Chapter – 10

" Collecting and Preserving Digital Evidence"

This chapter provides an overview of the role evidence plays in a criminal case (particularly in a cybercrime case) and discusses standard procedures for dealing with digital evidence

Book Reference: Shinder L. D., Cross M., Scene of the Cybercrime, Syngress.

Outline

- Understanding the Role of Evidence in a Criminal Case
- Defining Evidence
- Admissibility of Evidence
- Forensic Examination Standards
- Collecting Digital Evidence
- Evidence Collection
- Preserving Digital Evidence
- Preserving Volatile Data
- Special Considerations
- Recovering Digital Evidence
- Deleted Files
- Computer Forensic Information
- Understanding Legal Issues
- Searching and Seizing Digital Evidence

UCS648: CYBER FORENSICS

L	T	P	Cr
2	0	2	3.0

Course Objectives: To maintain an appropriate level of awareness, knowledge and skill required to understand and recreate the criminal terminology and Cyber Forensics investigation process.

Introduction to Cybercrime: Defining Cybercrime, Understanding the Importance of Jurisdictional Issues, Quantifying Cybercrime, Differentiating Crimes That Use the Net from Crimes That Depend on the Net, working toward a Standard Definition of Cybercrime, Categorizing Cybercrime, Developing Categories of Cybercrimes, Prioritizing Cybercrime Enforcement, Reasons for Cybercrimes.

Understanding the People on the Scene: Understanding Cybercriminals, Profiling Cybercriminals, Categorizing Cybercriminals, Understanding Cyber victims, Categorizing Victims of Cybercrime, Making the Victim Part of the Crime-Fighting Team, Understanding Cyber investigators, Recognizing the Characteristics of a Good Cyber investigator, Categorizing Cyber investigators by Skill Set.

Computer Investigation Process: Demystifying Computer/Cybercrime, Investigating Computer Crime, How an Investigation Starts, Investigation Methodology, Securing Evidence, Before the Investigation, Professional Conduct, Investigating Company Policy Violations, Policy and Procedure Development, Policy Violations, Warning Banners, Conducting a Computer Forensic Investigation, The Investigation Process, Assessing Evidence, Acquiring Evidence, Examining Evidence, Documenting and Reporting Evidence, Closing the Case.

Acquiring, Duplicating and Recovering Deleted Files: Recovering Deleted Files and Deleted Partitions, recovering "Deleted" and "Erased" Data, Data Recovery in Linux, Recovering Deleted Files, Recovering Deleted Partitions, Data Acquisition and Duplication, Data Acquisition Tools, Recovering Data from Backups, Finding Hidden Data, Locating Forgotten Evidence, Defeating Data Recovery Techniques.

Collecting and Preserving Evidence: Understanding the Role of Evidence in a Criminal Case, Defining Evidence, Admissibility of Evidence, Forensic Examination Standards, Collecting Digital Evidence, Evidence Collection, Preserving Digital Evidence, Preserving Volatile Data, Special Considerations, Recovering Digital Evidence, Deleted Files, Computer Forensic Information, Understanding Legal Issues, Searching and Seizing Digital Evidence

Building the Cybercrime Case: Major Factors Complicating Prosecution, Difficulty of Defining the Crime, Jurisdictional Issues, The Nature of the Evidence, Human Factors, Overcoming Obstacles to Effective Prosecution, The Investigative Process, Investigative Tools, Steps in an Investigation, Defining Areas of Responsibility.

Self-Learning Contents:

Introduction

- The field of computer forensics involves identifying, extracting, documenting, and preserving information that is stored or transmitted in electronic or magnetic form (that is, digital evidence).

- Like fingerprints, digital evidence can be visible (such as files stored on disk that can be accessed via the normal directory structure using standard file management tools such as Windows Explorer) or it can be latent (not readily visible or accessible, requiring some sort of processing—via special software or techniques—to locate and identify it).

- Computer forensics involves finding and evaluating this "hidden data" for its evidentiary value.

- Computer forensics standards have been developed that apply to the collection and preservation of digital evidence, which differs in nature from most other types of evidence.

Introduction

- Adopting procedures that are proper, accepted, and prescribed by law in dealing with evidence is vital to the successful prosecution of a cybercrime case.
- The proper handling of these procedures comes into play at two different time points in a trial:
  1. If evidence is not collected and handled according to the proper standards, the judge may deem the evidence inadmissible when it is presented (usually based on the opposing attorney's *motion to suppress) and* the jury members will never get a chance to evaluate it or consider it in making their decision.
  2. If the evidence is admitted, the opposing attorney will attack its credibility during questioning of the witnesses who testify regarding it. Such an attack can create doubt in jury members' minds that will cause them to disregard the evidence in making their decision and perhaps even taint the credibility of the entire case.
- Thus, proper handling of evidence is one of the most important issues facing all criminal investigations.

Understanding the Role of Evidence in a Criminal Case

- The process of collecting, examining, preserving, and presenting evidence is a legal process and is governed by the laws of the jurisdiction of the court in which the evidence will be introduced.

- Thus it is extremely important for investigators to become familiar with the applicable laws. These rules are adopted by statute and are usually codified into a document titled *Rules of Evidence.*

- Evidence must be *authenticated i.e.* some witness must testify to its authenticity.

- In the case of digital evidence, witness is someone:
  1. Who has personal knowledge of the evidence (for example, a person who shared the computer with the accused and observed the document or file in question on the computer).
  2. Could also be the first responder who saw the evidence on screen when responding to the incident.
  3. An expert who examined the evidence after it was seized.

- Important aspects of preparing to introduce evidence in court is
  - determining which witnesses will testify as to its existence and validity,
  - describe the circumstances of its discovery, and
  - verify that it has not been tampered with.

Defining Evidence

Evidence can be defined as the means by which an alleged fact, the truth of which is subjected to scrutiny, is established or disproved.

There are three categories of evidence:

1. **Physical evidence (sometimes called *real evidence)*** Consists of tangible objects that can be seen and touched.
2. **Direct testamentary evidence** The testimony of a witness who can give an account of facts based on personal experience through the use of the five senses.
3. **Circumstantial evidence** Not based on personal observation of the offense but on observation or knowledge of facts that tend to support a conclusion indirectly but do not prove it definitively.

- It is the *totality of the evidence in the minds* of the jury members that matters—whether all that evidence, taken together, persuades them beyond a reasonable doubt that the defendant committed the crime.
- Under best-evidence rule, **the original** document must be presented as evidence unless it has been destroyed or falls under other exceptions.

  "If data are stored by computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."

- The burden is on the party introducing the evidence to show that it does indeed reflect the data accurately.
- Also, It must be proven that the evidence is what it is claimed to be and that it hasn't been changed since it was taken into custody. Otherwise, the evidence will be deemed inadmissible.

- **Most criminals are convicted based on circumstantial evidence** because in many cases criminals do not commit their offenses in front of witnesses, so there is no one to testify to having seen or heard the offense occur.

Example :-

- **Direct evidence** John Smith testifies under oath that he was in the room with his friend, Joe Hacker, when Joe broke into the ABC Corporation's computer network and that John saw the break-in take place on Joe's computer screen.

- **Circumstantial evidence** The network administrator of ABC Corporation testifies that an intruder using the IP address *xxx.xxx.xxx.xxx penetrated the network at 2:20 A.M. on* December 12, 2001. ISP records show that the IP address in question was assigned via DHCP to Joe Hacker's computer at that time on that date. Joe's girlfriend testifies that Joe was in the study room "doing something on the computer" between the hours of midnight and 4:00 A.M. on that date. No one actually saw Joe perform the intrusion, and none of the evidence definitively proves that he did, but taken all together, the evidence supports the conclusion that Joe Hacker broke into the ABC Corporation network.

Standards and best practices for digital forensics

- The International Organization on Computer Evidence (*IOCE*)
- The Scientific Working Group on Digital Evidence (*SWGDE*)
- International Association of Computer Investigative Specialists (IACIS)

In 2012, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published international standards for digital evidence handling (ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence).

In a computer crime case, evidence tends to be one of the following types:

1. **Digital evidence** Information of value to a criminal case that is stored or transmitted in digital form.
2. **Data objects** Information of value to a criminal case that is associated with physical items.
2. **Physical items** The physical media on which digital information is stored or through which it is transmitted or transferred.

- *Demonstrative evidence* is that which reconstructs the scene or incident in question and allows jurors to view it, using visual aids such as models, graphs, charts, drawings, simulations.

- *Documentary evidence usually* refers to written documents that constitute evidence. For example, a letter or photograph is generally considered documentary evidence.

- Many legal experts consider digital evidence to be more demonstrative than documentary, because the field of computer forensics basically concerns itself with reconstructing the crime scene.

Admissibility of Evidence

The necessary requirements for an evidence to be admissible are:

1. Competent : should be reliable and credible
2. Relevant : should be able to prove the existence of a fact of the case.
3. Material : it substantiates an issue that is in question.
4. Obtained Legally.
5. Pass General acceptance test : scientific technique / tool must be accepted in the field of digital forensics before the results of the technique /tool can be admitted as evidence.

Forensic Examination Standards

- Organizations such as the IACIS provide standards governing forensic examination procedures.
- Most computer forensics organizations and experts agree on some basic standards regarding the handling of digital evidence:

1. The original evidence should be preserved in a state as close as possible to the state it was in when found.
2. If at all possible, an exact duplicate (image) of the original disk should be used for examination so as not to damage the integrity of the original.
3. Copies of data made for examination should be made on media that is *forensically sterile—that is, there must be no pre-existing data on the disk* or other media; it should be completely "clean" and checked for freedom from viruses and defects.
4. All evidence should be properly tagged and documented and the chain of custody preserved, and each step of the forensic examination should be documented in detail. For example: **Computer forensics Chain of Custody support in Microsoft Azure.** To ensure a valid CoC, digital evidence storage must demonstrate adequate access control, data protection and integrity, monitoring & alerting and logging & auditing.

https://docs.microsoft.com/en-us/azure/architecture/example-scenario/forensics/

Collecting Digital Evidence

Process of collecting digital evidence usually involves several people:

A. The first responders (officers or official security personnel who arrive first at the crime scene). Their role includes:

1. **Identifying the crime scene:** establish a perimeter, create list of systems involved in the criminal incident.
2. **Protecting the crime scene:**
   - should not do anything with or to the computers other than protect them from tampering or damage.
   - should not attempt to shut down or unplug the computer or access it to look for evidence.
3. **Preserving temporary and fragile evidence:** preserve or record evidence that might disappear/vanish before investigators arrive.

B. Investigator / Investigative team is generally responsible for coordinating the activities of all others at the scene and is responsible for the following:

1. **Establishing the chain of command**
   - The senior investigator in charge of the scene should ensure that everyone else is aware of the chain of command and that important decisions are filtered through him or her.
   - Computers and related equipment **should not be** accessed, moved, or removed without permission from the senior investigator.
   - If the investigator in charge has to leave the scene, he or she should designate a person remaining on the scene to be in charge of the scene and stay in close contact with that person until all evidence has been collected and moved to secure storage.
2. **Conducting the crime scene search**
   - An investigator should direct the search of the crime scene, which may be carried out by investigators or by other officers.
   - If the search warrant allows, officers should look for all computer hardware, software, manuals, written notes, and logs related to the operation of the computers. This includes printers, scanners, and all storage media: diskettes, optical discs (CDs, DVDs, and so on), tapes, Zip and other removable disks, and any "extra" hard disks that might be lying around.
3. **Maintaining integrity of the evidence**
   - Investigators should continue to protect the evidence as preparations are made to preserve volatile evidence, duplicate the disks, and properly shut down the system.
   - The investigator should oversee the actions of the crime scene technicians and convey any special considerations that should be taken based on the nature of case and knowledge of the suspect(s).

C. Crime Scene Technicians are Computer forensics specialists must have a strong background in computer technology with an understanding of how disks are structured, how file systems work, and how and where data is recorded. Their responsibility includes:

- **Preserving volatile evidence and duplicating disks** Volatile data is that which is in the computer's memory and consists of processes that are running. Disks should be duplicated prior to shutdown, in case the system is rigged to wipe the disks on startup.

- **Shutting down the systems for transport** Proper shutdown is important to maintain the integrity of the original evidence.
- One school of thought says the computer should be shut down through the standard method (closing all programs and so on) to avoid corrupting files.
- Another says that after ensuring that no defragmentation or disk checking program is running, you should shut down the computer by disconnecting the power cord, to prevent running of self-destruct programs that are set to run on shutdown.
- UNIX computers usually should not be abruptly shut down this way while the root user is logged on because doing so can damage data.
- Some forensics experts recommend that the technician change accounts using the **su command or, if the** root password is available, that the **sync; sync; before halt command be used** before powering off. Generally Halt command just calls the shutdown command unless the run level is already 0(shutting) or 6(rebooting); Shutdown further calls umount which performs a sync of filesystem.

- **Tagging and logging the evidence** All evidence should be tagged and/or marked with the initials of the officer or technician, time and date collected, case number, and identifying information. The evidence on the tag or mark should also be entered in the evidence log.

- **Packaging the evidence** Computer evidence, especially any containing exposed circuit boards (such as hard disks), should be placed in antistatic bags for transport.

- Paper documentation such as manuals and books should be placed in plastic bags or otherwise protected from damage.

- **Transporting the evidence** All evidence should be transported as directly as possible to the secure evidence storage locker or room. The chain of custody must be meticulously maintained during transport.

- During transport, the evidence should not be allowed to come into contact with any equipment that generates a magnetic field (including police radios and other electronic equipment in the squad car) nor left in the sun or in a vehicle or other place where the temperature rises above about 75 degrees Fahrenheit.

- **Analysis of the evidence** When the duplicate disk is brought back to the lab, the disk image can be reconstructed and the data analyzed using special forensics software tools.

Preserving Digital Evidence

- Digital evidence is fragile by its nature. Some data is *volatile—that is, it is transient* in nature and, unlike data stored on disk, will be lost when the computer is shut down.
- Data on a computer disk can be easily damaged, destroyed, or changed either deliberately or accidentally.
- **The first step in handling such digital evidence is to protect it from any sort of manipulation or accident.**
- The best way to do this is to immediately make a complete bitstream image of the media on which the evidence is stored.

- A *bitstream image is a copy that records every data bit that was recorded to the original storage device*, including all hidden files, temp files, corrupted files, file fragments and erased files that have not yet been overwritten.

- In other words, every binary digit is duplicated exactly onto the copy media.

- Bitstream copies (sometimes called *bitstream backups) use CRC computations to validate that the copy is the same as the original source data*.

- The "Mirror Image" should be an exact duplicate of the original, and the original should then be stored in a safe place where its integrity can be maintained.

- The copy is made via a process called *disk imaging.*

- *In some cases, evidence could be limited to* a few data files that can be copied individually rather than creating a copy of the entire disk.

A. Preserving Volatile Data

- **The data that is held in temporary storage in the system's memory (including random access memory, cache memory, and the onboard memory of system peripherals such as the video card or NIC) is called *volatile data*** . When the system is powered off or if power is disrupted, the data disappears.

- According to the IEEE Internet draft titled *Guidelines for Evidence Collection and Archiving, the most volatile evidence should be collected first. The* volatile evidence is the most likely to disappear before it can be documented or collected.

- The draft lists the "order of volatility" as:

  1. Registers and cache
  2. Routing tables, ARP cache, Process tables, and kernel statistics
  3. Contents of system memory
  4. Temporary files / System configurations like time and date settings etc
  5. Data on disk
  6. Secondary storage devices

- Collecting volatile data presents a problem because doing so changes the state of the system (and the contents of the memory itself).

- It is recommend that investigators or crime scene technicians capture such data as running processes, the network status and connections, and a “dump” of the data in RAM, documenting each task or command they run to do so.

- Some of this work can be done by running such commands as **netstat (on both Windows and UNIX systems)** and **nbtstat (on Windows only)** to view current network connections.

- **The arp –a command** will tell you what addresses are in the ARP cache (and thus have recently connected to the system).

- The **dd command** can be used to create a snapshot of the contents of memory on UNIX machines.

- The **ps command** can be used to view the currently running processes. On windows machines, the downloadable **pslist utility** can be used to list running processes, or they can be viewed in **Task Manager.**

- Other commands such as **ipconfig (Windows) or ifconfig (UNIX)** can be used to gather information about the state of the network.

- These programs should be run from a special forensics CD that investigator should bring along (instead of running the same commands from the hard disk of the suspect computer) and should not require any programs or libraries from the computer’s hard disk to run.

Disk Imaging

- *Disk imaging refers to the process of making an exact copy of a disk.*
- *Imaging is* sometimes also called *disk cloning or ghosting, but the latter terms usually refer to* images created for purposes other than evidence preservation.
- *Disk imaging differs* from just copying all the files on a disk in that *the disk structure and relative location of data on the disk are preserved*.
- For Example : When you copy all the data on a disk to another disk, that data will usually be stored on the new disk in contiguous clusters as there is room to store it. That way, all the data on the two disks will be identical, but the way that the data is distributed on the disks will not.
- When you create a disk image (a bitstream copy),
  1. Each physical sector of the disk is copied so that the data is distributed in the same way, and then
  2. The image is compressed into a file called an *image file. This image is exactly like the original, both physically* and logically.
- There are a number of different ways to create a bit-level duplicate of a disk, including:
  - Removing the hard disk from the suspect computer and attaching it to another computer (preferably a forensic workstation) to make the copy
  - Attaching another hard disk to the suspect computer and making the copy
  - Using a standalone imaging device such as the DIBS Rapid Action Imaging Device (RAID)
  - Using a network connection to transfer the contents of the disk to another computer or forensic workstation
- Which of these methods you choose to apply, it is usually best to use software specifically designed for forensics purposes.

Imaging Software

- A number of disk-imaging programs are popular with law enforcement computer forensics specialists.
- These programs were developed specifically for the purpose of creating duplicate disks to be used in processing computer evidence and analyzing that evidence. Some examples of these products:

❑**SafeBack :** It is capable of duplicating individual partitions or entire disks of virtually any size, and the image files can be transferred to SCSI tape units or almost any other magnetic storage media.

- The product contains CRC functions to check integrity of the copies and date and timestamps to maintain an audit trail of the software's operations.

❑**Encase :** Encase has a friendly graphical interface that makes it easier for many forensics technicians to use. It provides for previewing evidence, copying targeted drives (creating a bitstream image), and searching and analyzing data.

- Documents, zipped files, and e-mail attachments can be automatically searched and analyzed, and Registry and graphics viewers are included.
- The software calls the bitstream drive image an Evidence File and mounts it as a virtual drive (a read-only file) that can be searched and examined using the GUI tools.
- Timestamps and other data remain unchanged during the examination.
- The "preview" mode allows the investigator to use a null modem cable or Ethernet connection to view data on the subject machine without changing anything;

- **ProDiscover** This Windows-based application, designed by the Technology Pathways forensics team, creates bitstream copies saved as compressed image files on the forensics workstation.

  - Its features include the ability to recover deleted files from slack space, analyze the Windows NT/2000 alternate datastreams for hidden data, and analyze images created with the UNIX dd utility and generate reports.

Standalone Imaging Tools

- Standalone imaging tools such as the *Portable Evidence Recovery Unit* (PERU) and *Rapid Action Imaging Device* (RAID) eliminate the need for a second computer while maintaining the integrity of the suspect computer.

- These portable units can make duplicates of the suspect computer's disk(s) onto another clean hard disk or optical media without the need to remove the original disk from the suspect computer.

Role of Imaging in Computer Forensics

- *Disk imaging* is accepted as standard practice in computer forensics to preserve the integrity of the original evidence.

- *Disk imaging* differs from creating a standard backup of a disk (for fault-tolerance purposes) in that ambient data is not copied to a backup; only active files are copied. Because a backup created with popular backup programs such as the Windows built-in backup utility, BackupExec, ARCserve, or the like is not an exact duplicate (in other words, a physical bitstream image), these programs should not be used for disk imaging.

- Programs such as Norton Ghost include switches that allow you to make a bitstream copy, but these programs were not originally designed for forensics use and do not include the features and analysis tools that are included with imaging programs and standalone imaging systems designed especially for forensics examination.

"Snapshot" Tools and File Copying

- Sometimes it is not possible or desirable to make a full bitstream image of a disk.
- This could be because the system is mission critical and management does not want to have it out of commission during an investigation.
- However, there are still ways to collect data about the intrusion or other crime for the purpose of analyzing what happened and preventing it from happening again.
- In some cases, when evidence is documentary in nature, it might be possible to introduce copies of individual files rather than copying the entire disk.
- This method should be used only when you need specific identifiable documents and there is no need to search for ambient data or other hidden data.
- For Example: One software tool designed to allow administrators to create a "snapshot" of the state of a machine that has been compromised is the *Coroner's Toolkit*, written by the authors of the popular UNIX utility called the System Administrator Tools for Analyzing Networks (SATAN).
- Running these tools on a UNIX system that has been breached is very helpful in performing a forensic analysis, because it will provide information on running processes, the state of the network, deleted files, user information, and much more.

Special Considerations

- Evidence can be damaged or compromised by improper copying, storage, or handling, it's essential to exercise extreme care and diligence when gathering and handling such evidence.

- Some special considerations can also come into play, including environmental factors, retention of time and datestamps, and ways to preserve specific types of data.

1. Environmental Factors

- Magnetically encoded data can be destroyed or damaged (scrambled) by exposure to a magnet or an electromagnetic field generated by many types of electronic equipment.

- Exposure to static electricity or extreme heat can also damage digital data.

- The crime scene technicians needs to be aware that digital evidence is packaged(antistatic bag, bubble wrap, Styrofoam "peanuts") in such a way (Labels warning carriers and tracking numbers)as to protect it from damage and stored in an electromagnetically "clean" environment that is properly cooled.

2. Retaining Time and Date stamps

- The time and date of creation or modification of a file can be an important issue in a criminal case.
- Remember that the time and date stamp on the files will be in accordance with the time and date set on the system clock.
- Some systems default to a particular time zone (usually Greenwich Mean Time GMT).
- If the user set up the system without configuring the proper time zone or if the user deliberately changed the date and time settings, the time and datestamps on the files might not correlate to "real-world" occurrences regarding when the files were created.
- This can be a problem, for example, the system records show that a file was created on a particular date and the suspect is able to prove that he or she was nowhere near the computer on that date.
- Therefore, it is important to note the system time and date settings before shutting down the computer and document them with a photograph, if possible; otherwise, with written notes.
- Opening a file changes the file's time and date records. Thus it might be prudent to photograph the screen showing the file access or modification times prior to opening the file.
- Investigator should be prepared to testify as to his actions and provide expert testimony that the actions he took changed the time and date stamps but did not modify the contents of the file in any way.
- When all the work is done on an image rather than the original, the original times and dates will be on the original disk. You can create a second copy of the original to illustrate this fact.

3. Preserving Data on PDAs and Handheld Computers

- If evidence is contained on a personal digital assistant (PDA) or a palm-sized handheld computer (Palm OS or Pocket PC device), be aware that some of these models will lose data if their batteries die.

- Most come with recharger units, and it is prudent to seize the charger and keep the unit charged until the data can be extracted.

- If you don't have such a tool available, another way to preserve data on a handheld is to copy the relevant files to a Compact Flash or Media card.

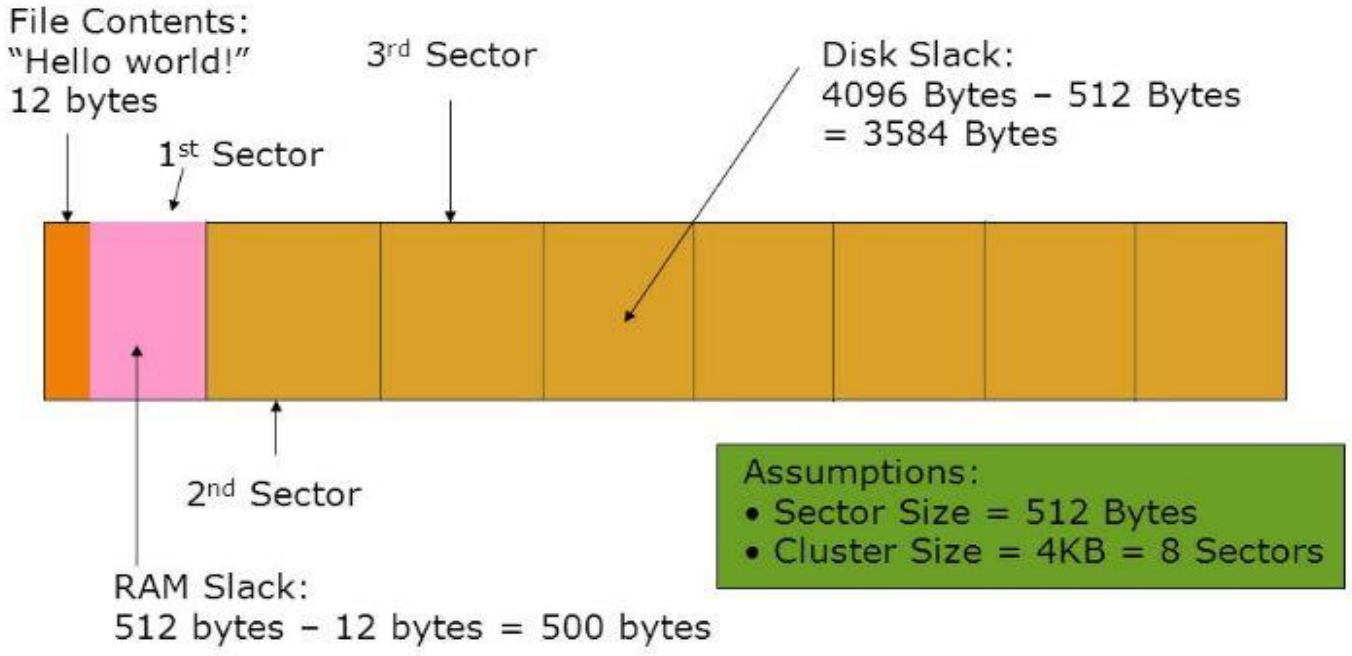
Recovering Digital Evidence

- Some particularly tech-savvy cybercriminals use sophisticated techniques to hide data in unlikely or nontraditional areas.

- Other times, the data that would be useful to the investigator is never stored on disk at all—at least, not to the computer user's knowledge.

- However, a great deal of *ambient data is stored in locations* such as cache files, swap/page files, and temporary (temp) files, as well as "leftover" data that occupies the "unallocated" space on the disk, the "slack" space in clusters that are larger than the files they hold, and the "gaps" between partitions or sectors.

- Investigators can recover this ambient data which is not immediately apparent when browsing the file structure but that can prove critical to building a criminal case.



Recovering “Deleted” and “Erased” Data

- Deleting a file does not remove the content of the file.
- It removes the pointer to that file from the file allocation table (FAT), master file table (MFT), or other scheme that the operating system uses to pinpoint the location of a particular file on the disk.
- Data is stored on the disk in *clusters, which are units consisting of a set* number of bits.
- Because parts of a file are not always stored in contiguous clusters on the physical disk, but instead parts of it could be spread across the disk in separate locations, removing the pointer makes it difficult for the file to be reconstructed— but *not impossible.*
- When the file is deleted, the disk location in which it is stored is marked as *unallocated space, which means that it is available when new data needs to be* written.
- However, on a large disk it might be a long time before that particular part of the disk is used to write new data.
- In the meantime, the old data is still there and can be recovered if the investigator has the proper tools.

- A brand-new disk is thought of as being “clean,” or completely empty, but in reality it is full of *format characters, which are repeated characters made by the test* machine at the factory.

- When files and directories are created and saved to disk, they overwrite the format characters.

- When the files or directories are deleted, the clusters in which they are stored are not reallocated until new data is written there.

- Formatting the disk does not remove this data. Even if the disk is repartitioned using FDISK, Partition Magic, or a similar utility, the data is still there until those clusters are overwritten.

A number of software programs can be used to recover files in unallocated space.

- One example is the GetFree tool marketed by New Technologies Inc. (www.forensics-intl.com/getfree.html), the maker of SafeBack. NTI makes a variety of forensics software packages, and GetFree is designed specifically for law enforcement and forensics specialists to capture data in unallocated space on computers running Microsoft operating systems.
- This data can then be viewed using other utilities such as NTI’s Filter I.

- WetStone Technologies (see the company Web site at www.wetstonetech.com) makes a program called Extractor (or SMART Extractor) that recovers deleted files in Red Hat Linux.

- Supposedly erased data can be located in many places on a computer. For example, when a disk is repartitioned, it is possible for data from the previously configured partitions to end up in the space between partitions, called the *partition gap.*

- *Disk search tools can locate this hidden data, which can then* become a potential source of evidence for investigators.

Decrypting Encrypted Data

- *Encryption* is a method of scrambling data so that it can't be read by anyone who doesn't have the password or key to decrypt it.
- Cybercriminals often use encryption to conceal the criminal nature of their data.
- They could encrypt e-mail messages that include incriminating statements, or they could encrypt documents that could be used as evidence or pornographic pictures of children that constitute contraband.
- Cryptanalysts specialize in "cracking" encryption algorithms.
- Strong encryption is difficult to break, but in many cases cybercriminals use relatively weak methods such as the password protection for Office documents that comes built into the applications.
- A number of "password recovery" programs exist for use by legitimate users who protect documents and then forget their passwords.
- Password recovery programs can also be used to crack the passwords on Word or Excel documents.
- They are basically brute-force/dictionary attacks.

- An example is Advanced Office 2000 Password Recovery. Similar programs are designed to crack the passwords for:

  - The Outlook Express e-mail client,
  - Internet Explorer passwords for protected Web sites,
  - files created by Quicken and QuickBooks financial management programs,
  - password-protected PDF files,
  - protected documents created by Lotus 1-2-3 and other Lotus Office Suite programs,
  - protected documents created by Corel WordPerfect,
  - password-protected .zip files and other archives files. For information about many of these password-cracking programs, see www.crackpassword.com.

- Paraben (www.paraben-forensics.com) markets a “decryption collection” software suite as part of its line of forensic programs.

- The suite is designed to crack passwords for a large number of popular software programs and file types, including the Windows operating systems, VBA Visual Basic modules, and many more.

Finding Hidden Data

- In many instances, data hidden on the hard disk can be very useful to investigators in building a case against a cybercrime suspect.
- Some of this data might be ambient data that was left behind when files were deleted or disks were repartitioned.
- There are also a number of places where data can be deliberately hidden by technically savvy criminals using a disk editor, steganographic software, and other methods.
- Finding, retrieving, and reconstructing this hidden data can be an extremely tedious process, but it's worth the effort if it results in evidence that can make or break a case.

Where Data Hides?

- A *disk sector is a unit of space of a fixed size (such as 512 bytes).*
- *Older hard disks* could have some wasted storage space on the outside tracks because of the way the disks are divided into sectors that contain an equal number of sectors per track.
- The discrepancy in circumference between the inside and outside tracks causes this wasted space.
- It is possible in some cases to hide data in the space between sectors on the larger outside tracks. This space is called the *sector gap.*
- Some data recovery services might be able to locate and retrieve data that is hidden in this gap.

- Another place that data can be hidden is in the *slack area caused by file sizes* that don't exactly match the size of the clusters in which they are stored.
- Clusters are made up of sectors. Cluster sizes can vary, but anytime a file or portion of a file is smaller than the cluster size, the "leftover" bits in that cluster go unused.
- In file systems such as FAT16, where cluster sizes increase based on the partition size, this can result in a very large amount of "empty" space, and that space can be used to covertly store other bits of data.
- Data can be hidden here, unbeknownst to the user. Clusters are made up of sectors.
- When the file is too small to fill up the last sector in a file, DOS and Windows use random data from the system's memory buffers to make up the difference.
- This is called *RAM slack and can result in data from the work session* (the time since the computer was last booted) being stored on the disk in this slack space to "pad" the final sector.
- All sorts of data dumped from memory can be lurking in the slack space and could prove useful to the investigator. Any kind of disk (diskette, hard disk, and removable disk) is subject to slack.
- Computer forensic analysis tools such as those marketed by NTI can recover data hidden in slack areas.
- *Shadow data is created because the vertical and horizontal alignment of the* mechanical heads that write to the disk are not exactly the same each time a write operation is performed.
- This means that even when data is overwritten, remnants of the old data could still be there. It is sometimes possible (although very time consuming and expensive) to reconstruct the data from these remnants.

Detecting Steganographic Data

- Steganography software hides files within other files, using empty space or the least significant bit to encode messages.
- For example: data can be hidden within an image file by slightly altering a single bit related to a particular pixel. If one pixel in the photo has a red component, represented by the binary number 10001100, the least significant bit (the last one) can be changed to a 1, making the binary 10001101. This will make that one pixel a tiny bit redder, which will not be noticeable to viewers. This creates one "hidden" bit, a 1. To create a 0, you would leave the least significant bit as it was.
- The entire file that you want to hide is broken up into its binary components, and these are then concealed in different parts of the photo image.
- Determining which pixels contain the hidden bits, and in what order, can be done by a random number generator that uses a key so that only someone who knows the key will be able to reconstruct the hidden message by retrieving the hidden bits in the correct order.
- Several "anti-steganography" programs on the market allow you to detect the presence of data that is hidden within other files using steganographic techniques.
- Detecting the presence of steganographic data is much easier than extracting the message itself. This is usually done by software that checks the statistical profile of an image and looks for statistical artifacts left by steganographic software.
- *Steganalysis is the process of detecting steganography in files* and rendering the covert messages useless.

Locating Forgotten Evidence

- A great deal of data is stored on computers automatically by application programs and/or the operating system.
- Some users are unaware of this stored data; others know about it but might forget to get rid of it when they are destroying evidence on a system.
- Depending on the nature of the offense, some of this data could be useful to the cybercrime investigator.
- Sources of forgotten evidence include Web caches, temporary (temp) files, swap/page files, and application logs.

Web Caches and URL Histories

- Web browsers are designed with performance in mind. Users want their Web pages to pop up in the browser as quickly as possible.
- One way to speed up access is to provide a way for the browser to get the file from the local computer's hard disk, rather than downloading it over a much slower Internet connection.
- For this reason, Web browsers by default *cache the pages that a user visits, along with related* graphics, sounds, and other embedded files, so that if user visit the same page again, it can be quickly retrieved from the disk..
- These files are usually called *temporary Internet files and are stored in a special folder, usually under the user's profile* name.
- They provide a visual record of the sites that the user has visited recently.
- This information can be especially useful in child pornography cases or cases of terrorists who frequently visit certain Web sites.

Recovering Data from Backups

- An often-overlooked source of data recovery is the backup(s) that the suspect or (if the suspect's computer is on a network) the systems administrator might have made for fault-tolerance purposes.
- In many cases in which suspects have destroyed incriminating files, copies of those files still existed on the backup media.
- This is especially true in a corporate situation, where system administrators often automatically back up user data to a server each day.
- Even when the suspect uses a home computer, it's worth checking for the existence of backups.
- Many computer hobbyists, having been the victims of system failure in the past and having lost valuable data because of it, regularly back up their important files.
- If there is a Magnetic tape drive attached to the system, there's a good chance it's used for backups.
- If there is a CD or DVD writer installed, the suspect might have used it for archiving.
- It is important that the search warrant specify seizure of any tapes, disks, CD-ROMs, or other media commonly used to back up files, in addition to the computer equipment itself.
- Backups have saved the day in many cases when no evidence could be found on the computer's hard disk.

Computer Forensics Information

- Computer forensics is a field that is not only growing fast but changing fast as well.
- New techniques and technologies are being developed and proven all the time, and it's important that investigators keep up with the latest news in the field.
- There are several ways to stay current, including:
  - ❑ Reading computer forensics and general forensics periodicals, both print publications and webzines such as *Computer Forensics Online* (www.shk-dplc.com/cfo) and *Computer Forensics Magazine* (www.forensic-computing.com).
  - ❑ Attending seminars and conferences that focus on computer crime and cybercrime, such as Foundstone's Incident Response and Computer Forensics, the Techno-Security Conference sponsored by Guidance Software (information on the 2003 event is located at www.thetrainingco.com/html/Techno2003.html), Cybercrime 2003 (www.cybercrime2002.com/2003.html), and many others.
  - ❑ Joining associations of computer forensics and cybercrime investigation professionals, such as IACIS (www.iacis.com), the High Technology Crime Investigators Association (http://htcia.org), the High Tech Crime Consortium (www.hightechcrimecops.org), and others.

Understanding Legal Issues

- Computer forensics is concerned as much with complying with the law and following prescribed procedures for evidence collection as with the technical aspects of collecting digital evidence.

- Evidence that is inadmissible in court is worse than useless; Not only can illegal search and seizure damage or destroy the prosecution's case and result in a cybercriminal going free, it can also result in administrative or even criminal actions against officers who violate the rules.

- Thus it is imperative that law enforcement officers and others who will be involved in the collection and preservation of evidence understand the legal issues under which they operate.

- The laws vary from one jurisdiction to another and change on a regular basis, so all cybercrime investigators should make it a practice to stay up to date on passage of statutes and court decisions that apply to their jurisdictions.

- Investigators should be aware of any new law or directions from the court pertaining to search and seizure of computers and digital evidence.

Searching and Seizing Digital Evidence

- A *search* *is legally defined by the courts as "an examination of a man's house or other buildings or premises, or of his person, or of his vehicle, aircraft, etc., with a view to the discovery of contraband or illicit or stolen property, or some evidence of guilt to be used in the prosecution of a criminal action for some crime or offense with which he is charged*".

- *A seizure is defined as "the act of taking possession of property, e.g., for a violation of law or by virtue of an execution*" [of a warrant].

- Traditional ideas of search and seizure did not take into account the ways in which computers are used today as a repository of information (and potential evidence).

- The courts have had to develop interpretations of the law to apply to the unique aspects of these digital "places" and the types of evidence that can be found there.

  For example, the laws generally restrict entering a person's private premises to conduct a search without a warrant, except under certain restricted circumstances.

- Courts have generally held that a person has a reasonable expectation of privacy when information is stored in a computer.
- On the other hand, when evidence is in plain view in a public place, the law allows officers to seize it.
- Attempting to apply these same rules to today's networked world brings up interesting questions.
- Is data on a person's private computer that is connected to the public Internet and accessible to the public considered to be on private premises or in a public place?
- The answers are still evolving as the courts address cases that hinge on such issues. however, states can impose further restrictions on police powers within their boundaries, so understanding federal guidelines is only the starting point.

Search Warrant Requirements

- A *search warrant is a document signed by a magistrate giving law enforcement* officers the authority to search a specified place for specific items that are particularly described in the warrant.

- A warrant must be based on another document called an *affidavit, which is signed under oath by some person (a police officer or* any other person) expressing the belief that certain items will be found at the location to be searched and giving facts that support the belief.

- Those facts must constitute *probable cause that the objects of the search will be found at the* described location. Only those items specifically named in the warrant can be searched for.

- A warrant can authorize the search and seizure of computer hardware, digital information, or both. Overly broad language (such as authorization to seize "all records" or "all computers") can result in the warrant being invalidated; the warrant must specify the crime(s) to which the evidence pertains.

- Search warrants can be obtained to search for specific types of property or for a person.

- Search warrants and the supporting affidavits must follow strict guidelines as to form and content, and the reliability of the affiant (the person signing the affidavit) must be established to the satisfaction of the magistrate who issues the warrant.

- From the officer's point of view, it is always preferable to have a search warrant rather than searching without a warrant, because a warrant relieves the officer of the responsibility of showing that probable cause.

- **Special problems** can arise in constructing search warrants for electronic evidence, because of the intangible nature of the evidence.

- For example, a suspect can move or destroy computer data quickly and easily without leaving the premises. A person with technical expertise should advise the officers and magistrate regarding the technical aspects of searching for and collecting digital evidence based on the facts of a particular case.

- It is important, to gather all the information possible about the object of the warrant in a computer-related case as in one involving the search of a physical location.

- This includes the hardware platforms, operating system environment, and software applications in use, as well as the network connections and configurations.

- This specificity will help pinpoint the types of files to look for in the search and possible locations where they might be stored.

Seizure of Digital Evidence

- There are several different ways digital evidence can be seized when it is located. Early computer crime investigators often printed incriminating files or made digital copies (on floppy disks or other removable media) of the files in question.

- Another option is to seize all the computer equipment and go through the data stored on it at another location(a forensic lab).

- The best accepted practice today is to first make a complete exact bitstream copy of the hard disk(s) before shutting down the computer. These copies can be used to reconstruct the suspect disk and analyze it at another location later.

- After making the copies, investigators should seize the equipment and original disk, mark it as evidence, and store it in a secure location.

- The search and seizure process should be well planned in advance. Determine the best day and time of day for the process, and estimate the number of officers and technicians and levels of expertise that will be needed on site when the search and seizure are to be conducted.

- **Forfeiture Laws**

  Computer equipment used as a tool or instrumentality of certain crimes (for example, in cases of illegal drug trafficking) can be subject to state and federal asset forfeiture laws. This means that the ownership of the equipment is transferred to the state or the law enforcement agency making the seizure and can be converted to their own use or sold.

Thank you