Module 21
Forensics

Ansh Bhawnani

Introduction to Forensics

Module 21

Computer Forensics

- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
- Digital forensics is the process of ***identifying***, ***preserving***, ***analyzing***, and ***documenting digital evidence***. This is done in order to present evidence in a court of law when required.
- Mainly **four** types:
  - ***Computer*** Forensics
  - ***Mobile*** Forensics
  - ***Network*** Forensics
  - ***Cloud*** Forensics

Computer Forensics

- **Objectives/Benefits** of Digital Forensics
  - Ensure the integrity of the system
  - Track down cyber criminals
  - Recover lost or deleted information
  - To find ***digital evidence*** which can be presented in the court of law
  - Cyber crime monitoring and investigation

Forensic Career Paths

Module 21

Computer Forensics

- **Prerequisites**
  - Basic Computer Fundamentals (A+, Network+, Sec+ or equivalent)
- **Job Titles**
  - Cyber Crime Investigator
  - Cyber Forensic Investigator/Analyst/Examiner
  - Incident Response Analyst
- **Supplementary knowledge**
  - Pentesting
  - Malware Analysis
  - Security Consulting

Computer Forensics

Module 21

Computer Forensics

- **Computer forensics** is a branch of digital forensic science pertaining to evidence found in computers and digital storage media.
- *According to Steve Hailey*, "The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found."
- Computer forensics is equivalent of surveying a crime scene or performing an autopsy on a victim.

Computer Forensics

- Presence of a majority of electronic documents nowadays
- Search and identify data in a computer
- Digital Evidence is delicate in nature
- For recovering
  - *Deleted*,
  - *Encrypted* or,
  - *Corrupted* files from a system

Computer Forensics

Role of Cyber Forensics in tracking Cyber Criminals

- Identifying the crime
- Gathering the evidence
- Building a chain of custody
- Analyzing the evidence
- Presenting the evidence
- Testifying
- Prosecution

Computer Forensics

Computer Forensics Methodology

- *Acquire* evidence without modification or corruption
- *Authenticate* that the recovered evidence is same as the originally seized data
- *Analyze* data without any alterations

Investigation Process

Module 21

Investigation Process

- *Identification*: Detecting/identifying the event/crime.
- *Preservation*: Chain of Evidence, Documentation.
- *Collection*: Data recovery, evidence collection.
- *Examination*: Tracing, Filtering, Extracting hidden data.
- *Analysis*: Analyzing evidence
- *Presentation*: Investigation report, Expert witness
- *Decision*: Report

Investigation Process

Personnel

- The stages of the digital forensics process require different specialist training and knowledge
  - **Digital forensic technician**: Technicians gather or process ***evidence*** at crime scenes
  - **Digital Evidence Examiners**: Examiners specialize in one area of digital evidence

Investigation Process

Seizure

- Prior to the actual examination
- In criminal cases this will often be performed to facilitate the preservation of evidence.
- In criminal matters, law related to search warrants is applicable.
- *Crime scene*, *Quarantine*, *Recording Status*, *Network and Communication*, *Power*, *Additional items*, *threats and risks*

Investigation Process

Acquisition

- Exact sector level duplicate (or "forensic duplicate") of the media is created, usually via a write blocking device. Also called ***imaging***.
- The original drive is then returned to secure storage to prevent tampering.
- The acquired image is verified by using the *SHA-1* or *MD5* hash functions.
- Given the problems associated with imaging large drives, multiple networked computers, file servers that cannot be shut down and cloud resources new techniques have been developed

Investigation Process

Analysis

- “An in-depth systematic search of evidence related to the suspected crime".
- An investigator usually recovers evidence material using a number of different methodologies and tools The type of data include ***email***, ***chat logs***, ***images***, ***internet history*** or ***documents***.
- The data can be recovered from accessible disk space, deleted (***unallocated***) space or from within operating system cache files.
- Techniques involve ***keyword searching*** within the acquired image file, to filter out known file types. If identified, a deleted file can be reconstructed. Acquired data is hashed and compared to pre-compiled lists such as the ***Reference Data Set*** (RDS)

Investigation Process

Reporting

- When an investigation is completed the information is often reported in a form suitable for non-technical individuals.
- Reports may also include audit information and other meta-documentation.[3]
- When completed, reports are usually passed to those commissioning the investigation, such as ***law enforcement*** (for criminal cases) or the ***employing company*** (in civil cases), who will then decide whether to use the evidence in court.
- Generally, the report package will consist of a written expert conclusion of the evidence as well as the evidence itself (often presented on digital media)

Incident Response

Module 21

Incident Response

- Computer security incident is defined as “*Any real or suspected adverse event in relation to the security of computer systems or computer networks*“
- It also includes external threats such as gaining access to systems, disrupting their services through malicious spamming, execution of malicious codes that destroy or corrupt systems

Incident Response

How to Identify an Incident?

- A system alarm from an intrusion detection tool indicating security breach
- Suspicious entries in network
- Accounting gaps of several minutes with no accounting log
- Other events like unsuccessful login attempts, unexplained new user or files, attempts to write system files, modification or deleting of data
- Unusual usage patterns, such as programs being compiled in the account of users who are non-programmers

Incident Response

Whom to Report an Incident?

- Incident reporting is the process of reporting the information regarding the ***encountered security breach*** in a proper format.
- The incident should be reported to the ***CERT Coordination center***, ***site security manage***r, and other site.
- It can also be reported to law enforcement agencies such as ***FBI,USSS Electronic crimes branch*** or ***Department of Defense Contractors***.
- It should be reported to receive technical assistance and to raise security awareness to minimize the losses

Incident Response

Incident Reporting

- Intensity of the security breach
- Circumstances, which revealed vulnerability
- Shortcomings in the design and impact or level of weakness
- Entry logs related to intruder's activity
- Specific help needed should be clearly defined
- Correct time-zone of the region and synchronization information of the system with a National time server via NTP (Network Time Protocol)

Incident Response

- **Category of Incidents**
  - *Low level*
    - Loss of personal password
    - Suspected sharing of organization's accounts
    - Unsuccessful scans and probes
    - Presence of any computer virus or worms

Incident Response

Category of Incidents

- *Mid Level*
  - Violation of special access to a computer or computing facility
  - Unfriendly employee termination
  - Unauthorized storing and processing data
  - Destruction of property related to a computer incident (less than $100,000)
  - Computer virus or worms of comparatively larger intensity
  - Illegal access to buildings

Incident Response

Category of Incidents

- *High Level*
  - Denial of Service attacks
  - Suspected computer break-in
  - Computer virus or worms of highest intensity; e.g.Trojan back door.
  - Changes to system hardware, firmware or software without authentication.
  - Destruction of property exceeding $100,000.
  - Any kind of pornography, gambling or violation of law.

Incident Response

Procedure for Handling Incident

- The stages are:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Follow up

Incident Response

What Is CSIRT?

- A team of trained professionals
- CSIRT members detect incidents at early stages and make reports to prevent further incidents
- It secures organization's data, hardware, and critical business policy
- It provides training on security awareness, intrusion detection, and penetration testing
- It strengthens organization's security
- Decreases the response time during future security breach

Hard Disks and File Systems

Module 21

1. Hard Disks

Module 21

Hard Disks and File Systems

Hard Disks

- A rapidly spinning platter is used as the recording medium. Heads just above the surface of the platter are used to read data from and write data to the platter. A standard interface connects a hard disk to a computer. Two common interfaces are IDE and SCSI.
- **Characteristics**
  - Capacity of the hard disk
  - Interface used
  - Speed in rotations per minute
  - Seek time
  - Access time
  - Transfer time

Hard Disks and File Systems

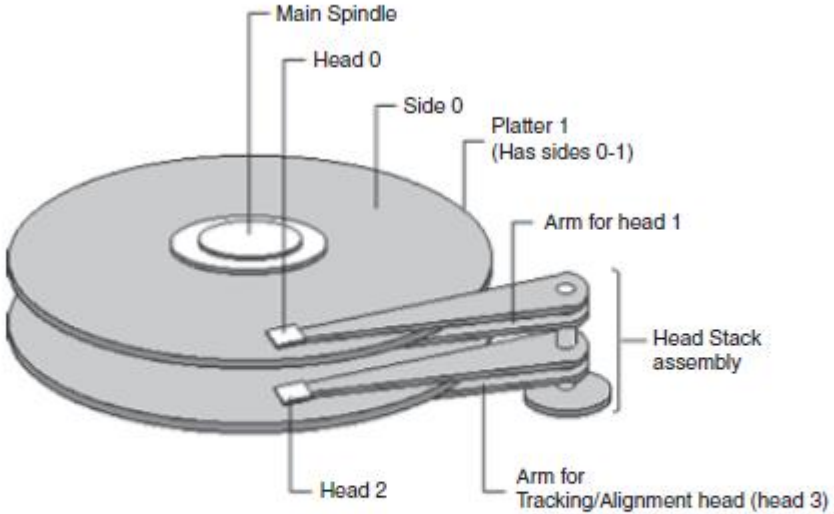
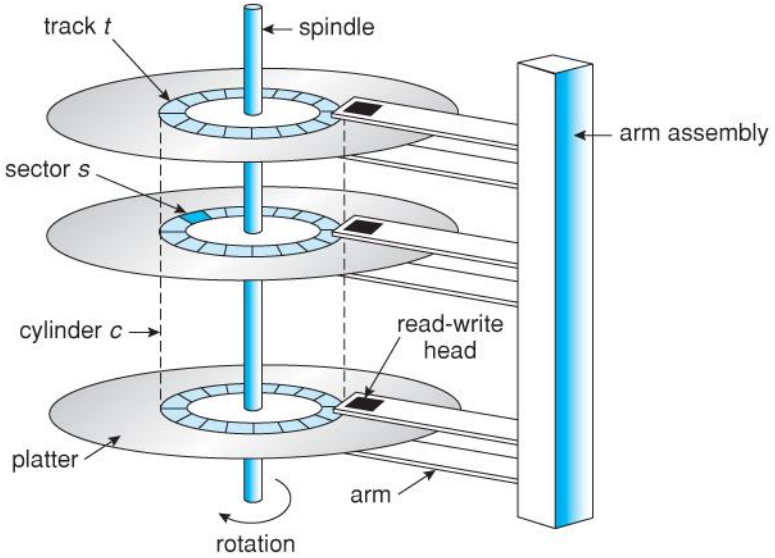
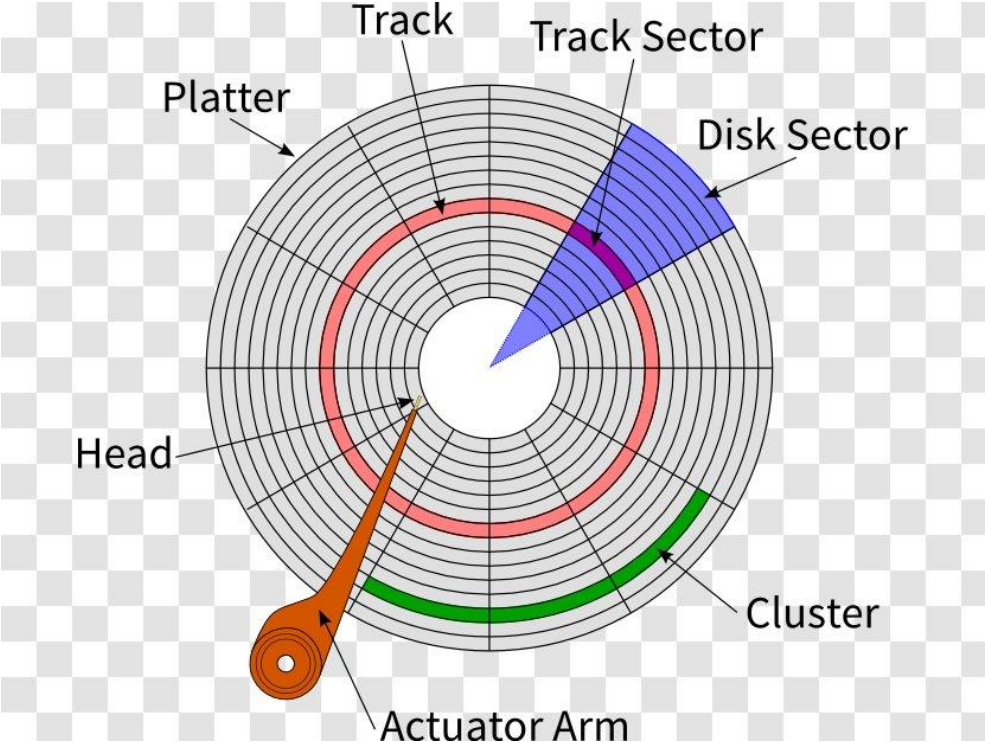


Figure 1-1 A hard disk platter has two sides, and there is a read/write head for each side.

Hard Disks and File Systems



Hard Disks and File Systems



Hard Disks and File Systems

Hard Disk Interfaces

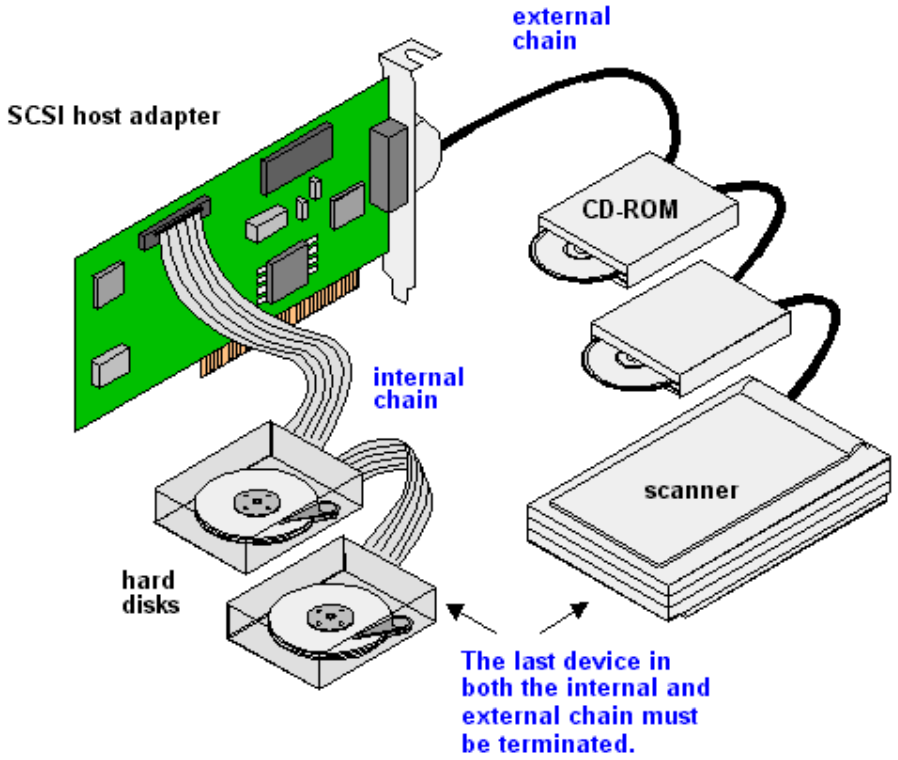
- *Small computer system interface (SCSI)*: Allows a user to connect 15 peripheral devices to one PCI board known as a SCSI host adapter, which is plugged into the motherboard.
- ***Integrated drive electronics/enhanced IDE (IDE/EIDE)***: Connects hard disk drives, optical disc drives, and tape drives to personal computers. With this type of interface, the drive controller is built into the motherboard.
- ***Universal Serial Bus (USB)***: Connects peripheral devices such as hard disks, modems, printers, digitizers, and data gloves to a computer.

Hard Disks and File Systems

Hard Disk Interfaces

- *Advanced technology attachment (ATA)*: This type of interface comes in two forms:
  - ***Serial ATA***: This provides a point-to-point channel between the motherboard and the drive.
  - ***Parallel ATA***: This provides a communications channel between the drive and the computer on which data can travel only one way at a time.
- *Fiber Channel*: A point-to-point bidirectional serial interface that supports up to 1.0625 Gbps transfer rates.

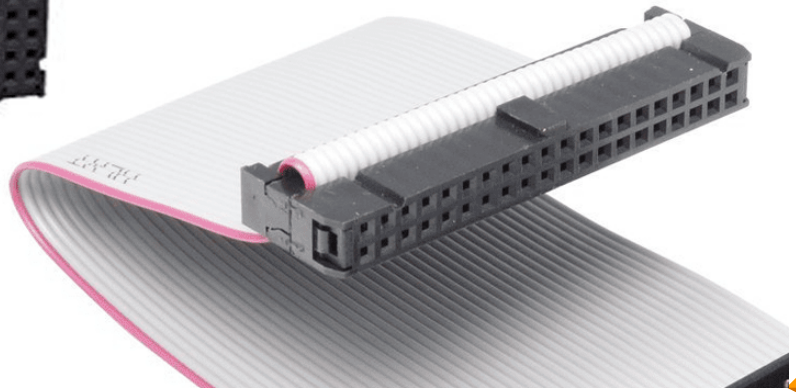
Hard Disks and File Systems



Hard Disks and File Systems

34-pin

40-pin



PATA and SATA cables

2. Master Boot Record

Module 21

Hard Disks and File Systems

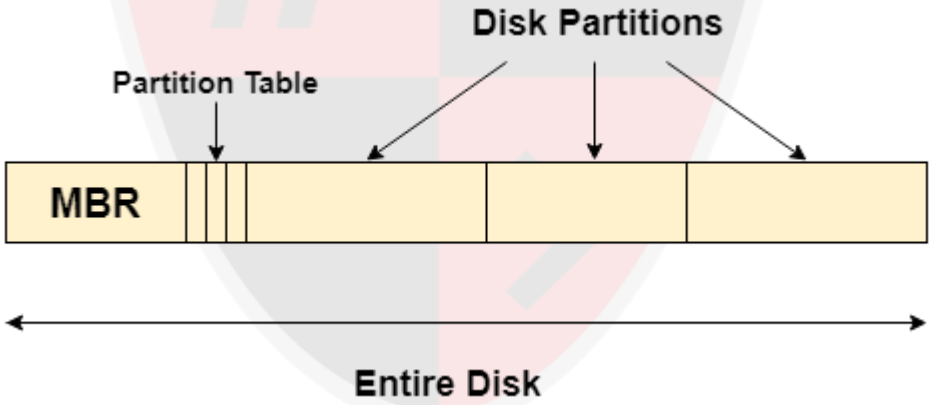
Master Boot Record

- The ***master boot record (MBR)*** is the first sector of a data storage device such as a hard disk.
- Also called the master partition table, it includes a table that contains information about each partition that the hard disk has been formatted into. The ***boot sector*** is the sector of a storage device that contains the code for bootstrapping a system.

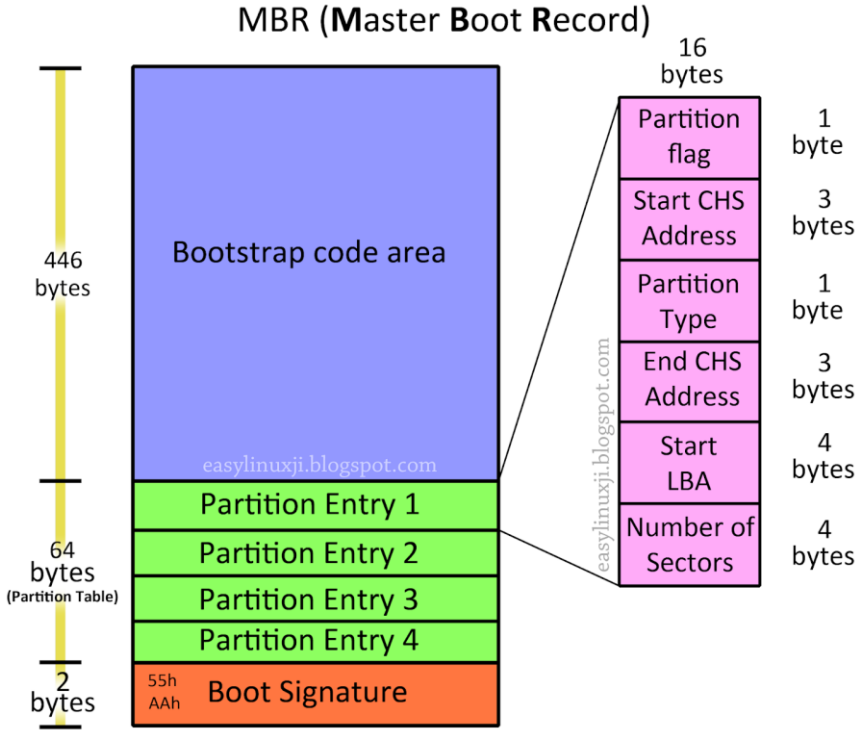
Bootstrapping is the process by which a small program actually initializes the operating system installed on a computer. In DOS and Windows systems, a user can create the MBR with the **fdisk/mbr** command.

Hard Disks and File Systems

- MBR is ***used*** to:
  - Bootstrap operating systems
  - Hold disk partition tables



Hard Disks and File Systems



Hard Disks and File Systems

- MBR **characteristics**:
  - Supports upto 2 TB disk
  - Maximum 4 primary partitions, supports extended partitioning
  - Compatible with UEFI

Hard Disks and File Systems

- **GUID Partition Table** (GPT)
  - New standard, Works with ***UEFI*** BIOS, new H/W
  - Supports upto 128 primary partitions
  - Support upto zettabytes of disk space
  - Support data integrity check (***CRC***), and inherent recovery
  - Supported in x64 architecture for Windows (starting Server 2003 SP1), and both for Linux
  - More robust than MBR

3. Registry Data

Module 21

Hard Disks and File Systems

- The window registry contains a set of predefined keys:
  - *HKEY_CURRENT_USER*: It is abbreviated HKCU and can be scanned for information about the configuration of the user currently logged in.
  - *HKEY_USERS*: HKEY_CURRENT_USER is a subkey of HKEY_USERS. It can be checked for all the user profiles loaded on the computer.
  - *HKEY_LOCAL_MACHINE*: It is abbreviated HKLM and can be searched for the configuration information of a particular computer.

Hard Disks and File Systems

- The window registry contains a set of predefined keys:
  - *HKEY_CLASSES_ROOT*: It is a subkey of HKEY_LOCAL_MACHINE\Software. The information stored in this key ensures that the correct program opens when a file is opened in Windows Explorer.
  - *HKEY_CURRENT_CONFIG*: This key contains data about the hardware profile used by the local computer at start-up.

Hard Disks and File Systems

- The various registry hives and their supporting files in Windows are listed below:
  - HKEY_LOCAL_MACHINE\SAM — Sam, Sam.log, Sam.sav
  - HKEY_LOCAL_MACHINE\Security — Security, Security.log, Security.sav
  - HKEY_LOCAL_MACHINE\Software — Software, Software.log, Software.sav
  - HKEY_LOCAL_MACHINE\System — System, System.alt, System.log, System.sav
  - HKEY_CURRENT_CONFIG — System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
  - HKEY_USERS\DEFAULT — Default, Default.log, Default.sav

4. Boot Sequence

Module 21

Hard Disks and File Systems

- **Boot Loader**: A boot loader or boot manager is a program that loads the operating system into a computer's memory when the system is booted. Multiple-stage boot loaders—where a number of small programs call each other, and the last program loads the operating system —are common.
- **Boot Sector**: A boot sector is a memory sector of a hard disk, floppy disk, or similar data storage device that contains code for bootstrapping systems. The boot sector on a disk is always the first sector on the first track.

Hard Disks and File Systems

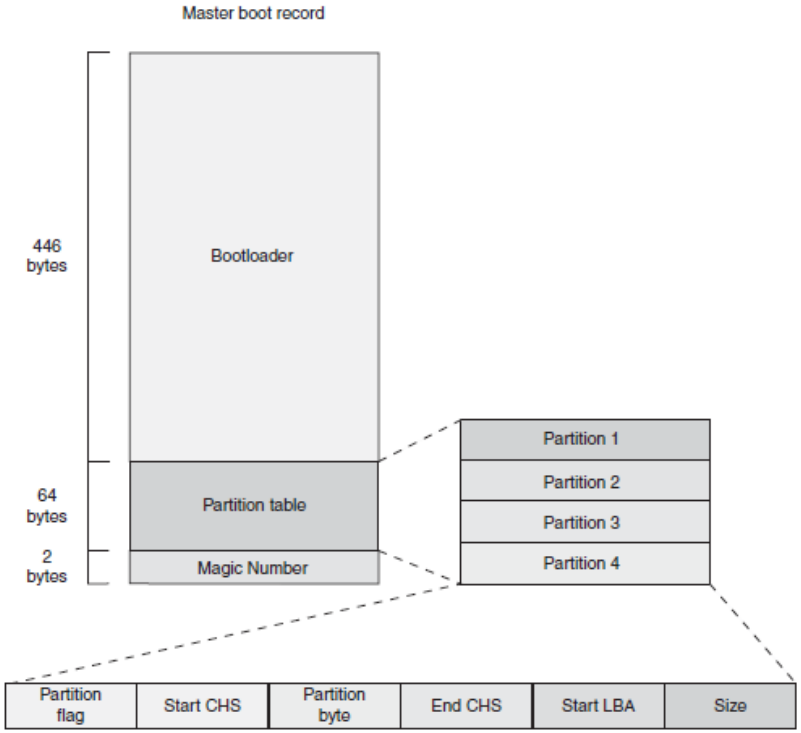
Basic System Boot Process:

- The system clock generates a series of clock ticks, which initializes the CPU.
- The CPU looks to the system's startup program in the ROM BIOS for its first instruction.
- The first instruction is to run the power-on self-test (POST), in a predetermined memory address.
- POST checks the BIOS chip and then tests CMOS RAM. ***CMOS* (complementary metal-oxide semiconductor)** memory holds the system date, time, and setup parameters.

Hard Disks and File Systems

- If there is no battery failure, POST checks the inventoried hardware devices such as the video card; secondary storage devices, such as hard drives and floppy drives; ports; and other hardware devices, such as the keyboard and mouse, to check whether they are functioning properly.
- CPU initialization is completed if everything is fine.
- The BIOS looks into the CMOS chip to find the drive where the OS is installed.
- The BIOS then checks the boot record of the drive to find the beginning of the OS and the subsequent program file that initializes the OS.
- The BIOS copies its files into memory after OS initialization.

Hard Disks and File Systems



Source: http://www.ibm.com/developerworks/linux/library/l-linuxboot/. Accessed 2/2007.

Windows Forensics

Module 21

1. Volatile Information

Module 21

Windows Forensics

- ***Volatile information*** is information that is lost the moment a system is powered down or loses power. Volatile information usually exists in physical memory, RAM
  - *System time*
  - *Logged-on user(s)*
  - *Open files*
  - *Network information*
  - *Network connections*
  - *Process information*
  - *Process-to-port mapping*

Windows Forensics

- *Process memory*
- *Network status*
- *Clipboard contents*
- *Service/driver information*
- *Command history*
- *Mapped drives*
- *Shares*

2. Non-Volatile Information

Module 21

Windows Forensics

- ***Nonvolatile information*** is kept on secondary storage devices and persists after a system is powered down. It is nonperishable and can be collected after the volatile information is collected.
  - *Hidden files*
  - *Slack space*
  - *Swap files*
  - *Index.dat files*
  - *Metadata*
  - *Hidden ADS (alternate data streams)*

Windows Forensics

- *Windows Search index*
- *Unallocated clusters*
- *Unused partitions*
- *Hidden partitions*
- *Registry settings*
- *Connected devices*
- *Event logs*

3. Inside the Registry

Module 21

Windows Forensics

- *Registry Structure Within a Hive File*
- *Registry Analysis*
- *System Information*
- *Time Zone Information*
- *Shares*
- *Audit Policy*
- *Wireless SSIDs*

Windows Forensics

- *Autostart Locations*
- *USB Removable Storage Devices*
- *MountedDevices*
- *Finding Users*
- *Tracking User Activity*
- *Analyzing Restore Point Registry Settings*
- *Determining the Startup Locations*

4. MD5 Calculation

Module 21

MD5 Calculation

- The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D.
- These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a nonlinear function F, modular addition, and left rotation.

MD5 Calculation

- The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D.
- These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a nonlinear function F, modular addition, and left rotation.

Tools: *ChaosMD5, Secure Hash Signature Generator, MatMD5, MD5 Checksum Verifier*

5. Recycler Bin

Module 21

Windows Forensics

- Forensic investigators are aware of the old adage that when a file is deleted, it is not really gone.
- The file is simply moved to the Recycle Bin, which appears by default as the Recycler directory at the root of each drive.
- As a user on a system begins to delete files through the shell, a subdirectory is created for that user within the Recycler directory; that subdirectory is named with the user's security identifier, or SID. For example, the subdirectory will look something like this:
  - C:\RECYCLER\S-1-5-21-1454471165-630328440-725345543-1003

Windows Forensics

- When an investigator opens the Recycle Bin from the desktop, the current user's subdirectory is automatically opened for view. Files sent to the Recycle Bin are maintained according to a specific naming convention. When a file is moved to the Recycle Bin, it is renamed using the following convention:
  - D<original drive letter of file><#>.<original extension>

6. NTFS Alternate Data Streams

Module 21

- ADSs were added to the file system to support the Hierarchal File System (HFS) used by the Macintosh. HFS employs resource forks so that the file system can maintain metadata about the file, such as icons, menus, or dialog boxes.
- The simplest way to ***create an ADS*** is to type the following command:
  - **notepad myfile.txt:ads.txt**
  - Add some text to the Notepad window, save the file, and then close Notepad.
  - Another way to create an ADS is to use the echo command:
  - **echo “This is another ADS test file” > myfile.txt:ads2.txt**

- Typing **dir** or viewing the contents of the directory in Windows Explorer will show that the file will be zero bytes in size.
- Yet another way to create an ADS is to use the type command to copy another file into the ADS:
  - **type c:\windows\system32\sol.exe > myfile.txt:ads3.exe**
- ADSs can be added to directory listings as well, using the following syntax:
  - **echo “This is an ADS attached to a directory” > :ads.txt**

Windows Forensics

Enumerating ADSs

- Vista allows a user to enumerate ADSs with dir using the /r switch. ***Lads.exe*** is another tool that a user can use to list ADSs and can be run against any directory.

Removing ADSs

- One way to remove an ADS is to simply delete the file to which the ADS is attached.
- Another option is to copy the file to a non-NTFS media like a partition formatted in FAT, FAT32, or some other file system.

7. Executable File Analysis

Module 21

Windows Forensics

- Executable file analysis is a process of gathering information from an executable file. It is classified into two types as follows:
  - ***Static analysis***: Static analysis is a process that consists of collecting information about and from an executable file without actually running or launching the file in any way.
  - ***Dynamic analysis***: Dynamic analysis involves launching an executable file in a controlled and monitored environment so that its effects on a system can be observed and documented.

Static Analysis Process:

- Scan the suspicious file with antivirus software like *Norton*, *AVG*, or *McAfee*.
- Search for strings.
- Analyze PE header.
- Analyze import tables.
- Analyze export table.

Dynamic Analysis Process:

- Create a testing environment.
- Use virtualization tools such as *Bochs*, *Parallels*, *Microsoft's Virtual PC*, Virtual Iron, and *VMware*.
- Start the process of testing the executable.

Linux Forensics

Module 21

Linux Forensics

- Linux has a number of simple utilities for imaging and basic disk analysis, including the following:
  - ***dd***: Copies data from an input file or device to an output file or device
  - ***sfdisk*** and ***fdisk***: Determines the disk structure
  - ***grep***: Searches files for instances of an expression or pattern
  - ***md5sum*** and ***sha1sum***: Create and store an MD5 or SHA-1 hash of a file or list of files (including devices)
  - ***file***: Reads file header information in an attempt to ascertain its type, regardless of name or extension
  - ***xxd***: Command-line hex dump tool

1. Data collection

Module 21

Linux Forensics

- **Media mounting:**
  - Mount the toolkit on the external media:
    - **mount -n /mnt/cdrom**
  - Calculate the hash value of the collected file:
    - **md5sum date_compromised > date_compromised.md5**
- **Current date:**
  - Collect the current date result, presented in UTC format:
    - **nc -l -p port > date_compromised**
    - **/mnt/cdrom/date -u | /mnt/cdrom/nc <remote port>**
    - **md5sum date_compromised > date_compromised.md5**

- Cache tables:
  - Collect the Mac address cache table:
    - nc -l -p <port> > arp_compromised
    - /mnt/cdrom/arp -an | /mnt/cdrom/nc <remote port>
    - md5sum arp_compromised > arp_compromised.md5
- Collect the kernel route cache table:
    - nc -l -p <port> > route_compromised
    - /mnt/cdrom/route -Cn | /mnt/cdrom/nc <remote port>
    - md5sum route_compromised > route_compromised.md5

Linux Forensics

- Current, **pending connections** and **open TCP/UDP ports**:
  - Collect information about current connections and open TCP/UDP ports:
    - **nc -l -p <port> > connections_compromised**
    - **/mnt/cdrom/netstat -an | /mnt/cdrom/nc <remote port>**
    - **md5sum connections_compromised > connections_compromised.md5**
- **Physical memory image**:
    - Access physical memory directly by copying the /dev/mem device or by copying the kcore file, located in the pseudo–file system mounted in the /proc directory:
    - **nc -l -p <port> > kcore_compromised**
    - **/mnt/cdrom/dd < /proc/kcore | /mnt/cdrom/nc <remote port>**

- **List modules loaded to kernel memory**:
  - Check which modules are currently loaded into memory:
    - **nc -l -p <port> > lkms_compromised**
    - **/mnt/cdrom/cat /proc/modules | /mnt/cdrom/nc <remote port>**
    - **nc -l -p <port> > lkms_compromised.md5**
    - **/mnt/cdrom/md5sum /proc/modules | /mnt/cdrom/nc <remote port>**
  - Analyze the ksyms file to detect the presence of an intruder:
    - **nc -l -p <port> > ksyms_compromised**
    - **/mnt/cdrom/cat /proc/ksyms | /mnt/cdrom/nc <remote port>**

- **List active processes:**
  - Collect information about all processes, open ports, and files with the use of the *lsof* command:
    - **nc -l -p <port> > lsof_compromised**
    - **/mnt/cdrom/lsof -n -P -l | /mnt/cdrom/nc <remote port>**
    - **md5sum lsof_compromised > lsof_compromised.md5**

Mobile Forensics

Module 21

Mobile Forensics

- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data

Mobile Forensics

- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
- User dictionary content
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all of the above

Mobile Forensics

Seizure

- Digital forensics operates on the principle that evidence should always be adequately preserved, processed, and admissible in a court of law. Some legal considerations go hand in hand with the confiscation of mobile devices.

Airplane Mode

- Mobile devices are often seized switched on; and since the purpose of their confiscation is to preserve evidence, the best way to transport them is to attempt to keep them turned on to avoid a shutdown, which would inevitably alter files.

Mobile Forensics

Phone Jammer

- A **mobile phone jammer** or **blocker** is a device which deliberately transmits signals on the same radio frequencies as mobile phones, disrupting the communication between the phone and the cell-phone base station.

Mobile Forensics

Faraday bag

- It is a container specifically designed to isolate mobile devices from network communications. Before putting the phone in the Faraday bag, disconnect it from the network, disable all network connections (Wi-Fi, GPS, Hotspots, etc.), and activate the flight mode

Mobile Forensics

Acquisition

- The goal of this phase is to retrieve data from the mobile device. A locked screen can be unlocked with the right PIN, password, pattern, or biometrics.
- Investigators should be attentive to any indications that may transcend the mobile device as a physical object, because such an occurrence may affect the collection and even preservation process.
- The forensic examiner should make a use of SIM Card imaging – a procedure that recreates a replica image of the SIM Card content. As with other replicas, the original evidence will remain intact while the replica image is being used for analysis.

Mobile Forensics

Examination & Analysis

- As the first step of every digital investigation involving a mobile device(s), the forensic expert needs to identify:
  - *Type of the mobile device(s)* – e.g., GPS, smartphone, tablet, etc.
  - *Type of network* – GSM, CDMA, and TDMA
  - *Carrier*
  - *Service provider* (Reverse Lookup)

Mobile Forensics

Non-invasive methods

- Non-invasive methods can deal with other tasks, such as unlocking the SIM lock or/and the operator lock, the operating system update, IMEI number modification, etc.
  - **Manual extraction:** Merely browses through the data using the mobile device's touchscreen or keypad. Information of interest discovered on the phone is photographically documented.
  - **Logical extraction**: Instituting a connection between the mobile device and the forensic workstation using a USB cable, Bluetooth, Infrared or RJ-45 cable.

Mobile Forensics

Non-invasive methods

- **JTAG method:** Could extract data from a mobile device even when data was difficult to access through software avenues because the device is damaged, locked or encrypted.
- **Hex Dump:** It is performed by connecting the forensic workstation to the device and then tunneling an unsigned code or a bootloader into the device, each of them will carry instructions to dump memory from the phone to the computer.

Mobile Forensics

Invasive Methods

- In cases where the device is entirely non-functional due to some severe damage, it is very likely the only way to retrieve data from the device might be to manually remove and image the flash memory chips of the device.
  - **Chip-off:** A process that refers to obtaining data straight from the mobile device's memory chip.
    - Detect the memory chip typology of the device
    - Physical extraction of the chip (for example, by unwelding it)
    - Interfacing of the chip using reading/programming software
    - Reading and transferring data from the chip to a PC
    - Interpretation of the acquired data (using reverse engineering)

Mobile Forensics

Invasive Methods

- **Micro read:** This method refers to manually taking an all-around view through the lenses of an electron microscope and analyzing data seen on the memory chip, more specifically the physical gates on the chip.
- In a nutshell, micro read is a method that demands utmost level of expertise, it is costly and time-consuming, and is reserved for serious national security crises.

Forensic Reporting

Module 21

Investigation Process

Reporting

- When an investigation is completed the information is often reported in a form suitable for non-technical individuals.
- Reports may also include audit information and other meta-documentation.[3]
- When completed, reports are usually passed to those commissioning the investigation, such as ***law enforcement*** (for criminal cases) or the ***employing company*** (in civil cases), who will then decide whether to use the evidence in court.
- Generally, the report package will consist of a written expert conclusion of the evidence as well as the evidence itself (often presented on digital media)

Forensic Reporting

Most forensic reports, follow the general guideline below for a table of contents:

1. Brief summary of information
2. Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
3. Repository #1 (For example A's work computer)
    a. Summary of evidence found on Employee A's work computer
    b. Analysis of relevant portions of Employee A's work computer
        i. Email history
        ii. Internet search history
        iii. USB registry analysis
        iv. Etc.
    c. Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)
4. Recommendations and next steps for counsel to continue or cease investigation based on the findings in the reports.

HACKING

Is an art, practised through a creative mind.