What is Computer Forensics?

Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.

In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil disputes, and human resources.

Use of Computer Forensics in law Enforcement:-

If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be tainted.

Choosing a Computer Forensics Specialist for a Criminal Case:-

When you require the services of a computer forensics specialist, there are an increasing number of people who claim to be experts in the field. There is far more to proper computer forensic analysis than the ability to retrieve data, especially when a criminal case is involved. The bottom line is that you will be retaining the services of an individual who will likely be called to testify in court to explain what he or she did to the computer and its data. The court will want to know that individual's

own level of training and experience, not the experience of his or her employer. Make sure you find someone who not only has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination.

Computer Forensics Assistance to Human Resources/Employment proceedings: - Computer forensics analysis is becoming increasingly useful to businesses. Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, and wrongful termination claims. Evidence can be found in electronic mail systems, on network servers, and on individual employee's computers. However, due to the ease with which computer data can be manipulated, if the search and analysis is not performed by a trained computer forensics specialist, it could likely be thrown out of court.

Employer Safeguard Program:-

As computers become more widespread in businesses, employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual. Whether you are looking for evidence in a criminal prosecution or civil suit or determining exactly what an employee has been up to, you should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy the evidence. For example, did you know?

- What Web sites have been visited?
- What files have been downloaded?

- When files were last accessed?
- Number of attempts to conceal or destroy evidence?
- Number of attempts to fabricate evidence?

Computer Forensics Services:-

A computer forensics professional does more than turn on a computer, make a directory listing, and search through files. Your forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case.
For example, they should be able to perform the following services:

✓ Data seizure
✓ Data duplication and preservation
✓ Data recovery
✓ Document searches
✓ Media conversion
✓ Expert witness services
✓ Computer evidence service options
✓ Other miscellaneous services

Data Seizure:-

Federal rules of civil procedure let a party or their representative inspect and copy designated documents or data compilations that may contain evidence. Your computer forensics experts, following federal guidelines, should act as representative, using their knowledge of data storage technologies to track down evidence.

Data Duplication and Preservation:-

When one party must seize data from another, two concerns must be addressed: the data must not be altered in any way, and the seizure must not put an undue burden on the responding party. Your computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data.

Data Recovery:-

Your computer forensics experts should be able to safely recover and analyze inaccessible evidence. The ability to recover lost evidence is made possible by the expert's advanced understanding of storage technologies.

Ex: - when a user deletes an email, traces of that message may still exist on the storage device

Document Searches:-

Your computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours. The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

Media Conversion:-

Clients need to obtain and investigate computer data stored on old and unreadable devices. Your computer forensics experts should extract the relevant data from these devices, convert it into readable formats, and place it onto new storage media for analysis.

Expert Witness Services:-

Computer forensics experts should be able to explain complex technical processes in an easy-to-understand fashion. This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

Computer Evidence Service Options:-

- ✓ Standard service
- ✓ On-site service
- ✓ Emergency service
- ✓ Priority service
- ✓ Weekend service

Benefits of Professional Forensics Methodology: -

Protection of evidence is critical. A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer
2. No possible computer virus is introduced to a subject computer during the analysis process
3. Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage
4. A continuing chain of custody is established and maintained
5. Business operations are affected for a limited amount of time, if at all
6. Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

Steps Taken by Computer Forensics Specialists:-

1. Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption or virus introduction.

2. Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files etc.
3. Recover all of discovered deleted files.
4. Access the contents of protected or encrypted files.
5. Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.
6. Provide expert consultation and/or testimony.

Who can use Computer Forensic Evidence?

1. Criminal prosecutors use computer evidence in a variety of crimes where incriminating documents can be found, including homicides, financial fraud, drug and embezzlement record-keeping and child pornography.
2. Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.
3. Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
4. Corporations often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, and theft or misappropriation of trade secrets, and other internal and confidential information.
5. Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
6. Individuals sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination.

Problems with Computer Forensic Evidence:-

Computer evidence is like any other evidence. It must be

- Authentic
- Accurate
- Complete
- Convincing to juries
- In conformity with common law and legislative rules

There are also special problems:

- Computer data changes moment by moment.
- Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.
- The process of collecting computer data may change it—in significant ways.
- The processes of opening a file or printing it out are not always neutral.
- Computer and telecommunications technologies are always changing so that forensic processes can rarely be fixed for very long.