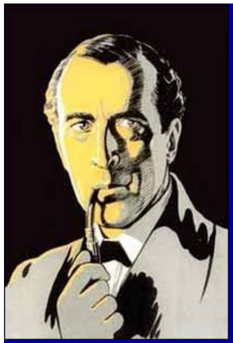
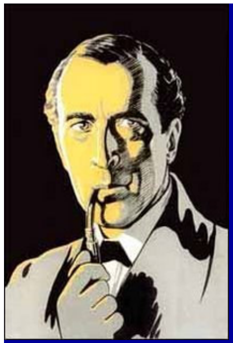


COMPUTER FORENSICS

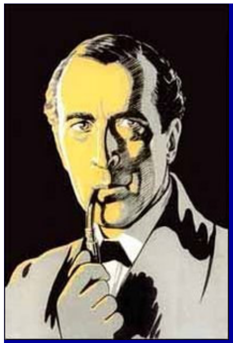
Forensic Science CC 30.07 Spring 2007 Prof. Nehru



Computer Forensics

- Computer forensics **involves the preservation, acquisition, extraction, and interpretation of computer data.**

- In today’s world of technology, ***many devices are capable of storing data and could thus be grouped into the field of computer forensics.***



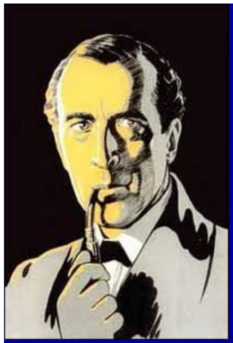
Computer Forensics

The Basics

- Distinction between hardware and software

- Hardware comprises the physical and tangible components of the computer.

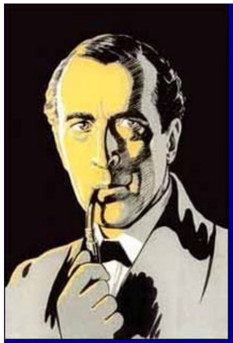
- Software is a set of instructions compiled into a program that performs a particular task.



Computer Forensics

Terminology

- Computer Case/Chassis
- Power Supply
- Motherboard
- System Bus: Contained on the motherboard

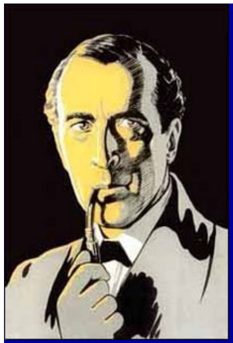


Computer Forensics

Terminology

- **Read Only Memory (ROM):** ROM chips store programs
  - used to start the boot process
  - configure a computer's components

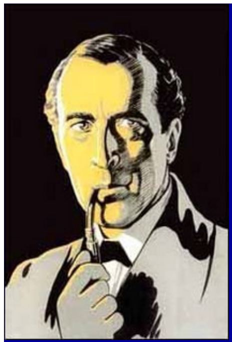
- **Random Access Memory (RAM):** RAM takes the burden off of the computer's processor and Hard Disk Drive (HDD)
  - The computer stores the data that it needs to use in RAM
  - **RAM is referred to as volatile memory** because it is not permanent; its contents undergo constant change and are forever lost once power is taken away from the computer



Computer Forensics
Terminology

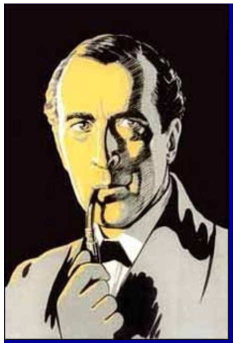
- **Central Processing Unit (CPU):**
  CPU, also referred to as a processor,
  is essentially the brains of the computer

- **Input Devices:** used to get data into the computer
  - To name a few:
    - Keyboard
    - Mouse
    - Joy stick
    - Scanner



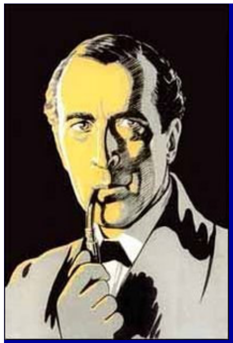
Computer Forensics
Terminology

- **Output Devices:** Equipment through which data is obtained from the computer.
  - To name a few:
    - Monitor
    - Printer
    - Speakers
- **Hard Disk Drive (HDD)** is typically the primary location of data storage within the computer.



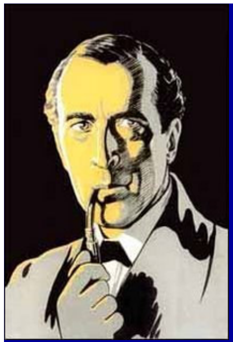
Computer Forensics
Terminology

- Different **operating systems** map out (partition) HDDs in different manners
- Examiners must be familiar with the file system they are examining.
- Evidence exists in many **different locations** and in numerous forms on a HDD.
- The type of evidence can be grouped under two major sub-headings: **visible and latent data**.



How Data is Stored

- HDD needs to have its space defined before it is ready for use.
- Partitioning HDD is the first step.
- When partitioned, HDDs are mapped (formatted) and have a defined layout.
- They are logically divided into **Sectors, Clusters, Tracks, and Cylinders.**



How Data is Stored - continued

- **Sectors** are typically 512 bytes in size.
  - Remember a byte is 8 bits .
  - A bit is a single 1 or 0.
- **Clusters are groups of sectors** and their size is defined by the operating system.
  - Clusters are always in sector multiples of two.
  - A cluster, therefore, will consist of 2, 4, 6, 8, or etc. sectors. (With modern day operating systems, the user can exercise some control over the amount of sectors per cluster.)
- **Tracks (concentric circles)** are defined around a platter.
- **Cylinders are groups of tracks** that reside directly above and below each other.

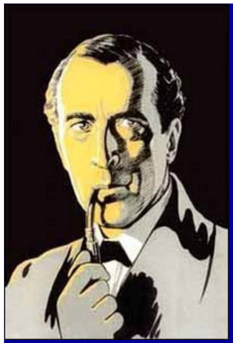
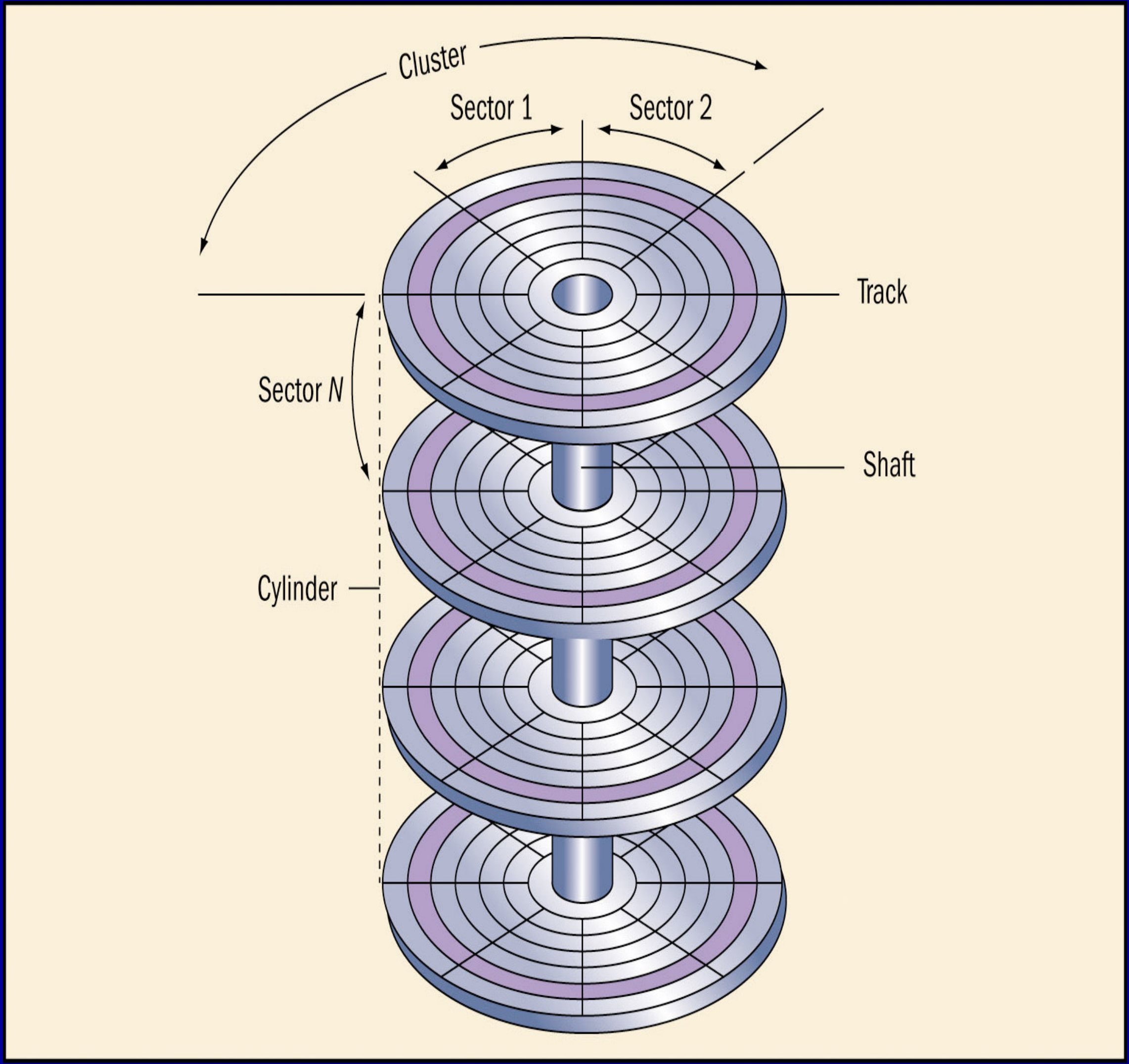
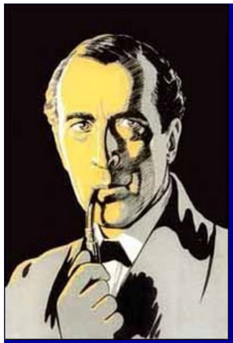


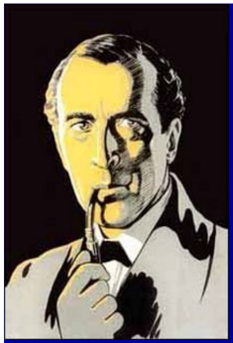
Fig. 17-3 Partitions of a Hard disc drive





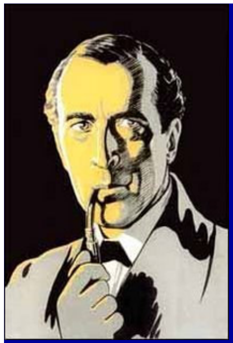
How Data is Stored - continued

- After partitioning and formatting are complete, the HDD will have a map of the layout of the defined space in that partition.
- Partitions utilize a File Allocation Table "FAT" to keep track of the location of files and folders (data) on the HDD.
- While the **NTFS partition** (most current Window systems-2000 and XP) utilizes, among other things, a **Master File Table** (MFT).



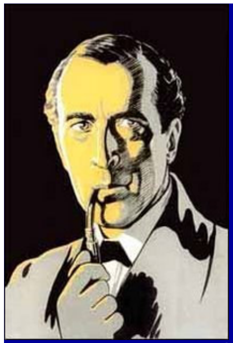
How Data is Stored - continued

- Each partition table (map) tracks data in different ways.
- The computer forensic examiners should be versed in the technical nuances of the HDDs they examine.
- It is sufficient for purposes here, however, to merely visualize the partition table as a map to where the data is located.
- This map uses the numbering sectors, clusters, tracks, and cylinders to keep track of the data.



Processing the Electronic CS

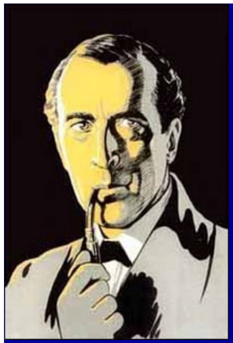
- Processing the electronic crime scene has a lot in common with processing a traditional crime scene.
  - Warrants
  - Documentation
  - Good investigation techniques
- At this point, a decision must be made as to whether a live acquisition of the data is necessary.



Shutdown vs. Pulling the Plug

- **Several factors influence the decision:**

- For example, if encryption is being used and pulling the plug will encrypt the data rendering it unreadable without a password or key, therefore pulling the plug would not be prudent.
- Similarly, if crucial evidentiary data exists in RAM and has not been saved to the HDD and will thus be lost with discontinuation of power to the system, another option must be considered.
- Regardless, the equipment will most likely be seized.

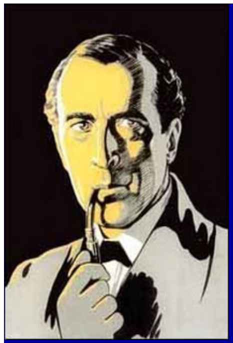


Forensic Image Acquisition

- After the items have been seized, the data needs to be obtained for analysis.
- The computer Hard Disk Drive will be used as an example, but the same “best practices” apply for other electronic devices as well.
- Throughout the entire process, the computer forensic examiner must adopt the method that is least intrusive.
- The goal with obtaining data from a HDD is to do so with out altering even one bit of data.

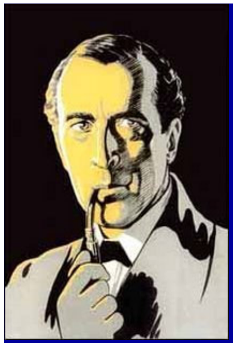
Forensic Image Acquisition – Continued

- Because booting a HDD to its operating system changes many files and could potentially destroy evidentiary data, obtaining data is generally accomplished by removing the HDD from the system and placing it in a laboratory forensic computer so that a forensic image can be created.
- Occasionally, in cases of specialized or unique equipment or systems the image of the HDD must be obtained utilizing the seized computer.
- Regardless, the examiner needs to be able to prove that the forensic image he/she obtained includes every bit of data and caused no changes (writes) to the HDD.



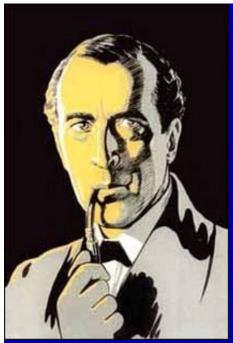
Computer Fingerprint

- To this end, a sort of fingerprint of the drive is taken before and after imaging.
- This fingerprint is accomplished through the use of a Message Digest 5 (MD5), Secure Hash Algorithm (SHA), or similar validated algorithm.
- Before imaging the drive the algorithm is run and a 32 character alphanumeric string is produced based on the drive's contents.
- It then run against the resulting forensic image and if nothing changed the same alphanumeric string will be produced, thus demonstrating that the image is all-inclusive of the original contents and that nothing was altered in the process.



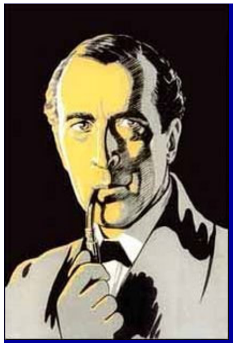
Visible Data

- Visible data is that data which the operating system is aware of.
- Consequently this data is easily accessible to the user.
- From an evidentiary standpoint, it can encompass any type of user created data like:
  - Word processing documents
  - Spread sheets
  - Accounting records
  - Databases
  - Pictures



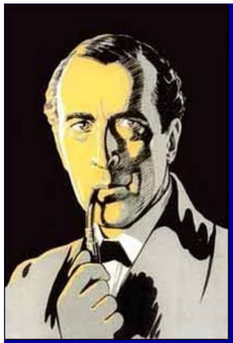
Temporary Files and Swap Space

- Temporary files, created by programs as a sort of “back-up on the fly” can also prove valuable as evidence.
- Finally, data in the swap space (utilized to conserve the valuable RAM within the computer system) can yield evidentiary data.
- Latent data, on the other hand, is that data which the operating system is not aware of.



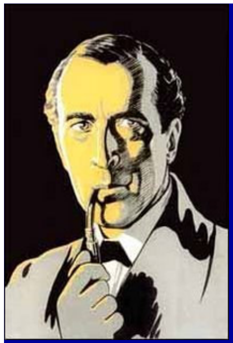
Latent Data

- Evidentiary latent data can exist in both in RAM and file slack.
- RAM slack is the area from the end of the logical file to the end of the sector.
- File slack is the remaining area from the end of the final sector containing data to the end of the cluster.
- Another area where latent data might be found is in unallocated space.
  - Unallocated space is that space on a HDD the operating system sees as empty and ready for data.



Latent Data - Continued

- The constant shuffling of data through deletion, defragmentation, swapping, etc., is one of the ways data is orphaned in latent areas.
- Finally, when a user deletes files the data typically remains behind.
- Deleted files are therefore another source of latent data to be examined during forensic analysis.

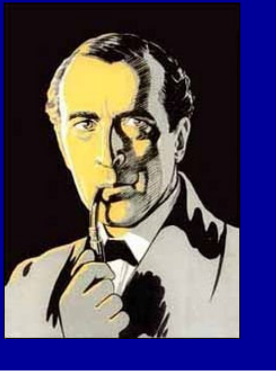


Knowledge and Skill

- Computer file systems and data structures are vast and complex.
- Therefore, areas of ***forensic analysis are almost limitless and constrained only by the knowledge and skill of the examiner.***
- With a working knowledge of a computer's function, how they are utilized, and how they store data, ***an examiner is on his or her way to begin to locate the evidentiary data.***

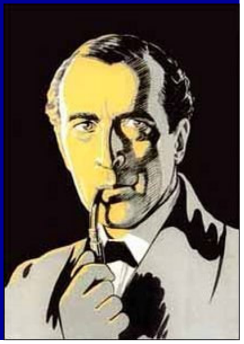
Computer Fraud !!

- Processing Electronic Crime Scene
  - Deleting files ?
    - How safe is it ?
    - How can you retrieve deleted data
    - Forensic Image Acquisition



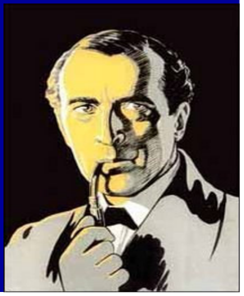
Computer Fraud !!

- Special techniques used by Computer experts
- Latent data (data supposed to be lost but found by computer expert)
- Unallocated space and its use
- Firewall
- Hacking



Computer Fraud !!

- Counterfeiting money - cases
- Internet fraud
- Search Engines
- Web sites
- Important Web sites



Computer Fraud !!

- The case of “Burning the house” after killing the wife
- Try to collect Insurance money
- Husband lies !!!
- But computer does not !!!!