Marks :

Page No. 108
Date

5) IT act AND Cyber Law

5.1 Introduction to deleted file recovery :-

When we delete a file on disk having FAT 32 or NTFS file system, its content is not erased from disk but only reference to file data in the File Allocation Table or Master File Table is marked as deleted. It means that we might able to recover deleted files, or make it visible to file system again.

There are various data / file recovery tools find and recover recoverable deleted files from NTFS and FAT-formatted volumes, regardless of their type. It is possible to recover pictures, songs, movies or documents.

These tools usally operate as per the following process ~~states~~ steps :

Step 1 :- Scan the hard drive and build an index of existing and deleted files and directories on any logical drive of your computer with supported file format.

Step 2 :- Provide control over the user to select which files to recover and what destination to recover them to. You can browse the hierarchy of existing and deleted files, or you can use search functionality to find deleted file if you remember at least one of the following :

* full / partial file name
* file size
* file creation date
* file last accessed date

Step 3 :- Allows previewing deleted files of certain type without performing recovery. This feature becomes really important if you are forced to recover deleted files to the same drive

Data Recovery Tools :-

Formatting refers to the dividing the disks in accordance with certain principles, allowing computer to store and search file. Low-level formatting is to divide track and section for blank disk, mark address information, set crossed factors and fix logical bad track and other low level operations. High-level formatting refers to remove disk data, create boot informations, initialize FAT and mark logical bad track.

Symptoms of FORMAT :-

Where previously the computer would boot and be usable, systems that have been formatted often report following errors :

* Operating system not found
* Invalid or corrupt FAT
* Cannot find file or program
* Invalid command.com
* Primary / secondary Hard disk failure
* Non-system disk
* Disk error
* Or when a partition has been formatted, the all data would disappear.

Step-1 :- If you cannot boot the computer, please use data recovery bootable disk or connect hard drive to another computer as a slave to recover lost data.

Step 2 :- Select the file types you want to recover and volume where the formatted drive is. The tool will automatically scan the selected volume.

Step 3 :- Then the founded data will be displayed on the screen and you can get a preview of it. Then select the file or directory that you want to recover and save them into healthy drive.

Data recovery procedures and ethics:-
There are standard ethical procedures that need to be followed as described in following steps :-
① Incident identification - identifying the incident and analysis of the case.
② Preparation of tools, monitoring techniques, management support and authorization etc.
③ Decide a clear and well defined approach, strategy to proceed with the case
④ Collection of the evidence and even duplicating the digital evidence is also an important part of ethical conduct.
⑤ The evidence that is collected should be incorporated with the data, time and the place where it was found.
⑥ The analysis of evidence should be carried out in such a way so as to eliminate the evidence that cannot be produced in the court of law.
⑦ This step in an ethical behaviour indudes the presentation of evidence in the court of law.
⑧ The return of evidence to the owner also forms part in ethical behaviour.

5.2 Introduction to Cyber Crimes:-

Cybercrime is an illegal behaviour, directed by means of electronic operations, that targets security of computer systems and the data possesed by them. Cyber crime was broken into two categories defined as:
① In a narrow sense (Computer crime): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and data possesed by them.

(2) In a broader sense (Computer related crime) :- Any illegal behaviour committed by means of, or in relation to a computer system or network, including such crimes as illegal possesion or offering or distributing information by means of a computer system or a network.

Hacking :- Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use computer programs to attack the target computer. They passes the desire to destruct and they got enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their bank accounts followed by withdrawl of money. Government websites are hot on hacker's target list and attacks on government websites receive wide press coverage.

Cracking :- A cracker is someone who breaks into someone else computer system, often on network; bypasses passwords or licences in computer program; or in other ways intentionally breaches computer security.

Viruses, Virus attacks :- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infection as it travels. It is a kind of threat to the security and integrity of computer systems. It can cause loss or alteration of programs or data, and can compromise their confidientiality.

Pornography :- Child pornography is a very serious cyber crime offence. It includes the following :
① Any photograph that can be considered obscence and/or unsuitable for the age of child viewers
② Film, video, picture
③ Computer generated image or sexually explicit conduct where the production of such visual depiction involves the use of minor engaging in sexually explicit conduct

Software Piracy :- Software piracy can be defined as "copying and using commercial software purchased by someone else". It is illegal. Each pirated piece of software takes away from company profits, reducing funds for further software development initiatives.

Ways to deal with software piracy :
① Have a central location for software programs
② Secure master copies of software and associate documentation, while providing faculty access to those programs when needed.
③ Never lend or give commercial software to unlicensed users
④ Permit only authorised persons to install software
⑤ Train and make staff aware of software use and security procedures which reduce likelihood of software piracy.

- Intellectual property :- Intellectual property (IP) rights are legally recognized exclusive rights to creations of mind. Under Intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols and design.

- Legal System of Information Technology :- With the development of ~~and~~ security for computers, came a need of legal system to prosecute perpetrators. Also with the recent boom in E-commerce, it has become pertinent to have legal system and laws in place to protect and uphold contracts, business transactions, data processing and development over internet. Legal system plays a vital part in the upholding a secure information technology infrastructure.

- Mail Bombs :- A mail bomb is the sending of a massive amount of email to a specific person or a system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. Senders of mail bombs should be wary of exposing themselves to reciprocal mail bombs or to legal actions.

- Bug exploits :- (Refer page no:- 7 of this book; point 5] Exploits)

Cyber Crime investigation :-

Computer Forensics is an important element in Cyber Crime investigation which deals in examination of digital media in forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the digital information.

5.3 Introduction to cyber laws :

Cyber law is a term that encapsulates the legal issues related to the use of the Internet. It is a law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices, the Internet websites, emails and even electronic devices such as cell phones, ATM machines, etc.

Introduction to IT act 2000 and IT act 2008 :-

Objectives of Information Technology act 2000 are :-

1. To grant legal recognition to transactions carried out by means of EDI and E-commerce in place of paper based methods of communication.
2. To give legal recognition to digital signatures for authentication of any information
3. To facilitate electronic filing of documents with Govt dept.
4. To facilitate electronic storage of data
5. To facilitate and give legal recognition to electronic fund transfer between bank and financial institutions.
6. To give legal recognition for keeping books of accounts in electronic form by bankers.

Computer crimes and penalty in IT act 2000 :

Section	Offence / section title	Punishment	Cognizable / Non-Cognizable	Bail-able / Non-bailable
65	Tampering with computer source docs.	Imprisonment upto 3 yrs or fine extending ₹ 2 lakh or both	Cognizable	Non-bailable
66	Hacking with computer system	Imprisonment upto 3 yrs or fine extending ₹ 2 lakh or both	Cognizable	Non-bailable
67	Publishing or transmitting of information which is obscene in electronic form	On 1st conviction: Imprisonment upto 5 yrs and ~~fine~~ fine upto ₹ 1 lakh On 2nd conviction: Imprisonment upto 10 yrs and fine upto ₹ 2 lakh	Cognizable	non-bailable
71	Misrepresenting or supressing any material	Imprisonment upto 2 yrs or fine upto ₹ 1 lakh or both	Non-cognizable	bailable
72	Breach of confidentiality & privacy of electronic records, books, info.	Imprisonment upto 2 yrs or fine which may extend to ₹ 1 lakh or both	Non-cognizable	bailable
73	Publishing false digital signature certificate	Imprisonment upto 2 yrs or fine upto ₹ 1 lakh, or both	Non-cognizable	bailable
74	Publishing of digital signature certificate for fraudulent purpose	Imprisonment upto 2 yrs or fine upto ₹ 1 lakh, or both	Non-cognizable	bailable

IT act 2008 :-

The IT act 2000 has been substantially amended through IT (Amendment) Act 2008. It addresses the issue of cyber security.

Penalty Action under Section 43 :-

Section 43 deals with penalty for damage to computer or computer system by any of these methods :

(1) Securing access to computer, computer system or computer network.
(2) Downloading or extracting any data, computer database or information from such computer system or those stored in any removable storage medium.
(3) Introducing any computer contaminant or computer virus into any computer, computer system or network.
(4) Damaging any computer, computer system or network or any computer data, database or programme.
(5) Disrupting any computer, computer system or network
(6) Denying access to any person authorised to access any computer, computer system or network.
(7) Providing assistance to any person to access any computer, computer system or network in contravention of any provisions of this Act or its Rules.
(8) Charging the services ahead of by one person to the account of another person by tampering with or manipulating any computer, computer system or network.

Terms related with reference to section 2 of IT Act, 2000 :-

① Key pair :- In an assymmetric crypto system, comprising of private key and its related public key. These keys are so related that the public key can be used to verify a digital signature created by the private key.

② Originator :- It refers to a person who sends, generates, stores or transmits any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary

③ Digital signature :- It refers to authentication of any electronic record by a subscriber by means of electronic method or procedure in accordance with the provision of section 3.

④ Secure system :- It means computer hardware, software and procedures which are reasonably secure from the unauthorised access and misuse, provide a reasonable level of reliability and correct operation and adhere to generally accepted security procedures.