DEPARTMENT OF CYBER SECURITY

Track VI (CYBER FORENSICS)

CYBER FORENSICS

Unit–I Introduction: Computer Forensics Fundamentals – Types of Computer Forensics Technology – Types of Computer Forensics Systems – Vendor and Computer Forensics Services.

Unit–II Computer forensics evidence and capture:Data Recovery – Evidence Collection and Data SeizurE-Duplication and Preservation of Digital EvidencE-Computer Image Verification and Authentication.

Unit–III Computer forensic analysis: Discover of Electronic EvidencE-Identification of Data – Reconstructing Past Events – Fighting against Macro Threats – Information Warfare Arsenal – Tactics of the Military – Tactics of Terrorist and Rogues – Tactics of Private Companies

Unit–IV Information warfare: Arsenal – Surveillance Tools – Hackers and Theft of Components – Contemporary Computer CrimE-Identity Theft and Identity Fraud – Organized Crime &Terrorism – Avenues Prosecution and Government Efforts – Applying the First Amendment to Computer Related CrimE-The Fourth Amendment and other Legal Issues.

Unit–V Computer forensic cases: Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence –Processing Evidence and Report Preparation – Future Issues.

TEXT BOOKS

1) John R. Vacca, "Computer Forensics: Computer Crime Scene Investigation", Cengage Learning, 2nd Edition, 2005. (CHAPTERS 1 – 18). (UNIT I – IV)

2) Marjie T Britz, "Computer Forensics and Cyber Crime: An Introduction", Pearson Education, 2nd Edition, 2008. (CHAPTERS 3 – 13). (UNIT IV – V)

REFERENCE BOOKS

1) MariE-Helen Maras, "Computer Forensics: Cybercriminals, Laws, and Evidence", Jones & Bartlett Learning; 2nd Edition, 2014.

2) Chad Steel, "Windows Forensics", Wiley, 1st Edition, 2006.

3) Majid Yar, "Cybercrime and Society", SAGE Publications Ltd, Hardcover, 2nd Edition, 2013.

4) Robert M Slade, "Software Forensics: Collecting Evidence from the Scene of a Digital Crime", Tata McGraw Hill, Paperback, 1st Edition, 2004.

UNIT–I

Syllabus:- Introduction: Computer Forensics Fundamentals – Types of Computer Forensics Technology – Types of Computer Forensics Systems – Vendor and Computer Forensics Services.

INTRODUCTION:

COMPUTER FORENSICS FUNDAMENTALS:

What is Computer Forensics?

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

(or)

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.

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

Choosing a Computer Forensics Specialist for a Criminal Case:- When you require the services of a computer forensics specialist, don't be afraid to shop around. There are an increasing number of people who claim to be experts in the field. Look very carefully at the level of experience of the

individuals involved. There is far more to proper computer forensic analysis than the ability to retrieve data, especially when a criminal case is involved.

The bottom line is that you will be retaining the services of an individual who will likely be called to testify in court to explain what he or she did to the computer and its data.

The court will want to know that individual's own level of training and experience, not the experience of his or her employer. Make sure you find someone who not only has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination.

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

Employer Safeguard Program:- As computers become more prevalent in businesses, employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual.

Whether you are looking for evidence in a criminal prosecution or civil suit or determining exactly what an employee has been up to, you should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have beenreformatted, or other steps have been taken to conceal or destroy the evidence. For example, did you know?

- ✓ What Web sites have been visited
- ✓ What files have been downloaded
- ✓ When files were last accessed
- ✓ Of attempts to conceal or destroy evidence

✓ Of attempts to fabricate evidence

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

For example, they should be able to perform the following services:

✓ Data seizure

✓ Data duplication and preservation

✓ Data recovery

✓ Document searches

✓ Media conversion

✓ Expert witness services

✓ Computer evidence service options

✓ Other miscellaneous services

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

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

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

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

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

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

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

Computer Evidence Service Options:-
- ✓ Standard service
- ✓ On-site service
- ✓ Emergency service
- ✓ Priority service
- ✓ Weekend service

Other Miscellaneous Services:-
- ✓ Analysis of computers and data in criminal investigations
- ✓ On-site seizure of computer data in criminal investigations
- ✓ Analysis of computers and data in civil litigation.
- ✓ On-site seizure of computer data in civil litigation
- ✓ Analysis of company computers to determine employee activity
- ✓ Assistance in preparing electronic discovery requests
- ✓ Reporting in a comprehensive and readily understandable manner
- ✓ Court-recognized computer expert witness testimony
- ✓ Computer forensics on both PC and Mac platforms
- ✓ Fast turnaround time

Benefits of Professional Forensics Methodology: - Protection of evidence is critical. A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer

2. No possible computer virus is introduced to a subject computer during the analysis process

3. Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage

4. A continuing chain of custody is established and maintained

5. Business operations are affected for a limited amount of time, if at all

6. Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

Steps Taken by Computer Forensics Specialists:-

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

2. Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files etc.

3. Recover all of discovered deleted files.

4. Access the contents of protected or encrypted files.

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

6. Provide expert consultation and/or testimony.

Who can use Computer Forensic Evidence?

1. Criminal prosecutors use computer evidence in a variety of crimes where incriminating documents can be found, including homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.

2. Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.

3. Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.

4. Corporations often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, and theft or misappropriation of trade secrets, and other internal and confidential information.

5. Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.

6. Individuals sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination.

Problems with Computer Forensic Evidence:-

Computer evidence is like any other evidence. It must be

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

There are also special problems:

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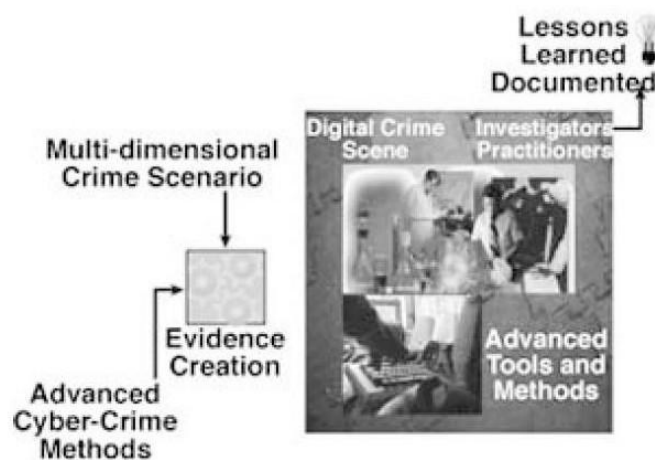
TYPES OF COMPUTER FORENSICS TECHNOLOGY:

Types of Military Computer Forensic Technology:- The U.S. Department of Defense (DoD) cyber forensics includes evaluation and in depth examination of data related to both the trans- and post-cyber attack periods. Key objectives of cyber forensics include rapid discovery of evidence,

estimation of potential impact of the malicious activity on the victim, and assessment of the intent and identity of the perpetrator. Real-time tracking of potentially malicious activity is especially difficult when the pertinent information has been intentionally hidden, destroyed, or modified in order to elude discovery.

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

The NLECTC assembled a diverse group of computer crime investigators from DoD and federal, state, and local law enforcement to participate in the CFX-2000 exercise hosted by the New York State Police's Forensic Investigative Center in Albany, New York. Officials divided the participants into three teams. Each team received an identical set of software tools and was presented with identical initial evidence of suspicious activity.

FIGURE 2.1 CFX-2000 schematic

Types of Law Enforcement Computer Forensic Technology:- 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 diskette to the computer that created it. Law enforcement and military agencies have been involved in processing computer evidence for years.

Computer Evidence Processing Procedures:-

- ✓ Preservation Of Evidence
- ✓ Mirror Image Backup Software
- ✓ Anadisk Diskette Analysis Tool
- ✓ Copyqm: Diskette Duplication Software
- ✓ Text Search Plus
- ✓ Intelligent Forensic Filter

Disk Structure:- Participants should be able to leave a training course with a good understanding of how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk. They should also demonstrate their knowledge of how to modify the structure and hide data in obscure places on floppy diskettes and hard disk drives.

Data Encryption:- computer forensics course should cover, in general, how data is encrypted; it should also illustrate the differences between good encryption and bad encryption. Furthermore, demonstrations of password-recovery software should be given regarding encrypted WordPerfect, Excel, Lotus, Microsoft Word, and PKZIP files. The participant should become familiar with the use of software to *crack* security associated with these different file structures.

Matching a Diskette to a Computer:- New Technology Inc. has also developed specialized techniques and tools that make it possible to conclusively tie a diskette to a computer that was used to create or edit files stored on it. Unlike some *special* government agencies, New Technology Inc. relies on logical rather than physical data storage areas to demonstrate this

technique. Each participant is taught how to use special software tools to complete this process.

Data Compression:- The participant should be shown how compression works and how compression programs can be used to hide and disguise sensitive data. Furthermore, the participant should learn how password-protected compressed files can be broken; this should be covered in hands-on workshops during the training course.

Erased Files:- The training participant should be shown how previously erased files can be recovered by using DOS programs and by manually using data-recovery techniques. These techniques should also be demonstrated by the participant, and cluster chaining will become familiar to the participant.

Internet Abuse Identification and Detection:- The participant should be shown how to use specialized software to identify how a targeted computer has been used on the Internet. This process will focus on computer forensics issues tied to data that the computer user probably doesn't realize exists.

The Boot Process and Memory Resident Programs:- The participant should be able to take part in a graphic demonstration of how the operating system can be modified to change data and destroy data at the whim of the person who configured the system. Such a technique could be used to covertly capture keyboard activity from corporate executives, for example. For this reason, it is important that the participants understand these potential risks and how to identify them.

Types of Business Computer Forensic Technology:-
- ✓ Remote monitoring of target computers
- ✓ Creating trackable electronic documents
- ✓ Theft recovery software for laptops and PCs
- ✓ Basic forensic tools and techniques
- ✓ Forensic services available

Remote monitoring of target computers:- Data Interception by Remote Transmission (DIRT) from Codex Data Systems(CDS), Inc. [7] 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.

Creating Trackable Electronic Documents:- Binary Audit Identification Transfer is another powerful intrusion detection tool.

Theft Recovery Software for Laptops and PCs:- Nationwide 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.

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. So many workshops have been created that it is beyond the scope of this chapter to mention them all. However, throughout the book, a number of them will be mentioned in detail.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.

Forensic Services Available:-
- ✓ 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
- ✓ Honey pot 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

TYPES OF COMPUTER FORENSICS SYSTEMS:-

✓ Internet security systems

✓ Intrusion detection systems

✓ Firewall security systems

✓ Storage area network security systems

✓ Network disaster recovery systems

✓ Public key infrastructure security systems

✓ Wireless network security systems

✓ Satellite encryption security systems

✓ Instant messaging (IM) security systems

✓ Net privacy systems

✓ Identity management security systems

✓ Identity theft prevention systems

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. 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.
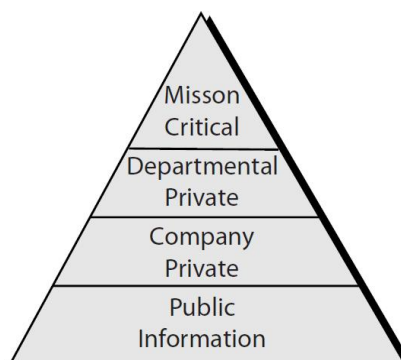
FIGURE 3.1 Internet security hierarchy.

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

- ✓ 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

Firewall Security Systems:- 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. Reacting to this threat, an increasing number of network administrators are installing the latest firewall technology as a *first line of defense* in the form of a barrier against outside attacks. These firewall gateways provide a choke point at which security and auditing can be imposed. They allow access to resources on the Internet from within the organization while providing controlled access from the Internet to hosts inside the virtual private network (VPN).

Storage area network security systems:- SANs are a relatively new methodology for attaching storage, whereby a separate network (separate from the traditional LAN) connects all storage and servers. This network would be a high-performance implementation, such as a fiber channel, that encapsulates protocols such as a small computer system interface (SCSI). These are more efficient at transferring data blocks from storage and have hardware implementations offering buffering and delivery guarantees. This is not available using TCP/IP.

The SAN development areas have not yet been realized, but there is great potential with regard to centralized storage SAN management and storage abstraction. Storage abstraction refers to an indirect representation of

storage that has also been called virtualization. Together with these potential enhancements, SANs should be able to generate greater functionality than has been possible previously. Thus, most system vendors have ambitious strategies to change the way enterprise operations store and manage data with new capabilities based on SANs.
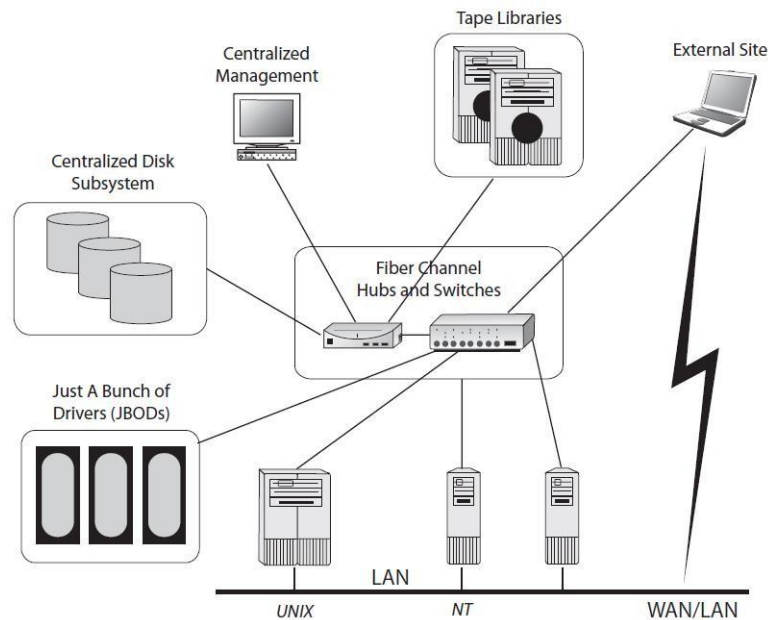
FIGURE 3.4 Storage-centric model of computing

Network Disaster Recovery Systems:- The high availability of mission-critical systems and communications is a major requirement for the viability of the modern organization. A network disaster could negate the capability of the organization to provide uninterrupted service to its internal and external customers.

How would your company respond in the event of a network disaster or emergency? 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.

Public Key Infrastructure Systems:- The PKI assumes the use of *public key cryptography*, which is the most common method on the Internet for authentication of a message sender or encryption of a message. Traditional cryptography involves the creation and sharing of a secret key for the encryption and decryption of messages. This secret key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the PKI is the preferred approach on 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

Wireless Network Security Systems:- The only reason the wireless viruses of today have not been more damaging is that there's a lack of functionality and a lack of mature infrastructure globally. That's about to change. Industry analysts predict dramatic increases in wireless handheld use and the proliferation of new mobile capabilities.

The wireless world, with its often-incompatible alphabet soup of standards, may be new territory for many IT managers. Many enterprises have felt that protecting their wireless processes against viruses is one piece of the complicated puzzle they can afford to omit. They'll soon need to think again or face threats that could wreak havoc.
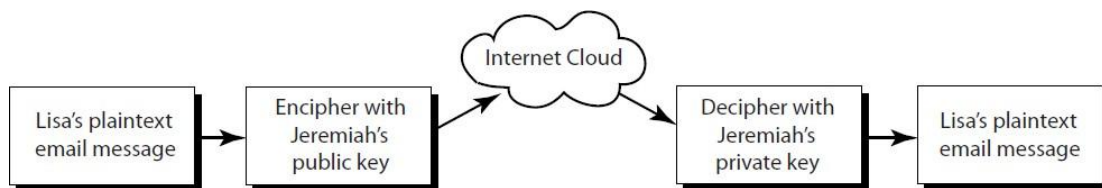
The good news is wireless network security vendors (even giants like IBM) are busy developing products to fight the viruses and security breaches of

the future. Among them are those that head off problems on a wireless network level, within applications and on devices.

Satellite Encryption Security Systems:-
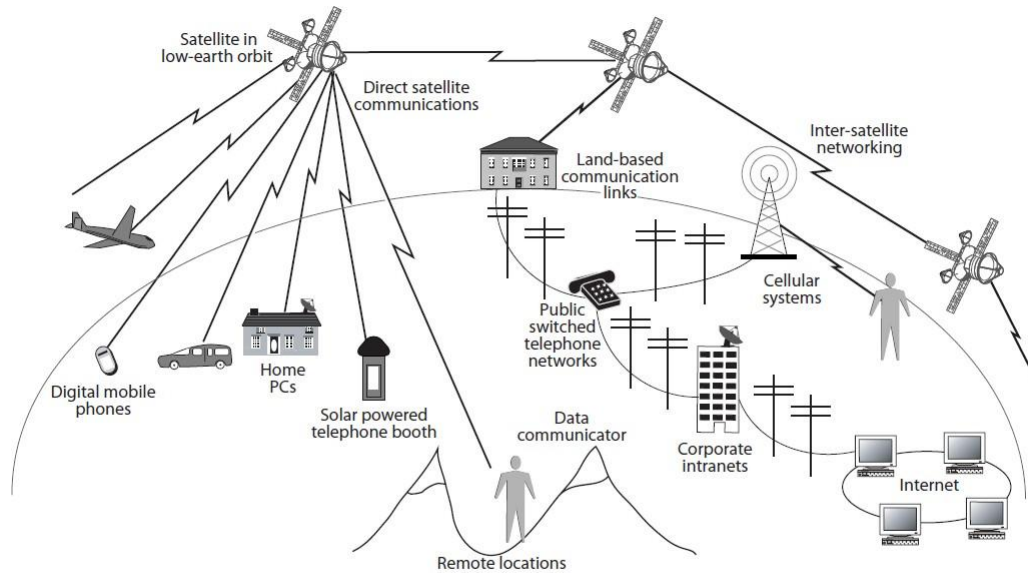
FIGURE 3.5 The low Earth orbit (LEO) network.

FIGURE 3.6 The path of a public-key-encrypted message.

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.

VENDOR AND COMPUTER FORENSICS SERVICES:-

Computer forensic services:-

- ✓ Forensic incident response
- ✓ Evidence collection
- ✓ Forensic analysis
- ✓ Expert witness
- ✓ Forensic litigation and insurance claims support
- ✓ Training
- ✓ Forensic process improvement

Occurrence of Cyber Crime:-

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

Cyber Detectives:- Computer forensics, therefore, is a leading defense in the corporate world's armory against cyber crime. 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 cyber crime. 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.

Fighting Cyber Crime with Risk-Management Techniques:- The best approach for organizations wanting to counter cyber crime is to apply risk-management techniques. The basic steps for minimizing cyber crime damage are creating well-communicated IT and staff policies, applying effective detection tools, ensuring procedures are in place to deal with incidents, and having a forensic response capability.

- ✓ Effective IT and Staff Policies
- ✓ Vendor Tools of the Trade

Computer Forensics Investigative Services:- 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. Many of these *specialists* are well meaning, but they tend to work in isolation or as part of a hierarchical structure where they are the *computer expert*. The specialists' management does not understand what they are doing (and probably don't want to admit it), and often they are faced with the question, Can't you just say this.....? It takes a very strong-minded person to resist this sort of pressure, and it is obvious that this has had an adverse effect in a number of cases.

Computer Intrusion Detection Services:- Intrusion detection is the latest security service to be offered on an outsourced basis, usually by the types of Internet service providers (ISPs) or specialized security firms that have been eager to manage your firewall and authentication. Although outsourcing security means divulging sensitive information about your network and corporate business practices, some companies say they have little choice but to get outside help, given the difficulty of hiring security experts.

Ex:- the Yankee Group reports that managed-security services (of which intrusion detection is the latest phenomenon) more than tripled, from $450 million in 2000 to $1.5 billion in 2003. By 2009, the market is expected to reach $7.4 billion, fueled by the trend toward outsourcing internal local area network (LAN) security to professional security firms as *virtual employees*.

Digital Evidence Collection:- 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:

1. Workstation computers

2. Off-site computers

3. Removable storage devices (zips, Jaz, Orb, floppy diskettes, CDs, Sony Memory Sticks, Smart Media, Compact Flash, LS-120, optical disks, SyQuest, Bernouli, microdrives, pocketdrives, USB disks, firewire disks, PCMICA)

4. Network storage devices (redundant array of independent disks [RAIDs], servers, storage area networks [SANs], network attached storage [NAS], spanned, remote network hard drives, back-up tapes, etc.)

Quarantine all in-house computers:

- Do not permit anyone to use the computers.
- Secure all removable media.
- Turn off the computers.
- Disconnect the computers from the network.

Forensically image all suspect media.

Forensic Process Improvement:- The risk any system connected to the Net faces is a product of vulnerability and threat. The techniques covered in this section will help you determine possible actions and possible motivations of the attacker. If you can understand your attacker, than you can better defend against and respond to attacks against your network. Of course, it is important to understand that hackers will loop through several systems during the attack phase.

- ✓ Dig –x /nslookup
- ✓ Whois
- ✓ Ping
- ✓ Traceroute
- ✓ Finger
- ✓ Anonymous Surfing
- ✓ USENET
- ✓ File Slack

The occurrence of random memory dumps in hidden storage areas [9] should be discussed and covered in detail during workshops. Techniques and automated tools used to capture and evaluate file slack should be demonstrated in the course. Such data is the source of potential security leaks regarding passwords, network logons, email, database entries, and word processing documents. These security and evidence issues should be discussed and demonstrated during the course. The participants should be able to demonstrate their ability to deal with slack from both an investigations and security risk standpoint. They should also be able demonstrate their proficiency in searching file slack, documenting their findings, and eliminating security risks associated with file slack.

Data-Hiding Techniques:- Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions. These issues should be discussed from a detection standpoint as well as from a security risk standpoint. Tools that help in the identification of such anomalies should demonstrated and discussed (AnaDisk). Participants should be required to demonstrate their understanding of such issues. This aspect of the training becomes especially important during the last day of the course when the participants are called on to identify and extract their Certificate of Completion from a *special* floppy diskette. *Data-hiding issues should be covered in much more depth in a data-hiding course.*

Internet-Related Investigations:- Issues and techniques related to the investigation of Internet-related matters should be covered in the course.

This should include a demonstration of how Internet related evidence differs from more traditional computer evidence. Emphasis should be placed on the investigation of Internet-based terrorist leads.

Dual-Purpose Programs:- Programs can be designed to perform multiple processes and tasks at the same time. They can also be designed for delayed tasks and processes. These concepts should be demonstrated to the participants during the course through the use of specialized software. The participants should also have hands-on experience with such programs.

Text Search Techniques:- Specialized search techniques and tools should be developed that can be used to find targeted strings of text in files, fileslack, unallocated file space, and Windows swap files. Each participantshould leave the class with the necessary knowledge to conduct computersecurity reviews and computer-related investigations. Because of the need tosearch for non-Latin words and word patterns tied to foreign languages, thecourse should also cover the search of such data tied to foreign languages **Fuzzy Logic Tools Used to Identify Previously Unknown Text:-** Amethodology and special computer forensics tools should be developed thataid in the identification of relevant evidence and *unknown* strings of text.Traditional computer evidence searches require that the computer specialistknow what is being searched for. However, many times not all is known in investigations. Thus, not all is known about what may be stored on a targeted computer system. In such cases, fuzzy logic tools can assist and can provide valuable leads as to how the subject computer was used. The participants should fully understand these methods and techniques. They should also be able to demonstrate their ability to use them to identify leads in file slack, unallocated file space, and Windows swap files.

Disk Structure:- Participants should leave the course with a solid understanding of how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk. They should also leave the class with a good understanding of how easy it is to modify the disk structure and to hide computer data in obscure places on floppy diskettes and hard disk drives.

Data Encryption:- A computer forensics training course should also cover how data is encrypted and illustrate the differences between good encryption and bad encryption. The participants should become familiar with the use of software to *crack* security associated with these different encryption file structures.

Matching a Floppy Diskette to a Computer:- Specialized computer forensics techniques and computer forensics tools should also be developed that make it possible to conclusively tie a floppy diskette to a computer hard disk drive. Each participant should also be taught how to use special software tools to complete a unique computer storage data-matching process. Some computer forensics experts believe floppy diskettes are no longer popular. They are wrong. Floppy diskettes are found to be a valuable source of computer evidence in some civil litigation cases that involve the theft of trade secrets.

Data Compression:- The participant should be shown how data compression programs can be used to hide and disguise critical computer data. Furthermore, the participant should learn how password-protected compressed files can be broken.

Erased Files:- Participants should be shown how previously erased files can be recovered using computer forensics processes and methods. Documentation of the process should also be covered in detail.

Internet Abuse Identification and Detection:- The participant should be shown how to use specialized software to identify how a targeted computer has been used on the Internet. This process should focus on computer forensics issues tied to data that the computer user probably doesn't realize exists (file slack, unallocated file space, and Windows swap files). Participants should get hands-on experience in using this unique technology and they should be given the opportunity to purchase the software for a nominal charge. Nevertheless, it should be provided free of charge to law enforcement computer crime specialists who attend the course. Law enforcement agencies are typically underfunded.

The Boot Process and Memory Resident Programs:- Participants should be able to see how easy it is to modify the operating system to capture data and to destroy computer evidence. Such techniques could be used to covertly capture keyboard activity from corporate executives, government computers, and the like. For this reason, it is important that the participants understand these potential risks and how to identify them.

<div align="center">

UNIT - II

</div>

Syllabus:- Computer forensics evidence and capture: Data Recovery – Evidence Collection and Data SeizurE-Duplication and Preservation of Digital EvidencE-Computer Image Verification and Authentication.

COMPUTER FORENSICS EVIDENCE AND CAPTURE:-
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 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. Fortunately, there are specialized hardware and software companies that manufacture products for the centralized backup and recovery of business critical data. Hardware manufacturers offer automated tape libraries that can manage millions of megabytes of backed up information and eliminate the need for operators charged with mounting tape cartridges. Software companies have created solutions that can back-up and recovery dozens of disparate systems from a single console.

Backup Obstacles:-
- ✓ Backup window
- ✓ Network bandwidth
- ✓ System throughput
- ✓ Lack of resources
- ✓ 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. However, many organizations now conduct operations 7 days a week, 24 hours a day— effectively eliminating traditional backup windows altogether.

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.

System Throughput:- Three I/O bottlenecks are commonly found in traditional backup schemes. These are

1. The ability of the system being backed up to push data to the backup server.

2. The ability of the backup server to accept data from multiple systems simultaneously.

3. The available throughput of the tape device(s) onto which the data is Moved.

The Future of Data Backup:-

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. In the past, the only way to overcome a backup server bottleneck was to invest in larger, more powerful backup servers or data backup and recovery and divide the backup network into smaller, independent groups. Fortunately, backup-software developers have created methods to work around these bottlenecks.
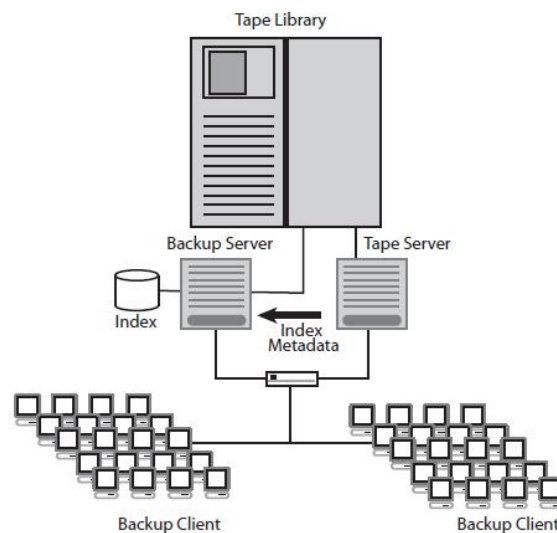
FIGURE 5.1 A backup using a shared tape library. (© Copyright 2002, StorNet. All rights reserved.)
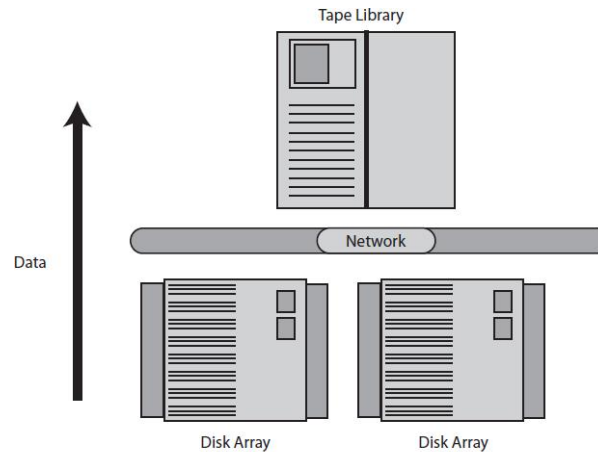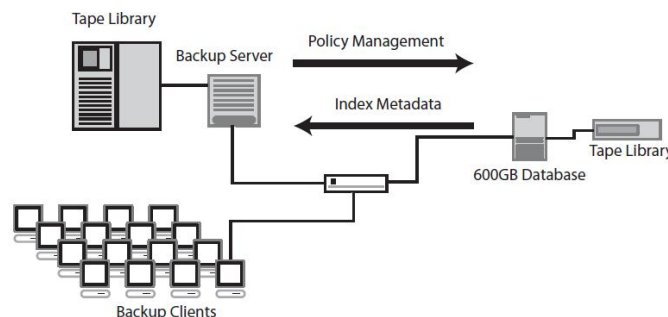
FIGURE 5.2 A serverless backup system. (© Copyright 2002, StorNet. All rights reserved.)
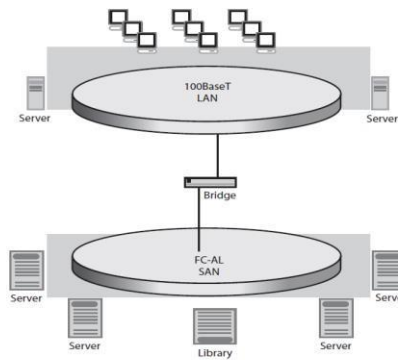
The Network Data Path:-

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. Unfortunately, many companies are already struggling with simply managing the existing data traffic created by applications such as e-commerce, the Internet, email, and multimedia document management. Although technology such as gigabit Ethernet and asynchronous transfer mode (ATM) can provide relief, it is rarely enough to accommodate management of large amounts of data movement.

SANs are quickly dominating the backup landscape, and applications such as serverless and LAN-less backup will continue to push this emerging technology forward. Figure 5.4 shows an example of a dedicated SAN topology.

FIGURE 5.3 A LAN-less back-up using a remote tape server. (© Copyright 2002, StorNet. All rights reserved.)

The Backup Window:- 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. Today, most companies are managing too much data to complete backup during these evershrinking backup windows.

In the past, companies pressured by inadequate backup windows were forced to add additional backup servers to the mix and divide the backup groups into smaller and smaller clusters of systems. However, the backup-software community has once again developed a way to overcome the element of time by using incremental backup, block-level backup, image backups, and data archiving.

Image Backups:- Image backups are quickly gaining favor among storage administrators. This type of backup creates copies, or *snapshots,* of a file system at a particular point in time. Image backups are much faster than incremental backups and provide the ability to easily perform a *bare bones* recovery of a server without loading the operating systems, applications, and the like. Image backups also provide specific point-in-time backups that can be done every hour rather than once a day.

Data Archiving:- Removing infrequently accessed data from a disk drive can reduce the size of a scheduled backup by up to 80%. By moving static, infrequently accessed data to tape, backup applications are able to focus on backing up and recovering only the most current and critical data. Static data that has been archived is easily recalled when needed but does not add to the daily data backup requirements of the enterprise. This method also

provides the additional benefit of freeing up existing disk space without adding required additional capacity.

Data Interleaving:- To back up multiple systems concurrently, the backup application must be able to write data from multiple clients to tape in an interleaved manner. Otherwise, the clients must be backed up sequentially, which takes much longer.

Remote Backup:- Many remote systems are exposed to unrecoverable data loss. Off-site locations are often not backed up at all because of the cost of deploying hardware and software remotely and the lack of administrative support in these remote locations. Laptop computers are especially vulnerable to data loss. A backup application should have a method to back up systems across WAN or over dial-up connections.

The Role of Backup in Data Recovery:-

Many factors affect back-up:

- ✓ Storage costs are decreasing.
- ✓ Systems have to be online continuously.
- ✓ The role of backup has changed.

Storage Costs Are Decreasing:- The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance. This has a huge impact on backup. As users become accustomed to having immediate access to more and more information online, the time required to restore data from secondary media is found to be unacceptable.

Systems Have to Be Online Continuously:- Seven/twenty-four (7 × 24) operations have become the norm in many of today's businesses. The amount of data that has to be kept online and available (operationally ready data) is very large and constantly increasing. Higher and higher levels of fault tolerance for the primary data repository are a growing requirement. Because systems must be continuously online, the dilemma becomes that you can no longer take files offline long enough to perform backup.

The Role of Backup has Changed:- It's no longer just about restoring data. Operationally, ready or *mirrored* data does not guard against data corruption

and user error. The role of backup now includes the responsibility for recovering user errors and ensuring that *good* data has been saved and can quickly be restored.

Conventional Tape Backup in Today's Market:- Current solutions offered by storage vendors and by backup vendors focus on network backup solutions. To effectively accomplish backup in today's environment, tape management software is generally bundled with several other components to provide a total backup solution. A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the backend controlling a repository of tape devices. The media server runs tape management software. It can administer backup devices throughout an enterprise and can run continuous parallel backups and restores.

The Data-Recovery Solution:-

Shrinking Expertise, Growing Complexity:- Increased availability is good, except for one fact: many systems programmers, database administrators (DBAs), and other mainframe experts are maturing. It takes a lot of care and feeding to keep applications ready for work, and the people who have maintained these environments for so long have other things they want to do. Many are starting to shift their sights toward that retirement community in Florida that they've heard so much about. Most of the bright youngsters who are graduating from college this term haven't had much exposure to mainframe concepts in their course work, much less any meaningful grasp of the day-to-day requirements for keeping mainframe systems running.

Failures:- Certainly, hardware failures were once more common than they are today. Disk storage is more reliable than ever, but failures are still possible. More likely to occur, though, is a simple mistake made by an application programmer, system programmer, or operations person. Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse, an undetected error in the database— undetected, that is, until minutes, hours, or days later when a customer calls, a reconciliation fails, or some other checking mechanism points out the integrity exposure.

Budgets and Downtime:- Does anyone need a reminder that budgets are tight? You have fewer resources (people, processing power, time, and money) to do more work than ever before, and you must keep your expenses under control. Shrinking expertise and growing complexity cry out for tools to make systems management more manageable, but the tools that can save resources (by making the most of the ones you have) also cost you resources to obtain, implement, and operate.

Recovery: Think Before You Back Up:- One of the most critical data-management tasks involves recovering data in the event of a problem. For this reason, installations around the world spend many hours each week preparing their environments for the possibility of having to recover. These preparations include backing up data, accumulating changes, and keeping track of all the needed resources.

Automated Recovery:- Having people with the required expertise to perform recoveries is a major consideration, particularly in disaster situations. For example, if the only person who understands your IBM Information Management System (IMS) systems (hierarchical database system) and can recover them moved far away, you're in trouble. However, if your recovery processes are planned and automated so that less-experienced personnel can aid in or manage the recovery process, then you're able to maximize all your resources and reduce the risk to your business.

EVIDENCE COLLECTION AND DATA SEIZURE:-

Why Collect Evidence?

Electronic evidence can be very expensive to collect. The processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed. So, why bother collecting the evidence in the first place? There are two simple reasons: future prevention and responsibility.

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.

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.

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.

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.

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

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.

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.

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.

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.

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:

- ✓ Minimize handling and corruption of original data.
- ✓ Account for any changes and keep detailed logs of your actions.
- ✓ Comply with the five rules of evidence.
- ✓ Do not exceed your knowledge.
- ✓ Follow your local security policy.
- ✓ Capture as accurate an image of the system as possible.
- ✓ Be prepared to testify.
- ✓ Work fast.
- ✓ Proceed from volatile to persistent evidence.
- ✓ Don't shutdown before collecting evidence.

✓ Don't run any programs on the affected system.

Volatile Evidence:-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:-

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.

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.

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. Always be sure that the person or people who are analyzing the evidence are fully qualified to do so.

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:-

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

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 themseparately. This doesn't mean you should ignore logs later—it may be what's missing from the log that is suspicious.

Information gathered while monitoring network traffic can be compiled into statistics to define normal behavior for your system. These statistics can be used as an early warning of an attacker's actions. You can also monitor the actions of your users. This can, once again, act as an early warning system. Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection.

Methods of Collection:- There are two basic forms of collection: freezing the scene and honey potting. The two aren't mutually exclusive. You can collect frozen information after or during any honey potting. 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. Honey potting 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.

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.* Artifacts may be difficult to find; trojaned programs may be identical in all obvious ways to the originals (file size, medium access control [MAC] times, etc.). Use of cryptographic checksums may be necessary, so you may need to know the original file's checksum. If you are performing regular file integrity assessments, this shouldn't be a problem. Analysis of artifacts can be useful in finding other systems the attacker (or his tools) has broken into.

Collection Steps:- You now have enough information to build a step-by-step guide for the collection of the evidence. Once again, this is only a guide. You should customize it to your specific situation. You should perform the following collection steps:

1. Find the evidence.

2. Find the relevant data.

3. Create an order of volatility.

4. Remove external avenues of change.

5. Collect the evidence.

6. Document everything.

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 isthere.

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.

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.

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. However, you have to be careful. The attacker may have been smart and left a dead-man switch. In the end, you should try to do as much as possible to prevent changes.

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.

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

A good way of ensuring that data remains uncorrupted is to keep a chain of custody. This is a detailed list of what was done with the original copies once they were collected. Remember that this will be questioned later on, so document everything (who found the data, when and where it was transported [and how], who had access to it, and what they did with it). You may find that your documentation ends up greater than the data you collected, but it is necessary to prove your case.

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. As always, you must make sure that you fully document everything you do. Your work will be questioned and you must be able to show that your results are consistently obtainable from the procedures you performed.

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.

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.

DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE:-

The three criminal evidence rules to gain admissibility are

1. Authentication

2. The best evidence rule

3. Exceptions to the hearsay rule

Authentication means showing a true copy of the original; best evidence means presenting the original; and the allowable exceptions are when a confession or business or official records are involved. Authentication appears to be the most commonly used rule, but experts disagree over what is the most essential, or most correct, element of this in practice.

If your documentation is poor, it will look like your processing procedures were poor, and when you testify in court, you will look ridiculous since you have no good written record to refresh your memory. Problems in the

documentation area arise when you try to take shortcuts or make do with less than adequate time, equipment, and resources.

If your preservation is poor, it becomes fairly evident that your collection and transportation of evidence gives rise to numerous possibilities for error in the form of destruction, mishandling, and contamination. Problems in the preservation area have implications for the integrity of law enforcement and crime labs. The basic chain of custody, for example, involves at least three initial sources of error.

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.

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.

4. Make bit stream backups of hard disks and floppy disks.

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.

9. Evaluate file slack.

10. Evaluate unallocated space (erased files).

11. Search files, file slack, and unallocated space for keywords.

12. Document files 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:- 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.

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

Legal Requirements:-

- ✓ This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
- ✓ In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
- ✓ Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Evidence Collection Procedure

- ✓ 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.
- ✓ A copy of the policy or policies that relate to accessing and using the systems previously listed.
- ✓ A list of administrators responsible for the routine maintenance of the system. A detailed list of steps used in collecting and analyzing evidence. Specifically, this list needs to identify the date and time each task was performed, a description of the task, who performed thetask, where the task was performed, and the results of the analysis.
- ✓ An access control list of who had access to the collected evidence at what date and time

Storage and Analysis of Data

- ✓ The date and time of analysis
- ✓ Tools used in performing the analysis
- ✓ Detailed methodology of the analysis
- ✓ Results of the analysis

COMPUTER IMAGE VERIFICATION AND AUTHENTICATION:-

Special Needs of Evidential Authentication:- A wealth of mathematical algorithms deal 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 these 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.
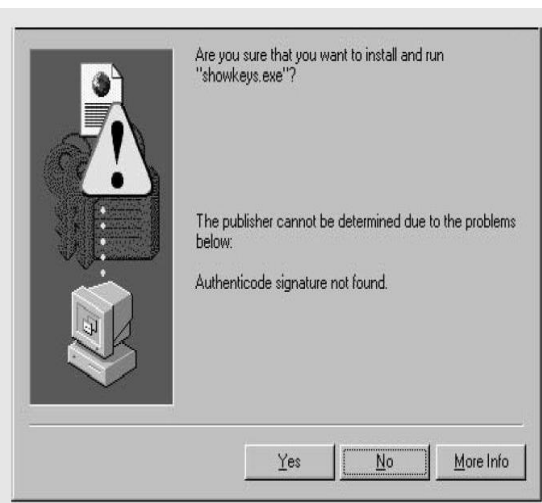
Digital IDS and Authentication Technology:- When customers buy software in a store, the source of that software is obvious. Customers can tell who published the software and they can see whether the package has been opened. These factors enable customers to make decisions about what software to purchase and how much to "trust" those products.

When customers download software from the Internet, the most they see is a message warning them about the dangers of using the software. The Internet lacks the subtle information provided by packaging, shelf space, shrink wrap, and the like. Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for customers to know how much to trust software. It's difficult to make the choice of downloading the software from the Internet.
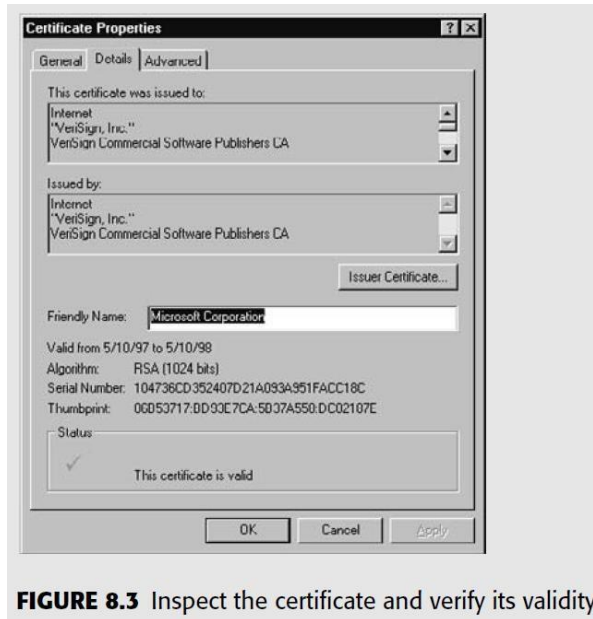
For example (when using Microsoft Authenticode coupled with Digital IDs™ from VeriSignR), through the use of digital signatures, software developers are able to include information about themselves and their code with their programs

FIGURE 8.1 Security warning screen.   **FIGURE 8.2** Client application security warning.

FIGURE 8.3 Inspect the certificate and verify its validity.

How Authenticode Works with VeriSign Digital IDS?
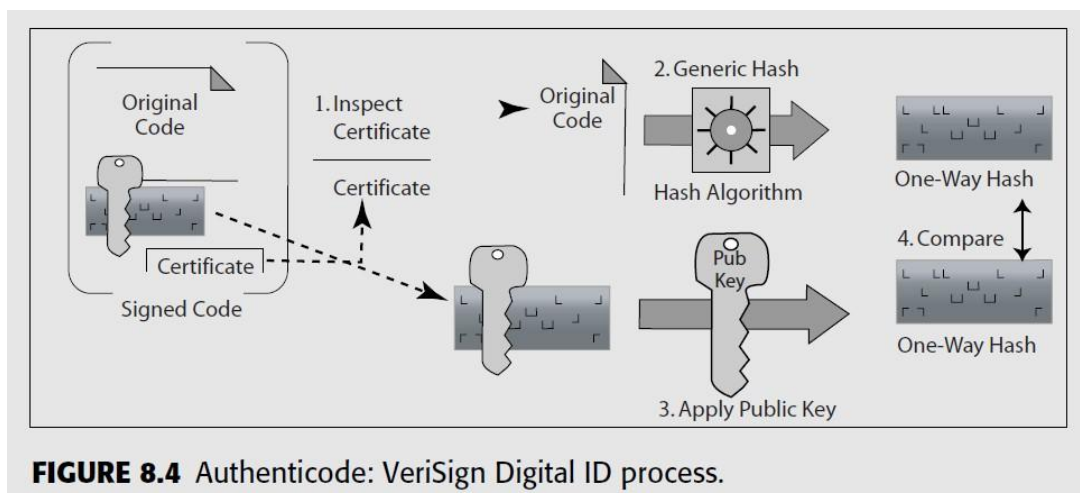
FIGURE 8.4 Authenticode: VeriSign Digital ID process.

1. Publisher obtains a software developer digital ID from VeriSign.

2. Publisher creates code

3. Using the SIGNCODE.EXE utility, the publisher

a. Creates a hash of the code, using an algorithm such as MD5 or SHA

b. Encrypts the hash using his private key

c. Creates a package containing the code, the encrypted hash, and the publisher's certificate

4. The end user encounters the package.

5. The end user's browser examines the publisher's digital ID. Using the VeriSignR root public key, which is already embedded in Authenticode-

enabled applications, the end user's browser verifies the authenticity of the software developer digital ID (which is itself signed by the VeriSign root Private Key).

6. Using the publisher's public key contained within the publisher's digital ID, the end user's browser decrypts the signed hash.

7. The end user's browser runs the code through the same hashing algorithm as the publisher, creating a new hash.

8. The end user's browser compares the two hashes. If they are identical, the browser messages that the content has been verified by VeriSign, and the end user has confidence that the code was signed by the publisher identified in the digital ID and that the code hasn't been altered since it was signed.

Time stamping:- Because key pairs are based on mathematical relationships that can theoretically be "cracked" with a great deal of time and effort, it is a well-established security principle that digital certificates should expire. Your VeriSign Digital ID will expire one year after it is issued. However, most software is intended to have a lifetime of longer than one year. To avoid having to resign software every time your certificate expires, a time stamping service is now available. Now, when you sign code, a hash of your code will be sent to VeriSign to be time stamped.

Practical Considerations

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.

UNIT - III

Syllabus:- Computer forensic analysis: Discover of Electronic Evidence-Identification of Data – Reconstructing Past Events – Fighting against Macro Threats – Information Warfare Arsenal – Tactics of the Military – Tactics of Terrorist and Rogues – Tactics of Private Companies

COMPUTER FORENSIC ANALYSIS:-

1. Computer technology has revolutionized the way we deal with information and the way we run our businesses. Increasingly important business information is created, stored, and communicated electronically.

2. Many types of information that can play a useful role in litigation are no longer printed on paper and stored in paper files, but rather are stored in a computer system or in computer-readable form.

3. As companies have increased their reliance on their computer systems, lawyers have begun to be aware of the valuable electronic treasures that are now being kept in these systems and have started aggressively to target electronic data for discovery in all types of litigation cases.

4. The primary purpose of these provisions is to enable the government to determine whether a company is complying with the record keeping and other requirements contained in the statute that imposes them.

5. Many businesses are increasingly storing the required records in electronic form. Government investigators will likely begin to focus their attention on the electronic forms of these records and the computer systems that house them.

6. The government also has access to records for investigatory purposes. Several statutes, such as the human rights codes, Competition Act, Criminal Code, and tax acts give government officials the right to enter a business establishment and inspect or seize records.

For example, under the Competition Act, peace officers with, or in exigent circumstances without, a search warrant, may enter the premises, examine records, and copy or seize them.

7. Lawyers representing parties with large amounts of electronic data need to understand that their clients' data will be targeted for such discovery and need to advise their clients on how to prepare.

8. Defensive strategies that should be implemented prior to litigation include a proper document retention program, periodic purging of magnetic media, and the implementation of a document management system.

9. Once litigation has commenced, defendants need to be better advised on how to preserve relevant electronic evidence adequately—to avoid possible sanctions or a negative inference at trial.

ELECTRONIC DOCUMENT DISCOVERY:-

A Powerful New Litigation Tool:- Other than direct testimony by an eyewitness, documentary evidence is probably the most compelling form of evidence in criminal and civil cases. Often, important communications are committed to writing, and such writings can make or break a case. The same is true about documents used to conduct financial transactions. The paper trail has always provided a wealth of information in criminal and civil cases involving fraud.

Traditional *paper* documents have been sought in the legal discovery process for hundreds of years in cases involving white collar crime (financial frauds, embezzlements). In more recent times, documentary evidence has become the keystone in civil cases involving wrongful employment dismissals, sexual discrimination, racial discrimination, stock fraud, and the theft of trade secrets.

Today, judges and attorneys are very familiar with documentary evidence in paper form. Unfortunately, the legal process has not kept pace with computer technology, and the document discovery rules have changed concerning the discovery of computer-created documents and related electronic data.

The best evidence rules also work differently today, because copies of computer files are as good as the original electronic document. From a computer forensics standpoint, this can be proven mathematically. There is no difference between the original and an exact copy. In addition, modern

technology has created new types of documentary evidence that previously did not exist. This is especially true for the creation of documents on a computer word processor. When electronic documents are created, bits and pieces of the drafts leading up to the creation of the final document are written in temporary computer files, the Windows swap file, and file slack. The computer user is usually not aware of this situation.

A historical perspective helps one understand the evolution of computer forensics and its transition into the new field of electronic document discovery. When computer mainframe giant International Business Machines (IBM) entered the personal computer market in October of 1981, the event quickly captured the attention of corporations and government agencies worldwide. Personal computers were no longer thought of as toys; almost overnight they were accepted as reliable business computers because of the IBM endorsement.

The worldwide popularity of both personal computers and the Internet has been a mixed blessing. Powerful personal computers are technology workhorses that increase productivity and provide portability. The Internet provides a conduit for the transfer of communication and computer files anywhere in the world via personal computers. However, essentially all personal computers lack meaningful security. This is because security was not factored into the design of the original personal computers, or the Internet for that matter.

The DOS operating system installed on the original IBM PC was never intended for commercial use. Security was never part of its design; in the interest of maintaining compatibility with the early versions of DOS, upgrades did not adequately address security. As a result, most popular desktop PCs and notebook computers lack adequate security. This situation creates an ideal environment for electronic document discovery of computer files, file fragments, and erased files. Some computer forensics specialists regard electronic document discovery as nothing more than the exploitation of the inherent security weaknesses in personal computers and the Internet. The attorney just needs to understand the potentials and the new twist in

thinking that is required to reap the benefits of electronic document discovery

IDENTIFICATION OF DATA:-

The popularity of the Internet has grown at incredible rates and today it reaches into the hearts of many corporations and households worldwide.The Internet gives computer users access to a wealth of information. It is also a wonderful mechanism for the exchange of email communications and file attachments globally. International boundaries no longer exist when it comes to the exchange of information over the Internet. This new technology has proven to be ideal for international commerce and has the potential to be a valuable communications tool for exchange of law enforcement and government information. However, the Internet also provides the crooks with communication capabilities that did not exist previously. Through the use of a modem and with just a few clicks of a mouse, criminals can share information worldwide. It is sad but very true. Cyber crime has become a reality in our modern world.

Let's look at how keeping an accurate and consistent sense of time is critical for many computer-forensic-related activities such as data identification. In other words, being able to investigate incidents that involve multiple computers is much easier when the timestamps on files (identified data) and in logs are in sync.

Timekeeping:- It seems that, although every computer has a clock, none of them appear to be synchronized— unless the computer in question is running the Network Time Protocol (NTP). With NTP, you can synchronize against truly accurate time sources such as the atomic clocks run by the National Institute of Standards and Technology (NIST), the U.S. Naval Observatory, or counterparts in other countries around the world.

NTP began as a tool that permitted researchers to synchronize workstation clocks to within milliseconds or better. With the growth of the Internet, the mechanisms that enabled NTP clients and servers to securely exchange time data have gone from sufficiently secure to not nearly secure enough. Newer versions of NTP fixed the problem by providing a model for automatic

configuration and key exchange. Let's take a look at time-synchronization systems, and how you can securely use them to set all your clocks accurately.

Time Matters:- Why bother having accurate clocks? Isn't the one that comes in your desktop PC or your enterprise server adequate? The answer is that accurate timekeeping is an advanced science, an avocation practiced by hundreds of scientists around the world, and the paltry clock chip you have in your PC or expensive server winds up being a bit less accurate than your SwatchR watch for several reasons. Computer clocks, like most electronic clocks, detect the oscillations of a quartz crystal and calculate the passing time based on these oscillations. Not all quartz crystals are the same to begin with, but put one inside a nice, hot computer that's cool whenever it's turned off, and the crystal's frequency tends to wander. Also, UNIX systems base their notion of time on interrupts generated by the hardware clock. Delays in processing these interrupts because UNIX system clocks to lose time slowly, but erratically. These small changes in timekeeping are what time scientists call *jitter*.

Over time, scientists and programmers have developed different techniques for synchronizing clocks over TCP/IP or other network protocols. The time protocol provides a server's notion of time in a machine-readable format, and there's also an Internet Control Message Protocol (ICMP) timestamp message. Though these remain available Internet standards, neither is currently sufficient for accurate timekeeping, and, hence, both are considered out-of-date.

An NTP support more than 15 stratums, but being closer to the top implies being closer to the most accurate source of time. To improve each server's notion of time, servers in the same stratum may peer (that is, act as equals) and perform the same timestamp exchanges done by NTP clients. NTP servers and clients don't blindly accept another system's notion of time, even if it comes from a higher stratum.

Clock Filters:- Automatically accepting another system's statement about the current time can be harmful: suppose the timekeeping system has been taken over by an attacker who needs to turn back the clock so that a replay attack can function. NTP guards against this in several ways. First, NTP assumes that time moves forward, not backward, although small backward changes are acceptable. Also, if a system has been using NTP, the NTP software assumes that changes in a local clock will be small, generally less than a second. This makes controlling a local clock or making large changes literally a time-consuming process—even a one-second change is a big deal.

NTP goes beyond this by collecting timestamps from many servers (and peers, if appropriate). NTP maintains a queue composed generally of eight samples and uses carefully crafted algorithms to compute the best approximation of exact time.

For example, the outliers in the sample (the timestamps with the largest divergence) are discarded. The remaining set of samples is then used to calculate what the local clock should read.

Auto key:- Using public key cryptography for signing timestamps is just too slow. Public key encryption algorithms aren't only slow (compared to private key algorithms such as RC4), they're also inconsistent in that the amount of time used to encrypt may vary by a factor of two—something very unpleasant for those obsessed with keeping accurate time. Using the list of key ids reduces the need for public key encryption to once an hour on average.

Forensic Identification and Analysis of Technical Surveillance Devices:-
It was one sentence among hundreds in a transcription of a dull congressional hearing on the environment, a statement anyone might have missed: Bristol-Myers Squibb Co. was looking to increase its harvest of the Pacific yew, a protected tree. However, the competitive intelligence (CI) officer at arch rival SmithKline Beecham Corp., happened to catch it, thanks to a routine search of competitors' activities on the Web. The intelligence officer sprang into action. He knew Bristol-Myers' researchers had been testing a substance in the tree's bark as an experimental agent against breast cancer.

But why was Bristol-Myers suddenly seeking to cut down 200 times as many yews? Was it ready to put its planned anticancer drug, Taxol, into production? Back at SmithKline headquarters in Philadelphia, the news was enough to trigger serious nail-biting in the boardroom.

The intelligence officer's team wasted no time. It immediately began canvassing conferences and scouring online resources for clues. It tapped into Web sources on the environment and got staffers to work the phones, gathering names of researchers working for Bristol-Myers. It even zeroed in on cities where Bristol-Myers had sponsored experimental trials of the substance.

Information Overload:- The growing information glut makes it critical for CIOs to start thinking about how they can support their company's CI snoopsters and do it with as much zeal and imagination as they already apply to building hacker-proof security systems. Most existing systems and organizations are still ill-equipped to keep pace with the evergrowing amount of information available. Many companies are still stumbling to process and respond to competitive information as fast as it pours in. The result is that the key to carving out the leading edge of the knowledge gap in one's industry (the difference between what you know and what your rival knows) lies in the ability to build IT systems that can scope out the movements of corporate rivals in real time. IT-aided intelligence gathering is so critical that entire industries will be redefined by the companies most skilled at snooping. Players unable to surmount their bureaucratic inertia will find their existence threatened.

The goal is to tie technology and business together in a common pursuit of becoming more competitive and responsive to rivals and customers in the marketplace. CI is to a company what radar is to an airplane. Companies are now installing radar in the corporate cockpit, and that's where the CIO comes in.

Companies that ignore the CIO do so at their peril. Recently, that happened to a large telecom equipment maker with 30,000 home pages on its supply-chain intranet. Several hundred of the home pages were dedicated to the

competition, but there was no coordination between home pages. This was a situation where the CIO could have taken charge and made sure the information was in one spot. How many tens of millions of dollars were thrown at that intranet and wasted annually in inefficient man-hours?

Building Teams:- You need to build teams with diverse membership. People who understand the concept of organizing information and indexing it could be paired with someone who understands different technology capabilities, such as a relational database showing connections between different terms or items. As managers, CIOs have to amass different strengths on a CI project so they don't have an abundance of hammer holders who look only for nails.

However, don't get carried away on the technology. A few years ago, a study conducted by Fuld & Company [1] found flaws with many of the 170 software packages with potential CI applications. None of them were able to take companies through the process of data identification, discovery, distribution, and analysis. Each did some part of the process, but not the whole thing. The thinking machine has not yet arrived. No company should buy a software package in the hope it will build an intelligence process for the corporation. CIOs need to help build that. It won't come off the shelf. In other words, in this business, you need to be aggressive. Take the offensive. Always recall the words of ancient Chinese general Sun Tzu (6th–5th century B.C.): "Be so subtle that you are invisible, be so mysterious that you are intangible; then you will control your rival's fate."

RECONSTRUCTING PAST EVENTS:-

The increase in computer-related crime has led to the development of special tools to recover and analyze computer data. A combination of hardware and software tools has been developed using commercial off-the-shelf utilities integrated with newly developed programs. Procedures have been defined and implemented to protect the original computer data. Processes have been developed to recover hidden, erased and password protected data. To that

end, all recovery and analysis work is performed on image copies of the original.

Because there is a wide variety of computers, peripherals, and software available, including many different forms of archival storage (Zip, Jaz, disk, tape, CDROM, etc.) [1] It is important that a wide variety of equipment be available for recovery and analysis of evidence residing on a computer's hard disk and external storage media. Recovered data must be analyzed, and a coherent file must be reconstructed using advanced search programs specifically developed for this work.

For example, these techniques were recently used to recover data from several computers that indicated a large check forgery ring was in operation throughout California and personal and business identities were being stolen without the knowledge of the victims. Case files going back over five years were cleared with the information obtained.

How to Become A Digital Detective:- Recovering electronic data is only the beginning. Once you recover it, you need to determine how to use it in your case. In other words, how do you reconstruct past events to ensure that your findings will be admissible as evidence in your case? What follows are some recommendations for accomplishing that goal.

Convert Digital Evidence:- Before you can reconstruct past events and present the data, you need it on a medium and in a format you can work with. In other words, you need to get the data onto a medium you can use, if it is not already on one. Today, data can come on a variety of media, such as holograms, video, data tapes, Zip disks, CD-ROM disks, and even 3.5-inch floppy disks.

For example, you could use Zip disks. Zip disks are simpler. The cost of Iomega Zip drives (*http://www.iomega.com/global/index.jsp*) is so low that you can keep one on hand just to copy data from Zip disks you receive (and to copy data to Zip disks when others request data from you on that medium). CDs are even simpler, as CD drives have become commonplace on PCs. Similarly, even 3.5-inch disks generally pose no problem.

Useable File Formats:- Even if the data is in a format that appears to be one you already use, conversion still may be necessary. The format may be too new. The problem is a basic one. In a similar vein, you may have to get the data converted if it comes to you in a format that is too old or runs on a different operating system.   Although   simple   files   created   with   one company's software generally can be opened without a problem using a competitor's comparable product, this often does not hold true for more complex files.

Unusable File Formats:- You may get electronic data in a format that you cannot use "out of the box." When that happens, you have to convert the files to a format you can use—or find someone to do the conversion for you. You may have already encountered these issues with a variety of files including email files, database files from mainframe systems, and ".txt" files containing data dumped from database files.

For example if you receive a ".txt" file that appears to contain information from a database file, try to find out, among other things, the make and model of the computer the file came from; the name and version of the operating system the computer ran; the name and version of the database program used; the name of the database file; a list of all fields in the database; and descriptions of each field with the descriptions including the type, length, and other characteristics of the field.

Converting Files:- If you are going to attempt converting the data yourself, you may be fortunate enough to have received electronic data that you can covert directly into programs such as Access or Excel using the wizards built into those programs. This can be the case with ".txt" files. Sometimes the first line in a file you are converting may even contain the names of the fields that need to be created, further simplifying your task. If that information is not in the file, then try to get the field names and descriptions from the producing party. Should you fail at that, you may have an exceedingly difficult time carrying out a meaningful conversion.

  ✓ Get the Right Software, Hardware, and Personnel

- ✓ Did You Get All the Data?
- ✓ Did the Evidence Come from the People You Thought It Would?
- ✓ Look for "Hidden" Data
- ✓ Test the Data
- ✓ Work the Evidence

FIGHTING AGAINST MACRO THREATS:-

Information warfare (IW), or sneak electronic assaults, could easily crash power grids, financial networks, transportation systems, and telecommunications, among other vital services. The National Security Agency (NSA) traces the macro threat from hostile or potentially hostile governments as well as drug lords, criminal cartels, and increasingly computer-savvy guerrilla groups. Some of these rogue organizations are doing reconnaissance today on U.S. networks, mapping them, and looking for vulnerabilities.

Is the U.S. Government Prepared for Information Warfare?

The answer is a resounding "no." A reasonable question that should be asked is "Why are we vulnerable?" In a recent report, the Defense Science Board Task Force on Information Warfare, lays the blame at the U.S. government's own doorstep.

The reality is that the vulnerability of the Department of Defense (and of the nation) to offensive IW attack is largely a self-created problem. Program by program, economic sector by economic sector, the U.S. government has based critical functions on inadequately protected telecomputing services. In aggregate, the U.S. government created a target-rich environment, and U.S. industry has sold globally much of the generic technology that can be used to strike these targets.

Recently, for example, a private security company alerted the FBI that it found a malicious program on some 3,000 computers that could be remotely activated to launch an attack on a site of choice—a trojan horse.

From an IW perspective, there are three primary targets for the attacker using psychological operations (psyops). The attacker can focus on the

enemy, those who are friendly to his or her cause, or those who are neutral, with each target chosen for a specific purpose. If the attacker is simply a hacker, cracker, or script-kiddie, it might be for nothing more than to grab a credit card number or prove to friends that he orshe could do it.

Education, not legislation, is the key component. The U.S. government can pass all the laws it wishes, but it won't affect the traffic that is coming out of countries such as Korea, China, and Singapore. The government needs to communicate these messages with intelligence. If the U.S. government knows what needs to be done and doesn't communicate it effectively, then whatever else it does is irrelevant. If the government scatter shots their communications without filtering them through an understanding of the message they need to convey, then all they are sending out is noise.

Are other Governments Prepared for Information Warfare?

Are other governments ready to use information-age tricks against their adversaries?

Yes, to some extent. Case in point is as follows:

At first, the urgent phone call from the U.S. Transportation Department confounded Cheng Wang, a Long Island–based webmaster for Falun Gong, the spiritual movement that has unnerved Chinese authorities. Why did the department think his computers were attacking theirs? The answer turned out to be startling. The electronic blitz hadn't come, as it seemed, from various Falun Gong Internet sites.

Rather, someone had lifted their electronic identities. Computer sleuths followed a trail back to the XinAn Information Service Center in Beijing— where an operator identified it as part of the Ministry of Public Security, China's secret police.

What Industry Groups have done to Prepare for Information Warfare?

On December 18, 2000, the National Security Council held the first meeting of the recently formed Cyber incident Steering Group, aimed at fostering cooperation between private industry and government to secure systems from domestic and international cyber attack. This meeting was an

important first step in building computer security programs for the nation. Among topics discussed were the creation of a rapid response system and communications between industry and government.

Doomsday Software:-

FBI Fingers China:- Many unnamed countries are developing technologies (previously discussed) to complicate what the U.S. military refers to as "power projection" and to undermine morale at home. The interagency, FBI-led National Infrastructure Protection Center, uses a slide depicting China's Great Wall in its standard presentation on cyberthreats, along with a quote from Sun Zi, author of a treatise on war in about 350 B.C.

Strategic Diplomacy and Information Warfare:- Strategic diplomacy, according to the Department of Defense, is the "art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat."

New tools and technologies for communication have created the potential for a new form of psychological warfare to a degree imagined only in science fiction. This new form of warfare has become known as information warfare (IW). In other words, the United States armed forces need to develop a systematic, capstone concept of military knowledge and diplomatic strategy. Such a strategy would include clear doctrine and a policy for how the armed forces will acquire process, distribute, and project knowledge.

Fictive or fictional operational environments, then, whether mass-targeted or niche-targeted, can be generated, transmitted, distributed, or broadcast by governments or all sorts of other players through increasingly diversified networks. The niche-manipulation potential available to states or private interests with access to the universe of internetted communications, such as the networks over which business, commercial, and banking information are transmitted could easily provoke financial chaos. The target state would not know what had happened until too late. Direct satellite broadcast to selected

cable systems [5], analogous to central control of pay-per-view programs, again offers the potential for people in one province or region of a targeted state to discover that the highest level of their leadership has decided to purge their clansmen from the army. To put it in the jargon of the info warriors, info-niche attack in an increasingly multisource fictive universe offers unlimited potential for societal-level net war.

Strategic Diplomatic Implications:- The tools, techniques, and strategy of cyber war will be developed and, during wartime, should be employed. In many ways, cyber war is more demanding than net war, but the resources, organization, and training needed for cyber war will be provided once it's war-winning, and casualty-reducing, potential is grasped by the national political leadership. Such a development would certainly be prudent. On the other hand, many of the tools and techniques of battlefield cyber war can be applied to net war or strategic-level IW. This application may not be prudent; however, as there are serious reasons to doubt the ability of the United States to prosecute information war successfully.

Info sphere dominance (controlling the world of information exchange) may be as complex and elusive as escalation dominance appeared to be in nuclear strategy. It will certainly be expensive: the U.S. business community and the U.S. armed forces are required to devote ever more resources and attention to computer, communications, and database security. The resources and skills required for battlefield cyber war are not insignificant, but the resources and skills required to wage an information war at the national strategic level would be massive.

The Role of International Organizations:- Information on countries with offensive IW initiatives is less authoritatively documented, but studies and foreign press reporting help point to international organizations that probably have such an initiative under way. A 1996 U.S. General Accounting Office (GAO) report on the threat to Defense D systems (otherwise known as Defense DARPA [Defense Advanced Research Projects Agency] systems) stated that the Department of Energy and the National Security Agency estimated that 120 countries had established computer

attack capabilities. At the low end, in June 1998, the director of central intelligence stated that several countries are sponsoring IW programs and that nations developing these programs recognize the value of attaching their country's computer systems—both on the battlefield and in the civilian arena.

TABLE 13.1 Publicly Identified Foreign Countries Involved in Economic Espionage, and Information Warfare: Initiatives and U.S. Remediation

Country	Economic Espionage	Information Warfare Initiative	Major Remediation Provider
Belarious	Yes	–	–
Bulgaria	Yes*	Yes	–
Canada	Yes*	Yes	Yes
China	Yes*	–	–
Cuba	Yes*	Yes	Yes
France	Yes*	Yes	Yes
Germany	Yes*	Yes	Yes
Hungary	Yes	–	–
India	Yes*	Yes	Yes
Iran	Yes*	Yes	Yes
Ireland	–	–	Yes
Israel	Yes*	Yes	Yes
Japan	Yes*	–	–
Moldavia	Yes	–	–
Pakistan	Yes	–	Yes
Philippines	Yes	–	Yes
Poland	Yes	–	–
Romania	Yes	–	–
Russia	Yes*	Yes	–
North Korea	Yes*	–	–
South Korea	Yes*	–	–
Taiwan	Yes*	–	–

*Countries identified by NCS as using electronic intrusions usually for economic espionage purposes.

All of these countries publicly acknowledge pursuing defensive IW initiatives to protect their military information capabilities or national information infrastructure:

India established a National Information Infrastructure-Defensive group several years ago, apparently in response to China's growing interest in IW.

As recently as January 2001, the Israel Defense Forces (IDF) acknowledged the existence of an IW defense unit whose mission is to protect military systems, but noted that the electric utility had organized its own defense.

Taiwan also recently announced the creation of a task force to study ways to protect their information infrastructure from the growing IW threat from China.

Creation of a national defensive information infrastructure program is a good (and probably necessary) indicator of an international offensive IW initiative. Defensive measures (deterrence, protection, and restoration) are difficult to implement without also developing an understanding of potential adversaries, investing in computer and software development, and creating a major operational capability— all steps directly applicable to creating an offensive IW capability.

The Role of Global Military Alliances:- The following discussion highlights what actually constitutes global military alliances with regard to information operations. Three terms are examined: military, information, and operations.

Military:- A look into the future of IW indicates an increasing role for information operations and the emergence of IW as a new paradigm of warfare. Global military planners must, therefore, prepare to develop information skills and strategies as part of their immediate capabilities and, ultimately, they must prepare their force for involvement in full-scale information wars through alliances with other countries. These global planners must also remember that IW is emerging as a paradigm of warfare, not a paradigm of information. Regardless of the extent that the IW paradigm influences the future warfare environment, war will still be war, and thus will still involve the human factors that have been associated with conflict since the dawn of time.

Global Information:- Although seemingly self-explanatory, understanding the nature of global information alliances is important. Information is the product of the processing of data, whereas data is simply the product of some observation. The processing of data into information involves placing the data into some context. This context can be the formation of a sentence or other human-readable form, a machine-readable sequence, or the classification of the data against some known measurement, such as time, height, weight, and the like.

Global Operations:- Global information operations seek to influence the decision-making process. Global military information operations (MIOs) alliances are not information technology support activities, such as system management and system administration. They are activities directly focused on warfare and include offensive and defensive activities aimed at all levels of the decision-making process. In the modern warfare environment, attacking and defending information technology systems is a vital combat task, and strategies must be considered in conjunction with the wider global military alliances plan. When correctly applied, offensive global information operations alliances can be just as lethal as the employment of conventional

weapons. As an example, certain aircraft flight control systems may be shut down using MIO techniques.

Marshall Law and Cyberspace:-In the Information Age, third wave nations have legitimate aspirations to create a global information system that adds value to their existing information infrastructures. Information technology is cooperative by nature and tremendous benefits can be derived from greater interconnectivity. Therefore, nations will seek out ways to integrate their networks with the international network. Once that integration takes place, each connected nation will have an interest in maintaining the stability and survivability of the overall network. Each nation has a vested interest in preventing global IW and Marshall Law.

Cyberspace has empowered the average person to explore and question the structure of our society and those who benefit from the way it is operated. Fundamental issues arise from hacker explorations. The United States must decide how, as a nation, it wishes to deal with these issues. Recent efforts in cloning produced a human fetus. The scientists who achieved this remarkable feat immediately halted research, arguing that a public debate must arise to deal with the ethical and moral issues surrounding thistechnology. They argued that before experimentation in cloning continued, the United States must decide as a society which direction that the new technology will go, what ends it hopes to achieve, and what the limits on the use of this new technology should be. A similar debate on the issues of cyberspace must take place. There is no need to stop the technology, but the United States must decide what direction it wants the technology to take and what rules will govern the use of this technology. The United States must do this now, before the technology starts dictating the rules—before it is too late to make changes in the basic structure of cyberspace without destroying the whole concept.

The Super Cyber Protection Agencies:- Some might call it paranoia, but the U.S. government is growing increasingly worried that foreign infiltrators are building secret trapdoors into government and corporate networks with the help of foreign-born programmers doing corporate work—their regular

jobs. A CIA (or Super Cyber Protection Agency [SCPA] as they are called now) representative recently named Israel and India as the countries most likely to be doing this because they each handle a large amount of software repair not done by U.S.-born workers. According to the CIA, these two countries each have plans to conduct information warfare, and planting trapdoors wherever they can would be a part of that. As previously explained, IW is a nation's concerted use of network hacking, denial-of-service attacks, or computer viruses to gain access to or disrupt computer networks, now the heart of modern society in terms of banking, telecommunications, and commerce.

TACTICS OF THE MILITARY:-

The growing reliance on computer networks makes the networks themselves likely sites for attack. What is more, civilian and military networks are becoming increasingly intertwined, so the U.S. military's focus has shifted from protecting every network to securing mission-critical systems. Current efforts include software agent–based systems (for real-time detection and recovery from a cyber attack) and network-level early-warning systems (for monitoring suspicious online activity). As tensions continue to mount in the Middle East because of the continued occupation of U.S. forces in Iraq and the recent death of Palestinian leader Yasser Arafat, a different sort of pitched battle is being waged behind the scenes. With all the fervor of their comrades in arms, computer-savvy patriots on both sides have managed to infiltrate and disable enemy Web servers.

The prospect of cyber warfare, or information warfare (IW), is a deadly serious matter in military circles. The electron is the ultimate precision-guided weapon. Indeed, the more heavily we come to rely on computer networks, the greater the fear that adversaries will attack the networks themselves. In the very worst case (what some have termed an electronic Pearl Harbor) a sudden, all-out network assault would knock out communications as well as financial, power, transportation, military, and other critical infrastructures, resulting in total societal collapse.

Renegotiating the Human–Machine Interface:- Creating inherently secure and robust information technologies for the U.S. military is one of the chief aims of the information technology systems (ITS) office at DARPA, in Arlington, Virginia. The work at the DARPA ITS office is defensive, rather than offensive, in nature. They are like the people who worry about seatbelts in cars, rather than the designers of large, fast engines.

Agent-Based Systems:- Software agents are defined very broadly: enabling real machine-to-machine communications, allowing machines to understand content, send messages, do negotiations, and so on. DARPA agent markup language (DAML) is a fairly large project to create a next-generation Web language, a successor to extensible markup language (XML). It's aimed at semantic interoperability—to make more of what's online machine readable. Right now, when a machine gets to a Web page, it sees natural language, photos, and so on, none of which are easy for machines to process. You can't ask it to do a content-based search for you, because it can't understand the content.

Overview of Military Tactics:- The planning, security, and intelligence considerations of military information warfare tactics (MIWT) must be present in all aspects of the military information operations (MIO) development process. These issues are fundamental to the success of MIWT.

Planning:- MIWT operations, like most operations, can only be effective when adequate attention is given to the overall objective to which they are being applied. Developing an MIWT strategy requires careful adherence to planning philosophies, starting with the development of an achievable goal. The main objective of planning is to ensure that information operations within the MIWT environment are focused on the wider military strategies and, therefore, the security objectives of the nation. This requires the development of formalized planning procedures.

Security:- Military operations are most effective when they surprise an enemy. Surprise can only be achieved when security procedures deny enemy access to friendly intentions, strategies, and capabilities. This applies to the MIWT environment as much as it does to any other discipline of warfare.

Security, therefore, must be considered throughout an MIWT program. The integrity of friendly software, hardware, communications, procedures, people, and strategies is an essential part of the MIWT environment. Developing a detailed strategy for information operations is pointless if that plan is known to enemy forces.

Intelligence:- Intelligence provides IW practitioners with assessments of an enemy's ITS and their likely reactions, both human- and machine-directed, following the commencement of an information attack. ITS are dynamic and their configuration can be changed with minimal effort. Planning attacks against such systems requires refinement in response to such changes, often at the last minute and occasionally during an attack. Accordingly, employment of successful MIWT strategies demands comprehensive and real-time intelligence support.

Offensive Ruinous IW Tools And Tactics:- The U.S. military has a new mission: Be ready to launch an offensive ruinous cyber attack against potential adversaries, some of whom are stockpiling cyber weapons. Such an attack would likely involve launching massive distributed denial-of-service assaults, unleashing crippling computer viruses or trojans, and jamming the enemy's computer systems through electronic radio-frequency interference.

A few of years ago, an order from the National Command Authority (backed by President Bush and Secretary of Defense Colin Powell) instructed the military to gear up to wage cyber war. The ability of the United States to conduct such warfare still doesn't exist today.

The military sees three emerging threats: ballistic missiles, cyber warfare, and space control. The U.S. Space Command, the agency in charge of satellite communications, has begun to craft a computer network attack strategy. This strategy would detail actions to be followed by the Unified Commanders in Chief (CINC) if the president and the secretary of defense order a cyber strike. The CINCs are senior commanders in the Army, Navy, Air Force, and Marines, deploying U.S. forces around the world.

Offensive Containment IW Tools and Tactics:- Countries like Australia, however, like most non-superpower nations of the world, will not be able to commit the substantial resources needed to follow the American model.

C2W is the war-fighting or tactical application of MIWT and is usually aimed at a specific and defined battlespace, although it may be conducted in conjunction with other MIWT that may be focused on strategic information targets. There are five elements of C2W, covering both offensive and defensive applications:

- ✓ Operations security
- ✓ Military deception
- ✓ Psychological operations
- ✓ Electronic warfare
- ✓ Targeting

Defensive Preventive IW Tools And Tactics:- Eight years after the military pioneered intrusion detection systems, the DoD now requires its massive networked systems to be protected by round-the-clock intrusion detection monitoring to defend against hacker and denial-of-service attacks. The DoD has developed a policy that mandates the use of intrusion detection systems in all military networks. The DoD has more than 69,000 computer networks that handle everything from weapons systems C2 to inventory to payroll. Roughly 15% of DoD networks, such as satellite links, are considered mission-critical.

Under this draft policy, every DoD entity needs to have a computer networkdetection service provider, which could be a DoD entity or a commercial entity. Thus, the Defense Information Systems Agency (DISA) is responsible for defining the intrusion detection plan. Whether the Navy, Army, or Air Force should buy commercial intrusion detection software or entrust network protection to an outside service provider should be decided on a case-by-case basis. The military helped pioneer intrusion detection systems by building its own software from scratch in 1996. Since then, various parts of the military have deployed products from vendors that include Internet Security Systems, Symantec, Cisco [3], and Network Ice.

Today, still only a small percentage of the military's overall networked systems are guarded by any form of intrusion detection. When
the final decision on the mandatory intrusion detection systems will arrive is still unclear, but deliberations taking place among the military's Joint Chiefs of Staff underscore their determination to do whatever it takes to prevent hackers and denialof- service attacks from disrupting its networks.

Defensive Ruinous IW Tools And Tactics:- Information operations has emerged as an area that is extremely well suited to the integration of reserve capabilities. Members of the reserves and National Guard are often way ahead because of the very nature of their civilian employment, trained in their workplaces to exploit technology. The DoD has long been battling a high-tech brain drain spurred by a booming economy and the lure of higher-paying jobs in the private sector. The change has made the National Guard and reserves a repository of high-tech skills. At the same time, the Pentagon is facing an increase in cyberattacks and intrusions and has increased its focus on using cybertactics to fight future conflicts. The teams could be involved in a wide range of efforts, including enemy computer network attacks, defense of U.S. critical infrastructures, psychological operations, intelligence support, vulnerability assessments, and reviews of Pentagon Web sites for sensitive information.

Defensive Responsive Containment IW Tools And Tactics:- One of the more recent additions to the military commander's toolbox are defensive responsive containment IW tools. Computers and associated technology have helped change the face of modern information warfare tactics by providing the capabilities to generate and process massive amounts of data and disseminate the resultant information throughout the battlespace. However, computers provide more than just an information-processing capability. They may also be used as weapons in their own right. The most common examples of computer operations include hacking, virus planting, and chipping. These techniques are primarily aimed at targeting the enemy's broad information environment. However, they may also be used to attack the enemy's computer-based weapon systems and computer-based

platforms, such as "fly-by-wire" aircraft. Although generally strategic in nature, computer operations may be applied to the tactical and operational components of the conventional warfare environment, either in support of C2W operations or in direct support of air, land, or sea operations.

1. Hacking

2. Viruses

3. Chipping

Countering Sustained Terrorist IW Tactics:- Terrorism is, among other things, a weapon used by the weak against the strong. The United States has moved into the 21st century as a preeminent, global power in a period of tremendous flux within societies, among nations, and across states and regions. Terrorism will accompany changes at each of these levels, as it has in other periods of flux in the international environment. To the extent that the United States continues to be engaged as a global power, terrorism will have the potential to affect American interests directly and indirectly, from attacks on U.S. territory (including low-probability but high-consequence "superterrorism" with weapons of mass destruction) to attacks affecting the United States diplomatic and economic ties abroad or the United States ability to maintain a forward military presence or project power in times of crisis.

Where societies and regions are fundamentally unstable, and where political outcomes are delicately poised, terrorism will have a particular ability to affect strategic futures.

Dealing With Random Terrorist IW:- During the 1970s and 1980s, political extremism and terrorism frequently focused on "national liberation" and economic issues. The collapse of the Soviet bloc and the end of its covert funding and encouragement of terrorism led to a decline in the militant and violent left-wing terrorist groups that were a feature of the age. The 1990s through the present have seen the development of a new terrorism: random terrorist IW. This is not to say that state-backed terrorism has ceased, but rather that the spectrum of terrorism has widened. This new extremism is frequently driven by religious fervor, is

transnational, sanctions extreme violence, and may often be millenialist. The new terrorism may seek out military or government targets, but it also seeks out symbolic civilian targets, and the victims have mostly been innocent civilians (Alfred P. Murrah Building, Oklahoma City; World Trade Center, New York; AMIA Headquarters, Buenos Aires; etc.).

Cyberspace is becoming a new arena for political extremists: the potential for physical conflict to be replaced by attacks on information infrastructures has caused states to rethink their concepts of warfare, threats, and national assets at a time when information is recognized as a national asset. The adoption of new information technologies and the use of new communication media, such as the Internet, create vulnerabilities that can be exploited by individuals, organizations, and states.

TACTICS OF TERRORIST AND ROGUES:-

The information warfare (IW) arsenal and tactics of terrorists and rogues have become increasingly transnational as the networked organizational form has expanded. When terrorism's mentors were the Soviet Union and the Eastern Bloc, they imposed their own rigid hierarchical structure on terrorist groups. Now that terrorism is increasingly substate, orsemidetached, networking and interconnectivity are necessary to find allies and influence others, as well as to affect command and control.

An analogy, using the Palestinian example, may be that the more networked form of Hamas now that Arafat is dead, is replacing the hierarchical structure of the PLO. In many ways the Afghan War was a seminal event in promoting the networked form in that it showed that fluidly organized groups, driven in this case by a religious imperative, could defeat an experienced hierarchically structured army.

Bin Laden Uses Web to Plan:- Osama bin Laden and other Muslim extremists are using the Internet to plan more terrorist activities against the United States and its allies. Recently, U.S. law enforcement officials and other experts disclosed details of how extremists hide maps and photographs of terrorist targets in sports chat rooms and on pornographic bulletin boards and other popular Web sites. Instructions for terrorist

activities also are posted on the sites, which the officials declined to name. To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden's al Qaeda, are using computerized files, email, and encryption to support their operations—like the train bombing in Madrid in the winter of 2004. According to various unnamed officials and investigators, the messages are scrambled using free encryption programs set up by groups that advocate privacy on the Internet. It's something the intelligence, law-enforcement, and military communities are struggling to deal with. The operational details and future targets, in many cases, are hidden in plain view on the Internet. Only the members of the terrorist organizations, knowing the hidden signals, are able to extract the information.

The Terrorist Profile:- Sid-Ra, a 6-foot-4-inch, 350-pound giant of a man, paces between his "subjects" in the smoke-filled Goth club Click + Drag, located in the old meat-packing district of Manhattan. Inside the club are leather-clad, black-lipped females and young men dressed in women's underwear. Sid is a hacker-terrorist and an acknowledged "social engineer" with curious nocturnal habits. There are thousands of people like him, who by day care system and network administrators, security analysts, and startup cofounders. When night comes, they transform into something quite different. Is this the profile of a "wanna-be" terrorist? Perhaps! These are the selfproclaimed freedom fighters of cyberspace. They even have a name for it: hactivism. Political parties and human rights groups are circling around to recruit hactivists into their many causes. Recently, for example, the Libertarian Party set up a table at the HOPE (Hackers on Planet Earth) conference. The San Francisco− based Electronic Frontier Foundation (EFF) collected donations, and members of civil-rights groups, including the Zapatistas, a Mexican rebel group, spoke up at one of two sessions on hactivism.

From Vietnam Marches to Cyberdisobedience:- Like any social engineer, Sid exaggerates. Except for the four-year jail terms handed down to Kevin

Mitnick and Kevin Poulsen, sentencing for even criminal hacking in 2003–2004 has been relatively light (mostly probation and fines) because of the suspects' young ages.

Hackers question conventional models. They don't just look at technology and say, "This is how it works." They say, "How can I make it better?" They look at society that way too—their government, their schools, and their social situations. They say, "I know how to make this better," and they go for it. In the Motion Picture Association of America (MPAA) case, staffers at 2600 Enterprises Inc., based in Middle Island, New York, were threatened with imprisonment if they didn't remove a link on the 2600 Web site to the code used to crack DVD encryption. Because the link was editorial content, it set Sid off on another diatribe. The Libertarian Party also recruits hackers and technologists. At HOPE, the party's New York State committee (http://www.cownow.com) handed out fliers, signed up recruits, and took a "sticker" poll of party affiliations. The poll got hacked, but about half the stickers were yellow—for libertarian, anarchist, or independent. Many party members are programmers

Why Terrorists and Rogues have an Advantage In IW:- Governments have neither the financial resources nor the technical know-how to stay on top of hackers and computer terrorists. This is why terrorists and rogues have an advantage in IW. The private sector must itself take much of the action that is necessary to prevent attacks being made on the Internet. It's no longer possible for governments to provide the resources and investment necessary to deal with these kinds of issues.

There are no cookie-cutter solutions; every network is different. At the top of chief information officers (CIOs) lists of concerns is denial of service (DoS) attacks, which recently brought Yahoo, Amazon.com, eBay, and other high-profile Web sites to their knees. DoS attacks are a key concern because the only way that is currently available to prevent them is to catch the perpetrators.

Solutions seem harder to come by today than solutions to the problems just discussed. Governments, businesses, and research institutions must band together to find the best technologies and courses of action to defeat cyber crimes. Companies must be more willing to invest in security systems to protect their networks. A few of these companies called on software companies and service providers to make their products more secure. Default settings for software products sold to consumers should be at the highest level of security. You wouldn't build a swimming pool in the center of town and not put a fence around it. Basically, that's just what the software companies are doing.

Although security firms have financial incentives for promoting security issues, for the average corporation, the benefits of spending millions of dollars to bolster security in networks aren't immediately obvious, thus making them slow to act. If you have a choice of spending five million dollars on getting 693,000 new customers, or five million dollars on better serving the ones you already have, that's a difficult value proposition. Most companies would take the additional customers. The severity of attacks could get worse, though, and businesses would be wise to make precautionary investments now. Most businesses have been lucky so far.

The Criminal Café in Cyberspace:- Not long ago, if a terrorist wanted to cause a blackout in, say, New York, it would have taken some work. He or she might have packed a truck with explosives and sent it careening into a power plant. Or he or she might have sought a job as a utility worker to sabotage the electrical system.

In a closed briefing to Congress, the CIA reported that at least a dozen countries, some hostile to America, are developing programs to attack other nations' information and computer systems. China, Cuba, Russia, Korea, and Iran are among those deemed a threat, sources later declared. Reflecting official thinking no doubt, the *People's Liberation Daily* in China noted that a foe of the United States only has to mess up the computer systems of its banks by high-tech means "Eligible Receiver" culminated

when three two-person "red teams" from the National Security Agency used hacker techniques that can be learned on the Internet to penetrate DoD computers. After gaining access to the military's electronic message systems, the teams were poised to intercept, delete, and modify all messages on the networks. Ultimately, the hackers achieved access to the DoD's classified network (see sidebar, "Espionage By Keystroke?") and, if they had wished, could have denied the Pentagon the ability to deploy forces. In another exercise, the DoD found that 74% of test attacks on its own systems went undetected.

Sabotage:- Sophisticated hackers, meanwhile, are breaking into sensitive Chinese computers (see sidebar, "Cyberspace Incidents on the Rise in China"). Members of the Hong Kong Blondes, a covert group, claim to have gotten into Chinese military computers and to have temporarily shut down a communications satellite last year in a hacktivist" protest. The ultimate aim is to use hacktivism to ameliorate human rights conditions.

The Super Computer Literate Terrorist:- During the next 20 years, the United States will face a new breed of Internet-enabled terrorists, super computer literate criminals, and nation-state adversaries who will launch attacks not with planes and tanks, but with computer viruses and logic bombs. America's adversaries around the world are hard at work developing tools to bring down the United States' private sector infrastructure. The United States faces an increasingly wired but dangerous world, as evidenced by the following:

1. Many countries have programs to develop cyberattack technologies and could develop such capabilities over the next decade and beyond.

2. The Unites States, Russia, China, France, and Israel are developing cyberarsenals and the means to wage all-out cyberwarfare.

3. Terrorist groups are developing weapons of mass destruction.

4. Russia has become a breeding ground for computer hackers. The Russian equivalent of the U.S. National Security Agency and organized crime groups recruit the best talent.

5. Electronic stock scams, robberies, and extortions are proliferating.

The other important topics to be discussed as follows.

- ✓ The brilliant and nasty rouge
- ✓ How they watch and what they know
- ✓ How and where they get their tools
- ✓ Why tools are easy to get and use
- ✓ Why nasty people are so hard to track down and capture
- ✓ What they will do next-the information warfare games

TACTICS OF PRIVATE COMPANIES:-

Surviving Offensive Ruinous IW:-

Sendmail program:- Installation of a malicious code in an email message sent over a network machine. As the sendmail program scans the message for its address, you will execute the attacker's code. Sendmail operates at the system's root level and therefore has all privileges to alter passwords or grant access privileges to an attacker.

Computer-searching programs:- Password cracking and theft is much easier with powerful computer-searching programs that can match numbers or alphanumeric passwords to a program in a limited amount of time. The success depends on the power of the attacking computer.

Packet sniffing:- An attacker inserts a software program at a remote network or host computer that monitors information packets sent through the system and reconstructs the first 125 keystrokes in the connection. The first 125 keystrokes would normally include a password and any logon and user identification. This could enable the attacker to obtain the password of a legitimate user and gain access to the system.

Access: Attackers who have gained access to a system can damage it from within, steal information, and deny service to authorized users.

Trojan horses:- An independent program that when called by an authorized user performs a useful function but also performs unauthorized functions, which may usurp the user's privileges.

Logic bomb:– An unauthorized code that creates havoc when a particular event occurs (for example, the dismissal of an employee).

Surviving Offensive Containment IW:- New technologies that aim to directly strengthen user authentication include the use of tokens and smart cards combined with digital certificates. The most compelling and intriguing authentication technologies involve biometrics matching the measurement of physical and behavioral characteristics such as facial structures, voice patterns, and fingerprints.

To gain widespread acceptance in businesses, multiple individual biometrics methods must coexist in a single-system solution, and the underlying architecture must better support the conditions ofinteroperability, scalability, and adaptability that govern the total cost of ownership calculations. A multitier authentication system built around these notions is one solution.

Many other important topics includes,

- ✓ Participating in defensive preventive information warfare planning.
- ✓ Benefiting from and surviving defensive ruinous information warfare.
- ✓ Benefiting from and surviving defensive responsive containment information warfare.
- ✓ Protection against random terrorist information warfare tactics.
- ✓ What to do when terrorists keep attacking.
- ✓ Countering sustained rogue information warfare protection against random rogue information warfare.
- ✓ Keeping the amateur rogue out of the cyber house.

UNIT - IV

SYLLABUS:- Information warfare: Arsenal – Surveillance Tools – Hackers and Theft of Components – Contemporary Computer Crime-Identity Theft and Identity Fraud –Organized Crime &Terrorism – Avenues Prosecution and Government Efforts –Applying the First Amendment to Computer Related Crime-The Fourth Amendment and other Legal Issues.

ARSENAL:-

Arsenal   is   the   only   weapon   available   to   the   weak   the   terror. Online terror sites concentrate on recruitment and propaganda platforms which deny their strength and their violence Instead, the groups emphasize their own weakness and the vulnerability of the community.

While not openly stated, this approach implies that terroris actions are all that is available in their depleted arsenal.

Digital evidence can be any information stored or transmitted in digital form. All digital evidence is printed out to be presented in court.

► Groups such as the **Scientific Working Group on Digital Evidence** (**SWGDE**) and the **International Organization on Computer Evidence** (IOCE) set standards for recovering, preserving, and examining digital evidence.

► The general tasks investigators perform when working with   digital evidence:

► Identify digital information or artifacts that can   be   used   as   evidence. Collect, preserve and document evidence.

► Analyze, identify and organize evidence.

► Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.

► Collecting computers and processing a criminal or incident scene must be done systematically.

► To minimize confusion, reduce the risk of losing evidence and avoid and avoid damaging evidence, only one person should collect and catalog digital

Evidence at crime scene or lab, if practical.

► If there's too much evidence or too many systems to make it practical for one person to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner should control collecting and cataloging evidence.

► You should also use standardized forms for tracking evidence to ensure that you consistently handle evidence in a safe, secure manner.

► An important challenge investigators face today is establishing recognized standards for digital evidence.

SURVEILLANCE TOOLS:-

1. Laser Ablation Inductively Coupled Plasma Mass Spectrometry (LA-ICP-MS): When broken glass is involved in a crime, putting together even tiny pieces can be key to finding important clues like the direction of bullets, the force of impact or the type of weapon used in a crime. Through its highly sensitive isotopic recognition ability, the LA-ICP-MS machine breaks glass samples of almost any size down to their atomic structure. Then, forensic scientists are able to match even the smallest shard of glass found on clothing to a glass sample from a crime scene. In order to work with this type of equipment in conjunction with forensic investigation, a Bachelor's Degree in Forensic Science is usually necessary.

2. Alternative Light Photography: For a forensic nurse, being able to quickly ascertain how much physical damage a patient has suffered can be the difference between life and death. Although they have many tools at their disposal to help make these calls quickly and accurately, Alternative Light Photography is one of the coolest tools to help see damage even before it is visible on the skin. A camera such as the Omnichrome uses blue light and orange filters to clearly show bruising below the skin"s surface. In order to use this equipment, you would need a MSN in Forensic Nursing.

3. High-Speed Ballistics Photography: You might not think of it right away as a tool for forensic scientists, but ballistics specialists often use high-speed cameras in order to understand how bullet holes, gunshot wounds and glass shatters are created. Virtually anyone, from a crime scene

investigator to a firearms examiner, can operate a high-speed camera without any additional education or training. Being able to identify and match bullet trajectories, impact marks and exit wounds must be done by someone with at least a Bachelor's of Science in Forensic Science.

4. Video Spectral Comparator 2000: For crime scene investigators and forensic scientists, this is one of the most valuable forensic technologies available anywhere. With this machine, scientists and investigators can look at a piece of paper and see obscured or hidden writing, determine quality of paper and origin and "lift" indented writing. It is sometimes possible to complete these analyses even after a piece of paper has been so damaged by water or fire that it looks unintelligible to the naked eye. In order to run this equipment, at least a Bachelors degree in Forensic Science or a Master's Degree in Document Analysis is usually required

5. Digital Surveillance for Xbox (XFT Device): Most people don't consider a gaming system a potential place for hiding illicit data, which is why criminals have come to use them so much. In one of the most ground-breaking forensic technologies for digital forensic specialists, the XFT is being developed to allow authorities visual access to hidden files on the Xbox hard drive. The XFT is also set up to record access sessions to be replayed in real time during court hearings. In order to be able to access and interpret this device, a Bachelor's Degree in Computer Forensics is necessary.

6. 3D Forensic Facial Reconstruction: Although this forensic technology is not considered the most reliable, it is definitely one of the most interesting available to forensic pathologists, forensic anthropologists and forensic scientists. In this technique, 3D facial reconstruction software takes a real-life human remains and extrapolates a possible physical appearance. In order to run this type of program, you should have a Bachelor's Degree in Forensic Science, a Master's Degree in Forensic Anthropology or a Medical Degree with an emphasis on Forensic Examination and Pathology.

7. DNA Sequencer: Most people are familiar with the importance of DNA testing in the forensic science lab. Still, most people don't know exactly

what DNA sequences are and how they may be used. Most forensic scientists and crime lab technicians use what's called DNA profiling to identify criminals and victims using trace evidence like hair or skin samples. In cases where those samples are highly degraded, however, they often turn to the more powerful DNA sequence, which allows them to analyze old bones or teeth to determine the specific ordering of a person's DNA nucleobases, and generate a "read" or a unique DNA pattern that can help identify that person as a possible suspect or criminal.

8. Forensic Carbon-14 Dating: Carbon dating has long been used to identify the age of unknown remains for anthropological and archaeological findings. Since the amount of radiocarbon (which is calculated in a Carbon-14 dating) has increased and decreased to distinct levels over the past 50 years, it is now possible to use this technique to identify forensic remains using this same tool. The only people in the forensic science field that have ready access to Carbon-14 Dating equipment are forensic scientists, usually with a Master's Degree in Forensic Anthropology or Forensic Archaeology.

9. Magnetic Fingerprinting and Automated Fingerprint Identification (AFIS) : With these forensic technologies, crime scene investigators, forensic scientists and police officers can quickly and easily compare a fingerprint at a crime scene with an extensive virtual database. In addition, the incorporation of magnetic fingerprinting dust and no touch wanding allows investigators to get a perfect impression of fingerprints at a crime scene without contamination. While using AFIS requires only an Associate's Degree in Law Enforcement, magnetic fingerprinting usually requires a Bachelor's Degree in Forensic Science or Crime Scene Investigation.

10. Link Analysis Software for Forensic Accountants: When a forensic accountant is trying to track illicit funds through a sea of paperwork, link analysis software is an invaluable tool to help highlight strange financial activity. This software combines observations of unusual digital financial transactions, customer profiling and statistics to generate probabilities of illegal behavior. In order to accurately understand and interpret findings

with this forensic technology, a Master's Degree in Forensic Accounting is necessary.

HACKERS AND THEFT OF COMPONENTS – CONTEMPORARY COMPUTER CRIME:-

Computer Crime: Computers can be involved in a wide variety of crimes including white-collar crimes, violent crimes such as murder and terrorism, counterintelligence, eco- nomic espionage, counterfeiting, and drug dealing. The Internet has made targets much more accessible, and the risks involved for the criminal are much lower than with traditional crime.

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

► Computer can be the target of the crime,

► It can be the instrument of the crime,

► It can serve as an evidence repository storing valuable information about the crime

For example, a hacker may use the computer as the tool to break into another computer and steal files, then store them on the computer. When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role. If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and password files. If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked.

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

The Computer Forensic Priority: - Computer forensics is concerned primarily with forensic procedures, rules of evi- dence, and legal processes. It is only secondarily concerned with computers. There- fore, in contrast to

all other areas of computing, where speed is the main concern, in computer forensics the absolute priority is accuracy. One talks of completing work as efficiently as possible, that is, as fast as possible without sacrificing accuracy.

Lack of Reporting: - Although estimates vary, most experts agree that the vast majority of Fortune 500 companies have been electronically compromised to the tune of at least $10 billion/year. However, early studies indicated that only 17 percent of such victimizations were reported to law enforcement authorities (Center for Strategic and International Studies, 1998). At the same time, number of reported incidents handled by Carnegie-Mellon University (CERT–Computer Emergency Response Team) has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999 (U.S. General Accounting Office, 1998). It does appear that reporting is getting better; a survey of 521 security personnel from American companies, financial institutions, universities and government agencies revealed that 32 percent of respondents reported electronic crime to law enforcement. This represented an increase of 15 percent of the previous study. However, computer intrusion is still vastly underreported.

Traditional Problems Associated with Computer Crime: - Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves non-specialist users (e.g., child pornography, drug dealers, harassment, etc.). In fact, the earliest computer crimes were characterized as non-technological specific. Theft of computer components and software piracy were particular favorites. Hacking and technologically complicated computer crime came later.

Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs.

As such, the law enforcement community has experienced unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display the levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators are ill-equipped to do so.

Physicality and Jurisdictional Concerns: - The physical environment that breeds computer crime is far different from traditional venues. In fact, the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents. For example, what forensic tools are available for identifying entry points in data breaking and entering? Certainly, seasoned investigators recognize the utility of pry mark analysis in home burglaries. But few recognize the how to and what for in abstract, intangible environments.

In many cases, such differences in technique, and even approach, are further complicated by the lack of precautionary boundaries and restraints both physical and virtual. Indeed, the intangibility of such environments creates unlimited opportunities.

The lack of physical boundaries and the removal of traditional jurisdictional demarcations allow perpetrators to commit multinational crime with little fear (or potential) of judicial sanctions. For the first time, criminals can cross international boundaries without the use of passports or official documentation.

Whereas traditional criminal activity required the physical presence of the perpetrators, cybercrime is facilitated by international connections that enable individuals to commit criminal activity in England while sitting in

their offices in Alabama. In addition, electronic crime does not require an extensive array of equipment or tools. It does not require vehicular transportation, physical storage capability, or labor-intensive practices, all of which increase the potential for discovery and enforcement. In addition, this shift from a corporeal environment, where items can be seen, touched, smelled, etc., to a virtual world where boundaries, concrete barriers and physical items are inconsequential, has further insulated the criminal from law enforcement. In fact, the sheer intangibility of crime scenes has all but crippled many criminal investigations.

A further concern regarding the physical intangibility of computer crime involves the traditional lack of cooperation inherent in law enforcement investigations. Issues of funding, political platforms and the like have traditionally reduced communication and cooperation among jurisdictions. These issues are further compounded when international components are considered. The lack of consensus among international entities regarding the criminalization of certain behaviors and the appropriate sanctions associated with same often negate cooperative agreements.

Perceived Insignificance and Stereotypes: - Investigators and administrators have displayed great reluctance to pursue computer criminals. A lack of knowledge coupled with general apathy towards cyber-criminality has resulted in an atmosphere of indifference. Many stereotype computer criminals as non-threatening, socially challenged individuals (i.e., nerds or geeks), and fail to see the insidious nature of computer crime. The potentiality of weapons and narcotics trafficking, conspiracies of mass destruction, and the like are all but alien to those individuals not actively involved in computer investigations. In addition, those administrators and investigators who grudgingly admit the presence and danger of electronic crime tend to concentrate exclusively on child pornography, overlooking motivations and criminal behaviors apart from sexual gratification. Unfortunately, these perceptions are often directly opposed to the reality experienced by seasoned investigators.

Lack of Reporting:- Although estimates vary, most experts agree that the vast majority of Fortune 500 companies have been electronically compromised to the tune of at least $10 bil- lion/year. However, early studies indicated that only 17 percent of such victim- izations were reported to law enforcement authorities (Center for Strategic and International Studies, 1998). At the same time, number of reported incidents handled by Carnegie-Mellon University (CERT–Computer Emergency Response Team) has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999 (U.S. General Accounting Office, 1998). It does appear that reporting is get- ting better; a survey of 521 security personnel from American companies, financial institutions, universities and government agencies revealed that 32 percent of respondents reported electronic crime to law enforcement. This represented an increase of 15 percent of the previous study. However, computer intrusion is still vastly underreported.

Lack of Resources:- Although computer intrusions have proven to be problematic within the corpo- rate world, their unwillingness or inability to effectively communicate with judi-cial authorities has led to an increase in computer crime. Unfortunately, law en- forcement and corporate entities desperately need to cooperate with one another. Unlike their civil service counterparts, the business communities have the re- sources (both financial and legal) necessary to effectively combat computer crimes. First, these companies, through their system administrators, have far more leeway in monitoring communications and system activities, and they have the ability to establish policies which enable wide-scale oversight.

Jurisprudential Inconsistency:- Unfortunately, the Supreme Court has remained resolutely averse to deciding matters of law in the newly emerging sphere of cyberspace. They have virtually denied cert on every computer privacy case to which individuals have appealed, and have refused to determine appropriate levels of Fourth Amendment protections of individuals and computer equipment. As such, the country is remarkably divided on fundamental elements of law establishing a legality standard of behavior in one jurisdiction which negates or supersedes another.

IDENTITY THEFT AND IDENTITY FRAUD:-

IDENTITY FRAUD: A typology of ID change:- Identity fraud can roughly be described as the unlawful changing of someone‟s identity. Rost, Meints, and Hansen [Le06:52-55, RoMe05] distinguish four closely related subcategories of identity change:

► identity takeover, when someone takes over the identity of another person with- out that person‟s consent;

► identity delegation, when someone uses someone else‟s identity with that per- son‟s consent;

► identity exchange, when two or more people, with mutual consent, use each other‟s identity;

► identity creation, when someone creates the identity of a non-existing person.

In all subtypes, the identity change can be perfectly lawful.

For instance, a Tony Blair doppelganger can walk the streets of Lon- don to see how the public reacts; a wife can lend her bank card to her husband to purchase something; the prince and the pauper can swap lives for a day; and Eric Arthur Blair may well choose a pseudonym to publish his books. Nevertheless, many cases of identity change can be considered unlawful. When the Tony Blair look-alike uses his doppel gängsterism to receive free services or goods, he commits fraud, and when a director gives the password to her digital signature to her secretary to sign documents he is not authorized to sign, she also commits fraud.

Swapping loyalty cards to thwart a supermarket's profiling will not generally be considered fraud, but depending on the terms and conditions may well constitute tort. And using a self- generated credit-card number that fulfils the characteristics of credit-card numbers clearly is unlawful. As these examples already illustrate, the bulk of identity fraud cases will readily fall within the ambit of the traditional notion of fraud. This means that, from a strictly legal perspective, there is no need to pay specific attention to identity-related fraud: most if not all cases can be prosecuted as fraud.

A significant part of any identity-fraud combating strategy is awareness-raising: - This is a second reason to treat identity fraud as a special category. Opportunities for identity fraud thrive as long as people develop and use identity-management technologies without heed of their potential for abuse. It is only when people are educated about the various risks of identity fraud, that the weakest link in identification vulnerabilities can be strengthened. In this respect, Europe can benefit from the example of the US, where through the Identity Theft and Assumption Deterrence Act, a complaint and education centre has been established with the Federal Trade Commission.3 In Europe, the UK has a similar web- site.

A third reason to look at identity fraud as a separate category is the victim's perspective: - Unlawful identity takeover („identity theft") differs from traditional fraud in two fundamental ways. First, it takes time for the victim to notice the crime, which may happen long after the identity „thief" has fled to Vanuatu with his gains.

Next , the victimization of the victim may well continue long after the crime, since, contrary to most traditional cases of fraud, a feature of identity takeover is that the victim is black- listed and has difficulty in regaining her credit history and trustworthy image. This difficulty is another characteristic of current identification infrastructures. It is therefore altogether important to study the specifics of identity fraud in order to support victims effectively.

Identity Theft: - Having focused on identity fraud as a useful target of research, we have still the prevalent term of „identity theft" to consider. What is usually meant by this term is the subcategory of unlawful identity takeover from the broader category of identity fraud.

„Identity theft" is a rather awkward term, since identity is not something that is typically stolen.

A characteristic of theft, after all, is that the owner no longer possesses the stolen thing. With identity, this is usually not the case: the victim of identity takeover still retains her identity. We should therefore speak of „identity „theft"" rather than of „identity theft".

Another reason to be hesitant in using this term broadly is that it invites overlooking the other forms of identity fraud. The consequences for third parties of identity takeover with consent (as in unlawful identity delegation or exchange) may be equally serious as those of identity takeover without consent (as in identity „theft").

Policymaking and action plans should therefore not be confined to unconsensual identity takeover.

Since identity „theft" is not primarily targeted at the person whose identity is used, and since the question who is the victim of the crime depends on the context of the modus operandi and the legal distribution of liabilities, we propose to stress the „target crime" – usually fraud, and occasionally other crimes such as slander or extortion – rather than the subsidiary element of using another's identity.

The latter element is nevertheless relevant, from the perspective of awareness and the grave consequences for identity bearers if they are victims.

This leads to the following definition.

Identity „theft" is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent.

ORGANIZED CRIME & TERRORISM:-

Terrorism:-

Terrorism is not a new phenomenon. On the contrary, terrorism has existed since the beginning of civilization. Attacks on legitimate structures have been perpetrated by individuals or groups of all cultures throughout history. Social reactions to such attacks have varied from horror to complacence to support depending upon the perceived legitimacy of such acts. While some terrorists have been publicly executed, others have been deified. In fact, the concept is quite complex and not easily defined. Most often, characterizations and designations of acts against the government vary across the population.

Defining Terrorism:- The word "terror" comes from the Latin term *terrere,* which is defined as"to arouse fear." Although individuals and organizations sought to arouse fear in ancient civilizations, the current etymology of the term is probably traced to Robespierre's "the Terror," which immediately followed the French Revolution.2 Etymological origins aside, no universal definition of terrorism exists. Rather, individual and social definitions are influenced by a variety of characteristics, including individual politics, ideologies, national original, theology or organizational agenda. As a result, definitions may vary by region, state or nation.

According to the United Nations Office on Drugs and Crime, there is no international definition for terrorism. Although attempted a number of times, consensus among all member states has not been achieved.

Below is a sampling of traditional definitions:

Government Definitions:-

League of Nations Convention (1937) - all criminal acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons or a group of persons or the general public.

UN Resolution Language (1994) - criminal acts intended or Calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them.

U.S. Department of Defense (2007) - the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological

Academic Definitions:-

Schmid and Jongman (1998) - Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby—in contrast to assassination— the direct targets of violence are not the main

targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.

T sfati and Weimann (2002) - An attempt to communicate messages through the use of orchestrated violence.

Perhaps it is not the definitions of terrorism which are lacking, but the approach taken by individuals or entities driven to reduce the phenomena to a concise, flowing statement. Like organized crime, terrorism is too complex to be so nicely packaged. Rather, encapsulation of the phenomena requires a listing approach. Thus, **terrorism** is a sum of the following components:

- An act of violence
- The victimization of innocents
- Methodical or serial operations
- Advance planning
- Criminal character
- Absence of moral restraints
- Political demands
- Attempts to garner attention
- Performed for an audience
- Unpredictability or unexpectedness
- Intended to instill fear

Classification through Motivation:- Terrorists and terrorist groups vary widely in their longevity, methodology, sophistication, and commitment. While some groups have shown great resiliency, others have been extinguished as quickly as they were ignited. Thus, it is impossible to discuss all groups which are, have been, or will be engaging in terrorists

acts. Rather, it is more appropriate to discuss the groups collectively by their motivation:

- Individual terrorism
- Nationalistic terrorism
- Religious terrorism
- political-social terrorism
- environmental terrorism
- state-sponsored terrorism

• **Individual terrorism:-** Individual terrorism is often overlooked in discussions of the phenomenon as there is a collective perception that such individuals have limited impact and do not constitute a significant threat. Such individuals act independently and typically eschew group involvement. Their motivations are as disparate as the individual actor themselves but are largely directed as a discontentment with society in general. Theodore "Ted" Kaczynski (aka the Unabomber) is an example of an individual terrorist.

• **Nationalist terrorism:-** Nationalist terrorism is characterized by groups which share a collective perception of oppression or persecution. Generally, these groups maintain some social commonality or group identification (i.e., ethnicity, race, culture, language, or religion). Historically, nationalist groups maintain large memberships and significant longevity due to their ability to recruit on platforms of persecution. These groups include many prominent Arab Palestinian terrorists groups, like HAMAS (Islamic Resistance Movement), Hezbollah, Palestine Islamin Jihad (PIJ), and Palestine Liberation Front (PLF). It also includes the Irish Republican Army (IRA) and the Spanish Basque separatists, Euzkadi Ta Askatasuna (ETA).

• **Religious terrorism:-** Perhaps the most prevalent, and certainly the most dangerous, groups of terrorists are motivated by religious ideologies. Historically, these groups have displayed the highest degree of longevity, devotion, and success. Claimed to be empowered by God and justified by scripture, these groups have waged war and slaughtered innocents—all in the name of religion. Their zealotry blinds them to human suffering, and even the most horrific acts are seen as glorious. Such ideologies are not

limited to one particular faith or denomination. Although Islamic groups have garnered the most attention in the past decade, Christian and Jewish groups remain. Some of the groups that are most actively engaged in acts of terror include:

• **Christian:** Army of God, God's Army, Nagaland Rebels, Phineas Priesthood, National Democratic Front of Bodoland

• **Judaic:** Kahane Chai, Kach, Jewish Defense League

• **Islamic:** al Qaeda, HAMAS, Jihad Rite, Turkish Hezbollah, Palestinian Islamic Jihad

• **Political-social terrorism:-** This type of terrorism is often the most ambiguous as the actors are often characterized by the success of their operations. Theoretically speaking, political-social terrorism is perpetrated by groups which are attempting to accomplish an articulable political agenda. Most often, these groups engage in behavior to overthrow the established order in order to replace it with their own. Depending upon the emergent government, groups which are successful are referred to as *patriots, revolutionaries, heroes, freedom fighters,* or *regimes.* An example of the former might include the early American colonists, while an example of the latter would include Castro's 26th of July Movement. Thus, yesterday's terrorists who are successful are often portrayed as today's heroes. After all, history is written by the victor.

• **Environmental terrorism:-** Commonly known as *ecoterrorism,* environmental terrorist groups base their ideology on the conservation of natural resources. Some groups also focus on animal rights. In the United States, the first group to engage in violent acts (i.e., arson) was *Earth First!.* However, their actions pale in comparison to later groups, such as the Earth Liberation Front (ELF), which has set fire to commercial properties and private vehicles. One of the most prominent animal rights groups, the Animal Liberation Front (ALF), has directed similar efforts at university research centers or industries which engage in activities which exploit or harm animals.

- **State-sponsored terrorism:-** Like political terrorism, state-sponsored terrorism is defined by the established order. In today's world, it contains two broad groups of actors: (1) those governments that engage in acts of terror against their own citizens (i.e., Nazi Germany, Bosnia, etc.); (2) those governments that support or carry out terrorist acts against othergovernments. According to the United States, the governments of Cambodia, Rwanda, and Bosnia are currently engaging in acts of terror against their own citizens, while Cuba, Syria, and Iran continue to support international terrorist acts against other countries.

Organized Crime:-

Some scholars posit that transnational organized crime will be one of the defining issues in the twenty-first century—like the Cold War was for the twentieth century and colonialism was for the nineteenth century.40 It has been noted that the scale of such activity poses a significant threat to national security in a variety of ways, including, but not limited to, trafficking in nuclear materials, sophisticated weaponry, and human smugglings. The illegal laundering of massive profits through Web-based financial transactions may indirectly result in the destabilization of national financial systems and world markets. The most catastrophic destabilizations will occur in transitional states but have the potential to dramatically affect even major economies like Japan and Italy, as evidenced in the 1990s.41

In fact, economies transitioning to democracy face the likelihood of the entrenchment of organized crime in both their political and economic systems. This has occurred in the wake of the collapse of the Soviet Union and in other Eastern European countries. Even China is confronting an increased organization of domestic crime groups. Like terrorist organizations, organized crime groups are increasingly turning to technology to enhance the complexity and profitability of their criminal pursuits.

Unfortunately, these transnational activities pose significant challenges to law enforcement authorities due to corrupt political systems, lax international banking laws, lack of mutual legal assistance treaties, and, most importantly, a lack of global definitions and international consensus.

Defining Organized Crime:-

As noted previously, all *organized crime groups* began as criminal gangs. Organized crime (OC) groups do not appear spontaneously. In fact, all OC groups discussed in this text were traditionally treated as street gangs. For the most part, the vast majority of organized crime groups originated as a result of perceived oppression and discrimination or perceptions of restrictive governments. Throughout history, the emergence of criminal groups and subsequent violence has been greatest during periods of economic depression. The deprivation experienced in the mid-1800s, for example, was characterized by a dramatic increase in gang affiliation in New York City.43 However, economic deprivation is not the sole determinant in gang development. Indeed, the convergence of a variety of variables bears greater weight than any single causative agent and may enhance the potentiality for organization within street gangs. A cultural emphasis on masculinity, historical territorial rivalries, and the advent of mass unemployment all serve to increase the primacy of group affiliation and decrease the likelihood of antigang maturation of members. Thus, the evolution of common street gangs into organized criminal syndicates involves a variety of factors. However, the majority of definitions associated with both fail to address this issue. In fact, definitions of *organized crime* are as diverse, as inaccurate, and as numerous as those traditionally associated with criminal gangs. Law enforcement gatherings, senatorial committees, academic consortiums, and even Hollywood studios have created definitions based largely on anecdotal recounts of mob informants. For the most part, these definitions have focused primarily on Italian organized crime—denying the existence of criminal syndicates among other ethnicities.

The first attempts to formally define *organized crime* were undertaken by two different government commissions. While both of them uncovered a network of sophisticated, multijurisdictional criminal entrepreneurs, they proved to be largely ineffectual at the time. The first definition of organized crime in the United States was created in 1915 by the Chicago Crime Commission. In an attempt to define what they considered *institutionalized*

crime, the commission was the first of its kind to recognize differences between traditional crimes and criminals and the emerging pattern of criminal behavior perpetrated by organized criminal groups. They found that such entities were unique in that they resembled an independent society of sorts, with systemized tasks and practices, unique traditions and rituals, and distinctive jargon. These findings were expanded upon by the Wickersham Commission of 1929. This commission, designed to evaluate the impact of prohibition, found that the organization of criminal activity surrounding prohibition was actually created by it. (Unfortunately, the structure that was created during and flourished throughout the period did not end with the repeal of the Eighteenth Amendment, as profits from bootlegging had been utilized to create additional criminal markets.) As with the recommendations of its predecessor, the admonitions put forth by the Wickersham Commission were largely ignored until the 1950s, and organized crime continued on its path of organizational sophistication and criminal maturation.

In 1957, a string of gangland murders and the discovery of a meeting of top echelon underworld figures in Apalachin, New York, propelled the Italian mafia into the national spotlight. Such events served as an impetus for government scrutiny and law enforcement activity. At that time, the Kefauver Committee, which had been in existence since 1950, increased their efforts to evaluate the connection of organized crime to gambling. In addition, the committee expanded their original focus to include a plethora of other organized criminal activities. Headed by Senator Estes Kefauver, the committee transfixed the American public as they televised the testimony of over 600 witnesses.

Contemporary definitions of organized crime must include the following characteristics:

1. Structure and hierarchy - Virtually all organized crime groups are characterized by recognition of responsibility, task assignment, and leadership. Whether formally appointed or elected, each organized crime groups has a system of interrelated positions specifically designed to

facilitate task accomplishment. Such officials, recognized by organizational members, assign responsibilities, dictate policy and procedures, and ensure compliance. However, contemporary groups are not as hierarchical as their predecessors and are characterized by loose networks.

2. Violence - The utilization of violence and the threat thereof is necessary for both task efficacy and organizational longevity. It is an essential component of criminal activities such as extortion, loansharking, and racketeering. It is also important in maintaining control over organizational members. Ironically, the potentiality for violence may be more important than the actual violence itself as reputations for violence often negate the need to employ it.

3. Recognizability - Organized crime groups are recognized not only by law enforcement authorities but by their communities as well. This is necessary for the extortion of funds, as they rely on the specter of a mass criminal organization to intimidate potential victims. It is also necessary for the corruption of political figures. Such recognizability may be likened to the threat of violence that is not employed in which targets realize their own vulnerability against an army of criminals.

4. Longevity - Whether guided by religious zeal or motivated by pecuniary gain, organizational goals must include its preservation. Members must recognize the continuity of group ideology and the organization itself. Such recognition necessarily includes their own impermanency and vulnerability.

5. Recruitment - To further ensure organizational longevity, criminal groups must maintain the ability to replenish their ranks as positions become available. Traditionally, ethnically based organized crime groups recruited youngsters from the neighborhood—evaluating their criminal prowess and organizational loyalty by assigning small tasks. While recent immigrant criminal groups have continued this practice, traditional groups like LCN are increasingly forced to replenish their personnel with family members or longtime associates. (Throughout the text, the author will discuss the various methods of recruitment employed by individual organizations.)

6. Innovative, entrepreneurial, and opportunistic - All organized crime groups are characterized by elevated levels of entrepreneurial criminal activity. Such innovation is necessary as changes in legislation and law enforcement efforts combine to reduce the cost–benefit ratio of various activities. The repeal of the Eighteenth Amendment, for example, forced organized crime groups to develop new markets to replace revenue lost by the legalization of alcohol. In the twentieth century, many groups turned to narcotics to refill depleted coffers. In the twenty-first century, the same groups have increasingly utilized nonmember hackers.

7. Exclusive membership - Entrance into the criminal group requires some commonality with organizational members. As Asbury (1928) discovered in his evaluation of criminal gangs in early twenty-first-century New York, those groups that came together for the sole purpose of committing criminal activity, lacking ethnic solidarity, also lacked organizational longevity. Culture, shared experiences, traditions, and religion often play a role in the solidification of norms and expectations of the group prior to criminalactivity. Such commonalities may include, but are not limited to, race, ethnicity, criminal background, or ideology. However, such common traits do not ensure organizational admittance. Just as money is not the sole factor in entrance to exclusive country clubs, incumbent members closely scrutinize a potential member's background. In fact, the level of inspection employed by these groups is often greater than that found in law enforcement agencies. Organizational fit, individual loyalty, and criminal ability are but a few of the factors which determine an individual's acceptance.

8. Strict rules and regulations - Organized crime groups are characterized by elevated levels of rules and restrictions. Paramount in each is the rule of silence. Individuals violating organizational secrecy are almost always killed. While rules vary between individual groups, all are established to ensure organizational longevity and task efficacy. Rules of conduct between members, for example, are necessary to negate potential friction within the

group. Noncompliance results in organizational discipline ranging from loss of respect to loss of life.

9. Ritualistic - Just like noncriminal societies, aberrant groups also display a tendency for ritualism. Induction ceremonies, organizational meetings, and the like are all characterized by ceremonial trappings. The development of jargon and customary displays of respect solidify members and further sanctify the organization itself.

10. Profitability - All members of organized crime syndicates are expected to enhance organizational coffers through criminal enterprise. The practice of tithing to organizational leaders or elders furthers the interests of the organization in the form of political bribery or, in some cases, the support of criminal defense. Even ideologically based groups must maintain a positive cash flow to support their dogmatic platform.

11. Racketeering and infiltration of legitimate business - Although traditionally associated with LCN, the practice of racketeering and the infiltration of legitimate businesses have permeated all corners of organized crime. With the increasing amount of legislation designed to identify illegal profits, the laundering of money through legitimate sources has become increasingly common. In addition, a façade of legitimacy furthers organizational goals and increases organizational longevity, as the business of crime becomes more palatable to an American public desensitized to white-collar crime.

12. Corruption of political officials - The organized corruption of political officials, including police officers, politicians, and jurists, has a long history in the United States. Criminal gangs have colluded with these entities beginning with Tammany Hall in the early 1800s. In fact, early systems of policing, which included the practice of appointments by Alderman and then the Board of Police Commissioners in New York City, established an incestuous relationship among politicians, police, and criminal gangs (i.e., the police owed the politicians that appointed them, the politicians owed the criminal gangs which fixed their elections, and the criminal gangs owed them both).

AVENUES PROSECUTION AND GOVERNMENT EFFORTS: -

The lack of resources available to small agencies, the traditional apathy toward nonviolent crime, and the reluctance of legislative action have enabled many computer criminals to act with virtual impunity.

While it is anticipated that an increase in technology-specific legislation and the modification of extant statutes are forthcoming, lawmakers should evaluate existing federal and state law for prosecutorial avenues currently available.

Traditionally, state and local officials have been forced to rely exclusively on the expertise of better-trained, better-funded federal agencies. Unfortunately, these agencies are incapable of addressing every call for assistance.

Traditional Statutes:- Title 18 of the U.S. Code has long been characterized as an invaluable resource for state and local legislators in development of state codes. As such, it can be used as a guideline for investigators seeking to apply non-technology-specific prohibitions generically to computer crime.

Computer Fraud and Abuse Act—18 U.S.C. § 1030:- Section 1030 expands the power of the Secret Service by specifying that "the United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section."However, due to Congress' refusal to remedy jurisdictional turf battles between the USSS and the FBI, authority is somewhat unclear.

• Section 1030 also prohibits simple access of full or part time governmental computers—no damage must be done in order for this act to be violated.

• Section 1030(a) (4) punishes those who use computers in schemes to defraud victims of property of more than $5,000.

• Section 1030(a)(5) creates three separate offenses, two felonies and one misdemeanor (depends on intent and authority of the actor) and criminalizes the transmission of a program, information, code, or command, as a result of which the actor intentionally causes damage without authorization to a protected computer (felony); the damage may include the availability or integrity of data, program, system, or information that (1)

causes loss of more than $5,000 within a year to one or more persons; (2) modifies or impairs, or potentially modifies or impairs.

The medical examination, diagnosis, treatment, or care of one or more persons; (3) causes physical injury to a person; or (4) threatens public health 1030(e)(8).

• Section 1030(a)(5) generally governs access without authority (outsiders).

• Section 1030(a)(5)(B) charges the individual who intentionally accesses a protected computer and, as a result of such conduct, recklessly causes damage as guilty of a felony.

• Section 1030(a)(5)(C) charges the individual who intentionally accesses a protected computer and, as a result of such conduct, causes damage as guilty of a misdemeanor when it cannot be shown that the damage caused was either intentional or reckless.

• Section 1030(a)(6) prohibits trafficking in passwords, information or devices through which unauthorized access may result, if such trafficking affects interstate or foreign commerce or is a government computer—*aimed primarily at hackers, and underground hacking boards.*

• Section 1030(a)(7) involves extortion through threats to damage a protected computer (this has been utilized against a variety of individuals who have threatened to exploit holes in security systems if their demands are not met).

The Evolution of Computer-Specific Statutes:-

Criminal Activity Statute	Applicable
Fraud and Embezzlement	
18 U.S.C. § 2314	Applies to goods known to be stolen or fraudulently obtained and worth more than $5,000 transported in interstate commerce.
18 U.S.C. § 641	Embezzlement or theft of public money, property, or records.
18 U.S.C. § 2071	Prohibits concealment, removal, or mutilation of public records.
18 U.S.C. § 1005	Prohibits concealment, removal, or mutilation of the records of banks or credit institutions. (Remote alteration or the like would clearly fall within these provisions.)
18 U.S.C. § 1006	Prohibits false, fictitious, or fraudulent statements to a department or agency concerning a matter within the jurisdiction of the same when something of value is involved. (May be utilized if individuals misrepresent themselves to gain access to programs or pages.)

Terrorism or Espionage

18 U.S.C. § 1905	Prohibits the disclosure of confidential information by a government employee.
18 U.S.C. §§ 793, 794, 795	Prohibits the gathering, transmission, or loss of defense information; prohibits the transmission or delivery of national defense information to a foreign government or agent; prohibits the sketching or photographing of defense installations. (May be utilized if individuals attach live feeds of military bases or the like or upload pictures or maps onto the Internet.)

Child Seduction & Exploitation

18 USC § 159118 U.S.C. § 2423	Prohibits the interstate or foreign commerce in which minors are recruited, enticed, harbored, transported, or provided for a commercial sex act. Additionally, it provides sentencing enhancements according to the age of the minor. Prohibits the interstate transportation of minors for sexual activity.
18 U.S.C. § 2251	Prohibits the sexual exploitation and other abuse of children.

Stalking

18 U.S.C. § 2261	This amendment to Title 18 makes it a federal crime to engage in repeated harassing or threatening behavior that places the victim in reasonable fear of death or bodily injury. Summarily stated, any person who travels (or causes to), uses (or causes to) the mail or any facility in interstate or foreign commerce, or enters or leaves (or causes to) Indian country is guilty of stalking if they place an individual in reasonable fear of death or harm to a loved one.

Criminal Activity Statute	Applicable
18 U.S.C. § 875(c)—The Hobbs Act	Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another shall be fined under this title or imprisoned not more than five years, or both.

Forgery and Counterfeiting 18 U.S.C. §§ 471–509

Credit Card Fraud

15 U.S.C. 41 § 1644	Prohibits the use, attempt, or conspiracy to fraudulently use credit cards in interstate or foreign commerce. In addition, it prohibits the transportation of such cards, and receipt or concealment of goods and tickets purchased and money received through card transactions. (This statute could be used on individuals posting credit card numbers on BBSs or on "carding"—hackers who use stolen credit card information to purchase goods or services.)

Extortion

18 U.S.C. § 1951

Copyright Infringement

17 U.S.C. §§ 102, 103	Provides definitional guidelines for protected information or material. In particular, it offers protection for idea(s), procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.
17 U.S.C. § 506	Prohibits the reproduction, preparation, distribution, or public release of copyrighted material. This includes art, photographs, writings, etc. Probably one of the most common forms of theft on the Internet—where ideas are routinely misrepresented.

Software Piracy

15 U.S.C. § 1114	Prohibits the manufacturing of counterfeit products (may include software or hardware).

RICO

18 U.S.C. §§ 1961–1968	Provides for the prosecution of individuals involved in a pattern of racketeering. It also provides for the punishment of offenders and the seizures of their assets.

Access Device Fraud	
18 U.S.C. § 1029	Individuals may be prosecuted under this statute if they knowingly, and with intent to defraud, produce, use, traffic, or in some cases simply possess counterfeit and/or unauthorized access devices or device-making equipment. Such devices are broadly defined as cards, plates, codes, account numbers, electronic serial numbers, mobile identification number, personal identification number, or other means (Soma et al., 1996). Although this statute was not directed toward computer-facilitated fraud, the courts have ruled that it may be used in cases where computer passwords are fraudulently obtained to steal things of value (U.S. v. Fernandez, No. 92 CR. 563 (RO), 1993 WL 88197 (S.D.N.Y. March 25, 1993)). In addition, this statute could be used to prosecute phreakers using illegal boxes or electronic passwords used to access financial accounts, and the like. This section, never mentioning the word "computer," has been utilized by the Secret Service to prosecute those individuals who have stolen information or software from computers.
Illegal Wiretapping	
18 U.S.C. § 119	A variety of laws at the state and federal level make it illegal for individuals to unlawfully intercept electronic communications. This would include utilization of keyloggers or other functions included in back-door programs like NetBus or Back Orifice (since these programs also grant access to them). These would include provisions under Title 18 (18 U.S.C.§ 2511). In addition, 18 U.S.C.§ 2701 prohibits the intentional acquisition of or alteration or destruction of stored communications. Thus, those individuals who intentionally access e-mail accounts not belonging to them may be prosecuted under this statute.

National Information Infrastructure Protection Act of 1996 (NIIPA):-

The CFAA was successfully used to prosecute hackers and individuals who exceeded their authorized use; it contained significant limitations in that it only involved those cases in which computer data was a target. It neither included other offenses committed via or in conjunction with computer technology nor included noninterest computers.

It also provided for federal criminal liability for the theft of trade secrets. To with, the subcategories criminalize the following acts:

• **18 U.S.C. § 1030(a)(1)**—transmitting classified government information.

• **18 U.S.C. § 1030(a)(2)**—obtaining information from financial institutions, private sector computers, and U.S. government.

• **18 U.S.C. § 1030(a)(3)**—affecting the government's use of a U.S. department or agency nonpublic computer.

• **18 U.S.C. § 1030(a)(4)**—fraud.

• **18 U.S.C. § 1030(a)(5)**—hacking and malicious programming. This section criminalizes damaging protected computers via hacking or malware even if the damage was not intentional.

• **18 U.S.C. § 1030(a)(6)**—intent to or trafficking in passwords.

• **18 U.S.C. § 1030(a)(7)**—extortion or communication of threats.

Evolving Child Pornography Statutes:- Although a variety of laws have been enacted to combat the increase in technological crime, none are more emotionally charged than those dealing with child pornography.

- ✓ Beginning in 1977, Congress has attempted to eliminate child pornography.
- ✓ Originally criminalized at the federal level with the *Protection of Children against Sexual Exploitation Act of 1977* (PCSE), Congress has periodically revised the legislation to protect children from sexual exploitation in keeping with emerging legal doctrine.
- ✓ Traditionally, evaluations of child pornography statutes relied primarily on two Supreme Court decisions, whose interpretation of and application to emerging laws have been diverse.

Child Pornography Protection Act (CPPA) in 1996:-

The most important of these included the following:

- ✓ Mandatory life sentences for offenders involved in a sex offense against a minor if;
- ✓ such offender has had a prior conviction of abuse against a minor;
- ✓ The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- ✓ Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- ✓ Prohibition against the pretrial release of persons charged with specific offenses against children;
- ✓ Elimination of the statutes of limitation for child abduction or child abuse;
- ✓ Prohibition against the pretrial release of persons charged with specific offenses against children;
- ✓ Provided for the appointment of a national AMBER alert coordinator;
- ✓ Elimination of waiting periods for missing persons cases involving victims between the ages of 18 and 21;
- ✓ Avenues for reporting missing persons between the ages of 18 and 21 to NCIC;

- ✓ Prohibition against computer-generated child pornography;
- ✓ Application of the *Miller* standard of obscenity in drawings, sculptures, and pictures of such, which depict minors in obscene situations or engaged in sexual activity;
- ✓ Enhancement of sentences for the possession and distribution of obscene images of minors; and
- ✓ Authorization of fines and imprisonment of up to 30 years for U.S. citizens or Residents engaging in illicit sexual conduct abroad.

Identity Theft and Financial Privacy Statutes:-

Identity theft/fraud has become the defining crime of the information age. It is estimate that at least 10 million incidents occur each year.

However, this figure does not approach the numbers imagined by the general public.

Although traditional statutes contain some provisions which may be applied to crime associated with the theft and misuse of person a information, statutes specifically addressing identity theft and financial privacy were not created until the waning days of the twentieth century.

Such statutes have often been hastily prepared by individuals attempting to assuage constituent fear. Ironically privacy advocates have often criticized the emerging legislation.

Identity Theft and Assumption Deterrence Act of 1998:-

In October 1998, the **Identity Theft and Assumption Deterrence Act(ITADA)** was passed by Congress.

It was the first act to make the possession of another's persona identifying information a crime, punishable by up to 20 years in prison. More specifically, the act stated that it is unlawful if an individual knowingly transfers or uses, without lawful authority, a means of identification o another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under an applicable State or local law.

In addition, the law expanded the traditional definition of "means of identification" to include:

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) Unique electronic identification number, address, or routing code; or

(D) Telecommunication identifying information or access device.

The Financial Modernization Act of 1999:-

Financial Modernization Act (FMA) was enacted to promote greater accountability of an provide civil remedies against corporate America. Also known as the *Gramm Leach-Blile Act* or *GLB* for short, the act includes provisions to protect consumers' personal financial information held by financial institutions.

Fair and Accurate Credit Transactions Act (FACTA) 2003:-

Major Provisions to FACTA

• **Free Credit Report**—Consumers may avail themselves of one free credit report from each of three largest credit reporting agencies (Equifax, Experian, TransUnion). This provision encourages consumers to regularly monitor their credit reports, therefore allowing the discovery of unlawful activity much more quickly. Initially, the provision was ineffective, as the process was not streamlined.

Consumers may now request their free copies through *www.annualcreditreport.com*. However, it is not recommended to request and access individual reports online. Ironically, the FTC has filed at least one suit against, and issued several warnings to, various imposter sites designed to steal your personal information.

• **Fraud Alerts:-** Consumers have the right to create alerts on their credit files, indicating that they have been the victim of identity theft and that some information included in the report may be based on the victimization. Such alerts must be attached to the credit file and provided to all entities requesting data. In addition, credit reporting agencies must exclude such accounts from those used for marketing purposes by third parties and

provide additional free credit reports to consumers who have initiated the alert process. In files containing alerts, businesses seeking to extend credit are required to contact the consumer directly or to take other reasonable steps to authenticate the applicant. These actions are designed to minimize the potential costs associated with the theft by hampering the acquisition of additional credit and by encouraging verification of identity by potential creditors.

• **Active Duty Alerts:-** FACTA also contains special provisions for individuals actively performing military duty. Requires credit reporting agencies to place an active duty alert within a credit file of an individual actively serving in the military. In addition, it also provides for an automatic two-year "opt out" from lists provided to third parties.

• **Truncation of Credit/Debit Account Numbers:-** FACTA prohibits merchants from putting any but the last five digits of a credit card number on customer receipts. This is designed to minimize the effectiveness of dumpster diving by limiting the amount of information printed on a receipt. As a result, many dumpster divers have modified their *mods operandi* to focus exclusively on manually imprinted receipts which are often used by small businesses or roadside merchants.

• **Truncation of Social Security Numbers:-** Like the previous provision, FACTA requires credit reporting agencies to exclude the first five digits of consumer social security numbers from their disclosures upon request.

• **One-Call Fraud Alerts and Enhanced Victims' Resolution Process:-** FACTA creates a national system of fraud detection and alerts to increase the ease of incident reporting and protection of credit standings. Known as "one-call fraud alerts," the system allows consumers to generate a nationwide fraud alert with one phone call.

• **Mandates to Card Issuers to Investigate Changes of Address and Requests for New or Additional Cards: -** It requires all creditors to send notification of changes to both the old and new addresses. It is intended to quickly alert victims.

• **Blocking or Elimination of Fraudulent Information: -** FACTA allows consumers to file "no fault letters" with police authorities to eliminate the release of fraudulent information. It also requires credit reporting agencies to block those entities which supplied fraudulent information from further submitting information on the credit report.

• **Fraud Alert Requirements by Credit Reporting Agencies: -** FACTA provides for the inclusion of a fraud alert upon request by a consumer which states that some information included in the report may be based on identity theft. Such alerts must be attached to the credit file and provided to all who request data.

• **Requirement of Credit Reporting Agencies to Divulge Consumer Credit Scores: -** This measure is designed to increase the probability of discovery of victimization.

• **Limits the Commingling of Medical and Financial Information: -** In order to decrease the possibility of identity theft/fraud which is perpetrated through dumpster diving or breaches of security of health providers, the act significantly limits the commingling of medical and financial information.

• **Debt Collectors:-** In situations where consumers notify debt collectors that the debt is unknown to them or may be a product of identity theft, FACTA requires debt collectors to inform their third-party employers that the alleged debt may be the result of identity theft. They must also provide the affected consumer with information regarding their rights and the handling of disputes. In addition, they must provide the consumer with all information regarding the debt, including applications, statements, and so on. Upon notification that the debt is the result of theft or fraud, the creditor is prohibited from placing the debt in collection or selling the debt to a third party.

• **Civil Action:-** The act provides for a civil action to be brought when violations occur. However, such suit must be brought within two years of the discovery of the violation *or* five years after the date of the violation itself, whichever is earlier.

• **Drivers Privacy Protection Act:-** Prohibits the disclosure of SSNs and other Personal information from a motor vehicle record in any situation not expressly permitted under the law. Permissible   purposes   include   the following:

1. The use by a government agency in carrying out its function;

2. In connection with motor vehicle or driver safety and theft (i.e., emissions, alterations, recalls, advisories, and research activities);

3. The use in the normal course of business to prevent fraud and verify the accuracy of information submitted or in the recovery of a debt;

4. The use in legal or arbitral proceedings; and

5. Any other use specifically authorized by state laws in regard to the operation of a motor vehicle or public safety.

• **Identity Theft and Financial Privacy Statutes:-** Identity theft/fraud has become the defining crime of the information age. It is estimated that at least 10 million incidents occur each year.

However, this figure does not approach the numbers imagined by the general public.

Although traditional statutes contain some provisions which may be applied to crime associated with the theft and misuse of personal information, statutes specifically addressing identity theft and financial privacy were not created until the waning days of the twentieth century.

Such statutes have often been hastily prepared by individuals attempting to assuage constituent fear. Ironically, privacy advocates have often criticized the emerging legislation.

• **Identity Theft and Assumption Deterrence Act of 1998:-** The law expanded the traditional definition of "means of identification" to include:

(A) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) Unique electronic identification number, address, or routing code; or

(D) Telecommunication identifying information or access device.

• **The Financial Modernization Act of 1999:-** Financial Modernization Act (FMA) was enacted to promote greater accountability of and provide civil remedies against corporate America.

Also known as the *Gramm- Leach-Bliley Act* or *GLB* for short, the act includes provisions to protect consumers' personal financial information held by financial institutions.

The regulations contained within the *Financial Privacy Rule* and the *Safeguards Rule* applies to various financial institutions and companies who receive personal financial information.

• **Fair and Accurate Credit Transactions Act (FACTA) 2003:-** It included a variety of changes which generally addressed consumer rights and specifically targeted identity theft. While many of the provisions contained therein remain unrealized,

• **Major Provisions to FACTA: -** Free Credit Report—Consumers may avail themselves of one free credit report from each of three largest credit reporting agencies (Equifax, Experian, TransUnion).

This provision encourages consumers to regularly monitor their creditreports, therefore allowing the discovery of unlawful activity much more quickly.

Initially, the provision was ineffective, as the process was not streamlined.Consumers may now request their free copies through *www.annualcreditreport* .*com*.

However, it is not recommended to request and access individual reports online. Ironically, the FTC has filed at least one suit against, and issued several warnings to, various imposter sites designed to steal your personal information.

• **Fraud Alerts: -** Consumers have the right to create alerts on their credit files, indicating that they have been the victim of identity theft and that some information included in the report may be based on the victimization. Such alerts must be attached to the credit file and provided to all entities requesting data. In addition, credit reporting agencies must exclude such

accounts from those used for marketing purposes by third parties and provide additional free credit reports to consumers who have initiated the alert process. In files containing alerts, businesses seeking to extend credit are required to contact the consumer directly or to take other reasonable steps to authenticate the applicant.

These actions are designed to minimize the potential costs associated with the theft by hampering the acquisition of additional credit and by encouraging verification of identity by potential creditors.

• **Active Duty Alerts—FACTA: -** It also contains special provisions for individuals actively performing military duty. Requires credit reporting gencies to place an active duty alert within a credit file of an individual actively serving in the military.

In addition, it also provides for an automatic two-year "opt out" from lists provided to third parties.

Truncation of Credit/Debit Account Numbers: - FACTA prohibits merchants from putting any but the last five digits of a credit card number on customer receipts. This is designed to minimize the effectiveness of dumpster diving by limiting the amount of information printed on a receipt. As a result, many dumpster divers have modified their *modus operandi* to focus exclusively on manually imprinted receipts which are often used by small businesses or roadside merchants.

• **Truncation of Social Security Numbers: -** Like the previous provision, FACTA requires credit reporting agencies to exclude the first five digits of consumer social security numbers from their disclosures upon request.

• **One-Call Fraud Alerts and Enhanced Victims' Resolution Process: -** FACTA creates a national system of fraud detection and alerts to increase the ease of incident reporting and protection of credit standings. Known as "one-call fraud alerts," the system allows consumers to generate a nationwide fraud alert with one phone call.

• **Mandates to Card Issuers to Investigate Changes of Address and Requests for New or Additional Cards: -** It requires all creditors to send

notification of changes to both the old and new addresses. It is intended to quickly alert victims.

• **Blocking or Elimination of Fraudulent Information: -** FACTA allows consumers to file "no fault letters" with police authorities to eliminate the release of fraudulent information. It also requires credit reporting agencies to block those entities which supplied fraudulent information from further submitting information on the credit report.

• **Fraud Alert Requirements by Credit Reporting Agencies: -** FACTA provides for the inclusion of a fraud alert upon request by a consumer which states that some information included in the report may be based on identity theft. Such alerts must be attached to the credit file and provided to all who request data.

• **Requirement of Credit Reporting Agencies to Divulge Consumer Credit Scores: -** This measure is designed to increase the probability of discovery of victimization.

• **Limits the Commingling of Medical and Financial Information: -** In order to decrease the possibility of identity theft/fraud which is perpetrated through dumpster diving or breaches of security of health providers, the act significantly limits the commingling of medical and financial information.

• **Debt Collectors:-** In situations where consumers notify debt collectors that the debt is unknown to them or may be a product of identity theft, FACTA requires debt collectors to inform their third-party employers that the alleged debt may be the result of identity theft. They must also provide the affected consumer with information regarding their rights and the handling of disputes. In addition, they must provide the consumer with all information regarding the debt, including applications, statements, and so on. Upon notification that the debt is the result of theft or fraud, the creditor is prohibited from placing the debt in collection or selling the debt to a third party.

• **Civil Action: -** The act provides for a civil action to be brought when violations occur. However, such suit must be brought within two years of

the discovery of the violation *or* five years after the date of the violation itself, whichever is earlier.

• **Additional Efforts to Protect Personal Information:-** Social security numbers are especially attractive to identity thieves, as they are permanently assigned to American citizens. Traditionally, they could be easily obtained through perusal of public records, where they are prominently displayed on various documents like bankruptcies, tax liens, civil judgments, real estate transactions, voter registrations, and the like.

• **Drivers Privacy Protection Act: -** Prohibits the disclosure of SSNs and other personal information from a motor vehicle record in any situation not expressly permitted under the law. Permissible purposes include the following:

1. The use by a government agency in carrying out its function;

2. In connection with motor vehicle or driver safety and theft (i.e., emissions, alterations, recalls, advisories, and research activities);

3. The use in the normal course of business to prevent fraud and verify the accuracy of information submitted or in the recovery of a debt;

4. The use in legal or arbitral proceedings; and

5. Any other use specifically authorized by state laws in regard to the operation of a motor vehicle or public safety.

Federally Funded Initiatives and Collaborations:-

This group was originally tasked with providing an analysis of legal and policy issues involving the Internet for criminal behavior. More specifically, they were charged to evaluate the following:

1. The extent to which existing federal laws are sufficient to address unlawful conduct via the Internet (provide a framework for analyzing policy and legal responses);

2. The extent to which new technologies or legal authorities may be needed to investigate and prosecute Internet crime (i.e., the development of new tools and formulating training strategies); and

3. The utility of education and "empowerment tools" to minimize the risks associated with this behavior (i.e., give teachers and parents the ability to teach their children proper usages) (DOJ, 2000).

Generally, the group developed a three-tiered approach:-

1. *Regulation* of Internet criminal activity in the spirit of traditional criminal law (i.e., consistent with statutory and constitutional mandates), stressing that technological crime should be treated the same as criminal activity which is not technologically advanced, ensuring privacy and protection of civil liberties;

2. *Recognition* of special needs and challenges of investigating and prosecuting such activity, while emphasizing the need for tool development, enhanced training, and interagency (and international) cooperation; and

3. *Development* of specialized curricula including cyberethics and support for leadership within the private sector.

Law Enforcement Operations and Tools in the United States:-

Although computer crimes date back several decades, criminal investigations and prosecutions started more slowly. Historically, such investigations focused almost exclusively on bulletin boards, the communication medium of choice for early computer criminals.

Other Government Initiatives and Budget Allocations

1980s

FCIC (Federal Computer Investigations Committee) is comprised of local officers, state officials, and federal agents. However, some claim this is a shadow group, which has no membership role, no official place of residence, And no formal funding.

CERT (Computer Emergency Response Team) was created in response to the Morris worm. It is located at Carnegie Mellon University's Software Engineering Institute in Pittsburgh. CERT acts as an informational clearinghouse for public and private computer networks and assists entities which have been victimized.

1990s

National Computer Crime Squad (NCCS) is located in Tysons Corner, Virginia, and is part of the Washington Metro Field Office of the FBI.

DOJ computer/telecommunications coordinator program designates at least one Assistant U.S. Attorney—each of the 93 U.S. Attorney's Offices has an in-house, high- tech expert.

Computer Crime Unit (CCU) was created within the General Litigation Section of the Justice Department, and it was later moved and renamed the **Computer Crime and Intellectual Property Section.**

2000–2011

The **National Institute of Justice Office of Science and Technology** (NIJ/OST) established the **CyberScience laboratory.**

The Federal Bureau of Investigation unveiled a new laboratory and training center in New Haven, Connecticut, which is designed to serve as a training ground for investigators and provide a state-of-the-art computer forensics laboratory

• Fiscal year 2010 saw a $75.1 million *increase* to Develop and deploy cyber security technologies to counter current threats and devise strategies to mitigate future threats; in addition, there was an *increase* of $6.6 million for ongoing and future cyber security research specifically to address critical Capability gaps identified in the Comprehensive National Cybersecurity Initiative (CNCI). More specifically, the funds were to be used toward the development of additional technologies to secure the nation's critical information infrastructure and networks.

• Fiscal year 2010 budget allotted a total of $2 million toward supporting the operational costs of the 13 Electronic Crime Task Forces and DHS-mandated Certification and Accreditation of the Secret Service online reporting system.

Since that time, methodologies of both computer communication and criminal investigations have changed dramatically.

OECD and the Select Committee of Experts on Computer-Related Crime of the Council of Europe. These suggestions included the criminalization of the following activities:

1. Any manipulation of data which is intended to commit illegal   transfer of funds or other valuables.

2. Any manipulation of data intended to commit forgery

3. Any manipulation intended to interfere with the functioning of a computer or other telecommunications system

4. Any incident of software theft or software piracy

5. Any unauthorized access or interception of another's computer with malicious intent.

The first list, including optional revisions, included the criminalization of the following:

1. The alteration of computer data or   computer   programs:-   The alteration of computer data or computer programs without rights.

2. The practice of computer espionage:- The   acquisition   by   improper means or the disclosure, transfer, or use of a trade or   commercial   secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person.

3. The unauthorized use of a computer:- The use of a computer system or network without right that either (i) is made with the acceptance of significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (ii) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (iii) causes loss to the person entitled to use the system or harm to the system or its functioning.

4. The unauthorized use of a protected computer program:- The use without the right of a computer program which is protected by law and which has been reproduced without right, with the intent either to procure an unlawful economic gain for oneself or for another person or to cause harm to the holder of the right.

The second list included mandatory offenses which   should   be criminalized by all participating countries. Their categories, more broad in nature, included the following:

1. Computer fraud—the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for oneself or for another person.

2. Computer forgery—the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions, as prescribed by national law, that it would constitute the offense of forgery if it had been committed with respect to a traditional object of such an offense.

3. Damage to computer data or computer programs—the erasure, damaging, deterioration, or suppression of computer data or computer programs without right.

4. Computer sabotage—the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunications system.

5. Unauthorized access—the access without right to a computer system or network by infringing security measures.

6. Unauthorized interception—the interception made without right and by technical means or communications to, from and within a computer system or network.

7. Unauthorized reproduction of a protected computer program—the reproduction, distribution, or communication to the public without right of a computer program which is protected by law.

8. Unauthorized reproduction of a topography—the reproduction without right of topography protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semiconductor product manufactured by using the topography.

APPLYING THE FIRST AMENDMENT TO COMPUTER-RELATED CRIME:-

Introduction and General Principles:- As stated previously, the most common judicial challenges facing computer crime investigators include inconsistent interpretations and applications of the First Fourth, and Fourteenth Amendments to emerging advancements in technology.

Obscenity in General:- Defining obscenity has long been a concern among civilized societies. In the most generic sense, it is something not easily defined, but recognizable on sight, irrespective of medium.

Although rare, such broad proclamations encompass myriad of situations, and provide legal justification and academic rationale for their existence. For example, broad laws which prohibited depictions of minors in explicit or sexual situations were upheld due to the sheer indecency of such portrayals and the increased potential for future victimization of generalized children due to their existence.

However, the advent of electronic communications and sophisticated graphical programs has muddied the waters—making it possible for child pornographers to argu that computer-generated images (or *virtual* children) lack the requisite specified victim.

Traditional Notions of Decency: - This statute develops a level of obscenity which evaluated the alleged immorality of Catholic priests. To wit, it evaluated "whether the tendency of the matter charged . . . is to deprave an corrupt those whose minds are open to such immoral influences and into whose hand a publication of this sort may fall.

Emerging Statutes and the Availability of Obscene Material to Children:

Traditional Statutes	
18 U.S.C. § 1460—crime to possess obscene material with intent to distribute 18 U.S.C. § 1462—crime to distribute or receive obscene material through a common carrier in interstate or foreign commerce 18 U.S.C. § 1464—crime to broadcast obscene, profane, or indecent language	18 U.S.C. §§ 1465 and 1466—crime to knowingly transport or engage in the business of selling obscene, lewd, or filthy material through interstate commerce (This statute was first successfully applied to the Internet in *U.S.* v. *Thomas*[15]—which held that using a computer to transmit pornographic material violated this statute.)

Traditional attempts to criminalize child pornography:- Like issues relating to the accessibility of obscenity to children on the Internet,

depictions of child pornography or the exploitation of children have been hotly debated by civil libertarians and law enforcement officials.

Unlike debates regarding accessibility or pervasiveness of obscenity, however, traditional classifications of child pornography have remained virtually absolute in most cases. Forsaking court categorizations of obscenity, indecency, or *profanity*, the majority of legislative and judicial entities traditionally upheld even the vaguest or most obscure of all child pornography definitions, citing the potential harm to children. However, the introductions of the Internet and the access to virtual images have confounded traditional interpretations, and even the most nobly designed statutes have come under attack.

New York* v. *Ferber:- The Supreme Court, however, held that states are granted more leeway in the regulation of pornographic depictions of children than in the regulation of obscenity (756) because of the following:

1. The use of children as subjects of pornographic materials is harmful to the physiological, emotional, and mental health of the child;

2. The standard of ***Miller* v. *California*** 21 for determining what is legally obscene is not a satisfactory solution to the child pornography problem;

3. The advertising and selling of child pornography provide an economic motive for and are thus an integral part of the production of such materials, an activity illegal throughout the nation;

4. The value of permitting live performances and photographic reproductions of children engaged in lewd exhibitions is exceedingly modest, if not *de minimis;* and

5. Recognizing and classifying child pornography as a category of material outside the First Amendment's protection is not incompatible with this Court's decisions dealing with what speech is unprotected. When a definable class of material, such as that covered by [458 U.S. 747, 748] the New York statute, bears so heavily and pervasively on the welfare of children engaged in its production, the balance of competing interests is clearly struck, and it is permissible to consider these materials as without the First Amendment's protection.

THE FOURTH AMENDMENT AND OTHER LEGAL ISSUES:-

WARRANTED SEARCHES AND COMPUTERS:- Constitution requires that all warrants particularly describe the place to be searched, the items to be seized, and applicable justifications to prevent *general, exploratory rummaging in a person's belonging.*

In addition, this particularity must be so specific that unrelated items remain immune from search and/or seizure. Unfortunately, the particularity requirement may prove somewhat burdensome for officers investigating computer related crime due to characteristics unique to computers.

Seizure of Evidence:- For purposes of the Fourth Amendment, the reasonable actions that are less intrusive than a traditional arrest depends on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers, and consideration of the constitutionality of such seizures involves a weighing of the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.

Third-Party Origination: - While the scope of the Fourth Amendment is unclear in searches conducted by law enforcement, no protection exists for those searches conducted by third parties acting independently absent direction from the government.

As always, the admissibility of information collected in an investigation by a third party hinges on whether the third party was constructively acting as an agent of the government.

Courts have repeatedly ruled that files which are open to the public negate any expectation of privacy and that relinquishing computers to a third party reduces or eliminates an expectation of privacy.

Legislating Privacy:-

Federal Wiretap Act, 18 U.S.C. § 2511 and the Stored Communications Act - derivatives of the original Wiretap Act enacted in 1968. Both were included in the Electronic Communications Privacy Act of 1986 and sought

to establish federal privacy protections and standards in light of advances in computer and telecommunications technologies.

Wiretap Act - protects against unauthorized "interception" of electronic communications (18 U.S.C. § 2511)

Stored Communications Act - protects against unauthorized access to electronic communications while in electronic storage (18 U.S.C. § 2701)

CALEA (Communications Assistance for Law Enforcement Act of 1994) - also known as Digital Telephony Act (47 U.S.C. § 1002). Amendments to the Federal Wiretap Act in 1994 extended protection to cordless and cellular calls. The legislation mandates that new technology does not interfere with and does not impede some law enforcement interception. It prohibits telephone carriers from developing technology which impedes law enforcement investigations (i.e., electronic interception). In addition, Congress required carriers to configure their systems to ensure the privacy and security of communications not authorized to be intercepted.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 - was enacted by Congress in response to the rulings by the Supreme Court. It delineated specific requirements for wiretapping. It stated that wiretaps are only permissible if issued upon a ruling of probable cause by a court official. It also required that all other investigative techniques were exhausted and that precautions were taken to ensure that "innocent" conversations were excluded from analysis. It further outlined punishments for violations, and required disclosure of such surveillance upon cessation of activity.

Foreign Intelligence Surveillance Act (FISA–1978) - Congressional act which regulated wiretapping in national security cases. Much broader than Title III, it allows more invasive searches with a lower probablecause threshold. The most important differences include

(1) No requirements to disclose the contents of or even the presence of the surveillance, unless the government seeks to introduce them in a criminal prosecution;

(2) Affords no protection for individuals who are not permanent residents or citizens of the United States;

(3) Does not necessarily require *criminal* activity—rather, it allows surveillance for individuals who are believed to be engaged in clandestine intelligence activities on behalf of a foreign power.

Comprehensive Crime Control Act (1984) - Congress extends to the U.S. Secret Service jurisdictional powers over credit card fraud and computer crime.

UNIT – V

Syllabus:- Computer forensic cases: Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence –Processing Evidence and Report Preparation – Future Issues.

DEVELOPING COMPUTER FORENSIC SCIENCE CAPABILITIES:-

Identify the procedures, policies, and practices that constitute the development of an effective computer forensics unit within a department.

Like other units found within law enforcement agencies, the development and regular review of **standard operating procedures (SOP)** are essential as technology changes.

MD5 Hash as a Verification Tool:- Although there are an infinite number of files which may be created and stored on any given system, there are only a finite number of hash values available.

Thus, it has been argued by some defense attorneys that the dawning of increasingly sophisticated machines will eventually lead to the creation of two disparate files with the same generated hash value.

However, Brian Deering (NDIC) analogizes the chance of randomly generated matching hash values to hitting the Pennsylvania Lottery Super 6, 5.582×1041 (or 558,205 billion, billion, billion, billion) times before this will occur. Thus, it does seem computationally infeasible to produce two messages having the same message digest.

Choosing Appropriate Tools:- Unfortunately, there is no magic formula for success in computer forensics. Information contained within affidavits, warrant parameters, number of personnel, and investigative tools will vary widely based on case characteristics. As such, forensic toolkits should be specifically tailored to individual searches or seizures. At a minimum, the following factors must be considered in the development of investigative approaches:

• Type of suspect device

• Type of suspect operating system

• Type of software applications employed by suspect device

• Type of hardware platforms characterizing suspect device

• Application of appropriate domestic and international law

• Potential negative repercussions (i.e., liability, public concern,or bad publicity)

SEARCHING AND SEIZING COMPUTER RELATED EVIDENCE:-

Traditional Problems Associated with Finding Digital Evidence:-

- ✓ Unlike traditional investigations in which forensic experts are tasked with analysis of criminal evidence, computer-related investigations often require role multiplicity on the part of investigators.

- ✓ In fact, computer crime investigators are often forced to act as case supervisors, investigators, crime-scene technicians, and forensic scientists.

- ✓ Such duality is further exacerbated by characteristics unique to digital evidence.

- ✓ First and foremost, digital evidence is especially volatile and voluminous, susceptible to climatic or environmental factors as well as human error. It may be vulnerable to power surges, electromagnetic fields, or extreme temperatures.

- ✓ Unlike traditional evidence in which analysis of small samples is utilized to preserve the totality of the evidence, assessment of digital evidence requires evaluation of the whole, making investigative mistakes quite costly.

- ✓ In fact, this characteristic may increase the potential of liability for criminal investigators if mistakes result in loss of critical data.

- ✓ Such is not the case with traditional evidentiary matters. (Mishandling of powdered substances or serological material rarely results in catastrophic damage to business operations, as does the destruction of business records or accounting spreadsheets.)

- ✓ The sheer volume of digital evidence further complicates its recovery, making it virtually impossible to conduct on-scene analysis.

- ✓   As such, investigators often overlook the significance of certain material or seize information which is not included in the warrant application.

- ✓ (Imagine searching for a stolen diamond ring at Chicago's O'Hare International Airport—securing the airport, ceasing all mobility, questioning all individuals present, searching every area, and releasing the scene in a timely manner.)

- ✓ Digital evidence is also unique in its level of camouflage possibilities, lending itself to concealment by individuals desiring to hide information.

- ✓ In essence, computer ne'erdo- wells may hide incriminating evidence in plain sight without damaging its utility.

- ✓ This is in direct contrast to many types of traditional evidence. (Imagine hiding cocaine by mixing it with sugar.) In fact, the software community and other interest groups are actively campaigning and creating tools counterproductive to computer investigations.

- ✓ Traditionally, individuals well-trained in computers could recover files relatively easily, using tools such as Norton Utilities' Un erase.

- ✓ It was a rare occurrence when systems and data were configured with multiple levels of security.

- ✓ The advent of encryption and steganography programs has made the process of recovering data increasingly complex.

- ✓ Currently, adequate tools exist to break through most of these layers. However, one look at hacker and civil libertarian pages reveals a new trend in software—ensuring privacy from all, but especially their self-identified nemesis, the government.

- ✓ Self-destructive programs are also readily available for private consumption, allowing users to sabotage their own systems upon unauthorized access.

- ✓ This may be likened to a cache of explosives with a triggering mechanism.

- ✓ Unfortunately for law enforcement, these characteristics create an inauspicious environment for the standardization of procedures.

- ✓ Indeed, the method of analysis of computer evidence is always contingent upon case characteristics. In some cases, for example, it may be necessary to shut off a computer.

- ✓ To prevent remote destruction, while in others the action of disconnecting the power supply may result in irreparable damage to computer programs and the corresponding data.

- ✓ Investigative agencies should develop strict search and seizure policies for computer- related scenes to reduce the potential for evidence contamination or destruction by untrained personnel.

- ✓ Computer crime investigators and/or computer experts should be present at all scenes in which digital evidence may be collected. Their presence and direction will be essential during both the investigation and the courtroom process.

- ✓ Indeed, individuals with technical expertise are critical to the success of both the criminal investigation and the subsequent legal prosecution of computer-related crime.

- ✓ As with training practices and personnel management, such lists should be evaluated and updated on a regular basis. Complex networks, multiuser systems, and unique operating systems may require the need for external assistance even in well-staffed computer crime units.

- ✓ Coupled with the establishment of a forensic lab, the identification and utilization of such experts should minimize potentially negative outcomes.

Pre-Search Activities:-

- ✓ Regardless of case characteristics, the construction and maintenance of a technologically sound forensic laboratory is the foundation for successful case disposition.

- ✓ Once in place, a forensic laboratory is critical for the analysis of computer-related evidence and courtroom presentation.

✓ However, even the best forensic laboratory and analyst may be rendered moot if the investigation is conducted in a haphazard manner or exhibits.

✓ Disregard for legal specifications. Thus, preanalysis activity is equally important and worthy of comparable attention to detail.

✓ This includes all pre-search activities (i.e.,warrant preparation, intelligence gathering, assembling an execution team, planning thesearch, and assigning responsibilities) and on-scene processing (i.e., executing the warrant, securing the scene, evidence collection and preservation, and the transportation of evidence).

✓ As stated, all phases of evidence identification, collection, preservation, and analysis are necessarily interdependent and will directly impact the success of a criminal prosecution regardless of case characteristics.

✓ Computer crime investigators, like their non technological counterparts, should remember that advance planning ensures the success of evidence collection.

✓ Proper intelligence gathering, for example, enables the investigative unit to collect the right experts, evidence containers, forensic software, and the like, while providing a blueprint for the corresponding warrant application.

✓ Thus, all investigators should carefully evaluate the scene in question and familiarize themselves with case parameters and applicable legal tools at their disposal.

✓ Tools specifically designed to facilitate the collection of this type of evidence include, but are not limited to, state law; the USA Patriot Act; the Foreign Intelligence Surveillance Act; and the Communications Assistance for Law Enforcement Act,

✓ Which requires telephone companies, Internet service providers (ISPs), and other communication carriers to provide technical assistance to carry out a legitimate law enforcement mission?

✓   Technological aspects notwithstanding, investigators may also rely on proven techniques for intelligence gathering, such as surveillance, undercover reconnaissance, informants, criminal histories, known photographs, and the like. Utility checks or architectural archives, for example, may be helpful in securing blueprints, floor plans, or maps of the are in question—essential not only for scene security but also for their illustration of electrical and telephone outlets.

Warrant Preparation and Application:-

✓ Available, operating systems, storage devices, and hardware specifications should be included in warrant applications.

✓ Such articulation insures that searches are tailored the particulars of the case at hand, and that evidence collected within the parameters of the warrant will withstand future judicial scrutiny.

✓   As with other issues in the investigation of computer-related crime, there are no givens in computer search warrants.

✓ Each case will vary based on scene characteristics and corresponding judicial jurisdiction.

✓ Although they are within the same system, federal circuit courts have issued widely differing opinions.

✓ Thus, investigators must be aware of the corresponding legislative an jurisprudential climate in their area and structure their application accordingly.

✓ As warrants provide a cornucopia of legal issues at the trial level, the importance of warrant preparation cannot be overstated.

✓ Thus, any warrant application should be reviewed by as many specialists (i.e., computer investigators, legal counsel, etc.) as possible prior to magistrate approval.

✓ This ensures that it will include all of the relevant protection and language. In addition, it ensures that all equipment, media, and incidental which may prove evidentiary are included.

✓ The investigator, which ensures judicial approval. (Unlike other

criminal search warrant applications, which are routinely processed

without much scrutiny, investigators should painstakingly point out the essentials to any judicial officer.

✓ This includes explaining terminology and defining case characteristics. This makes the warrant itself more defensible

✓ In court. However, it does not negate the possibility of issues related to the actual execution of the said warrant.) *Remember:*

✓ he first step in the preparation of any warrant application is the operationalization of the crime itself and, more specifically, defining

✓ The role of the computer in it. Such characterizations necessarily outline the scope of the corresponding search and seizure and are essential for the establishment of probable cause.

Seizing Equipment:-

✓ Probable cause notwithstanding, investigators must also justify the seizure of equipment which does not necessarily represent an instrument of the crime.

✓ As warrants are issued under the provisions found within the Fourth Amendment, it is essential that investigators clearly substantiate any requests for seizures of equipment.

✓ This will minimize claims of unconstitutional deprivations. It is highly recommended that investigators request explicit permission to seize all hardware and storage devices that are constitutionally justifiable, as on-site analysis might negate the utilization of some forensic approaches.

✓ (Investigators should be aware that such requests are often denied in cases where equipment is essential for business operations.) As always, fruits of the crime, criminal contraband, and those items criminally possessed may be seized without judicial authority.

No-Knock Warrants:- If exigent circumstances dictate it, a request for a "no-knock" warrant should be included in the application.

✓ As always, exigent circumstances would include the nature of the offense (violent vs. nonviolent), the potential for evidence destruction,

the sophistication and maturity of the target, and the absence of resident.

✓ With the vulnerability of computer data, investigators should be able to present a case to the magistrate for rapid entry if the suspect has prior knowledge of the search or if he or she has the technical expertise to destroy evidence.

✓   Although these types of warrants are much harder to justify and are closely scrutinized by the courts, investigators should attempt to obtain one in any situation in which case characteristics dictate it.

Preparing   a   Toolkit:-

Traditional Equipment:-

1. Evidence tape:- used to mark the perimeter of the crime scene; it not only prevents entry by individuals external to the investigation but also induces caution among on-scene personnel.

2. Packing tape:- used to secure evidence containers.

3. Evidence storage containers and labels:- although standard evidence labels are appropriate for computer-related evidence, special care should be devoted to the packaging materials used in these investigations, as evidence may be especially vulnerable. (Although the optimum packaging material (i.e., original) is often unavailable, investigators may solicit similar materials from computer stores, large corporations, and universities.) Additional packaging materials include, but are not limited to, jewel cases for protecting CD/DVDs; evidence envelopes for thumb drives and other portable storage devices; a multitude of folding boxes and paper bags; and antistatic peanuts. **Antistatic**, **conductive**, and **Faraday bags** are especially important in the storage, analysis, and transportation of digital   evidence. Usually characterized by distinctive colors (pink or black for polyethylene and silver for metalized PET film and other plastics), antistatic or conductive bags may be used to prevent data loss caused by static electricity. Faradaybags, on the other hand, are specifically designed to shield wireless devices (i.e., smartphones, Bluetooth, netbooks, tablets, and computers)   from remote corruption or deletion of data from cellular, Wi Fi, Bluetooth, and

radio signals. Investigators may purchase specialized Faraday bags or cages from various vendors or create their own. Faraday bags should be used for all devices with wireless capabilities.

4. Miscellaneous writing and labeling materials:- used to label evidence, maintain the chain of custody, and document scene characteristics.

    a. Materials to sketch the crime scene (i.e., graph paper, ruler, pencils, etc.)

    b. Blank forms, including inventory, evidence booking, search warrant templates, etc.

    c. Writing utensils (e.g., pens, markers, and highlighters). Indelible markers, such as laundry pens, are especially useful for marking floppies.

    d. Labels

    e. Note cards (usually 3–5)

    f. Stick-on circles for marking evidence

    g. Adhesive numbers or large labels for marking cards and cables

5. Sanitary materials:- used to prevent evidence contamination and to protect investigators from unsanitary environments. Such materials include, but are not limited to, rubber gloves, bleach, and disposable wipes.

6. Flashlight:- used in the event of a power outage or to illuminate dark areas (particularly useful under desks, behind equipment, and the like).

7. Extra batteries:- used to ensure continuity of investigative equipment, including, but not limited to, cameras, flashlights, cellular telephones, tape recorders, etc.

8. List of contacts:- including contact information about software support, computer experts, hardware manufacturers, magistrate's office, and support organizations.(e.g., HTCIA and FCIC).

9. Mobile carts or evidence transport units:- used to transport multiple containers and heavy equipment and investigative equipment.

10. Wireless communications:- used as mode of communication and point of contact while on-scene. (Investigators should not use suspect phone.)

11. Photographic equipment (camera, batteries, extra film):- used to produce visual documentation of crime scene. Such equipment should be

provided to investigators as well as scene photographers, while the latter should be equipped with magnification capabilities. As always, scenes should also be videotaped if departmental resources permit.

12. Nonmagnetic screwdrivers, hex wrenches, and players:- used to open computer boxes. Often overlooked, such tools are necessary for getting to the guts of the computer. (Although extremely unlikely to erase data, electric screwdrivers do emit magnetic fields. Thus, manual tools are preferred.)

13. Small diagonal cutters:- used for cutting nylon wire ties which are commonly utilized to secure multiple wires for organizational purposes.

14. Hammer or nail puller:- used for removing nails which secure multiple wires.

Computer-Specific Equipment and Materials:-

1. Multiple boot disks:-

 ➢ Used to avoid self-destructive programs employed by the suspect and to minimize changes to a suspect drive (i.e., during the routine boot process, disk space is reassigned and file slack may be overwritten).

 ➢ It is highly recommended that investigators maintain custom boot disks which will boot to controlled specifications. At an absolute minimum, investigators should have a Windows boot disks with imaging capabilities. Investigators should include a Terminate and Stay Resident (TSR) virus shield on their investigative systems and on any boot disks taken to the scene. Some examples include McAfee's *VSHIELD* and *FPROT*. Investigators should *remember* to update this file on a regular basis. Unlike other programs traditionally found on boot disks which do not necessitate updating, the antivirus software should be the most current. Boot disks should also include storage enhancement programs and popular drivers for computer peripherals. A custom boot disk should boot to controlled specifications.

2. Backup hardware and miscellaneous computer peripherals:-

    a. New hard drives:- They are the external devices and corresponding media to capture image of suspect drive. They may vary based on case

characteristics (e.g., size and number of suspect drives, amount of data) and departmental resources.

b. Color scanner:- Used to record potential evidence which may not be seized.

c. Color printer and an assortment of computer paper:- used to capture potential evidence residing in print buffers in those cases where on-scene printers are not included w thin the specifications of the applicable warrant. Printers may also be used to print additional forms, labels, and the like.

3. Antivirus software:- used for the documentation and validation of suspect machines and the prevention of infection of forensic machines.

4. Imaging software:- used for the preservation of the original evidence. As mentioned previously, all forensic analysis should be conducted on the forensic image, ensuring the integrity of the suspect data.

5. Application software.

6. Forensic software:-used for on-site evidence analysis (discussed in greater detail in the previous chapter).

a. Viewers enable investigators to quickly scan the contents of large numbers of computer files, providing, among other things, a rapid mechanism for identification of criminal contraband.

b. Text editors enable investigators to quickly search for keywords applicable to the current investigation.

c. Hex editors enable investigators to view files in hexadecimal formats and quickly search for files which may have been intentionally manipulated or which have been erased or deleted.

d. Password crackers enable investigators to circumvent many security measures employed by the suspect.

e. Verification software is used to demonstrate the validity of the imaged drive.

f. Time/date programs verify the system time on the suspect machine.

g. Wiping programs enable investigators to completely delete (i.e., wipe) files representing criminal contraband if seizure is not possible.

h. Locking programs ensure data integrity, preventing intentional or accidental manipulation of data.

i. Fuzzy logic tools.

j. File cataloging and indexing enable compartmentalizing of evidence for ease in further analysis and organization.

k. Recovery enables investigators to retrieve data from corrupted media, including hidden and deleted files.

l. Imaging helps to create an image of all areas of a data carrier. As discussed in the previous chapter, a bit stream image is an exact replica of each bit contained on the suspect drive.

m. Other forensic software depends on investigator expertise, case characteristics, and on-scene personnel. May include popular forensic packages like Encase, FTK, etc.

7. Extra media:- used for a variety of purposes including, copying potential digital evidence and creating additional boot disks.

8. Extra cables, serial port connectors, and gender changers:- used for connecting forensic units to suspect machine.

9. Extension cords and/or power strips:- used to connect machines to power supplies.

10. Surge protectors and/or UPS (uninterruptible power supply):- used to ensure electrical and telephonic continuity to prevent possible destruction of computer data.

11. Cell phone analysis software and necessary hardware:- used to read SIM cards and recover information contained on the increasingly popular smart phones.

12. Open purchase order:- although difficult to secure, optimal situations provide open purchase orders as the unexpected may occur. While investigators are strongly encouraged to provide for any possible situation and prepare investigative toolkits accordingly, they are often confounded by those situations which they had deemed impossible.

Securing the Crime Scene:-

1. Dangerous individuals or safety hazards must be immediately recognized and contained.

2. All computers must be located and secured.

3. All personnel must be removed from the immediate area of the evidence.

4. Network connections must be ascertained and appropriate action taken. (Depending on the particular case, the network administrator may prove to be quite helpful in this respect. She or he may immediately disable network access, preventing possible remote destruction.)

5. All suspects should be immediately separated and escorted to a predetermined location.

6. All computers should be protected by a police officer. This is necessary to ensure that the computer is not manipulated in any way—remotely or not. While many of the concerns involve remote destruction, it is not always possible to sever network connections immediately. Thus, some computers may remain vulnerable to outside actions.

PROCESSING OF EVIDENCE AND REPORT PREPARATION:-

How to Validate Your Forensic Tools:

Amber Schroader, Paraben Corporation

There are many issues out there that can disrupt even the best of forensic investigators.

One of these issues that are paramount is the validation of the technology associated with doing a digital forensic validation.

The tool examples used in this booklet will be for mobile forensic validation. Throughout the booklet you can substitute any software title with another or any other software tool with another.

Selecting a Forensic Tool

The selection of technology is often the hardest for any forensic examiner as there are many excellent choices out there. There are some basic rules that can be applied to be able to weed through the variety of materials on each of the tools available to help select the best options.

Ask the following questions when selecting digital forensic technology:

• **Is it read only?**

• Yes

• No

Can I repeat my results?

• What are your validation steps?

• **Is the data verified and if so how?**

• What hash values are used?

• Can those values be repeated?

• Are there other validations?

• **Was it designed for forensics, and is the images gathered valid?**

• Is it a commercial tool that is being used in forensics?

• How is the image file created?

The scientific process.
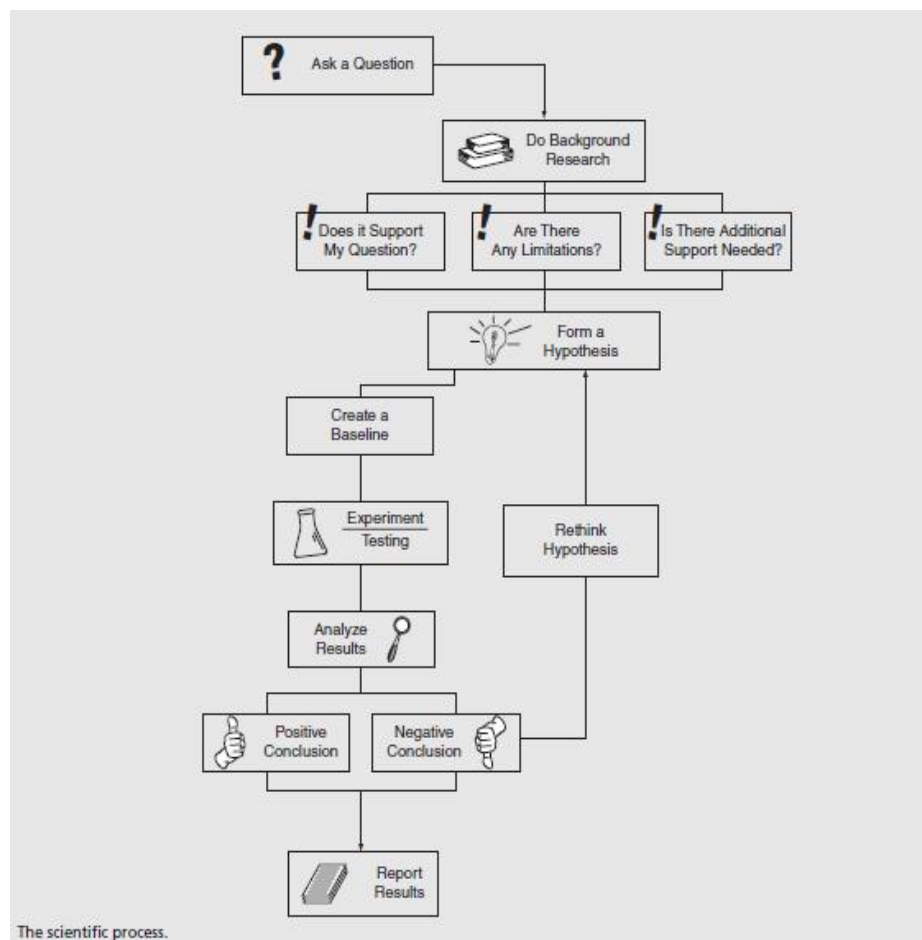
These are just the basics, but they are an excellent starting point to working through the process of tool selection. Once the tools are selected, licensed, and validated, an additional ranking system can be used based on the efficiency of the tool and results that are gathered, and they can be used in a Tier system of Tier 1, Tier 2, or Tier 3 tool. Remember, it is always important to use more than one tool in the processing of digital evidence.

What Makes Digital Forensics a Science?

In order for digital forensics to be the true practice of a science, the processes used must be repeatable and proven. If the examiner does a process that is haphazard or too varied from one examination to the next, the science then becomes more of an arbitrary art.

The Scientific Process

According to popular science Web sites, the process normally starts with a question that forms into a hypothesis. Here are my suggested changes:

> Scientific method: basic steps that scientists follow in uncovering facts and solving scientific problems.

> The scientific process is based on gathering, observing or investigating, and showing measurable and repeatable results. Most of the time the scientific process starts with a question that leads to a hypothesis that leads to experimentation and then a conclusion.

> When it comes to using the scientific process for validation of technology, the process stays the same.

Start with a Question

How well does Device Seizure support Motorola phones?
This is a very broad question that after some minor experimentation can then be refined to a more exact hypothesis:
How well does Device Seizure support CDMA Motorola phone physical and logical acquisitions?
This more exact hypothesis allows for specific experimentation to be done validating the statement with a positive or negative result. This same hypothesis can then be used in the validation process for any tool with a simple substitution of the software name. The area that takes the longest in any scientific process is the experimentation stage or, in the process of using this for technology the validation stage. This is where you have to setup specific devices and work with a baseline of that device and then add data to specific areas of the device. Acquisitions would have to be done after each addition to validate the primary baseline.
This principle is the same as if I were slowly adding one chemical to another to test the results; it is done drop by drop and evaluated after each addition or change to the baseline. Once a complete baseline is done full testing can begin with each tool that will be processed through the hypothesis. After all of the experimentation is done, you have your validation results that have to be analyzed and evaluated to see if you have a positive or a negative conclusion.

Settling up a Base Image

To setup a base image one, must first define what should be tested in the base image and any limitations for that image.

For Mobile Phone Forensics

1. Select a device that falls in the parameters of the hypothesis.
2. Gather information on the device from the manufacturer or from *www.phonescoop.com*, which has a full list of the base manufacturer details.
   Example from *www.phonescoop.com*

Modes	CDMA 850 / 1900
Weight	3.49 oz (99 g)
Dimensions	3.9" × 2.1" × 0.57" (99 × 53 × 14.5 mm)
Form Factor	Clamshell Internal Antenna
Battery	Talk: 3.3 hours max. (200 minutes) Standby: 325 hours max. (13.5 days) 780 mAhLilon
Display	Type: LCD (Color TFT/TFD) Resolution: 176 × 220 pixels Colors: 65,536 (16-bit)
Platform / OS	(proprietary)
Processor	Unknown
Memory	30 MB (internal memory available to user for storage)
Phone Book Capacity	1000
FCC ID	IHDT56FT1 » (Approved September 1, 2005)

3. Place items in a chart and determine what the basic data capabilities and storage of the device are:

Available Data	Data Input
Phonebook	
SMS	
Call Logs	
Camera	
Video	
Custom Ring tone	
Note System	
Calendar	
File System	

(continued)

4. Input data into the given areas of the device and record results:

Available Data	Data Input	Date Input	Data Deleted	Date Deleted
Phonebook	5 People input with complete details	5/1/2010	2 People deleted to complete the removal of all details	5/2/2010
SMS				
Call Logs				
Camera				
Video				
Custom Ring tone				
Note System				
Calendar				
File System				

This chart system should be filled in with as many exact details as possible. This will establish the baseline of available data on the device that your tool should be able to recover in the process. The validation plan should be kept with the device so that you can use the same baseline to revalidate new releases of the tool.

Designing a Proper Test Plan or Validation Plan

Here are the key areas for the experimentation or testing and validation stage of the process.

1. **Scope of the Plan**
   - Testing version

   What version of the tool will you be testing, be as exact as possible with the build number if possible.

   - Testing manufacturer

   This is where you will add the details of what device you are testing from your selection of baseline devices.

2. **How often will the test be redone?**

   This is something you should establish based on your organization standards; it is very typical to retest technology quarterly or biannually at the very least.

3. **Create baseline for test.**
   - Manufacturer details
   - Make, model, different flash versions

   This is noted in the section above about creating a baseline.

4. **Establish base parameters for tool.**
   - Known issues, bugs, limitation

   This is something you can typically get from the manufacturer of the technology that you retest. This will allow

you to establish the correct test parameters; a tool cannot fail in an area that it was not designed to support in the first place.

5. **Evaluate your base parameters against manufacturer.**

   Make sure the data you input is available for download from the device and is supported by the flash of the provider you are using. It is common for different providers to disable certain functions in devices based on the services they provide on your network. It is important to know what is and is not supported in your device.

6. **Run test image of baseline.**
   - Archive test image and version of tool

   This is the stage that you create a base image of the phone and make sure the data you input into the device is recovering properly and showing in your base image. You archive your results to insure that you have them as backup if they are needed for court purposes or to show your testing and validation process.

7. **Compare results with tool manufacturer if available.**

   If your tool manufacturer has available test baselines for you to evaluate, you can ask them to share their results. Sometimes their testing process will vary, but be assured that each manufacturer does do some type of testing process for their technology.

8. **Repeat process and note differences.**

   As a general rule of thumb, the results done through the experimentation or testing and validation stage must be repeated.

   Some example charts are given below that show how you can record the basics of your testing:

Test Results

Test Process 1

Available Data	Data Input	Data Acquired	Data Missed
Phonebook			
SMS			
Call Logs			
Camera			
Video			
Custom Ring tone			
Note System			
Calendar			
File System			

Test Process 2

Available Data	Data Input	Data Acquired	Data Missed
Phonebook			
SMS			
Call Logs			
Camera			
Video			
Custom Ring tone			
Note System			
Calendar			
File System			

Test Process 3

Available Data	Data Input	Data Acquired	Data Missed
Phonebook			
SMS			
Call Logs			
Camera			
Video			
Custom Ring tone			
Note System			
Calendar			
File System			

Note that the above charts have you repeat the results three times. If there are any variables in the device or communication with the system, you will be able to determine if they exist in as little as three tests. You can always add more or less testing runs against your baseline, but a minimum of three is recommended.

The comparing and contrasting of certain technologies goes beyond a surface look when it comes to the use of those technologies in a scientific process. You can use the scientific process as a validation process for any forensic technology, no matter what the discipline.

Aspects of Data Analysis:-

- ✓ As stated previously, every computer investigation is different, but one rule remains the same: *document*, *document*, *and document*! Other than that, procedures may vary depending upon departmental resources, expertise of personnel, and exigent circumstances.

- ✓ Again, each agency should develop its own investigative policy (formal or informal) and follow it as closely as possible.

- ✓ This is not to suggest, however, that one policy can completely account for all circumstances that may arise. Rather, it may be analogized to a coach's playbook, which changes weekly once the competition has been rated and evaluated.

- ✓ The importance of documentation cannot be overstated. Judicial oversight and defense challenges require that scrupulous attention be directed toward the documentation of any and all activities conducted on a particular piece of evidence.

- ✓ As such, analysts should continue the documentation process which was initiated by the evidence technicians or on-scene investigators by retrieving and updating the evidence logs.

- ✓ At a minimum, lab analysis should include the name, rank, and identifying information for any individual tasked with the analysis of such evidence; the condition of the evidence upon delivery to the analyst; the date and time of evidence arrival and return; and thename, rank, and identifying information of the person delivering such evidence. (As with traditional criminal investigations, any investigator or individual wishing access to the evidence *must* sign the evidence out.

- ✓ Once this process is completed, investigators or analysts may retrieve the digital information that may reside therein.)

- ✓ As stated previously, contemporary criminal behavior often requires the analysis of computer materials.

- ✓ Using a variety of software packages, it is now possible to thoroughly analyze all of the information on each piece of storage media.

Depending on the amount of media under analysis, this process can be quite cumbersome, and case characteristics may preclude the most comprehensive manual search.

✓ Indeed, many investigators prefer to use automated programs like FTK or Encase due to their ability to quickly analyze large disks.

✓ Although it is always recommended, case characteristics may be such that a search of every single file is superfluous or unnecessary.

✓ For example, in a child pornography case where hard-copy photographs were accompanied by desktop child pornography and a directory titled "child porn" containing 400 depictions of child pornography thorough search of slack space and file swap may not be compelling.

✓ However, it may contain addresses, phone numbers, or other evidence which may incriminate others.

✓ Evidence notwithstanding, investigators should properly document all forensic software utilized, analysis techniques employed, damaged or compromised media (i.e., bad sectors, physically damaged diskettes, etc.), and evidence recovered. This documentation process should continue throughout the investigation process and should not be completed until final case disposition has been achieved.

Establish Forensically Sterile Conditions:-

✓ All media used in the analysis of computer evidence must be forensically sterile for courtroom purposes.

✓ Investigators must be able to testify as to the condition of all media prior to the imaging process.

✓ As such, it is highly recommended that all media used for imaging purposes be brand new and forensically wiped prior to analysis, as some manufacturers have sold refurbished equipment as new.

✓ However, due to limited resources, this process may not be possible for poorly funded agencies.

✓ In this case, used media should be forensically wiped clean of data using software that meets Department of Defense standards.

Hard Drive Evidence Worksheet

✓ This will prevent data corruption from previous use and data contamination from destructive programs.

Non-Windows Operating Systems

✓ Although most forensic investigations on personal computers are conducted on Windows platforms, there are occasions when other operating systems are present.

✓ Unfortunately, many local agencies may not have the resources to process and analyze such data and may have to rely upon outside experts.

✓ The two most common non-Windows operating systems relevant to computer forensics are *Macintosh* and *Unix/Linux*.

Macintosh Operating System

The Macintosh operating system was designed by Apple computers and is currently used by Macintosh computers bearing the Apple logo. Although contemporary users are more familiar with Windows products,

Macintosh computers are largely responsible for the popularization of graphical user interfaces (GUI). Traditionally, Macintosh systems were incompatible with other systems and were susceptible to data loss. Today, Macs are increasingly popular due to increased interoperability, savvy advertising, graphics capability, and mobile media. In addition, they are attractive to users who prefer seamless integration and enhanced stability.

Due to market demand, most computer forensics specialists concentrate their efforts on Windows machines. As such, there are more commercially available forensic packages for Windows than Mac. However, there are some products that have been employed on Macintosh machines.

• **Imaging:-** As in investigations involving Windows platforms, preservation of the original drive is essential. The creation of a forensic copy should be accomplished without booting the suspect computer or mounting the physical disk onto an investigative machine. In order to accomplish this, the forensic Mac should have disk arbitration disabled.11 this can be accomplished by copying the *diskarbitrationd. plist* file in the

/etc/mach/_init.d directory to an alternate location and deleting the original. Once this is accomplished, investors can connect to the target hard drive by either using Target Disk Mode or removing the hard drive and connecting it via an external enclosure. Investigators may then use the *dd* command from the terminal or *dcfldd* to create the image.12 (Investigators may prefer to use *dcfldd*, an open-source UNIX tool, which provides for simultaneous imaging and image verification.). A further option would be *MacQuisition*, a tool developed by Black Bag Technologies.

• **Finding Evidence:-** Like Windows machines, Macintoshes can contain a plethora of criminal evidence. While much of this evidence can often be located in obvious places, some may reside in unallocated space. Case characteristics will dictate other areas of interest. For example, in cases involving security breaches, investigators may wish to examine the startup items, cron tabs, and assorted configuration files and logs. In addition, evidence may reside within images, history and temp, cache files, and executable code.13

• **Forensic Toolkits**

1. Black Bag Technologies Mac Forensic Software is a comprehensive toolkit designed for Mac OS X. The suite is a one-stop shop for most investigations and includes imaging, recovery, and analysis tools. The 19 utilities contained within the package include provisions for text searching, directory browsing, image viewing, examination of file headers and metadata, and data segmentation.

2. MacForensicsLab is similar to Black Bag's suite of tools. Operating within a self-contained environment, it has additional utilities which provide for automatic note taking and reporting. Thus, users may prepare comprehensive professional reports for courtroom presentation. Finally, the program provides powerful search tools. Investigators can employ string searches to identify credit card and social security numbers or skin-tone searches to identify pornographic material.

Linux/Unix Operating Systems

Below is a *sampling* of files which may contain criminal evidence:

• /etc/passwd - this file contains information on every account created on the suspect machine. This information includes the following:

1. Account ID

2. Encrypted password

3. Numeric UserID (UID)

4. Numeric GroupID (GID)

5. Account information (typically the user's name)

6. Home directory

7. Login shell

• /etc/shadow - If the installation is configured to use shadow passwords, this file would contain the encrypted password and associated user account information.

This file is accessible via root privileges only. An asterisk symbol (*) serves as a placeholder for the encrypted password. Information regarding password management is also contained herein.

- /etc/hosts - This file contains local domain name system entries. This DNS list may be used to evaluate Web activity.

- /etc/sysconfig - This file contains assorted configuration files like, configuration of peripherals, scripts running at boot, and so on.

- /etc/syslog/conf - This file contains information which identifies the location of log files.

- /home/useraccountID/Trash - When a particular user account ID is entered, investigators can access that user's trash. This folder contains deleted files which have not been permanently released to unallocated space (i.e., emptying the trash).

SMARTPHONES and GPS Forensics:-

Smartphones:-

✓ As mobile devices become more and more like minicomputers, there is a dawning realization that they may contain criminal evidence. Indeed, as Americans become less attached to hardwired devices, a demand for mobile forensics has emerged.

✓ While this section is not intended to provide an exhaustive accounting of all issues and technologies associated with cell phones and navigation devices, it is intended to familiarize the reader with device structure, emerging issues, and generic practices.

✓ Generally speaking, most smartphones have similar features and capabilities.

✓ They contain system-level microprocessors; read-only memory (ROM); random access memory (RAM); multiple hardware keys and interfaces; touch sensitive, liquid crystal display; and support memory cards and peripherals. In addition, they contain the capability for wireless communications like Infrared, Bluetooth, or WiFi.15 However, devices

✓ Will vary by their technical and physical characteristics as well as their expansion capabilities (i.e., I/O and memory card slots, device expansion sleeves, and external hardware interfaces).

- ✓ By design, all PDAs support basic Personal Information Management applications

- ✓ Which provide users with organizational tools like address books, appointments, mailboxes, and memo management.

- ✓ They are generally categorized by their operating system: iOS (iPhone OS), Symbian, Research In Motion (RIM), Palm OS, Pocket PC, or Linux-based.

- ✓ Many of the issues involved with forensically processing PDAs are the same that are found in traditional investigations of computer systems.

- ✓ The maintenance of the chain of custody, image verification, and evidence integrity are essential elements in criminal courts and must be carefully documented.

- ✓ While there are some tools out there which are capable of copying and searching data, it is highly recommended that only forensically designed products are used.

- ✓ Typically, forensic tools perform logical acquisitions using common protocols for synchronization, debugging, and communications, and provide data recovery capabilities.16 Irrespective of resources, minimal software requirements for handheld forensics labs and toolkits include imaging, verification, and analysis tools.

- ✓ Minimum hardware requirements, on the other hand, include removable storage media, spare batteries and power supplies, SIM reader, and phone cables.

- ✓ While many of the issues surrounding handheld forensics are similar to those in traditional computer forensics investigations, there are discrepancies which constrain the way in which the tools operate.

- ✓ Unlike traditional computer operating systems, for example, the file system on certain systems resides in volatile versus nonvolatile memory.

- ✓ This is extremely important to criminal investigations as data may prove more vulnerable on handheld devices.

✓   At the same time, the default hibernation mode of such devices mayprove useful to investigators as processes and applications remain active even on idle devices.

✓ Finally, the handheld market is characterized by product cycles that are far shorter than traditional computer technology.

✓ As a result, forensic tools should be chosen carefully, and vendors which have demonstrated a history of innovation and product adaptation should be strongly considered

Navigation Systems:

✓ The current emphasis on consistent accountability via mobile communications has been mirrored by an increasing demand for devices that maximize personal efficiency and time management.

✓ Toward this end, navigation systems allow individual users to avoid traffic, identify fastest destination routes, and eliminate unnecessary detours. In addition, they allow corporations to monitor employees' use of company resources.

✓   Coupled with these advantages are falling prices as vendors compete for market share.

✓ As a result, the popularity of both in-dash and portable units has surged internationally, and millions of individuals across the globe use the devices daily.

✓ Fortunately for law enforcement, such technological dependence has resulted in a new avenue for evidence acquisition in criminal investigations.

✓ More specifically, they contain the following data:

- **Ephemeris data -** This information contains the precise location of the satellite and the locations of all other satellites in the system.

- **Almanac data -** This information includes the time and date of signal transmission and the operational status of the satellite at the time of transmission.

- **Pseudorandom code -** This information is simply an identification code for the particular satellite transmitting the signal.

Report Preparation and Final Documentation:

✓ The development of a forensic laboratory and the collection and analysis of digital evidence are critical in criminal investigations.

✓ However, successful prosecution of computer-related offenses often hinges upon formal reporting and the competency and credibility of courtroom witnesses.

✓ Incomplete reports or inconsistent testimony can negate even the best-run investigations.

✓ Witnesses who are uncertain as to all aspects of their analysis or hesitant in their findings may be discredited or impeached during cross-examination.

✓ In addition, evidence may be ruled inadmissible if a proper chain of custody cannot be established.

✓ Thus, it is essential that investigators are properly trained in all methods employed and maintain comprehensive logs of their activities.

✓ Such logs include both traditional and computer-generated reports.

✓ Traditional documents typically include documents relating to the chain of custody of physical evidence, logs of crime-scene activity and evidence collection procedures, and the like.

✓ Computer generated reports, on the other hand, typically involve those activities associated with data analysis.