FACULTY OF ENGINEERING & TECHNOLOGY

RBS COLLEGE, BICHPURI, AGRA

SEMINAR REPORT

On

COMPUTER FORENSICS

SUBMITTED TO: -
SUBMITTED BY:-

Er. BRAJESH KUMAR SINGH
ANKIT MISHRA

ACKNOWLEDGEMENT

I express my sincere gratitude to the entire Faculty of Engineering & Technology, Raja Balwant Singh College, Agra for their support and guidance provided for this seminar.

I am highly indebted to our respected guide Er. Brajesh Kumar Singh, Dept. of Computer Science & Engineering for his excellent guidance and cooperation.

I would also like to thank all my friends and my family, who were the source of constant encouragement.

Above all I thank the Almighty for His grace.

ANKIT MISHRA

ABSTRACT

This paper will discuss the need for computer forensics to be practiced in an effective and legal way, outline basic technical issues, and point to references for further reading. It promotes the idea that the competent practice of computer forensics and awareness of applicable laws is essential for today's networked organizations.

This subject is important for managers who need to understand how computer forensics fits as a strategic element in overall organizational computer security. Network administrators and other computer security staff need to understand issues associated with computer forensics. Those who work in corporate governance, legal departments, or IT should find an overview of computer forensics in an organizational context useful.

Presently, computing forensics training is provided almost exclusively by law enforcement organizations; only a few universities support computing forensics programs, and most comprise only one course. We expect this to change over the next three to five years, and we hope that evolving programs can leverage experience gained through the recent US National Security Agency-prompted expansion of information-assurance education programs. The health of the Internet itself may depend on it.

CONTENTS

1. INTRODUCTION/HISTORY

a. **Definition: -** Computer forensic science was created to address the specific and articulated needs of law enforcement to make the most of this new form of electronic evidence. ***"Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable."(Rodney Mckemmish 1999).*** From this definition we can clearly identify four components:-

i. **Identifying: -** This is the process of identifying things such as what evidence is present, where and how it is stored, and which operating system is being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

ii. **Preserving: -** This is the process of preserving the integrity of digital evidence, ensuring the chain of custody is not broken. The data needs to be preserved (copied) on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any changes to the evidence should be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in the court of law.

iii. **Analysis: -** This is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact it can be viewed without the risk of accidental changes, therefore maintaining the integrity whilst examining the changes.

iv. **Presenting: -** This is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court the jury who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all efforts could be futile.

b. **Goals of computer forensics: -** The goal of computer forensics is to retrieve the data and interpret as much information about it as possible as compared to data recovery where the goal is to retrieve the lost data.

As a forensic discipline, nothing since DNA technology has had such a large potential effect on specific types of investigations and prosecutions as computer forensic science.

Computer forensic science is, at its core, different from most traditional forensic disciplines. The computer material that is examined and the techniques available to the examiner are products of a market-driven private sector. Furthermore, in contrast to traditional forensic analyses, there commonly is a requirement to perform computer examinations at virtually any physical location, not only in a controlled laboratory setting. Rather than producing interpretative conclusions, as in many forensic disciplines, computer forensic science produces direct information and data that may have significance in a case. This type of direct data collection has wide-ranging implications for both the relationship between the investigator and the forensic scientist and the work product of the forensic computer examination.

It is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. Although it is most often associated with the investigation of a wide variety of computer crime, it may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems.

c. **Computer forensics: An art or science: -** It is often more of an art than a science, but as in any discipline, computer forensic specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual. It is unfortunate that computer forensics is sometimes misunderstood as being somehow different from other types of investigations. For instance, if you were investigating a murder that took place in Times Square, you would photograph the scene, look for evidence, and take samples of the crime scene, including control samples to compare to the evidence. The collection of evidence proceeds similarly in a computer investigation, but for some reason, some people want to recreate the entire system, be it a standalone PC, a server with a terabyte RAID system, or even an entire network. Nobody expects the prosecution to rebuild Times Square in the courtroom, but that is often the expectation in a computer crime case. Admittedly, digital data can be highly volatile.

This is a good place to remind ourselves that we have to treat every case as if it will end up in court. Take a minute to think of the consequences; don't start poking around a computer, decide that you have a problem, and then start handling it as evidence. It is easier to regard the computer as evidence from the start, easing up on the evidentiary process if you discover that a crime wasn't committed. The opposite approach is more difficult, if not impossible. However, if you reasonably ("reasonableness" is a key to most laws) believe when you start "looking around" on the computer that it doesn't warrant a forensic analysis and later discover an overtly illicit act was committed, make sure that you fully document what you did and why. Your evidence may still be defensible if explained to a judge and jury that you initially had no reason to suspect that the computer was involved in a criminal act, and subsequently discovered the crime when conducting routine troubleshooting, but only if you fully documented your activities. The key to any investigation, particularly a computer crime investigation, is documentation.

If you manage or administer information systems and networks, you should understand computer forensics. Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive. Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. *We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.*

d. **History: -** In the early 1980s personal computers began to be more accessible to consumers and, subsequently, began to be used for criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as hacking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Today it is used to investigate a wide variety of crime, including child pornography, fraud, cyber stalking, murder and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery).

Forensic techniques and expert knowledge are used to explain the current state of a *digital artifact*; such as a computer system, storage medium (e.g. hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image). The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events. In a 2002 book *Computer Forensics* authors Kruse and Heiser define computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data".

The techniques used to recover information (particularly deleted information) are similar to data recovery processes. These are performed under forensic conditions to allow use of the evidence in court.

Computer forensic science is largely a response to a demand for service from the law enforcement community. As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence. To properly address the growing demands of investigators and prosecutors in a structured and programmatic manner, the FBI established the Computer Analysis and Response Team (CART) and charged it with the responsibility for computer analysis. Although CART is unique in the FBI, its functions and general organization are duplicated in many other law enforcement agencies in the United States and other countries.

An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence. These resources were often scattered throughout the agency. Today, there appears to be a trend toward moving these examinations to a laboratory environment. In 1995, a survey conducted by the U.S. Secret Service indicated that 48 percent of the agencies had computer forensic laboratories and that 68 percent of the computer evidence seized was forwarded to the experts in those laboratories. As encouraging as these statistics are for a controlled programmatic response to computer forensic needs, the same survey reported that 70 percent of these same law enforcement agencies were doing the work without a written procedures manual (Noblett 1995).

Computer forensic examinations are conducted in forensic laboratories, data processing departments, and in some cases, the detective's squad room. The assignment of personnel to conduct these examinations is based often on available expertise, as well as departmental policy. Regardless of where the examinations are conducted, a valid and reliable forensic examination is required. This requirement recognizes no political, bureaucratic, technological, or jurisdictional boundaries.

2. ABOUT THE PROBLEM

The problem basically behind the computers is the attacks. But a general question arises what are attacks in relation to a computer network or simply a computer system? An attack is defined as any kind of malicious activity targeted against computer system resources, including (but not limited to) a break-in (any unauthorized access), virus infestation, data alteration or destruction, or distributed denial of service attacks.

a. **General Problem: -** Computers systems may crash, files may be accidentally deleted, disks may accidentally be reformatted, viruses may corrupt files, file may be accidentally overwritten, disgruntled employees may try to destroy your files. All of this can lead to loss of your critical data. Your sensitive records and trade secrets are vulnerable to intentional attacks from, for e.g. hackers, disgruntled employees, viruses, etc. also unintentional loss of data due to accidental deletion, h/w or s/w crashes are equally threatening.

b. **Criminal Problem: -** The criminal element in society learns to use computers for personal and professional activities, police departments at all levels will most likely increase their hiring of computer forensic experts & on the other hand the number of computer forensics experts might not be large.

What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assigns liability if certain types of data are not adequately protected. Recent legislation makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data.

Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. Files may have been deleted, damaged, or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process.

c. **Global Problem: -** The world is becoming a smaller place in which to live and work. A technological revolution in communications and information exchange has taken place within business, industry, and our homes. America is substantially more invested in information processing and management than manufacturing goods, and this has affected our professional and personal lives. We bank and transfer money electronically, and we are much more likely to receive an E-mail than a letter. It is estimated that the worldwide Internet population is 349 million (CommerceNet Research Council 2000).

FBI computer

In this information technology age, the needs of law enforcement are changing as well. Some traditional crimes, especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. Crimes of violence also are not immune to the effects of the information age. A serious and costly terrorist act could come from the Internet instead of a truck bomb. The diary of a serial killer may be recorded on a floppy disk or hard disk drive rather than on paper in a notebook.

evidence examiners review the contents of a computer hard drive.

Just as the workforce has gradually converted from manufacturing goods to processing information, criminal activity has, to a large extent, also converted from a physical dimension, in which evidence and investigations are described in tangible terms, to a cyber dimension, in which evidence exists only electronically, and investigations are conducted online.

As difficult as it would be to scan a directory of every file on a computer system, it would be equally difficult for law enforcement personnel to read and assimilate the amount of information contained within the files. For example, 12 GB of printed text data would create a stack of paper 24 stories high.

d. **DNA analysis: -** DNA analysis attempts to develop specific identifying information relative to an individual. To support the conclusions, forensic DNA scientists had to gather extensive statistical data on the DNA profiles from which they base their conclusions but the absence of computer forensics led to its failure in the past. The purpose of the computer examination is to find information related to the case but without computer forensics it was not fully possible. To support this computer forensic examination was introduced, for which procedures are needed to ensure that only the information exists on the computer storage media, unaltered by the examination process. Forensic DNA analysis or other forensic disciplines, were not so accurate, reliable, or discriminating power of the actual data or information.

e. **Traditional & Computer forensic science: -** Beyond the forensic product and the case-related information needed to efficiently perform the work, there is another significant difference between most traditional forensic science and computer forensic science. Traditional forensic analysis can be controlled in the laboratory setting and can progress logically, incrementally, and in concert with widely accepted forensic practices. In comparison, computer forensic science is almost entirely technology and market driven, generally outside the laboratory setting, and the examinations present unique variations in almost every situation.

f. **Ignorance: -** What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected. Recent legislation makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data.

3. SOLUTION

a. Deciding How to Respond to An Attack: - In the event of a suspected attack on a computer system, the first step in preparing for the investigation is deciding how to respond to the attack. Your organization has a range of responses to consider, including:

- Doing nothing.
- Performing an analysis as fast as possible so that the compromised system can be repaired and put back into production, allowing business processes to resume.
- Performing as detailed an analysis as possible, properly collecting and preserving all evidence in anticipation of possible prosecution.

Your organization must decide its response on a case-by-case basis. However, this article makes the following recommends:

- Whenever possible, perform as detailed and comprehensive an investigation as possible.
- Your organization should assume that the information gathered during the investigation will, sometime in the future, need to be admitted as evidence in a court of law for the criminal prosecution of the person(s) participating in the attack.

Once your organization has decided on how to approach an investigation, investigators can take any of the following specific actions to conduct the investigation:

i. **Do Nothing: -** We do not consider this to be a viable option and strongly recommend any other approach instead. Nonetheless, this approach is taken more often than it should be, with victims of attacks hoping that attackers will get bored and go away. Many home users use this tactic, thinking they have no real value on their systems or wireless access points, thus they do not consider it much of an issue. The negative consequence to this approach is that your site might be used as a staging point to attack others. You might be the one who receives the knock on the door by the local police department with a search warrant because your system was used to stage attacks upon other systems. There might be legal ramifications that can leave your organization liable if one of its systems was, in fact, used for illegal purposes.

ii. **Reinstall and Move On: -** This approach is probably the fastest way to recover from an incident with minimal interruption to system operations. Unfortunately, it has become the de facto way in which most computer incidents are handled. In this case, an organization just chalks up the intrusion to the cost of doing business, reinstalls the OS, and gets the system back into production as soon as possible. Often, little or no negative publicity about the incident becomes public. The negative consequence of this approach is that it emboldens attackers. They might attack again, and one cannot be certain to have closed all the holes. Intruders often leave backdoors that are removed by reinstalling the OS. However, most often, during the initial break in an attacker will gather and retain enough information about your organization to be able to attack more efficiently again. For example, attackers might have already sniffed or cracked passwords that will allow them back into your systems. Without knowing for certain which initial security failure(s) allowed them access the first time, one cannot be sure to have closed all access points.

iii. **Investigate for Yourself: -** The positive aspect of this approach is that no outsider needs to be contacted. Depending on the level of expertise that is available from in-house resources, your organization might be able to complete the investigation in a timely and efficient manner. The downside of this approach is that, even if the investigation is successful, others do not know about the attack scenario and do not benefit from the results of the investigation.

iv. **Call for Help: -** Calling for outside help is the most practical of the four options, and it is the approach that we recommend for most scenarios. Many sites are not able to have an onsite specialist who knows computer forensic methodology. Computer forensics is a discipline that can take years to really understand intimately. It can be a daunting task to know all of the different techniques required to perform an investigation on all of the different types of operating systems.

Bringing in a trustworthy confidential investigator, when needed, might be less expensive than trying to keep a resident expert on the payroll (assuming that your system is not broken into on a regular basis). A hired consultant who knows computer forensic techniques will often be able to detect, isolate, and help your organization recover from attacks in a timely manner.

Certification of computer forensic investigators is a trend that is underway but still developing. If possible, hire a certified computer security forensic investigator. As of the writing of this article, few certification programs exist for computer forensic investigators, so finding a certified investigator might prove difficult.

Seeking bids for this type of consulting service just after an attack has occurred is not the right time to do so. When an attack has occurred, time is very important—both for the investigation, as well as for the recovery from the incident.

b. **DNA Examination: -** Forensic science disciplines have affected countless criminal investigations dramatically and have provided compelling testimony in scores of trials. To enhance objectivity and to minimize the perception of bias, forensic science traditionally has remained at arms length from much of the actual investigation. It uses only those specific details from the investigation that are necessary for the examination. These details might include possible sources of contamination at the crime scene or fingerprints of individuals not related to the investigation who have touched the evidence. Forensic science relies on the ability of the scientists to produce a report based on the objective results of a scientific examination. The actual overall case may play a small part in the examination process. As a case in point, a DNA examination in a rape case can be conducted without knowledge of the victim's name, the subject, or the specific circumstances of the crime.

c. **Forensic Results: -** Forensic science has historically produced results that have been judged to be both valid and reliable. For example, DNA analysis attempts to develop specific identifying information relative to an individual. To support their conclusions, forensic DNA scientists have gathered extensive statistical data on the DNA profiles from which they base their conclusions. Computer forensic science, by comparison, extracts or produces information. The purpose of the computer examination is to find information related to the case. To support the results of a computer forensic examination, procedures are needed to ensure that only the information exists on the computer storage media, unaltered by the examination process. Unlike forensic DNA analysis or other forensic disciplines, computer forensic science makes no interpretive statement as to the accuracy, reliability, or discriminating power of the actual data or information.

Beyond the forensic product and the case-related information needed to efficiently perform the work, there is another significant difference between most traditional forensic science and computer forensic science. Traditional forensic analysis can be controlled in the laboratory setting and can progress logically, incrementally, and in concert with widely accepted forensic practices. In comparison, computer forensic science is almost entirely technology and market driven, generally outside the laboratory setting, and the examinations present unique variations in almost every situation.

d. **Common Goals: -** These dissimilarities aside, both the scientific conclusions of traditional forensic analyses and the information of computer forensic science are distinctive forensic examinations. They share all the legal and good laboratory practice requirements of traditional forensic sciences in general. They both will be presented in court in adversarial and sometimes very probing proceedings. Both must produce valid and reliable results from state-of-the-art procedures that are detailed, documented, and peer-reviewed and from protocols acceptable to the relevant scientific community (ASCLD/LAB 1994).

As laboratories begin to examine more computer-related evidence, they must establish policies regarding computer forensic examinations and, from these policies, develop protocols and procedures. The policies should reflect the broad, community-wide goal of providing valid and reproducible results, even though the submissions may come from diverse sources and present novel examination issues. As the laboratory moves from the policy statement to protocol development, each individual procedure must be well-documented and sufficiently robust to withstand challenges to both the results and methodology.

However, computer forensic science, unlike some of its traditional forensic counterparts, cannot rely on receiving similar evidence in every submission. For instance, DNA from any source, once cleared of contaminants and reduced to its elemental form, is generic. From that point, the protocols for forensic DNA analysis may be applied similarly to all submissions. The criminal justice system has come to expect a valid and reliable result using those DNA protocols. For the following reasons, computer forensic science can rarely expect these same elements of standardized repetitive testing in many of its submissions:

- Operating systems, which define what a computer is and how it works, vary among manufacturers. For example, techniques developed for a personal computer using the Disk Operating System (DOS) environment may not correspond to operating systems such as UNIX, which are multi-user environments.

- Applications programs are unique.

- Storage methods may be unique to both the device and the media.

Typical computer examinations must recognize the fast-changing and diverse world in which the computer forensic science examiner works.

e. **An envisioned forensic workforce: -** In the just-described scenario, people with different skills fill different roles. To form a reasonable computer forensics education, we must identify the skills and positions such an educational program will fill. Many communities are interested in computer forensics:

- Law enforcement organizations need to train officers and administrators.
- Industry needs professionals with computer forensic competence as well as specialized computer forensics technicians.
- Academia needs personnel that can teach existing computer forensic techniques and research and validate new ones.

Recognizing the needs of the wider legal community is also important: judges, prosecutors, and defense lawyers might not want to learn about forensic computing in detail, but they'd certainly like to be able to understand and evaluate its results. Law enforcement personnel are classic just-in-time learners who prize immediate practical application, especially if it leads to a more efficient investigative process. Regardless of how technically educated law enforcement professionals are, they rely on human factors in their investigations — a videotaped confession is far more convincing to a jury than the most elegant technical explanation as to why someone is guilty. Four forensic positions represent a reasonable approach to developing a forensics curriculum. These positions represent a logical partitioning of the workforce, not the existing body of knowledge relevant to computer forensics. Our view of these positions was influenced in part by the US National Security Agency's information assurance workforce development programs.

f. **Importance: -** Adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure. You can help your organization if you consider computer forensics as a new basic element in what is known as a "defense-in-depth" approach to network and computer security.

For instance, understanding the legal and technical aspects of computer forensics will help you capture vital information if your network is compromised and will help you prosecute the case if the intruder is caught.

Computer forensics is also important because it can save your organization money. Many managers are allocating a greater portion of their information technology budgets for computer and network security. International Data Corporation (IDC) reported that the market for intrusion-detection and vulnerability-assessment software will reach 1.45 billion dollars in 2006. In increasing numbers, organizations are deploying network security devices such as intrusion detection systems (IDS), firewalls, proxies, and the like, which all report on the security status of networks. From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

g. **Recovery: -** System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

4. METHODOLOGY USED

The basic methodology consists of what you can think of as the three A’s:

- Acquire the evidence without altering or damaging the original.
- Authenticate that your recovered evidence is the same as the originally seized data.
- Analyze the data without modifying it.

We expand on each of these three topics in the sections that follow; they are the framework of every forensic game plan. The details of your specific game plan will depend upon the circumstances and your goals, but the plan will always follow these same three steps.

There are many possible goals other than successful criminal prosecution. Sometimes forensics is conducted to determine the root cause of an event to ensure that it will not happen again. This goal is important—you have to fully understand the extent of your problem before you can be reasonably sure that it will not be exploited again. You also have to fully understand a problem before you know how to respond to it. A friend recently confided a story about unexpectedly finding a high-port telnet daemon. After removing it, he thought that he had removed the intruder and "resecured" his system, but two weeks later, he found the same unauthorized process running. If you do not conduct a complete analysis and find the entire extent of the compromise, it is only a matter of time before you have a bigger problem. It's kind of like termites, but worse—termites don't deliberately retaliate! In addition to helping us determine what happened, forensics can also address the question of who was responsible. Forensics are used in investigations internal to private organizations and, increasingly, by law enforcement during investigations of all sorts of illegal activity that isn't necessarily characterized as computer crime. Just a few short years ago, as members of an emergency response team, we assisted in a raid on a drug dealer's home. While the detectives were collecting anything that they thought had potential as evidence, we asked if they were going to seize the drug dealer's personal computer. The lead detective replied with certainty that they did not need it. Perhaps they didn't realize how rich a source of information a computer can be about its user's activities. This attitude is much less common today, although the need for law enforcement officers trained for digital investigations still far outweighs the supply. Most computer crime cases are not prosecuted, but we should still consider acceptability in a court of law as our standard for investigative practice. We can debate whether or not to pull the plug, or if we should use DOS/Windows or Linux for our analysis, but those are minor details. Our ultimate goal is to conduct our investigation in a manner that will stand up to legal scrutiny. Treat every case like a court case, and you will develop good investigative habits. If your company has been lucky enough to avoid the need for computer forensics (or so you think), congratulations; it will come soon enough. What do you do when you are asked to investigate an incident, but your management wants the server reloaded and backed up as soon as possible? Do you tell the boss that you need several hours, if not several days, to analyze the system? Instead, you end up performing a watered-down version of forensics, and your results reflect the effort. Even under less-than-ideal circumstances, whatever level of rigor you can apply to the investigation will bear some fruit, and maybe it will convince your boss to give you more leeway during future events.

a. **Forensic process: -** Computer forensic investigations usually follow the standard digital forensic process (acquisition, analysis and reporting). Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices which, due to a lack of specialist tools, saw investigations commonly carried out on live data.

A portable Tableau write-blocker attached to a Hard Drive

Techniques: - A number of techniques are used during computer forensics investigations.

- **Cross-drive analysis: -** A forensic technique that correlates information found on multiple hard drives. The process, which is still being researched, can be used for identifying social networks and for performing anomaly detection.

- **Live analysis: -** The examination of computers from within the operating system using custom forensics or existing system administration tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

- **Deleted files: -** A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always delete physical file data, allowing it to be reconstructed from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

ii. Volatile data: - When seizing evidence, if the machine is still active, any information stored solely in **RAM** that is not recovered before powering down may be lost. One application of "live analysis" is to recover RAM data (for example, using Microsoft's **COFEE** tool) prior to removing an exhibit.

RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate. The length of time for which data recovery is possible is increased by low temperatures and higher cell voltages. Holding unpowered RAM below −60 °C will help preserve the residual data by an order of magnitude, thus improving the chances of successful recovery. However, it can be impractical to do this during a field examination.

Analysis tools: - A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review.

b. Methodology for an Investigator: - The application of science and education to computer related crime forensics is still largely limited to law enforcement organizations. Building a suitable workforce development program could support the rapidly growing field of computer and network forensics. We propose some generic requirements, resources, and pedagogical approaches for developing and implementing a forensics program in higher education. We don’t expect our results to be implemented directly, but we do intend them to stimulate thoughtful discussion, as did the workshop at which many of these ideas originated (the Center for Secure and Dependable Software Forensics Workshop held at the University of Idaho, 23–25 September 2002). Forensic investigation methodology is basically the approach that an investigator follows to retrieve possible evidence that may exit on a subject’s computer system. For e.g., the following steps should be taken:-

- Shut Down the Computer
- Document the Hardware Configuration of The System
- Transport the Computer System to A Secure Location
- Make Bit Stream Backups of Hard Disks and Floppy Disks
- Mathematically Authenticate Data on All Storage Devices
- Document the System Date and Time
- Make a List of Key Search Words
- Evaluate the Windows Swap File
- Evaluate File Slack
- Evaluate Unallocated Space (Erased Files)
- Search Files, File Slack and Unallocated Space for Key Words
- Document File Names, Dates and Times
- Identify File, Program and Storage Anomalies
- Evaluate Program Functionality
- Document Your Findings

5. CONCLUSION

Reporting of economic and cyber crime is problematic and grossly underestimated, as is estimated from the many risk associated with corporations in reporting or sharing fraud losses and activity. A uniform computer forensics crime reporting system should be developed that includes economic crimes.

The computer forensic needs and challenges can be accomplished only with the cooperation of the private, public, and international sectors. All stakeholders must be more willing to exchange information on the effect economic and cyber crime has on them and the methods they are using to detect and prevent it.

Valid and reliable methods to recover data from computers seized as evidence in criminal investigations are becoming fundamental for law enforcement agencies worldwide. These methods must be technologically robust to ensure that all probative information is recovered. They must also be legally defensible to ensure that nothing in the original evidence was altered and that no data was added to or deleted from the original. The forensic discipline of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media is computer forensic science.

This article examined issues surrounding the need to develop laboratory protocols for computer forensic science that meet critical technological and legal goals. Computer forensic scientists need to develop ongoing relationships with the criminal justice agencies they serve. The reasons for these relationships include the following:

- In their efforts to minimize the amount of data that must be recovered and to make their examinations more efficient and effective, computer forensic scientists must have specific knowledge of investigative details. This is a clear requirement that is generally more demanding than traditional forensic science requests, and it places more reliance on case information.

- Courts are requiring that more information rather than equipment be seized. This requires cooperative efforts between law enforcement officers and the computer forensic scientist to ensure that the technical resources necessary for the execution of the search warrant are sufficient to address both the scope and complexity of the search.

- Computers may logically contain both information identified in the warrant as well as information that may be constitutionally protected. Developing computer examination protocols for forensic computer analysis is unique for several reasons:

Unlike some traditional forensic analyses that attempt to gather as much information as possible from an evidence sample, computer forensic analysis attempts to recover only probative information from a large volume of generally heterogeneous information.

- Computer forensic science must take into account the reality that computer forensic science is primarily market driven, and the science must adapt quickly to new products and innovations with valid and reliable examination and analysis techniques.

- The work product of computer forensic science examinations also differs from most traditional forensic work products. Computer forensic science generally makes no interpretive statement as to the accuracy or reliability of the information obtained and normally renders only the information recovered.

6. REFERENCES

1. A Yasinsac; RF Erbacher, DG Marks, MM Pollitt (2003). "Computer forensics education". IEEE Security & Privacy.
2. Michael G. Noblett; Mark M. Pollitt, Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence".
3. P. Sommer, “Intrusion Detection Systems as Evidence,” *Computer Networks*, vol. 31, nos. 23–24, 1999, pp. 2477–2487.
4. K. Rosenblatt, “*High Technology Crime”*, KSK Publications, 1995.
5. D. Icove, K. Seger, and S. VonStorch, “*Computer Crime: A Crimefighter’s Handbook”*, O’Reilly & Associates, 1995.
6. R. McKemmish, “What Is Forensic Computing,” *Trends and Issues in Crime and Criminal Justice*, no. 118, Australian Inst. of Criminology; www.aic.gov.au/publications/tandi/index3.html.
7. C.E. Irvine, S.-K. Chin, and D.A. Frincke, “Integrating Security into the Curriculum,” *Computer*, vol. 31, no. 12, 1998, pp. 25–30.
8. C.E. Irvine, “Amplifying Security Education in the Laboratory,” *Proc. 1st World Conf. Information Security Education* (IFIP TCII WC 11.8), 1999, pp. 139–146.
9. A. Yasinsac, “Information Security Curricula in Computer Science Departments: Theory and Practice,” *5th Nat’l Colloquium Information Systems Security Education 2001: A Security Odyssey*, NCISSE Colloquium Press, 2001.

10. A. Yasinsac, J. Frazier, and M. Bogdonav, “Developing an Academic Security Laboratory,” *Proc. 6th Nat’l Colloquium Information Systems Security Education*, NCISSE Colloquium Press, 2002.

11. J.E. Anderson and P.H. Schwager, “Security in the Information Systems Curriculum: Identification & Status of Relevant Issues,” *J. Computer Information Systems*, vol. 32, no. 3, 2002, pp. 16–24.

12. G. Shpantzer and T. Ipsen, “Law Enforcement Challenges in Digital Forensics,” *Proc. 6th Nat’l Colloquium Information Systems Security Education*, NCISSE Colloquium Press, 2002.

13. S.L. Garfinkel and A. Shelat, “Remembrance of Data Passed: A Study of Disk Sanitization Practices,” *IEEE Security & Privacy*, vol. 1, no. 1, 2003, pp. 17–27.

14. Y. Manzano and A. Yasinsac, “Policies to Enhance Computer and Network Forensics,” *Proc. 2nd Ann. IEEE Systems, Man, and Cybernetics Information Assurance Workshop*, IEEE CS Press, 2001, pp. 289–295.

15. Noblett, M. G. Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. In: *Proceedings of the 11th INTERPOL Forensic Science Symposium*, Lyon, France. The Forensic Sciences Foundation Press, Boulder, Colorado, 1995.

16. Pollitt, M. The Federal Bureau of Investigation report on computer evidence and forensics. In: *Proceedings of the 12th INTERPOL Forensic Science Symposium*, Lyon, France. The Forensic Sciences Foundation Press, Boulder, Colorado, 1998.

17. Michael G. Noblett; Mark M. Pollitt, Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence". Retrieved 26 July 2010.

18. Warren G. Kruse; Jay G. Heiser (2002). “*Computer forensics: incident response essentials*.” Addison-Wesley. pp. 392. ISBN 0201707195. Retrieved 6 December 2010.

19. Casey, Eoghan (2004). “*Digital Evidence and Computer Crime, Second Edition*.” Elsevier. ISBN 0-12-163104-4.

20. Eoghan Casey. ed. “*Handbook of Digital Forensics and Investigation*”. Academic Press. pp. 567. ISBN 0123742676. Retrieved 27 August 2010.