Course Outline

Cyber Law

Introduction

- Cyber space
- Cyber law
- Importance of Cyber law
- Cyber Crime
- Reasons of Cyber crime
- Different types of cyber-crime

ICT Act 2006

- Section 2(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14), 3, 4, 5, 6, 7, 8, 9, 10, 11, 16, 17, 18, 19, 22, 23, 24, 25, 26, 38, 39, 58, 62, 64, 68, 69, 72, 73, 74, 79, 82, 83, 84, 90
- Objectives and Criticism

Digital Security Act 2018

- Section 2(1[b, c, d, e, g, i, j, k, l, n, t, u]), 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 39, 40, 52, 55, 61, 62

E-Governance

- E-Governance
- Types of Interactions in E-Governance
- Goals of E-Governance

E-contract

- E-contract
- Nature of E-contract

Virtual Court Act, 2020

Digital Evidence

- Digital Evidence
- Characteristics of Digital Evidence
- Challenges of Digital Evidence

UNCITRAL Model Law on Electronic Commerce

UNCITRAL Model Law on Electronic Signature

Resource Materials:

1. Justice Md. Azizul Haque: Cyber Law & Crimes
2. ICT Act 2006
3. Digital Security Act 2018
4. Virtual Court Act, 2020

Lecture 1

Introduction to Cyber Law

Why is Cyber Law needed?

There are various reasons which are extremely difficult for conventional law to cope with cyberspace that's why cyber law is needed. Some of these are discussed below:

- ❒ Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
- ❒ Cyberworld has complete disrespect for jurisdictional boundaries. A person in Bangladesh could break into a bank's electronic vault hosted on a computer in the USA and transfer millions of Takas to another bank in Switzerland, all within minutes. All he/she would need is a laptop/computer or a cell phone.
- ❒ Virtual world handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
- ❒ The online community is open to all participants. A ten-year-old boy in Bhutan can have a live chat session with an eight-year-old girl in Bali without any regard for the distance or the anonymity between them.
- ❒ Global village offers enormous potential for anonymity to its members. Readily available encryption software can seamlessly hide information within image and sound files to ensure the confidentiality of information exchanged between cyber-citizens.
- ❒ Electronic information has become the main object of cyber-crime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.
- ❒ A software source code worth crore of takas or a movie can be pirated across the globe within hours of their release.

What is Cyberspace?

The term ***cyberspace*** was first used by the American-Canadian author William Gibson in 1982 in a story published in Omni magazine and then 1984 in his book Neuromancer. In this science-fiction novel, Gibson described ***cyberspace as the creation of a computer network*** in a world filled with artificially intelligent beings.

Cyberspace supposedly a "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure.

According to ***Cambridge Dictionary***,

> ***Cyberspace*** means the notional environmental in which communication over computer networks occurs.

According to ***Chip Morningstar and F. Randall Farmer***,

> ***Cyberspace*** is defined more by the social interactions involved rather than its technical implementation. In their view, the computational medium in cyberspace is an augmentation of the communication channel between real people; the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other.

What is Cyber Law?

Cyber law means ***such law which prescribed the rules and regulations to protect the Internet and other online communication technologies***. It is the part of such legal system that deals with the Internet, cyberspace and their respective legal issues.

Cyber Law deals with the legal issues of the internet usage and all devices connected over the network, their proper use in order to prevent and control cyber-crimes.

According to ***Cambridge Dictionary***,

> ***Cyber Law*** is such a branch of law which prescribed the rules about how people should use computers, especially the internet.

According to ***Black's Law Dictionary***,

> ***Cyber law*** is such an evolving area of law that is applies to computers and the various activities over the internet and networks.''

Cyber Laws in Bangladesh

There are two Acts in Bangladesh for cyber-crimes. They are:

- Information and Communication Technology (ICT) Act 2006 on 8 October 2006
- Digital Security Act 2018 on 8 October 2018

Importance of Cyber Law

- Cyber law controls the misuse of technologies and cyber-crime.
- To protect nations and bring criminals within the jurisdiction of law, an effective cyber law can play a vital role.
- It helps to protect against computer fraud and unauthorized access over any computer network.
- Companies now can carry out electronic commerce using the legal infrastructure provided by the Cyber laws.
- Cyber law ensures the security of the mass people who uses the internet to their day-to-day life.
- It somehow guaranteed the safety of electronic transactions and communications over the internet.
- It gives proper redress to the victims of cyber-crime.
- It also protects individuals from getting trapped in any cyber violations.
- It controls the high rate of pornography, hacking, and cyber-terrorism.
- It also controls the defamatory, obnoxious publications in online social media.

Cyber-Crime

Cyber-Crime

Cyber-crime refers to any crime that involves a computer and a network. It includes those criminal acts which are performed with the aid of a computer. It is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.

Cyber-crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.

- **Debarati Halder and K. Jaishankar defines Cybercrimes as:**

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones "

- **According to Duggal:**

Any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cyber-crime.

Reasons of Cyber-Crime

There are several reasons for the wide spread of cyber-crime all over the world. Some of the notable reasons are –

- Expertise of offenders in technology
- Increasing dependence on computer and information technologies
- Minimum risk
- Complexity in taking legal action against offender
- Chance of huge monetary gain
- Carelessness and unskilled behavior of user of computer and internet
- Problems in identification of offenders
- Unwillingness of victims of cyber-crime to take legal measures
- Taking resort of new and sophisticated means for the commission of crime which exceeds the capability of law enforcement authorities
- Revenge
- Negligence

Different Modes of Cyber-Crimes

1. Hacking

Hacking is usually understood to be the unauthorized access of a computer system and networks. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously is said to commit hacking.

2. Email bombing

It refers to sending large numbers of mail to the victim and thereby ultimately resulting into crashing the computer network system. In Internet usage, an email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or crush down the mail server.

Shimla Case

In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application, it was rejected on the grounds that the schemes were available only for citizens of India. He decided to take his revenge. Consequently, he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed.

3. E-mail spoofing

It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc.

4. Data diddling

Data diddling (also called false data entry) is the unauthorized changing of data before or during their input to a computer system. It involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

5. Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files. It’s an event dependent program, as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities. Some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date, like the Chernobyl virus.

6. Salami Attacks

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. The Ziegler case, where a logic bomb was introduced in the bank system, which deducted 10 cents from every account and deposited it in a particular account.

The Ziegler Case

an employee of a bank in USA had his employment terminated. Angered by the supposed mistreatment by his employers, the man introduced a logic bomb into the bank's servers. The logic bomb was programmed to debit ten cents from all the accounts registered in the bank and transfer them into the account of the person whose name was alphabetically the last in the bank's records. Later, he had opened an account in the name of Ziegler. The amount transferred was so little that nobody had noticed the fault. However, it had been brought to light when a person by the name of Zygler opened his account in the same bank. He was surprised to find a large amount of money being transferred into his account every week. He reported the 'mistake' to the bank and the former employee was prosecuted.

7. Web Jacking

This term is derived from the term hi jacking. In these kinds of offences, the hacker gains access and control over the web site of another. He may even change the information on the site.

This occurs when someone forcefully takes control of a website by cracking the password and later changing it. The actual owner of the website does not have any more control over what appears on that website.

Piranha case

In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish.

Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

8. Cyber Pornography

Cyber pornography includes conducting pornographic websites; publish and print pornographic magazines by using computer and the Internet, to download and transmit pornographic pictures, photos; writing etc.

9. Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets, certificate etc. can be forged using sophisticated computers, printers and scanners. These are made using computers, and high-quality scanners and printers. This is becoming a booming business now days.

10. Denial of Service Attack

In case of Denial of Service attack the targeted computer received so many requests which it cannot handle. This crashes the computer resources. As a result, the computer resource denies giving proper service to the authorized user.

11. Cyber Defamation

This occurs when defamation takes place with the help of computers or the Internet. For example, someone publishes defamatory matter about someone on a website or sends E-mails to his friends containing defamatory information.

12. Trojan attacks

It is an unauthorized programme, which passively gains control over another's system by representing itself as an authorized programme. It is concealing what it is actually doing.

Lady Director Case

A Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber-criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

13. Fraud & Cheating

Online fraud and cheating are one of the most lucrative businesses that are growing today in the cyber 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, offering jobs, etc.

Azim's Cheating Case

Recently the Court of Metropolitan Magistrate Delhi found guilty a 24-year-old engineer Azim of fraudulently gaining the details of customers credit card. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating but did not send him to jail. Instead, Azim was asked to furnish a personal bond of Rs 20,000 and was released on a year's probation.

14. Cyber Bullying

According to Cambridge Dictionary, Cyber bullying means the activity of using the internet to harm or frighten another person, especially by sending them unpleasant messages.

Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

Hinduja defines cyberbullying as "willful and repeated harm through the use of computers, cell phones or other electronic devices.''

These elements include the following:

Willful: The behavior has to be deliberate, not accidental.

Repeated: Bullying reflects a pattern of behavior, not just one isolated incident.

Harm: The target must perceive that harm was inflicted.

Computers, cell phones, and other electronic devices: This, of course, is what differentiates cyberbullying from traditional bullying.

The most common places where cyberbullying occurs are:

- Social Media, such as- Facebook, Instagram, WhatsApp, Imo, Viber, Tiktok, Twitter etc.
- SMS (Short Message Service) also known as Text Message sent through devices
- Instant Message (via devices, email provider services, apps, and social media messaging features)
- Email

Cyberbullying in Bangladesh

Cyberbullying is not a new thing for Bangladesh and day by day it become a very serious issue. A recent study conducted by Telenor Group has found out that 49% school students of Bangladesh are the victims of cyberbullying (Telenor Group, 2016).

In case of cyberbullying, personal information, images are captured and videos of victims are recorded through digital devices and posted in the internet. This trend is increasing among students with the wide usage of digital devices.

According to IT specialist K.M. Nafiul Haque, Cyberbullying is pretty serious issue in Bangladesh. People are using different platforms and insulting each other randomly. He added that, it is happening because the zone of tolerance of the people is very low in our country.

The rate of Cyber bullying not only increases among the general people but also the celebrities are frequently being bullied online. We all know about the incident when the cricketer Mohammad Nasir put a picture with his sister and people started bullying them, even they used slangs. As a result, Nasir had to remove the picture. Then, the worldwide recognized, number one all-rounder in all three formats of cricket Sakib Al Hasan, he is being very often bullied when he put any picture with his family.

Legal Action Against Cyber bullying in Bangladesh

The victims of Cyber-bullying can directly contact with the BTRC and lodge complain. BTRC is supposed to take necessary actions within 24 hours and the perpetrators will be brought to justice within 3 days after the complaint is filed. The government has also launched a cyber-crime helpline. Victims can call at +8801766678888 to submit their complaints. Beside this, if the victim is a child or a woman, then there is a National Helpline number for their redress and the number is 10921.

Moreover, any victim of Cyber-bullying can also take resort the help of Police through dialing National Emergency Help Service Number 999.

Furthermore, Crime Research and Analysis Foundation (CRAF) a non-profit voluntary Organization also helped the victims of Cyber-bullying.

According to the Survey of CRAF, in our country every 20 second cyber-crime happened.

In order to prevent Cyber bullying Ain o Salish Kendro(ASK) and Insight Bangladesh Foundation also took lots of initiatives.

ReThink: Smart Solution to stop Cyber Bullying

Trisha Prabhu, a US innovator in 2015 launched the ReThink keyboard, which proved as highly effective way to detect and stop online hate speech and control the high rate of Cyber-bullying.

In the fall of 2013, Trisha, then just 13 years old, read the shocking news story of Rebecca Sedwick's suicide. After being cyberbullied for over a year and a half, Rebecca, a 12-year-old girl from Florida, took her own life.

Trisha herself was also the victim of cyber bullying for her wardrobe. For these reasons Trisha was shocked, heartbroken, and outraged. Deeply moved to action by the silent pandemic of cyberbullying and passionate to end online hate, Trisha created the patented technology product ReThink™, that detects and stops online hate at the source, before the bullying occurs, before the damage is done.

Her globally acclaimed research has found that with ReThink, adolescents change their mind 93% of the time and decide not to post an offensive message thus it can reduce the cyber-bullying a lot.

Rethink is an Anti-Cyberbullying keyboard app available for both Android and iOS. It compares the words and phrases that anyone type, with its database of offensive words and warns the netizen who typed hurtful words or phrases. This stops the writer from posting offensive messages on social media and social messaging apps, thus preventing Cyberbullying.

Technologies for preventing cyber crimes

As has been referred in 2010 Chu Journal Section, at page 349, Dr. R.C. Mishra, IPS, in his book "Cyber-crimes: Impact in new millennium" stated about certain technologies to prevent cyber-crimes.

a) **Firewall:** Firewall implemented with secure standards will not allow any intruder into the system.
b) **Encrypted tunneling:** An encrypted tunnel allows secure communications across internet. In this the data packets on internet are encrypted and then wrapped in IP at the initiation point of the tunnel. The encrypted packets can then be transmitted over the Internet when the packets came at the other end of the tunnel, they are unwrapped and decrypted.
c) **Secure Sockets Layer (SSL) and Secure HTTP:** This provides an encrypted TCP/IP Pathways between two hosts on the internet SSL can be used to encrypt any TCP protocol to encrypt HTTP.

d) **Secure Electric Transform (SET):** This technology involves cryptographic algorithms encrypt the credit card numbers, so it cannot be seen on the internet.
e) **Digital Signature:** Cryptographic techniques is used so that only authorized authenticated person can enter in the system.
f) **Employee Training**.

ICT Act 2006 Objectives and Criticism

Objectives of the ICT Act, 2006

- To make smooth the progress of electronic filing of documents with government agencies and statutory corporations and to promote efficient delivery of government services by means of reliable electronic records.
- To establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records.
- To facilitate electronic communications by means of reliable electronic records.
- To facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements.
- To promote the development of the legal and business infrastructure necessary to implement secure electronic commerce.
- To minimize the incidence of forged electronic records, intentional and unintentional alteration of records and fraud in electronic commerce and other electronic transactions.
- To establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records.
- To promote public confidence in the integrity and reliability of electronic records and electronic commerce and to foster the development of electronic commerce.

Criticism of the ICT Act, 2006

Practical Difficulty of Application

The legislation was originally intended to apply to crimes committed both in Bangladesh and worldwide but barely people practically take actions to execute their rights under the act. The legislation was initially supposed to be applied to crimes committed all over the world, but nobody knows how this can be achieved in practice.

Difficulties with Electronic Transaction

The enactment has an important effect on Bangladesh's e-commerce and m-commerce. But as for the electronic payment of any transaction it keeps itself almost impractical.

Intellectual property Security

The Act is not vocal on the various intellectual property rights, such as copyright, trademark, e-information and data patent rights.

Absence of Anti-spamming provision

Spamming has become a peril in the West as such they have made anti-spamming provisions in cyber law. However, there is no anti-spamming provision in our Act.

Silent on the liability issues of the Domain Name Holders

The Act does not discuss of the rights and liabilities of the domain name holders which is the first step of entering into the e-commerce.

E-Governance & E-Contract

E-Governance

Generally, E-Governance or Electronic Governance means computerization of current government procedures. E-governance is defined as the application of ICT in establishing interaction between the different levels of government, business, and the citizenry. E-governance is a one-stop Internet gateway to major government services. The concept of E-Governance emerged after the 1990's and Bangladesh government took the initiative to implement E-Governance in 2001.

In 2006 **UN** opines that, **E-Governance** means the employment of the internet and the world web for delivering government information and service to the citizens.

UNESCO defines as, **E- Governance** is the public sector's use of information and communication technologies with the aim of improving information and service delivery.

According to **Oakley**, E-Governance is a technology mediated service that facilitates a transformation in the relationship between government and citizen.

Chen says that it is the use of ICT to improve the quality of services and governance.

Saxena defined the term in very briefly but witfully as- 'An information age model of governance'.

Simply we can say that ***E-Governance means the versatile use of internet and technology in the overall activities of the government.***

Types of Interactions in E-Governance

1. G2C (Government-to-Citizen)

G2C are those activities in which the government provides non-stop, online access to information and services to citizens. This is the communication process of individual citizens with the government. It also involves prompt interaction of individual citizens with the government.

Examples include- payment of utility bills or downloading government forms from the Internet etc.

2. G2B (Government-to-Business)

It involves interaction of business entities with the government.

Examples include- corporate tax filing or government procurement process through the Internet.

3. G2G (Government-to-Government)

It involves interaction among government officials, whether within a government office or other country's government offices. **G2G** deals with those activities that take place between different government organizations or agencies. Many of these activities are aimed at improving the efficiency and effectiveness of overall government operations.

E**xamples** include-using E-mail for internal government communication or customized software for tracking progress of government projects. A popular G2G service is E-Nothi System in our country, through which the government offices can internally connect with each other.

4. G2E (Government-to-Employees)

It is the online interactions through instantaneous communication tools between government units and their employees. G2E is one out of the four primary delivery models of e-Government.

G2E is an effective way to provide E-learning to the employees, bring them together and to promote knowledge sharing among them. It also gives employees the possibility of accessing information in regard to compensation and benefit policies, training and learning opportunities and civil rights.

Examples include-Online training for govt. employees, online video conference with the govt. etc.

At present in our country, A2i took numerous initiatives to digitalize the G2E connections.

Examples include- The online platform for all the govt. school and high school teachers(https://www.teachers.gov.bd/), govt. online learning platform for officials and citizens called 'Mukopaath'(http://muktopaath.gov.bd/) etc.

Goals of E-Governance

- Improve the internal organizational processes of governments.
- Provide better information and service delivery.
- Increase government transparency and accountability in order to reduce corruption.
- Easy access to government public information.
- simplicity, efficient, cost-effective and responsive governance.
- Reinforce political credibility and accountability.
- Encourage democratic practices through public participation and consultation.

E-Contract

E-Contracts refer to contracts that are created and signed over the Internet. It is a contract modeled, executed and enacted by a software system. E-contract may be any kind of contract formed during e-commerce by the interaction of two or more individuals using electronic means, such as e-mail, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract. These contracts provide a fast and convenient way for individuals and organizations to enter into legally binding agreements with other parties.

The two main parties to an e-contract are-

Originator is a person who sends, generates, stores or transmits any electronic message to be sent, generated, stored or transmitted to any other person and does not include an Intermediary.

An **Addressee** is a person who is intended by the originator to receive the electronic record but does not include any Intermediary.

Nature of E-Contract

1. The parties do not, in most cases, meet physically.

2. There are no physical boundaries.

3. No handwritten signature and in most times, no handwriting is required.

4. Since there is no utmost security, risk factor is very high.

5. Jurisdictional issues are a major setback on e-contracts in case of breach.

6. There is no single authority to monitor the whole process

7. The three main methods of contracting electronically are e-mail, World Wide Web (www), and Cyber contracts (online contract).

The subject matter of E-Contract

(A) Physical goods, where goods are ordered online and paid over internet and physical delivery is made.

(B) Digitized products such as software which can also be ordered for.

(C) Services like electronic banking, sale of shares, financial advice etc.

Digital Evidence

Digital Evidence

National Institute of Justice of USA defined that-
Digital evidence is information and data of value to an investigation that is stored or, received, or transmitted by an electronic device.
Digital evidence means any probative information stored or transmitted in digital form that a party to a court case may use at trial.
However, it means any digital data that can establish that a crime has been committed.
Digital evidence is the data stored within electronic devices or systems that can be recovered by forensic experts and used as admissible evidence in court.
To define '**Digital Evidence'** simply, it may suffice to say in our domestic setting that digital evidence refers to any information stored or transmitted in electronic form on devices such as audio-visual cassettes or discs that may be produced in a case or suit being tried by a court of law.
Digital evidence includes the following computer related data-

- Normal File
- Deleted File
- Password protected files
- Hidden files
- Encrypted files
- User's cache memory
- Log files
- Boot recorded data
- All command files
- CD-ROM examination
- Zip & Rar files

What forms of media are considered Digital evidence?

Data recovered from the following devices and applications are considered as evidence. However, this is only admissible if recovered using a forensic methodology by a certified expert.

- Computers, laptops and tablets
- Mobile phone data
- HDD, RAID and SSD hard drives
- USB memory sticks and SD cards
- Social media information
- WhatsApp messages
- Cloud storage data

- Digital photographs
- CCTV

Five Intrinsic Characteristics of Digital Evidence

The five rules of gathering digital evidence that every forensic expert should keep in mind are that digital evidence should be –

- Admissible
- Authentic
- Complete
- Reliable
- Believable to be admissible in court.

Challenges of Digital Evidence

Acquiring digital evidence is not free of challenges. Only experts with the appropriate skillset and training are qualified to collect digital evidence. It is different from gathering physical evidence, and therefore, handling the digital acquisition of data is not free of risks.

Data stored in electronic media is volatile and is subject to changes or modifications. For example, a software update can change the data in the phone, or suspects can delete their data from the cloud or use the wipe-clean feature on their phones to remove any evidence. Consequently, this can prove tricky for investigators in carrying out the investigation. Besides, examining the massive volumes of data extracted from electronic media or devices is also a tedious task and requires the expertise of a skilled expert.

A forensic expert must be updated on the latest technological changes to be able to analyze and document the evidence. With the changes in big data and the latest technology updates, forensic experts need to be skilled in extracting data from multiple sources without modifying them and preserving the source of evidence for authenticity and integrity.

No action taken by law enforcement agencies, or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

Today, the biggest challenge the Courts have to deal with regard to digital evidence is its authenticity, veracity, genuineness and reliability for it to be admissible before the court of law.

Digital evidence must be authentic. Whether it's permissible in court or not will depend on how the evidence was obtained, its handling methods, and documentation of its chain of custody, from in situ to its presentation in the courtroom. At every stage, it must be ascertained that the evidence has not been altered in any way.

Challenges in Introducing Digital Evidence in our Court

There are some structural challenges facing the courts in introducing the Digital Evidence in our court system:

Firstly, our court rooms are not well-equipped to support digital evidence. So, the incorporation of digital evidence requires the arrangement of court rooms first.

Secondly, our judges and court staffs are not experienced or acquainted with such matters. It will be a challenge to train them.

Thirdly, common people may face hurdles with such change specially the people who are ignorant of technology.

Fourthly, Digital evidence can be easily modified, altered or transmitted. It may create a scope of altering important evidence unless precautionary measures are taken.

Fifthly, Quality IT experts may be required to deal with the modern technologies.

UNCITRAL Model Law on E-Commerce & E-Signature

UNCITRAL Model Law on E-Commerce

The United Nations Commission on International Trade Law (UNCITRAL) is the core legal body of the United Nations system in the field of international trade law. UNCITRAL's core business is the modernization and harmonization of rules on international business.

UNCITRAL Model Law on E-Commerce was passed by the Commission in **December 1996**. It was a breakthrough and initiative to provide a legal mechanism to govern the electronic transactions.

The UNCITRAL Model Law on Electronic Commerce aims to enable the commercial use of modern means of communications and storage of information. It establishes rules for the formation and validity of contracts concluded electronically and for the attribution and retention of data messages.

This Model law is divided into **two parts**. The first part relates to the General provisions related to E-commerce whereas the second part relates to the Specific provisions for e-commerce in certain areas.

The Model law provides that 'Electronic Communications' shall be given equivalent legal effect to paper-based communications. The member countries are required to prepare a relevant law within the framework of this Model law. Bangladesh also as a member of UNCITRAL accede this Model law. It is pertinent to mention here that, UNCITRAL document is a permissive document rather than a regulatory one.

This model laws

- establishes rules and norms that validate and recognize contracts formed through electronic means
- sets rules for forming contracts and governing electronic contract performance
- provides for the acceptability of electronic signatures for legal and commercial purposes

UNCITRAL Model Law on Electronic Signature

- The UNCITRAL Model Law on Electronic Signatures aims at bringing additional legal certainty to the use of electronic signatures.
- It establishes criteria of technical reliability for the equivalence between electronic and handwritten signatures.
- It follows a technology-neutral approach, which avoids favoring the use of any specific technical product.
- It establishes basic rules for assessing possible responsibilities and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process.