Cyber criminals are creating havoc on computer systems.

Computer Forensics – involves the preservation, identification, extraction and documentation of computer evidence stored as data or magnetically encoded information.

Securing computers & computer networks is become critical
Surveys show heavy cyber attacks and Cyber Crimes.

Computer Forensics is one of the largest growth professions of the twenty-first century.
Sudden increase in internet users along with constant computerization of business processes ⟹ new opportunities for comp. criminals & terrorist

Gathering and Analysing evidence

Computer Forensics Fundamentals

Considering Computer/Cyber Crimes and conflicts
⇒ gathering electronic evidence & analysing it & information gathering have become very important.
Today Lawenforcement officers seize data media & computers
Today investigators can collect evidence even from remote computers connected to Internet.

What exactly is Computer Forensics??
– is the collection, preservation, analysis and presentation of computer related evidence.
– is the process of methodically examining computer media for evidence
Computer evidence can be useful in criminal cases, civil disputes and human resources/employment proceedings.

Alternative names :- ① Computer Forensics analysis ② Electronic discovery ③ Digital discovery ④ Data recovery ⑤ Data discovery ⑥ Computer analysis .....

For more information is retained on a computer, than most people realize

Difference between Data recovery and Computer Forensics
In data recovery ⇒ the goal is to retrieve the lost data AND
In Computer Forensics ⇒ " to retrieve the data and interpret as much information about it as possible.

The Process of acquiring, examining and applying digital evidence is crucial to the success of prosecuting a cyber criminal.
With the continuous evolution of technology it is difficult for lawenforcement & computer professionals to stay one step ahead of the tech savvy criminals.

Computer / Cyber Crime

Computer users don't know how to protect their sensitive data, thus leaving the door open to criminals.

Types of Crimes that can be done with Computers

- White-collar crimes (Fraud, Bribery, Insider trading, ~~Identity theft, Forgery, money laundering~~ Copyright infringment)
- Violent crimes (Murders, Terrorism, Pornography)
- Counter intelligence (activities concerned with identifying & counteracting threats (plan countermeasures to neutralize threats))
- Economic espionage (establishing relationships with US companies to gather (sensitive / financial / trade / economic secrets))
- Counterfeiting (To imitate something with the intent to steal, destroy or replace the original, for use in illegal transaction)
- Drug dealing. Drug trafficking trade

Economic espionage methods – bribery, dumpster diving
wiretapping

Internet has made targets much more accessible. A person from his home can hack into a bank or any remote system.

Survey on Threats faced

30% → Subject to theft of Proprietary info.
23% → Sabotage of data / network
35% → System penetration from outsiders
12% → Financial fraud.

Survey on Computer Forensic efforts in Cyber Crimes

74% → White collar crimes
26% → (Violent crime, counterfeiting, drug dealing ...)

Roles of a computer in a Crime

A compute can play one of the 3 roles –

(1) It can be the target of the crime
(2) It can be the instrument of the crime (Smoking gun)
(3) It can serve as an evidence repository storing info about the crime. (File cabinet)

Knowing how the computer was used will help narrow down the evidence collection process.

Objective of Computer Forensic

- To recover, analyse and present computer based material in such a way that it is useable as evidence in a court of law.

Computer Forensics Priority

- Concerned with forensic procedures, rules of evidence and legal Processes.

Here the absolute priority is not speed but accuracy.

In Computer Forensics, the emphasis must be on evidential integrity and Security.

The Computer Forensic Specialist

- is the person responsible for doing computer forensics.

Role of Computer Forensic Specialist

⇒ Steps to identify and retrieve possible evidence that may exist-

(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, password-protected files and encrypted files.
(3) Recover all of discovered deleted files.
(4) Reveal the contents of hidden files as well as temporary or swap files.
(5) Accesses the contents of protected or encrypted files.
(6) Analyse all possibly relevant data found.
(7) Print out an overall analysis of the subject computer systems.
(8) Provide expert consultation as required.

Who can use Computer Forensic Evidence ??

① Criminal Prosecutors use computer evidence in a variety of crimes - homicides, financial fraud, drug, record keeping, child pornography.

② Civil litigations can readily make use of personal and business records found on computer system. (Fraud, divorce,

③ Corporations often hire Computer Forensics specialists to find evidence relating to sexual harassment, theft or misappropriation of trade secrets.

④ Law enforcement official frequently require assistance in pre-search warrant preparations & post seizure handling of computer equipment

⑤ Individuals sometimes hire computer Forensic specialists in support of possible claims of wrongful termination, sexual harassment

Use of Computer Forensics in Law Enforcement

If there is a computer at the premises of a crime scene, the chances of finding some evidence on the computer is high.

① Choosing a Computer Forensics Specialist

② Check the level of experience as the individual will be called to testify.

* The court will want to know the individual's level of training & experience.

② Computer Forensics assistance to human resources.

Computers can contain evidence in many types of human resources proceedings.....

ⓐ sexual harassment suits ⓑ allegations of discrimination

ⓒ wrongful termination

Evidence can be found in mainframe systems, on network servers and on individual employee's computers. A trained computer forensic specialist is needed as data can be easily manipulated

* Look not only for expertise & experience, but also the ability to stand up to the scrutiny and pressure of cross examination

Employee Safeguard Program

Considering our existence, in the data driven world, employers must safeguard critical business information. Concern today is the possibility that data could be damaged, destroyed or misappropriated by a discontented individual.

Before an individual is informed of their Termination, a computer forensic specialist should come on site and create an exact duplicate of the data on the individuals computer.
Thus if the employee chooses to create any damage, the employer will be protected.
Damaged or deleted data can be replaced and evidence can be recovered.
This method can also be used to bolster an employers case by showing the removal of proprietary information or to protect the employer from false charges made by the employee.

Whatever be the evidence, we should be able to find and interpret the clues that have been left behind.
clues from files that are deleted, disks that have been formatted or other steps taken to conceal or destroy the evidence.

It is difficult/time consuming for a person to find
(1) the websites visited/downloaded/last accessed.
(2) the attempts to fabricate evidence
(3) that some fax machines can contain exact duplicate of data.

For continuation
Please refer to Pays 9a, 9b, 9c, 9d

Types of Computer Forensic Technology

Cyber Forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media and computer peripherals that allows investigators to solve a crime.

Today Cyber Forensics focuses on real time, online evidence gathering rather than the traditional offline computer disk forensic technology.

Emerging field of Cyber Forensics technology

2 components

Computer Forensics	Network Forensics.
(Handling storage media, Recovering deleted, temp, swap files and info preservation)	(gathering digital info that is distributed across large scale complex network. This evidence is transient in nature and not preserved on storage media. Deals with in depth analysis of network intrusion evidence

The most common is → Postmortem Forensic analysis ie (After crime/attack takes place – analysis/investigation is done).

In the battle against malicious hackers, investigators must perform cyberforensic functions in support of various objectives – These objectives include

1. Cyberattack containment
2. Perpetrator location and identification
3. Damage mitigation
4. Recovery initiation in case of damaged network.

Standard intrusion analysis has to be done.

→ Includes examination of many sources of data evidence (firewall logs, audit trail, intrusion detection System log, network management information)

Analysis of this kind of evidence

Types of Military Computer Forensic Technology

The U.S DoD (Dept of Defense) cyber forensics includes evaluation and in depth examination of data related to both the trans and post cyber attack periods.

Key objectives of Computer Forensic include

1. Rapid discovery of evidence
2. Estimation of potential impact of the malicious activity on the victim.
3. Assessment of the intent and identity of the perpetrator.

Real time tracking of potentially malicious activity is difficult when the info is intentionally hidden, destroyed or modified in order to elude discovery.

The information directorate US entered into a partnership with National Institute of Justice. in association with National Law Enforcement and Correction Technology Center. There is a transitioning cyber Forensic technology from military research and development Lab to hands of Law enforcement.

This partnership resulted in CFX-2000.
(Computer Forensics Experiment 2000)

The central hypothesis of CFX-2000, is that it is pucible to accurately determine the motives, intents, targets sophistication, identity and location of cyber criminals and cyber terrorists by deploying an integrated forensic analysis framework.

The execution of CFX 2000 required the simulation of a realistic, complex cyber crime scenario as well as use of Cyber Forensic tools

CFX-2000 is an integrated forensic analysis framework

The Cyber Forensic Tools involved in CFX-2000 are Comercial off the shelf softwares.
The Synthesizing information forom Forensic Investigations (SI-FI) environment supports the collection, examination and analysis processes employed during a cyber forensic investigation
The SI-FI prototype uses digital evidence bags, which are secure and tamper-proof containers used to store digital evidence.
The result of CFX 2000 verified that the hypothesis was correct.

Types of Law enforcement Computer Forensic Technology

Computer Forensic Tools are used to gather evidence to be used for internal investigations, civil lawsuits and computer Security risk management.
* Law enforcement & Military agencies involved in processing computer evidence.

Computer Evidence Processing Procedures.

1. ~~Preservation of Evidence~~

All procedures & methodologies should conform to federal computer evidence processing standards.

1. Preservation of Evidence
   - ⇒ Computer evidence is fragile and susceptible to alteration or erasure.
   - ⇒ Computer evidence can be useful in criminal cases, civil disputes and human resources/employment proceedings.
   - ⇒ Black box computer forensic software tools are good for some basic investigation tasks, but do not offer a full forensic solution
   - ⇒ SafeBack technology has become a worldwide standard in making mirror image backups Since 1990

Trojan Horse Programs

⇒ The computer Forensic expert should be able to demonstrate his ability to avoid destructive programs and traps that can be planted by Computer users bent on destroying data and evidence

⇒ Such programs can also be used to capture sensitive information like passwords, logins ...

⇒

Computer Forensic Documentation

⇒ Without proper documentation, it is difficult to present findings.

⇒ If audit findings become the object of a criminal investigation, then documentation is very important.

File Slack

⇒ Slack space in a file is the remnant area at the end of a file in the last assigned disk cluster that is unused by current file data, but may be a possible site for previously created and relevant evidence

⇒ Techniques & automated tools are used by experts to capture and evaluate file slack.

Data hiding techniques

⇒ Trade Secrets and other sensitive data can easily be hidden using a number of techniques. It is possible to hide data with image/Audio/Video (STEGANOGRAPHY) or hide entire computer hard disk drive partitions. Computer Forensic experts should understand such issues & tools that help in the identification

E-Commerce Investigations

⇒ Various tools like "Net Threat Analyzer" are available and can be used to identify past Internet browsing and email activity on a Computer.

Computer Forensic experts must have hands on experience with these programs.

Text Search Techniques

⇒ Tools that can be used to find targeted strings of text in files, file slack, unallocated file space and Window swap files.

Fuzzy logic tools

Sometime the forensic expert may not be aware of what may be stored on a given computer system. In such situations, fuzzy logic tools can provide valuable leads.

2. Disk Structure

⇒ Computer Forensic expert must understand how computer hard disks, floppy disks, Flash drives are structured and how computer evidence can reside at various levels within them.

⇒ They should also demonstrate knowledge on how to modify the structure and hide data in obscure places on disks.

3. Data Encryption:

⇒ Computer Forensic expert must be familiar with the use of software to crack security associated with diff file structures.

4. Matching a Diskette to a Computer.

⇒ Must be acquainted with various specialized techniques and tools that make it possible to tie a diskette to a computer that was used to create or edit files.

5. Data Compression

⇒ Computer Forensic experts must be familiar with how compression works and how compression programs can be used to hide and disguise sensitive data and also learn how password protected compressed files can be broken.

6. Erased Files

⇒ Experts should be familiar with how previously erased files can be recovered by using DOS programs.

7. Internet Abuse Identification & Detection.

⇒ Forensic experts should become familiar with how to use specialized software to identify how a targeted computer has been used on the Internet.

8. The Boot Process and Memory Resident Programs

⇒ Computer Forensic experts should be familiar with how the operating system can be modified to change data and destroy data at the whim of the person who configured the System.

Types of Business Computer Forensic Technology

- Remote monitoring of Target Computers

⇒ DIRT (Data Interception by Remote Transmission) is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more computers simultaneously from a remote command centre.

⇒ The application also allows to remotely seize and secure digital evidence prior to physically entering the suspect premises.

- Creating Trackable Electronic documents

→ BAIT (Binary Audit Identification Transfer) is a powerful Intrusion detection Tool that allows users to create trackable electronic documents.

→ BAIT identifies unauthorized users/intruders who access, download and view these tagged docs.

→ BAIT also allows to track the chain of custody and chain of command of all who poses the stolen electronic documents.

- Theft Recovery Software for Laptops & PC's.

What does it cost to replace a stolen computer?
→ The price of replacement of hardware & software
→ The cost of recreating data, lost production time, time for reporting and investigating the theft, filing police report and insurance claims.
→ Loss of customer goodwill

PC PhoneHome is a software application that will track and locate a lost or stolen PC or laptop anywhere in the world. Easy to install.

Forensic Services Available

Services include but are not limited to —
1. Lost Password and file recovery.
2. Location & retrieval of deleted & hidden files
3. File and email decryption
4. Email supervision & authentication
5. Threatening email traced to source.
6. Identification of Internet activity
7. Computer usage policy & supervision
8. Remote PC & network monitoring
9. HoneyPot sting operations
10. Location & Identity of Unauthorized s/w users.
11. Theft recovery s/w for laptops & PC
12. Protection from hackers & viruses.

Computer Forensic Evidence & Capture

Data Recovery Defined

Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format.

It is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

Data Backup and Recovery

Backup Obstacles

⇒ Backup Window – is the period of time when backups can be run. Usually timed during nonproduction periods when network bandwidth and CPU utilization are low.

⇒ Network bandwidth – If network cannot handle impact of transporting hundreds of gigabytes of data over a short period of time, the organizations centralized backup strategy is not viable.

⇒ System throughput

→ Lack of Resources

The Role of Backup in Data Recovery

There are many factors that affect backup.

⇒ Storage costs are decreasing –

⇒ Systems have to be online continuously

⇒ The role of backup has changed.

Issues with todays backup

Network backup creates network performance problems.

Offline backup – affects data accessibility. This requires extremely high-speed, continuous parallel backup of the raw image of data.

Live backups - allows data access during the backup process but affect performance. It puts a tremendous burden on the host.

Mirroring - does not protect against user errors and replication of bad data

Requirement / Necessity

(1) Backup at extremely high speed is required.
(2) Remote hot recovery sites are needed for immediate resumption of data access.
(3) To achieve effective backup and recovery, the decoupling of data from its storage space is needed.
(4) Part of the primary storage area must be set aside for data to be backed up. We must have fast nonrandom restoration of critical data.

The Data Recovery Solution

Earlier availability was 9-5pm. Today it is 24 * 7.

* Shrinking expertise, growing Complexity

The complex systems created/evolved must be monitored, managed, controlled and optimized.
Backups today take place when an application is running. Application changes take place on the fly.

Benefits of Professional Forensics Methodology

Computer evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence even alternate formats of the same data can be discovered.

Protection of evidence is critical.
A Knowledgeable computer forensics expert / professional should ensure that a computer system is carefully handled to ensure that -

- No possible evidence is damaged, destroyed or otherwise compromised by the procedures used to investigate the computer.
- No possible computer virus is introduced to a subject computer during the analysis process.
- Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.
- A continuing chain of custody is established and maintained
- Business operations are affected for a limited amount of time.

Steps taken by Computer Forensic expert

The Computer Forensic specialists needs to complete an Evidence Identification and Retrieval checklist

Problems with Computer Forensic Evidence

(1) Computer evidence is like any other evidence. It must be
- Authentic • Accurate • Complete • Convincing to juries
- In conformity with common law and legislative rules.

(2) Computer data changes moment by moment.
(3) Computer data is invisible to the human eye, it can only be viewed indirectly after appropriate procedures.
(4) Computer and telecommunication Technologies are always changing.

The Forensic Technician

The scene of crime has to be frozen. There must be continuity of evidence also called as chain of custody. All procedures used in the examination should be auditable.

The Key features of the Forensic technician are
(1) Careful methodology of approach, including record keeping
(2) A sound knowledge of computing
(3) A sound knowledge of the law of evidence
(4) A sound knowledge of legal procedures
(5) Access to and skill in the use of appropriate utilities.

Important Points to Keep in mind for a Forensic Technician

(1) Legal Tests - Its the law that makes distinctions between real evidence, testimonial evidence and hearsay.

Real evidence is that which comes from an inanimate object that can be examined by the court.

Testimonial evidence is that which a live witness has seen and upon which he or she can be cross-examined.

The hearsay rule ~~is extremely restrictive~~ and operates to exclude assertions made other than those made by the witness who is testifying as evidence of the truth of what is being asserted.

Subject Matter of Computer Forensics

The ultimate aim of forensic investigation is its use in legal proceedings. Sometimes the judicial rules are likely to inhibit many investigations.

The broad tests for evidence include :

(1) Authenticity - Does the material come from where it purports?
(2) Reliability - Can you believe it and is it consistent?
(3) Completeness - Enough matter that helps complete the story.
(4) Freedom from interference & contamination - Are these levels acceptable as a result of forensic investigation and post event handling.

Computer Forensic includes the elements of :

(1) well defined procedures to address the various tasks
(2) An anticipation of likely criticism of each methodology on the grounds of failure to demonstrate authenticity, Reliability, completeness
(3) The possibility for repeat tests to be carried out, by experts hired by other side.
(4) checklists to support each methodology
(5) An anticipation of any problems in formal legal tests of admissibility

~~Divergences from Conventional Forensic investigation~~

- Main reason is the rate of change of computer technology
- In computers, newness and obsolence is the norm.

ex (1) Key feature is examination of data media. However new methods of data storage occurs at intervals of less than 4 years.
(2) Computer architectures have gone through profound changes.
(3) Computer Peripherals keep changing

Virus / Trojan / WORM protection

Tips to avoid :

(1) Dont open emails sent with junk email addr or from person you dont know
(2) Dont open any attachments in email if subject or extension is unexpected
(3) Disable the Windows Scripting Host on your PC (Control Panel → Add/Remove Programs → Windows setup → Accessories → Window Scripting host)
(4) Always download files from trusted sites
(5) Configure an antivirus software on PC. Keep auto scanning ON
(6) Back up your files on a regular basis.
(7) Write protect all system ed disks.
(8) Dont boot from a floppy disk.
(9) Scan floppy / pendrive before using them.
(10) Outlook / Outlook express are most targeted emails. Download Microsoft security patches

Specialized Forensic Techniques

Any attack involving a computer or a network as a media can be / result in huge strategic / financial loss of the organization. Systems hold a companys proprietary information and business processes. A simple and virtually undetectable fraud that posts a few rupees to a phony account, can reap a perpetrator thousands of dollars. A malicious change to an individuals personnel records could cost a person a job or a career. Divulging a companys financial records could damage it in the market and among stakeholders. Posting libelous information on the internet about a company or individual can damage reputation beyond recovery. Company employees can be using office time to surf pornographic sites and to play games.

Computer forensic investigators examine computer hardware & software using legal procedures to obtain evidence that proves or disproves allegations. Gathering legal evidence is difficult and requires trained specialists who know computers, the rules of evidence gathering and how to work with the law enforcement authorities.

Computer Forensic examiner / experts / technicians should be called in when a threat to a companys business and reputation is serious. Any organisation that does not have a way to detect and stop malicious behavior can be victimized with no legal recourse. Preserving evidence according to Federal rules of evidence gives choices that otherwise would not exist. When an intruder attacks or steals from an organization, the ability or threat to get law enforcement involved may be the only way to reduce damage or prevent future occurances. Companies employ computer forensics when there is a serious risk of information being compromised, a potential loss of competitive capability, a threat of lawsuits or potential damage to reputation and brand.
When the cost of a forensic investigation exceeds the potential gain, there is little reason to use it.

LEGAL EVIDENCE

* A computer Forensic examiner should always gather and preserve evidence according to the Federal rules of evidence. He has 3 basic tasks - Finding preserving and preparing Evidence. Preparing evidence requires patience and thorough documentation, so it can withstand judicial scrutiny. Preserving computer evidence requires training of employees in incident discovery procedures. ex. Never run programs on a computer under investigation. Running windows to examine files, destroys evidence on the such file. Examiners search at the bit levels of 1's and 0's across a wide range of areas inside a computer, including email, swapfile, OS, database, logs, slack files, cache, history than they correlate.

Computer Forensics Services

No matter, how careful people are, when they attempt to steal electronic info they leave behind traces of their activities. Likewise, when people try to destroy incriminating evidence contained on a computer, they leave behind vital clues.

The computer forensic professional should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case.

A computer Forensic professional must be able to perform foll. services :

- Data seizure
- Data duplication & preservation
- Data recovery
- Document Searches
- Media Conversion
- Expert witness Services
- Computer evidence service options
- Miscellaneous Services.

Data Seizure - Federal rules of civil procedure lets a party or their representatives inspect and copy designated documents or data compilations that may contain evidence.

Data duplication and Preservation - when one party must seize data from another, 2 concerns must be addressed -

(1) The data must not be altered in any way
(2) The seizure must not put an undue burden on the responding party.

The computer forensic expert must make an exact duplicate of the needed data. Because duplication is fast, the responding party can quickly resume its normal business functions and since the experts work on the duplicated data, the integrity of the original data is maintained.

Data Recovery - Using proprietary tools, the computer forensics expert should be able to safely recover and analyse otherwise inaccessible evidence. The ability to recover lost evidence is made possible by the experts advanced understanding of storage technologies.

ex when a user deletes, an email, the user does not get access to it again. But a forensic expert should be able to recover it and locate relevant evidence.

Document Searches - A computer Forensic expert should 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

Media Conversion - Some clients need to obtain and investigate computer data stored on old and unreadable devices. The computer forensic expert should be able to extract the relevant data from these devices, convert it to readable formats, and place it onto new storage media for analysis.

Expert Witness Services – Computer Forensic 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

The computer Forensic experts should be able to offer following services

- Standard Service – The computer forensic expert should be able to work on your case during normal business hours until your critical electronic evidence is found.
- On-site Service – Forensic expert should be able to travel to any location to perform computer evidence services. On site, the expert should be able to produce exact duplicates of the data storage media, minimizing the disruption of normal business services.
- Emergency Service – The forensic experts should be able to give the case the highest priority in their laboratories.
- Priority Service – Dedicated computer forensic experts should be able to work on the case, until evidence is found.
- Weekend Service – Forensic experts should be able to work on weekends also to locate the needed evidence and continue working until evidence objectives are met.

Miscellaneous Services

Analysis of computers and data in criminal investigation / civil litigation
On site seizure of computer data in criminal investigation / civil litigation
Analysis of company computers to determine employee activity.
Fast Turnaround time.
Court recognized computer expert witness testimony.