UNIT III
INTRODUCTION TO COMPUTER FORENSICS

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques – Incident and incident response methodology – Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. – Forensics Technology and Systems – Understanding Computer Investigation - Data Acquisition

Introduction to Traditional Computer Crime

- Computer crime is any criminal offense, activity or issue that involves computers
    - Computer misuse tends to fall into two categories.
        - Computer is used to commit a crime
        - Computer itself is a target of a crime. Computer is the victim. Computer Security Incident.

Computer Incident Response.

- **Computer Forensics** involves the preservation, identification, extraction, documentation and interpretation of computer data
- **Computer Forensics** is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law.
- **Computer forensics,** still a rather new discipline in computer security, focuses on finding digital evidence after a computer security incident has occurred .
- The goal of **computer forensics** is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it.

Introduction

- The introduction of the **Internet** has created unparalleled opportunities for commerce, research, education, entertainment, and public discourse. A global marketplace has emerged, in which fresh ideas and increased appreciation for multiculturalism have flourished.

- The introduction of computerized encyclopedias, international consortia, worldwide connectivity, and communications has greatly enhanced quality of life for many individuals.

- Indeed, the Internet can be utilized as a window to the world, allowing individuals to satiate their curiosity and develop global consciousness. It allows individuals to experience those things that they have only dreamed about.

- Interested parties can visit the Louvre, devouring priceless artifacts at their leisure or take an African safari without the heat or mosquitoes. They can find answers to the most complex legal or medical questions or search for their soul mates.

- They can download coupons for their favorite restaurants or search for recipes to their favorite dishes.
- In addition, individuals, corporations, public organizations, and institutions can more effectively advertise their products or services, using graphically highlighted information and providing links to supplemental information or support.

- In fact, computerized access to unprecedented information has cut across traditional boundaries of communication.

Cyberspace and Criminal Behavior

- Cyberspace may be defined as the indefinite place where individuals transact and communicate. It is the place between places.
- Telephonic conversations, occurring across time and space, were pre-dated by wire exchanges. However, the new medium known as the Internet has monumentally increased the **physicality** of the virtual world, outpaced only by the exponential growth in the number of users.

- No other method of communication converges audio, video, and data entities so effectively.
- Unlike traditional methods, the Internet combines mail, telephone, and mass media. As stated previously, it exposes individuals to a myriad of new ideas and may serve as a social gathering place, a library, or a place to be alone.
- In fact, the two created the **Electronic Frontier Foundation** (EFF) offering to ―fund, conduct, and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive and unconstitutional.

Clarification of Terms

- Just as debates rage over the appropriate codification of crime committed via electronic means, controversy surrounds the actual semantics associated with the phenomenon.
- For clarification purposes, then, it is necessary to define the historical usage of terms associated with technological or electronic crimes. **Computer crime** has been traditionally defined as any criminal act committed via computer. **Computer-related crime** has been defined as any criminal act in which a computer is involved, even peripherally.
- **Cybercrime** has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses. Finally, **digital crime,** a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. As data may be accessed or stored in a variety of ways and in a variety of locations, *digital crime* may be characterized as any of the three depending on case characteristics.
- While *computer crime* and *computer related crime* will be used interchangeably throughout the text, *cybercrime* will only be used to describe that criminal activity which has been facilitated via the Internet.

- Just as confusion exists regarding the appropriate terminology for crimes involving computers, the nomenclature of the science developed to investigate such activity lacks universality.

- For clarification purposes in this text, **computer forensic science, computer forensics, and digital forensics** may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence.

Traditional problems associated with Computer Crime.

- Physicality and Jurisdictional Concerns
- Perceived Insignificance, Stereotypes, and Incompetence
- Prosecutorial Reluctance
- Lack of Reporting

- Lack of Resources
- Jurisprudential Inconsistency
- Jurisprudential Inconsistency

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.
- 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.

Perceived Insignificance, Stereotypes, and Incompetence

- Investigators and administrators have displayed great reluctance to pursue computer criminals.
- A lack of knowledge coupled with general apathy toward cyber criminality has resulted in an atmosphere of indifference.

- Many stereotype computer criminals as nonthreatening, socially challenged individuals (i.e., nerds or geeks) and fail to see the insidious nature of computer crime;

- 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.

- Even in situations where law enforcement authorities recognize the insidious nature of computer or cybercrime, many do not perceive themselves or others in their department to be competent to investigate such criminal activity.

Prosecutorial Reluctance

- As media focus has increasingly highlighted the dangers of cyberspace, including those involving cyber bullying and child exploitation, public awareness has heightened an urgency to protect children's virtual playgrounds.
- In response, federal and state resources have often been allocated to fund specialized units to investigate and prosecute those offenses which affect the safety of American children.
- For example, the Federal Bureau of Investigation maintains a partnership with the Child Exploitation and Obscenity Section of the Department of Justice.
- This organization is composed of attorneys and computer forensic specialists who provide expertise to U.S. Attorney's Offices on crimes against children cases.

Lack of Reporting

- The number of reported incidents handled by Carnegie-Mellon University's Computer Emergency Response Team (CERT) has increased threefold, from 24,097 in 2006 to 72,065 in 2008.13 In their annual survey, *CSO Magazine* (in conjunction with the U.S. Secret Service; CERT, and Deloitte) reported that 58 percent of the organizations surveyed perceived themselves to be more prepared to prevent, detect, respond to, or recover from a cybercrime incident compared to the previous year.
- However, only 56 percent of respondents actually had a plan for reporting and responding to a crime.14 In 2011, it was reported that over 75 percent of all insider intrusions were handled internally without notification of authorities.

- Underreporting on the part of businesses and corporations may be attributed to a variety of reasons, but perhaps the most common are exposure to financial losses, data breach liabilities, damage to brand, regulatory issues, and loss of consumer confidence.

- Contemporary society, characterized by increased reliance on paperless transactions, demands assurances that the company's infrastructure is invulnerable and that confidential information remains inviolate.

Lack of Resources

- Computer intrusions have proven to be problematic within the corporate world, such institutions' unwillingness or inability to effectively communicate with judicial authorities has led to an increase in computer crime.
- Unfortunately, law enforcement and corporate entities desperately need to cooperate with one another.
- Unlike their civil service counterparts, the business communities have the resources (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.
- This hesitation has become even more pronounced with the emergence of wireless communications, social networking sites, and smart phones.
- As such, obvious demarcations of perception, application, and enforcement of computer crime laws vary widely across the country, and a standard of behavior in one jurisdiction may supersede or even negate legal standards in another.
- Traditionally, trial and appellate courts evaluated the constitutionality of computer crime statutes, searches, and investigations through the lens of the First and Fourth Amendment.
- Evaluating appropriate boundaries for free speech and establishing standards of reasonableness have varied across state and federal rulings, and an inconsistent patchwork of guidelines has resulted.

Identify theft and identify fraud

- The generic term **identity theft** has been utilized to describe any use of stolen personal information. However, such characterization fails to provide a comprehensive picture of the totality of possibilities surrounding that construct known as *identity*.
- Identity fraud, which encompasses identity theft within its purview, may be defined as the use of a vast array of illegal activities based on fraudulent use of identifying information of a real or fictitious person.

Typologies of Identity Theft/Fraud

a. Assumption of Identity

b. Theft for Employment and/or Border Entry

c. Criminal Record Identity Theft/Fraud

d. Virtual Identity Theft/Fraud e.

Credit Identity Theft/Fraud

a. Assumption of Identity

- This is the rarest form of identity theft/fraud and occurs when an individual simply assumes the identity of his or her victim, including all aspects of the victim's lives.
- It must be noted that this type of activity is atypical as it is significantly more difficult to accomplish.
- Even if a thief could identically duplicate the physical characteristics and appearance of his intended target, the likelihood of mastering personal histories, intimate relationships, and communication nuances is extremely remote.
- However, it is important to note that this type of identity fraud has occurred even in cases where the plausibility of such assumption borders on the ridiculous.

b. Theft for Employment and/or Border Entry

- This type of identity theft/fraud is increasingly common due to the growth of illegal immigration and alien smuggling. It involves the fraudulent use of stolen or fictitious personal information to obtain employment or to gain entry into the United States.
- The documents most frequently intercepted by officials included alien registration cards, nonimmigrant visas, passports and citizenship documents, and border crossing cards. These documents were presented by aliens who were attempting to enter the United States in search of employment or other immigration benefits, like naturalization or permanent residency status.

Here are some recent examples of identity theft for employment:

• **2008—Agriprocessors,** Inc.—CEO, company managers, and human resource employees were charged with multiple counts of federal immigration violations. Among other charges, the meat processing company was charged with harboring illegal aliens for profit, document fraud, bank fraud, and aggravated identity theft.

• **2009—George's Processing**, Inc.—Company paid nearly half a million dollars after 136 illegal aliens were found working at the Missouri plant.

• **2008—Columbia** Farms—Approximately 300 individuals, including eleven supervisors and one human resources manager, were arrested by federal authorities after a ten-month investigation revealed charges relating to identity theft for employment. The arrests in Greenville, South Carolina, followed earlier arrests of nearly two dozen plant managers.

Criminal Record Identity Theft/Fraud

- This type is often overlooked in discussions of identity theft, perhaps because it is not as common or because the immediate financial repercussions are not significant.
- It has been used historically by individuals attempting to evade capture or criminal prosecution.
- **Reverse criminal record identity theft** occurs when a criminal uses a victim's identity not to engage in criminal activity but to seek gainful employment. Unfortunately, criminal record identity theft/fraud is especially insidious as it often remains undiscovered until the victim is pulled over for a routine traffic violation. Unlike other types of identity fraud, in this case many victims are horrified to discover that they have been victimized by a friend or relative.

Virtual Identity Theft/Fraud

- A relatively new phenomenon, virtual identity theft/fraud involves the use of personal, professional, or other dimensions of identity toward the development of a fraudulent virtual personality.
- As in the previous types discussed, motivations range from the relatively innocuous to extreme malevolence.
- Unlike physical identities which are tied to social networks, legal documentation, and biological characteristics, virtual identities are largely personally constructed.

- Indeed, many individuals develop a virtual identity which is antithetical to their physical one—making themselves taller, richer, younger, more charismatic, and so on.
- In other words, virtual identities are often far removed from reality.
- As such, they are inherently less veracious and less trustworthy. They are often used for online dating, role-playing, and accessing deviant sites or locations containing questionable content.
- Although many individuals create virtual identities to explore forbidden areas or satisfy their curiosity behind a veil of anonymity, most do not cross the line between the legal and the illegal worlds.

Credit Identity Theft/Fraud

- It may be defined as the use of stolen personal and financial information to facilitate the creation of fraudulent accounts.
- This definition, specific by design, requires the affirmative act of securing additional credit.
- It does not include traditional activities like the illegal use of a stolen credit card, as that activity is more appropriately situated under statutes concerning credit card fraud.
- It is also not defined under identity theft, as the primary incentive is instant gratification.
- As credit cards are treated as cash by consumers and merchants alike, the use of a stolen one may be likened to purse snatching or pick-pocketing without physical contact.

Physical Methods of Identity Theft

a. Mail Theft
b. Dumpster Diving
c. Theft of Computers
d. Bag Operations
e. Child Identity Theft
f. Insiders
g. Fraudulent or Fictitious Companies

a. Mail Theft

- Although it is hard to identify which method of identity theft/fraud is most commonly employed, the theft of information from physical mailboxes is certainly one of the most common.

- Unfortunately, numerous documents containing personal and financial information are deposited in unlocked containers on the side of the road until it is retrieved.

- Oftentimes, such retrieval is conducted by someone other than the intended recipient and is used to generate illicit profit or to facilitate criminal activities. Physical mailboxes can contain a plethora of valuable information.

- Even as the government cautions citizens to take measures to protect their personal and financial information, they themselves are delivering government identification documents through U.S. Mail. Many times, they even mail breeder documents.

Some Instances of Compromised Data

Date	Institution	Type of Breach	Number of Victims
2011	Sutter Physicians Services	Theft of computer	3.3 million
2011	NASDAQ	Hack (cyberattack)	10 thousand
2011	SONY	Hack (cyberattack)	100 million
2011	Epsilon	Hack (cyberattack)	50–60 million
2011	Tricare	Theft of tapes	4.9 million
2011	University of Hawaii	Hack (cyberattack)	98 thousand
2011	Yale University	Accidental Web disclosure	43 thousand
2011	Texas comptroller	Accidental Web disclosure	3.5 million
2011	Ohio State University	Hack (cyberattack)	760 thousand

Dumpster Diving

- As the name implies, dumpster diving is the practice of sifting through commercial or residential trash or waste for information deemed valuable. Such information ranges widely, but may include account numbers, social security or tax payer identification numbers, and passwords.

- It may be located on discarded computer media or in paper form, and may be housed in personnel records, accounting spreadsheets, receipts, invoices, or the like.

- Fortunately, both consumers and businesses have increasingly taken measures to prevent the misuse of discarded information. Many now employ paper shredders and disk-wiping software.

- Diving for information has been practiced by criminals and law enforcement alike. Early hackers found the trash to be especially helpful toward their exploitation of computer vulnerabilities. Passwords, computer systems, and software could be located there.

Theft of Computers

- Physical theft of computers is among the most common techniques employed by identity thieves, as it alleviates the need to analyze and organize voluminous paper documents.

- As the majority of individuals necessarily store personal information on their computer, identity fraudsters are all but guaranteed a score.

- Even those individuals without technical expertise recognize that the computer as a warehouse of information has significant value on the black market, even if they themselves are incapable of retrieving the data.
- Areas vulnerable to such activity are limited only by the criminal mind.

Bag Operations

- Another tactic historically utilized by intelligence agents which is currently used by identity thieves and fraudsters is known as a ―bag operation,‖ and it involves the surreptitious entry into hotel rooms to steal, photograph, or photocopy documents; steal or copy magnetic media; or download information from laptop computers.

- Almost routine in many countries, bag operations are typically conducted by the host government's security or intelligence services, frequently with the cooperation of the hotel staff. They are most often committed when guests leave their room.

Child Identity Theft

- Increasingly, law enforcement authorities are reporting startling numbers of parents stealing their children's identities. According to the Federal Trade Commission, more than 140,000 children were victims of identity theft in 2011.28 This represented a marked increase in numbers released by the same group in 2003.

- Unfortunately, this type of identity theft or fraud is especially difficult to recognize and prosecute.

- The primary problem, of course, is the delayed identification of the victimization, as credit reports are usually not generated until the first application for credit, which usually occurs after the individual reaches the age of 18.

- Second, the theft itself is not characterized as either child abuse or exploitation, so the primary investigative agency for children

Insiders

- Many authorities suggest that corporate and government insiders pose the greatest risk to identity theft. As in other areas of computer crime, motivations vary and the facilitation of fraud is not always intentional.

- In fact, careless employees account for a large amount of the identity theft in the United States. Such negligence has been committed by both individual employees and corporate divisions.

- In 2005, for example, Bank of America reported that the personal information of 1.2 million U.S. government employees, including U.S. senators, had been

compromised when tapes were lost during shipment. In the same year, CitiGroup reported that UPS had lost the personal financial information of nearly 4 million Citigroup customers.

Fraudulent or Fictitious Companies

- Recently, a more sophisticated method of identity theft/fraud involves the creation of shell companies.
- Almost always conducted by an organized ring of criminals, fake companies are established which are engaged in the processing or collection of personal financial information.

- These fictitious businesses range from debt collection to insurance agents. In a highly visible case, over 145,000 consumers were put at risk by Choice point, an Atlanta-based company, which is one of the largest data aggregators and resellers in the country.

- Among other things, it compiles, stores, and sells information on the vast majority of American adults with over 19 billion records.

Card Skimming, ATM Manipulation, and Fraudulent Machines

- A more sophisticated method of data theft involves the reading and recording of Personal information encoded on the magnetic strip of an automated teller machine (ATM) or credit card.

- Once stored, the stolen data is re-coded onto the magnetic strip of a secondary or dummy card.

- This process, known as card skimming, results in a dummy card, which is a full-service credit or debit card indistinguishable from the original while purchasing.

- While card skimming was traditionally reserved to facilitate credit card fraud, it is increasingly being employed with the collection of other personal information to create additional accounts.

- Card **skimmers** come in a variety of shapes and sizes (most often miniaturized cameras or copiers and can be mounted on retail and ATMs).

- In some cases, thieves have actually developed fraudulent ATMs. Thus, consumers are strongly encouraged to only use those machines that are maintained by financial institutions, and to be alert for any suspicious equipment or appendage.

Introduction to the Incident Response Process

WHAT IS A COMPUTER SECURITY INCIDENT?

computer security incident as any unlawful, unauthorized, or unacceptable action that involves a computer system or a computer network. Such an action can include any of the following events:

- Theft of trade secrets
- Email spam or harassment
- Unauthorized or unlawful intrusions into computing systems
- Embezzlement
- Possession or dissemination of child pornography
- Denial-of-service (DoS) attacks
- Tortious interference of business relations
- Extortion
- Any unlawful action when the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes.

WHAT ARE THE GOALS OF INCIDENT RESPONSE?

In our incident response methodology, we emphasize the goals of corporate security professionals with legitimate business concerns, but we also take into consideration the concerns
of law enforcement officials. Thus, we developed a methodology that promotes a coordinated, cohesive response and achieves the following:

- Prevents a disjointed, noncohesive response (which could be disastrous)
- Confirms or dispels whether an incident occurred
- Promotes accumulation of accurate information
- Establishes controls for proper retrieval and handling of evidence
- Protects privacy rights established by law and policy
- Minimizes disruption to business and network operations
- Allows for criminal or civil action against perpetrators
- Provides accurate reports and useful recommendations
- Provides rapid detection and containment
- Minimizes exposure and compromise of proprietary data
- Protects your organization’s reputation and assets
- Educates senior management

- Promotes rapid detection and/or prevention of such incidents in the future (via lessons learned, policy changes, and so on)

WHO IS INVOLVED IN THE INCIDENT RESPONSE PROCESS?

- Incident response is a multifaceted discipline. It demands a myriad of capabilities that usually require resources from several different operational units of an organization.
- Human resources personnel, legal counsel, technical experts, security professionals, corporate security officers, business managers, end users, helpdesk workers, and other employees may find themselves involved in responding to a computer security incident.
- Most organizations establish a team of individuals, often referred to as a Computer Security Incident Response Team (CSIRT), to respond to any computer security incident.
- The CSIRT is a multidisciplined team with the appropriate legal, technical, and other expertise necessary to resolve an incident.
- Since the CSIRT members have special expertise, and incident response is not required at all times, the CSIRT is normally a dynamic team assembled when an organization requires its capabilities.

INCIDENT RESPONSE METHODOLOGY

- Since the incident response process can involve so many variables and factors that affect its flow, it is quite a challenge to create a simple picture of the process while maintaining a useful level of accuracy. Computer security incidents are often complex, multifaceted problems.
- Just as with any complex engineering problem, we use a “black box” approach.
- We divide the larger problem of incident resolution into components and examine the inputs and outputs of each component.

- Figure 2-1 illustrates our approach to incident response. In our methodology, there are seven major components of incident response:
- **Pre-incident preparation** : Take actions to prepare the organization and the CSIRT before an incident occurs
- **Detection of incidents:** Identify a potential computer security incident.
- **Initial response**: Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.

- **Formulate response strategy:** Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.
- **Investigate the incident**: Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.
- **Reporting** : Accurately report information about the investigation in a manner useful to decision makers.
- **Resolution**: Employ security measures and procedural changes, record lessons learned, and develop long-term fixes for any problems identified.

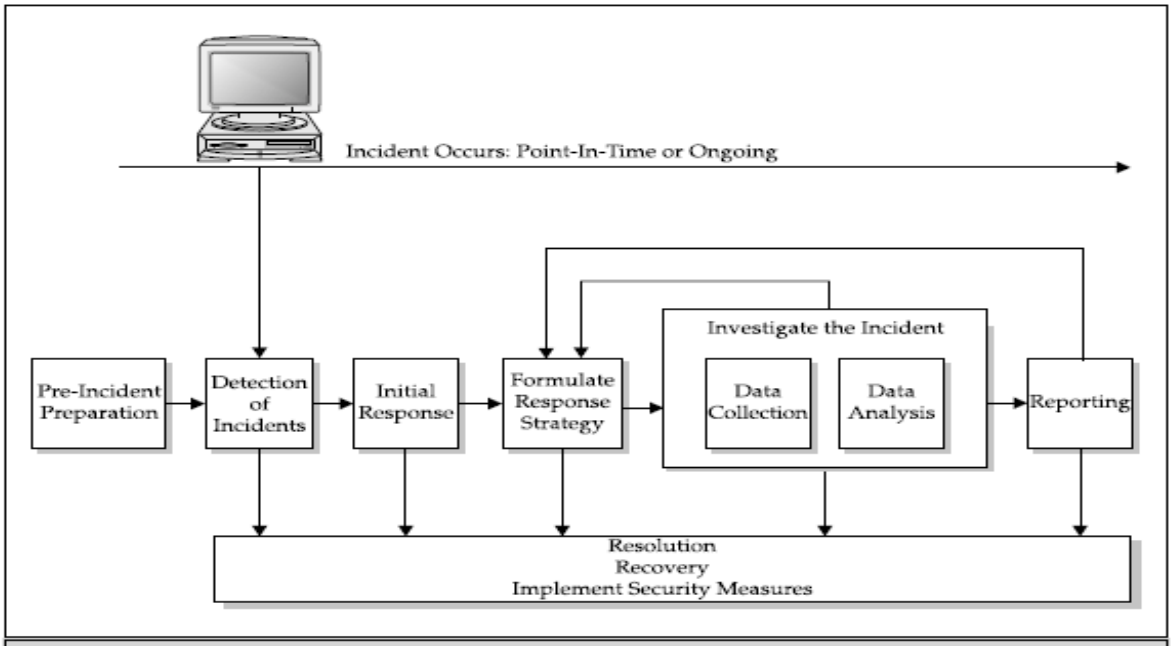

Figure 2-1. Seven components of incident response

Pre-Incident Preparation

Preparation of Organization

- Implementing host based security
- Implementing network based security
- Employing an intrusion detection system (IDS)
- Creating strong access control
- Training end user

Preparation of CSIRT

- The hardware needed to investigate computer security incidents
- The software needed to investigate computer security incidents

- The documentation needed to investigate computer security incidents
- The appropriate policies and operating procedures to implement your response strategies
- The training your staff or employees require to perform incident response in a manner that promotes successful forensics, investigations, and remediation

Detection of Incident

- IDS Detection of remote attack
- Numerous failed logon attempts
- Logins into dormant or default accounts
- New account not created by system administrator
- Unfamiliar file and executable program

- Altered pages on webserver
- Gaps in log files
- Slower System performance
- System Crash
- Receipt of Email Exporting your organization
- Child Pornography

Initial Response

- Interviewing system administrators who might have insight into the technical details of an incident
- Interviewing business unit personnel who might have insight into business events that may provide a context for the incident
- Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has occurred
- Reviewing the network topology and access control lists to determine if any avenues of attack can be ruled out

Formulate a Response Strategy

- The goal of the response strategy formulation phase is to determine the most appropriate response strategy, given the circumstances of the incident. The strategy should take into consideration the political, technical, legal, and business factors that surround the incident.The final solution depends on the objectives of the group or individual with responsibility for selecting the strategy Considering the Totality of the Circumstances .

- Response strategies will vary based on the circumstances of the computer security incident.

- The following factors need to be considered when deciding how many resources are needed to investigate an incident, whether to create a forensic duplication of relevant systems, whether to make a criminal referral, whether to pursue civil litigation, and other aspects of your response strategy:
    - How critical are the affected systems?
    - How sensitive is the compromised or stolen information?
    - Who are the potential perpetrators?
    - Is the incident known to the public?
    - What is the level of unauthorized access attained by the attacker?
    - What is the apparent skill of the attacker?
    - How much system and user downtime is involved?
    - What is the overall dollar loss?

Investigate the Incident

The investigation phase involves determining the who, what, when, where, how, and why surrounding an incident. You will conduct your investigation, reviewing host-based evidence, network-based evidence, and evidence gathered via traditional, nontechnical investigative steps.

Data Collection

Data collection is the accumulation of facts and clues that should be considered during your forensic analysis

Data collection involves several unique forensic challenges:

- You must collect electronic data in a forensically sound manner.
- You are often collecting more data than you can read in your lifetime (computer storage capacity continues to grow).
- You must handle the data you collect in a manner that protects its integrity (evidence handling).

Network-based Evidence

Network-based evidence includes information obtained from the following sources:

- IDS logs
- Consensual monitoring logs
- Nonconsensual wiretaps
- Pen-register/trap and traces

- Router logs
- Firewall logs
- Authentication servers

Host-based Information

- Host-based evidence includes logs, records, documents, and any other information that is found on a system and not obtained from network-based nodes

  You record the following volatile information:

  - The system date and time
  - The applications currently running on the system
  - The currently established network connections
  - The currently open sockets (ports)
  - The applications listening on the open sockets
  - The state of the network interface (promiscuous or not)

In order to collect this information, a live response must be performed. A live response is conducted when a computer system is still powered on and running There are three variations of live response:

Initial live response This involves obtaining only the volatile data from a target or victim system. An initial live response is usually performed when you have decided to conduct a forensic duplication of the media.

In-depth response This goes beyond obtaining merely the volatile data. The CSIRT obtains enough additional information from the target/victim system to determine a valid response strategy. Nonvolatile information such as log files are collected to help understand the nature of the incident.

Full live response This is a full investigation on a live system. All data for the investigation is collected from the live system, usually in lieu of performing a forensic duplication, which requires the system to be powered off.

Forensic Analysis

Forensic analysis includes reviewing all the data collected. This includes reviewing log files, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files. Forensic analysis also includes performing more low-level tasks, such as looking through information that has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to the investigation.

Figure 2-4 depicts the major steps taken during forensic analysis.

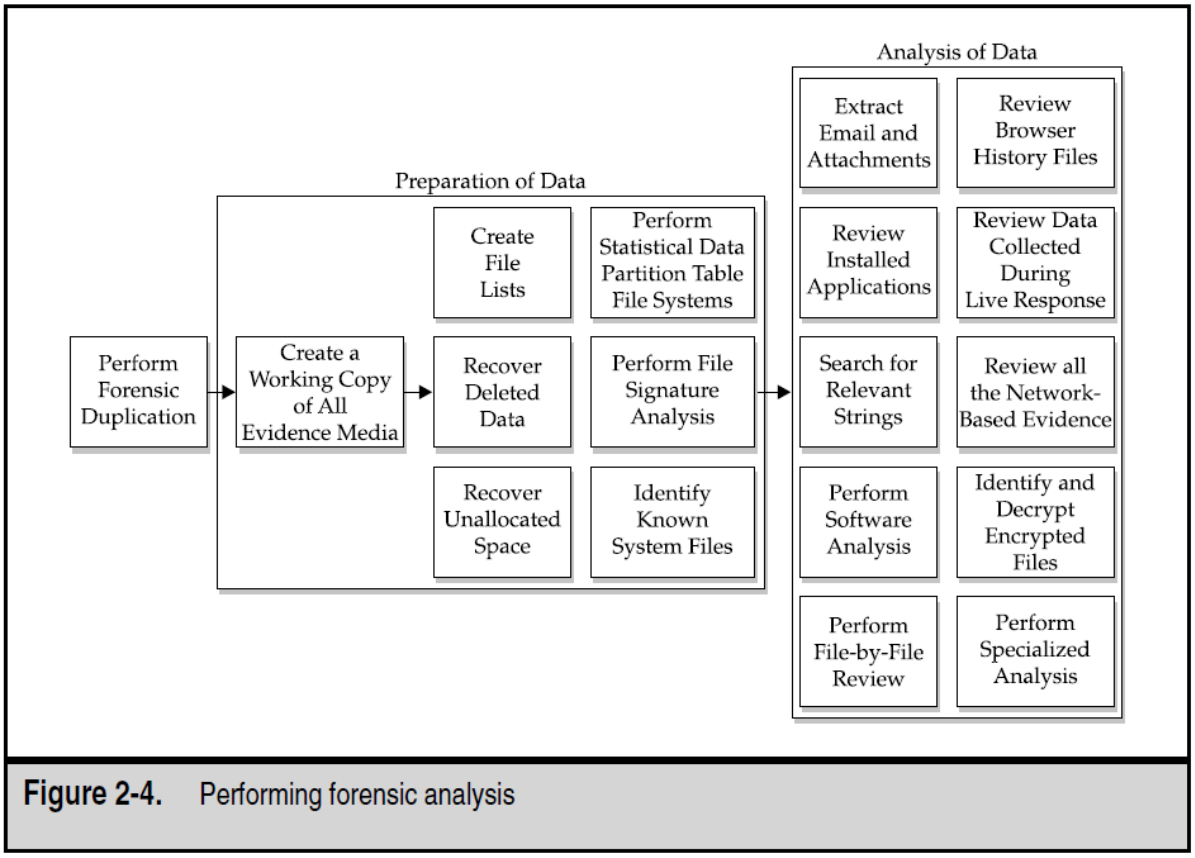

Figure 2-4. Performing forensic analysis

Reporting

Reporting can be the most difficult phase of the incident response process. The challenge is to create reports that accurately describe the details of an incident, that are understandable to decision makers, that can withstand the barrage of legal scrutiny, and that are produced in a timely manner.

Reports are also often used by investigators to refresh their recollections during criminal trials and in training employees new to the field of computer forensics. we have come up with some guidelines to ensure that the reporting phase does not become your CSIRT's nemesis

Document immediately

All investigative steps and conclusions need to be documented as soon as possible. Writing something clearly and concisely at the moment you discover evidence saves time, promotes accuracy, and ensures that the details of the investigation can be communicated more clearly to others at any moment, which is critical if new personnel become involved or are assigned to lead the investigation.

Write concisely and clearly

Enforce the "write it tight" philosophy. Documenting investigative steps requires discipline and organization. Write everything down in a fashion that is understandable to you and others.

Discourage shorthand or shortcuts. Vague notations, incomplete scribbling, and other unclear documentation can lead to redundant efforts, forced translation of notes, confirmation of notes, and a failure to comprehend notes made by yourself or others.

Use a standard format

Develop a format for your reports and stick to it. Create forms, outlines, and templates that organize the response process and foster the recording of all pertinent data. This makes report writing scalable, saves time, and promotes accuracy.

Use editors Employ technical editors to read your forensic reports. This helps develop reports that are comprehensible to nontechnical personnel who have an impact on your incident response strategy and resolution (such as Human

Resources personnel, legal counsel, and business leaders). Unfortunately, editors can inadvertently change the meaning of critical information. The burden is still on you to review the final product prior to submission

Resolution

The goal of the resolution phase is to implement host-based, network-based, and procedural countermeasures to prevent an incident from causing further damage and to return your organization to a secure, healthy operational status

The following steps are often taken to resolve a computer security incident:

1. Identify your organization's top priorities. Which of the following is the most critical to resolve: returning all systems to operational status, ensuring data integrity, containing the impact of the incident, collecting evidence, or avoiding public disclosure?
2. Determine the nature of the incident in enough detail to understand how the security occurred and what host-based and network-based remedies are required to address it.
3. Determine if there are underlying or systemic causes for the incident that need to be addressed (lack of standards, noncompliance with standards, and so on).
4. Restore any affected or compromised systems. You may need to rely on a prior version of the data, server platform software, or application software as needed to ensure that the system performs as you expect it to perform.
5. Apply corrections required to address any host-based vulnerabilities. Note that all fixes should be tested in a lab environment before being applied to production systems.
6. Apply network-based countermeasures such as access control lists, firewalls, or IDS.
7. Assign responsibility for correcting any systemic issues.

8. Track progress on all corrections that are required, especially if they will take significant time to complete.
9. Validate that all remedial steps or countermeasures are effective. In other words, verify that all the host-based, network-based, and systemic remedies have been applied correctly.
10. Update your security policy and procedures as needed to improve your response process

CREATING A RESPONSE TOOLKIT

- Regardless of the status of network, host, and policy preparation, the CSIRT will need to be prepared to respond to incidents.
- The response toolkit is a critical component of pre-incident preparation, and it is one of the few components in your control.
- The response toolkit includes the hardware, software, and documentation used during response

The Response Hardware

- The forensic hardware platform of choice these days seems to be the "brick" or "lunchbox" configuration.

- This robust and configurable platform uses full-size components, has attachments for various external devices, and includes a network interface card (NIC) as well as a CD-RW drive.

Here are the hardware specifications we suggest:

- High-end processor
- A minimum of 256MB of RAM
- Large-capacity IDE drives
- Large-capacity SCSI drives
- SCSI card and controller
- A fast CD-RW drive
- 8mm exabyte tape drive (20GB native, 40GB compressed), or a drive for DDS3 tapes (4mm) if you have less funding

Some other items that you may want to purchase ahead of time include the following:

- Extra power extenders for peripherals such as drives and any gear that goes in your forensic tower

- Extra power-extension cords
- Numerous SCSI cables and active terminators
- Parallel-to-SCSI adapters
- Plenty of Category 5 cabling and hubs
- Ribbon cables with more than three plugs
- Power strips
- An uninterruptible power supply (UPS)
- CD-Rs, 100 or more
- Labels for the CDs
- A permanent marker for labeling CDs
- Jaz or Zip media
- Folders and folder labels for evidence
- Operating manuals for all your hardware
- A digital camera
- Toolkit or Victorinox Cybertool (which is all we need)
- Lockable storage containers for evidence (if you are on the road)
- Printer and printer paper
- Burn bags (useful when you print sensitive reports concerning an incident for editing, and need to destroy them later)

The Response Software

Many specific software tools are used during incident response to investigate various operating systems and applications.

The following is a list of the more generic software that forms the basis of any software toolkit:

- Two to three native operating systems on the machine, such as Windows 98, Windows NT, Windows 2000, and Linux, all bootable via GRUB (a GNU bootloader) or on a CD-ROM "ghost" image
- Safeback, EnCase, DiskPro, or another forensics software package, used to re-create exact images of computer media for forensic-processing purposes

- All the drivers for all of the hardware on your forensic machine (absolutely necessary!)
- Selection of boot disks (DOS, EnCase, Maxtor, and so on)
- Quick View Plus or some other software that allows you to view nearly all types of files

- Disk-write blocking utilities
- An image of the complete setup on backup media such as DVD

The Networking Monitoring Platform

- There may come a time when you need to perform network monitoring. If you do, you will need a machine that can handle the amount of traffic your network has.

- The system running the network monitor should be a Pentium-class machine, 500MHz or higher, with at least 512MB of RAM (or more, depending on network traffic and the host operating system).

- Hard drive size depends on the amount of traffic collected, but a 30GB hard drive is a good start.

- Make sure that your network monitor system has a NIC that supports promiscuous mode (such as those manufactured by Madge and 3Com).

- This will be more of an issue if you are monitoring a Token Ring or wireless network. Most Token Ring adapters do not go into promiscuous mode.

- Some organizations use Shomiti adapters because they do not respond to Address Resolution Protocol (ARP) packets and maintain network silence.

Documentation

- The CSIRT must document all actions and findings. Documentation is necessary for further disciplinary, civil, or criminal action, as well as for a thorough response. Key areas for documentation include how the evidence is obtained, all actions taken, and where and how the evidence is stored.

- To facilitate complete documentation, standardized reporting and forms are helpful.

ESTABLISHING AN INCIDENT RESPONSE TEAM

- Deciding on the Team's Mission
- The mission of your CIRT may be to achieve all or most of the following:

- Respond to all security incidents or suspected incidents using an organized, formal investigative process.
- Conduct a complete investigation free from bias (well, as much as possible).
- Quickly confirm or dispel whether an intrusion or security incident actually occurred.
- Assess the damage and scope of an incident.
- Establish a 24-hour, 7-day-a-week hotline for clients during the duration of the
- investigation.
- Control and contain the incident.
- Collect and document all evidence related to an incident.
- Maintain a chain of custody (protect the evidence after collection).
- Select additional support when needed.
- Protect privacy rights established by law and/or corporate policy.
- Provide liaison to proper law enforcement and legal authorities.
- Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure.
- Provide expert testimony.
- Provide management with incident-handling recommendations that are fully supported by facts.

Training the Team

- It is also a good idea for CIRT members to join professional organizations to continue their education and to rub elbows with the individuals they may call for helpone day. There are several professional organizations that allow law enforcement officers to mingle with computer security professionals:
- **InfraGard** An FBI program designed to address the need for private and public-sector information sharing, at both the national and local level.
- **High Technology Crime Investigation Association (HTCIA)** An association designed to encourage and facilitate the exchange of information relating to computer incident investigations and security.
- **Information Systems Security Association (ISSA)** A not-for-profit international organization of information security professionals and practitioners. It provides education forums, publications, and peerinteraction opportunities.
- **Forum of Incident Response and Security Teams (FIRST)** A coalition that brings together incident response teams from government, commercial,and academic organizations.

Understanding Computer Investigation

Objective

- Explain how to prepare a computer investigation
- Apply a systematic approach to an investigation
- Describe procedures for corporate high-tech investigations
- Explain requirements for data recovery workstations and software
- Describe how to conduct an investigation
- Explain how to complete and critique a case

Preparing a Computer Investigation

- Role of computer forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect's computer
  - Preserve the evidence on a different computer
- Follow an accepted procedure to prepare a case
- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

An Overview of a Computer Crime

- Computers can contain information that helps law enforcement determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator
- Information on hard disks might be password protected

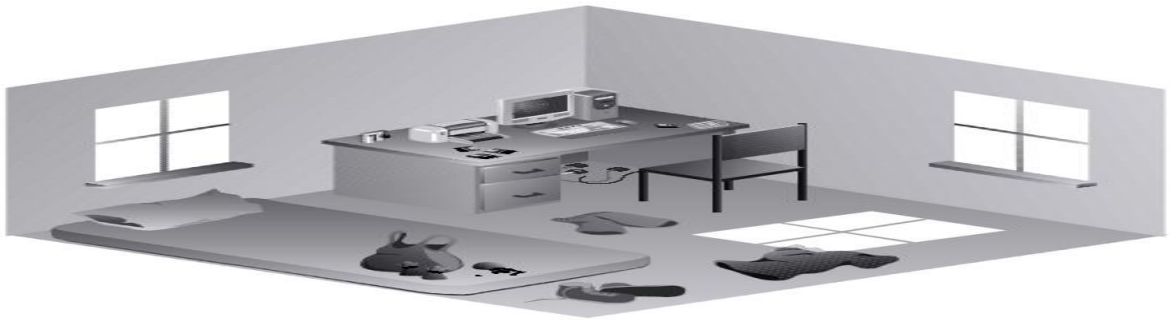

Figure 2-1 The crime scene

An Overview of a Company Policy Violation

- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
  - Surfing the Internet
  - Sending personal e-mails
  - Using company computers for personal tasks

Taking a Systematic Approach

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence disk drive
- Steps for problem solving (continued)
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

Assessing the Case

- Systematically outline the case details
  - Situation
  - Nature of the case
  - Specifics of the case
  - Type of evidence
  - Operating system
  - Known disk format
  - Location of evidence
- Based on case details, you can determine the case requirements
  - Type of evidence
  - Computer forensics tools
  - Special operating systems

Planning Your Investigation

- A basic investigation plan should include the following activities:
  - Acquire the evidence
  - Complete an evidence form and establish a chain of custody
  - Transport the evidence to a computer forensics lab
  - Secure evidence in an approved secure container
  - Prepare a forensics workstation
  - Obtain the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools
- An evidence custody form helps you document what has been done with the original evidence and its forensics copies
- Two types
  - Single-evidence form
    - Lists each piece of evidence on a separate page
  - Multi-evidence form

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Description of evidence:		Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page ___ of ___

Figure 2-2 A sample multi-evidence form used in a corporate environment

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of __

Figure 2-3 A single-evidence form

Securing Your Evidence

- Use evidence bags to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
  - Floppy disk or CD drives
  - Power supply electrical cord
- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges

Procedures for Corporate High-Tech Investigations

- Develop formal procedures and informal checklists
  - To cover all issues important to high-tech investigations

Employee Termination Cases

- Majority of investigative work for termination cases involves employee abuse of corporate assets
- Internet abuse investigations
  - To conduct an investigation you need:

        - Organization's Internet proxy server logs
        - Suspect computer's IP address
        - Suspect computer's disk drive
        - Your preferred computer forensics analysis tool
    - Recommended steps
        - Use standard forensic analysis techniques and procedures
        - Use appropriate tools to extract all Web page URL information
        - Contact the network firewall administrator and request a proxy server log
        - Compare the data recovered from forensic analysis to the proxy server log
        - Continue analyzing the computer's disk drive data
- **E-mail abuse investigations**
    - To conduct an investigation you need:
        - An electronic copy of the offending e-mail that contains message header data
        - If available, e-mail server log records
        - For e-mail systems that store users' messages on a central server, access to the server
        - Access to the computer so that you can perform a forensic analysis on it
        - Your preferred computer forensics analysis tool
    - Recommended steps
        - Use the standard forensic analysis techniques
        - Obtain an electronic copy of the suspect's and victim's e-mail folder or data
        - For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
        - Examine header data of all messages of interest to the investigation

Attorney-Client Privilege Investigations

- Under attorney-client privilege (ACP) rules for an attorney
    - You must keep all findings confidential
- Many attorneys like to have printouts of the data you have recovered
    - You need to persuade and educate many attorneys on how digital evidence can be viewed electronically
- You can also encounter problems if you find data in the form of binary files
- Steps for conducting an ACP case
    - Request a memorandum from the attorney directing you to start the investigation
    - Request a list of keywords of interest to the investigation

  - Initiate the investigation and analysis
  - For disk drive examinations, make two bit-stream images using different tools
  - Compare hash signatures on all files on the original and re-created disks
  - Methodically examine every portion of the disk drive and extract all data
  - Run keyword searches on allocated and unallocated disk space
  - For Windows OSs, use specialty tools to analyze and extract data from the Registry
    - AccessData Registry Viewer
  - For binary data files such as CAD drawings, locate the correct software product
  - For unallocated data recovery, use a tool that removes or replaces nonprintable data
  - Consolidate all recovered data from the evidence bit-stream image into folders and subfolders
- Other guidelines
  - Minimize written communications with the attorney
  - Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"
  - Assist attorney and paralegal in analyzing the data
- If you have difficulty complying with the directions
  - Contact the attorney and explain the problem
- Always keep an open line of verbal communication
- If you're communicating via e-mail, use encryption

Media Leak Investigations

- In the corporate environment, controlling sensitive data can be difficult
- Consider the following for media leak investigations
  - Examine e-mail
  - Examine Internet message boards
  - Examine proxy server logs
  - Examine known suspects' workstations
  - Examine all company telephone records, looking for calls to the media
- Steps to take for media leaks
  - Interview management privately
    - To get a list of employees who have direct knowledge of the sensitive data
  - Identify media source that published the information
  - Review company phone records
  - Obtain a list of keywords related to the media leak

  - Perform keyword searches on proxy and e-mail servers
  - Discreetly conduct forensic disk acquisitions and analysis
  - From the forensic disk examinations, analyze all e-mail correspondence
  - And trace any sensitive messages to other people
  - Expand the discreet forensic disk acquisition and analysis
  - Consolidate and review your findings periodically
  - Routinely report findings to management

Industrial Espionage Investigations

- All suspected industrial espionage cases should be treated as criminal investigations
- Staff needed
  - Computing investigator who is responsible for disk forensic examinations
  - Technology specialist who is knowledgeable of the suspected compromised technical data
  - Network specialist who can perform log analysis and set up network sniffers
  - Threat assessment specialist (typically an attorney)
- Guidelines
  - Determine whether this investigation involves a possible industrial espionage incident
  - Consult with corporate attorneys and upper management
  - Determine what information is needed to substantiate the allegation
  - Generate a list of keywords for disk forensics and sniffer monitoring
  - List and collect resources for the investigation
  - Determine goal and scope of the investigation
  - Initiate investigation after approval from management
- Planning considerations
  - Examine all e-mail of suspected employees
  - Search Internet newsgroups or message boards
  - Initiate physical surveillance
  - Examine facility physical access logs for sensitive areas
  - Determine suspect location in relation to the vulnerable asset
  - Study the suspect's work habits
  - Collect all incoming and outgoing phone logs
- Steps
  - Gather all personnel assigned to the investigation and brief them on the plan
  - Gather resources to conduct the investigation

  - Place surveillance systems
  - Discreetly gather any additional evidence
  - Collect all log data from networks and e-mail servers
  - Report regularly to management and corporate attorneys
  - Review the investigation's scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations

- Becoming a skilled interviewer and interrogator can take many years of experience
- Interview
  - Usually conducted to collect information from a witness or suspect
    - About specific facts related to an investigation
- Interrogation
  - Trying to get a suspect to confess
- Role as a computing investigator
  - To instruct the investigator conducting the interview on what questions to ask
    - And what the answers should be
- Ingredients for a successful interview or interrogation
  - Being patient throughout the session
  - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
  - Being tenacious

Understanding Data Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
- Computer forensics and data-recovery are related but different
- Computer forensics workstation
  - Specially configured personal computer
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use:
  - Forensics boot floppy disk OR cd
  - Write-blocker devices

Write Blocker

- Connects a hard drive in trusted read-only mode
- There are also Linux boot CDs that mount all drives read-only, such as Helix and some Knoppix distributions

Setting Up your Computer for Computer Forensics

- Basic requirements
  - A workstation running Windows XP or Vista
  - A write-blocker device
  - Computer forensics acquisition tool
    - Like FTK Imager
  - Computer forensics analysis tool
    - Like FTK
  - Target drive to receive the source or suspect disk data
  - Spare PATA or SATA ports
  - USB ports
- Additional useful items
  - Network interface card (NIC)
  - Extra USB ports
  - FireWire 400/800 ports
  - SCSI card
  - Disk editor tool
  - Text editor tool
  - Graphics viewer program
  - Other specialized viewing tools

Conducting an Investigation

- Gather resources identified in investigation plan
- Items needed
  - Original storage media
  - Evidence custody form
  - Evidence container for the storage media
  - Bit-stream imaging tool
  - Forensic workstation to copy and examine your evidence
  - Securable evidence locker, cabinet, or safe

Gathering the Evidence

- Avoid damaging the evidence
- Steps
  - Meet the IT manager to interview him
  - Fill out the evidence form, have the IT manager sign
  - Place the evidence in a secure container

- Complete the evidence custody form
- Carry the evidence to the computer forensics lab
- Create forensics copies (if possible)
- Secure evidence by locking the container

Understanding Bit-Stream Copies

- Bit-stream copy
  - Bit-by-bit copy of the original storage medium
  - Exact copy of the original disk
  - Different from a simple backup copy
    - Backup software only copies known files (active data)
    - Backup software cannot copy deleted files, e-mail messages or recover file fragments
- Bit-stream image
  - File containing the bit-stream copy of all data on a disk or partition
  - Also known as forensic copy
- Copy image file to a target disk that matches the original disk's manufacturer, size and model

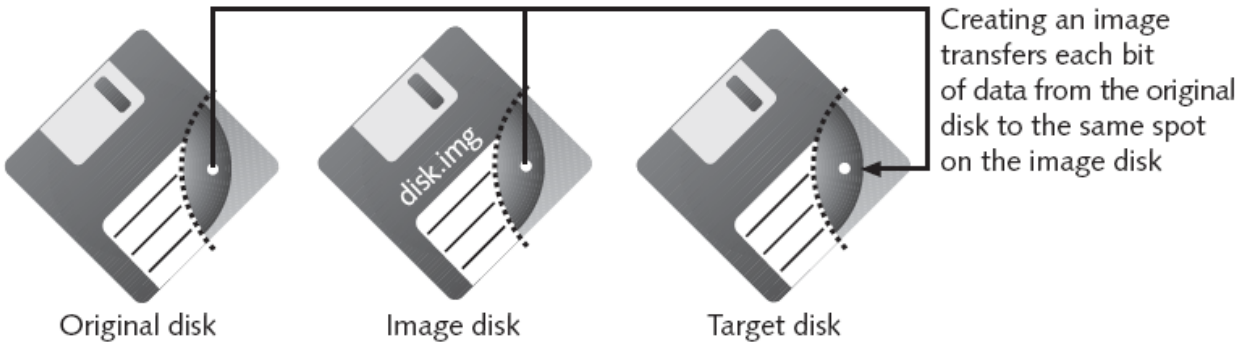

Figure 2-4 Transfer of data from original to image to target

Data Acquisition

Objectives

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to use acquisition tools
- Explain how to validate data acquisitions
- Describe RAID acquisition methods

- Explain how to use remote network acquisition tools
- List other forensic tools available for data acquisitions

Understanding Storage Formats for Digital Evidence

- Three formats
  - Raw format
  - Proprietary formats
  - Advanced Forensics Format (AFF)

Raw Format

In the past, there was only one practical way of copying data for the purpose of evidence preservation and examination.

Examiners performed a bit-by-bit copy from one disk to another disk the same size or larger.

As a practical way to preserve digital evidence, vendors (and some OS utilities, such as the Linux/UNIX dd command) made it possible to write bit-stream data to files.

This copy technique creates simple sequential flat files of a suspect drive or data set. The output of these flat files is referred to as a raw format.

- Makes it possible to write bit-stream data to files
- Advantages
  - Fast data transfers
  - Can ignore minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors

Proprietary Formats

Most commercial computer forensics tools have their own formats for collecting digital evidence.

- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
  - Can integrate metadata into the image file
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
- Design goals
  - Provide compressed or uncompressed image files
  - No size restriction for disk-to-image files
  - Provide space in the image file or segmented files for metadata
  - Simple design with extensibility
  - Open source for multiple platforms and OSs
  - Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata
- AFF is open source

Determining the Best Acquisition Method

- **Types of acquisitions**
  - Static acquisitions and live acquisitions
- **Four methods**
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk
  - Logical disk-to-disk or disk-to-disk data
  - Sparse data copy of a file or folder
- **Bit-stream disk-to-image file**
  - Most common method
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook
- **Bit-stream disk-to-disk**
  - When disk-to-image copy is not possible
  - Consider disk's geometry configuration
  - EnCase, SafeBack, SnapCopy
- **Logical acquisition** or **sparse acquisition**
  - When your time is limited
  - Logical acquisition captures only specific files of interest to the case
  - Sparse acquisition also collects fragments of unallocated (deleted) data
  - For large disks
  - PST or OST mail files, RAID servers
- When making a copy, consider:

- Size of the source disk
    - Lossless compression might be useful
    - Use digital signatures for verification
- When working with large drives, an alternative is using tape backup systems
- Whether you can retain the disk

Contingency Planning for Image Acquisitions

- Create a duplicate copy of your evidence image file
- Make at least two images of digital evidence
    - Use different tools or techniques
- Copy host protected area of a disk drive as well
    - Consider using a hardware acquisition tool that can access the drive at the BIOS level
- Be prepared to deal with encrypted drives
    - Whole disk encryption feature in Windows Vista Ultimate and Enterprise editions

Using Acquisition Tools

- Acquisition tools for Windows
    - Advantages
        - Make acquiring evidence from a suspect drive more convenient
            - Especially when used with hot-swappable devices
    - Disadvantages
        - Must protect acquired data with a well-tested write-blocking hardware device
        - Tools can’t acquire data from a disk’s host protected area

Windows XP Write-Protection with USB Devices

- USB write-protection feature
    - Blocks any writing to USB devices
- Target drive needs to be connected to an internal PATA (IDE), SATA, or SCSI controller
- Steps to update the Registry for Windows XP SP2
    - Back up the Registry
    - Modify the Registry with the write-protection feature
    - Create two desktop icons to automate switching between enabling and disabling writes to USB device

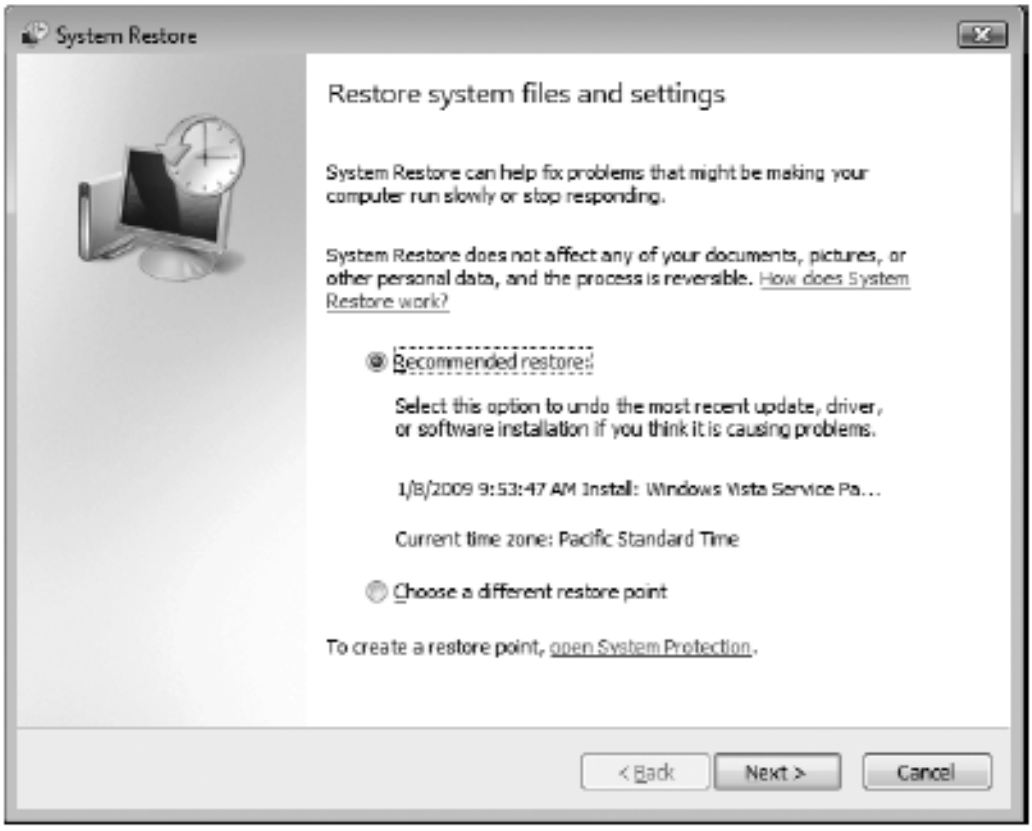

Figure 4-2 The System Restore Wizard

Acquiring Data with a Linux Boot CD

- Linux can access a drive that isn't mounted
- Windows OSs and newer Linux automatically mount and access a drive
- Forensic Linux Live CDs don't access media automatically
  - Which eliminates the need for a write-blocker
- Using Linux Live CD Distributions
  - Forensic Linux Live CDs
    - Contain additionally utilities
- Using Linux Live CD Distributions (continued)
  - Forensic Linux Live CDs (continued)
    - Configured not to mount, or to mount as read-only, any connected storage media
    - Well-designed Linux Live CDs for computer forensics
      - Helix
      - Penguin Sleuth
      - FCCU
- Preparing a target drive for acquisition in Linux

  - Linux distributions can create Microsoft FAT and NTFS partition tables
- Preparing a target drive for acquisition in Linux (continued)
  - **fdisk** command lists, creates, deletes, and verifies partitions in Linux
  - **mkfs.msdos** command formats a FAT file system from Linux
- Acquiring data with dd in Linux
  - dd ("data dump") command
    - Can read and write from media device and data file
    - Creates raw format file that most computer forensics analysis tools can read
- Acquiring data with dd in Linux (continued)
  - Shortcomings of dd command
    - Requires more advanced skills than average user
    - Does not compress data
  - dd command combined with the split command
    - Segments output into separate volumes
- Acquiring data with dcfldd in Linux
  - dd command is intended as a data management tool
    - Not designed for forensics acquisitions
- Acquiring data with dcfldd in Linux (continued)
  - dcfldd additional functions
    - Specify hex patterns or text for clearing disk space
    - Log errors to an output file for analysis and review
    - Use several hashing options
    - Refer to a status display indicating the progress of the acquisition in bytes
    - Split data acquisitions into segmented volumes with numeric extensions
    - Verify acquired data with original disk or media data

Capturing an Image with ProDiscover Basic

- Connecting the suspect's drive to your workstation
  - Document the chain of evidence for the drive
  - Remove the drive from the suspect's computer
  - Configure the suspect drive's jumpers as needed
  - Connect the suspect drive
  - Create a storage folder on the target drive
- Using ProDiscover's Proprietary Acquisition Format
  - Image file will be split into segments of 650MB

- Creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)

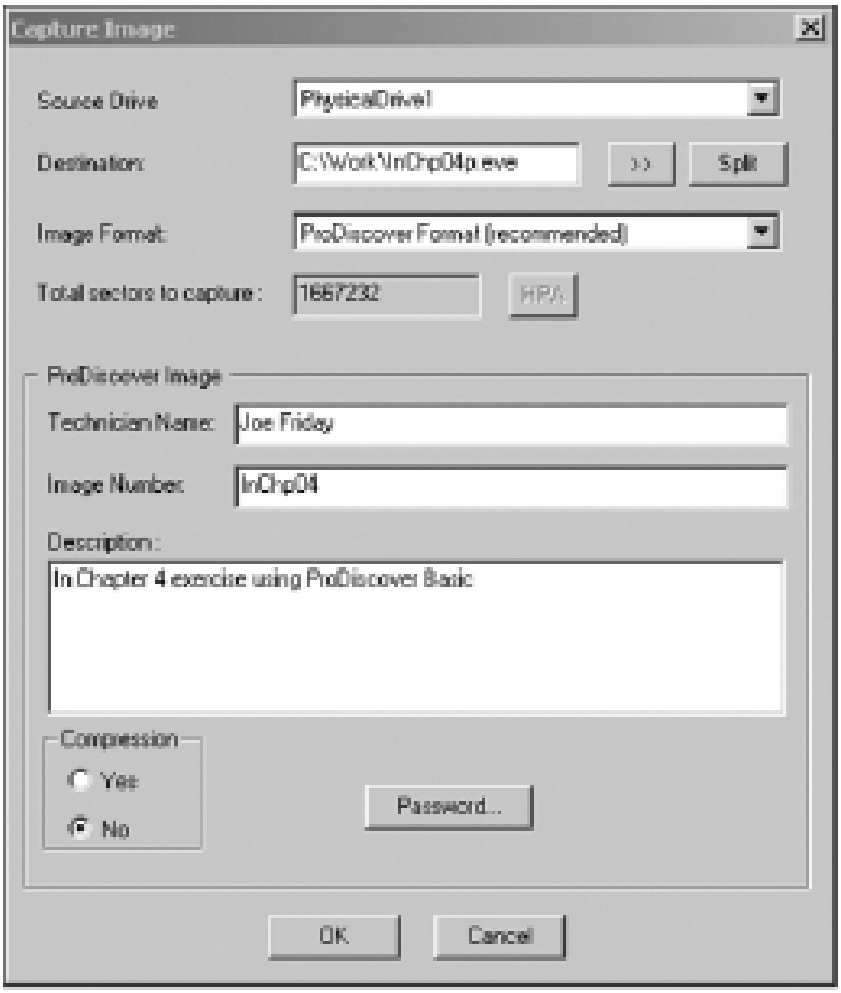

Figure 4-5 The Capture Image dialog box

- Using ProDiscover's Raw Acquisition Format
  - Select the UNIX style dd format in the Image Format list box
  - Raw acquisition saves only the image data and hash value

Capturing an Image with AccessData FTK Imager

- Included on AccessData Forensic Toolkit
- View evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a hardware write-blocking device

  - Or the USB write-protection Registry feature enabled
- FTK Imager can't acquire drive's host protected area

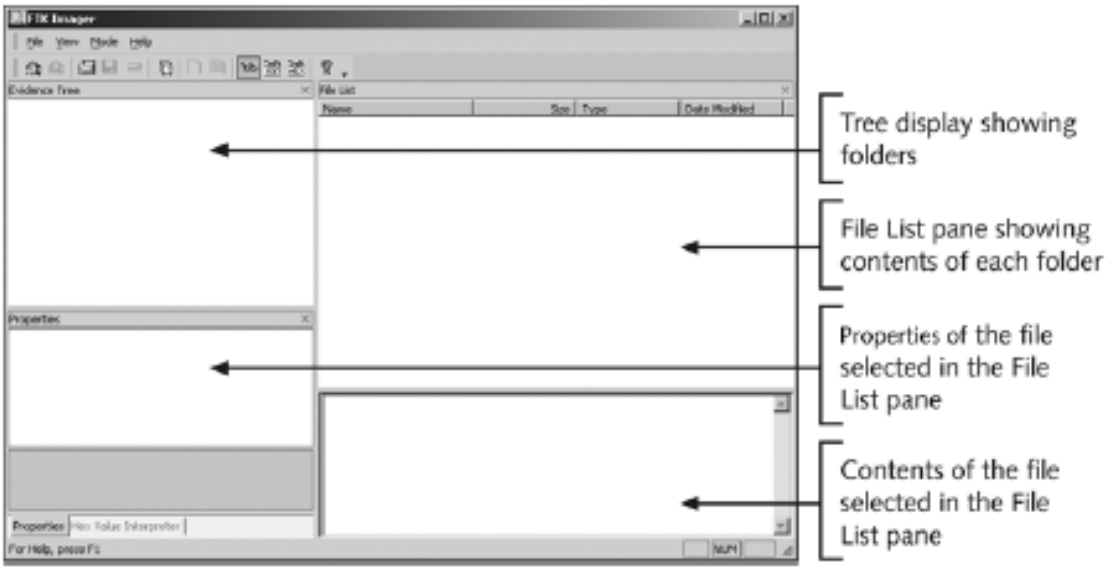

Figure 4-6 The FTK Imager main window

- Steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk to write-blocker
  - Start FTK Imager
  - Create Disk Image
    - Use Physical Drive option

Validating Data Acquisitions

- most critical aspect of computer forensics is validating digital evidence
- Requires using a hashing algorithm utility
- Validation techniques
  - CRC-32, MD5, and SHA-1 to SHA-512

Linux Validation Methods

- Validating dd acquired data
  - You can use md5sum or sha1sum utilities
  - md5sum or sha1sum utilities should be run on all suspect disks and volumes or segmented volumes

- Validating dcfldd acquired data
  - Use the hash option to designate a hashing algorithm of md5, sha1, sha256, sha384, or sha512
  - hashlog option outputs hash results to a text file that can be stored with the image files
  - vf (verify file) option compares the image file to the original medium

Windows Validation Methods

- Windows has no built-in hashing algorithm tools for computer forensics
  - Third-party utilities can be used
- Commercial computer forensics programs also have built-in validation features
  - Each program has its own validation technique
- Raw format image files don't contain metadata
  - Separate manual validation is recommended for all raw acquisitions

Performing RAID Data Acquisitions

- Acquisitions of RAID drives can be challenging and frustrating for computing forensics examiners because of how RAID systems are designed, configured, and sized
- **Redundant array of independent** (formerly "inexpensive") **disks (RAID)**
  - Computer configuration involving two or more disks
  - Originally developed as a data-redundancy measure
- RAID 0
  - Provides rapid access and increased storage
  - Lack of redundancy
- RAID 1
  - Designed for data recovery
  - More expensive than RAID 0
- RAID 2
  - Similar to RAID 1
  - Data is written to a disk on a bit level
  - Has better data integrity checking than RAID 0
  - Slower than RAID 0
- RAID 3
  - Uses data stripping and dedicated parity
- RAID 4

- Data is written in blocks

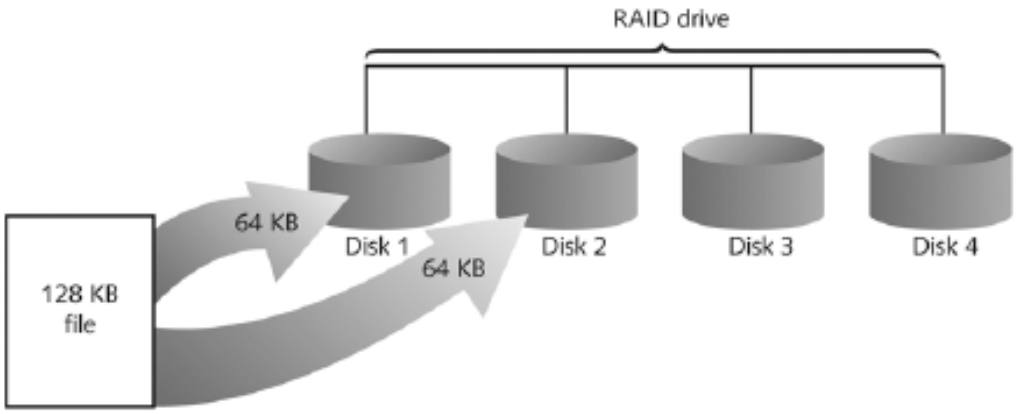

Figure 4-11 RAID 0: Striping

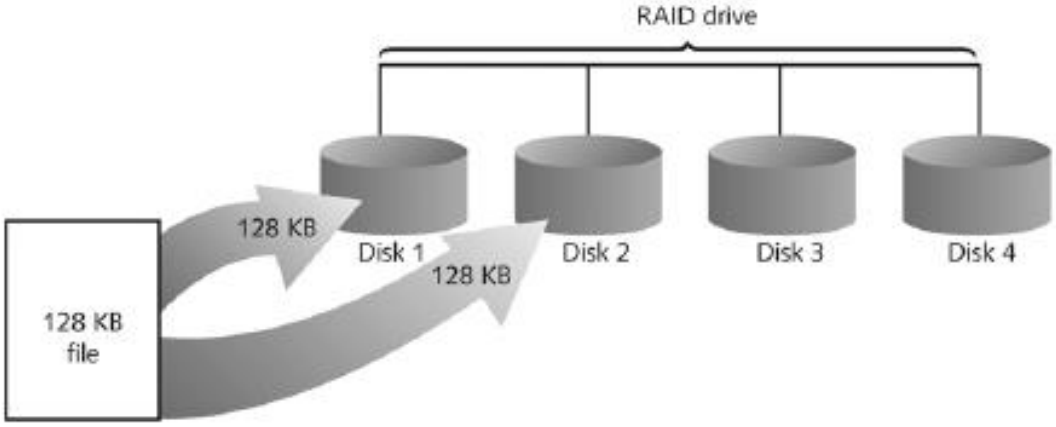

Figure 4-12 RAID 1: Mirroring

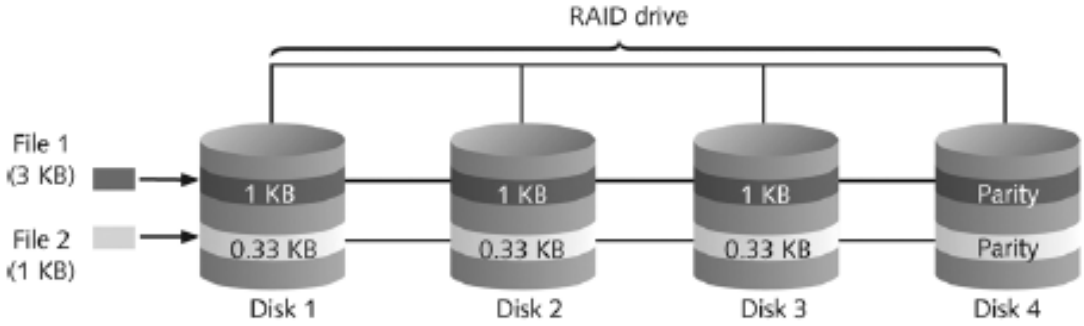

Figure 4-13 RAID 2: Striping (bit level)

- RAID 5
  - Similar to RAIDs 0 and 3
  - Places parity recovery data on each disk
- RAID 6
  - Redundant parity on each disk
- RAID 10, or mirrored striping

- Also known as RAID 1+0
- Combination of RAID 1 and RAID 0

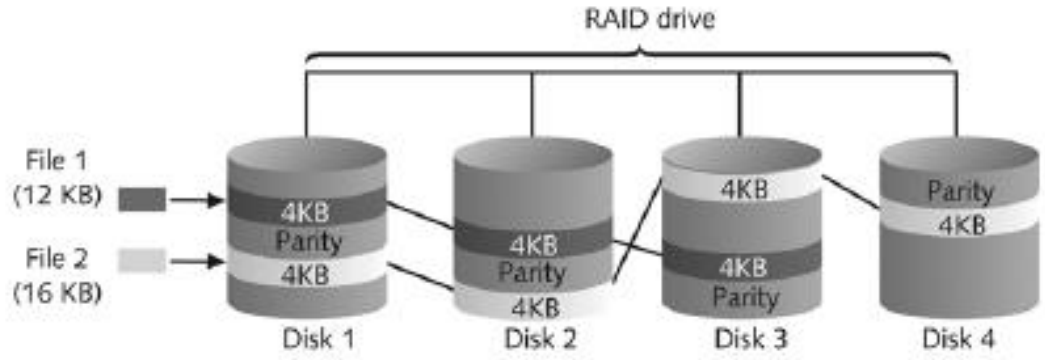

Figure 4-14 RAID 5: Block-level striping with distributed parity

Acquiring RAID Disks

- Concerns
  - How much data storage is needed?
  - What type of RAID is used?
  - Do you have the right acquisition tool?
  - Can the tool read a forensically copied RAID image?
  - Can the tool read split data saves of each RAID disk?
- Older hardware-firmware RAID systems can be a challenge when you're making an image
- Vendors offering RAID acquisition functions
  - Technologies Pathways ProDiscover
  - Guidance Software EnCase
  - X-Ways Forensics
  - Runtime Software
  - R-Tools Technologies
- Occasionally, a RAID system is too large for a static acquisition
  - Retrieve only the data relevant to the investigation with the sparse or logical acquisition method

Using Remote Network Acquisition Tools

- You can remotely connect to a suspect computer via a network connection and copy data from it
- Remote acquisition tools vary in configurations and capabilities
- Drawbacks
  - LAN's data transfer speeds and routing table conflicts could cause problems
  - Gaining the permissions needed to access more secure subnets

  - Heavy traffic could cause delays and errors

Remote Acquisition with ProDiscover

- With ProDiscover Investigator you can:
  - Preview a suspect's drive remotely while it's in use
  - Perform a live acquisition
  - Encrypt the connection
  - Copy the suspect computer's RAM
  - Use the optional stealth mode
- ProDiscover Incident Response additional functions
  - Capture volatile system state information
  - Analyze current running processes
- ProDiscover Incident Response additional functions (continued)
  - Locate unseen files and processes
  - Remotely view and listen to IP ports
  - Run hash comparisons
  - Create a hash inventory of all files remotely
- PDServer remote agent
  - ProDiscover utility for remote access
  - Needs to be loaded on the suspect
- PDServer installation modes
  - Trusted CD
  - Preinstallation
  - Pushing out and running remotely
- PDServer can run in a stealth mode
  - Can change process name to appear as OS function
- Remote connection security features
  - Password Protection
  - Encryption
  - Secure Communication Protocol
  - Write Protected Trusted Binaries
  - Digital Signatures