has to maintain the chain of custody. The treat is not form the intelligence of criminals but form our ignorance and the will to fight it.

The following recommendations can be taken under consideration for the betterment of the present conditions.

- The existing law is not sufficient to provide compensation to victims of the Digital Evidences Act crime for injuries caused or loss suffered by them due to the offender's Digital Evidences Act act.
- The government may constitute a separate authority to monitor the abuse of Digital Evidences Act.
- Digital Evidences Act crime related cases could be adjudicated under the Druto Bichar Tribunal.
- Regular training campaigning should be arranged for the skill development of experts.

This study confirms that Bangladeshi peoples using the internet are in risk it is found by this research that most of the people of Bangladesh are not more conscious to use the internet rightly. So, people have to more conscious about the using of internet in the proper way. The main reason behind this situation is lack of proper education about using internet and as such this system is also liable to misuse the internet technology. So, our Government has to take adequate movement to ensure the proper education to the mass people for using the internet and information technology in an appropriate way. On the other hand, now-a-days, most of young generation using Digital Evidences Act and a large number of them faced with Digital Evidences Act criminals. But in our country, there is no monitoring body or system to control the various use of Information Technology. It is a matter of great sorrow that, in our laws this issue is almost vague. So, we need an amendment on Information and Technology Communication Act-2006.

**Computer security Technique:**

Some important computer security techniques are given below:

**Human Integrity:** Always tries to keep morality inspiring good, honest business practices, etc.

**1. Built-in system safeguard:**

- **Record keeping system:** That automatically records who use the system.
- **A signal:** That will alter security personnel 'unauthorized user'.
- **Auditing programs:** That checks for potentially suspicious acts.
- **User identification and verification control:** That includes something other than a password that can be stolen. Biometrics (confirm by biological characteristics).

**2. Data Encryption:**

Sensitive data is translated into a secret code.

**3. Common sense:**

Change password time to time, keep password in character not in numeric number, give different people different job etc.

**4. Secure Network Confirmation:**

Extra care should be taken in case of networked system.

## 5.4. CONCLUSION

As we move forward into the 21st century, technological innovations have added the way for us to experience new and wonderful conveniences in the how we are educated, the way we shop, how were entertained and the manner in which we do business. It is not possible to eliminate Digital Evidences Act crime form the Digital Evidences Act space. But it is possible to check them or under control. If we look to the history then we can see that no legislation has succeeded in totally eliminating crime from the world. The only possible step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime. Undoubtedly the ICT Act is a historical step in the Digital Evidences Act world. Besides this it cannot be denied that there is a need to bring changes in the IT Act to make it more effective. The Penal Code, 1860 is not sufficient to protect the needs of new crimes emerging from internet or computer. Though there are some laws and convention, they cannot be implemented due to some technical difficulties like procedural complexities and lack of proper executing system. Taking these advantages, the criminals are occurring serious crimes like Hacking, Sending malicious mails, spreading vulgar pictures, Digital Evidences Act terrorism and illegal using of intellectual properties. It causes harm to the privacy of individuals as well as creates threat to the international peace and harmony. Now it is the demand of time to prevent such type of crimes for keeping individual privacy as well as international peace and security. Every country of the world should enact effective legal provisions within their national boundaries to protect Digital Evidences Act crimes.

# REFERENCES

## BOOKS

1. Abdullah Al Faruque, *Essentials of Legal Research*, (2nd ed., Dhaka: Palal prokashoni, 2010).

2. Farooq Ahmad, *Digital Evidences Act Law in India (Law on Internet),* (2nd ed., Delhi: New Era Law Publications, 2005).

3. R. K. Chaubey, *An Introduction to Digital Evidences Act Crime and Digital Evidences Act Laws,* (1sted., Kolkata: Kamal Law House, 2009).

4. Zulfiquar Ahmed, *A Text Book on Digital Evidences Act Law in Bangladesh*, (1st ed., Dhaka: National Law Book Company, 2009).

5. Md. Borhan Uddin, *Principles of Digital Evidences Act Law,* (1st ed., Shams Publications, Dhaka, 2010).

6. Yatindra Sign, *Digital Evidences Act Laws,* (2nd ed., Universal Law Publishing co. Pvt. Ltd. 2005).

## STATUTES

1. The Information and Communication Technology Act (ICT), 2006.

## JOURNAL

1. M. Abul Hasanat, 'Digital Evidences Act Crime: An Ill-going Techno - Culture', *Journal of Law*, Vol. i, no.1 (June 2003).

## NEWSPAPER

1. The Daily Star
2. The Daily Prothom Alo
3. The Daily Kalerkontho

## INTERNET

1. http://jabalpurpolice.org/Digital Evidences Act_crime.php
2. http://jabalpurpolice.org/Digital Evidences Act_crime.php
3. http://www.thedailystar.net/law/2009/06/03/watch.htm
5. http://en.wikipedia.org/wiki/Digital Evidences Act_crime
6. http://www.techterms.com/definition/Digital Evidences Actcrime

7.http://www.associatedcontent.com/article/44605/Digital Evidences Actcrime_a_revolution_in_terrorism.html?cat=37
8. www.ncjrs.gov/pdffiles1/nij/231832.pdf
9.http://www.pcworld.com/article/205309/65_of_web_users_are_victims_of_Digital Evidences Actcrime.html
10.http://spectrum.ieee.org/riskfactor/telecom/security/over-1-million-Digital Evidences Act-crime-victims-a-day-in-2010-
11. http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-022012&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5
12.http://nilakas-duronto.blogspot.com/2011/04/Digital Evidences Act-law-and-its-weakness-bangladesh.html
13. http://support.microsoft.com/kb/129972
14. http://en.wikipedia.org/wiki/Computer_virus
15. http://www.Digital Evidences Actguards.com/Digital Evidences ActStalking.html
16. http://en.wikipedia.org/wiki/Digital Evidences Actstalking
17. http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-022012&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5