Computer Forensics Fundamentals

- Electronic evidence and information gathering have become central issues in an increasing number of conflicts and crimes.
- Electronic or computer evidence used to mean the regular print-out from a computer—and a great deal of computer exhibits in court are just that.
- However, for many years, law enforcement officers have been seizing data media and computers themselves, as they have become smaller and more ubiquitous.
- In the very recent past, investigators generated their own printouts, sometimes using the original application program, sometimes specialist analytic and examination tools

- More recently, investigators have found ways of collecting evidence from remote computers to which they do not have immediate physical access, provided such computers are accessible via a phone line or network connection.
- It is even possible to track activities across a computer network, including the Internet.
- These procedures form part of what is called *computer forensics,* **though some people also use the term to include the use of computers to analyze complex data** (for example, connections between individuals by examination of telephone logs or bank account transactions)

- Another use of the term is when computers are employed in the court itself, in the form of computer graphics, to illustrate a complex situation such as a fraud or as a replacement for large volumes of paper-based exhibits and statements.
- **what actually is computer forensics? Computer forensics is about evidence from computers that is sufficiently reliable to stand up in court and be convincing.**
- You might employ a computer forensics specialist to acquire evidence from computers on your behalf.

Introduction to 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 methodically 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/employment proceedings.**
- **Computer forensics can often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted.**

- Computer forensics, although employing some of the same skills and software as data recovery, is a much more complex undertaking.
- **In data recovery, the goal is to retrieve the lost data.**
- **In computer forensics, the goal is to retrieve the data and interpret as much information about it as possible.**

- Computer crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence.
- This has developed into the science of computer forensics. **The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal**

- To effectively combat cyber crime, greater emphasis must be placed in the computer forensic field of study, including but not limited to financial support, international guidelines and laws, and training of the professionals involved in the process, as well as the following subject matter:
- **Computer crime**
- **The computer forensic objective**
- **The computer forensic priority**
- **The accuracy versus speed conflict**
- **The need for computer forensics**
- **The double tier approach**
- **Requirements for the double tier approach**
- **The computer forensics specialist**

Computer Crime

- **Computers can be involved in a wide variety of crimes including white-collar crimes, violent crimes such as murder and terrorism, counterintelligence(organized activity of an intelligence service designed to block an enemy's sources of information), economic espionage(unauthorised and usually criminal access to confidential systems and information for the purposes of gaining a commercial or political advantage.), counterfeiting(imitate fraudulently.), and drug dealing.**
- A 2003 FBI survey reported that the average bank robbery netted $6,900, whereas the average computer crime netted $900,000

- A person can sit in the comfort of his home or a remote site and hack into a bank and transfer millions of dollars to a fictitious account, in essence robbing the bank, without the threat of being gunned down while escaping.
- We hear such technological crimes almost daily, thus creating a perception of lawlessness in the cyber world

- Recently a survey was conducted to determine where the FBI was focusing their computer forensic efforts.
- An alarming 74% of their workload is cantered on white-collar crime. **This type of crime includes health care fraud, government fraud including erroneous IRS (Internal Revenue service and social Security benefit payments, and financial institution fraud. These are high-dollar crimes made easy by technology**
- The other 26% of the workload is split equally among **violent crime (child pornography, interstate theft), organized crime (drug dealing, criminal enterprise), and counterterrorism and national security**

Role of Computer in a crime

- A computer can play one of three roles in a computer crime.

1. **A computer can be the target of the crime,**
2. **it can be the instrument of the crime, or**
3. **it can serve as an evidence repository storing valuable information about the crime**

- For example, a hacker may use the computer as the tool to break into another computer and steal files, then store them on the computer.
- **When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role.**

- Applying information about how the computer was used in the crime also helps when searching the system for evidence.
- **If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and password files.**
- **If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked.**
- **Knowing how the computer was used will help narrow down the evidence collection process**

- With the size of hard drives these days, it can take a very long time to check and analyze every piece of data a computer contains.
- Often law enforcement officials need the information quickly, and having a general idea of what to look for will speed the evidence collection process.

The Computer Forensic Objective

- **The objective of the Computer Forensic is to recover, analyze, and present computer-based material in such a way that it is useable as evidence in a court of law.**
- **The key phrase here is *useable as evidence in a court of law*.**
- **It is essential that none of the equipment or procedures used during the examination of the computer obviate this.**

The Forensic Priority

- **Computer forensics is concerned primarily with forensic procedures, rules of evidence and legal processes. It is only secondarily concerned with computers.**
- **Therefore, in contrast to all other areas of computing, where speed is the main concern, in computer forensics the absolute priority is accuracy**.
- Need is completing work as efficiently as possible, that is, as fast as possible without sacrificing accuracy.

Accuracy versus speed

- Today time is precious and we need to speed up the work as fast as possible
- **Working under such pressure to achieve deadlines may induce people to take shortcuts in order to save time.**
- **In computer forensics, as in any branch of forensic science, the emphasis must be on evidential integrity and security**.
- **In observing this priority, every forensic practitioner must adhere to stringent guidelines.**
- Such guidelines do not encompass the taking of shortcuts, and the forensic practitioner accepts that the precious resource of time must be expended in order to maintain the highest standards of work.

The computer Forensic Specialist

- **A computer forensics specialist is the person who is responsible for doing computer forensics.**
- **The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system:**

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 (or as much as possible) of discovered deleted files.

4. Reveal (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.

5. **Accesses (if possible and if legally appropriate) the contents of protected or encrypted files.**

6. Analyze all possibly relevant data found in special (and typically in accessible) areas of a disk.

This includes but is not limited to what is called unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as slack space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data but once again may be a possible site for previously created and relevant evidence).

7. Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.

Further, provide an opinion of the system layout;

- The file structures discovered;
- Any discovered data and authorship information;
- Any attempts to hide, delete, protect, or encrypt information;
- And anything else that has been discovered and appears to be relevant to the overall computer system examination.

8. **Provide expert consultation and/or testimony, as required**

Who Can Use Computer Forensic Evidence?

- Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists:

1. **Criminal Prosecutors use computer evidence in a variety of crimes where incriminating documents can be found**: homicides, financial fraud, drug and embezzlement (theft or misappropriation of funds placed in one's trust or belonging to one's employer.) 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. **Insurance companies may be able to mitigate costs by** using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.

3. **Corporations often hire computer forensics specialists to find** evidence relating to sexual harassment, embezzlement(theft or misappropriation of funds placed in one's trust or belonging to one's employer), theft or misappropriation of trade secrets, and other internal/confidential information.
4. **Law enforcement officials frequently require assistance** in pre-search warrant preparations and post-seizure handling of the computer equipment.
5. **Individuals sometimes hire computer forensics specialists in** support of possible claims of wrongful termination, sexual harassment, or age discrimination

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 (even if very briefly) 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, look very carefully at the level of experience of the individuals involved.
- **There is far more to proper computer forensic analysis than the ability to retrieve data, especially when a criminal case is involved.**
- Think about computer forensics just as you would any other forensic science and look for a corresponding level of expertise.

- It is better to retain 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.
- 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.**

Employer Safeguard Program

- **As computers become more prevalent 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.
- **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 individual's computer**
- In this way, data of the employer is protected, damaged or deleted data can be replaced, and evidence can be recovered to show what occurred

- **Whether we are looking for evidence in a criminal prosecution or civil suit or determining exactly what an employee has been up to, we 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:

- **What Web sites have been visited**
- **What files have been downloaded**
- **When files were last accessed**
- **Of attempts to conceal or destroy evidence**
- **Of attempts to fabricate evidence**
- **That the electronic copy of a document can contain text that was removed from the final printed version**
- **That some fax machines can contain exact duplicates of the last several hundred pages received**
- **That faxes sent or received via computer may remain on the computer indefinitely**
- **That email is rapidly becoming the communications medium of choice for businesses**
- **That people tend to write things in email that they would never consider writing in a memorandum or letter**
- **That email has been used successfully in criminal cases as well as in civil litigation**
- **That email is often backed up on tapes that are generally kept for months or years**

- **That many people keep their financial records, including investments, on computers**

COMPUTER FORENSICS SERVICES

- No matter how careful they are, when people attempt to steal electronic information (everything from customer databases to blueprints), they leave behind traces of their activities.
- **Likewise, when people try to destroy incriminating evidence contained on a computer (from harassing memos to stolen technology), they leave behind vital clues**
- **Thus, computer data evidence is quickly becoming a reliable and essential form of evidence that should not be overlooked**

- A computer forensics professional more than turn on a computer, make a directory listing, and search through files. The forensics professional 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 lets a party or their representative inspect and copy designated documents or data compilations that may contain evidence.**
- **The computer forensics expert should follow the federal guidelines, and act as this representative, using his/her knowledge of data storage technologies to track down evidence**

Data Duplication and Preservation

- When a party has to 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.
- The computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data so that while working on the duplicated data, the integrity of the original data is maintained.

Data Recovery

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

Document Searches

- The 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

- Some clients need to obtain and investigate computer data stored on old and unreadable devices.
- **The 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

- **The computer forensics experts should offer various levels of service, each designed to suit the individual investigative needs.**
- For example, they should be able to offer the following services:

1. Standard service
2. On-site service
3. Emergency service
4. Priority service
5. Weekend service

- **Standard Service**
- The computer forensics experts should be able to work on your case during normal business hours until your critical electronic evidence is found.
- They must be able to provide clean rooms and ensure that all warranties on your equipment will still be valid following their services.

- **On-Site Service**
- The computer forensics experts should be able to travel to the location to perform complete computer evidence services.
- While on-site, the experts should quickly be able to produce exact duplicates of the data storage media in question
- Their services should then be performed on the duplicate, minimizing the disruption to business and the computer system.
- The experts should also be able to help federal marshals seize computer data and be very familiar with the Federal Guidelines for Searching and Seizing Computers

Emergency Service

- After receiving the computer storage media, your computer forensics experts should be able to give your case the highest priority in their laboratories.
- They should be able to work on it without interruption until your evidence objectives are met.

Priority Service

- Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found.
- Priority service typically cuts your turnaround time in half

- **Weekend Service**
- **Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue working on your case until your evidence objectives are met.**
- **Weekend service depends on the availability of computer forensics experts**

Other Miscellaneous Services

- Computer forensics experts should also be able to provide extended services. These services include

1. Analysis of computers and data in criminal investigations
2. On-site seizure of computer data in criminal investigations
3. Analysis of computers and data in civil litigation.
4. On-site seizure of computer data in civil litigation
5. Analysis of company computers to determine employee activity
6. Assistance in preparing electronic discovery requests
7. Reporting in a comprehensive and readily understandable manner
8. Court-recognized computer expert witness testimony
9. Computer forensics on both PC and Mac platforms
10. Fast turnaround time

Recover Data You Thought Was Lost Forever

1. Computers systems may crash.
2. Files may be accidentally deleted.
3. Disks may accidentally be reformatted.
4. Computer viruses may corrupt files. Files may be accidentally overwritten.
5. Disgruntled employees may try to destroy your files.

- **All of these can lead to the loss of your critical data.**
- **You may think it's lost forever, but computer forensics experts should be able to employ the latest tools and techniques to recover your data.**

- The advanced tools that computer forensics experts utilize allow them to find your files and restore them for your use.
- In the instances where the files have been irreparably damaged, the experts' computer forensics expertise allows them to recover even the smallest remaining fragments.

Advise You on How to Keep Your Data and Information Safe from Theft or Accidental Loss

- **Business today relies on computers. The sensitive client records or trade secrets are vulnerable to intentional attacks from, for example, computer hackers, disgruntled employees, viruses, and corporate espionage.**
- **Equally threatening, but far less considered, are unintentional data losses caused by accidental deletion, computer hardware and software crashes, and accidental modification**
- **Computer forensics experts should advise you on how to safeguard your data by such methods as encryption and back-up. The experts can also thoroughly clean sensitive data from any computer system you plan on eliminating**
- Computer forensics experts should survey your business and provide guidance for improving the security of your information

Examine a Computer to Find Out What Its User Has Been Doing

- **Whether you're looking for evidence in a criminal prosecution, looking for evidence in a civil suit, or determining exactly what an employee has been up to**.
- **The computer forensics experts 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 evidence

- The computer forensics experts should provide complete forensic services.
- **These include electronic discovery consultation, on-site seizure of evidence, thorough processing of evidence, interpretation of the results, reporting the results in an understandable manner, and court-recognized expert testimony**
- The computer forensics experts should also be able to regularly provide training to other forensic examiners, from both the government and private sectors

Sweep Your Office for Listening Devices

- In today's high-tech society, bugging devices, ranging from micro-miniature transmitters to micro-miniature recorders, are readily available.
- Automatic telephone recording devices are as close as your nearest Radio Shack store.
- **Your computer forensics experts should have the equipment and expertise to conduct thorough electronic countermeasures (ECM) sweeps of your premises.**

High-Tech Investigations

- **The computer forensics experts should have high level government investigative experience and the knowledge and experience to conduct investigations involving technology, whether the technology is the focus of the investigation or is required to conduct the investigation.**
- The experts should be uniquely qualified to conduct investigations involving cellular telephone cloning, cellular subscription fraud, software piracy, data or information theft, trade secrets, computer crimes, misuse of computers by employees, or any other technology issue

- So, what are your employees actually doing?

1. **Are they endlessly surfing the Web?**
2. **Are they downloading pornography and opening your company to a sexual harassment lawsuit?**
3. **Are they emailing trade secrets to your competitors?**
4. **Are they running their own business from your facilities while they are on your clock?**

- **Your computer forensics experts should be uniquely qualified to answer these questions and many more.**

BENEFITS OF PROFESSIONAL FORENSICS METHODOLOGY

- The impartial computer forensics expert who helps during discovery will typically have experience on a wide range of computer hardware and software.
- It is always beneficial when your case involves hardware and software with which this expert is directly familiar, but fundamental computer design and software implementation is often quite similar from one system to another.
- Experience in one application or operating system area is often easily transferable to a new system

- 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

- The computer forensics specialist needs to complete an Evidence Identification and Retrieval Checklist (as shown in Table F1.1 in Appendix F).
- He or she should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system.

- Provide an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.

9. Provide expert consultation and/or testimony, as required