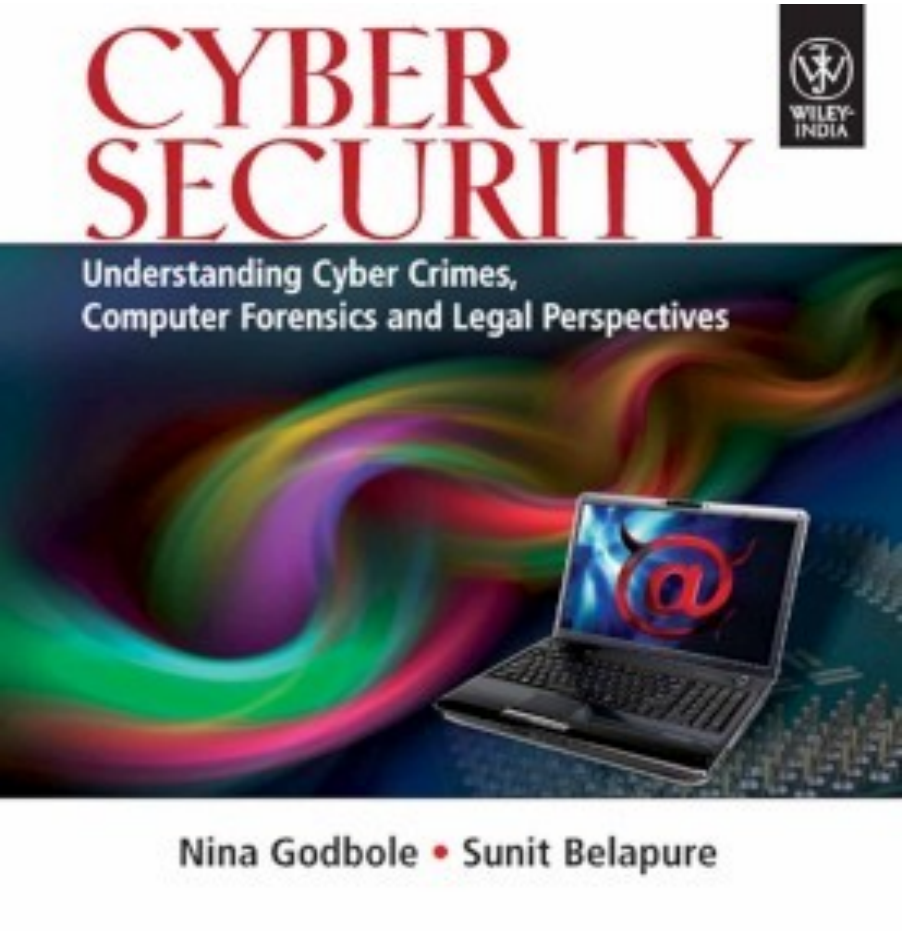
Chapter 7
Understanding Computer Forensics



Cyberforensics

✓ Provides digital evidence of a specific or general activity

✓ Key role in investigation of cybercrime

✓ "Evidence" in the case of "cyberoffenses"

✓ Handling of the digital forensics evidence

✓ Computer is either the subject or the object of cybercrimes or is used as a tool to commit a cybercrime

Computer Forensics (or Digital Forensics)

✓ Digital evidence is required

✓ A fast growing profession as well as business

Computer security and computer forensics are different from each other.

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Digital Forensics Science

- ✓ Application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence.
- ✓ The use of *scientifically derived and proven methods* toward the *preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence* derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Computer Forensics

- ✓ Related to the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is *magnetically stored or encoded*.
- ✓ The *lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information* that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.

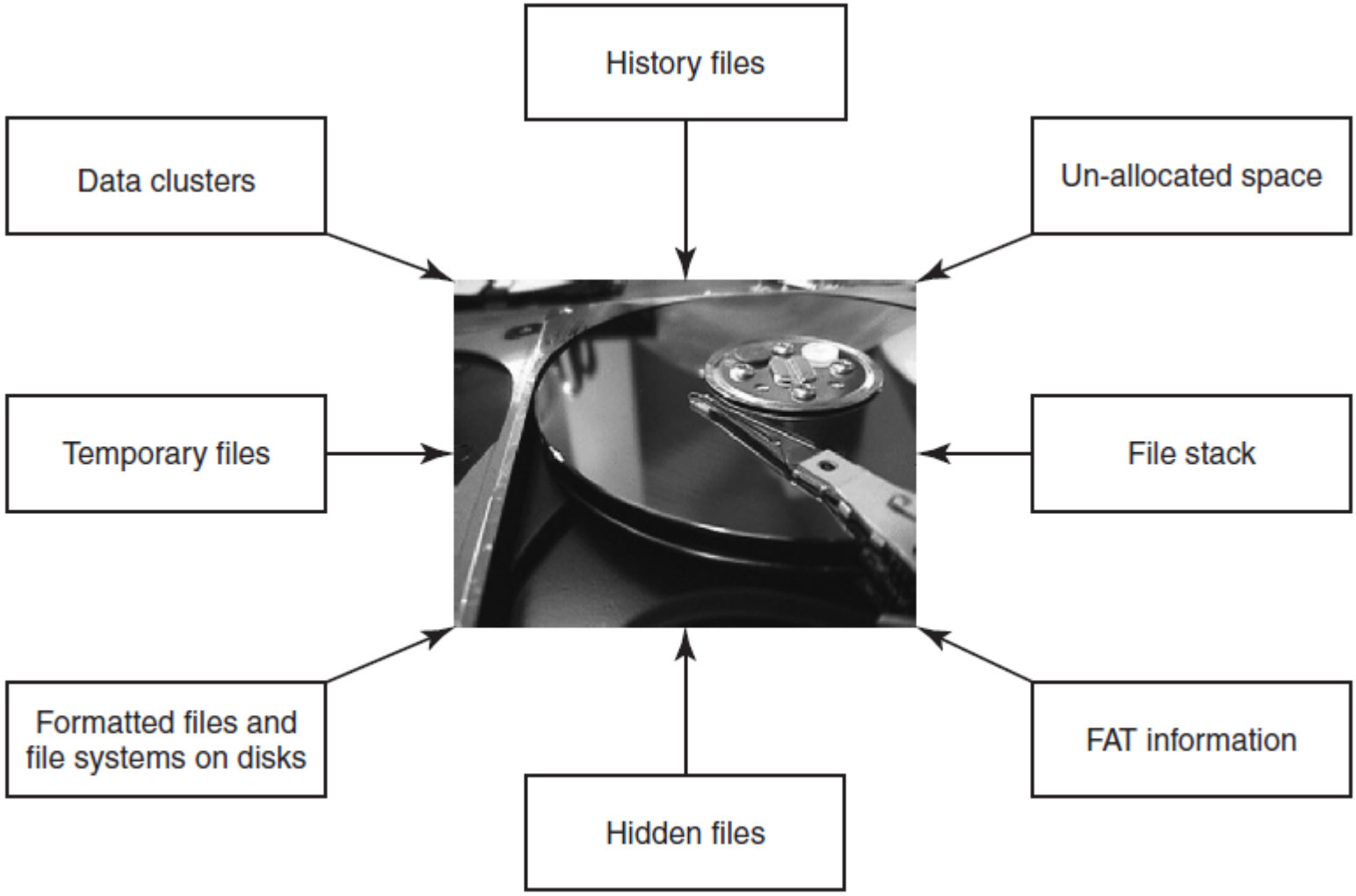


Figure 1 | Data seen using forensics tools. FAT means file allocation table.

Need for Computer Forensics

✓ Convergence of ICT advances and the pervasive use of computers worldwide
✓ High technical capacity of modern computers/computing devices
✓ New risks for computer users

Widespread use of computer forensics is the result of:
✓ Increasing dependence of law enforcement on digital evidence
✓ Ubiquity of computers that followed from the microcomputer revolution

Evidence

✓ Everything that is used to determine or demonstrate the truth of an assertion.
✓ Can be used in court to convict people who are believed to have committed crimes.
✓ Handle carefully.

Cyberforensics and Digital Evidence

1. Computer forensics
2. Network forensics

Computer forensics experts know the techniques to retrieve the data from files listed in standard directory search, hidden files, deleted files, deleted E-Mail and passwords, login IDs, encrypted files, hidden partitions, etc. Typically, the evidences reside on computer systems, user created files, user protected files, computer created files and on computer networks.

The Rules of Evidence

According to the "Indian Evidence Act 1872," "Evidence" means and includes:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
2. All documents that are produced for the inspection of the court are called documentary evidence.

Forensics Analysis of E-Mail

- ✓ It helps establish the authenticity of an E-Mail when suspected.
- ✓ E-Mails -- the most common means of communication.
- ✓ The subject of forensics analysis for "digital evidence."

E-Mail System

The hardware and software that controls the flow of E-Mail.

Components

1. E-Mail server
2. E-Mail gateway

Forensics Analysis of E-Mail

- ✓ It helps establish the authenticity of an E-Mail when suspected.
- ✓ E-Mails -- the most common means of communication.
- ✓ The subject of forensics analysis for "digital evidence."

The path taken by digital evidence can be conceptually depicted as shown in Fig. 2.

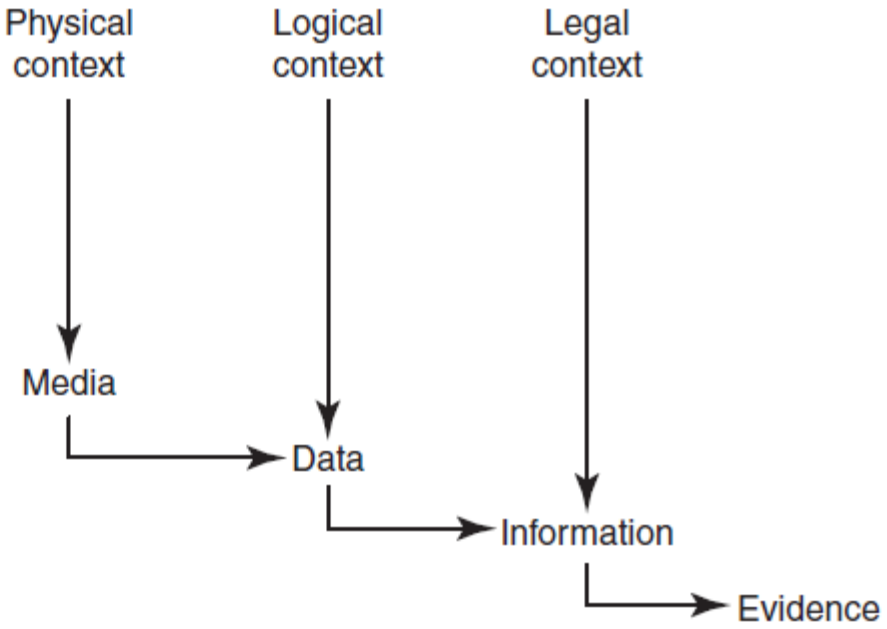


Figure 2 | Path of the digital evidence.

E-Mail System

The hardware and software that controls the flow of E-Mail.

Components

1. E-Mail server
2. E-Mail gateway

RFC2822

- ✓ Internet Message Format
- ✓ Several formats of valid E-Mail addresses: joshi@host.net, john@[10.0.3.19], “Joshi Ganesh” @host.net or “Joshi Ganesh”@[10.0.3.19]
- ✓ Many E-Mail address validators on the Web fail to recognize some of those valid E-Mail addresses
- ✓ RFC2822 standard applies only to the Internet Message Format
- ✓ Some of the semantics of message contents contains no specification of the information in the envelope

Digital Forensics Life Cycle

As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination.

Digital Forensics Process

- ✓ Digital forensics evidence consists of exhibits.
- ✓ The exhibits are introduced as evidence by either side.
- ✓ Testimony is presented to establish the process.
- ✓ The party must show the evidence.
- ✓ Digital forensics evidence can be challenged.
- ✓ Forensics experts formulate a cost proposal.
- ✓ Proposed timeline of activities, lists of anticipated deliverables and a plan for production and turnover of evidence.
- ✓ Submission of a preliminary risk analysis for the forensics service being proposed.

Phases in Computer Forensics/Digital Forensics

1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation and attribution
6. Reporting
7. Testifying

Collecting and Recording Digital Evidence

- ✓ Computers
- ✓ Cell phones
- ✓ Digital cameras
- ✓ Hard drives
- ✓ CD-ROM
- ✓ USB memory devices
- ✓ Digital thermometers
- ✓ Black boxes inside automobiles
- ✓ RFID tags and webpages

Collecting and Recording Digital Evidence

Sources

1. Computers
2. Cell phones
3. Digital cameras
4. Hard drives
5. CD-ROM
6. USB memory devices
7. Digital thermometers
8. Black boxes inside automobiles
9. RFID tags and webpages

Storing and Transporting Digital Evidence

1. Image computer media using a write-blocking tool to ensure that no data is added to the suspect device
2. Establish and maintain the chain of custody
3. Document everything that has been done
4. Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.
5. Care must be taken in transportation to prevent spoliation (in a hot car, digital media tends to lose bits).
6. Care must be taken to preserve chain of custody and assure that a witness can testify accurately about what took place.

Examining/Investigating Digital Evidence

- ✓ Special care must be taken to ensure that the forensics specialist has the legal authority to seize, copy and examine the data.
- ✓ Sometimes authority stems from a search warrant.
- ✓ As a general rule, one should not examine digital information unless one has the legal authority to do so.
- ✓ Amateur forensics examiners should keep this in mind before starting any unauthorized investigation.

Analysis, Interpretation and Attribution

- ✓ Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics analysts.
- ✓ Analysis, interpretation and attribution of digital forensics evidence can be reconciled with non-digital evidence.
- ✓ Digital forensics evidence can be externally stipulated.
- ✓ Open-source tools are available to conduct analysis of open ports, mapped drives on the live computer system.
- ✓ Holding unpowered RAM below −60°C will help preserve the residual data by an order of magnitude, thus improving the chances of successful recovery. However, it is impractical to do this during a field examination.

Reporting

- ✓ A report is generated.
- ✓ The report may be in a written form or an oral testimony (or combination of the two).
- ✓ Evidence, analysis, interpretation and attribution to be presented in the form of expert reports, depositions and testimony.
- ✓ Presentation of the report (a complex and tricky process)

Broad-Level Elements of the Report

1. Identity of the reporting agency
2. Case identifier or submission number
3. Case investigator
4. Identity of the submitter
5. Date of receipt
6. Date of report
7. Serial number, make and model
8. Identity and signature of the examiner
9. Steps taken during examination
10. Results/conclusions

Principles to maintain the integrity of digital evidence

1. ***Principle 1*****:** No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

2. ***Principle 2*****:** In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media that person must be competent to do so and be able to give evidence explaining the relevance and the implications of his/her actions.

3. ***Principle 3*****:** An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

4. ***Principle 4*****:** The person in-charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Chain of Custody Concept

- ✓ It is the central concept in cyberforensics/digital forensics investigation.
- ✓ It is the process of validating how many kinds of evidences have been gathered, tracked and protected on the way to a court of law.
- ✓ It is essential to get in the habit of protecting all evidences equally so that they will hold up in court.
- ✓ The purpose is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.
- ✓ The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition until its final disposition.
- ✓ A chain of custody begins when an item of relevant evidence is collected, and the chain is maintained until the evidence is disposed off.
- ✓ The chain of custody assumes continuous accountability.

Network Forensics

- ✓ This discipline is included within the computer forensics science.
- ✓ The goal is to provide the methodology and tools required to collect and analyze (wireless) network traffic.
- ✓ It involves capturing all data moving over Wi-Fi network and analyzing network events.
- ✓ The security analyst must follow the same general principles that apply to computer forensics.

Typical Elements in a Forensics Investigation Engagement Contract

1. Authorization
2. Confidentiality
3. Payment
4. Consent and acknowledgment
5. Limitation of liability

Steganography

- ✓ Hiding messages in image data (used by criminals and by noncriminals).
- ✓ The threat raised by steganography is very real.
- ✓ Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet.
- ✓ The hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world.
- ✓ *Steganalysis* is of increasing importance to cybersecurity.

Rootkits

- ✓ A "rootkit" is a set of tools used after cracking a computer operating system that hides logins, processes, password, etc., which would carefully hide any trace that those commands normally display.
- ✓ The mechanisms and techniques whereby malware including viruses, Spyware and Trojans attempt to hide their presence from Spyware blockers, antivirus and system management utilities.

- ✓ Rootkits can be classified as – persistent rootkits, memory-based rootkits, user-mode rootkits and kernel-mode rootkits.
- ✓ Rootkits are installed after an attacker has exploited a system vulnerability and gained root access.
- ✓ Rootkits by themselves do not give an attacker root access; they only work after a system compromise. Rootkits consist of tools that generally have three functions: (a) maintain root access to the system, (b) hide the presence of the attacker and (c) attack (or accelerate attacks) against other systems.

- ○ Binary rootkits take administrative utilities and modify them to hide specific connections, processes and activities of specific users.
- ○ Binary rootkits can be defeated through the use of file integrity scanners.
- ○ Binary rootkits can also be detected by system integrity tools.

Information Hiding

1. Three common approaches of hiding information in digital images
2. Least significant bit insertion
3. Masking and filtering
4. Algorithms and transformations

Relevance of the OSI 7 Layer Model to Computer Forensics

The steps taken by attackers who hack networks are:
Step 1: Foot Printing
Step 2: Scanning and Probing
Step 3: Gaining Access
Step 4: Privilege
Step 5: Exploit
Step 6: Retracting
Step 7: Installing Backdoors

Forensics and Social Networking Sites: The Security/Privacy Threats

- ✓ Sites: Orkut, Facebook, MySpace, Bebo, "Bigadda", etc.
- ✓ It enables people to reach out to their old/long lost friends and classmates, relatives, etc.
- ✓ Social networking sites help connect like-minded people, people with the same professions or collaboration and discussion of ideas.
- ✓ Social networking, thus, makes people part of a worldwide community and so the sites are getting popular. The usage of social network sites has increased rapidly in recent years.
- ✓ Kids, teenagers are the ones who are known to be making the maximum use of social networking sites. LinkedIn: Professional networking site
- ✓ Security threats emerging through careless use of social networking sites.

Forensics and Social Networking Sites: The Security/Privacy Threats

- ✓ Sites: Orkut, Facebook, MySpace, Bebo, "Bigadda", etc.
- ✓ It enables people to reach out to their old/long lost friends and classmates, relatives, etc.
- ✓ Social networking sites help connect like-minded people, people with the same professions or collaboration and discussion of ideas.
- ✓ Social networking, thus, makes people part of a worldwide community and so the sites are getting popular. The usage of social network sites has increased rapidly in recent years.
- ✓ Kids, teenagers are the ones who are known to be making the maximum use of social networking sites. LinkedIn: Professional networking site
- ✓ Security threats emerging through careless use of social networking sites.

Security issues that are associated with social networking sites:

1. Corporate espionage.
2. Cross-site scripting.
3. Viruses and worms.
4. Social networking site aggregators.
5. Spear Phishing and social networking specific Phishing.
6. Infiltration of networks leading to data leakage.
7. ID theft

The Regulatory Perspective for Forensics at the International Level

Internationally, there are a few laws and regulations that indicate the need for digital investigations: *Sarbanes Oxley* (the SOX), *California SB 1386*, *Gramm Leach Bliley Act* (the GLBA) and *Health Insurance Portability and Accountability Act* (HIPAA) of 1996.

Features of GLBA

1. Financial Privacy Rule (collection and dissemination of customers' information)

2. Safeguards Rule (governs the processes and controls in an organization to protect customers' financial data)

The Safeguards Rule of GLB calls for financial institutions to:

1. Ensure the security and confidentiality of customer information.

2. Protect against any anticipated threats or hazards to the security or integrity of such information.

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

HIPAA (Health Insurance Portability and Accountability Act of 1996) has the primary goal for healthcare providers to improve the privacy and security of their clients' medical information.

Computer Forensics Expertise Status in India

There is a rise in cybercrimes and in India, computer forensics is a much-needed expertise. At present, there seems to be a shortage of these skills.

Two-fold problem in India

1. Lack of availability of cyberforensics expertise as well as lack of awareness about cyberforensics/digital forensics/computer forensics
2. Involvement of cyberforensics in the day-to-day activities of individuals as well as corporations is going to increase due to the rising rate of cybercrimes in India.

- ➢ The reach of computer forensics must be enterprise-wide and ideally, the response time should be immediate in order to demonstrate that the organizations are utilizing best practices in managing and controlling their information security compliance.
- ➢ Organizations need to have a combination of in-house capability supplemented with external expert services.

- ❑ Cyberlaws of India need to be supported by sound cybersecurity and effective cyberforensics.
- ❑ A good team of techno-legal experts is needed who to help in the drafting of good laws and in its amendments and enforcement.

Challenges in Computer Forensics

➢A microcomputer may have 200 GB or more storage capacity.
➢There are more than 5.2 billion messages expected to be sent and received in the US alone per day.
➢There are more than 3 billion indexed webpages worldwide.
➢There are more than 550 billion documents online.
➢Terabytes of data are stored on tape or hard drives.
➢Most of existing tools and methods allow anyone to alter any attribute associated with digital data.
➢Encryption is a major antiforensics technique and key word search can be defeated by renaming file names.

Technical Challenges: Understanding the Raw Data and its Structure

✓ "Complexity" problem
✓ "Quantity" problem

Non-file system layers of abstraction

1. ASCII
2. HTML Files
3. Windows Registry
4. Network Packets
5. Source Code

Digital forensics is also challenged by the "quantity problem" – it involves the hugeness of digital forensics to analyze. It is inefficient to analyze every single piece of it. Data reduction techniques need to be used to solve this. Data reduction is done by grouping data into one larger event or by removing known data.

The Legal Challenges in Computer Forensics and Data Privacy Issues

- ✓ Evidence, to be admissible in court, must be relevant, material and competent, and its probative value must outweigh any prejudicial effect.
- ✓ Digital evidence can be easily duplicated and modified; often it can be without even leaving any traces; it can present special problems related to competency.
- ✓ Digital evidence needs to satisfy the legal admissibility requirements.
- ✓ Modern computers have enormous data storage facilities. Gigabyte disk drives are common and a single computer may contain several such drives.
- ✓ Seizing and freezing of digital evidence can no longer be accomplished just by burning a single CD-ROM.
- ✓ Failure to freeze the evidence prior to opening the files can invalidate critical evidence.
- ✓ There is also the problem of locating the relevant evidence within massive amounts of data.
- ✓ Artificial limitations imposed by constitutional, statutory and procedural issues.

Various personnel involved in digital forensics/computer forensics:

1. Technicians
2. Policy makers
3. Professionals

Special Tools and Techniques

Most tools have the same underlying principles:

1. Creating forensics quality or sector-by-sector images of media;
2. Locating deleted/old partitions;
3. Ascertaining date/time stamp information;
4. Obtaining data from slack space;
5. Recovering or "undeleting" files and directories, "carving" or recovering data based on file headers/file footers;
6. Performing keyword searches;
7. Recovering Internet history information.

Special Technique: Data Mining used in Cyberforensics

Depending on the type of cybercrimes, the impact and the impacted parties can vary.

Some impact and impacted parties

1. National security and government
2. Financial impacts and individuals
3. Brand image and organizations

Techniques of Data Mining

1. Entity extraction
2. Clustering techniques
3. Association rule mining

- Automated techniques to analyze different types of crimes need a unifying framework describing how to apply them.
- There is a need for understanding the relationship between analysis capability and crime type characteristics. This understanding can help investigators more effectively to use those techniques to identify trends and patterns, address problem areas and even predict crimes.

Forensics Auditing

1. It is also known as “forensics accounting.”
2. It is a specialized form of accounting.
3. It includes the steps needed to detect and deter fraud.
4. Forensics auditors make use of the latest technology to examine financial documents and investigate white-collar crimes.
5. Uses accounting, auditing and investigative techniques.
6. Forensics accounting professionals are assigned specialty tasks.
7. Forensics auditors are responsible for detecting fraud, identifying individuals involved, collecting evidence, presenting the evidence in criminal proceedings, etc.

Antiforensics

It is the application of scientific method to digital media to invalidate factual information for judicial review. Moreover, it is a combination of people, process and tools.

Four categories of antiforensics

1. Data destruction
2. Data hiding
3. Data encryption
4. Data contraception

Some well-known tools with "counter-forensics features"

1. Windows Washer
2. Windows and Internet Cleaner
3. CyberScrub Pro
4. Evidence Eliminator
5. Acronis Privacy Expert
6. SecureClean

Metasploit antiforensics investigation arsenal includes following tools

1. Timestomp
2. Slacker
3. Transmogrify
4. Sam Juicer