Quadrant II – Transcript and Related Materials

Programme: Bachelor of Science (First Year)
Subject: Computer Science
Course Code: CSG102
Course Title: Cyber space and cyber security
Unit: 05
Module Name: Cyber Laws: Evolution and Need for cyber law, the legal perspectives – Indian perspective, Global perspective, Information Technology Act(ITA) 2000, Provisions related to E commerce, Provisions for cyber-crimes

---

Notes:

Cyber Laws

- ✓ Cyber Law is the law governing cyber space.
- ✓ Cyber Law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web.
- ✓ Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of citizens and others, in Cyberspace comes within the ambit of Cyber Law.
- ✓ Cyber laws help to reduce or prevent people from cybercriminal activities on a large scale with the help of protecting information access from unauthorized people, freedom of speech related to the use of the Internet, privacy, communications, email, websites, intellectual property, hardware and software, such as data storage devices.

Evolution and Need for cyber law

- ✓ Cyber forensics in the simplest words means investigating, gathering, and analysing information from a computer device which can then be transformed into hardware proof to be presented in the court regarding the crime in question.
- ✓ Cyber forensics is an unavoidable force that is extremely significant in today's ever-changing, evolving, and technologically transforming world.

- ✓ A very important aspect of the investigation is making a digital copy of the storage cell of the computer and further analysing it so that the device itself doesn't get violated accidentally during the whole process.
- ✓ The need for cyber forensics is simple yet of utmost importance.
- ✓ It finds its application mainly in fighting vicious online crimes like hacking and DOS – denial of service attacks.

Evidence Collection:

- ✓ Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device.
- ✓ This evidence can be acquired when electronic devices are seized and secured for examination.
- ✓ Digital evidence can be like fingerprints or DNA evidence, it can be altered, damaged or destroyed with little effort, it can be time sensitive.
- ✓ Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices like digital cameras, hard drives, CD-ROM, USB memory sticks, cloud computers, servers and so on are used very effectively as evidence.
- ✓ For example, mobile devices use online-based based backup systems, also known as the "cloud", that provide forensic investigators with access to text messages and pictures taken from a particular phone.

Data Recovery:

- ✓ Forensic data recovery is the extraction of data from damaged, corrupted or lost evidence sources i.e. damaged or formatted hard drives, removable media.
- ✓ The data are recovered in a manner that will make the resulting evidence admissible in the law court.
- ✓ Data recovery is usually carried out in order to safely acquire evidence from computer systems by a away of forensic analysis (i.e. retrieve deleted, hidden, or mistakenly damaged data).
- ✓ There are several white-collar criminals, who delete data from their computer systems in other to hide their dubious activities.

- ✓ Cyber Forensic Data Recovery is the only way to gather sufficient evidences of fraud or any form of crime committed using a computer or internet

Cloning of Devices:

- ✓ Forensic Cloning, also known as a forensic image or bit-stream image is an exact bit-for-bit copy of a piece of digital evidence.
- ✓ It captures everything from the physical beginning to physical end. Through this method, files, folders, hard drives, etc. can be clones.
- ✓ In the eyes of the court, a properly authenticated forensic clone is as good as the original.
- ✓ Cloning a hard drive should be a pretty straightforward process, at least in theory. Typically, one will clone one hard drive to another.
- ✓ The suspect's drive is known as the source drive and the drive you are cloning to is called the destination drive.
- ✓ The destination drive must be at least as large as our source drive.