Catalog

1.1. 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.
- ✓ While early actions by the U.S. Secret Service may validate some of these early concerns, the efforts of the EFF have often overlooked the negative potentiality of this global marketplace that has reunited a society that had increasingly removed itself through suburbanization. Just as the Industrial Revolution enhanced threats to national security and created an environment conducive to street/predatory crime through the

concentration of the urban population, the **Information** or **Digital Revolution** has created a new forum for both terrorist activity and criminal behavior. Indeed, this latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike. Critical infrastructures, increasingly characterized by tight couplings and interdependency of IT, emergency services, public utilities, banking sectors, food supplies, and transportation systems, have resulted in an interconnectivity inconsistent with traditional security strategies. Such myopia has similarly impacted private citizens who have failed to employ rudimentary measures of cyberprotection even as they add additional doorlocks and alarm systems to insulate themselves from physical attacks.

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.
- ✓ C*ybercrime* 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, **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.

1.2. Traditional problems associated with Computer Crime

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.

1.3. Introduction to Identity Theft & Identity 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.

c. 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.

d. 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.

e. 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
h. Card Skimming, ATM Manipulation and Fraudulent Machines

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.

b. 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.

c. 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.

d. 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

e. 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.

f. 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.

g. 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.

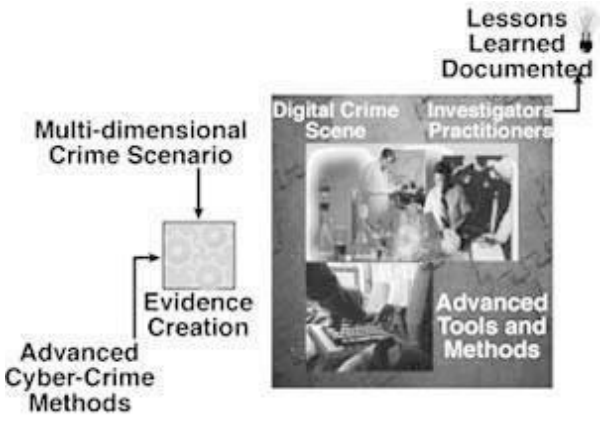
Card skimmers come in a variety of shapes and sizes (most often miniaturized cameras or copiers and can be mounted on retail and ATMs).

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.

1.4. Types of CF techniques

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 information directorate's cyber forensic concepts are new and untested.
- 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 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. , 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.

Types of Law Enforcement: Computer Forensic Technology

- Law enforcement and military agencies have been involved in processing computer evidence for years.
- Windows XP and Windows 2003 are operating systems that are often used on notebook and desktop computers in corporations and government agencies. Thus, they are currently the operating systems most likely to be encountered in computer investigations and computer security reviews.

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.

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.

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.

File Slack

- 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.

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 covertly capture keyboard activity from corporate executives, for example. For this reason, it is important that the participants understand these potential risks and how to identify them.

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.

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.

TYPES OF BUSINESS COMPUTER FORENSIC 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), is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center. No physical access is necessary.

Creating Trackable Electronic Documents

There are so many powerful intrusion detection tools that allow the user to create trackable electronic documents.

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

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 . According to a recent joint Computer Security Institute/FBI survey, 72% of the Fortune 1000 companies experienced laptop theft.

Basic Forensic Tools and Techniques

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

Forensic Services Available

- Through computer forensic evidence acquisition services, forensic experts for companies like Capitol Digital Document Solutions can provide management with a potent arsenal of digital tools at its disposal. They have the necessary software and hardware to travel to designated sites throughout the world to acquire an exact image of hard drives, tapes, etc.

- This image is an exact duplication of the source media and allows evaluation within their laboratories with minimal disruption to others. Services include but are not limited to
  - ✓ Lost password and file recovery
  - ✓ Location and retrieval of deleted and hidden files
  - ✓ File and email decryption
  - ✓ Email supervision and authentication
  - ✓ Threatening email traced to source
  - ✓ Identification of Internet activity
  - ✓ Computer usage policy and supervision
  - ✓ Remote PC and network monitoring
  - ✓ Tracking and location of stolen electronic files
  - ✓ Honeypot sting operations
  - ✓ Location and identity of unauthorized software users
  - ✓ Theft recovery software for laptops and PCs
  - ✓ Investigative and security software creation
  - ✓ Protection from hackers and viruses

1.5. Incident and incident response methodology

A computer security incident is a violation or imminent threat of violation1 of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- ✓ An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- ✓ Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- ✓ An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- ✓ A user provides or exposes sensitive information to others through peer-to-peer file sharing services

Need for Incident Response :

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. The concept of computer security incident response has become widely accepted and implemented. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data. An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

Incident Response Team Structure :

An incident response team should be available for anyone who discovers or suspects that an incident involving the organization has occurred. One or more team members, depending on the magnitude of the incident and availability of personnel, will then handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services. The incident response team's success depends on the participation and cooperation of individuals throughout the organization. This section identifies such individuals, discusses incident response team models, and provides advice on selecting an appropriate model.

Team Models Possible structures for an incident response team include the following:

- **Central Incident Response Team:** A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
- **Distributed Incident Response Teams:** The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single coordinated entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents.
- **Coordinating Team:** An incident response team provides advice to other teams without having authority over those teams—for example, a department wide team may assist individual agencies' teams. This model can be thought of as a CSIRT for CSIRTs. Because the focus of this document is central and distributed CSIRTs, the coordinating team model is not addressed in detail in this document.

Employees: The organization performs all of its incident response work, with limited technical and administrative support from contractors.

Partially Outsourced: The organization outsources portions of its incident response work. Although incident response duties can be divided among the organization and one or more outsourcers in many ways, a few arrangements have become commonplace: – The most prevalent arrangement is for the organization to outsource 24-hours-a-day, 7-days-aweek (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization's incident response team. – Some organizations perform basic incident response work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread.

Fully Outsourced: The organization completely outsources its incident response work, typically to an onsite contractor. This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees. It is assumed that the organization will have employees supervising and overseeing the outsourcer's work

When considering outsourcing, organizations should keep these issues in mind:

Current and Future Quality of Work: Organizations should consider not only the current quality (breadth and depth) of the outsourcer's work, but also efforts to ensure the quality of future work— for example, minimizing turnover and burnout and providing a solid training program for new employees. Organizations should think about how they could objectively assess the quality of the outsourcer's work.

Division of Responsibilities: Organizations are often unwilling to give an outsourcer authority to make operational decisions for the environment (e.g., disconnecting a web server). It is important to document the appropriate actions for these decision points. For example, one partially outsourced model addresses this issue by having the outsourcer provide incident data to the organization's internal team, along with recommendations for further handling

the incident. The internal team ultimately makes the operational decisions, with the outsourcer continuing to provide support as needed.

Sensitive Information Revealed to the Contractor: Dividing incident response responsibilities and restricting access to sensitive information can limit this. For example, a contractor may determine what user ID was used in an incident (e.g., ID 123456) but not know what person is associated with the user ID. Employees can then take over the investigation. Non-disclosure agreements (NDAs) are one possible option for protecting the disclosure of sensitive information.

Lack of Organization-Specific Knowledge: Accurate analysis and prioritization of incidents are dependent on specific knowledge of the organization's environment. The organization should provide the outsourcer regularly updated documents that define what incidents it is concerned about, which resources are critical, and what the level of response should be under various sets of circumstances. The organization should also report all changes and updates made to its IT infrastructure, network configuration, and systems. Otherwise, the contractor has to make a best guess as to how each incident should be handled, inevitably leading to mishandled incidents and frustration on both sides. Lack of organization-specific knowledge can also be a problem when incident response is not outsourced if communications are weak among teams or if the organization simply does not collect the necessary information.

Lack of Correlation: Correlation among multiple data sources is very important. If the intrusion detection system records an attempted attack against a web server, but the outsourcer has no access to the server's logs, it may be unable to determine whether the attack was successful. To be efficient, the outsourcer will require administrative privileges to critical systems and security device logs remotely over a secure channel. This will increase administration costs, introduce additional access entry points, and increase the risk of unauthorized disclosure of sensitive information.

Handling Incidents at Multiple Locations: Effective incident response work often requires a physical presence at the organization's facilities. If the outsourcer is offsite, consider where

the outsourcer is located, how quickly it can have an incident response team at any facility, and how much this will cost. Consider onsite visits; perhaps there are certain facilities or areas where the outsourcer should not be permitted to work.

Maintaining Incident Response Skills In-House: Organizations that completely outsource incident response should strive to maintain basic incident response skills in-house. Situations may arise in which the outsourcer is unavailable, so the organization should be prepared to perform its own incident handling. The organization's technical staff must also be able to understand the significance, technical implications, and impact of the outsourcer's recommendations.

Incident Response Personnel :

A single employee, with one or more designated alternates, should be in charge of incident response. In a fully outsourced model, this person oversees and evaluates the outsourcer's work. All other models generally have a team manager and one or more deputies who assumes authority in the absence of the team manager. The managers typically perform a variety of tasks, including acting as a liaison with upper management and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills.

Managers should be technically adept and have excellent communication skills, particularly an ability to communicate to a range of audiences. Managers are ultimately responsible for ensuring that incident response activities are performed properly. In addition to the team manager and deputy, some teams also have a technical lead—a person with strong technical skills and incident response experience who assumes oversight of and final responsibility for the quality of the team's technical work.

The position of technical lead should not be confused with the position of incident lead. Larger teams often assign an incident lead as the primary POC for handling a specific incident; the incident lead is held accountable for the incident's handling.

Depending on the size of the incident response team and the magnitude of the incident, the incident lead may not actually perform any actual incident handling, but rather coordinate the handlers' activities, gather information from the handlers, provide incident updates to other groups, and ensure that the team's needs are met. Members of the incident response team should have excellent technical skills, such as system administration, network administration, programming, technical support, or intrusion detection. Every team member should have good problem solving skills and critical thinking abilities.

It is not necessary for every team member to be a technical expert—to a large degree, practical and funding considerations will dictate this—but having at least one highly proficient person in each major area of technology (e.g., commonly attacked operating systems and applications) is a necessity. It may also be helpful to have some team members specialize in particular technical areas, such as network intrusion detection, malware analysis, or forensics.

It is also often helpful to temporarily bring in technical specialists that aren't normally part of the team. It is important to counteract staff burnout by providing opportunities for learning and growth. Suggestions for building and maintaining skills are as follows

- Budget enough funding to maintain, enhance, and expand proficiency in technical areas and security disciplines, as well as less technical topics such as the legal aspects of incident response. This should include sending staff to conferences and encouraging or otherwise incentivizing participation in conferences, ensuring the availability of technical references that promote deeper technical understanding, and occasionally bringing in outside experts (e.g., contractors) with deep technical knowledge in needed areas as funding permits.
- Give team members opportunities to perform other tasks, such as creating educational materials, conducting security awareness workshops, and performing research.

- Consider rotating staff members in and out of the incident response team, and participate in exchanges in which team members temporarily trade places with others (e.g., network administrators) to gain new technical skills.
- Maintain sufficient staffing so that team members can have uninterrupted time off work (e.g., vacations).
- Create a mentoring program to enable senior technical staff to help less experienced staff learn incident handling.
- Develop incident handling scenarios and have the team members discuss how they would handle them.

Incident response team members should have other skills in addition to technical expertise. Teamwork skills are of fundamental importance because cooperation and coordination are necessary for successful incident response. Every team member should also have good communication skills. Speaking skills are important because the team will interact with a wide variety of people, and writing skills are important when team members are preparing advisories and procedures. Although not everyone within a team needs to have strong writing and speaking skills, at least a few people within every team should possess them so the team can represent itself well in front of others.

Dependencies within Organizations :

It is important to identify other groups within the organization that may need to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including:

Management:

Management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various

stakeholders, minimizing damage, and reporting to Congress, OMB, the General Accounting Office (GAO), and other parties.

Information Assurance:

Information security staff members may be needed during certain stages of incident handling (prevention, containment, eradication, and recovery)—for example, to alter network security controls (e.g., firewall rulesets).

IT Support:

IT technical experts (e.g., system and network administrators) not only have the needed skills to assist but also usually have the best understanding of the technology they manage on a daily basis. This understanding can ensure that the appropriate actions are taken for the affected system, such as whether to disconnect an attacked system.

Legal Department:

Legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.

Public Affairs and Media Relations:

Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.

Human Resources:

If an employee is suspected of causing an incident, the human resources department may be involved—for example, in assisting with disciplinary proceedings.

Business Continuity Planning:

Organizations should ensure that incident response policies and procedures and business continuity processes are in sync. Computer security incidents undermine the business resilience of an organization. Business continuity planning professionals should be made aware of incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans. Further, because business continuity planners have extensive expertise in minimizing operational disruption during severe circumstances, they may be valuable in planning responses to certain situations, such as denial of service (DoS) conditions.

Physical Security and Facilities Management:

Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office.

Incident Response Team Services

The main focus of an incident response team is performing incident response, but it is fairly rare for a team to perform incident response only. The following are examples of other services a team might offer:

Intrusion Detection: The first tier of an incident response team often assumes responsibility for intrusion detection. The team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.

Advisory Distribution: A team may issue advisories within the organization regarding new vulnerabilities and threats. Automated methods should be used whenever appropriate to disseminate information; for example, the National Vulnerability Database (NVD) provides information via XML and RSS feeds when new vulnerabilities are added to it.

Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are likely to leverage in their social engineering. Only one group within the organization should distribute computer security advisories to avoid duplicated effort and conflicting information.

Education and Awareness: Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. This information can be communicated through many means: workshops, websites, newsletters, posters, and even stickers on monitors and laptops.

Information Sharing: Incident response teams often participate in information sharing groups, such as ISACs or regional partnerships. Accordingly, incident response teams often manage the organization's incident information sharing efforts, such as aggregating information related to incidents and effectively sharing that information with other organizations, as well as ensuring that pertinent information is shared within the enterprise.

Recommendations

The key recommendations presented in this section for organizing a computer security incident handling capability are summarized below.

Establish a formal incident response capability: Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. FISMA requires Federal agencies to establish incident response capabilities.

Create an incident response policy: The incident response policy is the foundation of the incident response program. It defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items.

Develop an incident response plan based on the incident response policy: The incident response plan provides a roadmap for implementing an incident response program based on the organization's policy. The plan indicates both short- and long-term goals for the program, including metrics for measuring the program. The incident response plan should also indicate how often incident handlers should be trained and the requirements for incident handlers.

Develop incident response procedures: The incident response procedures provide detailed steps for responding to an incident. The procedures should cover all the phases of the incident response process. The procedures should be based on the incident response policy and plan.

Establish policies and procedures regarding incident-related information sharing: The organization should communicate appropriate incident details with outside parties, such as the media, law enforcement agencies, and incident reporting organizations. The incident response team should discuss this with the organization's public affairs office, legal department, and management to establish policies and procedures regarding information sharing. The team should comply with existing organization policy on interacting with the media and other outside parties.

Provide pertinent information on incidents to the appropriate organization: Federal civilian agencies are required to report incidents to US-CERT; other organizations can contact US-CERT and/or their ISAC. Reporting is beneficial because US-CERT and the ISACs use the reported data to provide information to the reporting parties regarding new threats and incident trends.

Consider the relevant factors when selecting an incident response team model: Organizations should carefully weigh the advantages and disadvantages of each possible team structure model and staffing model in the context of the organization's needs and available resources.

Select people with appropriate skills for the incident response team: The credibility and proficiency of the team depend to a large extent on the technical skills and critical thinking abilities of its members. Critical technical skills include system administration, network

administration, programming, technical support, and intrusion detection. Teamwork and communications skills are also needed for effective incident handling. Necessary training should be provided to all team members.

Identify other groups within the organization that may need to participate in incident handling: Every incident response team relies on the expertise, judgment, and abilities of other teams, including management, information assurance, IT support, legal, public affairs, and facilities management.

Determine which services the team should offer: Although the main focus of the team is incident response, most teams perform additional functions. Examples include monitoring intrusion detection sensors, distributing security advisories, and educating users on security.

1.6. Forensics Technology and Systems

The Forensic systems are

- Internet security systems
- Intrusion detection systems
- Firewall security systems
- Storage area network security systems
- Network disaster recovery systems
- Public key infrastructure security systems
- Wireless network security systems
- Satellite encryption security systems
- Instant messaging (IM) security systems
- Net privacy systems
- Identity management security systems
- Identity theft prevention systems
- Biometric security systems
- Homeland security systems

INTERNET SECURITY SYSTEMS

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

General Internet Security Principles and Architecture

- The first step in defining a corporate Internet security policy is to draft a highlevel management policy statement establishing a framework and context for security within an organization.
- The next step is to start a systematic analysis of the assets of an organization, determining the value of information, or the possible damage to reputation should it be disclosed, along with possible risks.

Security Hierarchy

- Information such as trade secrets, vault and authorization codes, and lock and key information are clearly of a **mission critical** nature, and their unintended disclosure could cause severe loss to a business or operation.
- **Departmental information** is typically data that is private to a particular department, such as payroll information in finance and medical records in personnel. There may be legal requirements for securing this information.
- **Company private information** varies from company to company but typically consists of information that should only be disclosed to employees and partners of a company, such as policy and procedure manuals.
- **Public information** is information such as product literature, brochures, and catalogs that needs to be freely available to anyone, but whose integrity needs to be assured to prevent unauthorized alteration. This information is often provided to customers and interested parties by means of the Internet

INTRUSION DETECTION SYSTEMS

- Intrusion detection systems help computer systems prepare for and deal with attacks.
- They collect information from a variety of vantage points within computer systems and networks and analyze this information for symptoms of security problems.
- Vulnerability assessment systems check systems and networks for system problems and configuration errors that represent security vulnerabilities.
- Both intrusion detection and vulnerability assessment technologies allow organizations to protect themselves from losses associated with network security problems.
- This section explains how intrusion detection and vulnerability assessment fits into the overall framework of security products and techniques used in computer forensics.

Intrusion Detection Defined

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

Vulnerability Assessment and Intrusion Detection

- Vulnerability assessment products (also known as *scanners*) perform rigorous examinations of systems in order to determine weaknesses that might allow security violations.
- These products use two strategies for performing these examinations. First, *passive,* host-based mechanisms inspect system configuration files for unwise settings, system password files for weak passwords, and other system objects for security policy violations.

FIREWALL SECURITY SYSTEMS

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

The Reason for Firewalls

- The general reasoning behind firewall usage is that without a firewall, a subnet's systems are exposed to inherently insecure services such as Network
  File System (NFS) or Network Information Service (NIS) and to probes and attacks from hosts elsewhere on the network.

The Need For Firewalls

These attacks come from three basic groups:

- Persons who see attacking a corporation's information system as a technological challenge

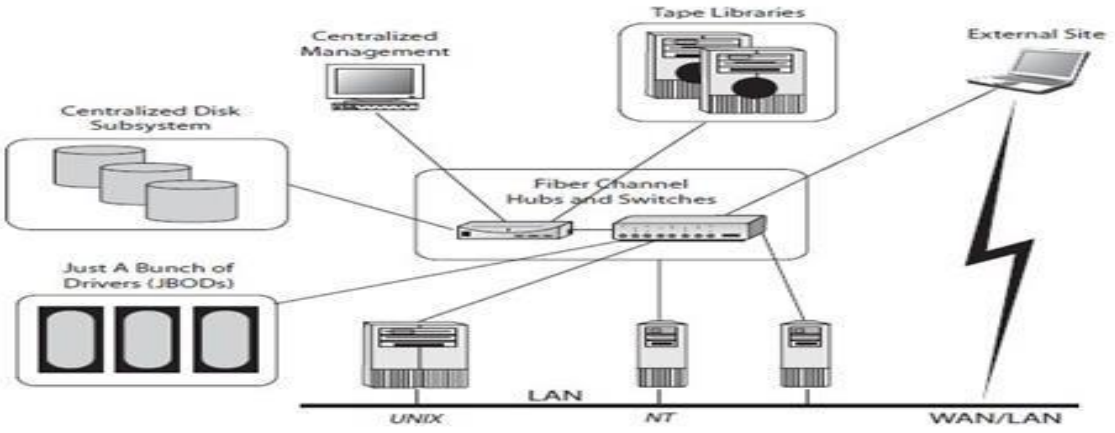
- Persons with no identified political or social agenda who see attacking a corporation's information system as an opportunity for high-tech vandalism
- Persons associated with a corporate competitor or political adversary who see the corporation's information system as a legitimate strategic target
- **Data Integrity:** Absolute verification that data has not been modified
- **Confidentiality:** Privacy with encryption, scrambled text
- **Authentication:** Verification of originator on contract
- **Non-Repudiation:** Undeniable proof-of-participation
- **Availability:** Assurance of service demand

Benefits of Firewalls

- Protection from vulnerable services
- Controlled access to site systems
- Concentrated security
- Enhanced privacy
- Logging and statistics on network use and misuse
- Policy enforcement

STORAGE AREA NETWORK SECURITY SYSTEMS

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



SAN Benefits

1. Centralized Management
2. Scalability
3. Reliability
4. Performance

NETWORK DISASTER RECOVERY SYSTEMS

- The high availability of mission-critical systems and communications is a major requirement for the viability of the modern organization.
- A network disaster could negate the capability of the organization to provide uninterrupted service to its internal and external customers.
- Network disaster recovery (NDR) is the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization's critical business functions.
- NDR is not a new idea. In recent years, data has become a vitally important corporate asset essential to business continuity. A fundamental requirement of economic viability is the ability to recover crucial data quickly after a disaster.

PUBLIC KEY INFRASTRUCTURE SYSTEMS

A Public Key Infrastructure Systems (PKI) enables users of an insecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The PKI provides for digital certificates that can identify individuals or organizations and directory services that can store and, when necessary, revoke them.

- PKI is the underlying technology that provides security for the secure sockets layer (SSL) and hyper text transfer protocol secure sockets (HTTPS) protocols, which are used extensively to conduct secure e-business over the Internet.

A PKI consists of

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

PKI is complicated but is a sound solution to a difficult problem, namely enabling two parties to exchange data securely over an insecure medium without the benefit of prior communication. It has been adopted by the popular Web browsers and is widely used for one-off business-to-customer (B2C) transactions. In general, however, PKI still faces

challenges in terms of application support, interoperability between vendors, differing government legislation, and practical key management.

WIRELESS NETWORK SECURITY SYSTEMS

- wireless network security vendors (even giants like IBM) are busy developing products to fight the viruses and security breaches of the future.
- Among them are those that head off problems on a wireless network level, within applications and on devices.
- The widely used wireless LAN standard, 802.11, came under fire recently when researchers at the University of California at Berkeley figured out how to crack its builtin encryption.
- Still, there is some hope, because developers addressed wireless network security from the start and are working to beef it up before wireless LANs become more pervasive.
- Companies will also have to secure wireless transactions. There will be attacks on the devices themselves, but they quickly will be focused on transactions.

SATELLITE ENCRYPTION SECURITY SYSTEMS

- The boom in satellite communications is changing the way we work and live, but it is becoming a security nightmare for those organizations and governments whose survival depends on the protection of intellectual property distribution, electronic commerce, electronic battlefields and national security.

- The ability to securely exchange information between billions of users around the globe involving perhaps trillions of transactions is vital to the continued growth and usefulness of satellite communications as well as the Internet and intranets.

Current and Future Satellite Technology

- High-Tech Mayhem
- *High-Tech Highwaymen*
- Prevention versus Detection
- Odd Person Out Attacks

Satellite Encryption Secure Exchange

- An *encryption* infrastructure can be effectively designed to solve most of the confidentiality and authentication concerns of satellite transmission with the Internet. However, secure exchange can be either a one-way or a two-way encounter, and the satellite encryption requirements and strategies are quite different for each.

- A one-way transaction is typified by email transmissions to and from satellites over the Internet. Although email messages are frequently answered, each message transmission is a unique, stand-alone event.

Pretty Good Privacy

- PGP uses the RSA (Rivest, Shamir, Adelman) public key encryption scheme and the MD5 (Message Digest 5) one-way hash function to form a digital signature, which assures the recipient that an incoming satellite transmission or message is authentic—that it not only comes from the alleged sender but also has not been altered.

The sequence for this is as follows:

1. The sender creates a private message.
2. MD5 generates a 128-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is attached to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it to the decrypted hash code. If the two match, the message is accepted as authentic.

This session key is bound to the message and transmitted with it as follows:

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted, using IDEA with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended (to prefix a string or statement with another or to place a word or set of numbers in front of an existing word or set of numbers; for example, to prepend "sub" to "net" would yield "subnet") to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message.

INSTANT MESSAGING (IM) SECURITY SYSTEMS

- The security threats from IM are straightforward. Since deployment isn't controlled, the enterprise can't keep a rein on how the systems are used. With the public IM networks, the individual employee registers for service.

Securing IM

- IM management and security systems act as proxies for IM traffic going into the network, which imposes policies before letting traffic through.

- Besides addressing security, this architecture puts the IM management and security vendors in a position to deal with the pesky problem of the lack of interoperability among networks.

NET PRIVACY SYSTEMS

- Privacy is a social, political, and economic issue. Privacy protection for the individual was born with democracy and was originally designed to keep oppressive governments from intruding on individual freedoms.
- In a world of advanced industrial societies where most major countries are at peace with each other, the violation of privacy and civil liberties has come under new threats.
- People still have every reason to keep a tight reign on snoopy governments (like the use of the Patriot Act), but now they must also be concerned about the commercial violation of individual privacy rights and desires.
- Some private companies have made a business out of selling information about individuals, groups, and organizations. This has raised considerable concern among privacy advocates.

IDENTITY MANAGEMENT SECURITY SYSTEMS

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

The Challenges of Managing Digital Identities

- Aggregation
- Web Services
- Online Partnerships

User Concerns and Business Issues

- Security
- Convenience
- Privacy

Business Issues: Trust, Control, and Accountability

- Trust via Authentication
- Control via Access Management
- Accountability via Audit

Approaches to Identity Management

- Silo
- Closed Community
- Federated

IDENTITY THEFT

- Identity theft is the appropriation of an individual's personal information in order to impersonate that person in a legal sense. stealing someone's identity enables the thief to make a frightening number of financial and personal transactions in someone else's name, leaving the victim responsible for what may turn out to be mind-boggling turmoil in his or her life.
- Identity theft can still be done by such low-tech means as knowing someone else's basic identifying information and initiating personal transactions in that person's name, but today, identities can also be stolen using highly technical and sophisticated means of obtaining the personal data of a stranger.

How Identity Theft Is Done

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

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, preapproved credit offers, telephone calling cards, and tax information.
- They complete a change of address form to divert your mail to another location. They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving." They get your business or personnel records at work.
- They find personal information in your home.
- They use personal information you share on the Internet.

BIOMETRIC SECURITY SYSTEMS

- A biometric system is the computer hardware and software used to recognize or verify an individual. Although there are many variations in how specific products and systems work, there are a number of common processing elements.

Collection

- As a first step, a system must collect or —capture the biometric to be used. One essential difference between the various techniques is the characteristic (body part or function) being analyzed.

Extraction

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

Comparison and Matching

- To use a biometric system, the specific features of a person's biometric characteristic are measured and captured each time he presents his —live biometric.
- This extracted information is translated into a mathematical code using the same method that created the template. The new code created from the live scan is compared against a central database of templates in the case of a one to-many match, or to a single stored template in the case of a one-to-one match.

HOMELAND SECURITY SYSTEMS

- The terms *homeland security* and *homeland defense* have received increased attention since the tragic events of September 11, 2001.
- While these terms are relatively new, the concepts behind them are not. Homeland security is defined as the deterrence, prevention, and preemption of and defense against aggression targeted at U.S. territory, sovereignty, population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies.
- Homeland defense on the other hand is a subset of homeland security.

Homeland Security Today

Security has the following organizational structure:

- Border and transportation security
- Emergency preparedness and response
- Chemical, biological, radiological, and nuclear countermeasures
- Information analysis and infrastructure protection

1.7. Understanding Computer Investigation

Digital investigations fall into two categories:

- ✓ Public-sector investigations
- ✓ Private-sector investigations

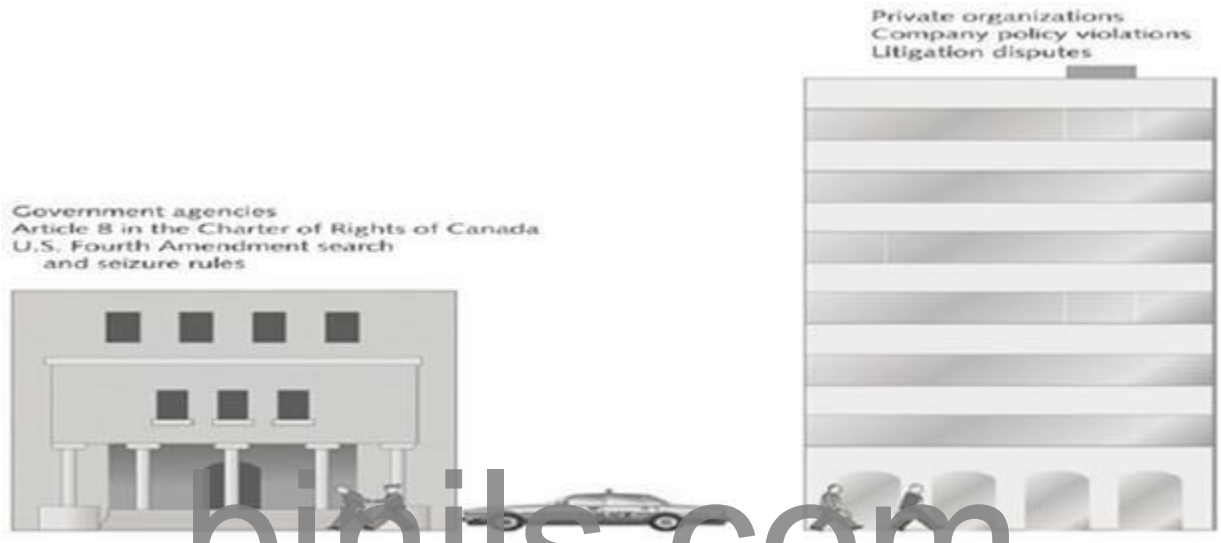


Fig. Public sector and Private sector Investigation

Public-sector investigations involve government agencies responsible for criminal investigations and prosecution Fourth Amendment to the U.S. Constitution Restrict government **search and seizure** . The Department of Justice (DOJ) updates information on computer search and seizure regularly .Private-sector investigations focus more on policy violations

Understanding Law Enforcement Agency Investigations

- When conducting public-sector investigations, you must understand laws on computer-related crimes including:
  - ✓ Standard legal processes
  - ✓ Guidelines on search and seizure
  - ✓ How to build a criminal case
- The Computer Fraud and Abuse Act was passed in 1986
  - – Specific state laws were generally developed later

Following Legal Processes

- A criminal investigation usually begins when someone finds evidence of or witnesses a crime . Witness or victim makes an **allegation** to the police
- Police interview the complainant and writes a report about the crime
- Report is processed and management decides to start an investigation or log the information in a police blotter
  – Blotter is a historical database of previous crimes
- **Digital Evidence First Responder (DEFR)**
  – Arrives on an incident scene, assesses the situation, and takes precautions to acquire and preserve evidence
- **Digital Evidence Specialist (DES)**
  – Has the skill to analyze the data and determine when another specialist should be called in to assist
- **Affidavit** - a sworn statement of support of facts about or evidence of a crime
  – Must include **exhibit**s that support the allegation

Understanding Private-Sector Investigations

- Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes
  – Example: wrongful termination
- Businesses strive to minimize or eliminate litigation
- Private-sector crimes can involve:
  – E-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage
- Businesses can reduce the risk of litigation by publishing and maintaining policies that employees find easy to read and follow
- Most important policies define rules for using the company's computers and networks
  – Known as an —Acceptable use policy

Line of authority - states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence Business can avoid litigation by displaying a **warning banner** on computer screens

- Informs end users that the organization reserves the right to inspect computer systems and network traffic

- Sample text that can be used in internal warning banners:
  - Use of this system and network is for official business only
  - Systems and networks are subject to monitoring at any time by the owner
  - Using this system implies consent to monitoring by the owner
  - Unauthorized or illegal users of this system or network will be subject to discipline or prosecution
- Businesses are advised to specify an **authorized requester** who has the power to initiate investigations
- Examples of groups with authority
  - ✓ Corporate security investigations
  - ✓ Corporate ethics office
  - ✓ Corporate equal employment opportunity office
  - ✓ Internal auditing
  - ✓ The general counsel or legal department
- During private investigations, you search for evidence to support allegations of violations of a company's rules or an attack on its assets
- Three types of situations are common:
  - ✦ Abuse or misuse of computing assets
  - ✦ E-mail abuse
  - ✦ Internet abuse
- A private-sector investigator's job is to minimize risk to the company
- The distinction between personal and company computer property can be difficult with cell phones, smartphones, personal notebooks, and tablet computers

- Bring your own device (BYOD) environment
  - Some companies state that if you connect a personal device to the business network, it falls under the same rules as company property

Maintaining Professional Conduct

- **Professional conduct** - includes ethics, morals, and standards of behavior
- An investigator must exhibit the highest level of professional behavior at all times
  - ✦ Maintain objectivity
  - ✦ Maintain credibility by maintaining confidentiality
- Investigators should also attend training to stay current with the latest technical changes in computer hardware and software, networking, and forensic tools

Preparing a Digital Forensics Investigation

The role of digital 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

- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

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 drive
  - 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
  - Known disk format
  - Location of evidence
- Based on these details, you can determine the case requirements

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 your **forensics workstation**
  - Retrieve 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

Organization 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 ___

Fig: Sample multi evidence form in Private sector environment

Securing Your Evidence

Use **evidence bags** to secure and catalog the evidence

- Use computer safe products when collecting computer evidence
- Antistatic bags
- Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
- CD drive bays
- Insertion slots for power supply electrical cords and USB cables

- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges
  - Make sure you have a safe environment for transporting and storing it until a secure evidence container is available

Procedures for Private-Sector High-Tech Investigations

- As an investigator, you need to develop formal procedures and informal checklists.To cover all issues important to high-tech investigations .Ensures that correct techniques areused in an investigation

Employee Termination Cases

- The majority of investigative work for termination cases involves employee abuse of corporate assets
- Incidents that create a hostile work environment are the predominant types of cases investigated
  - Viewing pornography in the workplace
  - Sending inappropriate e-mails
- Organizations must have appropriate policies in place

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
  - 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
  - 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 for each image
  - Compare hash signatures on all files on the original and re-created disks

- Steps for conducting an ACP case (cont'd)
  - 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
  - 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 the attorney and paralegal in analyzing data

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 when initiating an investigation
  - 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 to conducting an industrial espionage case
  - Gather all personnel assigned to the investigation and brief them on the plan
  - Gather resources to conduct the investigation
  - Place surveillance systems at key locations
  - 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**

  – Process of 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)

  – In data recovery, the customer or your company just wants the data back

- Computer forensics workstation
  - A specially configured PC
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use: – Write-blockers devices
- Enable you to boot to Windows without writing data to the evidence drive

Setting Up Your Workstation for Digital Forensics

- Basic requirements
  - A workstation running Windows XP or later
  - A write-blocker device
  - Digital forensics acquisition tool
  - Digital forensics analysis tool
  - 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
  - Carry the evidence to the computer forensics lab
  - Complete the evidence custody form
  - Secure evidence by locking the container

Analyzing the Digital Evidence

- Our job is to recover data from:
  - Deleted files
  - File fragments
  - Complete files
- Deleted files linger on the disk until new data is saved on the same physical location
- Tools can be used to retrieve deleted files

  ProDiscover Basic
- Steps to analyze a USB drive
  - Start ProDiscover Basic
  - Create a new case
  - Type the project number
  - Add an **Image File**
- Steps to display the contents of the acquired data
  - Click to expand **Content View**
  - Click **All Files** under the image filename path
- Steps to display the contents of the acquired data (cont'd)
  - Click **letter1** to view its contents in the data area
  - In the data area, view contents of letter1
- Analyze the data
  - Search for information related to the complaint
- Data analysis can be most time-consuming task

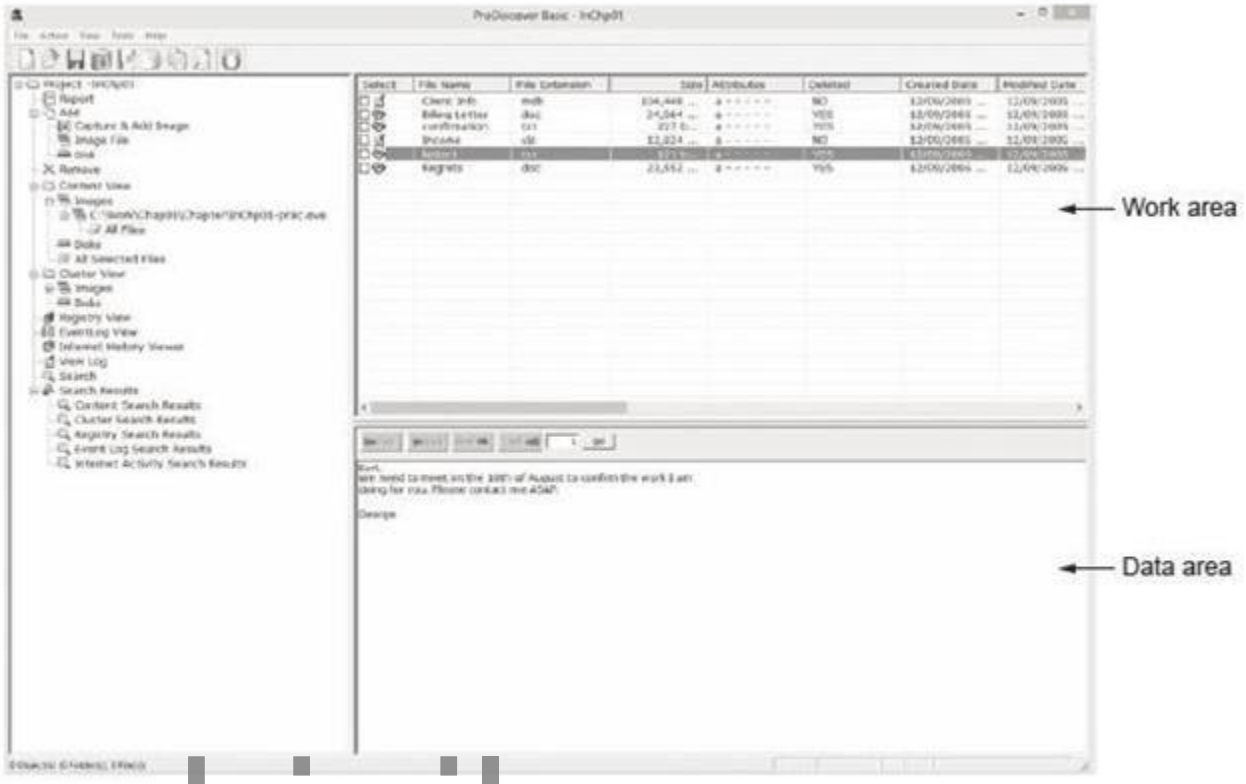


Fig: Selecting a file in the work area and viewing its contents in the data area.

- With ProDiscover Basic you can:
  - Search for keywords of interest in the case
  - Display the results in a search results window
  - Click each file in the search results window and examine its content in the data area
  - Export the data to a folder of your choice
  - Search for specific filenames
  - Generate a report of your activities

Completing the Case

- You need to produce a final report
  - State what you did and what you found
- Include ProDiscover report to document your work

- **Repeatable findings**
  - – Repeat the steps and produce the same result
- If required, use a report template
- Report should show conclusive evidence
  - – Suspect did or did not commit a crime or violate a company policy
- Keep a written journal of everything you do
  - – Your notes can be used in court
- Answer the six Ws:
  - – Who, what, when, where, why, and how
- You must also explain computer and network processes

Critiquing the Case

- Ask yourself the following questions:
  - – How could you improve your performance in the case?
  - – Did you expect the results you found? Did the case develop in ways you did not expect?
  - – Was the documentation as thorough as it could have been?
  - – What feedback has been received from the requesting source?
  - – Did you discover any new problems? If so, what are they?
  - – Did you use new techniques during the case or during research?

1.8. Data Acquisition

Understanding Storage Formats for Digital Evidence

- Data in a forensics acquisition tool is stored as an image file
- Three formats
  - Raw format
  - Proprietary formats
  - Advanced Forensics Format (AFF)

Raw Format

- Makes it possible to write bit-stream data to files
- ***Advantages***
  - Fast data transfers
  - Ignores 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 forensics tools have their own formats
- 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
- The Expert Witness format is unofficial standard

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format
- 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 of data collection
  - Creating a disk-to-image file
  - Creating a disk-to-disk
  - Creating a logical disk-to-disk or disk-to-data file
  - Creating a sparse data copy of a file or folder
- Determining the best method depends on the circumstances of the investigation
- Creating a disk-to-image file
  - Most common method and offers most flexibility
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLookIX
- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk's geometry configuration
  - EnCase, SafeBack, SnapCopy
- Logical acquisition or sparse acquisition
  - Can take several hours; use when your time is limited
  - Logical acquisition captures only specific files of interest to the case

- Sparse acquisition 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 called BitLocker makes static acquisitions more difficult and May require user to provide decryption key

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

- Some countries haven't accepted the use of write-blocking devices for data acquisitions

Mini-WinFE Boot CDs and USB Drives

Mini-WinFE

– Enables you to build a Windows forensic boot CD/DVD or USB drive so that connected drives are mounted as read-only

- Before booting a suspect's computer:

– Connect your target drive, such as a USB drive

- After Mini-WinFE is booted:

– You can list all connected drives and alter your target USB drive to readwrite mode so you can run an acquisition program

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 (cont'd) – Forensic Linux Live CDs (cont'd)
- Configured not to mount, or to mount as read-only, any connected storage media
- Well-designed Linux Live CDs for computer forensics
- Penguin Sleuth
- F.I.R.E
- CAINE
- Deft

- Kali Linux
- Knoppix
- SANS Investigative Toolkit
- Preparing a target drive for acquisition in Linux

– Current Linux distributions can create Microsoft FAT and NTFS partition tables

– **fdisk** command lists, creates, deletes, and verifies partitions in Linux

– **mkfs.msdos** command formats a FAT file system from Linux

– If you have a functioning Linux computer, follow steps starting on page 99 to learn how to prepare a target drive for acquisition

- 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

– 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 dd in Linux (cont'd)

– Follow the step starting on page 104 in the text to make an image of an NTFS disk on a FAT32 disk

- Acquiring data with dcfldd in Linux

– The dd command is intended as a data management tool

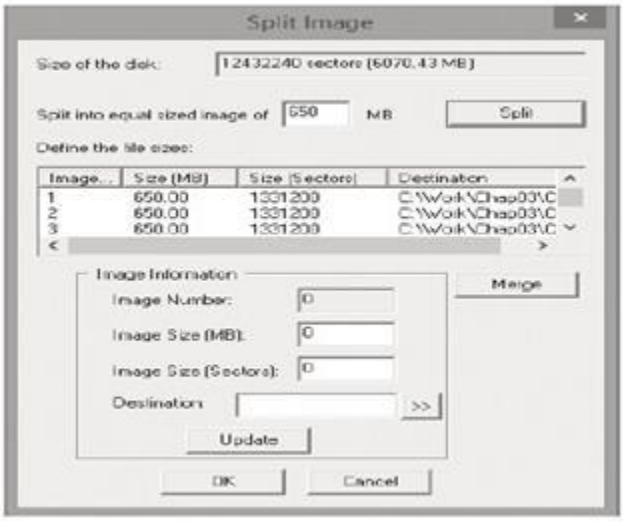
- Not designed for forensics acquisitions
- Acquiring data with dcfldd in Linux (cont'd) – dcfldd additional functions
- Specify hex patterns or text for clearing disk space

- 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 to write-blocker device
  - Create a storage folder on the target drive

- Using ProDiscover's Proprietary Acquisition Format
  - ProDiscover creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)
  - If the compression option was selected, ProDiscover uses a .cmp rather than an .eve extension on all segmented volumes
- Using ProDiscover's Raw Acquisition Format
  - Follow the same steps as for the proprietary format, but select the —UNIX style dd format in the Image Format list box
  - Raw acquisition saves only the image data and hash value
  - The raw format creates a log file (.pds extension) and segmented volume files



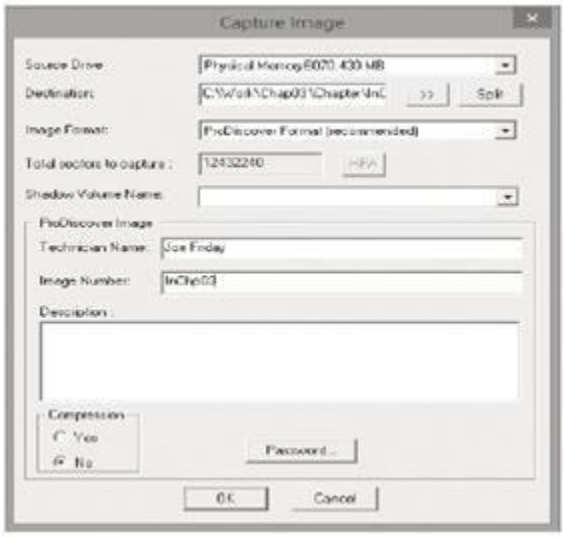


Fig: The split image dialog box

Fig: The Capture Image dialog box

Capturing an Image with Access Data FTK Imager Lite

- Included with AccessData Forensic Toolkit
- Designed for viewing 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 run from a Live CD, such as Mini-WinFE

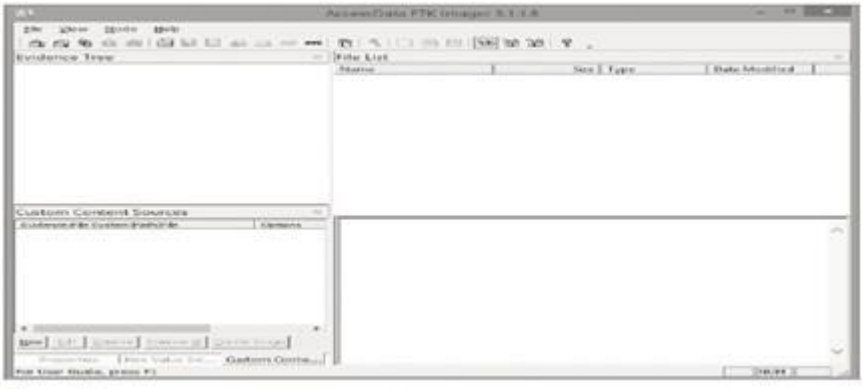


Fig: The FTK Imager main window

- FTK Imager can't acquire a drive's host protected area
- Use a write-blocking device and follow these steps – Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk to write-blocker
  - Start FTK Imager Lite
  - Create Disk Image - use Physical Drive option
  - See Figures on the following slides for more steps

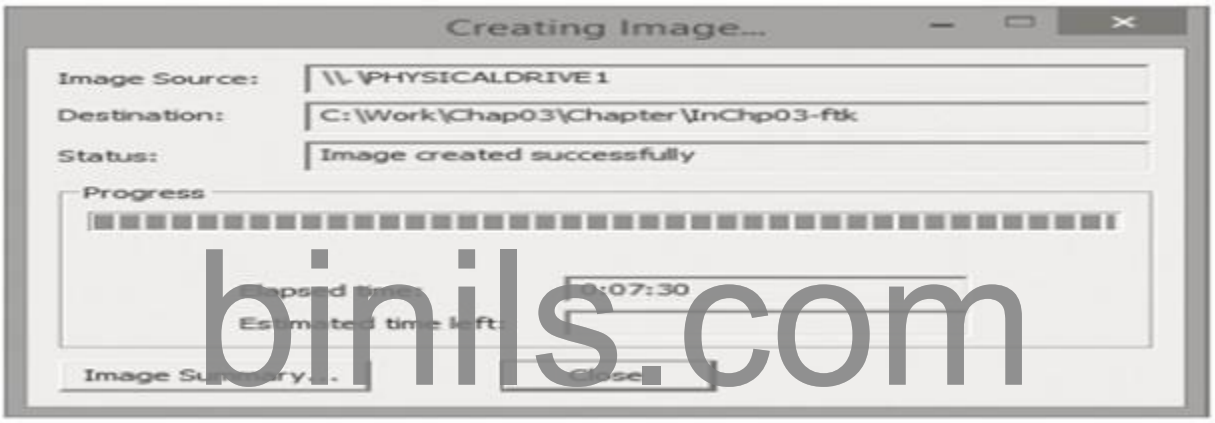


Fig: A complete image save

Validating Data Acquisitions

- Validating evidence may be the most critical aspect of computer forensics
- 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

- Acquisition of RAID drives can be challenging and frustrating because of how RAID systems are
  - Designed
  - Configured
  - Sized
- Size is the biggest concern
  - Many RAID systems now have terabytes of data

Understanding RAID

- 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
  - Biggest disadvantage is lack of redundancy

- RAID 1
  - Designed for data recovery
  - More expensive than RAID 0

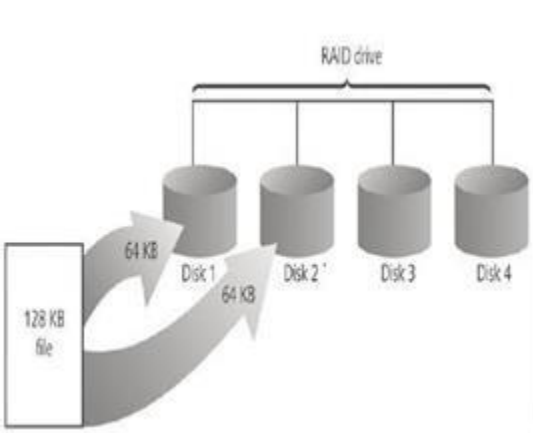


Fig: RAID 0-Striping

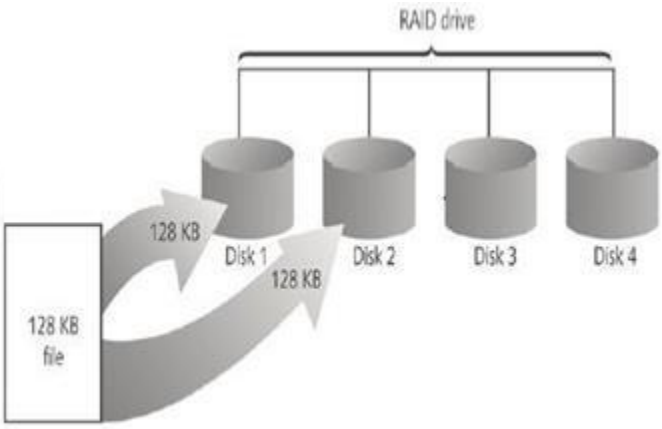


Fig: RAID 1-MIrroring

- 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

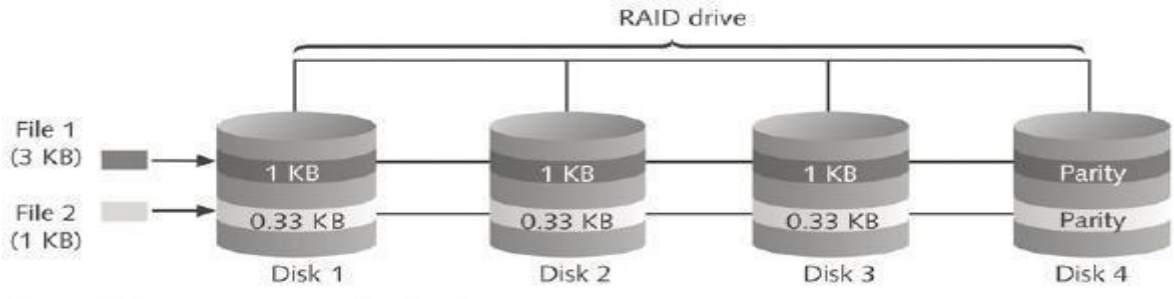


Fig: RAID 2-Striping (bit level)

- 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

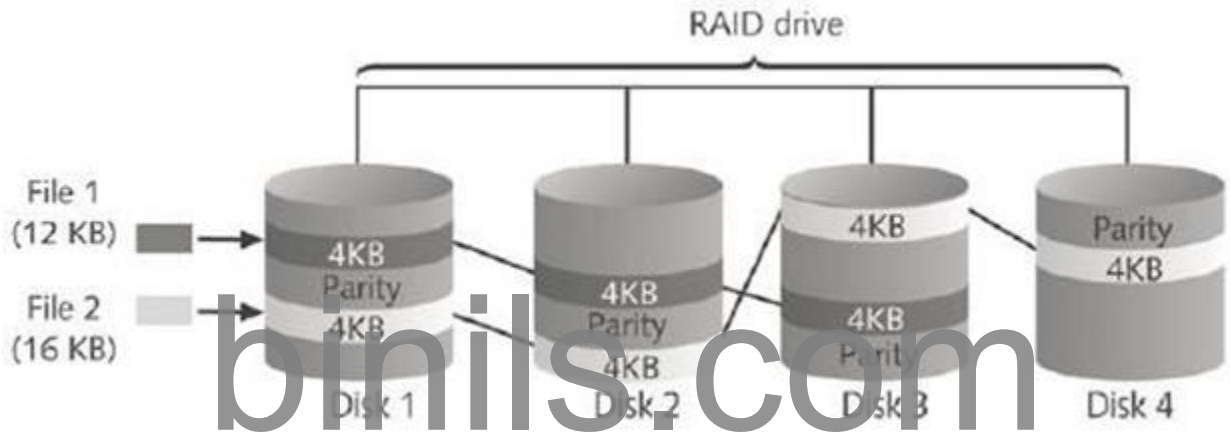


Fig: RAID 5:Block level striping with distributed parity

Acquiring RAID Disks

Address the following 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?

- Copying small RAID systems to one large disk is possible
- Vendors offering RAID acquisition functions
  - Technology Pathways ProDiscover
  - Guidance Software EnCase

  - X-Ways Forensics
  - AccessData FTK
  - 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
  - Antivirus, antispyware, and firewall tools can be configured to ignore remote access programs
  - Suspects could easily install their own security tools that trigger an alarm to notify them of remote access intrusions

Remote Acquisition with ProDiscover

- ProDiscover Incident Response additional functions
  - Capture volatile system state information
  - Analyze current running processes
  - 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

Remote Acquisition with EnCase Enterprise

- Remote acquisition features
  - Remote data acquisition of a computer's media and RAM data
  - Integration with intrusion detection system (IDS) tools
  - Options to create an image of data from one or more systems
  - Preview of systems
  - A wide range of file system formats
  - RAID support for both hardware and software

Remote Acquisition with R-Tools R-Studio

- R-Tools suite of software is designed for data recovery
- Remote connection uses Triple Data Encryption Standard (3DES) encryption
- Creates raw format acquisitions
- Supports various file systems

Remote Acquisition with WetStone US-LATT PRO

- US-LATT PRO
  - Part of a suite of tools developed by WetStone

- Can connect to a networked computer remotely and perform a live acquisition of all drives connected to it

Remote Acquisition with F-Response

F-Response

A vendor-neutral remote access utility

Designed to work with any digital forensics program

Sets up a security read-only connection

- Allows forensics examiners to access it
- Four different version of F-Response
  - Enterprise Edition, Consultant + Convert Edition, Consultant Edition, and TACTICAL Edition

Using Other Forensics-Acquisition Tools

- Other commercial acquisition tools
  - PassMark Software ImageUSB
  - ASRData SMART
  - Runtime Software
  - ILookIX Investigator IXimager
  - SourceForge

PassMark Software ImageUSB

- PassMark Software has an acquisition tool called ImageUSB for its OSForensics analysis product
- To create a bootable flash drive, you need:
  - Windows XP or later
  - ImageUSB downloaded from the OSForensics Web site

ASRData SMART

- ASRData SMART
  - A Linux forensics analysis tool that can make image files of a suspect drive
  - Can produce proprietary or raw format images

- Capabilities:
  - Data reading of bad sectors
  - Can mount drives in write-protected mode
  - Can mount target drives in read/write mode
  - Compression schemes to speed up acquisition or reduce amount of storage needed

Runtime Software

- Runtime Software offers shareware programs for data acquisition and recovery:
  - DiskExplorer for FAT and NTFS
- Features:
  - Create a raw format image file
  - Segment the raw format or compressed image for archiving purposes
  - Access network computers' drives

ILook Investigator IXimager

IXimager

  - Runs from a bootable floppy or CD
  - Designed to work only with ILook Investigator
  - Can acquire single drives and RAID drives – Supports:
- IDE (PATA)
- SCSI
- USB
- FireWire