TYPES OF COMPUTER FORENSICS TECHNOLOGY:

Types of Military Computer Forensic Technology:-

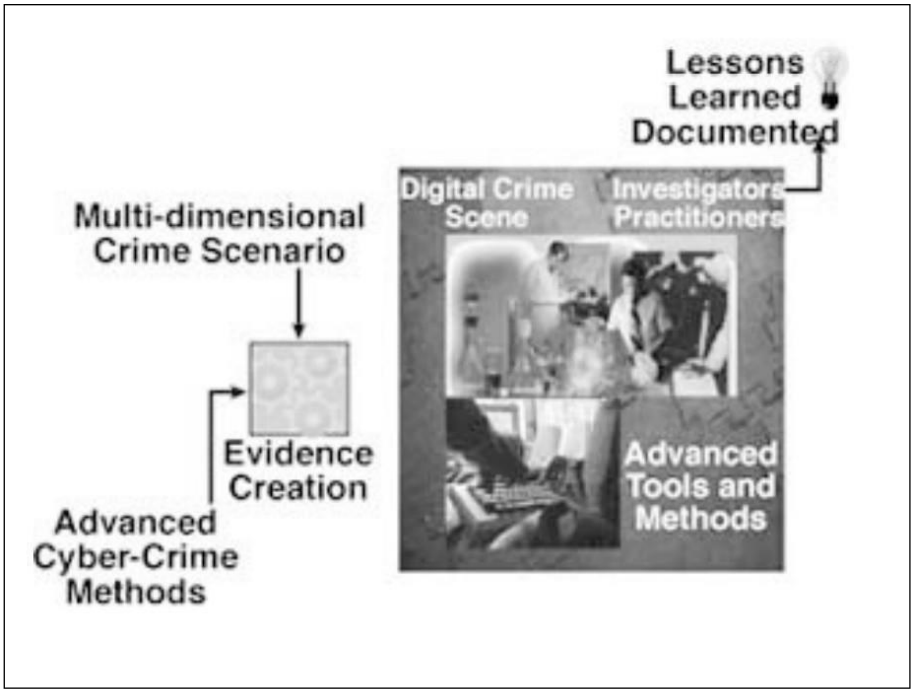
- Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and assessment of the intent and identity of the criminal.
- Real-time tracking of potentially malicious activity is especially difficult when the related information has been intentionally hidden, destroyed, or modified in order to avoid discovery.
- National Law Enforcement and Corrections Technology Center (NLECTC) works with criminal justice professionals to identify urgent and emerging technology needs.
- National Institute of Justice (NIJ) sponsors research and development or identifies best practices to address those needs.
- The information directorate entered into a partnership with the NIJ via the auspices of the NLECTC, to test the new ideas and prototype tools. The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership.

COMPUTER FORENSIC EXPERIMENT-2000 (CFX-2000)

- ✓ CFX-2000 is an integrated forensic analysis framework.
- ✓ The central hypothesis of CFX-2000 is that it is possible to accurately determine the motives, intent, targets, identity, and location of cyber criminals and cyber terrorists by deploying an integrated forensic analysis framework.
- ✓ The cyber forensic tools involved in CFX-2000 consisted of commercial off-the-shelf software and directorate-sponsored R&D prototypes. CFX includes SI-FI integration environment.
- ✓ The *Synthesizing Information from Forensic Investigations* (SI-FI) integration environment supports the collection, examination, and analysis processes employed during a cyber-forensic investigation.
- ✓ The SI-FI prototype uses digital evidence bags (DEBs), which are ***secure*** and ***tamperproof containers*** used to store digital evidence.
- ✓ Investigators can seal evidence in the DEBs and use the SI-FI implementation to collaborate on complex investigations.
- ✓ Authorized users can securely reopen the DEBs for examination, while automatic audit of all actions ensures the continued integrity of their contents.
- ✓ The teams used other forensic tools and prototypes to collect and analyze specific features of the digital evidence, perform case management and time lining of digital

events, automate event link analysis, and perform steganography detection. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

- ✓ **The results of CFX-2000 verified that the hypothesis was largely correct and that it is possible to ascertain the intent and identity of cyber criminals.**
- ✓ **As electronic technology continues its explosive growth, researchers need to continue vigorous R&D of cyber forensic technology in preparation for the offensive of cyber-attacks.**



Types of Law Enforcement Computer Forensic Technology:-

Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management. Law enforcement and military agencies have been involved in processing computer evidence for years.

Computer Evidence Processing Procedures

The Processing procedures and methodologies taught in a computer forensics course should follow the federal computer evidence processing standards.
Training and certification programs have also been developed for the International Association of Computer Investigation Specialists (IACIS).
For these reasons, computer forensic trainers and instructors should be well qualified to teach the correct computer-processing methods and procedure

Preservation of Evidence

- ✓ **Computer evidence is fragile (delicate) and susceptible to alteration by any number of occurrences.**
- ✓ **Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.**
- ✓ **Black box computer forensics software tools are good for some basic investigation tasks, but they do not offer a full computer forensics solution.**
- ✓ **SafeBack software overcomes some of the evidence weaknesses inherent in black box computer forensics approaches.**
- ✓ **SafeBack technology has become a worldwide standard in making mirror image backups since 1990.**

TROJAN HORSE PROGRAMS

- ✓ **The computer forensic expert should be able to demonstrate his or her ability to avoid destructive programs and traps that can be planted by computer users bent on destroying data and evidence.**
- ✓ **Such programs can also be used to secretly capture sensitive information, passwords, and network logons.**

COMPUTER FORENSICS DOCUMENTATION

- ✓ **Without proper documentation, it is difficult to present findings.**
- ✓ **If the security or audit findings become the object of a lawsuit or a criminal investigation, then documentation becomes even more important.**

FILE SLACK

- ✓ **File Slack, also called ‘slack space’, is the leftover space on a drive where a file is stored.**
- ✓ **The occurrence of random memory dumps in hidden storage areas should be discussed and covered in detail during workshops.**
- ✓ **Techniques and automated tools that are used to capture and evaluate file slack should be demonstrated in a training 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 also be discussed and demonstrated during the training course.**
- ✓ **The participants should be able to demonstrate their ability to deal with**

slack and should demonstrate proficiency in searching file slack, documenting their findings, and eliminating the security risk

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.
- ✓ Computer forensic experts should understand such issues and tools that help in the identification of such anomalies.

E-COMMERCE INVESTIGATIONS

- ✓ A new Internet forensic tool has recently been introduced that aims to help educators, police, and other law enforcement officials trace the past World Wide Web activity of computer users.
- ✓ Net Threat AnalyzerTM, from Gresham, Oregon-based New Technology Inc. (NTI), can be used to identify past Internet browsing and email activity done through specific computers. The software analyzes a computer's disk drives and other storage areas that are generally unknown to or beyond the reach of most general computer users.
- ✓ Net Threat Analyzer available free of charge to computer crime specialists, school officials, and police.

DUAL-PURPOSE PROGRAMS

- ✓ Programs can be designed to perform multiple processes and tasks at the same time. Computer forensics experts must have hands-on experience with these programs.

TEXT SEARCH TECHNIQUES

New Technology Inc. has also developed specialized search techniques and tools that can be used to find targeted strings of text in files, file slack, unallocated file space, and Windows swap files.

Each participant will leave their training class with a licensed copy of their TextSearch PlusTM software and the necessary knowledge to conduct computer security reviews and computer related investigations

FUZZY LOGIC TOOLS USED TO IDENTIFY UNKNOWN TEXT

- ✓ **New Technology Inc. has also developed a methodology and tools that aid in the identification of relevant evidence and unknown strings of text.**
- ✓ **Traditional computer evidence searches require that the computer specialist know what is being searched for. However, many times not all is known about what may be stored on a given computer system.**
- ✓ **In such cases, fuzzy logic tools can provide valuable leads as to how the subject computer was used. The training participants should be able to 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

- ✓ **Computer forensic experts must understand 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 unclear places on floppy diskettes and hard disk drives.**

Data Encryption

- ✓ **A 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 (file slack, unallocated file space, and Windows swap files).**

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 (urge) 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:-

Finally, let's briefly look at the following types of business computer forensics 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)* is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center.**
- ✓ **No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.**

CREATING TRACKABLE ELECTRONIC DOCUMENTS

- ✓ ***Binary Audit Identification Transfer (BAIT)* is a powerful intrusion detection tool that allows users to create *trackable* electronic documents.**
- ✓ **BAIT identifies (including their location) unauthorized intruders who access, download, and view these tagged documents.**

- ✓ **BAIT also allows security personnel to trace the chain of custody and chain** of command of all who possess the stolen electronic documents.

THEFT RECOVERY SOFTWARE FOR LAPTOPS AND PCS

When you lose your wallet, the last thing you think of is how much it is going to cost to replace your wallet. The same is true when equipment (especially a computer) is stolen. Our elders always told us, an ounce of prevention is worth a pound of cure. They were right. Think about what it really costs to replace a stolen computer.

- The price of the replacement hardware.
- The price of replacing the software.
- The cost of recreating data. If possible at all, do you keep perfect back-ups?
- The cost of lost production time or instruction time.
- The loss of customer goodwill (lost faxes, delayed correspondence or billings,
- Problems answering questions and accessing data).
- The cost of reporting and investigating the theft, filing police reports and insurance claims.
- The cost of increased insurance processing and ordering replacements, cutting a check, and the like.
- The cost of processing and ordering replacements, cutting a check, and the like.
- If a thief is ever caught, the cost of time involved in prosecution.

So, doesn’t it make sense to use an ounce of prevention? You don’t have to be a victim.

With that in mind, SecurityKit.com has a solution: PC PhoneHomeTM is a software application that will track and locate a lost or stolen PC or laptop anywhere in the world. It is easy to install. It is also completely transparent to the user.

If your PC PhoneHome-protected computer is lost or stolen, all you need to do is make a report to the local police. In other words, PC PhoneHome is a transparent theft protection and recovery software system that you install on your laptop or PC.

Once installed, it sends an stealth email message to your address every time the computer connects to the Internet.

Let’s look at the following scenario

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.

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

Through computer forensic evidence acquisition services, forensic experts for companies like Capitol Digital Document Solutions can provide management with a potent arsenal of digital tools at its disposal.

They have the necessary software and hardware to travel to designated sites throughout the world to acquire an exact image of hard drives, tapes, etc. Services include

- ✓ **Lost password and file recovery**
- ✓ **Location and retrieval of deleted and hidden files**
- ✓ **File and email decryption**
- ✓ **Email supervision and authentication Threatening email traced to source**
- ✓ **Identification of Internet activity**
- ✓ **Computer usage policy and supervision**
- ✓ **Remote PC and network monitoring**
- ✓ **Tracking and location of stolen electronic files**

- ✓ **Honeypot sting operations**
- ✓ **Location and identity of unauthorized software users**
- ✓ **Theft recovery software for laptops and PCs**
- ✓ **Investigative and security software creation**
- ✓ **Protection from hackers and viruses**