

Computer Forensics

Bassel Kateeb Tim Altimus



Introduction

- Topics to be covered
 - Defining Computer Forensics
 - Reasons for gathering evidence
 - Who uses Computer Forensics
 - Steps of Computer Forensics
 - Handling Evidence
 - Investigation initiation / response
 - Handling Information
 - Requirements
 - Anti-Forensics
 - Evidence processing guidelines
 - Methods of hiding Information/data
 - Methods of discovering information/data



Definition

- What is Computer Forensics??
 - Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.
 - Evidence might be required for a wide range of computer crimes and misuses
 - Multiple methods of
 - Discovering data on computer system
 - Recovering deleted, encrypted, or damaged file information
 - Monitoring live activity
 - Detecting violations of corporate policy
 - Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity



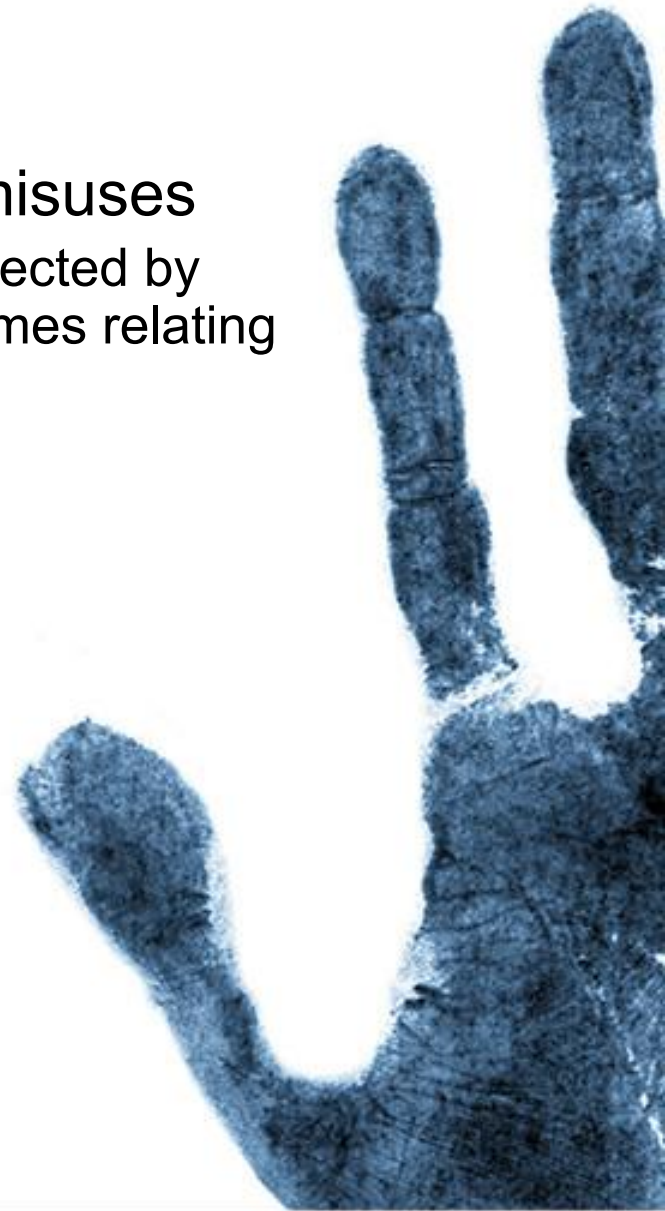
Definition (cont)

- What Constitutes Digital Evidence?
 - Any information being subject to human intervention or not, that can be extracted from a computer.
 - Must be in human-readable format or capable of being interpreted by a person with expertise in the subject.
- Computer Forensics Examples
 - Recovering thousands of deleted emails
 - Performing investigation post employment termination
 - Recovering evidence post formatting hard drive
 - Performing investigation after multiple users had taken over the system



Reasons For Evidence

- Wide range of computer crimes and misuses
 - Non-Business Environment: evidence collected by Federal, State and local authorities for crimes relating to:
 - Theft of trade secrets
 - Fraud
 - Extortion
 - Industrial espionage
 - Position of pornography
 - SPAM investigations
 - Virus/Trojan distribution
 - Homicide investigations
 - Intellectual property breaches
 - Unauthorized use of personal information
 - Forgery
 - Perjury



Reasons For Evidence (cont)

- Computer related crime and violations include a range of activities including:
 - Business Environment:
 - Theft of or destruction of intellectual property
 - Unauthorized activity
 - Tracking internet browsing habits
 - Reconstructing Events
 - Inferring intentions
 - Selling company bandwidth
 - Wrongful dismissal claims
 - Sexual harassment
 - Software Piracy



Who Uses Computer Forensics?

- Criminal Prosecutors
 - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- Civil Litigations
 - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- Insurance Companies
 - Evidence discovered on computer can be used to mollify costs (fraud, worker's compensation, arson, etc)
- Private Corporations
 - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases



Who Uses Computer Forensics? (cont)

- Law Enforcement Officials
 - Rely on computer forensics to backup search warrants and post-seizure handling
- Individual/Private Citizens
 - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment



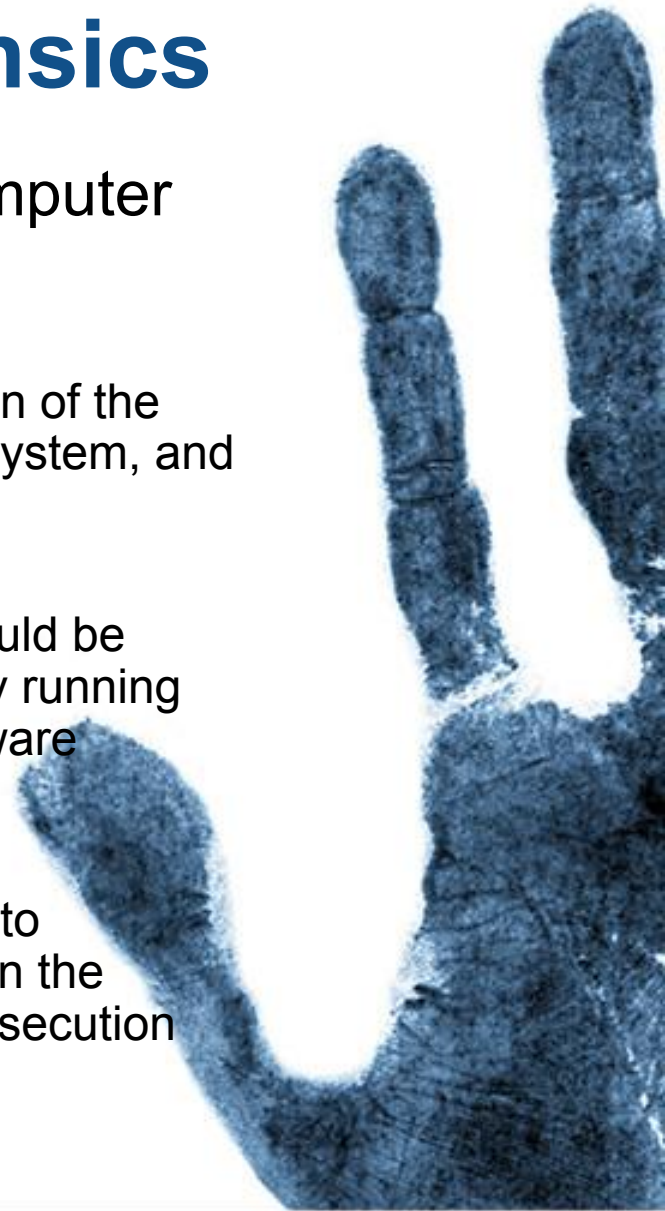
FBI Computer Forensic Services

- Content
- Comparison against known data
- Transaction sequencing
- Extraction of data
- Recovering deleted data files
- Format conversion
- Keyword searching
- Decrypting passwords
- Analyzing and comparing limited source code



Steps Of Computer Forensics

- According to many professionals, Computer Forensics is a four (4) step process
 - Acquisition
 - Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices
 - Identification
 - This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites
 - Evaluation
 - Evaluating the information/data recovered to determine if and how it could be used against the suspect for employment termination or prosecution in court



Steps Of Computer Forensics (cont)

- Presentation
 - This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws



Handling Evidence

- Admissibility of Evidence
 - Legal rules which determine whether potential evidence can be considered by a court
 - Must be obtained in a manner which ensures the authenticity and validity and that no tampering had taken place
- No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to search the computer
- Preventing viruses from being introduced to a computer during the analysis process
- Extracted / relevant evidence is properly handled and protected from later mechanical or electromagnetic damage



Handling Evidence (cont)

- Establishing and maintaining a continuing chain of custody
- Limiting the amount of time business operations are affected
- Not divulging and respecting any ethically [and legally] client-attorney information that is inadvertently acquired during a forensic exploration



Initiating An Investigation

- DO NOT begin by exploring files on system randomly
- Establish evidence custodian - start a detailed journal with the date and time and date/information discovered
- If possible, designate suspected equipment as “off-limits” to normal activity. This includes back-ups, remotely or locally scheduled house-keeping, and configuration changes
- Collect email, DNS, and other network service logs



Initiating An Investigation (cont)

- Capture exhaustive external TCP and UDP port scans of the host
 - Could present a problem if TCP is wrapped
- Contact security personnel [CERT], management, Federal and local enforcement, as well as affected sites or persons



Incidence Response

- Identify, designate, or become evidence custodian
- Review any existing journal of what has been done to system already and/or how intrusion was detected
- Begin new or maintain existing journal
- Install monitoring tools (sniffers, port detectors, etc.)
- Without rebooting or affecting running processes, perform a copy of physical disk
- Capture network information



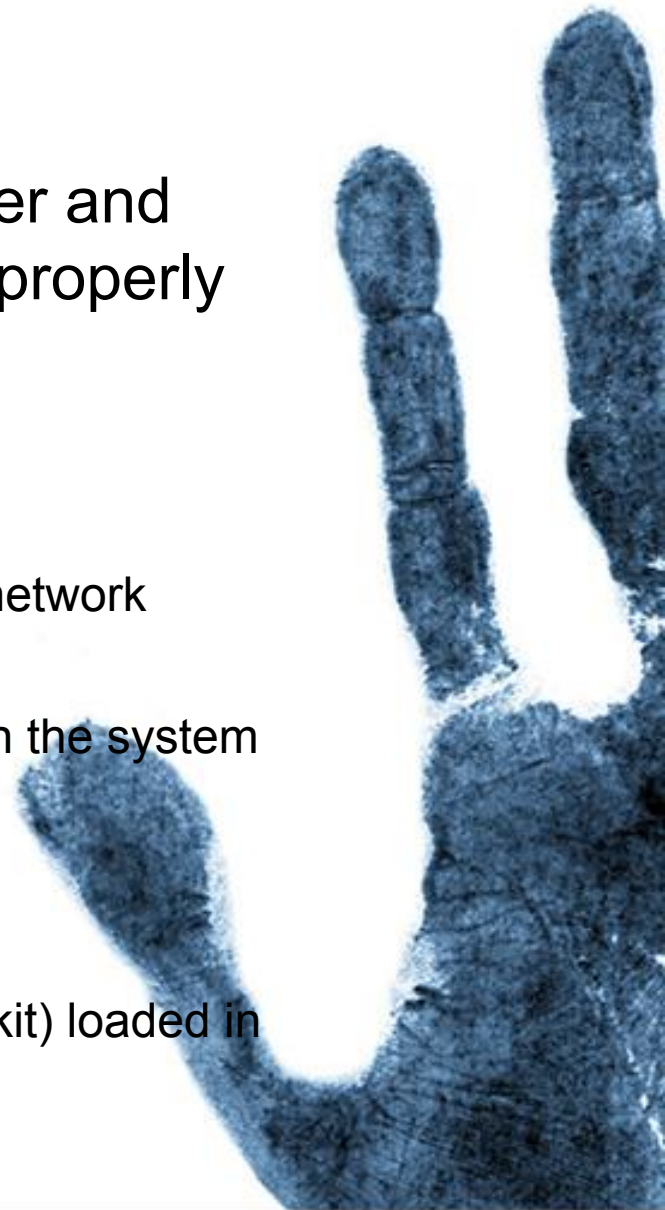
Incidence Response (cont)

- Capture processes and files in use (e.g. dll, exe)
- Capture config information
- Receipt and signing of data



Handling Information

- Information and data being sought after and collected in the investigation must be properly handled
- Volatile Information
 - Network Information
 - Communication between system and the network
 - Active Processes
 - Programs and daemons currently active on the system
 - Logged-on Users
 - Users/employees currently using system
 - Open Files
 - Libraries in use; hidden files; Trojans (rootkit) loaded in system



Handling Information (cont)

- Non-Volatile Information
 - This includes information, configuration settings, system files and registry settings that are available after reboot
 - Accessed through drive mappings from system
 - This information should investigated and reviewed from a backup copy



Computer Forensic Requirements

- Hardware
 - Familiarity with all internal and external devices/components of a computer
 - Thorough understanding of hard drives and settings
 - Understanding motherboards and the various chipsets used
 - Power connections
 - Memory
- BIOS
 - Understanding how the BIOS works
 - Familiarity with the various settings and limitations of the BIOS



Computer Forensic Requirements (cont)

- Operation Systems
 - Windows 3.1/95/98/ME/NT/2000/2003/XP
 - DOS
 - UNIX
 - LINUX
 - VAX/VMS
- Software
 - Familiarity with most popular software packages such as Office
- Forensic Tools
 - Familiarity with computer forensic techniques and the software packages that could be used



Anti-Forensics

- Software that limits and/or corrupts evidence that could be collected by an investigator
- Performs data hiding and distortion
- Exploits limitations of known and used forensic tools
- Works both on Windows and LINUX based systems
- In place prior to or post system acquisition



Evidence Processing Guidelines

- New Technologies Inc. recommends following 16 steps in processing evidence
- They offer training on properly handling each step
 - Step 1: Shut down the computer
 - Considerations must be given to volatile information
 - Prevents remote access to machine and destruction of evidence (manual or anti-forensic software)
 - Step 2: Document the Hardware Configuration of The System
 - Note everything about the computer configuration prior to re-locating



Evidence Processing Guidelines (cont)

- Step 3: Transport the Computer System to A Secure Location
 - Do not leave the computer unattended unless it is locked in a secure location
- Step 4: Make Bit Stream Backups of Hard Disks and Floppy Disks
- Step 5: Mathematically Authenticate Data on All Storage Devices
 - Must be able to prove that you did not alter any of the evidence after the computer came into your possession
- Step 6: Document the System Date and Time
- Step 7: Make a List of Key Search Words
- Step 8: Evaluate the Windows Swap File



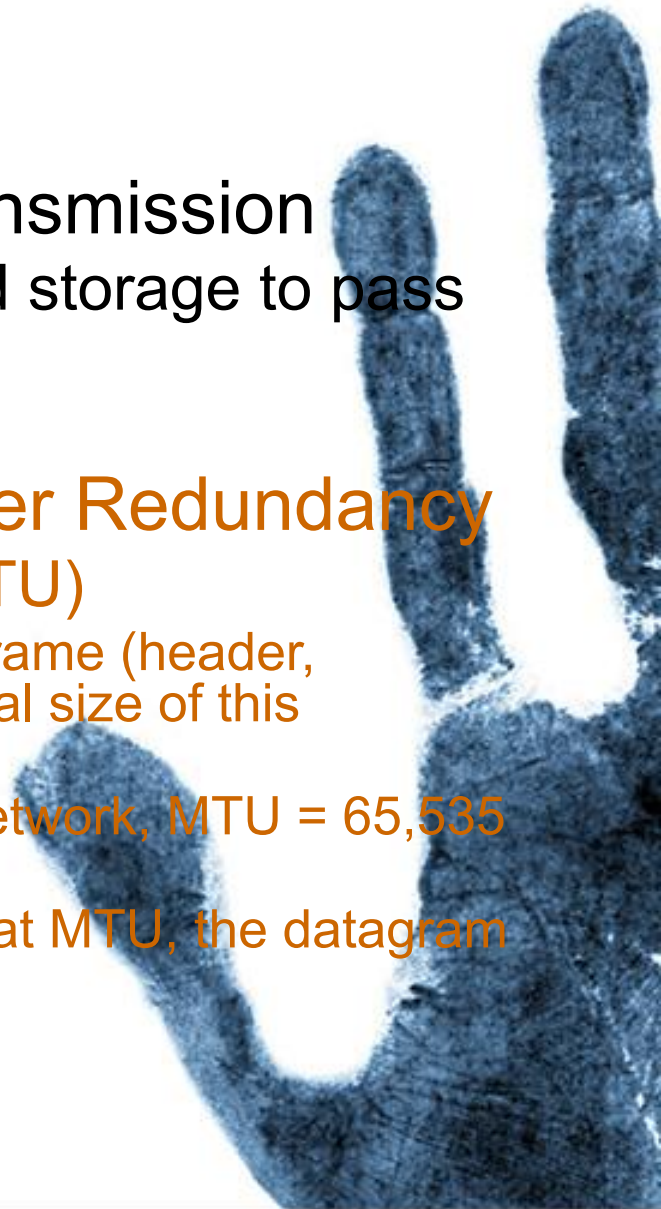
Evidence Processing Guidelines (cont)

- Step 9: Evaluate File Slack
 - File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.
- Step 10: Evaluate Unallocated Space (Erased Files)
- Step 11: Search Files, File Slack and Unallocated Space for Key Words
- Step 12: Document File Names, Dates and Times
- Step 13: Identify File, Program and Storage Anomalies
- Step 14: Evaluate Program Functionality
- Step 15: Document Your Findings
- Step 16: Retain Copies of Software Used



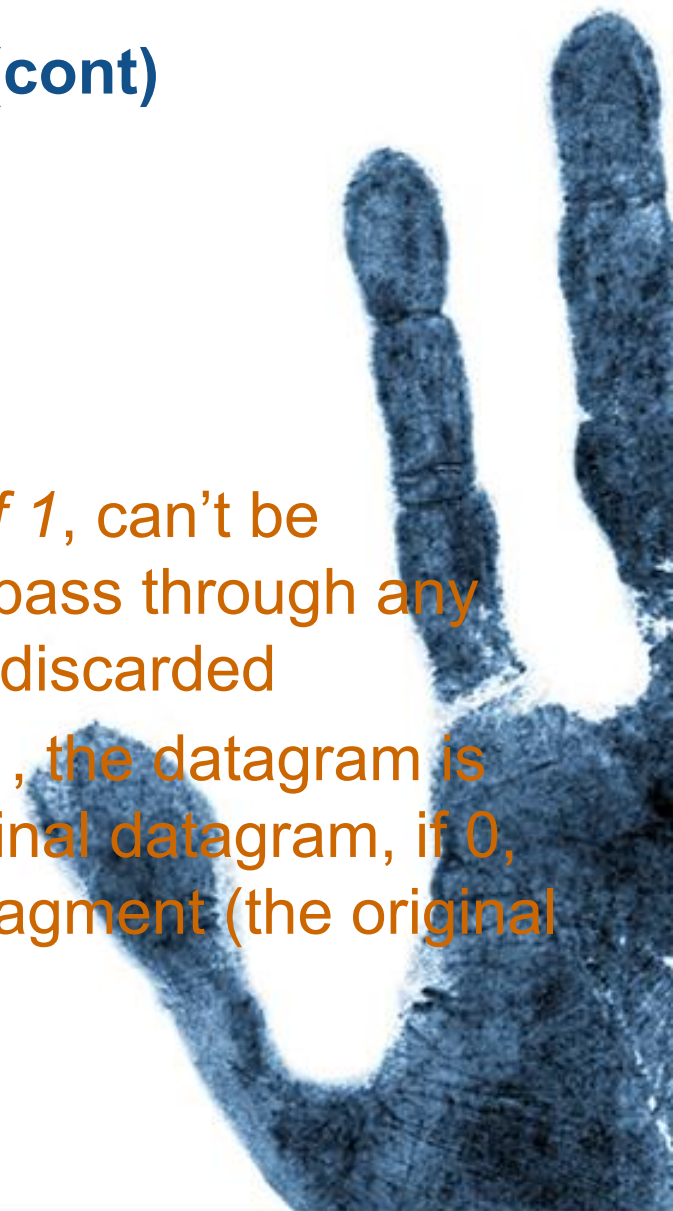
Methods Of Hiding Data

- Covert Channels – Hiding in Transmission
 - Take advantage of timing or shared storage to pass data through unsuspected channel
- EXAMPLE: IP datagram – Header Redundancy
 - Known Maximum Transfer Unit (MTU)
 - A datagram (IP) is encapsulated into frame (header, datagram, trailer). MTU is the max total size of this datagram.
 - To make IP independent of physical network, MTU = 65,535 bytes to give it more efficiency.
 - If the physical layer doesn't support that MTU, the datagram must be fragmented



Methods Of Hiding Data (cont)

- EXAMPLE: Continued...
 - Flags: 3 bits
 - 1st bit: *reserved* (always 0)
 - 2nd bit: *Do not fragment (DF)*: if 1, can't be fragmented. If it is too large to pass through any available physical network, it is discarded
 - 3rd bit: *More fragment (MF)*: if 1, the datagram is not the last fragment of the original datagram, if 0, it is last one or there is only 1 fragment (the original datagram)



Methods Of Hiding Data (cont)

- **EXAMPLE – TCP/IP Continued...**
 - An un-fragmented datagram has all 0's in the flag fields
 - Redundancy condition: the DF bit can be 1 or 0 if no fragment
 - From network perspective: Datagram 1 is not allowed to fragment (1 bit), datagram 2 is allowed but does not because it is under the maximum MTU size.

Datagram 1	16-bit Id. field	3-bit flag field	13-bit frag. offset	16-bit Total len.
1	XX...XX	0 1 0	00...00	472

Datagram 2	16-bit Id. field	3-bit flag field	13-bit frag. offset	16-bit Total len.
1	XX...XX	0 0 0	00...00	472



Methods Of Hiding Data (cont)

- To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These are media exploited using new controversial logical encodings: steganography and marking.
- **Steganography:** The art of storing information in such a way that the existence of the information is hidden.



Methods Of Hiding Data (cont)

- To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These are media exploited using new controversial logical encodings: steganography and marking.
- ***The duck flies at midnight. Tame uncle Sam***
 - Simple but effective when done well



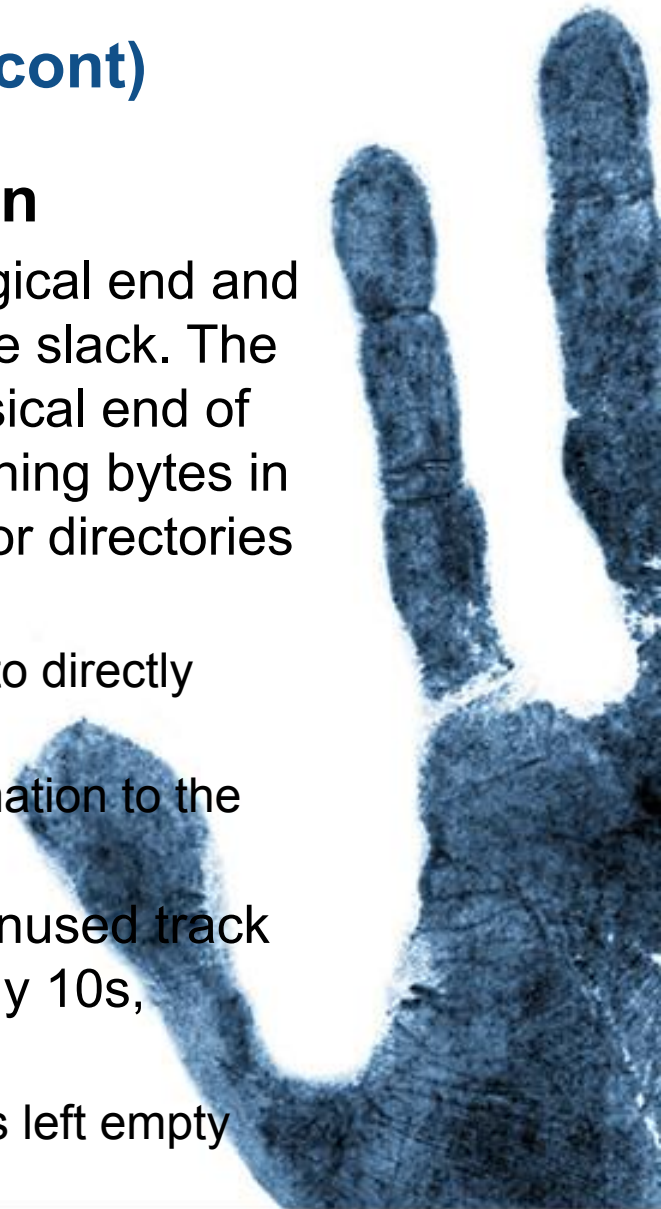
Methods Of Hiding Data (cont)

- **Watermarking:** Hiding data within data
 - Information can be hidden in almost any file format.
 - File formats with more room for compression are best
 - Image files (JPEG, GIF)
 - Sound files (MP3, WAV)
 - Video files (MPG, AVI)
 - The hidden information *may* be encrypted, but not necessarily
 - Numerous software applications will do this for you:
Many are freely available online



Methods Of Hiding Data (cont)

- **Hard Drive/File System manipulation**
 - **Slack Space** is the space between the logical end and the physical end of file and is called the file slack. The logical end of a file comes before the physical end of the cluster in which it is stored. The remaining bytes in the cluster are remnants of previous files or directories stored in that cluster.
 - Slack space can be accessed and written to directly using a hex editor.
 - This does not add any “used space” information to the drive
 - **Partition waste space** is the rest of the unused track which the boot sector is stored on – usually 10s, possibly 100s of sectors skipped
 - After the boot sector, the rest of the track is left empty



Methods Of Hiding Data (cont)

- **Hard Drive/File System manipulation cont...**
 - **Hidden drive space** is non-partitioned space in-between partitions
 - The File Allocation Table (FAT) is modified to remove any reference to the non-partitioned space
 - The address of the sectors must be known in order to read/write information to them
 - **Bad sectors** occur when the OS attempts to read info from a sector unsuccessfully. After a (specified) # of unsuccessful tries, it copies (if possible) the information to another sector and marks (flags) the sector as bad so it is not read from/written to again
 - users can control the flagging of bad sectors
 - Flagged sectors can be read to /written from with direct reads and writes using a hex editor



Methods Of Hiding Data (cont)

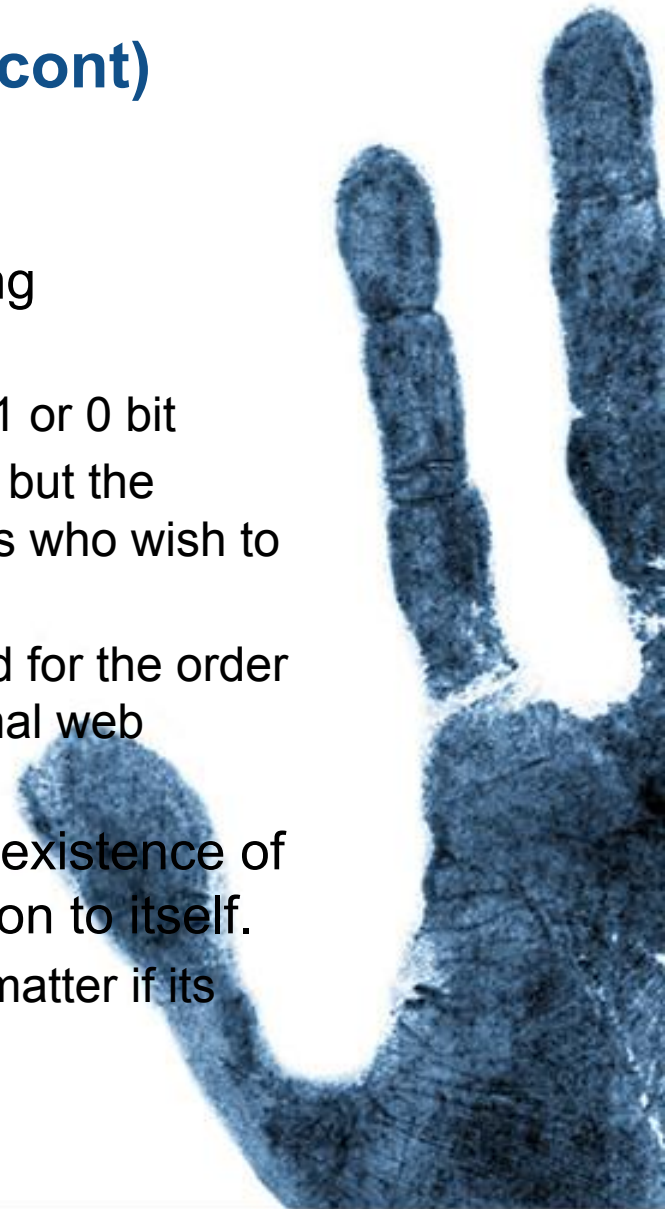
- **Hard Drive/File System manipulation cont...**
 - **Extra Tracks:** most hard disks have more than the rated # of tracks to make up for flaws in manufacturing (to keep from being thrown away because failure to meet minimum #).
 - Usually not required or used, but with direct (hex editor) reads and writes, they can be used to hide/read data
 - **Change file names and extensions** – i.e. rename a .doc file to a .dll file



Methods Of Hiding Data (cont)

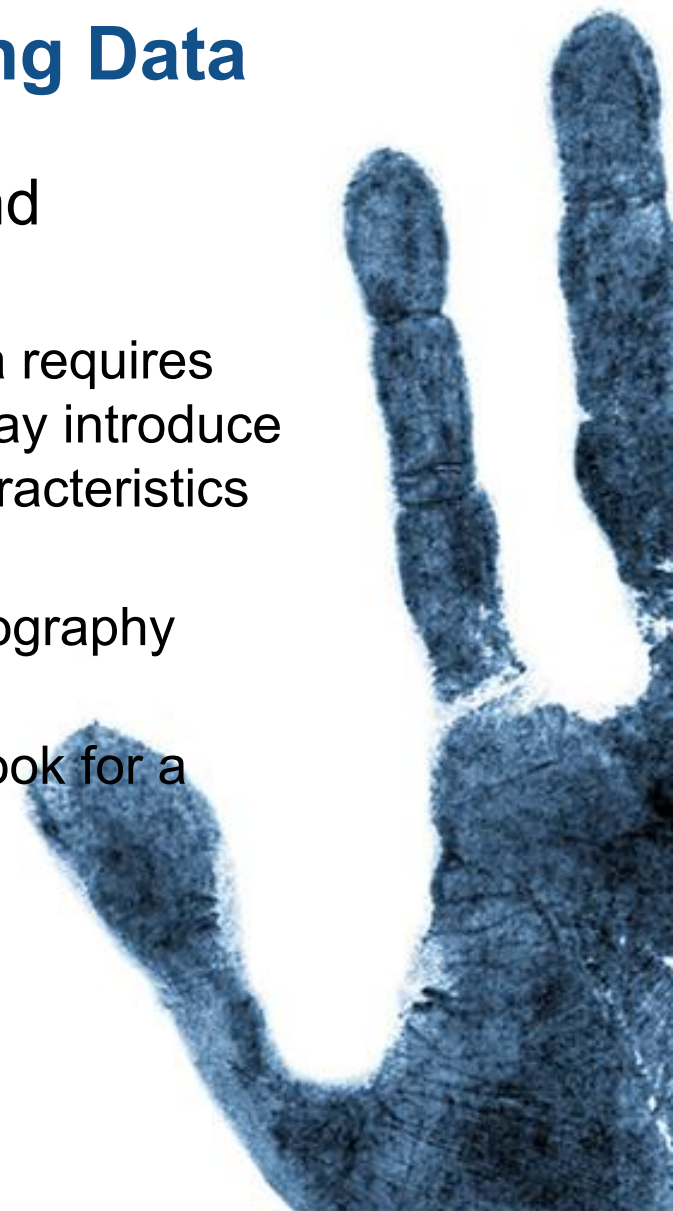
- **Other Methods**

- **Manipulating HTTP requests** by changing (unconstrained) order of elements
 - The order of elements can be preset as a 1 or 0 bit
 - No public software is available for use yet, but the government uses this method for its agents who wish to transfer sensitive information online
 - Undetectable because there is no standard for the order of elements and it is, in essence, just normal web browsing
- **Encryption:** The problem with this is that existence of data is not hidden, instead it draws attention to itself.
 - With strong enough encryption, it doesn't matter if its existence is known



Methods Of Detecting/Recovering Data

- **Steganalysis** - the art of detecting and decoding hidden data
 - Hiding information within electronic media requires alterations of the media properties that may introduce some form of degradation or unusual characteristics
 - The pattern of degradation or the unusual characteristic of a specific type of steganography method is called a **signature**
 - Steganalysis software can be trained to look for a signature



Methods Of Detecting/Recovering Data (cont)

- **Steganalysis Methods - Detection**

- **Human Observation**

- Opening a text document in a common word processor may show appended spaces and “invisible” characters
 - Images and sound/video clips can be viewed or listened to and distortions may be found
 - Generally, this only occurs if the amount of data hidden inside the media is too large to be successfully hidden within the media (15% rule)

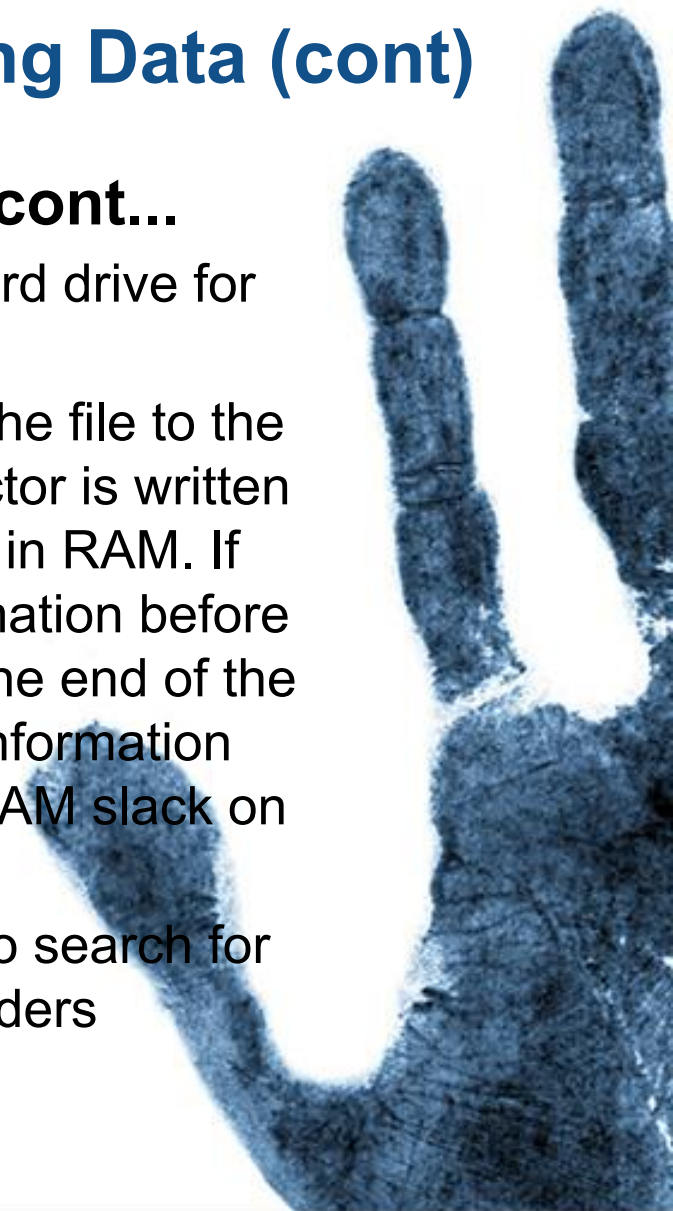
- **Software analysis**

- Even small amounts of processing can filter out echoes and shadow noise within an audio file to search for hidden information
 - If the original media file is available, hash values can easily detect modifications



Methods Of Detecting/Recovering Data (cont)

- **Steganalysis Methods – Detection cont...**
 - **Disk analysis utilities** can search the hard drive for hidden tracks/sectors/data
 - **RAM slack** is the space from the end of the file to the end of the containing sector. Before a sector is written to disk, it is stored in a buffer somewhere in RAM. If the buffer is only partially filled with information before being committed to disk, remnants from the end of the buffer will be written to disk. In this way, information that was never "saved" can be found in RAM slack on disk.
 - **Firewall/Router filters** can be applied to search for hidden or invalid data in IP datagram headers



Methods Of Detecting/Recovering Data (cont)

- **Steganalysis Methods – Detection cont...**
 - **Statistical Analysis**
 - Most steganographic algorithms that work on images assume that the Least Significant Bit (LSB) is random
 - If a filter is applied to an image, the LSB bits will produce a recognizable image, so the assumption is wrong
 - After inserting hidden information into an image, the LSB is no longer non-random (especially with encrypted data). If you apply the same filter, it will no longer produce a recognizable image
 - Statistical analysis of the LSB will tell you if the LSB bits are random or not
 - Can be applied to audio files as well (using LSB)
 - **Frequency scanning**
 - Software can search for high, inaudible frequencies



Methods Of Detecting/Recovering Data (cont)

- **Steganalysis Methods – Recovery**

- Recovery of watermarked data is extremely hard
 - Currently, there are very few methods to recover hidden, encrypted data.
- Data hidden on disk is much easier to find. Once found, if unencrypted, it is already recovered
- Deleted data can be reconstructed (even on hard drives that have been magnetically wiped)
- Check swap files for passwords and encryption keys which are stored in the clear (unencrypted)
- **Software Tools**
 - Scan for and reconstruct deleted data
 - Break encryption
 - Destroy hidden information (overwrite)

