1. COMPUTER FORENSICS FUNDAMENTALS

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, USB, 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. Far more information is retained on a computer than most people realize. It’s also more difficult to completely remove information than is generally thought. For these reasons (and many more), computer forensics can often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted.

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.

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. In both cases, those traces can prove to be the smoking gun that successfully wins a court case. Thus, computer data evidence is quickly becoming a reliable and essential form of evidence that should not be overlooked.

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

- Data seizure
- Data duplication and preservation
- Data recovery
- Document searches
- Media conversion
- Expert witness services
g. Computer evidence service options
h. Other miscellaneous services

STEPS TAKEN BY COMPUTER FORENSICS SPECIALISTS
The computer forensics specialist needs to complete an Evidence Identification and Retrieval Checklist. 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.

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

Problems with Computer Forensic Evidence
Computer evidence is like any other evidence. It must be
  • Authentic
  • Accurate
  • Complete
  • Convincing to juries
  • In conformity with common law and legislative rules (i.e. admissible)

There are also special problems:
  • Computer data changes moment by moment.
  • Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.
  • The process of collecting computer data may change it—in significant ways.
  • The processes of opening a file or printing it out are not always neutral.
  • Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long.
2 TYPES OF COMPUTER FORENSIC TECHNOLOGY

Two distinct components exist in the emerging field of cyber forensics technology. The first, computer forensics, deals with gathering evidence from computer media seized at the crime scene. Principal concerns with computer forensics involve storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes. Several computer forensic tools are available to investigators.

The second component, network forensics, is a more technically challenging aspect of cyber forensics. It involves gathering digital evidence that is distributed across large-scale, complex networks. Often this evidence is transient in nature and is not preserved within permanent storage media.

Network forensics deals primarily with in-depth analysis of computer network intrusion evidence, because current commercial intrusion analysis tools are inadequate to deal with today’s networked, distributed environments. Similar to traditional medical forensics, such as pathology, today’s computer forensics is generally performed postmortem (after the crime or event occurred). In a networked, distributed environment, it is imperative to perform forensic-like examinations of victim information systems on an almost continuous basis, in addition to traditional postmortem forensic analysis.

Types of Law Enforcement: Computer Forensic Technology

As previously defined, computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data). Often the computer evidence was created transparently by the computer’s operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related computer evidence.

Computer forensics tools and techniques have proven to be a valuable resource for law enforcement in the identification of leads and in the processing of computer related evidence. Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management.

Forensic software tools and methods can be used to identify passwords, logons, and other information that is automatically dumped from the computer memory as a transparent operation of today’s popular personal computer operating systems. Such computer forensic software tools can also be used to identify backdated files and to tie a disc to the computer that created it.

Types of Business Computer Forensic Technology

The following are types of business computer forensics technology:
a. Remote monitoring of target computers
b. Creating trackable electronic documents
c. Theft recovery software for laptops and PCs
d. Basic forensic tools and techniques
e. Forensic services available

a) Remote Monitoring of Target Computers
Data Interception by Remote Transmission (DIRT) from Codex Data Systems (CDS), Inc. is a powerful remote-control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center. No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

b) Creating Trackable Electronic Documents
There are so many powerful intrusion detection tools that allow the user to create trackable electronic documents that it is beyond our scope.

In general, most of these tools identify (including their location) unauthorized intruders who access, download, and view these tagged documents. The tools also allow security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.

c) Theft Recovery Software for Laptops and PCs
If your PC or laptop is stolen, is it smart enough to tell you where it is? According to an FBI report, 98% of stolen computers are never recovered. About 72% of the Fortune 1000 companies experienced laptop theft losses to computer component theft cost corporate America over $11 billion a year. So if your company experiences computer-related thefts and you do nothing to correct the problem, there is a 92% chance you will be hit again.

d) Basic Forensic Tools and Techniques
Today, many computer forensics workshops have been created to familiarize investigators and security personnel with the basic techniques and tools necessary for a successful investigation of Internet and computer-related crimes. Workshop topics normally include: types of computer crime, cyber law basics, tracing email to its source, digital evidence acquisition, cracking passwords, monitoring computers remotely, tracking online activity, finding and recovering hidden and deleted data, locating stolen computers, creating trackable files, identifying software pirates, and so on.

e) Forensic Services Available
Through computer forensic evidence acquisition services, forensic experts for companies like Capitol Digital Document Solutions can provide management with a potent arsenal of digital tools at its disposal. They have the necessary software and hardware to travel to designated sites throughout the world to acquire an exact image of hard drives, USBs, etc. This image is an exact duplication of the source media and
allows evaluation within their laboratories with minimal disruption to others. Services include but are not limited to

- Lost password and file recovery
- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision
- Remote PC and network monitoring
- Tracking and location of stolen electronic files
- Honeypot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses.

SPECIALIZED FORENSICS TECHNIQUES

Threats to the strategic value of your business almost always involve a computer or network because that is where your company’s proprietary information and business processes are located.

A simple and virtually undetectable fraud that posts a few cents to a phony account can reap a perpetrator thousands of dollars flowing through accounts payable.

A malicious change to an individual’s personnel records could cost the person a job and a career. Divulging a company’s financial records could damage it on Wall Street, in the marketplace, and before shareholders.

Corporate espionage can steal trade secrets. Posting libelous information on the Internet about a company or individual can damage a reputation beyond recovery.

Employees of a company might be stealing from it or using company resources to work for themselves, or they can be using excessive work time to surf pornographic sites and play games.

Computer forensics investigators examine computer hardware and 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 law enforcement authorities.

Computer forensics examiners should be called in when a threat to a company’s business and reputation is serious. Any organization that does not have a way to detect and stop malicious behavior can be victimized with no legal recourse.

The relationship between the computer and an event under inquiry is critical, and sometimes until a forensics examination has been done, one cannot know whether a computer was a significant part of an event or not.
Hidden Data and How to Find It
As if you didn’t have enough to worry about, today’s technology presents your business with as many problems as it does solutions. Computers that work miracles in your day-to-day operations often malfunction—and you lose valuable data. The email that makes communicating so simple, carries deadly viruses that infect your machines and spread, causing massive data losses throughout your network. Hackers, both inside and outside your company, can access your information, manipulate it, hide it, steal it, and cause huge losses of data.

In many cases, documents and files deleted from a computer can be found and recovered using the methods of computer forensics. When files or documents are deleted from a computer, the majority of the actual information is typically left behind. Although the user may think the deleted document has been eradicated, this is usually not the case. Documents and files deleted or hidden even years ago may be recovered through a computer investigation. Deleted or hidden files are one of the prime targets of the computer forensic technician searching for evidence.

Spyware and Adware
Spyware is Internet jargon for advertising supported software (adware). It is a way for shareware authors to make money from a product, other than by selling it to the users. There are several large media companies that approach shareware authors to place banner ads in their products in exchange for a portion of the revenue from banner sales.

Encryption Methods and Vulnerabilities
The use of encryption provides a different kind of challenge for the forensic investigator. Here, data recovery is only half the story, with the task of decryption providing a potentially greater obstacle to be overcome. Encryption, whether built into an application or provided by a separate software package, comes in different types and strengths.

Some of the most commonly used applications provide encryption protected by passwords that can be readily defeated by investigators with the right tools and the time to use them. Other types of encryption, readily available to the general public, can be configured and used to create encrypted data that goes beyond the ability of the professional investigator to decrypt it using software. Nevertheless, in these cases it may still be possible to decrypt data by widening the scope of the investigation to include intelligence sources beyond the computer under investigation. For example, public key encryption can be used to create highly secure, encrypted data. To decrypt data encrypted in this fashion, a private key and passphrase is needed. The private key may be found on the suspect’s machine or backed up to removable media.
The Fallacies of Encryption and Password Protection
How serious is the problem? Very. If a snoop can gain physical access to your computer where you store your secret key, he can modify it and wait for you to use it. When you do, he or she is secretly notified. From that point on, he has access to the rest of your encrypted personal information and you never know it. In effect, the snoop bypasses a user’s password and bypasses the effects of encryption entirely.

In this instance, the protection offered by encryption is illusory. Likewise, if a hacker can electronically break into your computer, and you have your secret key stored there, the security of your digital signature or your encrypted files is worthless.

INTERNET TRACKING METHODS
If an email comes from a real, valid email account and you want to know who the person behind that email account is, then you most likely will need to serve the Internet provider who is hosting that email account a court-order. Another idea would be to take that email address and search for it on the Web and use net. Who knows, he might have posted somewhere with his real name and address.

Sometimes people might send you information or hate mail from a fake address. This can be done quite easily by simply changing the Sender and Return-to fields to something different. You can do this, since these fields (your identity), are normally not checked by the mail server when you send mail, but only when you receive mail.

AVOIDING PITFALLS WITH FIREWALLS
All the traffic going through a firewall is part of a connection. A connection consists of the pair of IP addresses that are talking to each other, as well a pair of port numbers that identify the protocol or service. The destination port number of the first packet often indicates the type of service being connected to. When a firewall blocks a connection, it will save the destination port number to its logfile. Here, description is made of some these port numbers as well as avoiding some of the pitfalls. Port numbers are divided into three ranges:

- The well-known ports are those from 0 through 1023. These are tightly bound to services, and usually traffic on this port clearly indicates the protocol for that service. For example, port 80 virtually always indicates HTTP traffic.
- The registered ports are those from 1024 through 49151. These are loosely bound to services, which means that while there are numerous services “bound” to these ports, these ports are likewise used for many other purposes that have nothing to do with the official server.
- The dynamic and private ports are those from 49152 through 65535. In theory, no service should be assigned to these ports.

You can also attempt to go back further in your logs, looking for all the decoy addresses or people from the same subnets. You will often see that the attacker has actually connected to you recently, while the decoyed addresses haven’t.
BIOMETRIC SECURITY SYSTEMS
The verification of individuals for computer forensics purposes is achieved using a recognized ID credential issued from a secure and effective identity confirmation process. A secure personal ID system design will include a complex set of decisions to select and put in place the appropriate policies and procedures, architecture, technology, and staff to deliver the desired level of security. A secure biometric ID system can provide individuals with trusted credentials for a wide range of applications— from enabling access to facilities or secure networks, to proving an individual’s rights to services, to conducting online transactions.

With the preceding in mind, biometric security systems for computer forensics purposes are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics.

Biometric technologies, when used with a well-designed ID system, can provide the means to ensure that an individual presenting a secure ID credential has the absolute right to use that credential. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology.

Finally, in an ID system that combines smart card and biometric technologies for computer forensics proposes to verify the identity of individuals, a “live” biometric image (scan of a fingerprint or hand geometry) is captured at the point of interaction and compared to a stored biometric image that was captured when the individual enrolled in the ID system. Smart cards provide the secure, convenient, and cost-effective ID technology that stores the enrolled biometric template and compares it to the live biometric template. A secure ID system using smart card and biometric technology provides:

- Enhanced privacy, securing information on the card, allowing the individual to control access to that information, and removing the need for central database access during identity verification
- Improved security, protecting information and processes within the ID system and actively authenticating the trust level of the environment before releasing information
- Improved ID system performance and availability through local information processing and contactless ID card and reader implementations
- Improved system return on investment through the flexibility and upgradability that smart cards provide, allowing support of different authentication methods Band multiple, evolving applications.
3. TYPES OF COMPUTER FORENSIC SYSTEMS

Computer forensics has become a buzz word in today’s world of increased concern for security. It seems that any product that can remotely be tied to network or computer security is quickly labeled as a “forensics” system. This phenomenon makes designing clear incident response plans and corporate security plans that support computer forensics difficult. Today’s corporate climate of increased competition, cutbacks and layoffs, and outsourcing makes it essential that corporate security policy and practices support the inevitability of future litigation.

This is intended to raise awareness of the different types of computer forensics systems and to identify crucial questions for corporate planning in support of computer forensics.

The following are computer forensics systems:
1. Internet security systems
2. Intrusion detection systems
3. Firewall security systems
4. Storage area network security systems
5. Network disaster recovery systems
6. Public key infrastructure security systems
7. Wireless network security systems
8. Satellite encryption security systems
9. Instant messaging (IM) security systems
10. Net privacy systems
11. Identity management security systems
12. Identity theft prevention systems
13. Biometric security systems
14. Homeland security systems

1. INTERNET SECURITY SYSTEMS
Internet and network security are topics that many executives and managers avoid talking about. Many feel that discussing their security implementations and policies will cause their companies to become vulnerable to attack. This lack of dialog has resulted in some executives not being fully aware of the many advances and innovations in security technology that enable companies to confidently take full advantage of the benefits and capabilities of the Internet and intranets.

Ironically, Internet security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions to security problems of employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone.

2. INTRUSION DETECTION SYSTEMS
Intrusion detection systems help computer systems prepare for and deal with attacks.
They collect information from a variety of vantage points within computer systems and networks and analyze this information for symptoms of security problems. Vulnerability assessment systems check systems and networks for system problems and configuration errors that represent security vulnerabilities. Both intrusion detection and vulnerability assessment technologies allow organizations to protect themselves from losses associated with network security problems.

**Intrusion Detection Defined**

Intrusion detection systems help computer systems prepare for and deal with attacks. They accomplish this goal by collecting information from a variety of system and network sources and then analyzing the information for symptoms of security problems.

In some cases, intrusion detection systems allow the user to specify real-time responses to the violations. Intrusion detection systems perform a variety of functions:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis of abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations.

Some systems provide additional features, including

- Automatic installation of vendor-provided software patches
- Installation and operation of decoy servers to record information about intruders.

The combination of these features allows system managers to more easily handle the monitoring, audit, and assessment of their systems and networks.

**Vulnerability Assessment and Intrusion Detection**

Vulnerability assessment products (also known as scanners) perform rigorous examinations of systems in order to determine weaknesses that might allow security violations. These products use two strategies for performing these examinations. First, passive, host-based mechanisms inspect system configuration files for unwise settings, system password files for weak passwords, and other system objects for security policy violations. These checks are followed, in most cases, by active, network-based assessment, which reenacts common intrusion scripts, recording system responses to the scripts.

The results of vulnerability assessment tools represent a snapshot of system security at a point in time. Although these systems cannot reliably detect an attack in progress, they can determine that an attack is possible, and furthermore, they can sometimes determine that an attack has occurred. Because they offer benefits that
are similar to those provided by intrusion detection systems, they are included in the sphere of intrusion detection technologies and products.

The objective of intrusion detection and vulnerability assessment is to make complex, tedious, and sometimes virtually impossible system security management functions possible for those who are not security experts. Products are therefore designed with user-friendly interfaces that assist system administrators in their installation, configuration, and use. Most products include information about the problems they discover, including how to correct these problems, and provide valuable guidance for those who need to improve their security skills. Many vendors provide consulting and integration services to assist customers in successfully using their products to achieve their security goals.

**Network Security Management**

Network security management is a process in which one establishes and maintains policies, procedures, and practices required for protecting networked information system assets. Intrusion detection and vulnerability assessment products provide capabilities needed as part of sound network security management practice.

### 3. FIREWALL SECURITY SYSTEMS

Today, when an organization connects its private network to the Internet, security has to be one of primary concerns. In the past, before the widespread interest in the Internet, most network administrators were concerned about attacks on their networks from within, perhaps from disgruntled workers. For most organizations now connecting to the Internet and big business and big money moving toward electronic commerce at warp speed, the motive for mischief from outside is growing rapidly and creating a major security risk to enterprise networks.

The threat of attack on your network increases proportionally with the continued exponential growth of the Internet. If it is necessary for you to connect your network to the Internet, an appropriate security protocol should be decided on and implemented. This book illustrates many reasons why this is necessary, as well as many techniques to consider for your firewall solution. The bottom line is, do not connect your network to the Internet without some sort of protection.

Also, do not put sensitive information in a place where it can be accessed over the Internet. The firewall you decide to use will prevent most of the attacks on your network; however, firewalls will not protect against dial-in modem attacks, virus attacks, or attacks from within your company. Nevertheless, a number of the security problems with the Internet can be remedied or made less serious through the use of existing and well-known techniques and controls for host security. A firewall can significantly improve the level of site security while at the same time permitting access to vital Internet services.

**Firewall Defined**
A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that blocks traffic and one that permits traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy.

A firewall can also provide audit and alarm mechanisms that will allow you to keep a record of all access attempts to and from your network, as well as a real-time notification of things that you determine to be important.

Perhaps it is best to describe first what a firewall is not: a firewall is not simply a router, host system, or collection of systems that provides security to a network. Rather, a firewall is an approach to security; it helps implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network (a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

The Reason for Firewalls
The general reasoning behind firewall usage is that without a firewall, a subnet’s systems are exposed to inherently insecure services such as Network File System (NFS) or Network Information Service (NIS) and to probes and attacks from hosts elsewhere on the network.
In a firewall-less environment, network security relies totally on host security, and all hosts must, in a sense, cooperate to achieve a uniformly high level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break-ins occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords.

The Need for Firewalls
As technology has advanced to greatly expand the information technology systems capabilities of corporations, the threats to these systems have become numerous and complex. In today’s world, corporations face a variety of information system attacks against their local area networks (LANs) and wide area networks (WANs). Many of these attacks are directed through the Internet. These attacks come from three basic groups:
- Persons who see attacking a corporation’s information system as a technological challenge
- Persons with no identified political or social agenda who see attacking a corporation’s information system as an opportunity for high-tech vandalism
• Persons associated with a corporate competitor or political adversary who see the corporation’s information system as a legitimate strategic target

To combat this growing and complex threat to a corporation’s LAN and Internet site, a series of protective countermeasures needs to be developed, continually updated, and improved. Security services that are important to protecting a corporation’s strategic information include:

a) **Data Integrity**: Absolute verification that data has not been modified
b) **Confidentiality**: Privacy with encryption, scrambled text
c) **Authentication**: Verification of originator on contract
d) **Non-Repudiation**: Undeniable proof-of-participation
e) **Availability**: Assurance of service demand

**Benefits of Firewalls**
The following are the primary benefits of using a firewall:
- a) Protection from vulnerable services
- b) Controlled access to site systems
- c) Concentrated security
- d) Enhanced privacy
- e) Logging and statistics on network use and misuse
- f) Policy enforcement

**Limitations of Firewalls**
Firewalls can’t protect against attacks that don’t go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Many organizations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected.

Another thing a firewall can’t protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he or she is just as likely to export it through a telephone, fax machine, or USB.

A firewall opens communications channels between two networks and has no control over what users choose to transmit using these channels. It has no concept of the value or sensitivity of the data it is transferring between networks and therefore cannot protect information on that basis. A firewall cannot control what a user chooses to do with the data once he has received it. If a user chooses to modify or propagate that information, the firewall has no effect.

A firewall cannot completely protect your systems from data driven attacks such as viruses.

**4. STORAGE AREA NETWORK SECURITY SYSTEMS**
In the aftermath of the devastation that occurred when the World Trade Center collapsed, disaster recovery services used storage area networks (SANs) to restore thousands of terabytes of business data and get hundreds of companies running. As distasteful as the idea might be, with disaster comes opportunity, and the disasters of September 11, 2001, provided a good opportunity for storage networks to show their value by providing critically important business continuity. Rarely has technology demonstrated its value in a more demanding environment.

Today, organizations continue to expose their IT systems to a wide range of potential security threats as they continue to broaden their reach to business partners and customers around the globe. Furthermore, data theft, eavesdropping, fraud, and hacker attempts increasingly threaten secure electronic information exchange within the enterprise and across public networks (such as the Internet). Because IT systems are only as secure as the weakest link in the network, organizations need to consider outsourcing their data storage security needs to one vendor, which will help them develop a comprehensive security plan and architecture that helps ensure safe, reliable data processing throughout a SAN. In other words, an organization needs an integrated solution that addresses a wide variety of potential security threats—thus enabling a robust, mission-critical SAN infrastructure.

**SAN Benefits**

A SAN provides a perfect environment for clustering that can extend to dozens of servers and storage devices—all the while having redundant links in a fiber channel fabric. Servers will continue to function because their data is still available through the SAN, even if storage devices fail during an NDR.

- **Centralized Management**
  When a disk or controller fails in a direct-attached environment, redundant systems keep the redundant array of independent (or inexpensive) disks (RAID) array operating normally and generate an alarm. However, the redundant component may fail as well, bringing the system down if the failed component isn’t replaced quickly.

- **Scalability**
  A storage area network can lower acquisition and expansion costs, in addition to lowering management costs. Even as new servers, disk arrays, and disc subsystems are added, the SAN architecture supports access between all servers and all storage resources in the network. Without disrupting data access, customers can add storage resources and even servers online.

- **Reliability**
  A SAN is a network that resides between the host bus adapter and the storage device. This position inherently creates a critical point at the physical level, but by implementing multiple paths and redundant infrastructure devices, the SAN reduces or eliminates single points of failure. Because monitoring of the network is
much easier now, centralization facilitates more rigorous, consistent management practices and thus increases the overall reliability.

- **Performance**
  In application environments that depend on bulk data transfer (such as data warehousing and data-mining applications), maximum bandwidth is of particular interest. Backup and restore times can be shortened dramatically by the high channel speed and low latency obtained by using a SAN.

5. **NETWORK DISASTER RECOVERY SYSTEMS**
Network disaster recovery (NDR) is the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization’s critical business functions. NDR is not a new idea. In recent years, data has become a vitally important corporate asset essential to business continuity. A fundamental requirement of economic viability is the ability to recover crucial data quickly after a disaster.

Many companies see their disaster recovery efforts as being focused primarily on their IT departments. IT people are in the lead in sponsoring and managing their disaster recovery plans, and relatively few companies involve line-of-business staff and partners in designing and testing such plans at all. Not surprisingly, the person most frequently cited as being responsible for the management of an NDR plan is the company’s chief information officer (CIO) or another IT manager.

There's general agreement on what should be covered in an NDR plan. Network outages are the number-one issue for smaller companies and high on the list for larger companies. This puts a premium on reliable networking hardware and software. Natural disasters also ranked high. At the bottom of the list are attacks on company Web sites, employee-initiated outages, and service provider failures.

As for components that are or will be part of their NDR plan, larger businesses are more likely to perform or plan to perform a business impact analysis than smaller firms. However, most companies cite components such as a process for administering the NDR plan, setting out what individuals should do in the aftermath of a disaster, and recovery strategies.

6. **PUBLIC KEY INFRASTRUCTURE SYSTEMS**
To mitigate the security risks of conducting business in an open environment while at the same time maintaining the cost advantages of doing so, enterprises are turning their attention to an emerging segment of the security market known as public key infrastructure (PKI). The purpose of PKI is to provide an environment that addresses today’s business, legal, network, and security demands for trust and confidentiality in data transmission and storage. PKI accomplishes these goals for an enterprise through policy and technology components. These components determine and identify the
roles, responsibilities, constraints, range of use, and services available. This section briefly identifies the key concepts and issues surrounding the technologies and policies required to implement and support an enterprise PKI.

In other words, PKI is a system for supporting digital signatures and document encryption for an organization.

**PKI Defined**
A PKI enables users of an insecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The PKI provides for digital certificates that can identify individuals or organizations and directory services that can store and, when necessary, revoke them. PKI is the underlying technology that provides security for the secure sockets layer (SSL) and hypertext transfer protocol secure sockets (HTTPS) protocols, which are used extensively to conduct secure e-business over the Internet.

A PKI consists of
- A certificate authority that issues and verifies digital certificates
- A registration authority that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system

7. **WIRELESS NETWORK SECURITY SYSTEMS**
It’s an epidemic waiting to happen to many security experts. While most IT managers today have their hands full securing wired networks, their companies have been spending billions of dollars on wireless.

8. **SATELLITE ENCRYPTION SECURITY SYSTEMS**
The boom in satellite communications is changing the way we work and live, but it is becoming a security nightmare for those organizations and governments whose survival depends on the protection of intellectual property distribution, electronic commerce, electronic battlefields and national security. The ability to securely exchange information between billions of users around the globe involving perhaps trillions of transactions is vital to the continued growth and usefulness of satellite communications as well as the Internet and intranets. Encryption especially several layers of encryption on top of compressed data that is to be transmitted (via a highly directional microwave radio signal) to a satellite (uplink) from Earth and then transmitted down to Earth (downlink) and decrypted—can effectively solve the Internet’s confidentiality and authentication problems.

9. **INSTANT MESSAGING (IM) SECURITY SYSTEMS**
The security threats from IM are straightforward. Since deployment isn’t controlled, the enterprise can’t keep a rein on how the systems are used. With the public IM networks, the individual employee registers for service. If the employee leaves a company, the firm has no (technology-based) way to prevent him from continuing to use the account, or from continuing to represent himself as still working for the company. Furthermore, without additional tools, the company has no way of archiving IM messages for legal or regulatory purposes, or of monitoring and controlling the content of messages to filter for inappropriate communications.

There are the obvious holes that IM opens up on the corporate network. Each of the IM networks uses a well-known port that must either be left open on the corporate firewall to allow traffic in or closed, which, at least in theory, bans that service to end users.

10. NET PRIVACY SYSTEMS
The philosophical focus of a privacy management perspective is geared toward the improvement of the bottom line for private companies and cost control and resource optimization for nonprofit and government organizations. All types of organizations need to develop privacy policies that maximize the benefit of reusing information in as many ways as possible while minimizing the risks associated with potential privacy violations. Although this balance is essential in an information intensive world, it is clear that it is not going to be easy for organizations to achieve the balance between privacy and the optimization of resources.

11. IDENTITY MANAGEMENT SECURITY SYSTEMS
Identity management is the creation, management, and use of online, or digital, identities. Hundreds of millions of people around the world now use the Internet daily at home and at work, facing a multiplicity of corporate applications and e-business interfaces. Many such applications and interfaces require a unique user name, and as a result, an individual typically possesses not one but several digital identities.

Additionally, digital identities are not perpetual: they are created for new employees, and when those employees leave, their digital identity expires (or should expire) as of their termination date. An employee moving from one part of an organization to another—or being promoted to a higher management level—may need to have updated access rights and other information attached to his or her digital identity. Identity management is therefore also about being able to manage the full life cycle of a digital identity from creation and maintenance to termination, as well as enforce organizational policies regarding access to electronic resources. It is not simply the ability to store or provision digital identities. While these are critical capabilities, they are just two components of an overall solution.

The Challenges of Managing Digital Identities
The recent convergence of three events has created a sense of urgency around identity management.
• **Aggregation**
  There is an incalculable amount of content on the Internet. To help business and home users find the sites and services they want, corporate portals and content aggregators like Yahoo emerged.
  In the process of providing more content and services, these aggregators have developed relationships with users—including capturing their online identities.

  When a user accesses content and services through these aggregators, his or her digital identity is captured. In an enterprise environment, this provides valuable tracking of information; for Web sites, each captured identity is an asset they can leverage for their own—and their business partners’—marketing purposes.

• **Web Services**
  Web services are modular applications that enable the transformation from a software purchasing and physical ownership model to a software subscription or “rental” model with remote execution. Examples of Web services currently prevalent on the Internet include calendaring, supply chain management, customer relationship management, order fulfillment, sales force automation, music on demand, and instant messaging.
  A company can trust an employee’s identity more than that of an external partner or customer because the company has more control over the provisioning and maintenance of the employee’s identity. An identity management solution provides that trust as it confirms that a user is authenticated and authorized to access applications and services.

• **Online Partnerships**
  Many businesses are forging online partnerships with organizations that offer complementary services, both internally (to improve productivity) and externally (to expand their customer reach).

12. **IDENTITY THEFT PREVENTION SYSTEMS**
  Quite simply, identity theft is the appropriation of an individual’s personal information in order to impersonate that person in a legal sense. Stealing someone’s identity enables the thief to make a frightening number of financial and personal transactions in someone else’s name, leaving the victim responsible for what may turn out to be mind-boggling turmoil in his or her life.

  Identity theft is not new. It has been around for a long time. There was a time when an individual could flee his or her life, town, and mistakes and go somewhere far away pretending to be someone else—and, no one knew better. The ramifications of stealing someone’s identity did not have the far-reaching implications that they do today for the person whose identity is stolen. Those were the days before credit reporting and high-tech methods of tracking and sharing information were commonplace.
Identity theft can still be done by such low-tech means as knowing someone else’s basic identifying information and initiating personal transactions in that person’s name, but today, identities can also be stolen using highly technical and sophisticated means of obtaining the personal data of a stranger. However it is done, whether the identity thief uses high- or low-tech means of getting your personal information, an individual can become someone else very easily.

The difference today is that what an identity thief does as someone else reflects very quickly on the victim’s reputation. An individual’s life can be devastated by the loss of good name and the financial or personal mess that results.

Identity theft is always personal—after all, it is one’s own identity that is stolen! Someone literally assumes your identity and leaves a damaging trail of credit card abuse and exposed personal information all over the Internet (to your creditors and possibly worse). Thieves could be roommates, relatives, friends, estranged spouses, or household workers—with ready access to their victims’ personal papers.

How Identity Theft Is Done
In the course of a normal day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks, or apply for a credit card. You may do any of a hundred little things each of us does every day that involve someone knowing who we are.

The following are some of the ways imposters can get and use your personal information and take over your identity:

a. They steal wallets and purses containing your identification and credit and bank cards.
b. They steal your mail, including your bank and credit card statements, preapproved credit offers, telephone calling cards, and tax information.
c. They complete a change of address form to divert your mail to another location.
d. They rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”

13. **BIOMETRIC SECURITY SYSTEMS**
While a biometric is the actual characteristic or trait, a biometric system is the computer hardware and software used to recognize or verify an individual. Although there are many variations in how specific products and systems work, there are a number of common processing elements.

- **Collection**
As a first step, a system must collect or “capture” the biometric to be used. One essential difference between the various techniques is the characteristic (body part or function) being analyzed. Obviously, this will influence the method of capture. All biometric systems have some sort of collection mechanism. This could be a reader or
sensor upon which a person places his finger or hand, a camera that takes a picture of his face or eye, or software that captures the rhythm and speed of his typing.

In order to “enroll” in a system, an individual presents his “live” biometric a number of times so the system can build a composition or profile of his characteristic, allowing for slight variations (different degrees of pressure when he places his finger on the reader). Depending upon the purpose of the system, enrollment could also involve the collection of other personally identifiable information.

• Extraction
Commercially available biometric devices generally do not record full images of biometrics the way law enforcement agencies collect actual fingerprints. Instead, specific features of the biometric are “extracted.” Only certain attributes are collected (particular measurements of a fingerprint or pressure points of a signature).

Which parts are used depends upon the type of biometric, as well as the design of the proprietary system. This extracted information, sometimes called “raw data,” is converted into a mathematical code. Again, exactly how this is done varies among the different proprietary systems. This code is then stored as a “sample” or “template.” The specific configuration of a system will dictate what, how, and where that information is stored. Regardless of the variations, all biometric systems must create and retain a template of the biometric in order to recognize or verify the individual. While the raw data can be translated into a set of numbers for the template, commercial biometric systems are generally designed so that the code cannot be re-engineered or translated back into the extracted data or biometric.

• Comparison and Matching
To use a biometric system, the specific features of a person’s biometric characteristic are measured and captured each time he presents his “live” biometric. This extracted information is translated into a mathematical code using the same method that created the template. The new code created from the live scan is compared against a central database of templates in the case of a one-to-many match, or to a single stored template in the case of a one-to-one match. If it falls within a certain statistical range of values, the match is considered to be valid by the system.

14. HOMELAND SECURITY SYSTEMS

Homeland Security Defined
The terms homeland security and homeland defense have received increased attention since the tragic events of September 11, 2001. While these terms are relatively new, the concepts behind them are not. Homeland security is defined as the deterrence, prevention, and preemption of and defense against aggression targeted at U.S. territory, sovereignty, population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies.
Homeland defense on the other hand is a subset of homeland security. It is defined as the deterrence, prevention, and preemption of and defense against direct attacks aimed at U.S. territory, population, and infrastructure. In other words, you might consider homeland security to encompass policies, actions, and structures designed to protect the rights and freedoms inherent in the U.S. Constitution and homeland defense a subset of homeland security with policies, activities, and actions designed to defend against extra-territorial threats, including preemptive operations.

The Department of Homeland Security has the following organizational structure:

a. Border and transportation security
b. Emergency preparedness and response
c. Chemical, biological, radiological, and nuclear countermeasures
d. Information analysis and infrastructure protection
4. DIGITAL FORENSICS

WHAT IS DIGITAL FORENSICS?
The field of Digital Forensics is a young one and yet evolving so fast that practicing experts have to struggle to keep abreast of development in the field. The term is interchangeably used with Computer Forensics when broadly used. This may sometime be confusing to new entrants into the field who needed a clear demarcation between the two. When the chips are down indeed, Digital Forensics concerns with all electronic evidence matters while computer Forensics when clearly delineated limits to the electronic evidence that are from the computer and its peripheral units. There is no particular single accepted definition yet by stakeholders except that it is a methodology for producing electronic evidence that can be acceptable in court. It is a branch of Forensics Science and sometimes referred to as Digital Forensics Science.

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a scientific methodology of finding evidence from digital media like a computer, mobile phone, server, network, etc. It is the application of technology to law which solutions to complexities of cases requiring digital evidence.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices

ORIGIN OF DIGITAL FORENSICS
It originates from the individual efforts of law enforcement agents in the United States side by side with the personal computer revolution of the late 1970s and the early 1980s. The FBI took the lead through the 1980s as a reactionary measure to the evolution of business documentation of the professional drug cartels and organized crime from hard papers to soft copies in USB devices and compact disks. The developments in Digital Forensics were carried out by well-trained hobbyist which have largely been responsible for the late development of standards unlike other areas of Forensic Science which came out of the researches of the scientific communities. By the year 2000, national legal frameworks and government policies on Digital Forensics have become the way to go for many advanced nations. This resulted in many bodies and agencies publishing guidelines and standards to respond to the gaps created by absence of regulatory bodies and guidelines for practitioners. Today, nations are forging national policies to combat cyber and cyber related crimes as international organizations are showing up. Much is still expected to happen on the international scene towards common standards.

Period before legislation: Until the late 1970s in the USA, computer related crimes were treated under any related legislation. It continue to be so for many countries
until one after another each country began to have specialized law specifically prohibiting specific computer related crimes.

Some earlier global landmark information in Digital Forensics and that of Africa which though is more recent, is still very relevant for practitioners in the world. These are:

- First prohibition of computer crime in Florida Computer Crimes Act 1978 in the USA
- Francis Galton conducted first recorded study of fingerprints in 1982
- Computer legislation 1983 in Canada
- FBI launched Computer Analysis and Response Team in 1984
- The British Metropolitan Police Fraud Squad set up a Computer Crime Department in 1985
- Computer Fraud Abuse Act 1986 in USA
- Cliff Stoll investigated Markus Hess, a hacker in 1986, using Computer and Network Forensics (first documented use of Digital Forensics in a case)
- Australian Amendment to crimes Act 1989
- British Computer Misuse Act 1990
- Mobile Forensics began in the 1990s due to the increasing use of mobile devices and its implication for crime investigation
- In 1992, the term Computer Forensics was used in academic literature.
- The term “Computer Forensics was first used in an academic paper by Collier and S. Paul in 1992”
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- Britain set up the National Hi-Tech Crime Unit in 2001 to provide national infrastructure for computer crime. They operated in London and collaborated with other regional police forces
- The Scientific Working group on Digital Evidence (SWGDE) published the guideline titled “Best practices for Computer Forensics” in 2002
- A European lead international treaty in an attempt to reconcile national computer crime laws, investigative techniques and international co-operation, began the Convention on Cybercrime in 2004. The treaty has been signed by 43 nations which includes the US, Canada, Japan, South Africa, UK and other European nations while 16 nations have ratified it
- The ISO standard (ISO 17025, General requirements for the competence of testing and calibration laboratories) was published in 2005
- Set up Serious Organized Crime Agency (SOCA) 2006. It absolved the Hi-Tech Crime Unit
- In 2010, Simson Garfinkel identified issues facing digital investigations.
The opinion of a Digital Forensics expert on an electronic evidence is often required by the court in various types of cases whether criminal or civil. Cases involving, murder, cybercrimes, terrorism, money laundering, divorce, theft of proprietary document, contractual disputes among others are common areas that require Digital Forensics. The global statistics is that over 90% of successfully prosecuted cases globally use electronic evidence.

**TYPES OR BRANCHES OF DIGITAL FORENSICS**

The nature of cases requiring the services of a Digital Forensic Examiner is usually dependent on the devices and the nature of the evidence on which he is expected to conduct examination and analysis. Each of these have their own unique methodology for handling, examining and analyzing the evidence which need to be followed for the admissibility of the evidence in court. Digital Forensics investigation concerns with all breaches of a computer, small digital devices (e.g. tablets, smartphones, flash drives) and other electronic devices. Data retrieved from these devices are used to prove or disprove that a crime prohibited under the law has been breached. Digital Forensics investigation is branched into various types. The following are branches of Digital Forensics:

1. Computer Forensics
2. Network Forensics
3. Mobile Forensics
4. Forensics Data Analysis
5. Database Forensics
6. Malware Forensics
7. Email Forensics
8. Live Forensics
9. Questioned Document Examination
10. Forensic Graphology (Handwriting Analysis)
11. Vehicle Forensics
12. Steganalysis (Steganographic investigation)
13. Cryptographic investigation

1. **Computer Forensics:** When referring to computer Forensics as a branch of Digital Forensics, we are definitely focusing on the branch of Digital Forensics that concerns with the examination and analysis of electronic evidence that are directly taking from the computer device.

   Computer Forensics is also “the preservation, identification, extraction, interpretation, and documentation of computer evidence to include the rule of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was
found. We shall look deeper later into these terms when considering the Digital Forensics processes.

2. **Network Forensics**: Network Forensics is concerned with the monitoring and analysis of computer networks whether local or WAN/Internet. Data on intrusion detection and prevention are the target here. Although, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) log their activities and can be reached to understand intrusion activities within a particular period, most network information are volatile and therefore the detection and response usually targets real time. Successful Network Forensics is more reactionary than other areas of Digital Forensics. Wireless Forensics is a division of Network Forensics concerned mainly with offering needed tools to collect and analyze data from wireless network traffic.

3. **Mobile Forensics**: Mobile Forensics is a sub-branch of Digital Forensics relating to recovery of digital evidence or data from a mobile device. Mobile devices usually have inbuilt communication system (e.g. GSM) and proprietary storage mechanisms. The focus here is on data such as call logs, SMS, media files internet logs, deleted data, device location, SIM card information, etc.

4. **Forensics Data Analysis**: It is a branch of Digital Forensics that examines structured data with the purpose of discovering and analyzing patterns of fraudulent activities. Big data are maintained by businesses and governments and such databases are targets of financial and economic crimes.

5. **Database Forensics**: Database Forensics is the forensic study of databases and their metadata. Database contents, log files, data gotten from the device RAM and sometime recovered deleted information may be used to build a timeline or recover relevant information.

6. **Malware Forensics**: This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

7. **Email Forensics**: It deals with the recovery and analysis of emails, including deleted emails, calendars, and contacts. Here, the interest is usually the origin of the email and sometimes the contents may be the subject of the investigation.

8. **Live Forensics**: It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump. These is the investigation carried out on a computer when the system is still live. This is usually at the crime scene or when the target of the expert is for intelligence process.

9. **Questioned Document Examination**: The investigation carried out on a document whose origin, content, etc. is in dispute or of interest. Bid rigging, business document related dispute, suspected forgery or falsification cases, etc. are few of the situation requiring this type of analysis.
10. Forensic Graphology (Handwriting Analysis): The origin of the handwriting and signature on a document often becomes subject of investigation in business documents, ransom notes, will of a deceased, death threats, suicide notes, etc. This branch of Digital forensics concerns itself with these kind of investigating.

11. Vehicle Forensics: Location of a vehicle

12. Steganalysis (Steganographic investigation): The proliferation of steganography tools that enable users embed information in seemingly ordinary files have become a challenge to law enforcement in many investigations. Steganalysis therefore concerns with the investigations of such embedded files to identify crimes. Copyright issues, theft of proprietary documents, etc. are examples of areas of applicability of this skills.

13. Cryptographic investigation: Encryption and decryption of information are normal part of our communication in other to limit unauthorized access to such information. This tools and methodology are also available to criminals who use it to cover their tracks. Sometimes, the need to access an encrypted information from a computer may be key to solving a case.

**DIGITAL FORENSICS PROCESSES**

Typically, the Digital Forensics processes includes:

a. Seizures  
b. Imaging (Acquisition)  
c. Analysis  
d. Report Writing

This is in line with the model originally proposed by the United States of America’s Department of Justice. This model has four phases:

a. Collection  
b. Examination  
c. Analysis, and  
d. Reporting.

These processes are far from being exhaustive as we have seen in the definition of computer Forensics.

Digital Forensics investigation processes include the following:

a. Identification  
b. Seizures  
c. Preservation  
d. Extraction (Acquisition or Imaging)  
e. Interpretation (Analysis)  
f. Documentation  
g. Evidence Reporting  
h. Evidence Presentation
a. **Identification:** Identification is mostly accepted to be the first step in the forensic process. It includes what evidence is present, where it is stored, and in which format. Electronic storage media can be retrieved from personal computers or may be Mobile phones, PDAs, drives, notes, etc.

b. **Seizures:** Once evidence or items that is suspected to have probative value is identified at the crime scene, the investigator seize the item following legal provisions. For instance, a warrant is required to access the house of a suspect before the law enforcement agent can search it. Any item gotten from a house without appropriate warrant will not be admissible at the law court regardless of the extent of evidence contained in it. Where an unauthorized person access a crime scene and identified an evidence, such an evidence may be suspect and may lose its probative value.

c. **Preservation:** In this phase, data is isolated, secured, and preserved. Those accessing the evidence must be professionals and it includes the prevention of unauthorized persons from accessing the digital device to avoid contamination of the digital evidence. Some have argued that preservation actually precedes identification since the first actions taken at the crime scene by the Crime Scene Managers is to preserve it from contamination even before any evidence have been identified.

d. **Extraction (Acquisition or Imaging):** The forensic duplication of the evidence drive is done at this stage. This duplicate is referred to as an image or mirror image and the process is called imaging. Specialized tools such as FTK Imager is used to create a forensic image of the drive and it is on this drive that the Digital Forensics investigator conduct analysis. Write blocker device is used to prevent modification of the original evidence media.

e. **Analysis:** This is the main step that determine the final outcome of the investigation. Seemingly disjointed and fragmented data are connected together at this stage. It may include data reconstruction from available fragments, connecting timelines to events and interpretation of hidden meanings of recovered data. This may entails numerous iterations of examinations of available data to support or disprove a specific crime theory.

f. **Documentation:** Some have argued that the step is the real first step of the Digital Forensics process. It is a known fact that documentation of the evidence precedes its discovery. Investigators begin to process appropriate documentations such as warrants, job assignment approvals, etc. before reaching the crime scene. The documentation of the crime scene precedes the identification of an evidence which is then followed by a carefully documented record of the evidence. Chain of custody of the evidence starts here and ends only when the evidence is returned to the owner. Records of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.
g. **Report Writing:** This is where the Digital Forensic examiner put his thought to paper by carefully documenting all information about the case from the moment when he got involved, documentation of the evidence, methodologies, equipment, software and tools used, his conclusions and his final opinion on the evidence. Reports should be in simple layperson's language and avoid using technical jargons that may be misinterpreted at the court. All abstracted terminologies should reference the specific details and carefully explained.

h. **Presentation:** Presentation is the last step of the digital forensics process. Here, the Digital Forensics examiner presents his opinion of the evidence at the court of law or administrative panels or proceedings. He explains his opinion of the evidence usually under cross examination as Expert Witness.

**PURPOSE OF DIGITAL FORENSICS**
The purpose of Digital forensics are as numerous as there are crime, and may depend on the particular case under investigation. The broad goal of Digital forensics are as follows:

- It helps to identify, recover, analyze, and preserve computer based or electronic evidence in a manner that it can be admissible in a court of law.
- Determine source of evidence
- Determine Document originality or authentication
- Make available enough evidence to confirm or disprove hypothesis of a case, alibis, statements
- It helps to determine the reason, intent or motive behind the crime
- Provides evidence to identity who is responsible for a crime among others.
- Connecting timelines to events
- Provides methodology to ensure the integrity of digital evidence recovered at a crime scene.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Providing evidence of location
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Provides ingredient for a computer forensic report which offers a complete report on the investigation process.
- Preservation of electronic evidence using the chain of custody.

**CHALLENGES OF DIGITAL FORENSICS**

- Training and certification programs are largely in the hands of commercial companies (often forensic software developers)
- The proprietary nature of devices has affected Mobile Forensics regardless of its rich source of evidence
• High risk of cyber warfare and cyber-terrorism.
• A general bias towards Windows operating systems in Digital Forensics research at the expense of other platforms. This platforms such as UNIX, etc. are largely preferred by large corporations.
• Increasing size of digital media.
• Widespread availability of encryption software to consumers
• Growing variety of operating systems and file formats
• Increasing access to Information and Communication Technology (ICT) devices
• Limitations created by heterogeneous legal frameworks across countries.
• Constantly changing technology
• Need for continuous training for practitioners
• Prohibitively high cost of entering the field

USES OF DIGITAL FORENSICS
Digital Forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts. As with other areas of Forensics this is often a part of a wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes other than court proceedings (for example to locate, identify or halt other crimes). As a result, intelligence gathering is sometimes held to a less strict forensic standard.

In recent time, commercial organizations have used digital forensics in the following type of cases:

• Intellectual Property theft
• Industrial espionage
• Employment disputes
• Fraud investigations
• Inappropriate use of the Internet and email in the workplace
• Forgeries related matters
• Bankruptcy investigations
• Issues concern with the regulatory compliance
• Network intrusion investigation to identify attacker
• Identification of owner of device
• To prove or disprove alibis and statements
• To prove the intent of a criminal.
• Identification of the origin of a particular piece of data.
• Document authentication. This is related to "Evaluation of source," meta data associated with digital documents can be easily modified (for example, by
changing the computer clock you can affect the creation date of a file). Document authentication relates to detecting and identifying falsification of such details.

ADVANTAGES OF DIGITAL FORENSICS
Below are benefits of Digital forensics
a. Ensure the integrity of the computer system.
b. Provide evidence in the court, which can lead to the punishment of the culprit.
c. It helps the companies to capture important information if their computer systems or networks are compromised.
d. Efficiently tracks down cybercriminals from anywhere in the world.
e. Helps to protect the organization's money and valuable time.
f. Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

DISADVANTAGES OF DIGITAL FORENSICS
Here, are major drawbacks of using Digital Forensic
a. Digital evidence accepted into court. However, it is must be proved that there is no tampering
b. Producing electronic records and storing them is an extremely costly affair
c. Legal practitioners must have extensive computer knowledge
d. Need to produce authentic and convincing evidence
e. If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
f. Lack of technical knowledge by the investigating officer might not offer the desired result
g. Experience in evidence presentation in court processes and cross examination

CHALLENGES FACED BY DIGITAL FORENSICS
Here, are major challenges faced by Digital Forensic:

a. The increase of PC's and extensive use of internet access
b. Easy availability of hacking tools
c. Lack of physical evidence makes prosecution difficult.
d. The large amount of storage space into Terabytes that makes this investigation job difficult.
e. Any technological changes require an upgrade or changes to solutions
f. Widespread use of encryption. This disrupts initial examination where pertinent evidence might be located. Laws to compel individuals to disclose encryption keys are still relatively new and controversial.
5. CASES IN DIGITAL FORENSICS

CASE STUDY ONE: Locational data - geotags

The facts: Following the Russian annexation of Crimea in February 2014, international tensions built over allegations that Russian troops were operating in other parts of Ukraine. Russian officials repeatedly denied these allegations. Starting in late June 2014, Alexander Sotkin, a sergeant in the Russian Army, posted a month-long series of selfies taken from his cell phone to his public Instagram account. The press picked the story up when it was discovered that the jpeg. files posted included geotag metadata, and that the geotags and pictures showed the sergeant moving on-duty from a military base in Russia into eastern Ukraine and then back to the base.

The takeaway: Geotags, such as those embedded in Sotkin’s pictures, are a form of locational metadata. Geotags generated by smartphones tend to be very accurate and are associated with other types of file metadata, like date- and timestamps. Combine these attributes with the conventional wisdom that a picture is worth a thousand words and reports showing that smartphone users take over 150 pictures per month, and you have a treasure trove of data to pin down who/what/when/where details during an investigation.

Geotags and other types of locational data can also be embedded in other types of files, such as video files and SMS text messages. Other cell phone locational data can be drawn from routes stored in mapping applications, Wi-Fi connections, cell towers in call history and applications like weather or real estate tools.

CASE STUDY TWO: Wearable sensors

The facts: Connie Dabate was murdered in her home in 2015. According to his arrest warrant, her husband Richard provided an elaborate explanation of the day’s events, claiming that he returned home after receiving an alarm alert. Richard went on to claim that, upon entering his house, he was immobilized and tortured by an intruder. He told police that the intruder then shot and killed Connie when she returned home from the gym. Relying on evidence collected from Connie’s Fitbit, police were able to show that she had been in the house at the time Richard said she was at the gym. According to the Fitbit’s data, Connie stopped moving one minute before the home alarm went off.

The takeaway: Wearable devices like Fitbits monitor location via GPS and activities like distance traveled, steps taken, sleep time and heart rate. The devices are configured to synchronize data to applications on smartphones and personal computers or to cloud or social media sites. Evidentiary collections can be made from either of these sources using standard digital forensics tools and techniques.

CASE STUDY THREE: Data from asset trackers - sensors and IoT devices

The facts: The case of Howze v. Western Express, Inc. revolved around injuries caused when a tractor-trailer forced a motorcycle off the road. The truck in question
could not be definitively identified by an eye witness, although the witness recalled that the trailer logo read “Western Express.” The defendant’s trucks were equipped with asset trackers which included a GPS feature. Data from the trackers was collected and retained in a centralized database. The defendant claimed that a search of the database showed that it had no trucks on the road in question on the night of the accident. To counter that claim, the plaintiff cited Western Express’ six-month GPS data retention policy, and challenged the validity of the defendant’s search, which was conducted 27 months after the accident. The judge decided that there was a question of material fact that needed to be sorted out by a jury.

The takeaway: Asset trackers take advantage of GPS, Wi-Fi and Bluetooth technology to allow organizations to monitor their moveable assets. They may collect basic locational data or may have expanded features that capture other information like diagnostics, messaging, weather conditions, or compliance data. They are used to track high-value, moveable assets (e.g., fleet vehicles, construction equipment, medical devices) and are starting to show up in the growing array of consumer IoT devices. Howze helps demonstrate that asset tracker evidence is highly probative. It is also highly available to investigators who are working for an organization that owns or finances the asset. As in Howze, the client’s database can be searched or the data can be extracted to a better platform to help understand and preserve the who/what/when/where details in a controlled manner. The investigators can avoid having to examine the asset itself or involve the asset custodian in their inquiry. Howze also demonstrates the need to handle structured data (i.e., records stored in a database) in a defensible manner. Structured data should be collected and validated early in the investigation to avoid spoliative events like a regularly-scheduled database purge. Handling of the structured data should be defensibly documented. If the dataset is large or if queries are complex, a forensic consultant who understands structured data should be retained. Structured data analytics is a complex discipline and is not included in the standard forensic examiner’s toolkit. Specialists will be needed.

CASE STUDY FOUR: Network data reveals theft of trade secrets

The facts: Xiaolang Zhang worked as an engineer for Apple’s autonomous car division. He had been with the company 2½ years when he announced that he would be resigning and returning to China to take care of his elderly mother. He told his manager that he would be working for an electric car manufacturer in China. The conversation left the manager suspicious. Company security started an investigation. They searched Zhang’s two work phones and laptop—but were most alarmed when they reviewed Zhang’s network activity. The story the network data told was that Zhang’s activity had spiked to a two-year high in the days leading up to his resignation. It consisted of “bulk searches and targeted downloading copious pages of information” taken from secret databases he could access. When confronted, Zhang admitted to taking company data. The matter was referred to the FBI, and Zhang was indicted for theft of trade secrets.
The takeaway: Network forensics is a sub-specialty of digital forensics. It involves analysis of log data from servers and other networking tools (e.g., firewalls, routers, intrusion detection applications) in order to trace or monitor network activity. Attorneys with cyber law practices have become very familiar with network forensics, as it is one of the go-to tools for intrusion and breach detection. Network forensics can involve retroactive analysis or live-stream traffic monitoring. The volume of data collected can be enormous, so data analytics techniques are used heavily.

It used to be the case that network forensics was seldom practiced. To reduce the need for storage hardware, few organizations had their network logging features turned on. Fewer still retained their logs long enough to be of value when investigators came calling. Practices have changed as companies have become more sophisticated and diligent about cyber security. The Zhang case demonstrates that the availability of network data presents opportunities to investigate user activity in non-cyber cases, (i.e., a theft of trade secrets matter). As in the Zhang case, network logs can be analyzed to identify mass movements or deletions of data and other suspect user activity.

CASE STUDY FIVE: Data from vehicle infotainment, telematics and black box systems

The facts: A 2017 story from Digital Forensics Magazine describes a hit-and-run car crash caused by the driver of a dark SUV without lights on. The SUV hit a car, ran into a clump of trees and then drove off. Police were able to locate an SUV that fit the description. After downloading data from its on-board diagnostics, infotainment and telematics systems, police were able to determine that the vehicle had passed the scene at the approximate time the crash had occurred, that the lights had not been on and that the SUV had been placed in reverse and forward several times immediately after the time of the crash in the proximity of the damaged trees. Police also found other implicating details of the SUV’s trip that night from routes and destinations in the navigation system.

The takeaway: Vehicles are becoming nearly as rich a target for investigative data as personal computers or smartphones. According to Edmunds.com, the top five things a car knows about its driver are:

1. A home or business address
2. A list of recently-navigated or commonly-frequented locations
3. Phone contacts
4. Emails and texts
5. Speed, braking and seatbelt use data

And there is more—some vehicles are also equipped with web browsers that may keep history, cookies and cache information. There also may be data from manufacturer-embedded applications such as Facebook. As with personal computers, it is possible to identify devices that have been attached to a vehicle’s computer. It may also be possible in the near future to recover video data and history from the autonomous driving features already showing up in cars.
Vehicle forensics has emerged as a developing specialization in digital forensics. To date, most of the activity has centered on a single forensic tool; however, the tool’s developers claim that it works on over 10,000 makes of automobiles and trucks. There is already an active user base in vehicle forensics among auto insurance investigators, auto manufacturers, car rental companies, law enforcement and intelligence agencies.
6. VENDORS AND COMPUTER FORENSIC SERVICES

This chapter looks at how a swift and measured forensic incident response, drawing on sound policies, vendor tools, and support, allows an organization to contain the potential damage of an attack and effectively seek compensation or prosecution. In addition, this chapter covers the following computer forensic services:

1. Forensic incident response  
2. Evidence collection  
3. Forensic analysis  
4. Expert witness  
5. Forensic litigation and insurance claims support  
6. Training  
7. Forensic process improvement

OCCURRENCE OF CYBER CRIME

Cybercrime occurs when information technology is used to commit or conceal an offense. Computer crimes include:

a. Financial fraud  
b. Sabotage of data or networks  
c. Theft of proprietary information  
d. System penetration from the outside and denial of service  
e. Unauthorized access by insiders and employee misuse of Internet access privileges  
f. Viruses, which are the leading cause of unauthorized users gaining access to systems and networks through the Internet.

Cybercrimes can be categorized as either internal or external events. Typically, the largest threat to organizations has been employees and insiders, which is why computer crime is often referred to as an insider crime. For example, Ernst & Young’s global research has found that 93% of all identified frauds were committed by employees, almost 44% of which were committed by management. Internal events are committed by those with a substantial link to the intended victim, for example, a bank employee who siphons electronic funds from a customer’s account. Other examples include downloading or distributing offensive material, theft of intellectual property, internal system intrusions, fraud, and intentional or unintentional deletion or damage of data or systems.

CYBER DETECTIVES

Computer forensics, therefore, is a leading defense in the corporate world’s armory against cybercrime. Forensic investigators detect the extent of a security breach, recover lost data, determine how an intruder got past security mechanisms, and, possibly, identify the culprit. Forensic experts need to be qualified in both investigative and technical fields and trained in countering cybercrime. They should also be knowledgeable in the law, particularly legal jurisdictions, court requirements, and the laws on admissible evidence and production.
In many cases, forensic investigations lead to calling in law enforcement agencies and building a case for potential prosecution, which could lead to a criminal trial. The alternative is pursuing civil remedies, for instance, pursuing breach of trust and loss of intellectual property rights.

**Legal Issues**
The most common legal difficulty faced by organizations seeking to redress cybercrime in the courts is having digitally based evidence accepted. Notwithstanding the technical expertise of information technology (IT) teams, most companies are ill-equipped to investigate cybercrime in a way that results in the collection of admissible evidence. For example, data collected as evidence must be shown to not be tampered with and be accounted for at every stage of its life from collection to presentation in court. In other words, it must meet the requirements of the jurisdiction’s laws of evidence.

Another issue is the lag time between legislation and change and improvements in technology. As a result, law enforcement organizations and computer forensic experts are often forced to use archaic and nonspecific laws to fit unusual circumstances. For example, to commit *theft*, a person must permanently deprive the victim of property. However, if a disgruntled employee copied an organization’s database and sold it to a rival company, the organization is not permanently deprived of the data; therefore, technically, no offense of *theft* has been committed. In addition, it is unclear whether *data* fits into the legal definition of property. However, even in cases where there is a clearly defined crime, corporations are often hesitant to pursue a criminal conviction because of the time, cost, and reputation risk involved in reaching a legal outcome.

**FIGHTING CYBERCRIME WITH RISK-MANAGEMENT TECHNIQUES**
The rate of technological change, the spread of computer literacy, and the growth of e-commerce collaboration, such as alliances and marketplaces, make the challenge of restricting cybercrime damage daunting. With legislation lagging behind technology, businesses have had no choice but to absorb the responsibility for the security of their most valuable asset—their information. Risks range from expensive downtime, sales and productivity losses to corrupted data, damage to reputation and consumer confidence and loyalty, and hefty compensation payments or lawsuits for breaches of client information.

The best approach for organizations wanting to counter cybercrime is to apply risk-management techniques. The basic steps for minimizing cybercrime damage are:

**a) Effective IT and Staff Policies**
Well-communicated and “plain language” IT policies educate staff about their rights and obligations in the workplace. The goal of these policies is to create a security solution that is owned by all staff, not only by those in the IT division. To be effective, IT policies should make plain what an individual employee can and cannot do on the organization’s systems and the legal implications of misuse. It is also vital
to make a continuing investment in policies, which must evolve and be supported by ongoing training initiatives.

Effective policies diminish the risk of internal attack, particularly unintentional attack. In addition, when attack does occur, these policies clearly define what constitutes a breach of security, making it easier to prosecute or seek compensation from the perpetrator.

b) Vendor Tools of the Trade
Although internal policies will not dissuade external cyber criminals, the right vendor tools will detect an external attack and alert the organization to the threat. These tools are programs that either analyze a computer system to detect anomalies, which may form the basis of an attack, or locate data that can be used as evidence of a crime or network intrusion.

Choosing the right cybercrime detection tools is essential for risk management in all organizations, but like most applications associated with an organization, the question is, what is the right tool? The right tools are those that deliver appropriate information that the forensic expert can interpret to achieve the best outcome. Ultimately, the evidence must withstand the rigors of legal proceedings. To deliver the information needed, software tools should be probing (without compromising the target of interrogation), concise, able to report findings fully, supported, and easy to use. Such tools will save forensic experts valuable time and allow them to concentrate on data interpretation.

c) Effective Procedures
Even in an organization that has implemented the hardware, installed the software, produced the policies, and employed competent staff to run an effective IT environment, it is not possible to prevent an incident from occurring. However, the attack itself does not have the greatest impact on a company. How the business responds to that attack has the greatest impact on a company. Without the appropriate procedures in place to counter detected attacks, an organization is exposed to the risks of lost data, financial loss, network damage, and loss of reputation.

d) Forensic Response Capability
When an incident occurs, an organization needs an appropriate forensic response in place. By appointing a forensic expert to manage the response to an incident, organizations ensure all avenues are canvassed, all evidence located and handled correctly, and all those involved treated impartially.

COMPUTER FORENSICS INVESTIGATIVE SERVICES
There are without doubt some very knowledgeable experts in the field of computer forensics investigations; however, there has been an increase in the number of people purporting to be experts or specialists who produce flawed opinions or take actions
that are just plain wrong. The reasons for these errors are manifold but range from peer or management pressure, restricted timescales, and problems with software, to sheer lack of knowledge. Most investigations are basically the same in that they are either proving or disproving whether certain actions have taken place. The emphasis depends on whether the work is for the accuser or the accused.

In many companies, forensic computer examiners are kings because they have more knowledge of the subject than their peers. However, they are still subject to management pressures to produce results, and at times this can color their judgment. Time restrictions can cause them to take short cuts that invalidate the very evidence they are trying to gather, and when they do not find the evidence that people are demanding (even if it isn’t there), they are subject to criticism and undue pressure.

**Computer Intrusion Detection Services**
Installing technical safeguards to spot network intruders or detect denial-of-service attacks at e-commerce servers is prudent, but if your staff doesn’t have the time or skills to install and monitor intrusion detection software, you might consider outsourcing the job.

**Digital Evidence Collection**
Perhaps one of the most crucial points of your case lies hidden in a computer. The digital evidence collection process not only allows you to locate that key evidence, but also maintains the integrity and reliability of that evidence. Timing during this digital evidence collection process is of the essence. Any delay or continued use of the suspect computer may overwrite data prior to the forensic analysis and result in destruction of critical evidence. The following are some helpful tips that you can follow to help preserve the data for future computer forensic examination:

- Do not turn on or attempt to examine the suspect computer. This could result in destruction of evidence.
- Identify all devices that may contain evidence:
  - Workstation computers

**Litigation Support and Insurance Claims**
Since its inception, cyber-insurance has been billed as a way for companies to underwrite potential hacking losses for things technology cannot protect. The concept of insuring digital assets has been slow in catching on because the risks and damages were hard to quantify and put a price tag on.

The September 11, 2001, terrorist attacks quickly elevated corporate America’s interest in cyber-insurance, as industry magnates looked for ways to mitigate their exposure to cyberterrorism and security breaches. At the same time, it has become harder to find underwriters willing to insure multimillion-dollar cyberspace policies.
FORENSIC PROCESS IMPROVEMENT
These are the steps taken in the threat identification process.

i) Dig \texttt{-x /nslookup}
The first step in the process is to reverse the offending IP address. The Dig \texttt{-x ip} command will perform a reverse lookup on an IP address from its domain name server. The \texttt{"-x"} option will ensure that you receive all records possible about your host from the Domain Name Service (DNS) table. This might include nameservers, email servers, and the host’s resolved name. The “nslookup” command, \texttt{Nslookup ip}, will also perform a reverse lookup of the host IP address, but will only return the resolved name.

ii) Whois
The next step in the process is to perform a “whois” lookup on the IP address to see who owns the offending IP or at least who it is registered to. This can be a tricky operation.

iii) Ping
Conduct the Ping IP command to determine if your attacking IP is currently online. Note that many administrators block ICMP traffic, so this is not conclusive evidence either way.

iv) Traceroute
The next step in the process is to conduct a Traceroute IP to determine possible paths from your proxy site to the target system. Traceroute may help you in two ways. If your IP does not resolve possible paths from your proxy site to the target system, there may be a clue about its parentage. Also, a traceroute might give you an important clue about the physical location of the attacking box. If you can determine what city the attack came from, you have just considerably narrowed down the possible pool of candidates of who the attacker might be.

v) Finger
Conduct a finger@ip command to determine who is currently logged onto the system that attacked you. Now, to be frank, this command will rarely work, because most administrators wisely turn this service off. However, it does not hurt to try.

Keep in mind that many systems that are compromised and used as lily pads to attack other hosts are poorly configured (that is why they were compromised in the first place). They may also have the finger service running. If it is running, finger root@ip sees the last time root was logged on and, more important, from where root was logged on. You might be surprised to see root logged on from a third system in another country. Keep following the trail as long as your commands are not refused. You should be able to trace back hackers through several countries using this simple, often-overlooked technique. Look for
strange login names and for users logged into the system remotely. This may indicate where the host was compromised from and is the next clue to where to focus your research.

vi) **Anonymous Surfing**  
Surfing anonymously to the domain where your attacking IP is hosted is the next step in the threat identification process. You will know this domain name by looking at the resolved name of the host and the whois data. One technique that is useful is to use a search engine such as [http://www.altavista.com](http://www.altavista.com) with the specialized advanced search option of “+host:domain name and hack*.” This query will return Web links of possible hackers who operate from the domain name you queried.

vii) **USENET**  
The last step in the process of threat identification is to conduct a USENET traffic search on your domain. Search on the attacking IP address in quotes to see if other people are reporting activity from this IP in any security newsgroups. Search on the domain name or hacker aliases that you might have collected from your anonymous surfing, or from the returns of your finger queries. You can expand the headers of the postings by clicking on “view original posting.” This may show you the actual server that posted the message, even if the hacker attempted to spoof his or her mailing address in the visible header. This method can reveal the true location of your hacker. Clicking on “author profile” can also give you valuable information. Look at the new groups your hacker posts to and look at the number and sophistication of those postings.
7. DATA RECOVERY

Computers systems may crash. Files may be accidentally deleted. Disks may accidentally be reformatted. Computer viruses may corrupt files. Files may be accidentally overwritten. 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 you should employ the latest tools and techniques to recover your data.

Data recovery is, of course, of potential interest to anyone who has lost data to the ravages of time, malice, or carelessness, but in forensic computing or analysis, it takes on a new meaning—suddenly what other people have thrown away can become an important component in understanding what has happened in the past, as burglary tools, data files, correspondence, and other clues can be left behind by interlopers.

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. Many people, even computer experts, fail to recognize data recovery as an option during a data crisis, yet 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.

As computers are used in more important transactions and storage functions, and more important data is stored on them, the importance of qualified data recovery experts becomes clear. Perhaps your information has been subjected to a virus attack, suffered damage from smoke or fire, or your drive has been immersed in water—the data recovery experts can help you. Perhaps your mainframe software has malfunctioned or your file allocation tables are damaged—data recovery experts can help you.

DATA BACKUP AND RECOVERY

You live in a world that is driven by the exchange of information. Ownership of information is one of the most highly valued assets of any business striving to compete in today’s global economy. Companies that can provide reliable and rapid access to their information are now the fastest growing organizations in the world. To remain competitive and succeed, they must protect their most valuable asset—data.

Backup Obstacles

The following are obstacles to backing up applications:

- Backup window
- Network bandwidth
- System throughput
- Lack of resources

i) Backup Window

The backup window is the period of time when backups can be run. The backup window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low.
ii) **Network Bandwidth**
Many companies now have more data to protect than can be transported across existing local area networks (LANs) and wide area networks (WANs). If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization’s centralized backup strategy is not viable.

iii) **System Throughput**
Three I/O bottlenecks are commonly found in traditional backup schemes. These are
a. The ability of the system being backed up to push data to the backup server
b. The ability of the backup server to accept data from multiple systems simultaneously
c. The available throughput of the storage device(s) onto which the data is moved.

iv) **Lack of Resources**
Many companies fail to make appropriate investments in data protection until it is too late. Often, information technology (IT) managers choose not to allocate funding for centralized data protection because of competing demands resulting from emerging issues such as e-commerce, Internet and intranet applications, and other new technologies.

**The Future of Data Backup**
Successful data backup and recovery is composed of four key elements: the backup server, the network, the backup window, and the backup storage device (or devices). These components are highly dependent on one another, and the overall system can only operate as well as its weakest link.

a. **The Backup Server**
The backup server is responsible for managing the policies, schedules, media catalogs, and indexes associated with the systems it is configured to back up. The systems being backed up are called *clients*. Traditionally, all managed data that was being backed up had to be processed through the backup server. Conversely, all data that needed to be restored had to be accessed through the backup server as well. This meant that the overall performance of a backup or recovery was directly related to the ability of the backup server to handle the I/O load created by the backup process.

b. **The Network Data Path**
Centralization of a data-management process such as backup and recovery requires a robust and available network data path. The movement and management of hundreds or thousands of megabytes of data can put a strain on even the best-designed networks.

c. **The Backup Window**
Of all the parameters that drive the design of a backup application, one remains an absolute constant, and that is time. A backup window defines how much time is available to back up the network. Time plays an important role in choosing how much server, network, and resource support needs to be deployed.

d. Backup Storage Devices
In many cases, the single most expensive item in a backup project is the backup storage device itself. Therefore, it is important that the technical specifications of the storage device provide adequate capacity and performance to accommodate existing and planned data. Determining the storage format, number of drives, and how many slots are required is predicated on many variables. Backup windows, growth rates, retention policies, duplicate drive copies, and network and server throughputs all affect which backup storage device is best for your needs.

THE ROLE OF BACKUP IN DATA RECOVERY
Many factors affect back-up:
  a. Storage costs are decreasing.
  b. Systems have to be online continuously.
  c. The role of backup has changed.

THE DATA-RECOVERY SOLUTION
Availability once meant that an application would be available during the week, from 9 to 5, regardless of whether customers needed anything. Batch processing took over the evenings and nights, and most people didn’t care because they were at home asleep or out having fun. But the world has changed. It’s now common to offer extended service hours in which a customer can call for help with a bill, inquiry, or complaint. Even if a live human being isn’t available to help, many enterprise applications are Web-enabled so that customers can access their accounts in the middle of the night while sitting at home in their pajamas.
8. EVIDENCE COLLECTION AND SEIZURE
Evidence is difficult to collect at the best of times, but when that evidence is electronic, an investigator faces some extra complexities. Electronic evidence has none of the permanence that conventional evidence has, and it is even more difficult to form into a coherent argument.

WHY COLLECT EVIDENCE?
There are two simple reasons: future prevention and responsibility.

1. Future Prevention
Without knowing what happened, you have no hope of ever being able to stop someone else (or even the original attacker) from doing it again. It would be analogous to not fixing the lock on your door after someone broke in. Even though the cost of collection can be high, the cost of repeatedly recovering from compromises is much higher, both in monetary and corporate image terms.

2. Responsibility
There are two responsible parties after an attack: the attacker and the victim. The attacker is responsible for the damage done, and the only way to bring him to justice (and to seek recompense) is with adequate evidence to prove his actions. The victim, on the other hand, has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks. The victim may also have a legal obligation to perform an analysis of evidence collected, for instance if the attack on their system was part of a larger attack.

COLLECTION OPTIONS
Once a compromise has been detected, you have two options: pull the system off the network and begin collecting evidence or leave it online and attempt to monitor the intruder. Both have their pros and cons. In the case of monitoring, you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes. You also leave yourself open to possible liability issues if the attacker launches further attacks at other systems from your own network system. If you disconnect the system from the network, you may find that you have insufficient evidence or, worse, that the attacker left a dead man switch that destroys any evidence once the system detects that it’s offline. What you choose to do should be based on the situation.

OBSTACLES
Electronic crime is difficult to investigate and prosecute. Investigators have to build their case purely on any records left after the transactions have been completed.

Add to this the fact that electronic records are extremely (and sometimes transparently) malleable and that electronic transactions currently have fewer limitations than their paper-based counterparts and you get a collection nightmare. Computer transactions are fast, they can be conducted from anywhere (through
anywhere, to anywhere), can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible.

Any paper trail of computer records they may leave can be easily modified or destroyed, or may be only temporary. Worse still, auditing programs may automatically destroy the records left when computer transactions are finished with them. Because of this, even if the details of the transactions can be restored through analysis, it is very difficult to tie the transaction to a person. Identifying information such as passwords or PIN numbers (or any other electronic identifier) does not prove who was responsible for the transaction. Such information merely shows that whoever did it either knew or could get past those identifiers.

Even though technology is constantly evolving, investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously. The best you can do is to follow the rules of evidence collection and be as assiduous as possible.

TYPES OF EVIDENCE
Before you start collecting evidence, it is important to know the different types of evidence categories. Without taking these into consideration, you may find that the evidence you’ve spent several weeks and quite a bit of money collecting is useless. Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function—provided that the log can be shown to be free from contamination.

a) Testimonial Evidence
Testimonial evidence is any evidence supplied by a witness. This type of evidence is subject to the perceived reliability of the witness, but as long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence. Word processor documents written by a witness may be considered testimonial—as long as the author is willing to state that he wrote it.

b) Hearsay
Hearsay is any evidence presented by a person who was not a direct witness. Word processor documents written by someone without direct knowledge of the incident are hearsay. Hearsay is generally inadmissible in court and should be avoided.

THE RULES OF EVIDENCE
There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful.

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable
1. Admissible
Admissible is the most basic rule. The evidence must be able to be used in court or otherwise. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

2. Authentic
If you can’t tie the evidence positively to the incident, you can’t use it to prove anything. You must be able to show that the evidence relates to the incident in a relevant way.

3. Complete
It’s not enough to collect evidence that just shows one perspective of the incident. You collect not only evidence that can prove the attacker’s actions, but also evidence that could prove their innocence. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and why you think they didn’t do it. This is called exculpatory evidence and is an important part of proving a case.

4. Reliable
The evidence you collect must be reliable. Your evidence collection and analysis procedures must not cast doubt on the evidence’s authenticity and veracity.

5. Believable
The evidence you present should be clearly understandable and believable to a jury. There’s no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if you present them with a formatted, human understandable version, you must be able to show the relationship to the original binary, otherwise there’s no way for the jury to know whether you’ve faked it.

Using the preceding five rules, you can derive some basic do’s and don’ts:

a) Minimize handling and corruption of original data.

b) Account for any changes and keep detailed logs of your actions.

c) Comply with the five rules of evidence.

d) Do not exceed your knowledge.

e) Follow your local security policy.

f) Capture as accurate an image of the system as possible.

g) Be prepared to testify.

h) Work fast.

i) Proceed from volatile to persistent evidence.

j) Don’t shutdown before collecting evidence.

k) Don’t run any programs on the affected system.

a) Minimize Handling and Corruption of Original Data: Once you’ve created a master copy of the original data, don’t touch it or the original. Always handle secondary copies. Any changes made to the originals will affect the outcomes of any analysis later done to copies. You should also remove any
external avenues for change and, in general, analyze the evidence after it has been collected.

b) **Account for Any Changes and Keep Detailed Logs of Your Actions:** Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented. Any changes at all should be accounted for—not only data alteration but also physical alteration of the originals (the removal of hardware components).

c) **Comply with the Five Rules of Evidence:** The five rules are there for a reason. If you don’t follow them, you are probably wasting your time and money. Following these rules is essential to guaranteeing successful evidence collection.

d) **Do Not Exceed Your Knowledge:** If you don’t understand what you are doing, you can’t account for any changes you make and you can’t describe what exactly you did. If you ever find yourself “out of your depth,” either go and learn more before continuing (if time is available) or find someone who knows the territory.

e) **Follow Your Local Security Policy:** If you fail to comply with your company’s security policy, you may find yourself with some difficulties. Not only may you end up in trouble (and possibly fired if you’ve done something really against policy), but you may not be able to use the evidence you’ve gathered. If in doubt, talk to those who know.

f) **Capture as Accurate an Image of the System as Possible:** Capturing an accurate image of the system is related to minimizing the handling or corruption of original data. Differences between the original system and the master copy count as a change to the data. You must be able to account for the differences.

g) **Be Prepared to Testify:** If you’re not willing to testify to the evidence you have collected, you might as well stop before you start. Without the collector of the evidence being there to validate the documents created during the evidence-collection process, the evidence becomes hearsay, which is inadmissible.

h) **Work Fast:** The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don’t collect it in time. This is not to say that you should rush. You must still collect accurate data. If multiple systems are involved, work on them in parallel (a team of investigators would be handy here), but each single system should still be worked on methodically. Automation of certain tasks makes collection proceed even faster.
i) Proceed from Volatile to Persistent Evidence: Some electronic evidence is more volatile than others are. Because of this, you should always try to collect the most volatile evidence first.

j) Don’t Shutdown Before Collecting Evidence: You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned (via a trojan horse) the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out. Rebooting is even worse and should be avoided at all costs. As a general rule, until the compromised disk is finished with and restored, it should never be used as a boot disk.

k) Don’t Run Any Programs on the Affected System: Because the attacker may have left trojaned programs and libraries on the system, you may inadvertently trigger something that could change or destroy the evidence you’re looking for. Any programs you use should be on read-only media (such as a CD-ROM or a write-protected USB disk) and should be statically linked.

VOLATILE EVIDENCE
Not all the evidence on a system is going to last very long. Some evidence resides in storage that requires a consistent power supply; other evidence may be stored in information that is continuously changing. When collecting evidence, you should always try to proceed from the most volatile to the least. Of course, you should still take the individual circumstances into account. To determine what evidence to collect first, you should draw up an order of Volatility a list of evidence sources ordered by relative volatility. An example an order of volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology

GENERAL PROCEDURE
When collecting and analyzing evidence, there is a general four-step procedure you should follow. Note that this is a very general outline. You can customize the details to suit your situation.

a) Identification of Evidence: You must be able to distinguish between evidence and junk data. For this purpose, you should know what the data is, where it is
located, and how it is stored. Once this is done, you will be able to work out the best way to retrieve and store any evidence you find.

b) **Preservation of Evidence**: The evidence you find must be preserved as close as possible to its original state. Any changes made during this phase must be documented and justified.

c) **Analysis of Evidence**: The stored evidence must then be analyzed to extract the relevant information and recreate the chain of events. Analysis requires in-depth knowledge of what you are looking for and how to get it.

d) **Presentation of Evidence**: Communicating the meaning of your evidence is vitally important—otherwise you can’t do anything with it. The manner of presentation is important, and it must be understandable by a layman to be effective. It should remain technically correct and credible. A good presenter can help in this respect.

### COLLECTING AND ARCHIVING

Once you’ve developed a plan of attack and identified the evidence that needs to be collected, it’s time to start the actual process of capturing the data. Storage of that data is also important, as it can affect how the data is perceived.

**Logs and Logging**

You should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Because logs are usually automatically timestamped, a simple copy should suffice, although you should digitally sign and encrypt any logs that are important to protect them from contamination. Remember, if the logs are kept locally on the compromised machine, they are susceptible to either alteration or deletion by an attacker. Regular auditing and accounting of your system is useful not only for detecting intruders but also as a form of evidence.

**Monitoring**

Monitoring network traffic can be useful for many reasons—you can gather statistics, watch out for irregular activity (and possibly stop an intrusion before it happens), and trace where an attacker is coming from and what he is doing. Monitoring logs as they are created can often show you important information you might have missed had you seen them separately. This doesn’t mean you should ignore logs later—it may be what’s missing from the logs that is suspicious.

**METHODS OF COLLECTION**

There are two basic forms of collection: *freezing the scene* and *honeypotting*. The two aren’t mutually exclusive. You can collect *frozen* information after or during any honeypotting.

*Freezing* the scene involves taking a snapshot of the system in its compromised state. The necessary authorities should be notified (the police and your incident response
and legal teams), but you shouldn’t go out and tell the world just yet. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format. Make sure the programs and utilities used to collect the data are also collected onto the same media as the data. All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

Honeypotting is the process of creating a replica system and luring the attacker into it for further monitoring. A related method (sandboxing) involves limiting what the attacker can do while still on the compromised system, so he can be monitored without (much) further damage. The placement of misleading information and the attacker’s response to it is a good method for determining the attacker’s motives.

**ARTIFACTS**
Whenever a system is compromised, there is almost always something left behind by the attacker—be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as *artifacts*. They are one of the important things you should collect, but you must be careful. You should never attempt to analyze an artifact on the compromised system. Artifacts are capable of anything, and you want to make sure their effects are controlled.

**COLLECTION STEPS**
You now have enough information to build a step-by-step guide for the collection of the evidence. This guide should be customize to your specific situation. You should perform the following collection steps:

1. **Find the Evidence**
   Determine where the evidence you are looking for is stored. Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.

2. **Find the Relevant Data**
   Once you’ve found the evidence, you must figure out what part of it is relevant to the case. In general, you should err on the side of over-collection, but you must remember that you have to work fast. Don’t spend hours collecting information that is obviously useless.

3. **Create an Order of Volatility**
Now that you know exactly what to gather, work out the best order in which to gather it. The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.

4. **Remove External Avenues of Change**
   It is essential that you avoid alterations to the original data, and prevention is always better than a cure. Preventing anyone from tampering with the evidence helps you create as exact an image as possible.

5. **Collect the Evidence**
   You can now start to collect the evidence using the appropriate tools for the job. As you go, reevaluate the evidence you’ve already collected. You may find that you missed something important. Now is the time to make sure you get it.

6. **Document Everything**
   Your collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important. Don’t leave anything out.

**CONTROLLING CONTAMINATION: THE CHAIN OF CUSTODY**

Once the data has been collected, it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used. This not only ensures that the original data remains clean, but also enables examiners to try more dangerous, potentially data-corrupting tests. Of course, any tests done should be done on a clean, isolated host machine. You don’t want to make the problem worse by letting the attacker’s programs get access to a network.

**Analysis**

Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened.

**Time**

To reconstruct the events that led to your system being corrupted, you must be able to create a timeline. This can be particularly difficult when it comes to computers. Clock drift, delayed reporting, and differing time zones can create confusion in abundance. One thing to remember is to never, ever change the clock on an affected system. Record any clock drift and the time zone in use, as you will need this later, but changing the clock just adds in an extra level of complexity that is best avoided.

**Forensic Analysis of Backups**

When analyzing backups, it is best to have a dedicated host for the job. This examination host should be secure, clean (a fresh, hardened install of the operating system is a good idea), and isolated from any network. You don’t want it tampered with while you work, and you don’t want to accidentally send something nasty down the line. Once this system is available, you can commence analysis of the backups.
RECONSTRUCTING THE ATTACK
Now that you have collected the data, you can attempt to reconstruct the chain of events leading to and following the attacker’s break-in. You must correlate all the evidence you have gathered (which is why accurate timestamps are critical), so it’s probably best to use graphical tools, diagrams, and spreadsheets. Include all of the evidence you’ve found when reconstructing the attack—no matter how small it is. You may miss something if you leave a piece of evidence out.
9. DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE

Computer evidence is odd, to say the least. It lurks on computer hard disk drives, USB drives, and at different levels. Such evidence is fragile and can easily be destroyed by something as simple as the normal operation of the computer.

Electromagnets and planted destructive trojan horse programs are other hazards that can permanently destroy computer evidence within seconds. There is no other type of evidence that presents the investigator with as many potential problems and challenges. In the old days, defense lawyers didn’t know much about computer evidence. As a result, cross-examination by the defense wasn’t as strong a few years ago as it is today. However, things are changing because lawyers are becoming educated because of the current popularity of electronic document discovery in the legal community. Times have changed and it is all the more important to do things by the book.

The three criminal evidence rules to gain admissibility are
1. Authentication: showing a true copy of the original.
2. The best evidence rule: presenting the original; and
3. Exceptions to the hearsay rule: are when a confession or business or official records are involved.

PRESERVING THE DIGITAL CRIME SCENE
The computer investigator not only needs to be worried about destructive process and devices being planted by the computer owner, he or she also needs to be concerned about the operating system of the computer and applications. Evidence is easily found in typical storage areas (spreadsheet, database, and word processing files). Unfortunately, potential evidence can also reside in file slack, erased files, and the Windows swap file. Such evidence is usually in the form of data fragments and can be easily overwritten by something as simple as the booting of the computer or the running of Microsoft Windows. When Windows starts, it potentially creates new files and opens existing ones as a normal process. This situation can cause erased files to be overwritten, and data previously stored in the Windows swap file can be altered or destroyed. As you can imagine, file dates are important from an evidence standpoint.

Another concern of the computer investigator is the running of any programs on the subject computer. Criminals can easily modify the operating system to destroy evidence when standard operating systems commands are executed. Perpetrators could modify the operating system such that the execution of the DIR command destroys simulated evidence. Standard program names and familiar Windows program icons can also be altered and tied to destructive processes by a crafty high-tech criminal.

Many inherent problems associated with computer evidence processing vanish when tried and proven processing procedures are followed.
Your first objective, after securing the computer, should be to make a complete bit stream backup of all computer data before it is reviewed or processed. This should normally be done before the computer is operated. Preservation of evidence is the primary element of all criminal investigations, and computer evidence is certainly no exception.

The importance of bit stream image backups cannot be stressed enough. To process a computer hard disk drive for evidence without a bit stream image backup is like playing with fire in a gas station. The basic rule is that only on rare occasions should you process computer evidence without first making an image backup. The hard disk drive should be imaged using a specialized bit stream backup product.

**COMPUTER EVIDENCE PROCESSING STEPS**

Computer evidence is fragile by its very nature, and the problem is compounded by the potential of destructive programs and hidden data. Even the normal operation of the computer can destroy computer evidence that might be lurking in unallocated space, file slack, or in the Windows swap file. There really are no strict rules that must be followed regarding the processing of computer evidence. Every case is different, and flexibility on the part of the computer investigator is important.

With that in mind, the following general computer evidence processing steps have been provided. Remember that these do not represent the only true way of processing computer evidence. They are general guidelines provided as food for thought:

1. Shut down the computer.
2. Document the hardware configuration of the system.
3. Transport the computer system to a secure location.
5. Mathematically authenticate data on all storage devices.
6. Document the system date and time.
7. Make a list of key search words.
8. Evaluate the Windows swap file.
10. Evaluate unallocated space (erased files).
11. Search files, file slack, and unallocated space for keywords.
12. Document file names, dates, and times.
13. Identify file, program, and storage anomalies.
14. Evaluate program functionality.
15. Document your findings.
16. Retain copies of software used.

**LEGAL ASPECTS OF COLLECTING AND PRESERVING COMPUTER FORENSIC EVIDENCE**

Some of the most common reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, lack of incident response training, and a broken chain of custody.
Definition
In simple terms, a chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court. Establishing a clear chain of custody is crucial because electronic evidence can be easily altered. A clear chain of custody demonstrates that electronic evidence is trustworthy. Preserving a chain of custody for electronic evidence, at a minimum, requires proving that:

- No information has been added or changed.
- A complete copy was made.
- A reliable copying process was used.
- All media was secured

Legal Requirements
When evidence is collected, certain legal requirements must be met. These legal requirements are vast, complex, and vary from country to country. However, there are certain requirements that are generally agreed on within the United States. U.S. Code Title 28, Section 1732 provides that log files are admissible as evidence if they are collected in the regular course of business. Also, Rule 803(6) of the Federal Rules of Evidence provides that logs, which might otherwise be considered hearsay, are admissible as long as they are collected in the course of regularly conducted business activity. This means you’d be much safer to log everything all the time and deal with the storage issues than to turn on logging only after an incident is suspected. Not only is this a bit like closing the barn door after the horse has fled, but it may also render your logs inadmissible in court.

Evidence Collection Procedure
When the time arrives to begin collecting evidence, the first rule that must be followed is do not rush. Tensions will probably be high and people will want to find answers as quickly as possible. The investigation team will need to bring certain tools with them to the incident site.

They will need a copy of their incident-handling procedure, an evidence collection notebook, and evidence identification tags. Depending on the type of incident and whether the team will be able to retrieve an entire system or just the data, they may also need to bring tools to produce reliable copies of electronic evidence, including media to use in the copying process.

When an incident is reported, this individual will contact the other members of the response team as outlined in the Incident Response Policy. Upon arrival at the incident site, this individual will be responsible for ensuring that every detail of the incident-handling procedure is followed. The incident coordinator will also assign team members the various tasks outlined in the incident-handling procedure and will serve as the liaison to the legal team, law enforcement officials, management, and public relations personnel. Ultimate responsibility for ensuring that evidence is properly collected and preserved, and that the chain of custody is properly maintained, belongs to the incident coordinator. One team member will be assigned
the task of maintaining the evidence notebook. This person will record the who, what, where, when, and how of the investigation process. At a minimum, items to be recorded in the notebook include

- Who initially reported the suspected incident along with time, date, and circumstances surrounding the suspected incident.
- Details of the initial assessment leading to the formal investigation.
- Names of all persons conducting the investigation.
- The case number of the incident.
- Reasons for the investigation.
- A list of all computer systems included in the investigation, along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.
- Network diagrams.
- Applications running on the computer systems previously listed.

Storage and Analysis of Data

Finally, the chain of custody must be maintained throughout the analysis process. One of the keys to maintaining the chain is a secure storage location. It is important that evidence never be left in an unsecured area. If a defense lawyer can show that unauthorized persons had access to the evidence, it could easily be declared inadmissible.

Pieces of evidence should be grouped and stored by case along with the evidence notebook. In an effort to be as thorough as possible, investigators should follow a clearly documented analysis plan. A detailed plan will help prevent mistakes (which could lead to the evidence becoming inadmissible) during analysis. As analysis of evidence is performed, investigators must log the details of their actions in the evidence notebook. The following should be included at a minimum:

- The date and time of analysis
- Tools used in performing the analysis
- Detailed methodology of the analysis
- Results of the analysis
10. COMPUTER IMAGE VERIFICATION AND AUTHENTICATION
As law enforcement and other computer forensics investigators become more familiar with handling evidential computer material, it is apparent that a number of more or less formalized procedures have evolved to maintain both the continuity and integrity of the material to be investigated. Although these procedures are extremely effective under the current rules of evidence, it is expected that alternative procedures will develop as technology advances. The current procedures, in use by both law enforcement and computer forensics investigators, work something like this:

At least two copies are taken of the evidential computer. One of these is sealed in the presence of the computer owner and then placed in secure storage. This is the master copy and it will only be opened for examination under instruction from the court in the event of a challenge to the evidence presented after forensic analysis on the second copy. If the computer has been seized and held in secure storage by law enforcement, this will constitute best evidence. If the computer has not been seized, then the master copy becomes best evidence. In either case, the assumption is that while in secure storage, there can be no possibility of tampering with the evidence. This does not protect the computer owner from the possibility that secured evidence may be tampered with.

SPECIAL NEEDS OF EVIDENTIAL AUTHENTICATION
A wealth of mathematical algorithms deals with secure encryption, verification, and authentication of computer-based material. These display varying degrees of security and complexity, but all of them rely on a second channel of information, whereby certain elements of the encryption/decryption/authentication processes are kept secret. This is characterized most plainly in the systems of public and private key encryption but is also apparent in other protocols. Consider the investigative process where computers are concerned. During an investigation, it is decided that evidence may reside on a computer system. It may be possible to seize or impound the computer system, but this risks violating the basic principle of innocent until proven guilty, by depriving an innocent party of the use of his or her system. It should be perfectly possible to copy all the information from the computer system in a manner that leaves the original system untouched and yet makes all contents available for forensic analysis.

When this is done, the courts may rightly insist that the copied evidence is protected from either accidental or deliberate modification and that the investigating authority should prove that this has been done. Thus, it is not the content that needs protection, but its integrity.

PRACTICAL CONSIDERATIONS
It is useful to present some fundamental requirements of a forensic data collection system before considering how these can be securely protected. These requirements were chosen to reflect the experience of computer forensic investigators. Other forensic experts may argue against some or all of them:
1. Forensic data collection should be complete and non-software specific, thus avoiding software traps and hidden partitioning.
2. In operation, it should be as quick and as simple as possible to avoid error or delay.
3. It should be possible for anyone to use a forensic data collection system with the minimum amount of training.
4. Necessary costs and resources should be kept to a minimum.

To meet the conditions specified in items 2, 3, and 4, the digital integrity verification and authentication protocol must be tailored to suit. For the collection phase to remain quick and simple, the digital integrity verification and authentication protocol must not add significantly to the time required for copying, nor should there be additional (possibly complex) procedures.

**PRACTICAL IMPLEMENTATION**

The emphasis here is on a practical application of proven technology, such that a minimum amount of reliance is placed on the technical ability of the operator/investigator. It must be understood that during the copying process, procedures are implemented to trap and handle hardware errors, mapping exceptions where necessary.

**Security Considerations**

Day after day, in every company, university, and government agency, a never-ending parry and thrust with those who threaten the security of their networks continues. Ultimately, with everything changing, the struggle for security is a constant battle. Everything has to be updated as new and different threats are received.

Organizations must be constantly vigilant. New technologies in the areas of image verification and authentication bring new vulnerabilities, and computer forensics investigators are constantly discovering vulnerabilities in old image verification and authentication products.