Chapter 4 Data Recovery and Cyber Security

Data Recovery is the process of retrieving lost data from storage devices. Data can be lost because of following reasons:

- Accidental Deletion of a file or partition
- Due to Disk malfunction or failure
- Due to accidentally formatting the storage device
- Due to problems with system and/or application software
- Due to physical damage to the storage device
- Due to Viruses and Spywares which clean hard drives and servers.

There are following types of failures in storage devices :

1. Logical Failure:

- Data is highly recoverable by using Data Recovery Softwares
- File can be recovered if it is not over-written

2. Physical Failure:

- Part of the data is retrievable
- If physical damage is extreme, the data is irrecoverable.

Step-wise Procedure to recover deleted files

1. Download, install and run the program on your computer. A welcome screen will appear. Click “Next” to proceed.
2. It will ask you which kind of files you are trying to retrieve? Check any one of the given options. If you want to retrieve two kinds of files, ex. pictures and music then you cannot select both the options simultaneously.
3. Select the location where you want to retrieve the files from.
4. In the next screen, click “Start” button. Don’t select deep scan option until you fail on your first attempt to recover the file. Note that “Deep scan” could take over an hour depending upon the size of your hard disk. The process will start.
5. It will show all the deleted files. To retrieve the file, check the box next to file name and click on “Recover” button.
6. Select the folder where you want to recover your file. You should select a drive or a folder different from the scanned drive (Say you scanned C drive to search all the deleted files so you should select D drive to recover those files). After selecting the appropriate location, click OK button.
7. Now check the folder. You will get your file back.

Types of hard drive partitions

- **Primary Partition** is a partition that is needed to store and boot an operating system, though applications and user data can reside there as well, and what's more, you can have a primary partition without any operating system on it. There can be up to a maximum of four primary partitions on a single hard disk, with only one of them set as active
- **Active (boot) partition** is a primary partition that has an operating system installed on it. It is used for booting your machine. If you have a single primary partition, it is regarded as active. If you have more than one primary partition, only one of them is marked active (in a given PC session).
- **Extended partition** can be sub-divided into logical drives and is viewed as a container for logical drives, where data proper is located. An extended partition is not formatted or assigned a drive letter. The extended partition is used only for creating a desired number of logical partitions.
- **Logical drive** is created within an extended partition.
- A logical partition is a way to extend the initial limitation of four partitions.
- An extended partition can contain up to 24 logical partitions (you're limited by the number of drive letters and the amount of hard drive space available for creating drives; of course, it's senseless to use 24 partitions on a system in most cases, because it will be a data organization nightmare).
- Logical partitions are used for storing data mainly, they can be formatted and assigned drive letters; their details are listed in the extended partition's table - EMBR (Extended Master Boot Record).

NTFS (New Technology File System) Recovery

- It is the best file system which supports large volumes, Encrypts all data, and makes file compression and auditing easier. NTFS makes it easier for modern data recovery software to recover lost files
- Steps to recover files from an NTFS Drive
- Install Data Recovery Software
- Run Data Recovery Software
- Select partition from where you need to recover lost data. Depending on the size of the partition, scanning may take 15-20 minutes
- Once the scan is complete, the software will show you recoverable files.
- Select the files you wish to recover and let the software retrieve the file. Some files may be partially recoverable and some may be irrecoverable
- After file is recovered, create backup of the important file for future reference

Cyber Crimes

- Cyber crime is an activity done using computers and internet. We can say that it is an unlawful acts wherein the computer either a tool or target or both.

Categories of cyber crime

We can categorize cyber crime in two ways.

- The computer as a target: - using a computer to attacks other computer, e.g. Hacking, virus/worms attacks, Dos attack etc.
- The computer as a weapon: - using a computer to commit real world crime e.g. cyber terrorism, credit card fraud and pornography etc.

Types of cyber crime

1) **HACKING**: - Hacking in simple terms means an illegal intrusion into a computer system and/or network. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage.

Motive behind the crime called HACKERS

Motive behind the crime called hacking greed power, publicity, revenge, adventure desire to access forbidden information destructive mindset wants to sell n/w security services.

Types of Hackers

- **White Hat**
  - This type of hackers is someone who has non-malicious purpose whenever he breaks into security systems.
  - Most of these are security experts who push the boundaries of their own IT security ciphers
  - These security experts are even penetration testers specifically hired to test out how vulnerable or how impenetrable is the present protective setup.
  - A white hat that does vulnerability assessments and penetration tests is also known as an ethical hacker.
- **Black Hat**
  - This type of hackers is also known as a cracker and has a malicious purpose when he goes about breaking into computer security systems with the use of technology such as network, telecommunication systems or computer and without authorization.
  - The crackers malicious purpose can range from all sorts of cybercrimes such as piracy, identity theft, credit card fraud, damage, deploying worms, malicious sites and so forth
- **Grey Hat**
  - A grey hat hacker is a combination of both white hats and black hats.
  - This is the kind of hacker that is not a penetration tester but will go ahead and surf the Internet for vulnerable systems he could exploit.
  - Like a white hat, he will inform the administrator of the website of the vulnerabilities he found after hacking through the site

- Like a black hat , he will hack any site freely and without any prompting or authorization from owners whatsoever, he will even offer to repair the vulnerable site he exposed in the first place for a small fee.

- **Elite Hacker**
  - These are talented people and having social status among the hacker underground
  - These are hackers among hackers in the culture
  - They are the masters of deception that have a solid reputation among their peers

- **Script Kiddie**
  - A script kiddie is basically an part-time or non-expert hacker, who breaks into computer systems not through his knowledge in IT security and the ins and outs of a given website, but through the prepackages automated scripts, tools and software written by real hackers.
  - He usually has little knowledge of the underlying concept behind how those scripts he has on hand works.

2) **Virus and VIRUS ATTACKS** : Malicious software that attaches itself to other software. VIRUS , WORMS, TROJAN HORSE ,WEB JACKING, E-MAIL BOMBING etc.

a) **DENIAL OF SERVICE ATTACKS** : This is an act by the criminals who floods the bandwidth of the victims network or fills his E-mail box with spam mail depriving him of the service he is entitled to access or provide. Many DOS attacks, such as the ping of death and Tear drop attacks.

b) **SPAM**: Junk E-mails, Unsolicited Advertisements for Products and services, Wastes both the storage and network capacities of ISPs.

c) PHISHING

Web fraud that tricks users into submitting personal information such as credit card data, social security numbers, passwords etc.) and then using that information fraudulently in identity theft

Phishing exploits are usually attempted in two ways

i) Email: An Email is sent from what looks to be a legitimate organization, asking for personal information in order to fix an issue.

ii) Web Sites: Legitimate Web Sites are copied to lure users into a false sense of security when entering in personal information

d) BOTNETS

Group of Computers connected to the Internet that have been taken over by a hacker. The hacker controls all the computers and they behave like a “Robot Network”

Botnets contain anywhere from 100 to 1000 computers. The hacker, who controls the botnet then uses these computers to send spam email, spread viruses and attack other networks or any other variety of malicious activity.

3) **CHILD PORNOGRAPHY**: The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of Pedophiles.

   How Do They Operate :

   How do they operate Pedophiles use false identity to trap the children , Pedophiles connect children in various chat rooms which are used by children to interact with other children.

4) **CYBER TERRORISM** : Terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate E-mails , attacks on service network etc.

5) **SOFTWARE PIRACY** : Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

6) Intellectual Property

Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.

Intellectual property rights reward Creativity and human endeavour, which fuel the progress of humankind. E.g. Billion Dollar Software Industry

Categories of Intellectual Property

- Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, dance, artistic works such as drawings, paintings, photographs , sculptures, and architectural designs.
- Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs.
- Industrial property, which includes :
    - Inventions (Patents),
    - Trademarks,
    - Industrial designs, and
    - Geographic indications of source

What is Copyright?

- Copyright is a legal term describing rights given to creators for their literary and artistic works. (©)
- Copyright in a literary work, lasts for the-
    - Author’s lifetime plus 50 years from the end of
    - The calendar year in which the author dies
    - 50 years for films and sound recordings
    - 25 years for typographical arrangements of a published edition

- The World Intellectual Property Organization (WIPO) is a specialized agency of the United Nations.
- It is dedicated to developing a balanced and accessible international intellectual property (IP) system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest

Industrial Property: Patent

- A patent is an exclusive right granted for an invention –
  - a product or process that provides a new way of doing something,
  - or that offers a new technical solution to a problem.
- A patent provides patent owners
  - with protection for their inventions. Protection is granted for a limited period, generally 20 years.
- Why are patents necessary?
- Patents provide incentives to individuals by recognizing their creativity and offering the possibility of material reward for their marketable inventions. These incentives encourage innovation, which in turn enhances the quality of human life.
- What kind of protection do patents offer?
- Patent protection means an invention cannot be commercially made, used, distributed or sold without the patent owner's consent.
- Patent rights are usually enforced in courts that, in most systems, hold the authority to stop patent infringement.
- Conversely, a court can also declare a patent invalid upon a successful challenge by a third party.
- What rights do patent owners have?
- A patent owner has the right to decide who may – or may not – use the patented invention for the period during which it is protected. Patent owners may give permission to, or license, other parties to use their inventions on mutually agreed terms.
- Owners may also sell their invention rights

  to someone else, who then becomes the new owner of the patent. Once a patent expires, protection ends and the invention enters the public domain. This is also known as becoming off patent, meaning the owner no longer holds exclusive rights to the invention, and it becomes available for commercial exploitation by others.

Industrial Property: Trademark

- A trademark is a distinctive sign that identifies certain goods or services produced or provided by an individual or a company.
- Its origin dates back to ancient times when craftsmen reproduced their signatures, or "marks", on their artistic works or products of a functional or practical nature.

- Over the years, these marks have evolved into today's system of trademark registration and protection.
- The system helps consumers to identify and purchase a product or service based on whether its specific characteristics and quality – as indicated by its unique trademark – meet their needs.
- What do trademarks do?
- Trademark protection ensures that the owners of marks have the exclusive right to use them to identify goods or services, or to authorize others to use them in return for payment.
- The period of protection varies, but a trademark can be renewed indefinitely upon payment of the corresponding fees.
- Trademark protection is legally enforced by courts that, in most systems, have the authority to stop trademark infringement.
- In a larger sense, trademarks promote initiative and enterprise worldwide by rewarding their owners with recognition and financial profit.

Industrial Property: Industrial Design

- An industrial design refers to the ornamental or aesthetic aspects of an article. A design may consist of three-dimensional features, such as the shape or surface of an article, or two-dimensional features, such as patterns, lines or color.
- Industrial designs are applied to a wide variety of industrial products and handicrafts: from technical and medical instruments to watches, jewellery and other luxury items; from house wares and electrical appliances to vehicles and architectural structures; from textile designs to leisure goods.
- To be protected under most national laws, an industrial design must be new or original and non-functional. This means that an industrial design is primarily of an aesthetic nature, and any technical features of the article to which it is applied are not protected by the design registration. However, those features could be protected by a patent.
- Why protect industrial designs?
- Industrial designs are what make an article attractive and appealing; hence, they add to the commercial value of a product and increase its marketability.
- When an industrial design is protected, the owner – the person or entity that has registered the design – is assured an exclusive right and protection against unauthorized copying or imitation of the design by third parties.
- This helps to ensure a fair return on investment. An effective system of protection also benefits consumers and the public at large, by promoting fair competition and honest trade practices, encouraging creativity and promoting more aesthetically pleasing products.
- Protecting industrial designs helps to promote economic development by encouraging creativity in the industrial and manufacturing sectors, as well as in traditional arts and crafts. Designs contribute to the expansion of commercial activity and the export of national products.

- Industrial designs can be relatively simple and inexpensive to develop and protect. They are reasonably accessible to small and medium-sized enterprises as well as to individual artists and crafts makers, in both developed and developing countries.
- The term of protection granted is generally five years, with the possibility of further renewal, in most cases for a period of up to 15 years.

  Industrial Property: Geographical Indication

- A geographical indication is a sign used on goods that have a specific geographical origin and possess qualities or a reputation due to that place of origin.
- Most commonly, a geographical indication consists of the name of the place of origin of the goods. Agricultural products typically have qualities that derive from their place of production and are influenced by specific local geographical factors, such as climate and soil. Whether a sign functions as a geographical indication is a matter of national law and consumer perception.
- Geographical indications may be used for a wide variety of agricultural products, such as, for example, “Tuscany” for olive oil produced in a specific area of Italy, or “Roquefort” for cheese produced in that region of France.
- The use of geographical indications is not limited to agricultural products. They may also highlight specific qualities of a product that are due to human factors found in the product’s place of origin, such as specific manufacturing skills and traditions.
- The place of origin may be a village or town, a region or a country. An example of the latter is “Switzerland” or “Swiss”, perceived as a geographical indication in many countries for products made in Switzerland and, in particular, for watches.

7) Mail Bombs
   It refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
   The solution to the repeated mail bomb attack is to block the traffic from originating network using packet filters.
8) Bug exploits
   Application Software exploit are those that take advantage of weaknesses of particular application programs, such weaknesses are called as Bugs.
   Criminals can use these bugs to maintain unauthorized access to computers or networks or to crash the system to deny services to others.
   Common Bugs can be categorized as:
   a) Buffer Overflows: It occurs when number of bytes or characters input exceeds the maximum number allowed by the programmer.
   b) Unexpected input: It occurs when programmer is not defining what happens if invalid input is entered. This may cause the program to crash or open a way into the system.
   c) Configuration Bugs: These are the ways of configuring the software that leaves it vulnerable to the penetration.

   Major Software Vendors regularly releasing security patches to fix exploitable bugs

Process of Cyber Investigation

Standard cybercrime investigation features a number of proven investigative techniques each designed to track and capture cyber criminals

- Interviews
  - For identifying cybercrime, investigator arrange a personal interviews with the parties to collect information about the case.
  - Recorded interview of witness plays important role in the investigation and also helps to build the legal case against suspects.
- Surveillance-
  - It is another important way of information gathering.
  - In computer surveillance, investigator checks the digital activities, monitors all elements of a suspects that the computer uses and its online behavior
- Forensics
  - After collection of enough information through interviews and surveillance, the investigators will get warrants and this used to collect targeted computer for advanced forensic analysis.
  - Computer Forensics means mining a computer for all related information and to detect the potential evidence.
  - This type of information may be located on local hard drives or in caches, RAM memories and registries etc.
  - Forensics technician uses electronic trail to search the digital fingerprints in emails, files and Web-browsing histories.
- Undercover:
  - Cybercrime may include steps to go undercover to trap criminals using fake Online Identities.
  - Such type of technique is very essential in case of pornography.

Cyber Laws:

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly“cyberspace”, i.e. the Internet.

Need of Cyber Crime Law:

- **<u>Cyber space is an intangible and provides an extreme mobility</u>**

Events taking place on the internet are not happening in the locations where participants or servers are physically located, but "in cyberspace".

- **<u>Cyber space offers great economic efficiency.</u>**

Billions of dollars’ worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

- **<u>Cyber space has complete disrespect for national boundaries.</u>**

A person in India could break into a bank’s electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

- **Cyber space is absolutely open to participation by all.**

  A ten year-old to an eighty year-old grandmother without any regard for the distance or the anonymity between them.

- On the Internet, it is very easier to create several copies and transmitting the same in different locations of world in few minutes. For these reasons, the Internet has been described as "th e world's biggest copy machine". "It's the World's Biggest Copy Machine," PC week (January 27, 1997).

Objectives of IT Act 2000

- To grant legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication;
- To give legal recognition to digital signature / electronic signature for authentication accepting of any information or matter which require authentication under any law;
- To facilitate electronic filing of documents with Government departments;
- To facilitate electronic storage of data ;
- To facilitate and give legal sanction to electronic fund transfer between banks and financial institution ;
- To give legal recognition for keeping books of account by bankers in electronic form.

To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

IT Amendment Act 2008

Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cybercrimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)