Types of Computer Forensics Technology

- Today, there is an increased opportunity for cyber crime, making advances in the law enforcement, legal, and forensic computing technical arenas imperative

- Criminal investigators rely on recognized scientific forensic disciplines, such as medical pathology, to provide vital information used in apprehending criminals and determining their motives
- **Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of Computer systems, Computer networks, Computer media, and Computer peripherals that allow investigators to solve a crime.**
- **Cyber forensics focuses on real-time, online evidence gathering rather than the traditional offline computer disk forensic technology.**

- **Two distinct components exist in the emerging field of cyber forensics technology:**
- **The first, computer forensics, deals with gathering evidence from computer media seized at the crime scene.**
  - Principal concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes.
  - Several computer forensic tools are available to investigators.
- **The second component, network forensics, is a more technically challenging aspect of cyber forensics**.
  - ***It involves gathering digital evidence that is distributed across large-scale, Complex networks.***
  - Often this evidence is transient in nature and is not preserved within permanent storage media
  - **Network forensics deals primarily with in-depth analysis of computer network intrusion evidence**

- **Similar to traditional medical forensics, such as pathology, today's computer forensics is generally performed post-mortem (after the crime or event occurred).**
- **In a networked, distributed environment, it is imperative to perform forensic-like examinations of victim information systems on an almost continuous basis, in addition to traditional post-mortem forensic analysis.**

- Forensic tools are available to assist in pre-empting the attacks or locating the perpetrators.
- **In locating hackers investigators must perform cyber forensic functions in support of various objectives, these objectives include timely cyber attack containment, perpetrator location and identification, damage mitigation, and recovery initiation in the case of a crippled, yet still functioning, network.**
- Standard intrusion analysis includes examination of many sources of data evidence (intrusion detection system logs, firewall logs, audit trails, and network management information).

- Cyber forensics adds inspection of transient and other frequently overlooked elements such as **contents or state of memory, registers, basic input/output system, input/output buffers, serial receive buffers, L2 cache, front side and back side system caches, and various system buffers (drive and video buffers).**

- Some of the specific types of computer forensics technology that are being used by military, law enforcement, and business computer specialists are as discussed

Types of Military Computer Forensic Technology

- The U.S. Department of Defense (DoD) cyber forensics includes evaluation and indepth examination of data related to both the trans- and post-cyberattack 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 directorate entered into a partnership with the National Institute of Justice via the auspices of the National Law Enforcement and Corrections Technology Center (NLECTC) located in Rome, New York, to test these new ideas and prototype tools.
- The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership.
- This first of-a-kind event represents a new paradigm for transitioning cyber forensic technology from military research and development (R&D) laboratories into the hands of law enforcement.
- The experiment used a realistic cyber crime scenario specifically designed to exercise and show the value added of the directorate-developed cyber forensic technology.

- **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.
- **The objective of each team was to uncover several linked criminal activities from a maze of about 30 milestones that culminated in an information warfare crime as shown in figure**

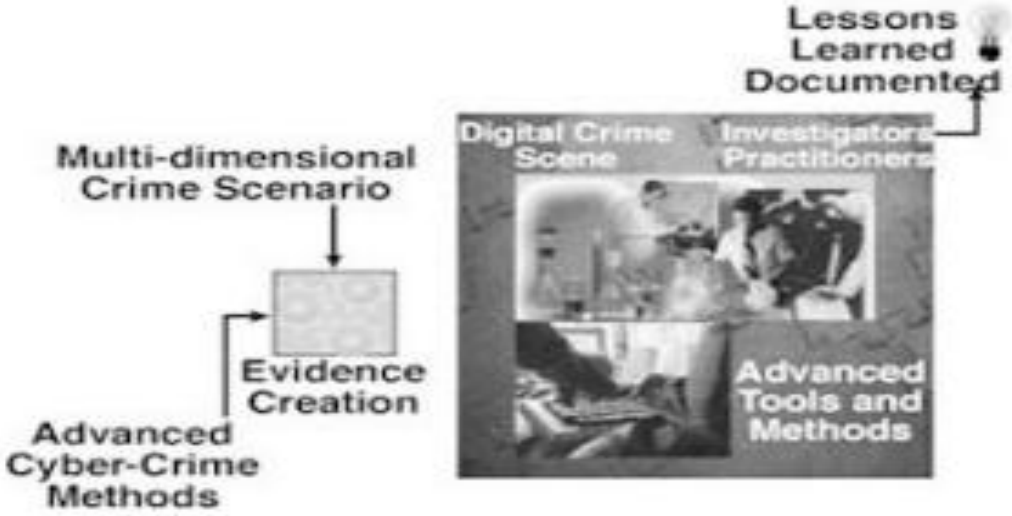

FIGURE 2.1 CFX-2000 schematic (© 2002, Associated Business Publications. All rights reserved).

- The cyber forensic tools involved in CFX-2000 consisted of commercial off the-shelf software and directorate-sponsored R&D prototypes.
- The Synthesizing Information from Forensic Investigations (SI-FI) integration environment, developed under contract by WetStone Technologies, Inc. [2], was the cornerstone of the technology demonstrated.
- SI-FI 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 timelining of digital events, automate event link analysis, and perform steganography detection.**
- **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**

Types of Law Enforcement Computer Forensic Technology

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

- 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.
- This section touches very briefly on issues dealing with Windows NT, Windows 2000, XP and 2003 and their use within law enforcement computer forensic technology

Computer Evidence processing procedures

- Processing procedures and methodologies should conform to federal computer evidence processing standards.
- Computer processing procedures have also been developed for the U.S. Treasury Department.
- **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 procedures**

Preservation of Evidence

- **Computer evidence is fragile and susceptible to alteration or erasure by any number of occurrences.**
- **Computer forensic instructors should expose their trainees to bit stream backup theories that ensure the preservation of all storage levels that may contain evidence.**
- **For example, SafeBack software overcomes some of the evidence weaknesses inherent in black box computer forensics approaches (see sidebar, "Mirror Image Backup Software").**
- **SafeBack technology can be purchased from New Technologies, Inc. [3] and has become a worldwide standard in making mirror image backups since 1990, when it was developed based on requirements then established by the U.S. Treasury Department and the IACIS.**

- CASE Study
- **MIRROR IMAGE BACKUP SOFTWARE**

Trojan Horse Programs

- The need to preserve the computer evidence before processing a computer should be clearly demonstrated by the computer forensic instructor through the use of programs designed to destroy data and modify the operating systems.
- **The participant 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 covertly capture sensitive information, passwords, and network logons.

Computer Forensics Documentation

- **The documentation of forensic processing methodologies and findings is important.**
- This is even true concerning computer security risk assessments and internal audits, because 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**
- **Thus, the computer forensic instructor should also teach the participant the ins and outs of computer evidence processing methodology (which facilitates good evidence-processing documentation and good evidence chain of custody procedures)**

File Slack

- **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.

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 in any computer forensics training course from a detection standpoint, as well as from a security risk standpoint.**
- **Tools that help in the identification of such anomalies should be demonstrated and discussed (like AnaDiskTM [see sidebar, "AnaDisk Diskette Analysis Tool"]) in the training course**

- Data-hiding courses are only open to classified government agencies and businesses that have a demonstrated need to know about this kind of information as outlined in a company's training policies.
- This is because the information covered in a data-hiding course can be used to defeat government computer security review processes and techniques.

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.**

- **New Technology Inc., which specializes in computer forensics tools and training, has posted order forms for its software on its Web site at *http://www.forensicsintl.com***
- **The tool is not available to the public, but a special version can be purchased by Fortune 500 companies, government agencies, military agencies, and consultants who have a legitimate need for the software**

Dual-Purpose Programs

- **Programs can be designed to perform multiple processes and tasks at the same time.**
- **They can also be designed for delayed tasking. These concepts should be demonstrated to the training participants during the course through the use of specialized software.**
- **The participant should also 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.**
- **Each training participant should also leave the class with a licensed copy of New Technology Inc.'s Filter_GTM software (see sidebar,"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

- **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 of the person who configured the system.**
- **Such a technique could be used to 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

- **The following are types of business computer forensics technology:**

1. **Remote monitoring of target computers**
2. **Creating trackable electronic documents**
3. **Theft recovery software for laptops and PCs**
4. **Basic forensic tools and techniques**
5. **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. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

Creating Trackable Electronic Documents

- There are so many powerful intrusion detection tools that allow the user to create trackable electronic documents that it is beyond the scope of this chapter to mention them all.

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

Theft Recovery Software for Laptops and PCs

- If your PC or laptop is stolen, is it smart enough to tell you where it is? According to a recent FBI report, 98% of stolen computers are never recovered.
- According to Safeware Insurance, 1,201,000 PCs and laptops were stolen in 2002 and 2003, costing owners $7.8 billion dollars [9]. According to a recent joint Computer Security Institute/FBI survey, 72% of the Fortune 1000 companies experienced laptop theft

What Is the Real Cost of a Stolen Laptop or PC?

- 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. 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.
Types of Computer Forensics Technology
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 [9] 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.**

- It’s PC PhoneHome, the latest in computer theft recovery software [9].

- **PC PhoneHome is a software application that, when installed in your laptop or desktop computer, secretly transmits an electronic message to an email address of your choice.**
- **This allows you to track and locate your computer, thus providing the potential for its ultimate recovery as well as apprehension of the thief**

How Does PC PhoneHome Work?

- **It's simple. First, you install PC PhoneHome on your computer, configuring it to send its recovery information to an email address of your choosing.**
- **PC PhoneHome sends a stealth email to your designated email address once a day, or every time you connect to the Internet and are assigned an IP address different from your previous IP address.**
- **If your computer is lost or stolen, you report the loss to the police and continue to monitor (with the additional help of the PC PhoneHome Recovery Center) your designated email address**

- When your stolen computer accesses the Internet by any method, your lost or stolen computer will send you its stealth email message, informing you of its location.

- If you are a registered user of PC PhoneHome, you may seek the PC PhoneHome technical service center's assistance in locating your computer's exact coordinates and alerting the local police to recover it.
- As a side benefit, any other items of your property (like expensive jewelry) that might have been taken at the same time may also be recovered [9].

- A success story, PC PhoneHome has been enthusiastically embraced by police forces, insurance companies, and the computer industry.
- The product is a natural fit for the security monitoring and Internet service provider (ISP) industry. PC PhoneHome is compatible with all Windows and Macintosh operating systems [9].

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 the mall.
- 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

- Through computer forensic evidence acquisition services, forensic experts for companies like Capitol Digital Document Solutions [10] 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.
- This image is an exact duplication of the source media and allows evaluation within their laboratories with minimal disruption to others.

- **Services include but are not limited to**

  Lost password and file recovery Location and retrieval of deleted and hidden files
  File and email decryption
  Email supervision and authentication
  Threatening email traced to source
  Identification of Internet activity
  Computer usage policy and supervision
  Remote PC and network monitoring
  Types of Computer Forensics Technology 55
  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