Dr. D. Y. Patil Pratishthan's

Institute for Advanced Computing &Software Development

IACSD

CYBER FORENSICS

INDEX

Chapter 1: Introduction 1

Chapter 2: Evidence Collection And Data Seizure 26

Chapter 3: Computer Forensics Analysis And Validation 58

Chapter 4: Computer Forensic Tools..... 90

Chapter 5: Windows and DOS Systems 115

UNIT-1

INTRODUCTION

1.1 WHAT IS COMPUTER FORENSICS?

- Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.
- Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.
- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.

1.2 USE OF COMPUTER FORENSICS IN LAW ENFORCEMENT

Computer forensics assists in Law Enforcement. This can include:

- Recovering deleted files such as documents, graphics, and photos.
- Searching unallocated space on the hard drive, places where an abundance of data often resides.
- Tracing artifacts, those tidbits of data left behind by the operating system. Our experts know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find.
- Processing hidden files — files that are not visible or accessible to the user — that contain past usage information. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was

created, last modified, last accessed and when deleted.

- Running a string-search for e-mail, when no e-mail client is obvious.

1.3 COMPUTER FORENSICS ASSISTANCE TO HUMAN RESOURCES / EMPLOYMENT PROCEEDINGS

Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, and wrongful termination claims. Evidence can be found in electronic mail systems, on network servers, and on individual employee's computers.

EMPLOYER SAFEGUARD PROGRAM

Employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual. Before an individual is informed of their termination, a computer forensic specialist should come on-site and create an exact duplicate of the data on the individual's computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected. Damaged or deleted data can be re-placed, and evidence can be recovered to show what occurred. This method can also be used to bolster an employer's case by showing the removal of proprietary information or to protect the employer from false charges made by the employee. You should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy the evidence. For example, did you know?

- ✓ What Web sites have been visited?

- ✓ What files have been downloaded?
- ✓ When files were last accessed?
- ✓ Of attempts to conceal or destroy evidence?
- ✓ Of attempts to fabricate evidence?
- ✓ That the electronic copy of a document can contain text that was removed from the final printed version?
- ✓ That some fax machines can contain exact duplicates of the last several hundred pages received?
- ✓ That faxes sent or received via computer may remain on the computer indefinitely?
- ✓ That email is rapidly becoming the communications medium of choice for businesses?
- ✓ That people tend to write things in email that they would never consider writing in a memorandum or letter?
- ✓ That email has been used successfully in criminal cases as well as in civil litigation?
- ✓ That email is often backed up on tapes that are generally kept for months or years?
- ✓ That many people keep their financial records, including investments, on computers?

1.4 COMPUTER FORENSICS SERVICES

Computer forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case.

For example, they should be able to perform the following services:

1. DATA SEIZURE

- ✓ Following federal guidelines, computer forensics experts should act as the representative, using their knowledge of data storage technologies to track down evidence.
- ✓ The experts should also be able to assist officials during the equipment seizure process.

2. DATA DUPLICATION/PRESERVATION

- ✓ When one party must seize data from another, two concerns must be addressed:
  - the data must not be altered in any way
  - the seizure must not put an undue burden on the responding party
- ✓ The computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data.
- ✓ When experts works on the duplicate data, the integrity of the original is maintained.

3. DATA RECOVERY

- ✓ Using proprietary tools, your computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence.
- ✓ The ability to recover lost evidence is made possible by the expert's advanced understanding of storage technologies.

4. DOCUMENT SEARCHES

- ✓ Computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours.
- ✓ The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

5. MEDIA CONVERSION

- ✓ Computer forensics experts should extract the relevant data from old and un-readable devices, convert it into readable formats, and place it onto new storage media for analysis.

6. EXPERT WITNESS SERVICES

- ✓ Computer forensics experts should be able to explain complex technical processes in an easy-to- understand fashion.
- ✓ This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

7. COMPUTER EVIDENCE SERVICE OPTIONS

Computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:

- ✓ **Standard service**: Computer forensics experts should be able to work on your case during nor-mal business hours until your critical electronic evidence is found.
- ✓ **On-site service**: Computer forensics experts should be able to travel to your location to per-form complete computer evidence services. While on-site, the experts should quickly be able to produce exact duplicates of the data storage media in question.
- ✓ **Emergency service**: Your computer forensics experts should be able to give your case the highest priority in their laboratories. They should be able to work on it without interruption until your evidence objectives are met.
- ✓ **Priority service**: Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found. Priority service typically cuts your turnaround time in half.
- ✓ **Weekend service**: Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue 14 Computer Forensics, Second Edition working

on your case until your evidence objectives are met.

8. OTHER MISCELLANEOUS SERVICES

Computer forensics experts should also be able to provide extended services. These services include:

- ✓ Analysis of computers and data in criminal investigations
- ✓ On-site seizure of computer data in criminal investigations
- ✓ Analysis of computers and data in civil litigation.
- ✓ On-site seizure of computer data in civil litigation
- ✓ Analysis of company computers to determine employee activity
- ✓ Assistance in preparing electronic discovery requests
- ✓ Reporting in a comprehensive and readily understandable manner
- ✓ Court-recognized computer expert witness testimony
- ✓ Computer forensics on both PC and Mac platforms
- ✓ Fast turnaround time.

1.5 BENEFITS OF PROFESSIONAL FORENSIC METHODOLOGY

A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that:

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
2. No possible computer virus is introduced to a subject computer during the analysis process.
3. Extracted and possibly relevant evidence is properly handled and protected

from later mechanical or electromagnetic damage.

4. A continuing chain of custody is established and maintained.
5. Business operations are affected for a limited amount of time, if at all.
6. Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

1.6 STEPS TAKEN BY COMPUTER FORENSICS SPECIALISTS

The computer forensics specialist should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system. For example, the following steps should be taken:

1. **Protect** the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. **Discover** all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. **Recover** all of discovered deleted files.
4. **Reveal** the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
5. **Access** the contents of protected or encrypted files.
6. **Analyze** all possibly relevant data found in special areas of a disk. This includes but is not limited to what is called unallocated space on a disk, as well as slack space in a file (the remnant area at the end of a file in the last assigned disk cluster, that is unused by current file data, but once again, may be a possible site for previously created and relevant evidence).
7. **Print out** an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.

8. **Provide** an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.
9. **Provide** expert consultation and/or testimony, as required.

TYPES OF COMPUTER FORENSIC TECHNOLOGY

1.7 TYPES OF MILITARY COMPUTER FORENSIC TECHNOLOGY

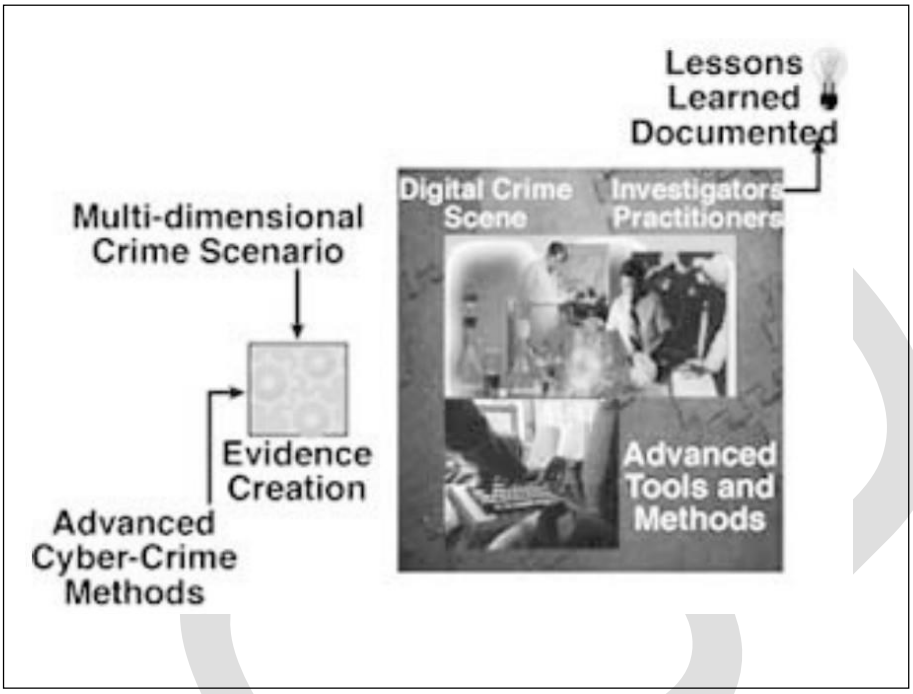
- Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and assessment of the intent and identity of the perpetrator.
- Real-time tracking of potentially malicious activity is especially difficult when the pertinent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

COMPUTER FORENSIC EXPERIMENT-2000 (CFX-2000)

- ✓CFX-2000 is an integrated forensic analysis framework.

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

continue vigorous R&D of cyber forensic technology in preparation for the onslaught of cyber reconnaissance probes and attacks.



1.8 TYPES OF LAW ENFORCEMENT COMPUTER FORENSIC TECHNOLOGY

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

Computer Evidence Processing Procedures

Processing procedures and methodologies should conform to federal computer evidence processing standards.

1. Preservation of Evidence

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

TROJAN HORSE PROGRAMS

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

COMPUTER FORENSICS DOCUMENTATION

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

FILE SLACK

- ✓ Slack space in a file is the remnant area at the end of a file in the last assigned disk cluster, that is unused by current file data, but once again, may be a possible site for previously created and relevant evidence.
- ✓ Techniques and automated tools that are used by the experts to capture and evaluate file slack.

DATA-HIDING TECHNIQUES

- ✓ Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions. Computer forensic experts should understand such issues and tools that help in the identification of such anomalies.

E-C OOMMERCE INVESTIGATIONS

- **Net Threat Analyzer** can be used to identify past Internet browsing and email activity done through specific computers. The software analyzes a computer's disk drives and other storage areas that are generally unknown to or beyond the reach of most general computer users. Net Threat Analyzer avail-able free of charge to computer crime specialists, school officials, and police.

DUAL-PURPOSE PROGRAMS

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

these programs.

TEXT SEARCH TECHNIQUES

- Tools that can be used to find targeted strings of text in files, file slack, unallocated file space, and Windows swap files.

FUZZY LOGIC TOOLS USED TO IDENTIFY UNKNOWN TEXT

- Computer evidence searches require that the computer specialist know what is being searched for. Many times not all is known about what may be stored on a given computer system.
- In such cases, fuzzy logic tools can provide valuable leads as to how the subject computer was used.

2. Disk Structure

- Computer forensic experts must understand how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk.
- They should also demonstrate their knowledge of how to modify the structure and hide data in obscure places on floppy diskettes and hard disk drives.

3. Data Encryption

- Computer forensic experts should become familiar with the use of software to crack security associated with the different file structures.

4. Matching a Diskette to a Computer

- 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. Computer forensic experts should become familiar how to use special software tools to complete this process.

5. Data Compression

- Computer forensic experts should become familiar with how compression works and how compression programs can be used to hide and disguise sensitive data and also learn how password- protected compressed files can be broken.

6. Erased Files

- Computer forensic experts should become familiar with how previously erased files can be recovered by using DOS programs and by manually using data-recovery technique & familiar with cluster chaining.

7. Internet Abuse Identification and Detection

- Computer forensic experts should become familiar with 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).

8. The Boot Process and Memory Resident Programs

- Computer forensic experts should become familiar with 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 experts understand these potential risks and how to identify them.

1.9 TYPES OF BUSINESS COMPUTER FORENSIC TECHNOLOGY

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

REMOTE MONITORING OF TARGET COMPUTERS

- ✓ *Data Interception by Remote Transmission* (*DIRT*) is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center.
- ✓ No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

CREATING TRACKABLE ELECTRONIC DOCUMENTS

- ✓ *Binary Audit Identification Transfer* (*BAIT*) is a powerful intrusion detection tool that allows users to create *trackable* electronic documents.
- ✓ BAIT identifies (including their location) unauthorized intruders who access, download, and view these tagged documents.
- ✓ BAIT also allows security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.

THEFT RECOVERY SOFTWARE FOR LAPTOPS AND PCS

- ✓ **What it really costs to replace a stolen computer:**

  - The price of the replacement hardware & software.
  - The cost of recreating data, lost production time or instruction time, reporting and investigating the theft, filing police reports and insurance claims, increased insurance, processing and ordering replacements, cutting a check, and the like.
  - The loss of customer goodwill.
  - If a thief is ever caught, the cost of time involved in prosecution.
  -

- ✓ **PC PHONEHOME**

  - PC PhoneHome is a software application that will track and locate a lost or stolen PC or laptop any-where in the world. It is easy to install. It is also completely transparent to the user.
  - If your *PC PhoneHome*-protected computer is lost or stolen, all you need to do is make a report to the local police and call CD's 24-hour command center. CD's recovery specialists will assist local law enforcement in the recovery of your property.

FORENSIC SERVICES AVAILABLE

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.

COMPUTER FORENSIC EVIDENCE & CAPTURE

1.10 Data Recovery Defined

- Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format.
- Many people, even computer experts, fail to recognize data recovery as an option during a data crisis. But it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

1.11 Data Back-up and Recovery

Back-up Obstacles

- **Back-up Window**: The back-up window is the period of time when

back-ups can be run. The back-up window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low.

- **Network bandwidth**: If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization's centralized backup strategy is not viable.
- **System throughput**: Three I/O bottlenecks are commonly found in traditional backup schemes. These are
  - The ability of the system being backed up to push data to the backup server
  - The ability of the backup server to accept data from multiple systems simultaneously
  - The available throughput of the tape device(s) onto which the data is moved
- **Lack-of Resources**: Many companies fail to make appropriate investments in data protection until it is too late.

1.12 The Role of Back-up in Data Recovery

There are many factors that affect back-up. For example:

- **Storage costs are decreasing**: The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance.
- **Systems have to be on-line continuously**: Because systems must be

continuously online, the dilemma becomes that you can no longer take files offline long enough to perform backup.

- **The role of Back-up has changed**: The role of backup now includes the responsibility for recovering user errors and ensuring that good data has been saved and can quickly be restored.

CONVENTIONAL TAPE BACK-UP IN TODAY'S MARKET

- ✓ A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the back-end controlling a repository of tape devices. The media server runs tape management software. It can administer backup devices throughout an enterprise and can run continuous parallel backups and restores.
- ✓ An alternative to tape backup is to physically replicate or mirror all data and keep two copies online at all times. The advantage is that the data does not have to be restored, so there are no issues with immediate data availability.

ISSUES WITH TODAY'S BACK-UP

- ✓ **NETWORK BACKUP** creates network performance problems. Using the production network to carry backup data, as well as for normal user data access, can severely overburden today's busy network resources.

- ✓ **OFFLINE BACKUP** affects data accessibility. The time that the host is offline for data backup must be minimized. This requires extremely high- speed, continuous parallel backup of the raw image of the data.
- ✓ **LIVE BACKUPS** allow data access during the backup process but affect performance. The downside to the live backup is that it puts a tremendous burden on the host.
- ✓ **MIRRORING** doesn't protect against user error and replication of bad data. Fully replicated online data sounds great, albeit at twice the cost per megabyte of a single copy of online data.

NEW ARCHITECTURES AND TECHNIQUES ARE REQUIRED

- ✓ Backup at extremely high speed is required. Recovery must be available at file level. The time that systems off-line for back-up must be eliminated.
- ✓ Remote hot recovery sites are needed for immediate resumption of data access. Backup of critical data is still required to ensure against data errors and user errors.
- ✓ To achieve effective backup and recovery, the decoupling of data from its storage space is needed.
- ✓ It is necessary to develop techniques to journal modified pages, so that journaling can be invoked within the primary storage device, without host intervention.
- ✓ Part of the primary storage area must be set aside for data to be backed up. This area must be as large as the largest backup block. We should have fast nonrandom restoration of critical data.

The Data Recovery Solution

SHRINKING EXPERTISE, GROWING COMPLEXITY

a. The complex systems that have evolved over the past 30 years must be monitored, managed, controlled, and optimized. But most of the bright young graduates this term haven't had much exposure to mainframe concepts.

b. Backups often take place while an application is running. Application changes take place on the fly. If an outage occurs, the company stands to lose tens of thousands of dollars an hour.

FAILURES:

Disk storage is more reliable than ever, but hardware failures are still possible. A simple mistake can be made by an application programmer, system programmer, or operations person. Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse. Disasters do really occurs! Floods, tornadoes, earthquakes, tsunamis, and even terrorism can do strike. We must be ready.

BUDGETS AND DOWNTIME

We have fewer resources (people, processing power, time, and money) to do more work than ever before, and we must keep your expenses under control. Systems must remain available to make money and serve customers. Downtime is much too expensive to be tolerated.

RECOVERY: THINK BEFORE YOU BACK-UP

One of the most critical data-management tasks involves recovering data in the event of a problem. You must evaluate your preparations, make sure that all resources are available in usable condition, automate processes as much as possible, and make sure you have the right kind of resources.

Evaluate your preparation

If all of the resources (image copies, change accumulations, and logs) are available at recovery time, these preparations certainly allow for a standard recovery. Finding out at recovery time that some critical resource is missing can be disastrous!

Don't let your resources fall through the cracks

Identifying different types of conditions is critical to ensuring a successful recovery. Checking your assets to make sure they're ready should be part of your plan.

Automated Recovery

With proper planning and automation, recovery is made possible, reliance on specific personnel is reduced, and the human-error factor is nearly eliminated.

Data integrity and your business relay on building recovery job control language (JCL). In the event of a disaster, the Information Management System (IMS) recovery control (RECON) data sets must be modified in preparation for the recovery.

Cleaning your RECON data sets can take hours if done manually, and it's an error-prone process.

Make Recoveries Efficient

Multithreading tasks shorten the recovery process. Recovering multiple databases with one pass through your log data certainly will save time. Taking image copies, rebuilding indexes, and validating pointers concurrently with the recovery process further reduce downtime.

Take Back-ups

The first step to a successful recovery is the backup of your data. Your goal in backing up data is to do so quickly, efficiently, and usually with minimal impact to your customers. You might need only very brief out-ages to take instant copies of your data, or you might have intelligent storage devices that allow you to take a snapshot of your data. Both methods call for tools to assist in the management of resources.

BACK-UP AND RECOVERY SOLUTION

BMC software has developed a model called the *Back-up and Recovery Solution* (BRS) for the Information Management System (IMS) product.

Image Copy

BRS contains an Image Copy component to help manage your image copy process. BRS can take batch, on-line (fuzzy), or incremental image copies; Snapshot copies; or Instant Snapshot copies.

The Image Copy component of BRS offers a variety of powerful features: dynamic allocation of all input and output data sets, stacking of output data sets, high performance access methods (faster I/O), copying by volume, compression of output

image copies, and database group processing--- all while interfacing with DBRC and processing asynchronously.

Change Accumulation

The BRS *Change Accumulation* component takes advantage of multiple engines, large virtual storage resources, and high-speed channels and controllers that are available in many environments.

Use of multiple tack control block (TCB) structures enables overlapping of as much processing as possible, reducing both elapsed and CPU time.

Recovery

- The BRS *Recovery* component, which functionally replaces the IMS *Database Recovery* utility for null- function (DL/I) databases and data-entry databases (DEDBs), allow recovery of multiple databases with one pass of the log and change accumulation data sets while dynamically allocating all data sets required for recovery.
- BRS recovers multiple databases to any point in time. BRS can determine the best choice for a Point-in- Time (PIT) recovery. Full DBRS support includes:

RECOVERY MANAGER

- *Recovery Manager* component lets you automate and synchronize recoveries across applications and databases by creating meaningful groups of related databases and creating optimized JCL to perform the recovery of these groups.
- *Recovery Manager* component provides a positive response for the IMS commands that are used to deallocate and start your databases.

- *Recovery Manager* component fully automates the process of cleaning the RECON data sets for restart following a disaster recovery.
- *Recovery Manager* component also allows you to test your recovery strategy and notifies you when media errors have jeopardized your recovery resources.

POINTER CHECKING

BRS offers the capability to verify the validity of database pointers through the *Concurrent Pointer Checking* function for both full-function databases and Fast Path data-entry databases (DEDBs).

INDEX REBUILD

If indexes are ever damaged or lost, the *Index Rebuild* function of BRS allows you rebuild them rather than recover them.

RECOVERY ADVISOR

The *Recovery Advisor* component of BRS allows you to monitor the frequency of your image copies and change accumulations.

It helps you to determine whether all your databases are being backed-up. By using any number of back-up and recovery tools available, you can better manage your world and be ready to recover!

Unit-II

EVIDENCE COLLECTION AND DATA SEIZURE

2.1 Why Collect Evidence?

The simple reasons for collecting evidence are:

- **Future Prevention**: Without knowing what happened, you have no hope of ever being able to stop someone else from doing it again.

- **Responsibility**: The attacker is responsible for the damage done, and the only way to bring him to justice is with adequate evidence to prove his actions. The victim has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks.

2.2 Collection Options

Once a compromise has been detected, you have two options:

- **Pull the system off the network and begin collecting evidence**: In this case you may find that you have insufficient evidence or, worse, that the attacker left a dead man switch that destroys any evidence once the system detects that its offline.

- **Leave it online and attempt to monitor the intruder**: you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes.

2.3 Obstacles

- Computer transactions are fast, they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible.

- Any paper trail of computer records they may leave can be easily modified or destroyed, or may be only temporary.
- Auditing programs may automatically destroy the records left when computer transactions are finished with them.
- Investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously.
- The best we can do is to follow the rules of evidence collection and be as assiduous as possible.

2.4 Types of Evidence

- **Real Evidence:** Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function— provided that the log can be shown to be free from contamination.
- **Testimonial Evidence:** Testimonial evidence is any evidence supplied by a witness. As long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.
- **Hearsay:** Hearsay is any evidence presented by a person who was not a direct witness. Hearsay is generally inadmissible in court and should be avoided.

2.5 The Rules of Evidence

1. **Admissible**: Admissible is the most basic rule. The evidence must be able to be used in court.
2. **Authentic**: You must be able to show that the evidence relates to the incident

in a relevant way.

3. **Complete**: It's not enough to collect evidence that just shows one perspective of the incident.
4. **Reliable**: Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.
5. **Believable**: The evidence you present should be clearly understandable and believable to a jury.

Using the preceding five rules, we can derive some basic do's and don'ts:

- **Minimize handling and corruption of original data:** Once you've created a master copy of the original data, don't touch it or the original. Any changes made to the originals will affect the outcomes of any analysis later done to copies.
- **Account for any changes and keep detailed logs of your actions:** Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented.
- **Comply with the five rules of evidence:** Following these rules is essential to guaranteeing successful evidence collection.
- **Do not exceed your knowledge**: If you ever find yourself "out of your depth," either go and learn more before continuing (if time is available) or find someone who knows the territory.
- **Follow your local security policy:** If you fail to comply with your company's security policy, you may find yourself with some difficulties.
- **Capture as accurate an image of the system as possible:** Capturing an accurate image of the system is related to minimizing the handling or corruption of original data.

- Be prepared to testify: If you're not willing to testify to the evidence you have collected, you might as well stop before you start. No one is going to believe you if they can't replicate your actions and reach the same results.
- **Work fast:** The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don't collect it in time. If multiple systems are involved, work parallel.
- **Proceed from volatile to persistent evidence:** Always try to collect the most volatile evidence first.
- **Don't shutdown before collecting evidence**: You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.
- **Don't run any programs on the affected system:** The attacker may have left trojaned programs and libraries on the system; you may inadvertently trigger something that could change or destroy the evidence you're looking for.

2.6 Volatile Evidence

Always try to collect the most volatile evidence first. An example an order of volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table

5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology

2.7 General Procedure

- ✓ **Identification of Evidence**: You must be able to distinguish between evidence and junk data
- ✓ **Preservation of Evidence**: The evidence you find must be preserved as close as possible to its original state.
- ✓ **Analysis of Evidence**: Analysis requires in-depth knowledge of what you are looking for and how to get it.
- ✓ **Presentation of Evidence**: The manner of presentation is important, and it must be understandable by a layman to be effective.

2.8 Collection and Archiving

Once we've developed a plan of attack and identified the evidence that needs to be collected.

Logs and Logging: You should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Messages and logs from programs can be used to show what damage an attacker did.

Monitoring: By monitoring we can gather statistics, watch out for irregular, and trace where an attacker is coming from and what he is doing. Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection. You should display a disclaimer stating what monitoring is done when users log on.

2.9 Methods of Collection

There are two basic forms of collection: freezing the scene and honeypotting.

Freezing the Scene

- ✓ It involves taking a snapshot of the system in its compromised state. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format.
- ✓ All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

Honeypotting

- ✓ It is the process of creating a replica system and luring the attacker into it for further monitoring.
- ✓ The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

2.10 Artifacts

- ➢ There is almost always something left behind by the attacker be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as artifacts.
- ➢ Never attempt to analyze an artifact on the compromised system.

- Artifacts are capable of anything, and we want to make sure their effects are controlled.

2.11 Collection Steps

1. **Find the Evidence:** Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.
2. **Find the Relevant Data:** Once you've found the evidence, you must figure out what part of it is relevant to the case.
3. **Create an Order of Volatility:** The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.
4. **Remove external avenues of change:** It is essential that you avoid alterations to the original data.
5. **Collect the Evidence:** Collect the evidence using the appropriate tools for the job.
6. **Document everything:** Collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important.

2.12 Controlling Contamination: The Chain of Custody

Once the data has been collected, it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used.

A good way of ensuring that data remains uncorrupted is to keep a chain of custody. This is a detailed list of what was done with the original copies once they were collected.

Analysis

- Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened.

Time

- To reconstruct the events that led to your system being corrupted, you must be able to create a timeline.
- Never, ever change the clock on an affected system.

Forensic Analysis of Back-ups

- When we analyze back-ups, it is best to have a dedicated host for the job. We need a dedicated host which is secure, clean and isolated from any network for analyzing back- ups.
- Document everything you do. Ensure that what you do is repeatable and capable of always giving the same results.

Reconstructing the Attack

After collecting the data, we can attempt to reconstruct the chain of events leading to and following the attacker's break-in. We must correlate all the evidence we have gathered. Include all of the evidence we've found when reconstructing the attack---no matter how small it is.

Searching and Seizing

There is no one methodology for performing a computer forensic investigation and analysis.

There are too many variables for to be just one way. Some of the typical variable that comes to the mind includes operating systems; software applications; cryptographic algorithms and applications; and hardware platforms. But moving beyond these obvious variables spring other equally challenging variables: law, international boundaries, publicity, and methodology.

There are a few widely accepted guidelines for computer forensic analysis:

- ✓ A computer forensic examiner is impartial. Our job is to analyze the media and report our findings with no presumption of guilt or innocence.
- ✓ The media used in computer forensic examinations must be sterilized before each use.
- ✓ A true image (bit stream) of the original media must be made and used for the analysis.
- ✓ The integrity of the original media must be maintained throughout the entire investigation.

Before the Investigation

 For the sake of first argument, you must have skilled technicians in-house and a

top notch lab the right equipment, the right computer forensic tools, and so on.

- District attorneys may require more documentation on the chain of evidence handling.
- When you have a case arise, you know what is required and can work the case from the inception in support of these requirements.

Methodology Development

- Define your methodology, and working according to this methodology.
- Here methodology defines a method, a set of rules: guidelines that are employed by a discipline.

Document Everything

The chain of evidence is so important in computer forensic investigations. If resources allow, have two computer forensic personnel assigned to each case every step of the way. Important in the documentation are the times that dates steps were taken; the names of those involved; and under whose authority were the steps taken?

Evidence Search and Seizure

Prior to search and seizure, you already have the proper documents filled as well as permission from the authority to search and seize the suspect's machine.

Step 1: Preparation

You should check all media that is to be used in the examination process. Document the wiping and scanning process. Check to make sure that all

computer forensic tools are licensed for use and all lab equipment is in working order.

Step 2: Snapshot

We should photograph the scene, whether it is a room in a home or in a business. You should also note the scene. Take advantage of your investigative skills here. Note pictures, personal items, and the like. Photograph the actual Evidence. For example, the evidence is a PC in a home office. Take a photograph of the monitor. Remove the case cover carefully and photograph the internals.

Step 3: Transport

If you have the legal authority to transport the evidence to your lab, you should pack the evidence securely. Photograph/videotape and document the handling of evidence leaving the scene to the transport vehicle and from transport vehicle to the lab examination facility.

Step 4: Examination

You should prepare the acquired evidence for examination in your lab. There are many options to on what tool to use image the drive. You could use *EnCase,* the Unix command DD, *ByetBack*, or also *SafeBack*. It is wise to have a variety of tools in your lab. Each of these tools has its respective strengths. The important note to remember here is: Turn off virus-scanning software. We must record the time and date of the COMS. Do not boot the suspect machine.

When making the image, make sure that the tool you use does not access the file system of the target evidence media. After making the image, seal the original media in an electrostatic-safe container, catalog it, and initial the container.

Finally, the examination of the acquired image begins.

DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE

2.13 Preserving the Digital Crime Scene

- ✓ After securing the computer, we should make a complete bit stream backup of all computer data before it is reviewed or processed.
- ✓ Bit stream backups are much more thorough than standard backups.
- ✓ They involve copying of every bit of data on a storage device, and it is recommended that two such copies be made of the original when hard disk drives are involved.
- ✓ Any processing should be performed on one of the backup copies.
- ✓ **IMDUMP** was the first software for taking bit stream back-ups developed by Michael White.

SafeBack

- ➢ **SafeBack** has become a law enforcement standard and is used by numerous government intelligence agencies, military agencies, and law enforcement agencies worldwide.
- ➢ SafeBack program copies and preserves all data contained on the hard disk.
- ➢ Even it goes so far as to circumvent attempts made to hide data in bad clusters and even sectors with invalid CRCs.

SnapBack

- Another bit steam back-up program, called **SnapBack**, is also available and is used by some law enforcement agencies primarily because of its ease of use.
- Its prices several hundreds of dollars higher than SafeBack.
- It has error-checking built into every phase of the evidence back-up and restoration process.
- The hard disk drive should be imaged using specialized bit stream back-up software.
- The floppy diskettes can be imaged using the standard DOS DISKCOPY program.
- When DOS DISKCOPY is used, it is recommended that the **MS DOS Version 6.22** be used and (data verification) switch should be invoked from the command line.
- Know and practice using all of your forensic software tools before you use them in the processing of computer evidence.
- We may only get one chance to do it right.

2.14 Computer Evidence Processing Steps

There really are no strict rules that must be followed regarding the processing of computer evidence.

The following are general computer evidence processing steps:

1. Shut down the computer.

Depending on the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved. Generally, time is of the essence, and the computer system should be shut down as quickly as possible.

2. Document the hardware configuration of the system.

Be-fore dismantling the computer, it is important that pictures are taken of the computer from all angles to document the system hardware components and how they are connected. Labeling each wire is also important, so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

3. Transport the computer system to a secure location.

A seized computer left unattended can easily be compromised. Don't leave the computer unattended unless it is locked up in a secure location.

4. Make bit stream backups of hard disks and floppy disks.

All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. Bit stream backups are much like an insurance policy and are essential for any serious computer evidence processing.

***5.* Mathematically authenticate data on all storage devices.**

You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Since 1989, law enforcement and military agencies have used a 32- bit mathematical process to do the authentication process.

6. Document the system date and time.

If the system clock is one hour slow because of daylight-savings time, then file timestamps will also reflect the wrong time. To adjust for these inaccuracies, documenting the system date and time settings at the time the computer is taken into evidence is essential.

7. Make a list of key search words.

it is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive. Gathering information from individuals familiar with the case to help com-pile a list of relevant keywords is important. Such keywords can be used in the search of all computer hard disk drives and floppy diskettes using automated soft-ware.

8. Evaluate the Windows swap file.

The Windows swap file is a potentially valuable source of evidence and leads. When the computer is turned off, the swap file is erased. But the content of the swap file can easily be captured and evaluated.

9. Evaluate file slack.

It is a source of significant security leakage and consists of raw memory dumps that occur during the work session as files are closed. File slack should be evaluated for relevant keywords to supplement the keywords identified in the previous steps. File slack is typically a good source of Internet leads. Tests suggest that file slack provides approximately 80 times more Internet leads than the Windows swap file.

10.Evaluate unallocated space (erased files).

Unallocated space should be evaluated for relevant keywords to supplement the keywords identified in the previous steps.

11.Search files, file slack, and unallocated space for keywords.

The list of relevant keywords identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes. It is important to review the output of the text search utility and equally important to document relevant findings.

12.Document file names, dates, and times.

From an evidence standpoint, file names, creation dates, and last modified dates and times can be relevant. The output should be in the form of a word-processing-compatible file that can be used to help document computer evidence issues tied to specific files.

13.Identify file, program, and storage anomalies.

Encrypted, compressed, and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program. Manual evaluation of these files is required. Depending on the type of file involved, the contents should be viewed and evaluated for its potential as evidence.

14.Evaluate program functionality.

Depending on the application software involved, running programs to learn their purpose may be necessary. When destructive processes that are tied to relevant evidence are discovered, this can be used to prove willfulness.

15.Document your findings.

It is important to document your findings as is-sues are identified and as evidence is found. Documenting all of the software used in your forensic evaluation of the evidence, including the version numbers of the programs used, is also important. Be sure you are legally licensed to USE the forensic software.

Screen prints of the operating software also help document the version of the software and how it was used to find or process the evidence.

16.Retain copies of software used.

As part of your documentation process, it is recommended that a copy of the software used be included with the output of the forensic tool involved. Duplication of results can be difficult or impossible to achieve if the soft-ware has been upgraded and the original version used was not retained.

2.15 Legal Aspects of Collecting and Preserving Computer Forensic Evidence

Definition

- A chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court.
- Preserving a chain of custody for electronic evidence requires proving that:
  - ✓ No information has been added or changed.
  - ✓ A complete copy was made.
  - ✓ A reliable copying process was used.
  - ✓ All media was secured.

Legal Requirements

- When evidence is collected, certain legal requirements must be met. These legal requirements are vast, complex, and vary from country to country.
- CERT Advisory CA-1992-19 suggests the following text be tailored to a

corporation's specific needs under the guidance of legal counsel:

- ✓ This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
- ✓ In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
- ✓ Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

- The legality of workplace monitoring depends primarily on whether employment policies exist that authorize monitoring and whether that policy has been clearly communicated to employees.
- To prove that the policy has been communicated, employees should sign a statement indicating that they have read, understood, and agreed to comply with corporate policy and consent to sys-tem monitoring.

Evidence Collection Procedure

When the time arrives to begin collecting evidence, the first rule that must be followed is

Do not rush.

- The investigation team will need a copy of their incident-handling

procedure, an evidence collection notebook, and evidence identification tags.

- They may also need to bring tools to produce reliable copies of electronic evidence, including media to use in the copying process.
- In some cases, legal counsel will want photographs of the system prior to search and seizure. Then include a *Polaroid camera* in the list of tools.

The Incident Coordinator

Policy and procedure should indicate who is to act as incident coordinator.

The Incident coordinator

- ✓ will contact the other members of the response team as outlined in the Incident Response Policy, when an incident is reported.
- ✓ will be responsible for ensuring that every detail of the incident-handling procedure is followed, upon arrival at the incident site.
- ✓ will assign team members the various tasks outlined in the incident-handling procedure.
- ✓ serve as the liaison to the legal team, law enforcement officials, management, and public relations personnel.

Ultimate responsibility for ensuring that evidence is properly collected and preserved, and that the chain of custody is properly maintained, belongs to the incident coordinator.

The Evidence Notebook

- One team member will be assigned the task of maintaining the evidence note-book.
- This person will record the who, what, where, when, and how of the

investigation process. At a minimum, items to be recorded in the notebook include the following task.

a) Who initially reported the suspected incident along with time, date, and circumstances surrounding the suspected incident?

b) Details of the initial assessment leading to the formal investigation.

c) Names of all persons conducting the investigation.

d) The case number of the incident.

e) Reasons for the investigation.

f) A list of all computer systems included in the investigation, along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.

g) Network diagrams.

h) Applications running on the computer systems previously listed.

i) A copy of the policy or policies that relate to accessing and using the systems previously listed.

j) A list of administrators responsible for the routine maintenance of the system.

k) A detailed list of steps used in collecting and analyzing evidence. Specifically, this list needs to identify the date and time each task was performed, a description of the task, who performed the task, where the task

was performed, and the results of the analysis.

l) An access control list of who had access to the collected evidence at what date and time.

- A separate notebook should be used for each investigation. It should be bound in such a way that it is obvious if a page or pages have been removed.
- This notebook is a crucial element in maintaining chain of custody. Therefore, it must be as detailed as possible to assist in maintaining this chain.

Evidence Collection

- ✓ Another team member (or members) will be assigned the task of evidence collection.
- ✓ To avoid confusion, the number of people assigned this task should be kept to a minimum.
- ✓ This member (or members) should also be highly proficient with copying and analysis tools.
- ✓ This person will tag all evidence and work with the person responsible for the evidence notebook to ensure that this information is properly recorded.
- ✓ Next, the person will also be responsible for making a reliable copy of all data to be used as evidence.
- ✓ The data will include complete copies of drives on compromised or suspect systems, as well as all relevant log files.

- ✓This can be done on-site or the entire system can be moved to a forensics lab, as needs dictate.
- ✓A binary copy of the data is the proper way to preserve evidence.
- ✓A reliable copy process has three critical characteristics.
  - The process must meet industry standards for quality and reliability.
  - The copies must be capable of independent verification.
  - The copies must be tamperproof.
- ✓Once all evidence is collected and logged, it can be securely transported to the forensics lab.
- ✓ A detailed description of how data was transported and who was responsible for the transport, along with date, time, and route, should be included in the log.

Storage and Analysis of Data

- ➢The lab must provide some form of access control; a log should be kept detailing entrance and exit times of all individuals.
- ➢It is important that evidence never be left in an unsecured area.
- ➢If a defense lawyer can show that unauthorized persons had access to the evidence, it could easily be declared inadmissible.
- ➢As analysis of evidence is performed, investigators must log the details of

their actions in the evidence notebook. The following should be included at a minimum:

- The date and time of analysis
- Tools used in performing the analysis
- Detailed methodology of the analysis
- Results of the analysis.
- Finally, once all evidence has been analyzed and all results have been recorded in the evidence notebook, a copy of the notebook should be made and given to the legal team.
- If the legal team finds that sufficient evidence exists to take legal action, it will be important to maintain the chain of custody until the evidence is handed over to the proper legal authorities.
- Legal officials should provide a receipt detailing all of the items received for entry into evidence.

COMPUTER IMAGE VERIFICATION AND AUTHENTICATION

2.16 Special Needs of Evidential Authentication

- During an investigation, it is decided that evidence may reside on a computer system.
- It may be possible to seize or impound the computer system, but this risks

violating the basic principle of *innocent until proven guilty*, by depriving an innocent party of the use of his or her system.

- It should be perfectly possible to copy all the information from the computer system in a manner that leaves the original system untouched and yet makes all contents available for forensic analysis.

- The courts may rightly insist that the copied evidence is protected from either accidental or deliberate modification and that the investigating authority should prove that this has been done. Thus, it is not the content that needs protection, but its integrity.

- This protection takes two forms:
  - A secure method of determining that the data has not been altered by even a single bit since the copy was taken.
  - A secure method of determining that the copy is genuinely the one taken at the time and on the computer in question.

- These elements are collectively referred as the ***Digital Image Verification and Authentication Protocol*.**

DIGITAL IDS AND AUTHENTICATION TECHNOLOGY

- ✓ Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for customers to know how much to trust software.
- ✓ It's difficult to make the choice of downloading the software from the Internet.
- ✓ For example (when using Microsoft Authenticode coupled with Digital IDs™ from VeriSign®), through the use of digital signatures, software developers are able to include information about themselves and their code with their programs.

- ✓ When customers download software signed with **Authenticode** and verified by **VeriSign**, they should be assured of content source, indicating that the software really comes from the publisher who signed it, and **content integrity**, indicating that the software has not been altered or corrupted since it was signed.

Authenticode

- Microsoft Authenticode allows developers to include information about themselves and their code with their programs through the use of digital signatures.
- Through *Authenticode*, the user is informed:

1. Of the true identity of the publisher
2. Of a place to find out more about the control
3. The authenticity of the preceding information

- Users can choose to trust all subsequent downloads of software from the same publisher and all software published by commercial publishers that has been verified by VeriSign.

Public Key Cryptography

- ✓ In public key cryptographic systems, every entity has two complementary keys (a public key and private key) that function only when they are held together.
- ✓ Public keys are widely distributed to users, whereas private keys are kept safe

and only used by their owner.

- ✓ Any code digitally signed with the publisher's private key can only be successfully verified using the complementary public key.
- ✓ Code that successfully verified using the publisher's public key, could only have been digitally signed using the publisher's private key, and has not been tampered with.

Certificate Authorities

- Certification Authorities such as VeriSign are organizations that issue digital certificates to applicants whose identity they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it.
- VeriSign has the following responsibilities:

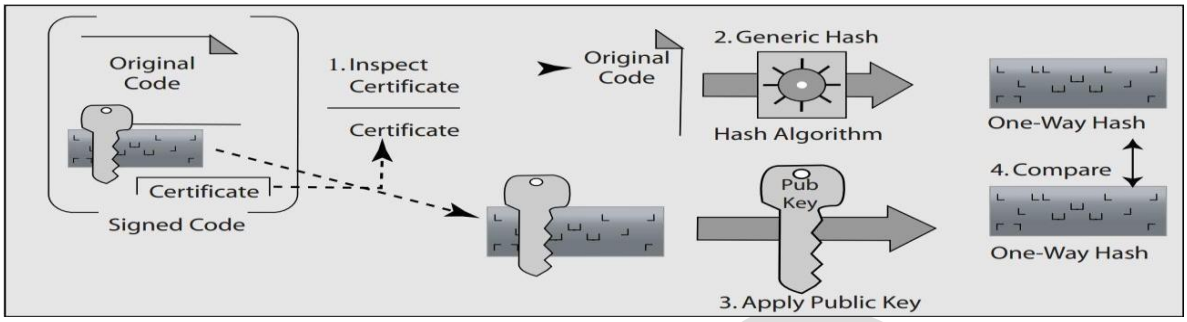
1. Publishing the criteria for granting, revoking, and managing certificates
2. Granting certificates to applications who meet the published criteria
3. Managing certificates
4. Storing VeriSign's root keys in an exceptionally secure manner
5. Verifying evidence submitted by applicants
6. Providing tools for enrollment
7. Accepting the liability associated with these responsibilities

8. Time-stamping digital signatures.

Digital ID

- A Digital ID/Certificate is a form of electronic credentials for the Internet.
- A Digital ID is issued by a trusted third party to establish the identity of the ID holder.
- The third party who issues certificates is known as a Certificate Authority (CA).
- Digital ID technology is based on the theory of public key cryptography.
- The purpose of a Digital ID is to reliably link a public/private key pair with its owner.
- When a CA such as VeriSign issues a Digital IDs, it verifies that the owner is not claiming a false identity.
- When a CA issues you a digital certificate, it puts its name behind the statement that you are the rightful owner of your public/private key pair.

How Authenticode works with VeriSign Digital IDs?



Authenticode: VeriSign Digital ID process

1. Publisher obtains a Software Developer Digital ID from VeriSign
2. Publisher creates code
3. Using the SIGNCODE.EXE utility, the publisher
   - Creates a hash of the code, using an algorithm such as MD5 or SHA
   - Encrypts the has using his/her private key
   - Creates a package containing the code, the encrypted hash, and the publisher's certificate
4. The end user encounters the package
5. The end user's browser examines the publisher's Digital ID. Using the VeriSign root Public Key, which is already embedded in Authenticode enabled applications, the end user browser verifies the authenticity of Software Developer Digital ID (which is itself signed by the VeriSign root Private Key)
6. Using the publisher's public key contained within the publisher's Digital ID, the end user browser decrypts the signed hash.
7. The end browser runs the code through the same hashing algorithm as the publisher, creating a new hash.

8. The end user browser compares the two hashes. If they are identical, the browser messages that the content has been verified by VeriSign, and the end user has the confidence that the code was signed by the publisher identified in the Digital ID, and the code hasn't been altered since it was signed.

Time Stamping: Because key pairs are based on mathematical relationships that can theoretically be ―cracked‖ with a great deal of time and effort, it is a well-established security principle that digital certificates should expire.

2.17 Practical Consideration

- It is useful to present some fundamental requirements of a forensic data collection system before considering how these can be securely protected.
- Other forensic experts may argue against some or all of them:
    a. Forensic data collection should be complete and non-software specific,thus avoiding software traps and hidden partitioning.
    b. In operation, it should be as quick and as simple as possible to avoid error or delay.
    c. It should be possible for anyone to use a forensic data collection system with the minimum amount of training.
    d. Necessary costs and resources should be kept to a minimum.
- To meet the conditions specified in items 2, 3, and 4, the digital integrity verification and authentication protocol must be tailored to suit.
- Only investigators issued with a valid digital signature would be able to complete copies.

2.18 Practical Implementation

- ✓ A minimum amount of reliance is placed on the technical ability of the operator/investigator.
- ✓ It must be understood that during the copying process, procedures are implemented to trap and handle hardware errors, mapping exceptions where necessary.
- ✓ It must also be understood that procedures are implemented to verify that information is copied correctly.
- ✓ This information is stored on each cartridge within a copy series.
- ✓ Also stored on each cartridge is a reference area containing copy-specific information such as CPU type and speed, hardware equipment indicators, copying drive serial number, cartridge sequence number, exhibit details and reference comments, operator name together with a unique password, and the real date and time as entered by the operator.
- ✓ The cartridge is divided into blocks of an arbitrary chosen size. Blocks may contain reference, ROM, CMOS, or disk data depending on their location on the cartridge. Each cartridge contains the information copied from the suspect drive on a sector by sector basis.

Safe Boxes and the Vault

- As each block is copied and verified, a hash value is generated such that a single bit change anywhere within the block would produce a different hash. The result is stored in the relevant safe box and copying to the next block.
- Once all the blocks relevant to a particular cartridge have been copied and

treated in this way, the whole group of safe boxes, collectively referred to as the vault, are treated as an individual block and a vault hash value is generated and stored in the final safe box. The vault is then copied to another area of the cartridge and this second copy is encrypted.

- The vault hash value for each cartridge is stored in a separate area in memory and the operator is prompted to insert a new cartridge until the copy is completed. The final cartridge will contain similar information to the others in the series and in addition will have the accumulated vault hash values from all other cartridges in the series.

- Once the final cartridge has been copied, the operator is prompted to insert a preformatted floppy disk into the drive used to start the DIBS process. All of the accumulated vault hash values are then written to a floppy disk together with the reference details of the whole copy procedure. At least two identical floppy disks are created in this manner.

- The floppy disks are then sealed in numbered, tamperproof bags and both numbers are written on both envelops. The computer owner is given his or her chosen floppy and the other is placed in secure storage.

Security Considerations

- Computer forensics investigators are constantly discovering new vulnerabilities in old image verification and authentication products.

- As a result CIOs (Chief information Officers) are devoting more money and time to image verification and authentication security.

- Staff-members are the ones who make sure viruses don't come in and holes aren't created in the firewall.

- They have to understand that most business is built on trust, and their role in maintaining trust is crucial.
- It's difficult, perhaps impossible, to measure the return on investment in security.
- You have to protect your data. It only takes one time ---one hacker getting in and hacking all your financial data.
- It would be irresponsible on CIO's part not have the toughest image verification and authentication security possible.

UNIT-III

COMPUTER FORENSICS ANALYSIS AND VALIDATION

3.1 Determining What Data to Collect and Analyze

Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process. Criminal investigations are limited to finding data defined in the search warrant, and civil investigations are often limited by court orders for discovery. Corp.- rate investigators might be searching for company policy violations that require examining only specific items, such as e-mail. Therefore, investigations often involve locating and recovering a few specific items, which simplifies and speeds processing.

In the corporate environment, however, especially if litigation is involved, the company attar- nay often directs the investigator to recover as much information as possible. Satisfying this demand becomes a major undertaking with many hours of tedious work. These types of invest- ligations can also result in scope creep, in which an investigation expands beyond the original description because of unexpected evidence you find, prompting the attorney to ask you to examine other areas to recover more evidence. Scope creep increases the time and resources needed to extract, analyze, and present evidence. Be sure to document any requests for add- tonal investigation, in case you must explain why the investigation took longer than planned, why the scope widened during the course of the investigation, and so forth.

One reason scope creep has become more common is that criminal investigations increasingly require more detailed examination of evidence just before trial to help prosecutors fend off attacks from defense attorneys. Because defense attorneys typically have the right of full discovery of digital evidence used against their clients, it’s possible for new evidence to come to light while complying with the defense request for full

discovery. However, this new evidence often isn't revealed to the prosecution; instead, the defense uses it to defend the accused. For this reason, it's become more important for prosecution teams to ensure that they have analyzed the evidence exhaustively before trial. (It should be noted that the defense request for full discovery applies only to criminal cases in the however, depends on whether it's an internal corporate investigation or a civil or criminal investigation carried out by law enforcement. In an internal investigation, evidence collection tends to be fairly easy and straightforward because corporate investigators usually have ready access to the necessary records and files. In contrast, when investigating a criminal cyber- stalking case, you need to contact the ISP and e-mail service.

Some companies, such as AOL, have a system set up to handle these situations, but others do not. Many companies don't keep e-mail for longer than 90 days, and some keep it only two weeks.

An employee suspected of industrial espionage can require the most work. You might need to set up a small camera to monitor his or her physical activities in the office. You might also need to plant a software or hardware key logger (for capturing a suspect's keystrokes remotely), and you need to engage the network administrator's services to monitor Internet and network activities. In this situation, you might want to do a remote acquisition of the employee's drive, and then use another tool to determine what peripheral devices have been accessed.

1. For target drives, use only recently wiped media that have been reformatted and inspected for computer viruses. For example, use ProDiscover Secure Wipe Disk, Digital Intelligence PDWipe, or White Canyon Secure Clean to clean all data from the target drive you plan to use.

2. Inventory the hardware on the suspect's computer and note the condition of the computer when seized. Document all physical hardware components as part of your

evidence acquisition process.

3. For static acquisitions, remove the original drive from the computer, if practical, and then check the date and time values in the system's CMOS.

4. Record how you acquired data from the suspect drive note, for example, that you created a bit- stream image and which tool you used. The tool you use should also create an MD5 or SHA-1 or better hash for validating the image.

5. When examining the image of the drive's contents, process the data methodically and logically. List all folders and files on the image or drive. For example, FTK can generate a Microsoft Access database listing all files and folders on a suspect drive. Note where specific evidence is found, and indicate how it's related to the investigation.

6. If possible, examine the contents of all data files in all folders, starting at the root directory of the volume partition. The exception is for civil cases, in which you look for only specific items in the investigation.

7. For all password-protected files that might be related to the investigation, make your best effort to recover file contents. You can use password recovery tools for this purpose, such as Access Data Password Recovery Toolkit (PRTK), NTI Password Recovery, or Pass ware Kit Enterprise

1. Identify the function of every executable (binary or .exe) file that doesn't match known hash values. Make note of any system files or folders, such as the System32 folder or its content, that are out of place. If you can't find information on an executable file by using a disk editor, examine the file to see what it does and how it works.

1. Maintain control of all evidence and findings, and document everything as you progress through your examination. ps to locate specific message Refining and Modifying the Investigation Plan In civil and criminal cases, the scope is often defined by search warrants or subpoenas, which specify what data you can recover. However,

private sector cases, such as employee abuse investigations, might not spec- ify limitations in recovering data. For these cases, it's important to refine the investigation plan as much as possible by trying to determine what the case requires. Generally, you want the investigation to be broad enough to encompass all relevant evidence, yet not so wide- ranging that you waste time and resources analyzing data that's not going to help yourcase.

Of course, even if your initial plan is sound, at times you'll find that you need to deviate from the plan and follow where the evidence leads you. Even in these cases, having a plan that you deliberately revise along the way is much better than searching for evidence haphazardly.

Suppose, for example, an employee is accused of operating an Internet-based side business using company resources during normal business hours. You use this timeframe to narrow the set of data you're searching, and because you're looking for unauthorized Internet use, you focus the search on temporary Internet files, Internet history, and e-mail communicate- ion. Knowing the types of data you're looking for at the outset helps you make the best use of your time and prevents you from casting too wide a net. However, in the course of reviewing e-mails related to the case, you might find references to spreadsheets or Word documents containing financial information related to the side business. In this case, it makes sense to broaden the range of data you're looking for to include these types of files. Again, the key is to start with a plan but remain flexible in the face of new evidence.

3.1.1 Using Access Data Forensic Toolkit to Analyze Data

So far, you have used several different features of FTK; this section goes into more detail on its search and report functions. FTK can perform forensics analysis on the following file systems:

- Microsoft FAT12, FAT16, and FAT32

- Microsoft NTFS (for Windows NT, 2000, XP, and Vista)
- Linux Ext2fs and Ext3fs

FTK can analyze data from several sources, including image files from other vendors. It can also read entire evidence drives or subsets of data, allowing you to consolidate large volumes of data from many sources when conducting a computer forensics analysis. With FTK, you can store everything from image files to recovered server folders on one investigation drive.

FTK also produces a case log file, where you can maintain a detailed record of all activities during your examination, such as keyword searches and data extractions. This log is also handy for reporting errors to Access Data. At times, however, you might not want the log feature turned on. If you're following a hunch, for example, but aren't sure the evidence you recover is applicable to the investigation, you might not want opposing counsel to see a record of this information because he or she could use it to question your methods and perhaps discredit your testimony. Look through the evidence first before enabling the log feature to record searches. This approach isn't meant to conceal evidence; it's a precaution to ensure that your testimony can be used in court.

FTK has two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly. This option returns search results quickly, although it does have some shortcomings. For example, you can't search for hexadecimal string values, and depending on how data is stored on the eve- dense drive, indexing might not catalog every word. If you do use this feature, keep in mind that indexing an image file can take several hours, so it's best to run this process overnight.

The other option is a live search, which can locate items such as text hidden in

unallocated space that might not turn up in an indexed search. You can also search for alphanumeric and hexadecimal values on the evidence drive and search for specific items, such as phone numbers, credit card numbers, and Social Security numbers. Figure 9-1 shows the hits found during a live search of an image of a suspected arsonist's laptop. You can right-click a search hit to add it to your bookmarks, which includes the result in your final report.

3.2 Validating Forensic Data

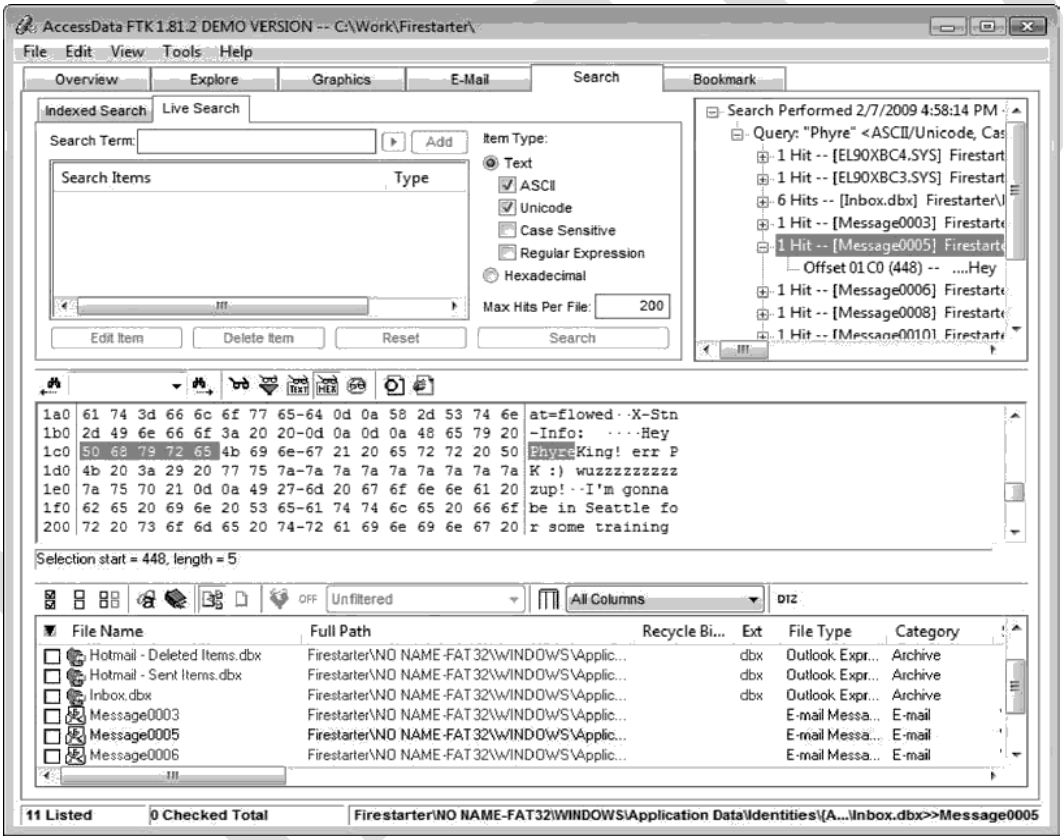


Fig: Validating Forensic Data

One of the most critical aspects of computer forensics is validating digital evidence because ensuring the integrity of data you collect is essential for presenting evidence in court. Chapter 5 introduced forensic hashing algorithms, and in this section, you learn more about validating an acquired image before you analyze it.

Most computer forensic tools such as ProDiscover, X-Ways Forensics, FTK, and Encase provide automated hashing of image files. For example, when ProDiscover loads an image file, it runs a hash and compares that value to the original hash calculated when the image was first acquired. You might remember seeing this feature when the Auto Image Checksum Verification message box opens after you load an image file in ProDiscover. Computer foren- sics tools have some

limitations in performing hashing, however, so learning how to use advanced hexadecimal editors is necessary to ensure data integrity.

3.2.1 Validating with Hexadecimal Editors

Advanced hexadecimal editors offer many features not available in computer forensics tools, such as hashing specific files or sectors. Learning how to use these tools is important, especially when you need to find a particular file—for example, a known contraband image. With the hash value in hand, you can use a computer forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file. (Recall that two files with exactly the same content have the same hash value, even if they have different names.) Getting a hash value with a full-featured hexadecimal editor is much faster and easier than with a computer forensics tool.

3.3 Addressing Data-Hiding Techniques

Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection. Some of these techniques are discussed in the following sections.

3.3.1 Hiding Partitions

One way to hide partitions is to create a partition and then use a disk editor, such as Norton Disk Edit, to delete any reference to it manually. To access the deleted partition, users can edit the partition table to re-create the links, and then the hidden partition reappears when the computer is restarted. Another way to hide partitions is with a disk-partitioning utility, such as G Disk, Partition Magic, System Commander, or Linux Grand Unified Boot loader (GRUB), which provides a startup menu where you can select an OS. The system then ignores other bootable partitions.

To circumvent these techniques, be sure to account for all disk space when you're examining an evidence drive. Analyze any disk areas containing space you can't account for so that you can determine whether they contain additional evidence. For example, in the following code, Disk Manager recognizes the extended partition (labeled EXT DOS) as being 5381.1 MB (listed as Mbytes). The LOG DOS labels for partitions E through F indicate that they're logical partitions that make up the extended partition. However, if you add the sizes of drives E and F, the result is only 5271.3 MB, which is your first clue to examine the disk more closely. The remaining 109.8 MB could be a previously deleted partition or a hidden partition. For this example, the following code shows the letter ―H‖ to indicate a hidden partition. Disk Partitions Cylinders Heads Sectors Mbytes Sectors 2 5111661663 5495.8 11255328

Partition	Status	Type	Volume Label	Mbytes	System	Usage
D:	1		PRI DOS	109.8	FAT16	2%
	2		EXT DOS	5381.1		98%
E:	3		LOG DOS	109.8	FAT16	2%
	4	H	LOG DOS	109.8	FAT16	2%

F:	5		LOG DOS	5161.5	FAT32	94%

Windows creates a partition gap between partitions automatically; however, you might find a gap that's larger than it should be. For example, in Windows 2000/XP, the partition gap is only 63 sectors, so 109.8 MB is too large to be a standard partition gap. In Windows Vista, the gap is approximately 128 sectors.

In Figure, you can see a hidden partition in Disk Manager, which shows it as an unknown partition. In addition, the drive letters in the visible partitions are nonconsecutive (drive I is skipped), which can be another clue that a hidden partition exists. Most skilled users would make sure this anomaly doesn't occur, however.

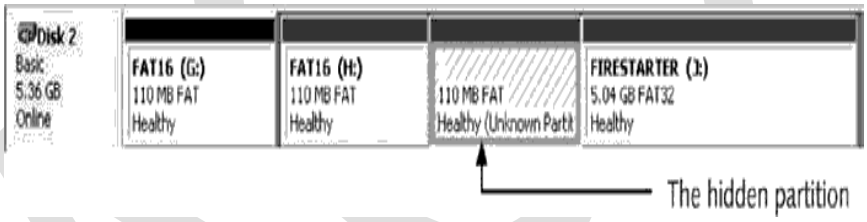


Fig: Viewing a hidden partition in Disk Manager

In ProDiscover, a hidden partition appears as the highest available drive letter set in the BIOS. Figure 9-9 shows four partitions, similar to Figure 9-8, except the hidden partition shows as the drive letter Z. To carve (or salvage) data from the recovered partition gap, you can use other computer forensics tools, such as FTK or WinHex.

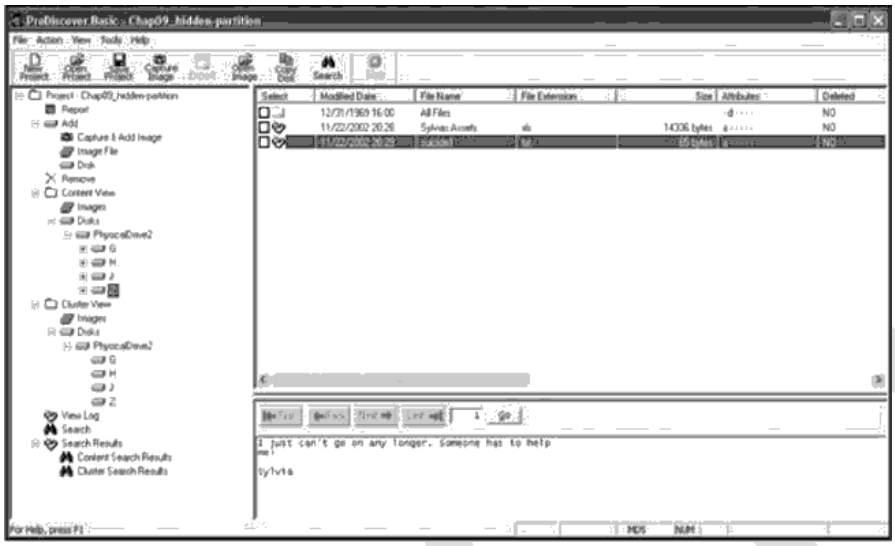


Fig: Viewing a hidden partition in ProDiscover

3.3.2 Marking Bad Clusters

Another data-hiding technique, more common in FAT file systems, is placing sensitive or incriminating data in free or slack space on disk partition clusters. This technique involves using a disk editor, such as Norton Disk Edit, to mark good clusters as bad clusters. The OS then considers these clusters unusable. The only way they can be accessed from the OS is by changing them to good clusters with a disk editor.

3.3.3 Bit-Shifting

Some home computer users developed the skill of programming in the computer manufacturer's assembly language and learned how to create a low-level encryption program that changes the order of binary data, making the altered data unreadable when accessed with a text editor or word processor. These programs rearrange bits for each byte in a file. To secure a file containing sensitive or incriminating information, these users run an assembler program (also called a macro) on the file

to scramble the bits. To access the file, they run another program that restores the scrambled bits to their original order. Some of these pro- grams are still used today and can make it difficult for investigators to analyze data on a suspect drive.

Start Notepad, and in a text document, type TEST FILE. Test file is to see how shifting bits will alter the data in a file. Save the file as Bit_shift.txt in your work folder, and exit Notepad.

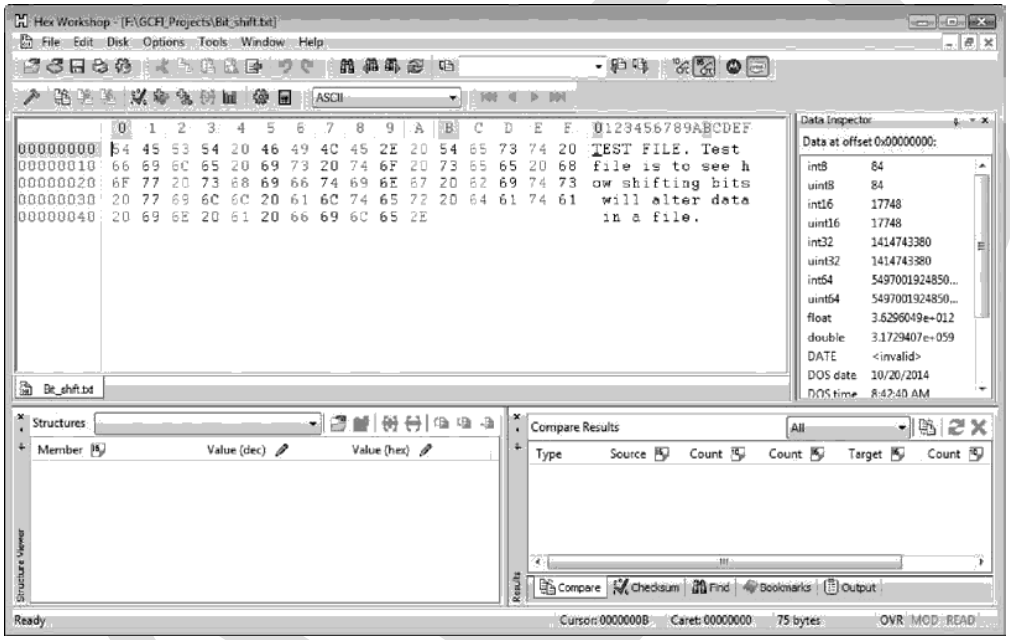


Fig: Hex workshop

Start Hex Workshop. Click File, Open from the menu. Navigate to your work folder, and then double-click Bit_shift.txt. Bit_shift.txt open in Hex Workshop.

To set up Hex Workshop for the bit-shifting exercise, click Options, Toolbars from the menu. In the Customize dialog box, click the Data Operations check box, and then click OK.

Click the Shift Left button (<< icon) on the Data Operations toolbar. The Shift Left Operation dialog box opens, where you specify how you want to treat the data, the ordering scheme to use for bytes, and whether you shift bits for selected text or the

entire file.

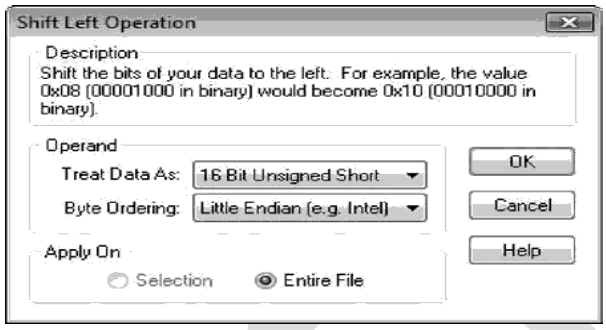


Fig: The Shift Left Operation dialog box

1. Click OK to accept the default settings and shift the bits in Bit_shift.txt to the left.

2.Save the file as Bit_shift_left.txt in your work folder. above Figure shows the file in Hex Workshop, with the @ symbols indicating shifted bits.

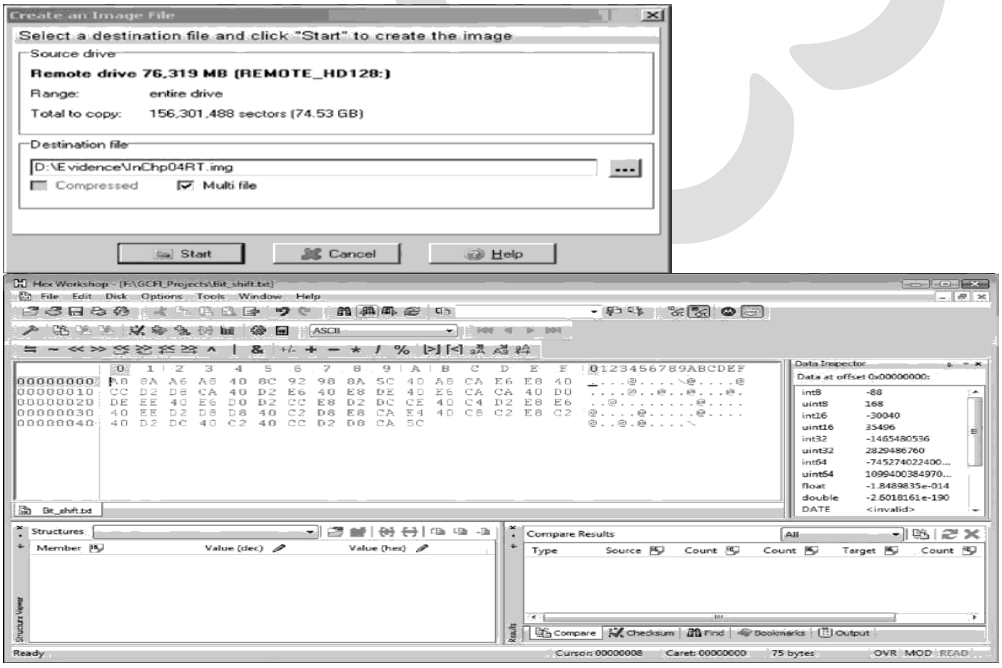


Fig:Viewing the shifted bits

1. To return the file to its original configuration, shift the bits back to the right by

clicking the Shift Right button (>> icon) on the Data Operations toolbar. Click Ok to accept the default settings in the Shift Right Operation dialog box. The file is displayed in its original format.

2. Save the file as Bit_shift_right.txt in your work folder, and leave Hex Workshop open for the next activity. Now you can use Hex Workshop to find the MD5 hash values for these three files and determine whether Bit_shift.txt is different from Bit_shift_right.txt and Bit_shift_left.txt. (You could also use FTK or ProDiscover to find the MD5 hash values.) To check the MD5 values in Hex Workshop, follow these steps:

1. With Bit_shift_right.txt open in Hex Workshop, click File, Open to open Bit_shift.txt, and then repeat to open Bit_shift_left.txt.

2. Click the Bit_shift.txt tab in the upper pane to make it the active file.

3. Click Tools, Generate Checksum from the menu to open the Generate Checksum dialog box. In the Select Algorithms list box, click MD5, and then click the Generate button. Copy the MD5 hash value of Bit_shift.txt, shown in the lower-right pane, and paste it in a new text document in Notepad.

4. Repeat Steps 2 and 3 for Bit_shift_left.txt and Bit_shift_right.txt, pasting their hash values in the same text file in Notepad.

5. Compare the MD5 hash values to determine whether the files are different. When you're finished, exit Notepad and Hex Workshop.

Typically, antivirus tools run hashes on potential malware files, but some advanced malware uses bit-shifting as a way to hide its malicious code from antivirus tools. With the bit-shifting functions in Hex Workshop, however, you can inspect potential malicious code manually. In addition, some malware that attacks

Microsoft Office files consists of executable code that's embedded at the end of document files, such as Word documents, and hidden with bit- shifting. When an Office document is opened, the malware reverses the bit-shifting on the executable code and then runs it.

3.4 Performing Remote Acquisitions

Remote acquisitions are handy when you need to image the drive of a computer far away from your location or when you don't want a suspect to be aware of an ongoing investiga- tion. This method can save time and money, too. Many tools are available for remote acquisi- tions; in the following sections, you use Runtime Software to learn how remote acquisitions are made.

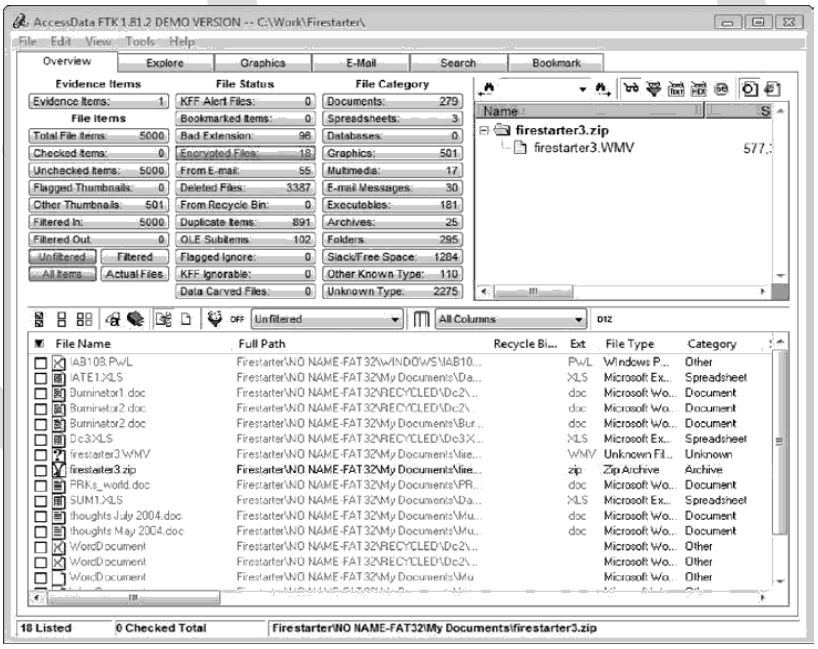


Fig: FTK displaying encrypted files

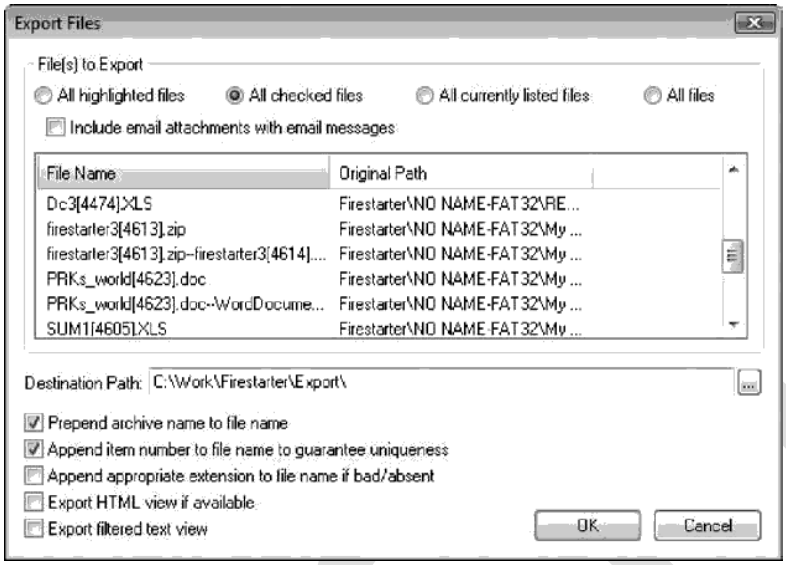


Fig: Exporting encrypted files

3.4.1 Remote Acquisitions with Runtime Software

Runtime Software (*www.runtime.org*) offers the following shareware programs for remote acquisitions:

DiskExplorer for FAT

- DiskExplorer for NTFS
- HDHOST

Chapter 4 introduced these tools; remember that they're designed to be file system specific, so there are DiskExplorer versions for both FAT and NTFS that you can use to create raw for- mat image files or segmented image files for archiving purposes.

HDHOST is a remote access program for communication between two computers. The connection is established by using the DiskExplorer program (FAT or NTFS) corresponding to the suspect (remote) computer's file system. The following sections show how to make a live remote acquisition of another computer over a

network. To use these tools, it's best to have computers connected on the same local hub or router with minimal network traffic.

3.5 Network Forensics Overview

Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network. Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians. Labor forecasts predict a shortfall of 50,000 network forensics specialists in law enforcement, legal firms, corporations, and universities.

Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program, for example. A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused the –attack.‖

Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident. Typically, network administrators want to find compromised.

3.5.1 Securing a Network

Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents. Hardening includes a range of tasks, from applying the latest patches to using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the

more safeguards are in place. The National Security Agency (NSA) developed a similar approach, called the defense in depth (DiD) strategy. DiD have three modes of protection:

- People
- Technology
- Operations

If one mode of protection fails, the others can be used to thwart the attack. Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge. In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organize- tion's security policy. Physical and personnel security measures are included in this mode of protection. The technology mode includes choosing strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with risk assessment can help improve network security, too. Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

3.6 Performing Live Acquisitions

The problem investigators face is the order of volatility (OOV), meaning how long a piece of information lasts on a system. Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years. The fol- lowing steps show the general procedure for a live

acquisition, although investigators differ on exact steps:

- Create or download a bootable forensic CD, and test it before using it on a suspect drive. If the suspect system is on your network and you can access it remotely, add the appropriate network forensics tools to your workstation. If not, insert the bootable forensics CD in the suspect system.
- Make sure you keep a log of all your actions; documenting your actions and reasons for these actions is critical.
- A network drive is ideal as a place to send the information you collect. If you don't have one available, connect a USB thumb drive to the suspect system for collecting data. Be sure to note this step in your log.
- Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or you can use available freeware tools, such as mem fetch (*www.freshports.org/sysutils/ memfetch*) and Back Track (discussed in the following section).
- The next step varies, depending on the incident you're investigating. With an intrusion, for example, you might want to see whether a rootkit is present by using a tool such as Root Kit Revealer (*www.microsoft.com/technet/sysinternals/Utilities/ RootkitRevealer.mspx*). You can also access the system's firmware to see whether it has changed, create an image of the drive over the network, or shut the system down and make a static acquisition later.
- Be sure to get a forensically sound digital hash value of all files you recover during the live acquisition to make sure they aren't altered later.

Performing a Live Acquisition in Windows

Live acquisitions are becoming more necessary, and several tools are available for capturing RAM. ManTech Memory DD (*www.mantech.com/msma/MDD.asp*) can access up to 4 GB RAM in standard did format. Another freeware tool, Win32dd (*http://win32dd.msuiche.net*), runs from the command line to perform a memory dump in Windows. In addition, comer- coal tools, such as Guidance Software Winen.exe, can be used.

Another popular tool is Backtrack (*www.remote-exploit.org/backtrack.html*), which com- bines tools from the White Hat Hackers CD and The Auditor CD (see Figure 11-3). More than 300 tools are available, including password crackers, network sniffers, and freeware for- entices tools. Backtrack has become popular with penetration testers and is used at the annual Collegiate Cyber Defense Competitions.

Fig:Some of the tools available in BackTrack

3.7 Developing Standard Procedures for Network Forensics

Network forensics is a long, tedious process, and unfortunately, the trail can go cold quickly. A standard procedure often used in network forensics

is as follows:

- Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files.
- When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.
- Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.
- Acquire the compromised drive and make a forensic image of it.
- Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.

In computer forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes you restore the image to a physical drive so that you can run programs on the drive. In network forensics, you have to restore the drive to see how mal- ware attackers have installed on the system works. For example, intruders might have trans- mitted a Trojan program that gives them access to the system and then installed a root kit, which is a collection of tools that can perform network reconnaissance tasks (using the ls or net stat command to collect information, for instance), key logging, and other actions.

3.8Using Network Tools

A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more. The tools covered in this chapter are freeware and work in Windows and UNIX. Sysinternals (*www.microsoft.com/technet/sysinternals/*) is a collection of free tools for examining Windows products. They were created by Mark Russinovich and Bryce Cogs well and acquired by Microsoft.

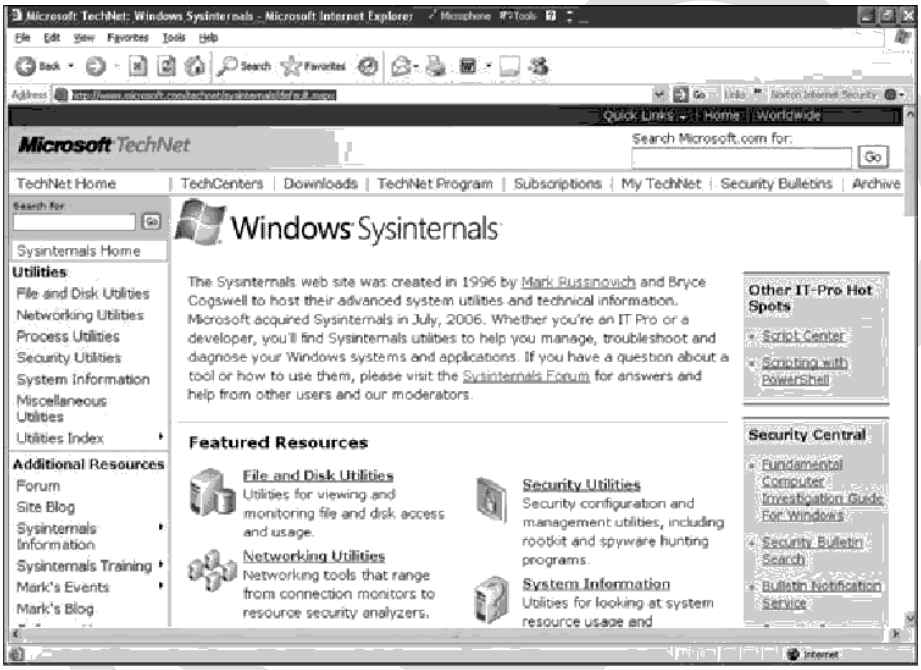


Fig: Opening page of Sysinternals

As you can see in above Figure, you can choose from file and system, networking, process, and security tools, among others. The following list describes a few examples of the powerful Windows tools available at Sysinternals:

- RegMon shows all Registry data in real time.
- Process Explorer shows what files, Registry keys, and dynamic link libraries (DLLs) are loaded at a specific

time.

- Handle shows what files are open and which processes are using these files.
- Filemon shows file system activity.

Far too many tools are available to list here, but you should take some time to explore the site and see what's available. One in particular that's worth investigating is PsTools, a suite created by Sysinternals that includes the following tools:

- *PsExec*—Runs processes remotely
- *PsGetSid*—Displays the security identifier (SID) of a computer or user
- *PsKill*—Kills processes by name or process ID
- *PsList*—Lists detailed information about processes
- *PsLoggedOn*—Displays who's logged on locally
- *PsPasswd*—Allows you to change account passwords
- *PsService*—Enables you to view and control services
- *PsShutdown*—Shuts down and optionally restarts a computer
- *PsSuspend*—Allows you to suspend processes

3.9 Understanding Rules of Evidence

Consistent practices help verify your work and enhance your credibility, so you must handle all evidence consistently. Apply the same security and accountability controls

for evidence in a civil lawsuit as in a major crime to comply with your state's rules of evidence or with the Federal Rules of Evidence. Also, keep in mind that evidence admitted in a criminal case might also be used in a civil suit, and vice versa. For example, suppose someone is charged with murder and acquitted at the criminal trial because the jury isn't convinced beyond a reasonable doubt of the person's guilt. If enough evidence shows that the accused's negligence contributed to a wrongful death, however, the victim's relatives can use the evidence in a civil lawsuit to recover damages.

As part of your professional growth, keep current on the latest rulings and directives on col- lecting, processing, storing, and admitting digital evidence. The following sections discuss some key concepts of digital evidence. You can find additional information at the U.S. Department of Justice Web site (*www.usdoj.gov*) and by searching the Internet for ‒digital evidence,‖ ‒best evidence rule,‖ ‒hearsay,‖ and other relevant keywords. Consult with your prosecuting attorney, Crown attorney, corporate general counsel, or the attorney who retained you to learn more about managing evidence for your investigation. DVD to your work folder. The work folder path shown in screenshots might differ slightly from yours.

- Start Microsoft Word, and in a new document, type By creating a file, you can identify the author with file metadata. Save it in your work folder as InChp05-01. doc, and then exit Microsoft Word.
- To start FTK, click Start, point to All Programs, point to Access Data, point to Forensic Toolkit, and click Forensic Toolkit. If you're prompted with a warning dialog box and/or notification, click OK to continue, and click OK, if necessary, in the message box thanking you for evaluating the program.
- Click Go directly to working in program, and then click OK. Click File, Add Evidence from the menu.

- In the Add Evidence dialog box, enter your name as the investigator, and then click Next. In the Evidence Processing Options dialog box, accept the default setting, and then click Next.
- In the main Add Evidence to Case dialog box, click the Add Evidence button. In the next Add Evidence to Case dialog box, click the Individual File option button, and then click Continue.
- In the Browse for Folder dialog box, navigate to your work folder, click
- InChp05-01.doc, click Open, and then click OK. Click Next, and then click Finish.
- In the main window, click the Overview tab, if necessary. Under the File Category heading, click the Documents button. Click to select the InChp05- 01.doc file in the bottom pane; its contents are then displayed in the upper-right pane. Figure shows an example (although the filename in this figure is different).

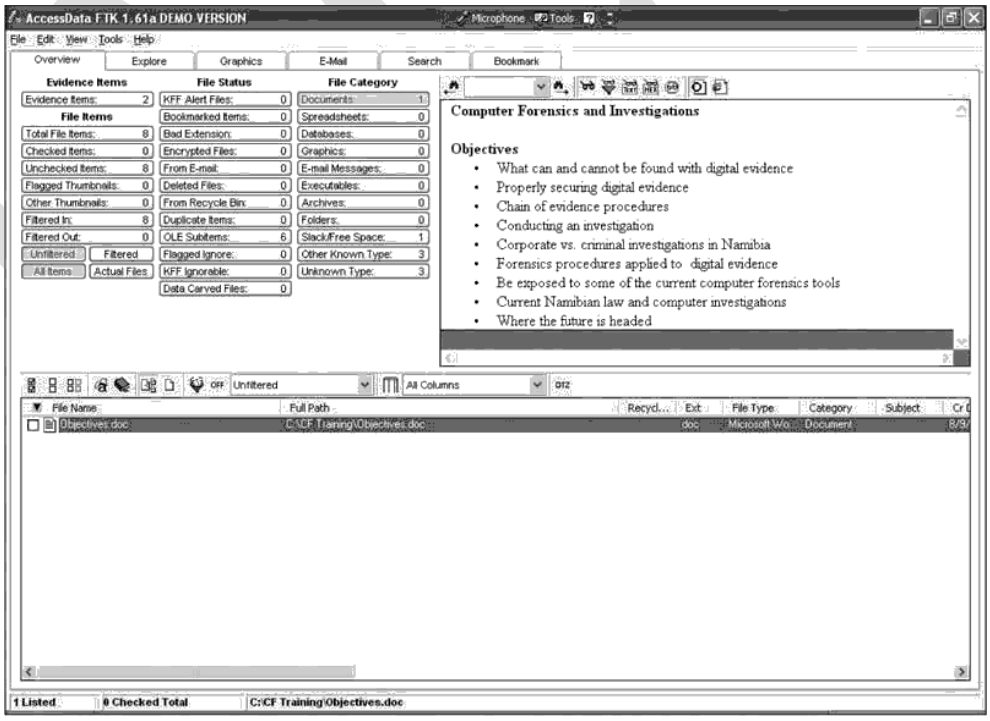


Fig: Selecting a document

- On the File List toolbar at the upper right, click the View files in native format button, if the button isn't already selected. (*Hint*: Hover your mouse over buttons to see their names displayed.)
- Next, click the View files in filtered text format button. If you entered your username and organization when you installed Word, that information is displayed (see Figure 5-2).

10. Exit FTK, clicking No if prompted to back up your work.

11. In addition to revealing the author, computer-stored records must be proved authentic, which is the most difficult requirement to prove when you're trying to qualify evidence as an exception to the hearsay rule. The process of establishing digital evidence's trustworthiness originated with written documents and the best evidence rule, which states that to prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required (see Federal Rules of Evidence, 1002). In other words, the original of a document is preferred to a duplicate. The best evidence, therefore, is the document created and saved on a computer's hard disk.

3.10 Collecting Evidence in Private-Sector Incident Scenes

Private-sector organizations include businesses and government agencies that aren't involved in law enforcement. In the United States, these agencies must comply with state public disclo- sure and federal Freedom of Information Act (FOIA) laws and make certain documents avail- able as public records. State public disclosure laws define state public records as

open and available for inspection. For example, divorces recorded in a public office, such as a court- house, become matter of public record unless a judge orders the documents sealed. Anyone can request a copy of a public divorce decree. Figure 5-3 shows an excerpt of a public disclosure law for the state of Idaho.

State public disclosure laws apply to state records, but the FOIA allows citizens to request copies of public documents created by federal agencies. The FOIA was originally enacted in the 1960s, and several subsequent amendments have broadened its laws. Some Web sites now provide copies of publicly accessible records for a fee.

A special category of private-sector businesses includes ISPs and other communication companies. ISPs can investigate computer abuse committed by their employees, but not by customers. ISPs must preserve customer privacy, especially when dealing with e-mail. However, federal regulations related to the Homeland Security Act and the Patriot Act of 2001 has redefined how ISPs and large corporate Internet users operate and maintain their records. ISPs and other communication companies now can investigate customers' activities that are deemed to create an emergency situation. An emergency situation under the Patriot Act is the immediate risk of death or personal injury, such as finding a bomb threat in an e-mail mes- sage. Some provisions of those laws have been revised over the past few years, so you should stay abreast of their implications.

3.11Processing Law Enforcement Crime Scenes

To process a crime scene properly, you must be familiar with criminal rules of search and sei- zure. You should also understand how a search warrant works and

what to do when you process one. For all criminal investigations in the United States, the Fourth Amendment limits how governments search and seize evidence. A law enforcement officer can search for and seize criminal evidence only with probable cause. Probable cause refers to the standard speci- fying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest. With probable cause, a police officer can obtain a search warrant from a judge that authorizes a search and the seizure of specific evidence related to the criminal complaint. Although several court cases have allowed latitude when searching and seizing computer evidence, making your warrant as specific as possible to avoid challenges from defense attorneys is a good practice. Often a warrant is written and issued in haste because of the nature of the investigation. Law enforcement officers might not have the time to research the correct language for stating the nature of the complaint to meet probable cause requirements. However, because a judge can exclude evidence obtained from a poorly worded warrant, you should review these issues with your local prosecutor before investigating a case.

3.12 Preparing for a Search

Preparing for a computer search and seizure is probably the most important step in computing investigations. The better you prepare, the smoother your investigation will be. The following sections discuss the tasks you should complete before you search for evidence. To perform these tasks, you might need to get answers from the victim (the complainant) and an informant, who could be a police detective assigned to the case, a law enforcement witness, or a manager or co-worker of the person of interest to the investigation.

3.13 Securing a Computer Incident or Crime Scene

Investigators secure an incident or crime scene to preserve the evidence and to keep information about the incident or crime confidential. Information made public could jeopardize the investigation. If you're in charge of securing a computer incident or crime scene, use yellow barrier tape to prevent bystanders from accidentally entering the scene. Use police officers or security guards to prevent others from entering the scene. Legal authority for a corporate incident scene includes trespassing violations; for a crime scene, it includes obstructing justice or failing to comply with a police officer. Access to the scene should be restricted to only those people who have a specific reason to be there. The reason for the standard practice of securing an incident or crime scene is to expand the area of control beyond the scene's immediate location. In this way, you avoid overlooking an area that might be part of the scene. Shrinking the scene's perimeter is easier than expanding it.

For major crime scenes, computer investigators aren't usually responsible for defining a scene's security perimeter. These cases involve other specialists and detectives who are collecting physical evidence and recording the scene. For incidents primarily involving computers, the computers can be a crime scene within a crime scene, containing evidence to be processed.

3.14 Seizing Digital Evidence at the Scene

With proper search warrants, law enforcement can seize all computing systems and peripherals. In corporate investigations, you might have similar authority; however, you might have the authority only to make an image of the suspect's drive. Depending on company policies, corporate investigators rarely have the authority to seize all computers and peripherals.

When seizing computer evidence in criminal investigations, follow the U.S. DOJ standards for seizing digital data (described later in this chapter, or see *www.usdoj.gov/criminal/cybercrime/ searching.html*). For civil investigations,

follow the same rules of evidence as for criminal investigation. You might be looking for specific evidence, such a particular e-mail message or spreadsheet. In a criminal matter, investigators seize entire drives to preserve as much information as possible and ensure that no evidence is overlooked. If you have any questions, doubts, or concerns, consult with your attorney for additional guidance.

3.15 Storing Digital Evidence

With digital evidence, you need to consider how and on what type of media to save it and what type of storage device is recommended to secure it. The media you use to store digital

Evidence usually depends on how long you need to keep it. If you investigate criminal matters, store the evidence as long as you can. The ideal media on which to store digital data are CD- Rs or DVDs. These media have long lives, but copying data to them takes a long time. Older CDs had lives up to five years. Research is currently being done on CD-Rs and CD-RWs with life spans of only one or two years. Today's larger drives demand more storage capacity; 200 GB drives are common, and DVDs can store up to only 17 GB of data.

You can also use magnetic tape to preserve evidence data. The 4-mm DAT magnetic tapes store between 40 to 72 GB or more of data, but like CD-Rs, they are slow at reading and writing data. If you're using these tapes, test your data by copying the contents from the tape back to a disk drive. Then verify that the data is good by examining it with your computer forensics tools or doing an MD5 hash comparison of the original data set and the newly restored dataset.

If a 30-year lifespan for data storage is acceptable for your digital evidence, older DLT magnetic tape cartridge systems are a good choice. Keep in mind that you never know how long it will take for a case to go to trial. Figure shows a 4-mm DAT drive and tape and a DLT tape drive.

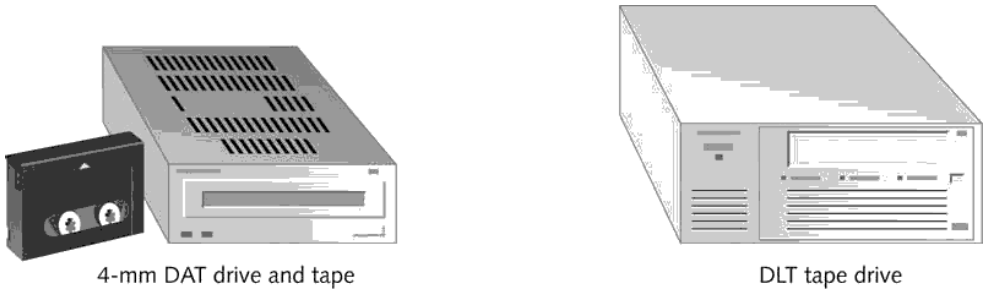


Fig: 4-mm DAT and DLT tape drives

DLT systems have been used with mainframe computers for several decades and are reliable data- archiving systems. Depending on the size of the DLT cartridge, one cartridge can store up to 80 GB of data in compressed mode. Speed of data transfer from your hard drive to a DLT tape is also faster than transferring data to a CD-R or DVD. The only major drawback of a DLT drive and tapes is cost. A drive can cost from $400 to $800, and each tape is about $40. However, with the current large disk drives, the DLT system does offer significant labor savings over other systems. Recently, manufacturers such as Quantum Corp. have introduced a high-speed, high-capacity tape cartridge drive system called Super Digital Linear Tape (Super-DLT or SLDT). These systems are specifically designed for large RAID data backups and can store more than 1 TB of data. Smaller external Super-DLT drives can connect to a workstation through a SCSI card.

However, don't rely on one media storage method to preserve your evidence—be sure to make two copies of every image to prevent data loss. Also, if practical, use different tools to create the two images. For example, you can use the Linux dd command to create the first image and ProDiscover to create the second image.

3.16 Obtaining a Digital Hash

To verify data integrity, different methods of obtaining a unique identity for file data have been developed. One of the first methods, the Cyclic Redundancy Check

(CRC) is a mathematical algorithm that determines whether a file's contents have changed. The most recent version is CRC-32. CRC, however, is not considered a forensic hashing algorithm. The first algorithm for computer forensics use was Message Digest 5 (MD5). Like CRC, MD5 is a mathematical formula that translates a file into a hexadecimal code value, or a hash value. If a bit or byte in the file changes, it alters the hash value, a unique hexadecimal value that identifies a file or drive. (Before you process or analyze a file, you can use a software tool to calculate its hash value.) After you process the file, you produce another digital hash. If it's the same as the original one, you can verify the integrity of your digital evidence with mathematical proof that the file didn't change.

3.17 Reviewing a Case

Some of which are repeated in the following list. Later in this section, you apply each task to a hypothetical investigation to create a preparation plan for searching an incident or crime scene. The following are the general tasks you perform in any computer forensics case**:**

- Identify the case requirements.
- Plan your investigation.
- Conduct the investigation.
- Complete the case report.
- Critique the case.

UNIT-4

COMPUTER FORENSIC TOOLS

4.1 Types of Computer Forensics Tools

Computer forensics tools are divided into two major categories: hardware and software. Each category has additional subcategories discussed in more depth later in this chapter. The following sections outline basic features required and expected of most computer forensics tools.

Hardware Forensics Tools Hardware forensics tools range from simple, single purpose components to complete computer systems and servers. Single-purpose components can be devices, such as the ACARD AEC-7720WP Ultra Wide SCSI-to-IDE Bridge, which is designed to write-block an IDE drive connected to a SCSI cable.

Some examples of complete systems are Digital Intelligence F.R.E.D. systems, DIBS Advanced Forensic Workstations, and Forensic Computers Forensic Examination Stations and portable units.

Software Forensics Tools Software forensics tools are grouped into command-line applications and GUI applications. Some tools are specialized to perform one task, such as Safe Back, a command-line disk acquisition tool from New Technologies, Inc. (NTI). Other tools are designed to perform many different tasks. For example, Technology Pathways Pro- Discover, X-Ways Forensics, Guidance Software En Case, and Access Data FTK are GUI tools designed to perform most computer forensics acquisition and analysis functions.

Software forensics tools are commonly used to copy data from a suspect's drive to an image file. Many GUI acquisition tools can read all structures in an image file as

though the image were the original drive. Many analysis tools, such as ProDiscover, En Case, FTK, X-Ways Forensics, ILook, and others, have the capability to analyze image files. In Chapter 4, you learned how some of these tools are used to acquire data from suspects' drives.

Tasks Performed by Computer Forensics Tools

All computer forensics tools, both hardware and software, perform specific functions. These functions are grouped into five major categories, each with sub functions for further refining data analysis and recovery:

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

In the following sections, you learn how these five functions and associated sub functions apply to computing investigations.

Acquisition, the first task in computer forensics investigations, is making a copy of the original drive. As described in Chapter 4, this procedure preserves the original drive to make sure it doesn't become corrupt and damage the digital evidence. Sub functions in the acquisition category include the following:

- Physical data copy
- Logical data copy
- Data acquisition format

- Command-line acquisition
- GUI acquisition
- Remote acquisition
- Verification

Some computer forensics software suites, such as Access Data FTK and En Case, provide separate tools for acquiring an image. However, some investigators opt to use hardware devices, such as the Logic be Talon, VOOM Hard Copy 3, or Image MASSter Solo III Forensic unit from Intelligent Computer Solutions, Inc., for acquiring an image. These hardware devices have their own built-in software for data acquisition. No other device or program is needed to make a duplicate drive; however, you still need forensics software to analyze the data.

4.1.1 Validation and Discrimination

Two issues in dealing with computer evidence are critical. First is ensuring the integrity of data being copied—the validation process. Second is the discrimination of data, which involves sorting and searching through all investigation data. The process of validating data is what allows discrimination of data. Many forensics software vendors offer three methods for discriminating data values. These are the sub functions of the validation and discrimination function:

- Hashing
- Filtering
- Analyzing file headers

Validating data is done by obtaining hash values. As a standard feature, most forensics

tools and many disk editors have one or more types of data hashing. How data hashing is used depends on the investigation, but using a hashing algorithm on the entire suspect drive and all its files is a good idea. This method produces a unique hexadecimal value for data, used to make sure the original data hasn't changed.

This unique value has other potential uses. For example, in the corporate environment, you could create a known good hash value list of a fresh installation of an OS, all applications, and all known good images and documents (spreadsheets, text files, and so on). With this information, an investigator could ignore all files on this known good list and focus on other files on the disk that aren't on this list. This process is known as filtering. Filtering can also be used to find data for evidence in criminal investigations or to build a case for terminating an employee.

The primary purpose of data discrimination is to remove good data from suspicious data. Good data consists of known files, such as OS files and common programs (Microsoft Word, for example).

Several computer forensics programs can integrate known good file hash sets, such as the ones from the NSRL, and compare them to file hashes from a suspect drive to see whether they match. With this process, you can eliminate large amounts of data quickly so that you can focus your evidence analysis. You can also begin building your own hash sets.

Another feature to consider for hashing functions is hashing and comparing sectors of data. This feature is useful for identifying fragments of data in slack and free disk space that might be partially overwritten.

An additional method of discriminating data is analyzing and verifying header values for known file types. Similar to the hash values of known files, many computer forensics pro- grams include a list of common header values. With this information, you can see whether a file extension is incorrect

for the file type. Renaming file extensions is a common way to try to hide data, and you could miss pertinent data if you don't check file headers.

4.1.2 Extraction

The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.

Recovering data is the first step in analyzing an investigation's data. The following sub functions of extraction are used in investigations:

- Data viewing
- Keyword searching
- Decompressing
- Carving
- Decrypting
- Bookmarking

Many computer forensics tools include a data-viewing mechanism for digital evidence. How data is viewed depends on the tool. Tools such as ProDiscover, X-Ways Forensics, FTK, EnCase, SMART, ILook, and others offer several ways to view data, including logical drive structures, such as folders and files. These tools also display allocated file data and unallocated disk areas with special file and disk viewers. Being able to view this data in its normal form makes analyzing and collecting clues for the investigation easier

.4.2 Computer Forensics Software Tools

Whether you use a suite of tools or a task-specific tool, you have the option of selecting one that enables you to analyze digital evidence through the command line or in a GUI. The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux.

Command-Line Forensics Tools

Computers used several OSs before MS-DOS dominated the market. During this time, computer forensics wasn't a major concern. After people started using PCs, however, they figured out how to use them for illegal and destructive purposes and to commit crimes and civil infractions.

Software developers began releasing computer forensics tools to help private- and public-sector investigators examine PCs. The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems.

One of the first MS-DOS tools used for computer investigations was Norton Disk Edit. This tool used manual processes that required investigators to spend considerable time on a typical 500 MB drive. Eventually, programs designed for computer forensics were developed for DOS, Windows, Apple, NetWare, and UNIX systems. Some of these early programs could extract data from slack and free disk space; others were capable only of retrieving deleted files. Current programs are more robust and can search for specific words or characters, import a keyword list to search, calculate hash values, recover deleted items, conduct physical and logical analyses, and more.

One advantage of using command-line tools for an investigation is that they require few sys- tem resources because they're designed to run in minimal configurations. In fact, most tools fit on bootable media (floppy disk, USB drive, CD, or DVD). Conducting an initial inquiry or a complete investigation with bootable media can

save time and effort. Most tools also produce a text report small enough to fit on a floppy disk.

Forensic Workstations

Many computer vendors offer a wide range of forensic workstations that you can tailor to meet your investigation needs. The more diverse your investigation environment, the more options you need. In general, forensic workstations can be divided into the following categories:

- *Stationary workstation*—A tower with several bays and many peripheral devices
- *Portable workstation*—A laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation
- *Lightweight workstation*—usually a laptop computer built into a carrying case with a small selection of peripheral options

When considering options to add to a basic workstation, keep in mind that PCs have limitations on how many peripherals they can handle. The more peripherals you add, the more potential problems you might have, especially if you're using an older version of Windows. You must learn to balance what you actually need with what your system can handle.

4.3 Validating and Testing Forensics Software

Now that you have selected some tools to use, you need to make sure the evidence you recover and analyze can be admitted in court. To do this, you must test and validate your software. The following sections discuss validation tools available at the time of this writing and how to develop your own validation protocols.

Using National Institute of Standards and Technology (NIST) Tools

The National Institute of Standards and Technology publishes articles, provides tools, and creates procedures for testing and validating computer forensics software. Software should be verified to improve evidence admissibility in judicial proceedings. NIST sponsors the Computer Forensics Tool Testing (CFTT) project to manage research on computer forensics tools.

- Establish categories for computer forensics tools—Group computer forensics software according to categories, such as forensics tools designed to retrieve and trace e-mail.
- Identify computer forensics category requirements—For each category, describe the technical features or functions a forensics tool must have.
- Develop test assertions—Based on the requirements, create tests that prove or diSprove the tool's capability to meet the requirements.
- Identify test cases—Find or create types of cases to investigate with the forensics tool, and identify information to retrieve from a sample drive or other media. For example, use the image of a closed case file created with a trusted forensics tool to test a new tool in the same category and see whether it produces the same results.
- Establish a test method—Considering the tool's purpose and design, specify how to test it.
- Report test results—Describe the test results in a report that complies with ISO 17025, which requires accurate, clear, unambiguous, and objective test reports.

Another standards document, ISO 5725, demands accuracy for all aspects of the testing pro- cess, so results must be repeatable and reproducible. –Repeatable results‖ means that if you work in the same lab on the same machine, you generate the same results. –Reproducible results‖ means that if you're in a different lab working on a different machine, the tool still retrieves the same information.

4.4 Exploring the Role of E-mail in Investigations

E-mail evidence has become an important part of many computing investigations, so computer forensics investigators must know how e-mail is processed to collect this essential evidence. In addition, with the increase in e-mail scams and fraud attempts with phishing or spoofing, investigators need to know how to examine and interpret the unique content of e-mail messages.

As a computing investigator, you might be called on to examine a phishing e-mail to see whether it's authentic. Later, in –Tracing an E-mail Message,‖ you learn about resources for looking up e-mail and Web addresses to verify whether they're associated with a spoofed message.

One of the most noteworthy e-mail scams was 419, or the Nigerian Scam, which originated as a chain letter from Nigeria, Africa. Fraudsters now need only access to Internet e-mail to solicit victims, thus saving postage costs of international mail. Unlike newer, more sophisticated phishing e-mail frauds, 419 messages have certain characteristic ploys and a typical writing style. For example, the sender asks for access to your bank account so that he can transfer his money to it as a way to prevent corrupt government officials in his homeland from confiscating it. The sender often promises to reward you financially if you make a minor payment or allow access to your bank account. The messages are usually in uppercase letters and use poor grammar

4.5 Exploring the Roles of the Client and Server in E-mail

You can send and receive e-mail in two environments: via the Internet or an intranet (an internal network). In both e-mail environments, messages are distributed from a central server to many connected client computers, a configuration called client/server architecture. The server runs an e-mail server program, such as Microsoft Exchange Server, Novell GroupWise, or UNIX Send mail, to provide e-mail services. Client computers use e-mail programs (also called e-mail clients), such as Novell Evolution or Microsoft Outlook, to contact the e-mail server and send and retrieve e-mail messages.

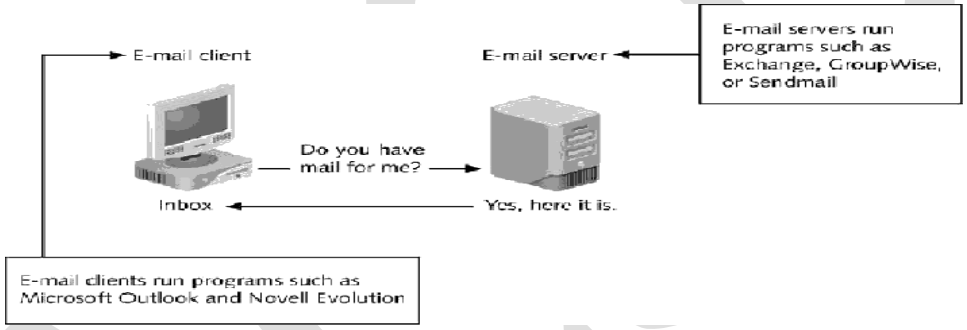


Fig: Role of client and server in E-mail

Regardless of the OS or e-mail program, users access their e-mail based on permissions the e-mail server administrator grants. These permissions prevent users from accessing each other's e-mail. To retrieve messages from the e-mail server, users identify themselves to the server, as when logging on to the network. Then e-mails are delivered to their computers.

E-mail services on both the Internet and an intranet use a client/server architecture, but they differ in how client accounts are assigned, used, and managed and in how users access their e-mail. Overall, an intranet e-mail system is for the private use of network users, and Internet e-mail systems are for public use. On an intranet, the e-mail server

is generally part of the local network, and an administrator manages the server and its services. In most cases, an intranet e-mail system is specific to a company, used only by its employees, and regulated by its business practices, which usually include strict security and acceptable use policies. For example, network users can't create their own e-mail accounts, and usernames tend to follow a naming convention that the e-mail administrator determines.

4.6 Investigating E-mail Crimes and Violations

Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes. Your goal is to find out who's behind the crime or policy violation, collect the evidence, and present your findings to build a case for prosecution or arbitration.

E-mail crimes and violations depend on the city, state, and sometimes country in which the e-mail originated. For example, in Washington State, sending unsolicited e-mail is illegal. However, in other states, it isn't considered a crime. Consult with an attorney for your organization to determine what constitutes an e-mail crime.

Committing crimes with e-mail is becoming commonplace, and more investigators are finding communications that link suspects to a crime or policy violation through e-mail. For example, some people use e-mail when committing crimes such as narcotics trafficking, extortion, sexual harassment, stalking, fraud, child abductions, terrorism, child pornography, and so on. Because e- mail has become a major communication medium, any crime or policy violation can involve e-mail.

4.6.1 Examining E-mail Messages

After you have determined that a crime has been committed involving e-mail, first access the victim's computer to recover the evidence. Using the victim's e-mail client, find and copy any potential evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders. If you can't actually sit down at the

victim's com- puter, you have to guide the victim on the phone to open and print a copy of an offending message, including the header. The header contains unique identifying numbers, such as the IP address of the server that sent the message. This information helps you trace the e-mail to the suspect.

4.6.2 Copying an E-mail Message

Before you start an e-mail investigation, you need to copy and print the e-mail involved in the crime or policy violation. You might also want to forward the message as an attachment to another e- mail address, depending on your organization's guidelines.

The following activity shows you how to use Outlook 2007, included with Microsoft Office, to copy an e-mail message to a USB drive. (*Note*: Depending on the Outlook version you use, the steps might vary slightly.) You use a similar procedure to copy messages in other e-mail programs, such as Outlook Express and Evolution. If Outlook or Outlook Express is installed on your computer, follow these steps:

- Insert a USB drive into a USB port.
- Open Windows Explorer or the Computer window, navigate to the USB drive, and leave this window open.
- Start Outlook by clicking Start, pointing to All Programs, pointing to Microsoft Office, and clicking Microsoft Office Outlook 2007.
- In the Mail Folders pane (see Figure 12-2), click the folder containing the message you want to copy. For example, click the Inbox folder. A list of messages in that folder is displayed in the pane in the middle. Click the message you want to copy.
- Resize the Outlook window so that you can see the message you want to copy and the USB drive icon in Windows Explorer or the Computer window.

- Drag the message from the Outlook window to the USB drive icon in Windows Explorer or the Computer window.
- Click File, Print from the Outlook menu to open the Print dialog box. After printing the e-mail so that you have a copy to include in your final report, exit Outlook.

4.6.3 Viewing E-mail Headers

After you copy and print a message, use the e-mail program that created it to find the e-mail header. This section includes instructions for viewing e-mail headers in a variety of e-mail programs, including Windows GUI clients, a UNIX command-line e-mail program, and some common Web- based e-mail providers. After you open e-mail headers, copy and paste them into a text document so that you can read them with a text editor, such as Windows.

To retrieve an Outlook e-mail header, follow these steps:

- Start Outlook, and then select the original of the message you copied in the previous section.
- Right-click the message and click Message Options to open the Message Options dia- log box. The Internet headers text box at the bottom contains the message header.

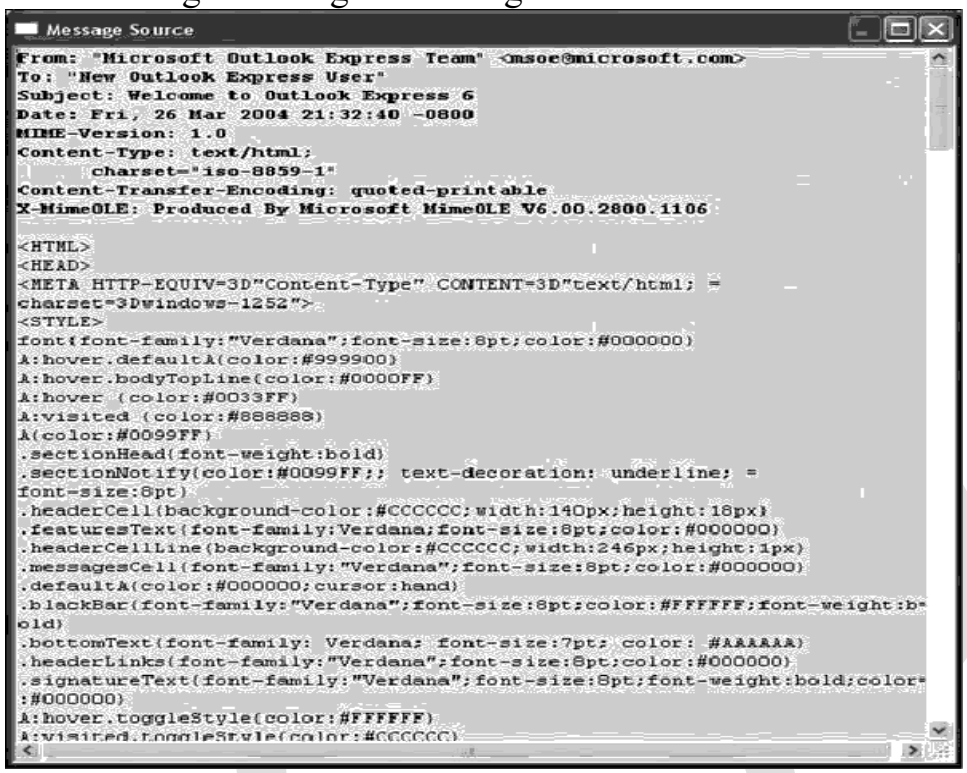
Fig: An Outlook e-mail header

- Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.
- Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Outlook Header.txt in your work folder. Then close the document and exit Outlook. To retrieve an Outlook Express e-mail header, follow these steps:
- Start Outlook Express, and then display the message you want to examine.
- Right-click the message and click Properties to open a dialog box showing general information about the message.

Fig: An Outlook Express e-mail header

- Click the Message Source button to view the e-mail's HTML source code ,which can be helpful in examining possible phishing messages.
- Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.
- Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Outlook Express Header.txt in your work folder, and then exit Notepad.
- Close all open windows and dialog boxes, and then exit Outlook Express.

Fig: Viewing the message's HTML source code



4.7Understanding E-mail Servers

An e-mail server is loaded with software that uses e-mail protocols for its services and maintains logs you can examine and use in your investigation. As a computer forensics investigator, you can't know everything about e-mail servers. Your focus is not to learn how a particular e-mail server works but how to retrieve information about e-mails for an investigation. Usually, you must work closely with the network administrator or e-mail administrator, who is often willing to help you find the data or files you need and might even suggest new ways to find this information. If you can't work with an administrator, conduct research on the Internet or use the forensics tools discussed later in this chapter to investigate the e-mail server software and OS.

To investigate e-mail abuse, you should know how an e-mail server records and handles the e-mail it receives. Some e-mail servers use databases that store users' e-mails, and

others use a flat file system. All e-mail servers can maintain a log of e-mails that are processed. Some e-mail servers are set up to log e-mail transactions by default; others must be configured to do so. Most e-mail administrators log system operations and message traffic to recover e-mails in case of a disaster, to make sure the firewall and e-mail filters are working correctly, and to enforce company policy.

However, the e-mail administrator can disable logging or use circular logging, which over- writes the log file when it reaches a specified size or at the end of a specified time frame. Circular logging saves valuable server space, but you can't recover a log after it's overwritten. For example, on Monday the e-mail server records traffic in the Mon.log file. For the next six days, the e-mail server uses a log for each day, such as Tues.log, Wed.log, and so forth. On Sunday at midnight, the e-mail server starts recording e-mail traffic in Mon.log, overwriting the information logged the previous Monday. The only way to access the log file information is from a backup file, which many e-mail administrators create before a log file is overwritten.

E-mail logs generally identify the e-mail messages an account received, the IP address from which they were sent, the time and date the e-mail server received them, the time and date the client computer accessed the e-mail, the e-mail contents, system-specific information, and any other information the e-mail administrator wants to track. These e-mail logs are usually formatted in plain text and can be read with a basic text editor, such as Notepad or vi.

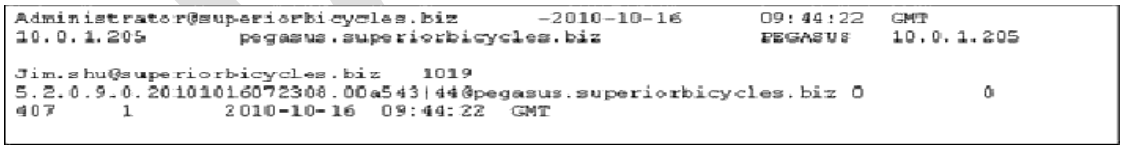


Fig: An e-mail server log file

4.8 Using Specialized E-mail Forensics Tools

For many e-mail investigations, you can rely on e-mail message files, e-mail headers,

and e-mail server log files. However, if you can't find an e-mail administrator willing to help with the investigation, or you encounter a highly customized e-mail environment, you can use data recovery tools and forensics tools designed to recover e-mail files.

As technology has progressed in e-mail and other services, so have the tools for recovering information lost or deleted from a hard drive. In previous chapters, you have reviewed many tools for data recovery, such as ProDiscover Basic and Access Data FTK. You can also use these tools to investigate and recover e-mail files. Other tools, such as the ones in the follow- ing list, are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

- Data Numen for Outlook and Outlook Express
- FINAL e MAIL for Outlook Express and Eudora
- Sawmill-GroupWise for log analysis office_agent.html)
- DBX tract for Outlook Express
- Fookes Aid4Mail and Mail Bag Assistant for Outlook, Thunderbird, and Eudora
- Paraben E-Mail Examiner, configured to recover several e-mail formats
- Access Data FTK for Outlook and Outlook Express
- On track Easy Recovery Email Repair for Outlook and Outlook Express
- R-Tools R-Mail for Outlook and Outlook Express.
- Office Recovery's Mail Recovery for Outlook, Outlook Express, Exchange, Exchange Server, and IBM Lotus Notes

When you use a third-party tool to search for a .db file, for example, you can find where the administrator stores .db files for the e-mail server. To find log files, use .log as the search criteria. You're likely to find at least two logs related to e-mail—one listing logged events for messages and the other listing logged events for accounts accessing e-mail.

FTK, En Case, and other forensics tools enable you to find e-mail database files, personal e-mail files, offline storage files, and log files. Some tools allow you to view messages and other files with a special viewer; others require using a text editor to compare information, such as the date and time stamp, username, domain, and message contents, to determine whether it matches what was found on the victim's computer.

One advantage of using data recovery tools is that you don't need to know how the e-mail server or e-mail client operates to extract data from these computers. Data recovery tools do the work for you and allow you to view evidence on the computer.

After you compare e-mail logs with the messages, you should verify the e-mail account, message ID, IP address, and date and time stamp to determine whether there's enough evidence for a warrant. If so, you can obtain and serve your warrant for the suspect's computer equipment.

4.9 Understanding Mobile Device Forensics

People store a wealth of information on cell phones, and the thought of losing your cell phone and, therefore, the information stored on it can be a frightening prospect. Despite this concern, not many people think about securing their cell phones, although they routinely lock and secure laptops or desktops. Depending on your phone's model, the following items might be stored on it:

- Incoming, outgoing, and missed calls

- Text and Short Message Service (SMS) messages
- E-mail
- Instant messaging (IM) logs
- Web pages
- Pictures
- Personal calendars
- Address books
- Music files
- Voice recordings

Many people store more information on their cell phones than they do on their computers and with this variety of information, piecing together the facts of a case is possible. Recent cases, such as the rape allegations at Duke University and the Scott Peterson murder trial, show that cell phone data is used increasingly in court as evidence. In some countries, cell phones are even used to log in to bank accounts and transfer funds from one cell phone to another, which provides even more potential evidence. This handheld device is one of the most versatile pieces of equipment invented yet.

Despite the usefulness of these devices in providing clues for investigations, investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics. No single standard exists for how and where cell phones store messages, although many phones use similar storage schemes. In addition, new phones come out about every six months, and they're rarely compatible with

previous models. Therefore, the cables and accessories you have might become obsolete in a short time. Also, cell phones are often combined with PDAs, which can make forensics investigations more complex.

Mobile Phone Basics

Since the 1970s, when Motorola introduced cell phones, mobile phone technology has advanced rapidly. Gone are the days of two-pound cell phones that only the wealthy could afford. In the past 40 years, mobile phone technology has developed far beyond what the inventors could have imagined.

Up to the end of 2008, there have been three generations of mobile phones: analog, digital personal communications service (PCS), and third-generation (3G). 3G offers increased band- width, compared with the other technologies:

- 384 Kbps for pedestrian use
- 128 Kbps in a moving vehicle
- 2 Mbps in fixed locations, such as office building.

4.10 Understanding Acquisition Procedures for Cell Phones and Mobile Devices

All mobile devices have volatile memory, so making sure they don't lose power before you can retrieve RAM data is critical. At the investigation scene, determine whether the device is on or off. If it's off, leave it off, but find the recharger and attach it as soon as possible. Note this step in your log if you can't determine whether the device was charged at the time of seizure. If the device is on, check the LCD display for the battery's current charge level.

Because mobile devices are often designed to synchronize with applications on a

user's PC, any mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately. This precaution helps prevent synchronization that might occur automatically on a preset schedule and overwrite data on the device. In addition, collect the PC and any peripheral devices to determine whether the hard drive contains any information that's not on the mobile device.

Depending on the warrant or subpoena, the time of seizure might be relevant. In addition, messages might be received on the mobile device after seizure that may or may not be admissible in court. If you determine that the device should be turned off to preserve battery power or a possible attack, note the time and date at which you take this step. The alternative is to isolate the device from incoming signals with one of the following options:

- Place the device in paint can, preferably one that previously contained radio wave– blocking paint.
- Use the Paraben Wireless Strong Hold Bag which conforms to Faraday wire cage standards.
- Use eight layers of antistatic bags (for example, the bags that new hard drives are wrapped in) to block the signal.

The drawback of using these isolating options is that the mobile device is put into roaming mode, which accelerates battery drainage. NIST suggests supplying a portable means of power, such as a battery-powered charger, to prevent this problem. Newer mobile devices shut themselves off or enter a –sleep state after reaching a certain low battery level.

As mentioned, memory resides in the phone itself and in the SIM card, if the device is equipped with one. The file system for a SIM card is a hierarchical structure. This file structure begins with the root of the system (MF). The next level consists of

directory files (DF), and under them are files containing elementary data (EF). EFs under the GSM and DCS1800 DFs contain network data on different frequency bands of operation. The EFs under the Telecom DF contain service-related data.

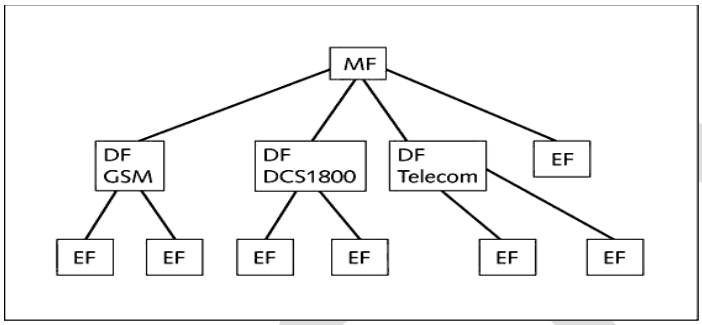


Fig: SIM file structure

You can retrieve quite a bit of data from a SIM card. The information that can be retrieved falls into four categories:

- Service-related data, such as identifiers for the SIM card and subscriber
- Call data, such as numbers dialed
- Message information
- Location information

If power has been lost, you might need PINs or other access codes to view files. Typically, users keep the original PIN assigned to the SIM card, so when you're collecting evidence at he scene, look for users' manuals and other documentation that can help you access the SIM card. With most SIM cards, you have three attempts at entering an access code before the device is locked, which then requires calling the service provider or waiting a certain amount of time before trying again. Common codes to try are 1-1-1-1 or 1-2-3-4.

SIM Card Readers With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/ software device called a SIM card reader. To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you're ready to proceed to this step. The general procedure is as follows:

- Remove the back panel of the device.
- Remove the battery.
- Under the battery, remove the SIM card from its holder.
- Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.

A variety of SIM card readers are on the market. Some are forensically sound and some are not; make sure you note this feature of the device in your investigation log. Another problem with SIM card readers is dealing with text and SMS messages that haven't been read yet. After you view a message, the device shows the message as opened or read. For this reason, documenting messages that haven't been read is critical. Using a tool that takes pictures of each screen can be valuable in this situation. These screen captures can provide additional documentation.

IPhone Forensics Because the iPhone is so popular, its features are copied in many other mobile devices. The wealth of information that can be stored on this device makes iPhone forensics particularly challenging. At first, many researchers and hackers tried to find a way to

–crack‖ the iPhone but were unsuccessful because the device is practically impenetrable. A more fruitful approach was hacking backup files. However, this

method does have limitations: You can access only files included in a standard backup, so deleted files, for example, can't be accessed

UNIT –V

WORKING WITH WINDOWS and DOS SYSTEMS

5.1. Understanding file systems

To investigate computer evidence effectively, you must understand how the most commonly used OSs work and how they store files. In addition to this section on file systems, you should review books on Computer Technology Industry Association. A file system gives an OS a road map to data on a disk. The type of file system an OS uses determines how data is stored on the disk. A file system is usually directly related to an OS, although some vendors grandfather in previous OSs so that newer ones can read them. For example, most current Linux releases can access disks configured in the older Linux Ext2fs and Ext3fs file systems.

No matter which platform you use, you need to know how to access and modify system settings when necessary. When you need to access a suspect's computer to acquire or inspect data related to your investigation, you should be familiar with the computer's plat- form.

Understanding the Boot Sequence:

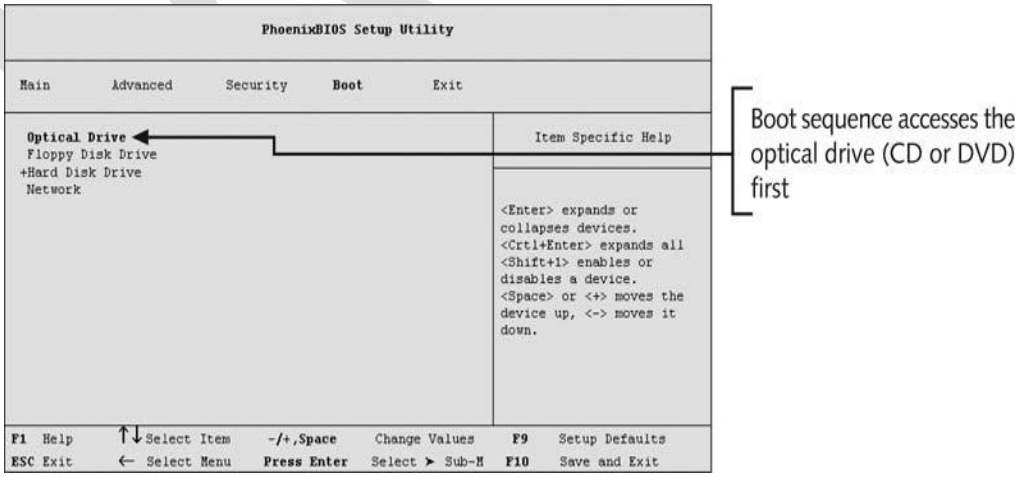
To ensure that you don't contaminate or alter data on a suspect's Windows or DOS PC, you must know how to access and modify a PC's Complementary Metal Oxide Semi- conductor (CMOS) and Basic Input/ Output System (BIOS) settings. A computer stores system configuration and date and time information in the CMOS when power to the system is off. The system BIOS contains programs that perform input and output at the hardware level.

When a subject's computer starts, you must make sure it boots to a forensic floppy

disk or CD, because booting to the hard disk overwrites and changes evidentiary data. To do this, you access the CMOS setup by monitoring the subject's computer during the initial bootstrap process to identify the correct key or keys to use. The bootstrap process is contained in ROM and tells the computer how to proceed. As the computer starts, the screen usually displays the key or keys, such as the Delete key; you press to open the CMOS setup screen. You can also try unhooking the keyboard to force the system to tell you what keys to use. The key you press to access.

CMOS depends on the computer's BIOS. The popular BIOS manufacturers Award and AMI use the Delete key to access CMOS; other manufacturers use Ctrl+Alt+Insert, Ctrl+A, Ctrl+A, or Ctrl+F1, F2, and F10.

Figure shows a typical CMOS setup screen, where you check a computer's boot sequence. If necessary, you can change the boot sequence so that the OS accesses the CD/ DVD drive or a floppy drive (if available) before any other boot device. Each BIOS vendor's screen is different,but you can refer to the vendor's documentation or Web site for instructions on changing the boot sequence.



Understanding Disk Drives:

You should be familiar with disk drives and how data is organized on a disk so that you can find data effectively. Disk drives are made up of one or more platters coated with magnetic material, and data is stored on platters in a particular way. For additional information on disk drive configurations, see *www.storagereview.com/guide2000/ref/hdd/index.html*. Follow- ing is a list of disk drive components:

- *Geometry*—Geometry refers to a disk's structure of platters, tracks, and sectors.
- *Head*—the head is the device that reads and writes data to a drive. There's one head per platter.
- *Tracks*—Tracks are concentric circles on a disk platter where data is located.
- *Cylinders*—a cylinder is a column of tracks on two or more disk platters. Typically, each platter has two surfaces: top and bottom.

Sectors—a sector is a section on a track, usually made up of 512 bytes

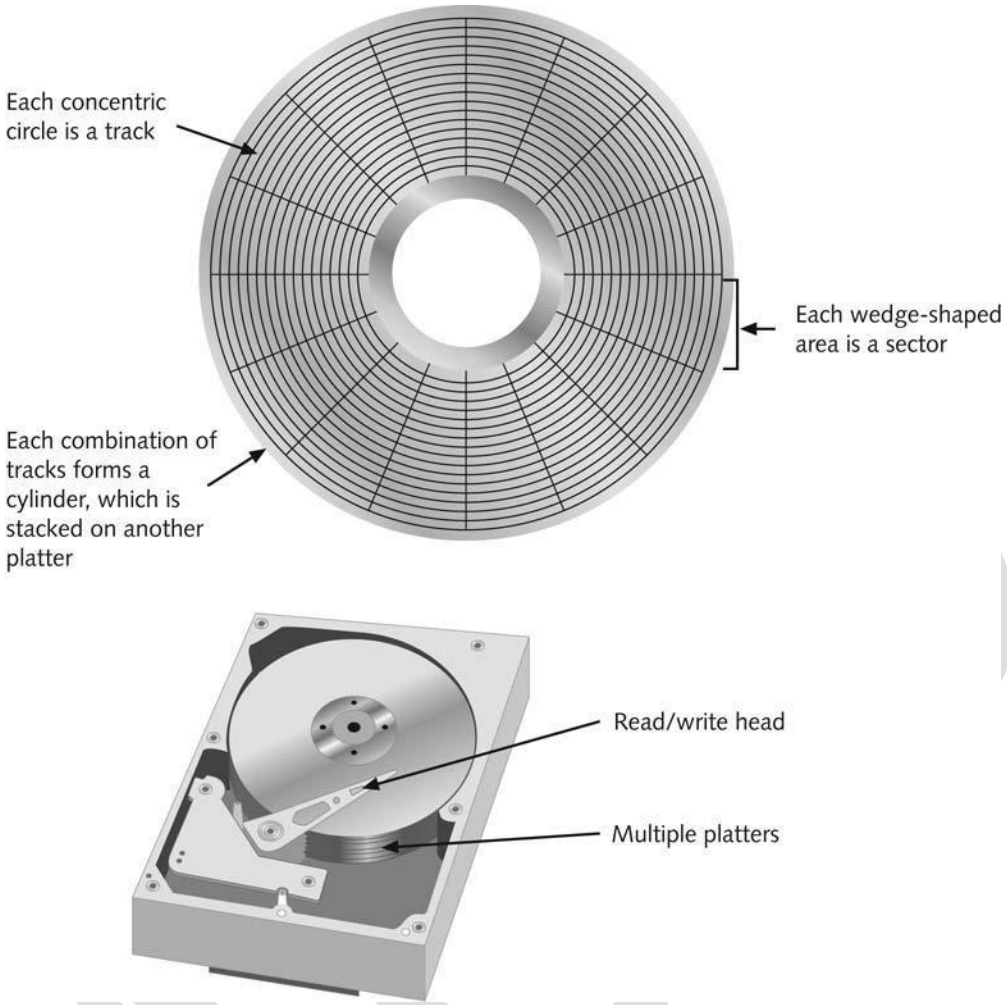


Fig : disk drives

5.2 Exploring Microsoft File Structures

Because most PCs use Microsoft software products, you should understand Microsoft file systems so that you know how Windows and DOS computers store files. In particular, you need to understand clusters, File Allocation Table (FAT), and New Technology File System (NTFS). The method an OS uses to store files determines where data can be hidden. When you examine a computer for forensic evidence, you need to explore these hiding places to determine whether they contain files or parts of files that might be evidence of a crime or policy violation. The manufacturer engineers a disk to have a certain number of sectors per track, and a typical disk drive stores 512 bytes per

sector. To determine the total number of addressable bytes on a disk, multiply the number of cylinders by the number of heads (actually tracks) and by the number of sectors (groups of 512 or more bytes). In Microsoft file structures, sectors are grouped to form clusters, which are storage allocation units of one or more sectors. Clusters are typically 512, 1024, 2048, 4096, or more bytes each. Combining sectors minimizes the overhead of writing or reading files to a disk. The OS groups one or more sectors into a cluster. The number of sectors in a cluster varies according to the disk size. For example, a double-sided floppy disk has one sector per cluster; a hard disk has four or more sectors per cluster.

Clusters are numbered sequentially starting at 2 because the first sector of all disks contains a system area, the boot record, and a file structure database. The OS assigns these cluster numbers, which are referred to as logical addresses. These addresses point to relative cluster positions; for example, cluster address 100 is 98 clusters from cluster address

Sector numbers, however, are referred to as physical addresses because they reside at the hardware or firmware level and go from address 0 (the first sector on the disk) to the last sector on the disk. Clusters and their addresses are specific to a logical disk drive, which is a disk partition.

Disk Partitions

Many hard disks are partitioned, or divided, into two or more sections. A partition is a logi- cal drive. For example, an 8 GB hard disk might contain four partitions or logical drives. FAT16 does not recognize disks larger than 2 MB, so these disks have to be partitioned into smaller sections for FAT to recognize the additional space. Someone who wants to hide data on a hard disk can create hidden partitions or voids—large unused gaps between partitions on a disk drive. For example, partitions containing unused space (voids) can be created between the primary partition and

the first logical partition. This unused space between partitions is called the partition gap. If data is hidden in a partition gap, a disk editor utility could also be used to alter information in the disk's partition table. Doing so removes all references to the hidden partition, concealing it from the computer's OS. Another technique is to hide incriminating digital evidence at the end of a disk by declaring a smaller number of bytes than the actual drive size. With disk-editing tools, however, you can access these hid- den or empty areas of the disk.

One way to examine a partition's physical level is to use a disk editor, such as Norton Disk- Edit,

WinHex, or Hex Workshop. These tools enable you to view file headers and other critical parts of a file. Both tasks involve analyzing the key hexadecimal codes the OS uses to identify and maintain the file system. Table 5-1 lists the hexadecimal codes in a partition table and identifies some common file system structures.

Hexadecimal code	File system
01	DOS 12-bit FAT
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
17	Hidden NTFS partition (XP and earlier)

1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66–69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Reiser, Xiafs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

Table 5-1 Hexadecimal codes in the partition table

1. If necessary, download Hex Workshop from BreakPoint Software and install it. Check with your instructor about where you should install it on your computer.
2. Insert a USB drive into a USB port.
3. Start Hex Workshop by right-clicking the Hex Workshop desktop icon and clicking Run as administrator, and then clicking the Continue button in the UAC message box.
4. In Hex Workshop, click Disk, Open Drive from the menu to see a list of your logical drives. Click the C: drive (or your working drive), and click OK.

5. Click Disk, Open Drive again, but this time, in the Open Drive drop-down list, click your USB drive, and then click OK. Compare the file system label for this drive to the one you saw in Step 4. Leave Hex Workshop open for the next activity.

With tools such as Hex Workshop, you can also identify file headers to identify file types with or without an extension. Before performing the following steps in Hex Workshop, use Windows Explorer or My Computer to find a folder on your system containing a bitmap (.bmp) file and a folder containing a Word document (.doc). Then follow these steps:

1. To open a bitmap file on your computer, click File, Open from the Hex Workshop menu. Navigate to a folder containing a bitmap (.bmp) file, and then double-click the .bmp file. (If you're prompted to select any bookmarks, click Cancel and continue with this activity.)
2. Hex Workshop window identifies the file type for the graphic. For .bmp files, it shows –BM6,‖ –BM,‖ or –BMF.‖ As shown in the figure, –42 4D‖ is also displayed toindicate a .bmp file.
3. To open a Word document, click File, Open from the menu. Navigate to a folder containing a Word document (.doc) file, and then double-click the .doc file. As shown in Figure 6-6, the first line contains a row of 0s followed by –D0 CF 11 E0 A1 B1 1A E1,‖ which identifies the file as a Microsoft Office document. The same file header is displayed for an Excel or a PowerPoint file but doesn't apply to Access databases.
4. Exit Hex Workshop.

5.3 Examining NTFS Disks

New Technology File System (NTFS) was introduced when Microsoft created Windows NT and is the primary file system for Windows Vista. Each generation of Windows since NT has included minor changes in NTFS configuration and features. The NTFS design was partially based on, and incorporated many features from, Microsoft's project for IBM with the OS/2 operating system; in this OS, the file system was High Performance File System (HPFS). When Microsoft created Windows NT, it provided backward compatibility so that NT could read OS/2 HPFS disk drives. Since the release of Windows 2000, this back- ward compatibility is no longer available.

NTFS offers significant improvements over FAT file systems. It provides more information about a file, including security features, file ownership, and other file attributes. With NTFS, you also have more control over files and folders (directories) than with FAT file systems.

In NTFS, everything written to the disk is considered a file. On an NTFS disk, the first data set is the Partition Boot Sector, which starts at sector [0] of the disk and can expand to 16 sectors. Immediately after the Partition Boot Sector is the Master File Table (MFT). The MFT, similar to FAT in earlier Microsoft OSs, is the first file on the disk. An MFT file is cre- ated at the same time a disk partition is formatted as an NTFS volume and usually consumes about 12.5% of the disk when it's created. As data is added, the MFT can expand to take up 50 % of the disk. An important advantage of NTFS over FAT is that it results in much less file slack space. Compare the cluster sizes in Table 5-3 to Table 5-2, which showed FAT cluster sizes. Clusters are smaller for smaller disk drives. This feature saves more space on all disks using NTFS.

Drive size	Sectors per cluster	FAT16
0–32 MB	1	512 bytes
33–64 MB	2	1 KB
65–128 MB	4	2 KB
129–255 MB	8	4 KB
256–511 MB	16	8 KB
512–1023 MB	32	16 KB
1024–2047 MB	64	32 KB
2048–4095 MB	128	68 KB

Table 5-2 Sectors and bytes per cluster

Drive size	Sectors per cluster	Cluster size
0–512 MB	1	512 bytes
512 MB–1 GB	2	1024 bytes
1–2 GB	4	2048 bytes
2–4 GB	8	4096 bytes
4–8 GB	16	8192 bytes
8–16 GB	32	16,384 bytes
16–32 GB	64	32,768 bytes
More than 32 GB	128	65,536 bytes

Table 5-3 Cluster sizes in an NTFS disk

NTFS System Files

Because everything on an NTFS disk is a file, the first file, the MFT, contains information about all files on the disk, including the system files the OS uses. In the MFT, the first 15 records are reserved for system files. Records in the MFT are referred to as metadata. Table 6-4 lists the first 16 metadata records you find in the MFT.

Filename	System file	Record position	Description
$Mft	MFT	0	Base file record for each folder on the NTFS volume; other record positions in the MFT are allocated if more space is needed.
$MftMirr	MFT 2	1	The first four records of the MFT are saved in this position. If a single sector fails in the first MFT, the records can be restored, allowing recovery of the MFT.
$LogFile	Log file	2	Previous transactions are stored here to allow recovery after a system failure in the NTFS volume.
$Volume	Volume	3	Information specific to the volume, such as label and version, is stored here.
$AttrDef	Attribute definitions	4	A table listing attribute names, numbers, and definitions.
$	Root filename index	5	This is the root folder on the NTFS volume.
$Bitmap	Boot sector	6	A map of the NTFS volume showing which

			clusters are in use and which are available.
$Boot	Boot sector	7	Used to mount the NTFS volume during the bootstrap process; additional code is listed here if it's the boot drive for the system.
$BadClus	Bad cluster file	8	For clusters that have unrecoverable errors, an entry of the cluster location is made in this file.
$Secure	Security file	9	Unique security descriptors for the volume are listed in this file. It's where the access control list (ACL) is maintained for all files and folders on the NTFS volume.
$Upcase	Upcase table	10	Converts all lowercase characters to uppercase Unicode characters for the NTFS volume.
$Extend	NTFS extension file	11	Optional extensions are listed here, such as quotas, object identifiers, and reparse point data.
		12–15	Reserved for future use.

Table 5-2 Metadata records in the MFT

MFT and File Attributes

When Microsoft introduced NTFS, the way the OS stores data on disks changed signifiy. In the NTFS MFT, all files and folders are stored in separate records of 1024 bytes Each record contains file or folder information. This information is divided into record fields containing metadata about the file or folder and the file's data or links to the file's data. A record field is referred to as an attribute ID.

File or folder information is typically stored in one of two ways in an MFT record: resident and nonresident. For very small files, about 512 bytes or less, all file metadata and data are stored in the MFT record. These types of records are called resident files because all their

information is stored in the MFT record.

Files larger than 512 bytes are stored outside the MFT. The file or folder's MFT record pro- vides cluster addresses where the file is stored on the drive's partition. These cluster addresses are referred to as data runs. This type of MFT record is called nonresident because the file's data is stored in its own separate file outside the MFT.

MFT Structures for File Data

When viewing an MFT record with a hexadecimal editor, such as WinHex, the data is displayed in little endian format, meaning it's read from right to left. For example, the hexadecimal value 400 is displayed as 00 04 00 00, and the number 0x40000 is displayed as 00 00 04 00.

The first section of an MFT record is the header that defines the size and starting position of the first attribute. Following the header are the attributes that are specific for the file type, such as an application file or a data file. MFT records for directories and system files have additional attributes that don't appear in a file MFT record. The following sections explain how data files are configured in the MFT.

MFT Header Fields

For the header of all MFT records, the record fields of interest are as follows:

- *At offset 0x00*—The MFT record identifier FILE; the letter F is at offset 0.
- *At offset 0x1C to 0x1F*—Size of the MFT record; the default is 0x400 (1024) bytes, or two sectors.
- *At offset 0x14*—Length of the header, which indicates where the next attribute starts; it's typically 0x38 bytes.

- *At offset 0x32 and 0x33*—The update sequence array, which stores the 2 two bytes of the first sector of the MFT record. It's used only when MFT data exceeds 512 bytes. The update sequence array is used as a checksum for record integrity validation.

NTFS Compressed Files

To improve data storage on disk drives, NTFS provides compression similar to FAT Drive- Space 3, a Windows 98 compression utility. Under NTFS, files, folders, or entire volumes can
be compressed. With FAT16, you can compress only a volume. On a Windows Vista, XP, 2000, or NT system, compressed data is displayed normally when you view it in Windows Explorer or applications such as Microsoft Word.

During an investigation, typically you work from an image of a compressed disk, folder, or file. Most computer forensics tools can uncompress and analyze compressed Windows data, including data compressed with the Lempel-Ziv-Huffman (LZH) algorithm and in formats such as PKZip, WinZip, and GNU gzip. Forensics tools might have difficulty with third- party compression utilities, such as the RAR format. If you identify third-party compressed data, you need to uncompress it with the utility that created it.

NTFS Encrypting File System (EFS)

When Microsoft introduced Windows 2000, it added built-in encryption to NTFS called Encrypting File System (EFS). EFS implements a public key and private key method of encrypting files, folders, or disk volumes (partitions). Only the owner or user who encrypted the data can access encrypted files. The owner holds the private

key, and the public key is held by a certificate authority, such as a global registry, network server, or company such as VeriSign.

When EFS is used in Windows Vista Business Edition or higher, XP Professional, or 2000, a recovery certificate is generated and sent to the local Windows administrator account. The purpose of the recovery certificate is to provide a mechanism for recovering encrypted files under EFS if there's a problem with the user's original private key. The recovery key is stored in one of two places. When the user of a network workstation initiates EFS, the recovery key is sent to the local domain server's administrator account. If the workstation is standalone, the recovery key is sent to the workstation's administrator account.

EFS Recovery Key Agent

The Recovery Key Agent implements the recovery certificate, which is in the Windows administrator account. Windows administrators can recover a key in two ways: through Windows or from an MS-DOS command prompt. These three commands are available from the MS-DOS command prompt:

- Cipher
- Copy
- Efsrecvr (used to decrypt EFS files)

Deleting NTFS Files

Typically, you use Windows Explorer to delete files from a disk. When a file is deleted in Windows NT and later, the OS renames it and moves it to the Recycle Bin. Another method is using the Del (delete) MS-DOS command. This method doesn't rename and move the file to the Recycle Bin, but it eliminates the file from

the MFT listing in the same way FAT does.

When you delete a file in Windows Explorer, you can restore it from the Recycle Bin. The OS takes the following steps when you delete a file or a folder in Windows Explorer:

1. Windows changes the filename and moves the file to a subfolder with unique identity in the Recycle Bin.
2. Windows stores information about the original path and filename in the Info2 file, which is the control file for the Recycle Bin. It contains ASCII data, Unicode data, and the date and time of deletion for each file or folder.

Examining Microsoft BitLocker

Microsoft's utility for protecting drive data is called BitLocker, available only with Vista Enterprise and Ultimate editions. BitLocker's current hardware and software requirements are as follows:

- A computer capable of running Windows Vista
- The TPM microchip, version 1.2 or newer
- A computer BIOS compliant with Trusted Computing Group (TCG)
- Two NTFS partitions for the OS and an active system volume with 1.5 GB available space
- The BIOS configured so that the hard drive boots first before checking the CD/DVD drive or other bootable peripherals

5.4 Windows Registry

When Microsoft created Windows 95, it consolidated initialization (.ini) files into the Reg- istry, a database that stores hardware and software configuration

information, network con- nections, user preferences (including usernames and passwords), and setup information. The Registry has been updated and is still used in Windows Vista.

For investigative purposes, the Registry can contain valuable evidence. To view the Registry, you can use the Regedit (Registry Editor) program for Windows 9x and Regedt32 for Windows 2000, XP, and Vista. For more information on how to use Regedit and Regedt32, see the Microsoft Windows Resource Kit documentation for the OS.

Exploring the Organization of the Windows Registry

The Windows Registry is organized in a specific way that has changed slightly with each new version of Windows. However, the major Registry sections have been consistent, with some minor changes, since Windows 2000; they're slightly different in Windows 9x/Me. Before proceeding, review the following list of Registry terminology:

- *Registry*—A collection of files containing system and user information.
- *Registry Editor*—A Windows utility for viewing and modifying data in the Registry. There are two Registry Editors: Regedit and Regedt32.
- *HKEY*—Windows splits the Registry into categories with the prefix HKEY_. Windows 9x systems have six HKEY categories and Windows 2000 and later have five. Windows programmers refer to the ―H‖ as the handle for the key.
- *Key*—Each HKEY contains folders referred to as keys. Keys can contain other key folders or values.
- *Sub key*—A key displayed under another key is a subkey, similar to a subfolder in Windows Explorer.

- *Branch*—A key and its contents, including sub keys, make up a branch in the Registry.

- *Value*—A name and value in a key; it's similar to a file and its data content.

- *Default value*—All keys have a default value that may or may not contain data.

- *Hives*—Hives are specific branches in HKEY_USER and HKEY_LOCAL_MACHINE. Hive branches in HKEY_LOCAL_MACHINE\Software are SAM, Security, Components, and System. For HKEY_USER, each user account has its own hive link to Ntuser.dat.

Examining the Windows Registry

Some forensics tools, such as ProDiscover and FTK, have built-in Registry viewers. For this next activity, your company's Legal Department has asked you to search for any references to the Superior Bicycles company and e-mail addresses containing the name Denise. A parale- gal tells you the home page for Superior Bicycles (*www.superiorbicycles.biz*) and gives you a ProDiscover .eve file containing the image of a Windows 98 computer belonging to a Superior Bicycle employee named Denise Robinson.For this activity, you use ProDiscover Basic to extract System.dat and User.dat from the image file, and then use Access Data Registry Viewer to see what information you can find in these files. If you find any items of interest, you copy the Registry path and name to a text file that you can give to the paralegal. Although the file is an image of a Windows 98 computer, you can use Windows XP or Vista to run ProDiscover Basic and Access Data Registry Viewer in the following activities. Registry Viewer can run in Windows 9x and later and analyze all Windows Registry versions.

To extract Registry files with ProDiscover Basic, follow these steps:

1. Start ProDiscover Basic with the Run as administrator option. If the Launch Dialog box opens, click Cancel.
2. Click File, New Project from the menu.
3. In the New Project dialog box, type InChap06 in the Project Number text box and the Project File Name text box, and then click OK.
4. In the tree view of the main window, click to expand Add and then click Image File.
5. In the Open dialog box, navigate to your work folder, click the GCFI-Win98.eve image file, and click Open. Click Yes in the Auto Image Checksum message box, if necessary.Click the Search toolbar button. In the Search dialog box, click the Content Search

1. Click the Search for files named option button, and in the Search text box, type system.dat and user.dat. Under Select the Disk(s)/Image(s) you want to search in, click the image file (see Figure 6-26), and then click OK.
2. In the search results, click the check box next to the SYSTEM.DAT file. When the Add Comment dialog box opens, type Registry files to extract, click the Apply to all items check box, and then click OK (see Figure 6-27).
3. Click the check box next to the USER.DAT file, and then click Tools, Copy Selected Files from the menu. In the Choose Destination dialog box, click Browse. In the Browse for Folder dialog box, navigate to and click your work folder, and then click OK. Click OK again in the Choose Destination dialog box.
4. Exit ProDiscover Basic, saving the project if prompted.

5.5 Microsoft Startup Tasks

You should have a good understanding of what happens to disk data at startup. In some investigations, you must preserve data on the disk exactly as the suspect last used it. Any access to a computer system after it was used for illicit purposes alters your disk evidence. As you learned in Chapter 4, altering disk data lessens its evidentiary quality considerably. In some instances, accessing a suspect computer incorrectly could make the digital evidence corrupt and less credible for any litigation.

In the following sections, you learn what files are accessed when Windows starts. This information helps you determine when a suspect's computer was last accessed, which is particularly important with computers that might have been used after an incident was reported.

Startup in Windows NT and Later

Although Windows NT is much different from Windows 95 and 98, the startup method for the NT OSs—NT, 2000, XP, and Vista—is about the same. There are some minor differences in how certain system start files function, but basically, they accomplish the same orderly startup.

All NTFS computers perform the following steps when the computer is turned on:

- Power-on self test (POST)
- Initial startup
- Boot loader
- Hardware detection and configuration
- Kernel loading
- User logon

Windows OSs use the files discussed in the following sections to start. These files can be located on the system partition or boot partition.

Startup Files for Windows Vista When Microsoft developed Vista, it updated the boot process to use the new Extensible Firmware Interface (EFI) as well as the older BIOS sys- tem. The EFI boot firmware is designed to provide better protection against malware than BIOS does. EFI Vista's boot processes have also changed since Windows XP. The Ntldr program in Windows XP used to load the OS has been replaced with these three boot utilities:

- *Bootmgr.exe*—The Windows Boot Manager program controls boot flow and allows booting multiple OSs, such as booting Vista along with XP.
- *Winload.exe*—The Windows Vista OS loader installs the kernel and the Hardware Abstraction Layer (HAL) and loads memory with the necessary boot drivers.
- *Winresume.exe*—This tool restarts Vista after the OS goes into hibernation mode.

Startup Files for Windows XP unless otherwise specified, most startup files for Windows XP are located in the root folder of the system partition. The NT Loader (Ntldr) file loads the OS. When the system is powered on, Ntldr reads the Boot.ini file, which dis- plays a boot menu. After you select the mode to boot to, Boot.ini runs Ntoskrnl.exe and reads Bootvid.dll, Hal.dll, and startup device drivers. Boot.ini specifies the Windows XP path installation and contains options for selecting the Windows version.

If a system has multiple boot OSs, including older ones such as Windows 9x or DOS, Ntldr reads BootSect.dos (a hidden file), which contains the address (boot sector location) of each OS.

When the boot selection is made, Ntldr runs NTDetect.com, a 16-bit real-mode program that queries the system for device and configuration data, and then passes its findings to Ntldr. This program identifies components and values on the computer system, such as the following:

- CMOS time and date value
- Buses attached to the motherboard, such as Industry Standard Architecture (ISA) or Peripheral Component Interconnect (PCI)
- Disk drives connected to the system
- Mouse input devices connected to the system