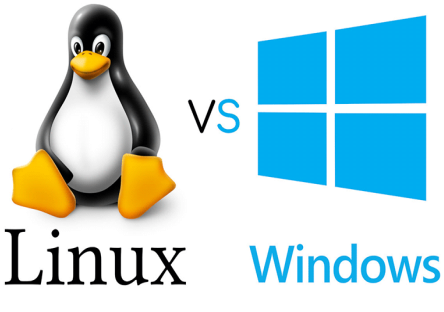
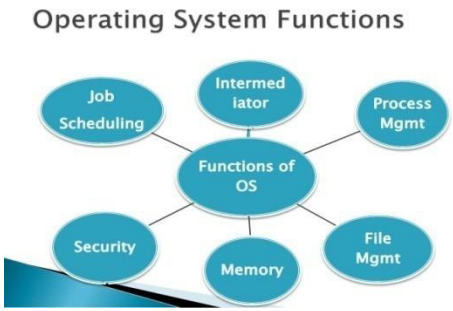
CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

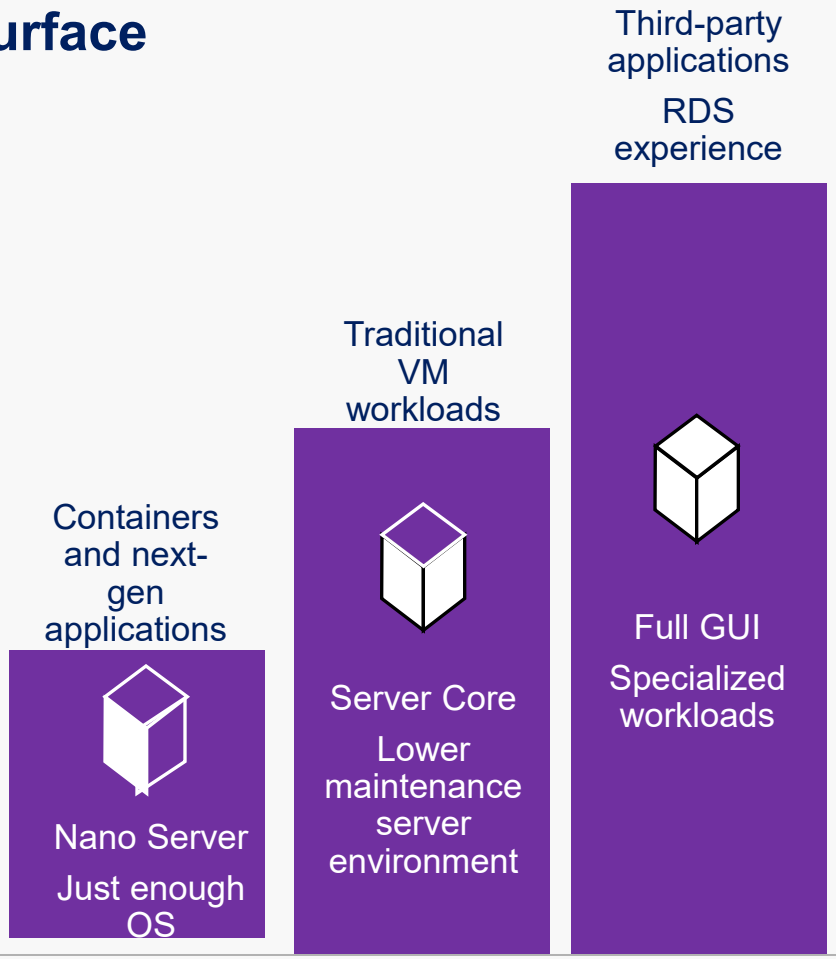
Week3Day2 : Windows Operating Systems: Configuring Server Devices, Containers, Software Defined Storage System File Checker, Windows Boot Sequence, UEFI, File System





Optimized for next-gen distributed applications

- Higher density and Reduced attack surface and servicing requirements
- Next-gen distributed app frameworks
- Interoperate with existing server applications



Windows Server 2022 Standard

- The Standard Edition is the base version of Windows Server 2022.
- The single license of the standard version can only work with two virtual machines and one Hyper-V host.
- The Replica Storage option is available with one partnership and one resource group with a capacity of 2 terabytes.
  - Features such as hot patching, software-defined networking and storage are not available in the standard version.

Windows Server 2022 Datacenter

- This version has elite features that are not part of the Standard Edition, such as protected VMs.
  - This feature protects the firmware and startup files of the VM and also enables BitLocker disk encryption.
- As data protection and management are critical to enterprise-level infrastructure, Microsoft integrates two key functions:
  - Software-defined storage and
  - Storage replication with Storage Spaces Direct.
- Storage replication provides block-level data replication without data loss and even replicates open files.
- Software-defined storage with Storage Spaces Direct enables manageability and scalability – supports up to 16 servers and up to 1 petabyte of cluster storage.

Windows Server 2022 Datacenter Azure Edition

- It is designed for the Microsoft Azure platform.
- It has excellent features that are not available in Standard Edition and Data Center Edition.
  - For example, the Hot Patch feature allows you to install updates without restarting the server, and Server Message Block via QUIC provides access to shared files without the need for a VPN over the network.
- Windows 2022 Azure Edition runs virtual machines on the Azure Stack Hyper-Converged Infrastructure (HCI) operating system, known for its security, performance, and new hybrid capabilities.

Storage Enhancement

- **The innovation at the storage level represents one of the major improvements on Windows 2022 servers. Daily data management has become a problem for data engineers. In such scenarios, advanced storage upgrades are built into the 2022 servers:**
  - **Advanced caching:** Automatically stores important data on faster storage volumes and less critical data on slower volumes. This allows for faster access to read and write operations.
  - **Faster, Manageable Storage Improvements:** Fixes the hard drive faster in case of server restart or hardware failure.
  - **ReFS file snapshots:** ReFS snapshots use a unique method known as fast metadata operations to take snapshots of data at constant time, regardless of size.

Security Updates

- Windows Server 2022 offers three major security enhancements, including
  - hardware trust,
  - firmware protection, and
  - virtual environment security, as the cloud is the second most used platform.
- The most notable improvements are secure DNS support with DNS-over-HTTPS, Server Message Block AES-256 and SMB East-West encryption, SMB over QUIC, HTTPS and TLS 1.3, Azure Arc, and Azure Auto-manage.
- These security protocols and enhancements ensure that the windows 2022 server is self-reliant to process sensitive data and critical applications.
- The entire server core is protected from the perspective of hardware, firmware, and the drivers to prevent today's complex attacks.

Security Updates

- **Firmware attack prevention:** Extended threats and attacks occur during a server restart via firmware. Technologies such as DRTM (Dynamic Root of Trust for Measurement) and DMA (Direct Memory Access) are used to prevent such cyber attacks.
- **Hypervisor security:** The hypervisor is protected by virtualization-based security technology (VBS). This technology isolates individual processes from the operating system. In the event of an attack, the attack does not spread to other parts of the system and avoids the entire server getting compromised.
- **Secure Connectivity:** By default, the latest version of the internet protocol, Transport Layer Security (TLS), is used to establish a secure connection between two nodes. Even the name resolution is separated using encrypted DNS queries.
- **Server Message Block (SMB):** The new SMB functionality through QUIC eliminates the need for a VPN for remote workers, mobile users, and highly secure organizations. It uses UDP (Use Datagram Protocol) and ensures that Internet traffic always remains encrypted.
  - SMB over QUIC **offers an "SMB VPN" for telecommuters, mobile device users, and high security organizations**. The server certificate creates a TLS 1.3-encrypted tunnel over the internet-friendly UDP port 443 instead of the legacy TCP port 445.

Security Updates

- SMB over QUIC introduces an alternative to the TCP network transport, providing secure, reliable connectivity to edge file servers over untrusted networks like the Internet. QUIC is an IETF-standardized protocol with many benefits when compared with TCP:
  - All packets are always encrypted and handshake is authenticated with TLS 1.3
  - Parallel streams of reliable and unreliable application data
  - Exchanges application data in the first round trip (0-RTT)
  - Improved congestion control and loss recovery
  - Survives a change in the clients IP address or port
- All SMB traffic, including authentication and authorization within the tunnel is never exposed to the underlying network. SMB behaves normally within the QUIC tunnel, meaning the user experience doesn't change. SMB features like multichannel, signing, compression, continuous availability, directory leasing, and so on, work normally.

Deprecated Features in Windows Server 2022

- With its release of Windows Server 2022, Microsoft has deprecated, either partially or entirely, the following features found in Windows Server 2019 and earlier Windows Server versions:
  - **Internet Storage Name Service (iSNS):** With its focus on SMB, Microsoft finally decided to remove iSNS altogether. However, you can still connect to existing iSNS servers or add individual iSCSI targets.
  - **Guarded Fabric and Shielded VMs:** With Azure Confidential Computing and Azure Security Center becoming a significant focus, further development of this feature has been halted, although support for the feature will continue.
  - **Running sconfig.cmd from a CMD window:** Sconfig is now launched by default when signing into a server with Server Core installed. If you need to run Sconfig, you must do it from PowerShell, which is now the default shell on Server Core.
  - **Deploying images with Windows Deployment Services (WDS) boot.wim:** Workflows that rely on WDS will still be allowed to run but not after showing a deprecation notice. Moving forward, WDS images will be blocked on Windows 11 and future Windows Server versions. This is being done since there are now better, more capable options for deploying Windows images.

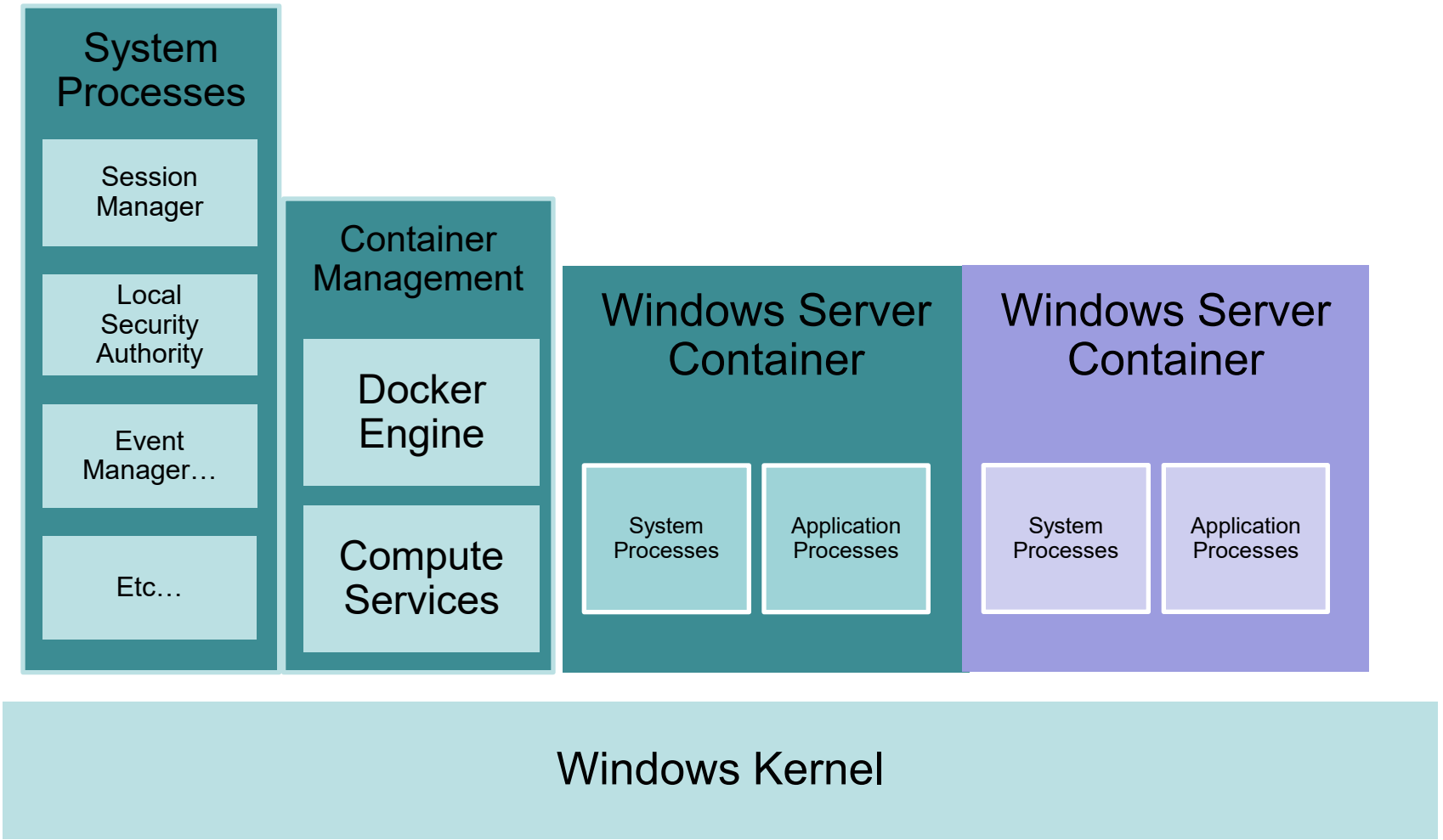
Containers and Virtulization

- Virtualization and container-based apps are focus areas for Windows Server 2022 including some features that lean heavily toward hybrid capabilities with Azure.
- One of these is the HostProcess container type for Kubernetes, which is new in Windows Server 2022 but will also be backported to Windows Server 2019.
- HostProcess containers run directly at the host layer in the same network namespace as the host, with similar access to the host OS as processes running directly on the server.
  - Because of the level of access that HostProcess containers have to the OS, they can be used for management tasks and DevOps scenarios, taking advantage of both the access and the development and deployment tools inherently offered by containers.

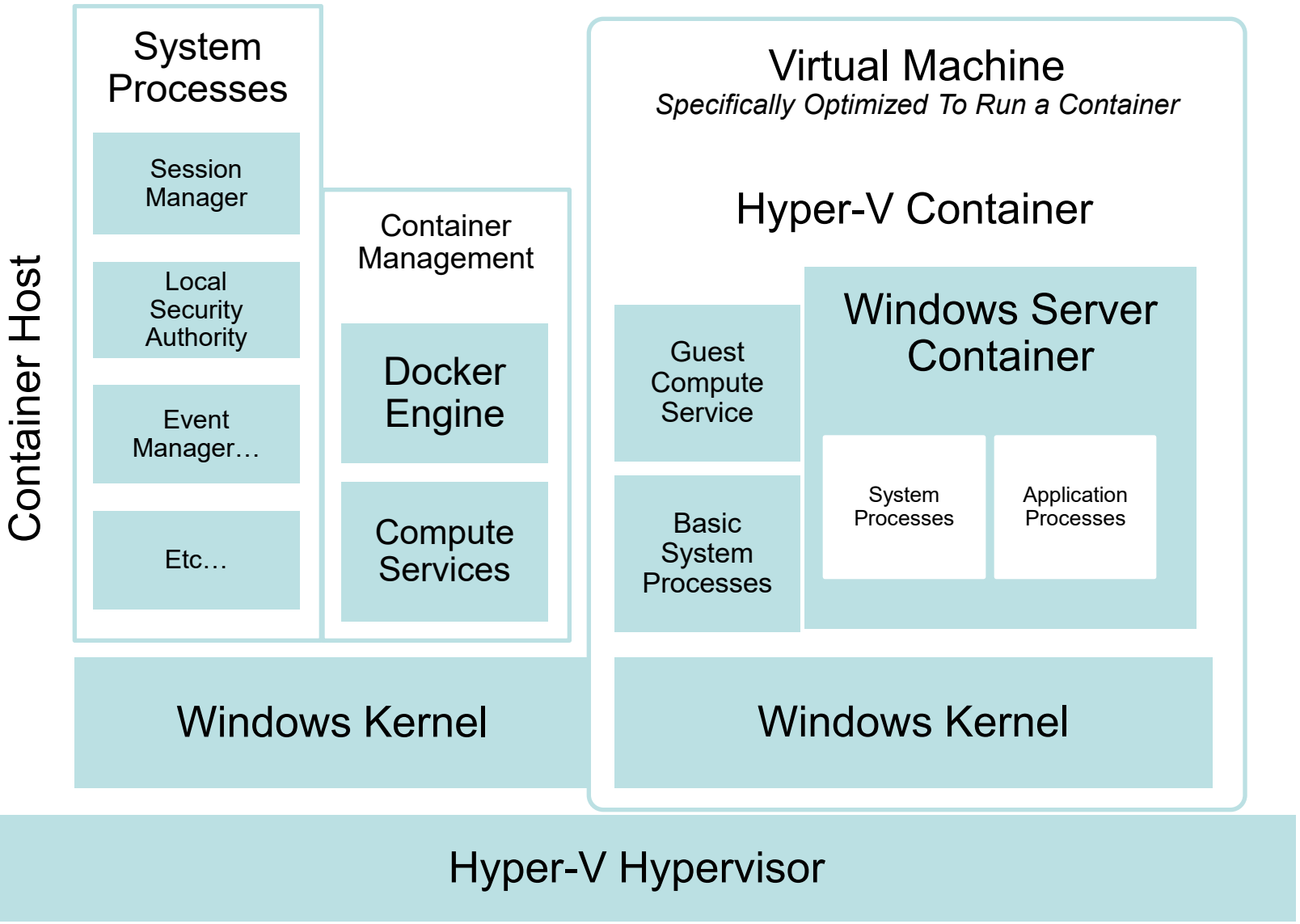
Containers and Virtulization

- New to Windows Server 2022 is support for nesting virtual machines on AMD processors. Previously, nested virtualization--running Hyper-V within a Hyper-V guest--was limited to Intel processors.
- Nested virtualization can be used for a variety of scenarios including packaging and distributing multi-server systems for things like development or training or spinning up virtual machines from backup within isolated environments.
- Group Managed Service Accounts (gMSA)
  - In Active Directory, gMSAs provide a secure mechanism for applications, even those distributed across multiple nodes, to access network resources without requiring manual account management like making password changes; instead Active Directory manages the account.
  - What's new about gMSA in Windows Server 2022 is that gMSA can be leveraged on hosts not joined to an Active Directory domain.
  - This is done by creating an account in Azure AD, providing the benefits of gMSA by allowing container apps to access resources through the Azure AD account. There are additional benefits as well: Removing the requirement to domain-join Worker nodes facilitates scalability, and a secret store can be leveraged in order to manage and share credentials between multiple container hosts.

Windows Server Containers



Hyper-V Containers



Multitasking and Multithreading

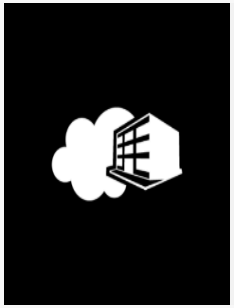
- **Multitasking**
  - The ability to run two or more programs at the same time
- **Multithreading**
  - The capability of programs written to run several program code blocks, or "threads," at the same time
- **Preemptive multitasking**
  - Each program runs in an area of memory separate from areas used by other programs
  - Reduces the risk of one program interfering with the smooth running of another program

Physical and Logical Processors

- **Physical processor**
  - Is plugged into a processor socket on the motherboard of the computer
  - Windows Server can support 64 sockets for physical processors
- **Logical processor**
  - A core than can run its own executable threads
  - One physical processor can house several logical processors
- **Virtual processor**
  - A logical processor or one or more of its cores that function for the use of a specific VM
- **With Hyper-V in use**
  - Windows Server supports 320 logical processors

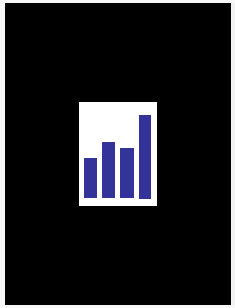
What is Software-defined Storage (SDS) ?

Software intelligence delivering feature-rich cloud scale storage and economics built on industry standard hardware



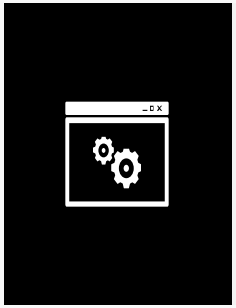
Cloud-inspired infrastructure and design

- Using Industry-standard hardware
- Integrating cloud design points in software
- Driving cloud cost efficiencies



Data explosion

- Device proliferation
- Modern apps
- Unstructured data analytics



Evolving technologies

- Flash is transforming storage
- Network delivering extreme performance
- Maturity in software-based solutions
- Virtual machines and containers

Scale out with simplicity

- Integrated solutions
- Rapid time to solution
- Policy-based management

Network Function Virtualization

- Network functions that are being performed by hardware appliances are increasingly being virtualized as virtual appliances
- Virtual appliances are quickly emerging and creating a new market
- Dynamic and easy to change because they are a pre-built, customized virtual machine

It can be one or more virtual machines packaged, updated, and maintained as a unit

- Can easily be moved or scaled up/down
- Minimizes operational complexity

Microsoft included a standalone gateway as a virtual appliance starting with Windows Server

Using Control Panel and the Devices and Printers Utility

- The Devices and Printers utility is used for the following tasks:
  - Invoke the operating system to use PnP to detect new hardware
  - Install new non-PnP hardware and hardware drivers
  - Troubleshoot problems you might be having with existing hardware
- Device Manager
  - Used to check for a resource conflict and to examine other properties associated with a device
  - Provides a view of all hardware currently installed on your computer

Using Control Panel and the Devices and Printers Utility

- **Driver signing**
  - When a driver is verified, a unique digital signature is incorporated into it
  - When Windows Server determines that a device driver is not signed, it gives you a warning
  - Device drivers that are unsigned cannot be loaded in x64 versions of Windows Server

Using the System File Checker

- Use the System File Checker
  - To scan system files for integrity
- You can run this utility to:
  - Scan all system files to verify integrity
  - Scan and replace files as needed
  - Scan only certain files
- The System File Checker can be manually run from the Command Prompt window or Windows PowerShell window

Using Sigverif to Verify System and Critical Files

- Sigverif verifies system and critical files to determine if they have a signature
  - Only scans files and does not overwrite inappropriate files, enabling you to use the tool while users are logged on
- After the scan is complete, the results are written to a log file, called sigverif.txt
- If the tool finds a file without a signature that you believe needs to be replaced
  - You can replace the file when users are off the system

Configuring the Operating System

- After the operating system has been installed
  - It can be configured to optimize performance and meet very specific requirements
- Using tools included with Windows Server you can configure elements of the OS such as:
  - Performance options
  - Environment variables
  - Startup and recovery options
  - Power options
  - Protocols

Configuring Performance Options (1 of 3)

- **You can configure basic areas of performance including:**
  - **Processor scheduling and Data Execution Prevention**
  - **Virtual memory**
  - **File caching and flushing**
- **Configuring Processor Scheduling and Data Execution Prevention**
  - **Processor scheduling**
    - Allows you to configure how processor resources are allocated to programs
  - **Data Execution Prevention (DEP)**
    - Monitors how programs use memory to ensure they are not causing memory problems

Configuring Performance Options (2 of 3)

- **Configuring virtual memory**
  - **Virtual memory - Disk storage used to expand the capacity of the physical RAM installed in the computer**
  - **Virtual memory works through a technique called paging**
    - Whereby blocks of information, called pages, are moved from RAM into virtual memory on disk
  - **The area of disk that is allocated for this purpose is called the paging file**

Configuring Performance Options (3 of 3)

- **Tips for placement of the paging file:**
  - Server performance is better if the paging file is not placed on the boot partition
  - If there are multiple disks, performance can be improved by placing a paging file on each disk
  - In a mirrored set or volume, place the paging file on the main disk
  - Do not place the paging file on a stripe set, striped volume, stripe set with parity, or RAID-5 volume

Configuring File Caching

- File caching is turned on by default
  - Uses an area of RAM already established for file caching
  - Is controlled by the cache manager in Windows OSs
- Flushing
  - After data is written to disk, the RAM used for that cached data is freed
- When file caching is off
  - Server can seem slower to users
- In most cases, server performance is better and disk operations are safer when file caching and flushing are turned on

Configuring Startup and Recovery

- You can configure the following system startup options:
  - Which operating system to boot by default, if more than one operating system is installed
  - How long to display a list of operating systems from which to boot
  - How long to display a list of recovery options, if the computer needs to go into recovery mode after a system failure
- In the event of a system failure, you can configure these options:
  - Writing information to the system log (hard configured so you cannot change this)
  - Whether to start automatically after a system failure
  - How and where to write debugging information

Configuring Power Options

- The Power Options that you can set are as follows:
  - Select a power plan
  - Choose what the power button does
  - Create a power plan
  - Choose when to turn off the display
- Three power plans are already created: balanced, power saver, and high performance
- Choosing what the power button does give you three options:
  - Shut down
  - Do nothing
  - Hibernate
- The option to create a power plan enables you to customize a power plan

Installing a Protocol

- You might need to add other protocols to customize the server for your network
- Hyper-V Extensible Virtual Switch Protocol
  - Used when the Hyper-V role is installed in Windows Server
  - Enables the use of a software virtual switch between the main operating system and the operating systems on virtual partitions
  - Reduces the overhead in network communications when Hyper-V is installed
- Reliable Multicast Protocol
  - Used for multimedia transmissions
  - Runs on top of IP and simplifies multicast communications
    - Because multicasting can be done even without routers to direct network traffic

Understanding the Windows Server Registry

- **Windows Server Registry**
  - A very complex database containing all information the operating system needs about the entire server
  - The Registry is the coordinating center for a specific server
- **Data contained in the Registry include:**
  - Information about all hardware components
  - Information about Windows Server services that are installed
  - Data about user profiles and Windows Server group policies
  - Data on the last current and last known setup used to boot the computer
  - Configuration information about all software in use
  - Software licensing information
  - Server Manager and Control Panel parameter configurations

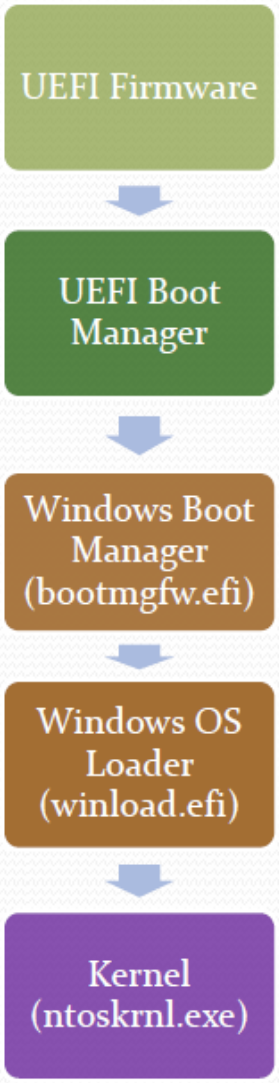
Windows PowerShell

- Windows PowerShell is a command-line interface or shell
- A shell is a customized environment for executing commands and scripts
- Script
  - A file of commands that is run when you run the script
- cmdlets
  - Specialized commands for completing common tasks in PowerShell

Windows PowerShell

- Some of the tasks you can complete using Windows PowerShell include the following:
  - Manage files and folders
  - Manage network tasks
  - Manage fixed and removable storage
  - Configure printing services
  - Manage software applications and updates
  - Manage Remote Desktop Services
  - Manage server services and features
  - Work with the Registry

Typical Boot Flow



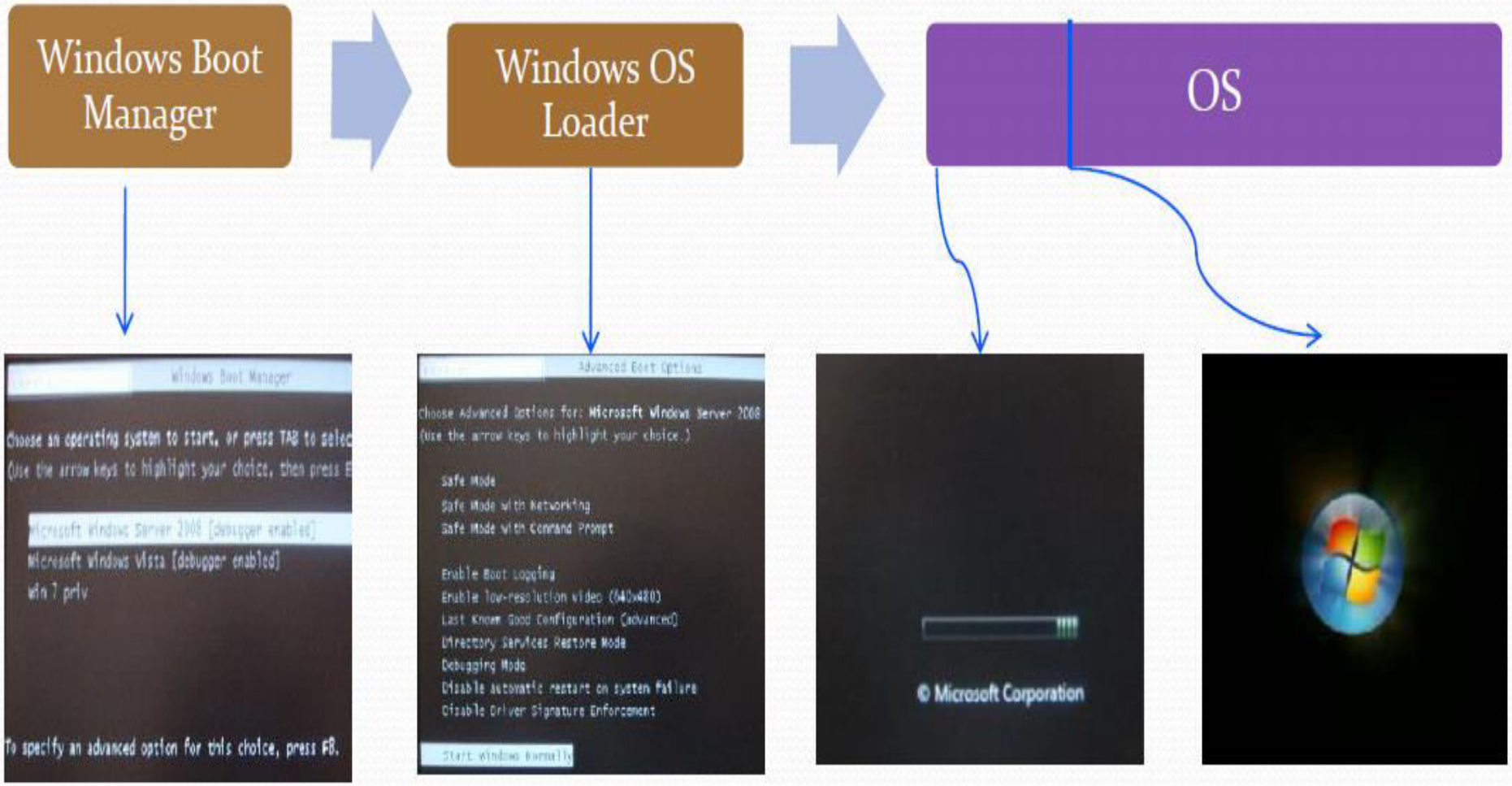
Performs CPU and Chipset initialization, load drivers etc.

Loads UEFI device drivers (based on NVRAM DriverXxx variable), loads boot application

Loads Windows OS loader selected by user

Loads the Windows OS, calls ExitBootServices()

Typical Boot Screens



What Is Firmware - Power on sequence

- Installed with a computer in non-volatile location (PROM\EEPROM)
- Initializes low level hardware
  - Initializes memory controller timings, powers on critical boot devices
- Hands off control to operating system loader
  - Operating system loader uses firmware interfaces to initialize the operating system
- Refer to as pre-boot firmware
  - Examples: BIOS and UEFI (Unified Extensible Firmware Interface)

What Is Firmware - Limited runtime usage

- Firmware may still be involved after operating system starts
  - This is called runtime firmware
  - Operating system normally strives to place runtime firmware into a sandbox for reliability
  - An exception is System Management Mode (SMM) firmware
- Firmware is used in cases where a high-performance driver does not exist
  - Handles some of the specifics of a particular platform running Windows

What Is firmware - Limited runtime usage

- **Advanced Configuration and Power Interface (ACPI) defines an industry standard for runtime firmware**
  - **Primary supported runtime firmware interface for Windows**
  - **Microsoft co-authored industry standard ACPI specification**
  - **Used to identify and configure 'soldered on motherboard' hardware and more**
  - **Asynchronously notifies operating system of changes in hardware (e.g., when a laptop switches from AC to battery power)**
  - **Firmware runs in an OS-provided virtual machine**

EFI Firmware - Motivation and history

- **EFI creation motivated by Itanium bring up**
  - **Desire to avoid BIOS limitations in a brand new high end architecture**
  - **Also designed as a BIOS replacement**
- **Avoids BIOS pitfalls**
  - **Modern design incorporates twenty five years of progress in computer science**
    - Runs in native processor mode
    - Can be programmed in C/C++
    - More accessible than BIOS
  - **Well specified; largely in one self-contained document**
  - **Architecture is modular and extensible**
    - EFI Interfaces are object oriented
    - For example, Block IO Protocol contains a ‘base class’ for reading from any block IO device
  - **Interfaces should be consistent by virtue of EFI conformance test**

Key changes: EFI To UEFI - 64-bit native firmware

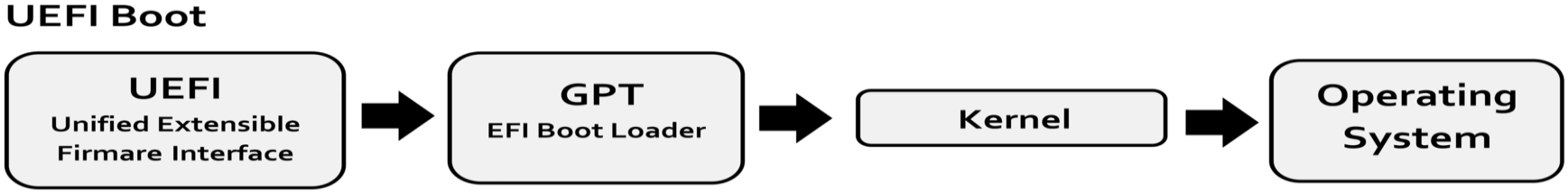
- UEFI nearly identical to EFI 1.10, but there are a few key differences
  - X64 required some changes to EFI specification
- Runtime calls must run in same mode as operating system; for native EFI boot,
  - A 64-bit operating system requires 64-bit UEFI firmware
  - A 32-bit operating system requires 32-bit UEFI firmware
- Architectural changes for BIOS

UEFI Advantages

- Ability to boot a disk containing large partitions (over 2 TB) with a GUID Partition Table (GPT)
- Flexible pre-OS environment, including network capability, GUI, multi language
- 32-bit (for example IA-32, ARM32) or 64-bit (for example x64, AArch64) pre-OS environment
- C language programming
- Modular design
- Backward and forward compatibility

UEFI booting

- UEFI does not rely on boot sectors, defining instead a boot manager as part of the UEFI specification.
- When a computer is powered on, the boot manager checks the boot configuration and based on its settings, then executes the specified OS boot loader or operating system kernel (usually boot loader).
- The boot configuration is defined by variables stored in NVRAM, including variables that indicate the file system paths to OS loaders or OS kernels.
- OS boot loaders can be automatically detected by UEFI, which enables easy booting from removable devices such as USB flash drives.
- This automated detection relies on standardized file paths to the OS boot loader, with the path varying depending on the computer architecture.



UEFI Support

- The Linux kernel has been able to use EFI at boot time since early 2000s
- HP-UX has used (U)EFI as its boot mechanism on IA-64 systems since 2002.
- Apple uses EFI for its line of Intel-based Macs.
- Microsoft introduced UEFI for x64 Windows operating systems.
- Microsoft began requiring UEFI to run Windows with Windows 11.
- The FreeBSD Foundation awarded a grant to a developer seeking to add UEFI support to the FreeBSD kernel and bootloader.

UEFI with virtualization

- HP Integrity Virtual Machines provides UEFI boot on HP Integrity Servers. It also provides a virtualized UEFI environment for the guest UEFI-aware OSes.
- VMware Fusion 3 software for Mac OS X can boot Mac OS X Server virtual machines using UEFI.
- VMware Workstation prior to version 11 unofficially supports UEFI, but is manually enabled by editing the .vmx file.
- The vSphere ESXi 5.0 hypervisor officially support UEFI. Version 6.5 adds support for Secure Boot.

UEFI with virtualization

- VirtualBox has implemented UEFI since 3.1,but limited to Unix/Linux operating systems
- The VMware ESXi version 5 hypervisor, part of VMware vSphere, supports virtualized UEFI as an alternative to the legacy PC BIOS inside a virtual machine.
- The second generation of the Microsoft Hyper-V virtual machine supports virtualized UEFI.
- Google Cloud Platform Shielded VMs support virtualized UEFI to enable Secure Boot.

Pre-boot Configuration - Boot Configuration Data (BCD)

- Windows Vista introduces BCD data store
- Abstracted data store
  - Replacement for boot.ini
  - Replacement for NVRAM settings
- BCD is a container for BCD objects
  - A BCD object represents a pre-boot application
  - One object for Windows boot manager, another for Windows OS loader
  - An application option is represented as an element of a BCD object
- Programmatic access
  - Accessible via utilities and WMI provider
  - Fully documented on MSDN

Windows Boot manager (Bootmgr)

- Loads the Windows boot applications
- OS loader, Resume loader, memory tester
- Display boot menu and handles user to select
- Loads the BCDstore to get a list of boot options
- Locate the OS loader on the device
- Load the appropriate OS loader into memory
- Transfer control to OS loader

Boot Configuration Data (BCD) store

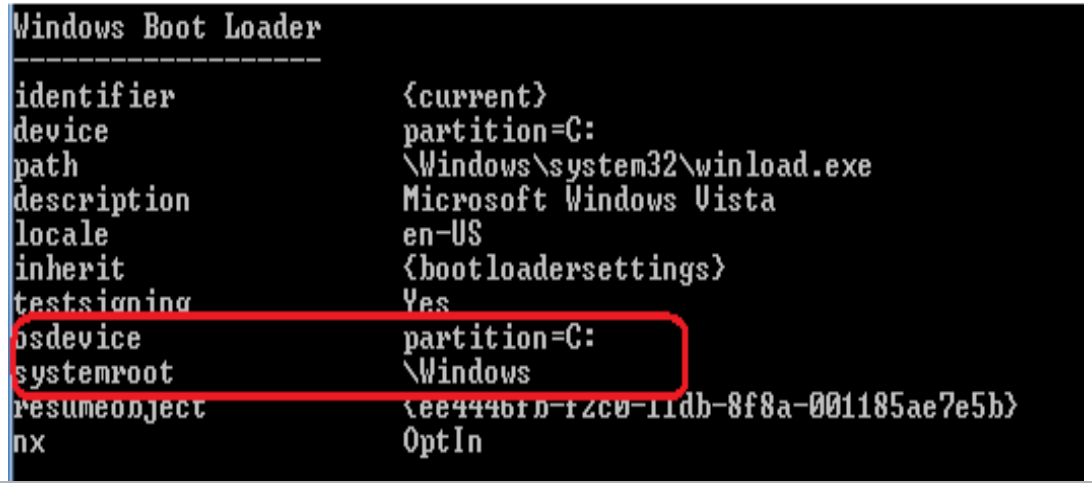
- Stores configuration information required to boot
- Replaces legacy boot.ini (BIOS) and efinvr.exe (on Itanium)
- BCD is a container for BCD objects
- Each boot application is represented by a BCD object
- Object are identified by GUIDs or aliases ({bootmgr}, {default})
- BCD object is a container of BCD elements
- Elements contain configuration setting for a boot application

Windows OS Loader

- Load all files needed by the kernel to initialize
- Setup the execution environment for the kernel
- Terminate boot services
- Transfer control to the kernel

Loading OS binaries

- **What files are loaded?**
- **Kernel + other kernel components required for initialization (ntoskrnl.exe, hal.dll, kdcom, …)**
- **All drivers marked as boot start**
- **The system hive (**A *hive* is a logical group of keys, subkeys, and values in the registry that has a set of supporting files containing backups of its data.)
- **Boot entry provides the path to the OS files**



Booting the System

- One of the most frustrating problems to troubleshoot is when Windows does not boot and you cannot log in to Windows.
- To overcome these problems, you need to understand how the computer boots and be familiar with the tools available during boot up.
- Every time you turn on a computer, it goes through the Power-On Self Test (POST), which initializes hardware and finds an operating system to load.

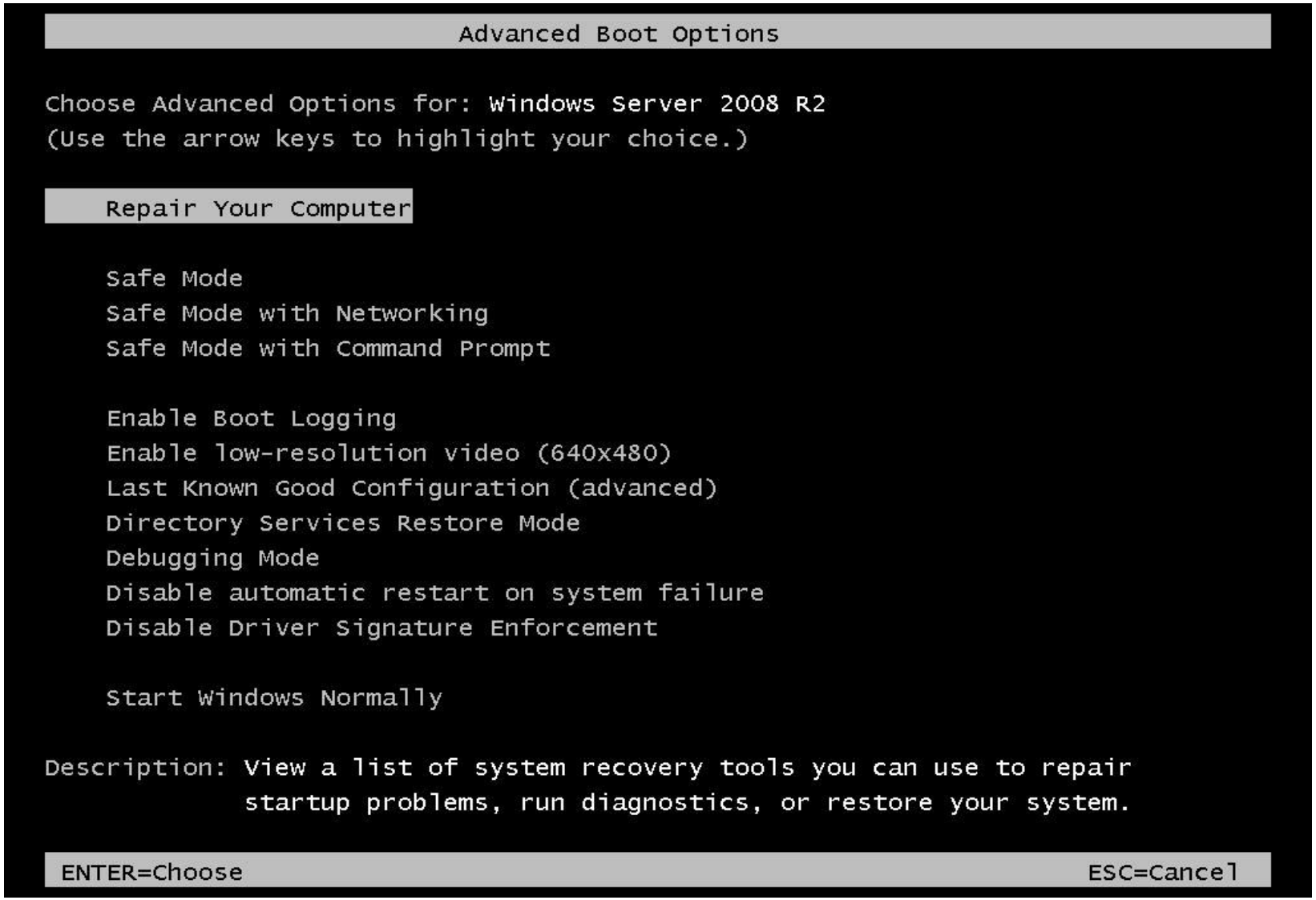
Master Boot Record

- A master boot record (MBR) is the first 512-byte boot sector of a partitioned data storage device such as a hard disk.
  - It is used to hold the disk's primary partition table, contains the code to bootstrap an operating system, which usually passes control to the volume boot record and uniquely identifies the disk media.
- A *volume boot record (VBR)* is a type of boot sector, stored in a disk volume on a hard disk or similar data storage device that contains code for booting an operating system such as NTLDR and BOOTMGR.

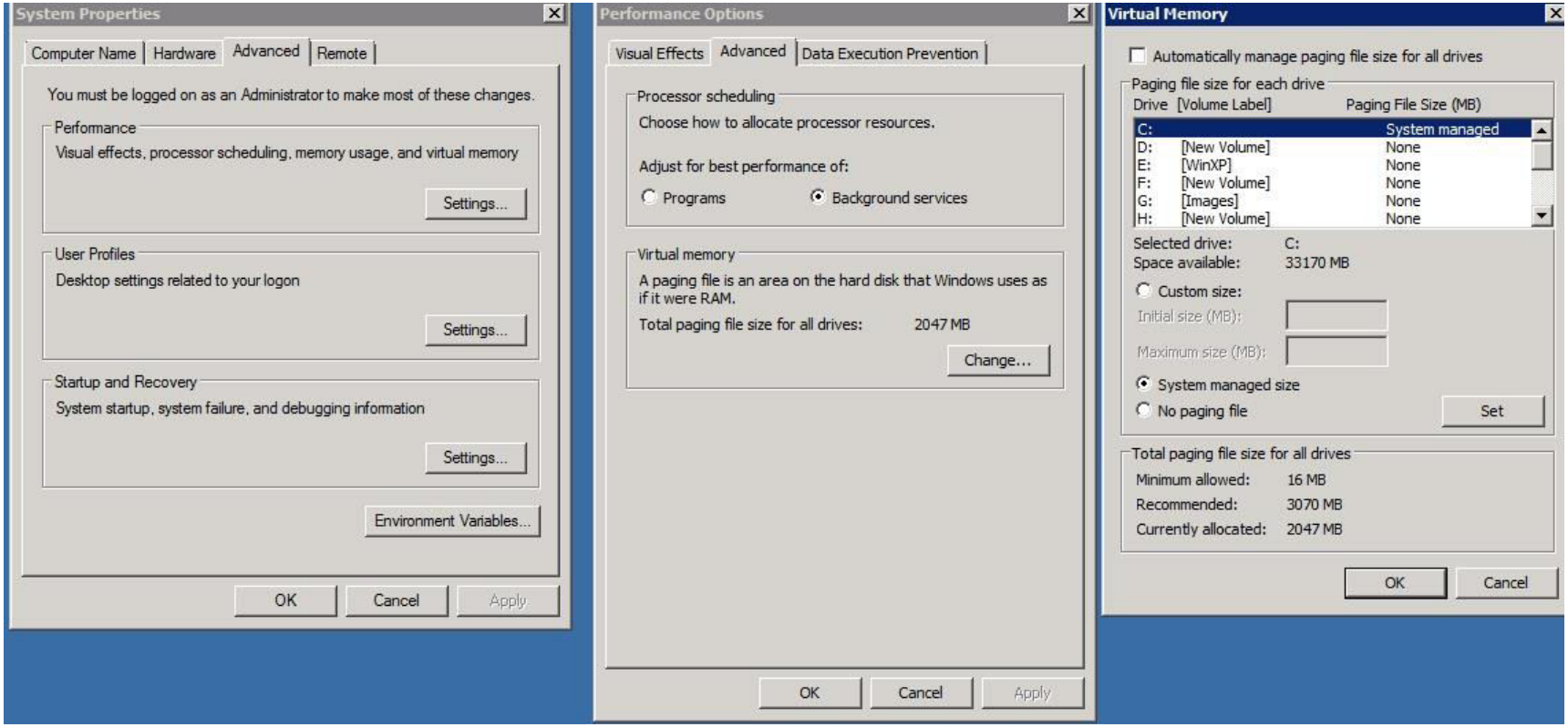
BCDEdit

- *Boot Configuration Data (BCD)* is a firmware-independent database for boot-time configuration data used by Microsoft's Windows Boot Manager found with Windows 7,10 and Windows Server 2016,2019
- To edit the Boot Configuration, you typically use Bcdedit.exe.

Advanced Boot Options



Virtual Memory and Paging File



Understanding the Windows Registry

- Contains information and settings for all the hardware, software, users, and preferences of the Server.
- Whenever a user makes changes to a Control Panel settings, or File Associations, System Policies, or installed software, the changes are reflected and stored in the Registry.

Registry Content

The registry holds critical information about the system, the users of the system, and installed applications:

- Operating System version number, build number, and registered user.
- Information for every properly installed application,
- Information about the computer's processor type and system memory.
- User-specific information (home directory, app. preferences)
- Security information such as user account names.
- Installed services
- Mapping from file names to programs/executables.
- Mapping network addressees to host machine names.

Registry Analysis

- **Registry is central database of Windows systems**
  - **Configuration of system**
  - **Information about user activity**
    - applications installed and opened
    - window positions and sizes
      - to provide user with a better experience
  - **Information is time-stamped**
- **Used to get systems information**
  - **Example: System has no prefetch files**
    - Investigate the corresponding registry key
      - Microsoft knowledge base 307498
      - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
- **Used to establish timelines of activity**

Understanding the Windows Registry

- The registry contains 6 main keys:
- HKEY_CLASSES_ROOT ----
  - Contains information on file types, including which programs are used to open a particular file type.
  - COM server info, file associations, shortcuts
- HKEY_CURRENT_USER ----
  - Contains user-specific settings that are built from information in the HKEY_USERS key during the logon process.
  - Logged in user name, desktop, start menu

Understanding the Windows Registry

- HKEY_LOCAL_MACHINE ----
  - Contains computer specific information including installed hardware and software. This is the one users tend to spend the most time in.
  - Hardware, software, preferences for all users
- HKEY_CURRENT_CONFIG ----
  - Contains information about the computer's hardware configuration
  - Links to part of HKEY_LOCAL_MACHINE for current hardware
- HKEY_DYN_DATA ----
  - Contains real-time performance statistics on the computer's hardware.
  - Links to part of HKEY_LOCAL_MACHINE for PlugAndPlay

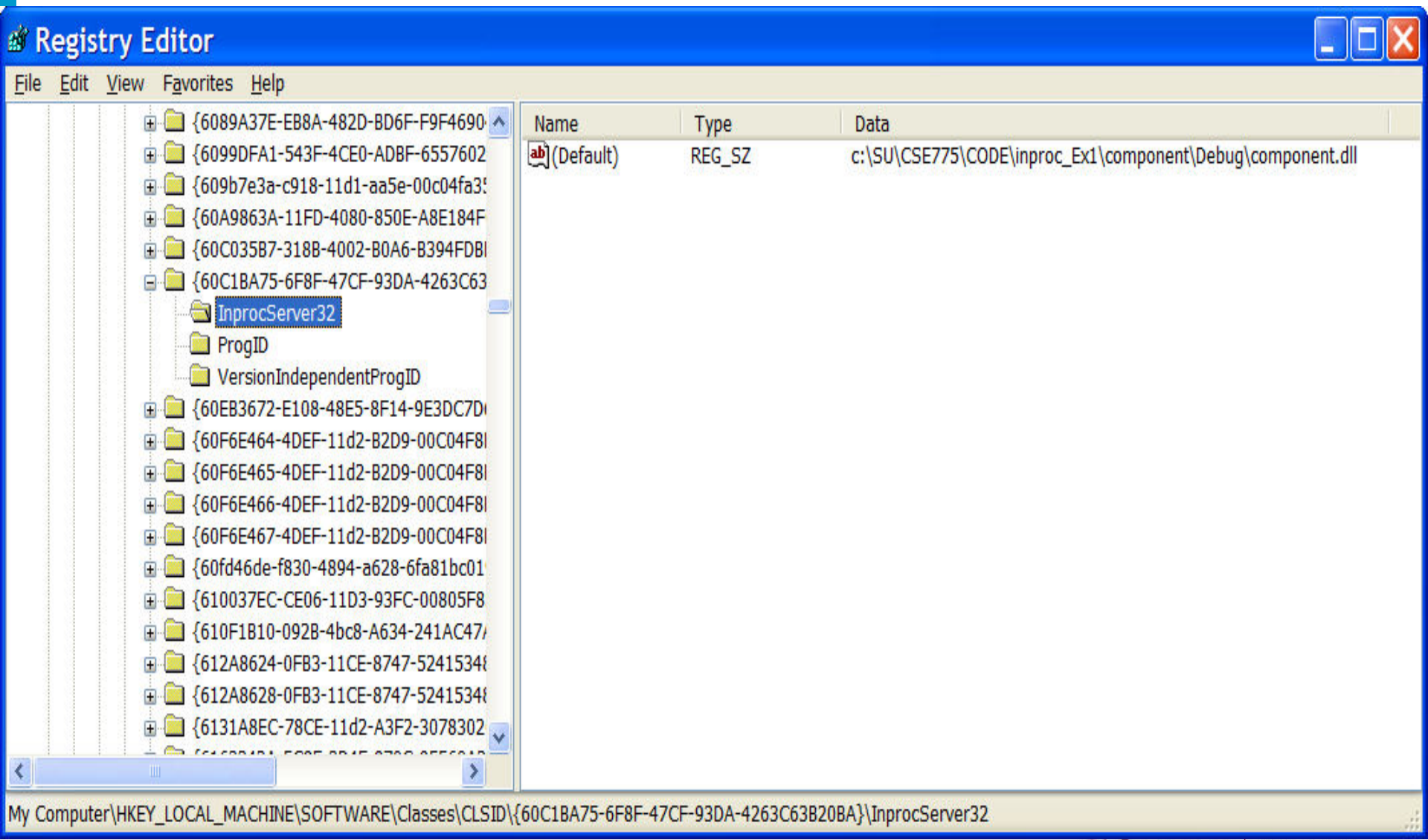
Understanding the Windows Registry

- **HKEY_USERS ----**
  - Contains information (generic and user-specific) about all the users who log on to the computer.
  - The generic settings are available to all users who log on to the computer.
  - The information is made up of default settings for programs, desktop configurations, and so on.
  - This key contains subkeys for each user that logs on to the computer.
  - Individual preferences for each user, represented by Security ID (SID)

Registry Value Types

- REG_BINARY
  - Raw binary data
- REG_DWORD
  - 32 bit integers – often representing boolean
- REG_SZ
  - string
- REG_EXPAND_SZ
  - Expandable string
- REG_MULTI_SZ
  - Container for null separated strings

COM Registry Entry

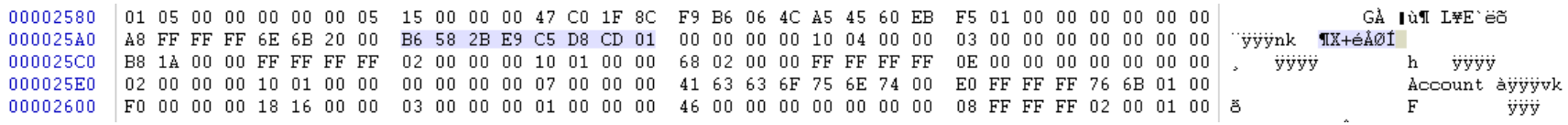


Registry Analysis

- **Contents:**
  - **Basic structure remains fixed**
  - **Location of values changes**
- **Storage location depends on *hive* and system**
  - **Main hives in Windows\system32\config**
  - **Other in system32\config**
  - **User information in NTUSER.dat hive in User Profile**
  - **Parts are volatile:**
    - Populated when need arises
      - HKEY_CURRENT_USER, HKEY
      - HKEY_LOCAL_MACHINE\System
      - HKEY_CLASSES_ROOT

Registry Analysis

- Key Cell Structure
  - 0-3 Size
  - 4-5 Node ID
  - 6-7 Node Type
  - 8-15 LastWrite Time
  - …
- Value Cell Structure
  - 0-3 Size
  - 4-5 Node ID
  - 6-7 Value name length
  - 8-11 Data length
  - 12-15 Offset to data
  - 16-20 Value type



Registry Analysis Tools

- **Life Analysis**
  - **regedit.exe**
    - Native tool (use with caution)
    - Does not give all information (especially not time of last write)
  - **reg.exe**
    - Native command line tool
  - **Autoruns.exe**
    - Russinovich, SysInternals (now MS) investigates registry and other places for programs that run automatically
  - **Scripting tools**
    - E.g.: Using Perl Win32::TieRegistry

Startup Files for Windows

- **Files used during boot process:**
  - **NTDetect.com**
    - responsible for detecting basic hardware that will be required to start the operating system.
- **ntoskrnl.exe (the kernel)**
- **hal.dll (type of hardware abstraction layer)**
- **kdcom.dll (Kernel Debugger HW Extension DLL)**
- **bootvid.dll (for the windows logo and side-scrolling bar)**

File System

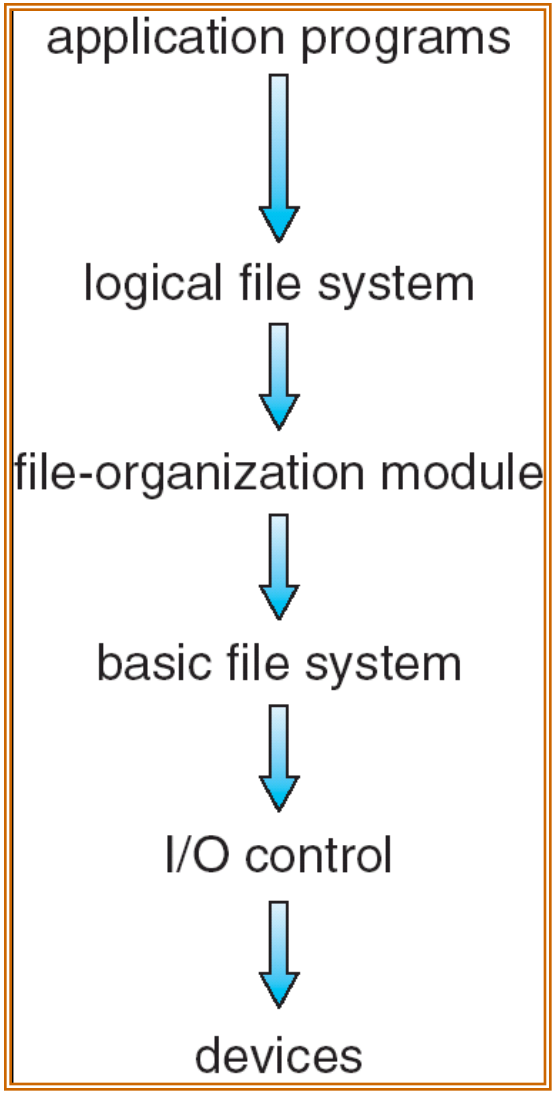
- A file system is a method for storing and organizing computer files and the data they contain to make it easy to find and access them.
- File systems exist on hard drives, pen drives, cd's, dvd's and any other form of data storage medium
- Most data storage devices have array of fixed-size blocks, sometimes called sectors, and file system is in charge of organizing these sectors into files and directories. It is also in charge of indexing the media so it knows where and what each file is

File System

- A file system provides efficient and convenient access to the disk
- The operating system imposes one or more file systems on a disk
- A file system poses two different design problems
  - Defining how the file system should look to the user
    - A file and its attributes
    - The operations allowed on a file
    - The directory structure for organizing files
  - Creating algorithms and data structures to map the logical file system onto the physical secondary-storage devices

Layered File System

- Application programs
- Logical file system
  - Manages the directory structure
  - Maintains the file structure via file control blocks
- File-organization module
  - Maps the logical blocks to the physical blocks
  - Manages the free space/blocks on the disk
- Basic file system
  - Issues generic commands to the appropriate device driver to read and write physical blocks on the disk
- I/O control
  - Consists of device drivers and interrupt handlers



Layered File System (continued)

- **Advantage of a layered structure: Duplication of code is minimized**
  - **I/O control and basic file-system code can be used by multiple file systems**
  - **Each file system can have its own logical file system and file-organization modules**
- **Many kinds of file systems are in use today**
  - **UNIX uses the UNIX file system (UFS)**
  - **Windows NT, 2008,2012 Server, Windows 7,8,10 support**
    - FAT, FAT32, and NTFS
    - CD-ROM, DVD, **ISO/IEC 13346** and **ECMA-167**
  - **Linux supports over 40 different file systems**
    - Main file system is the extended file system (versions ext2 and ext3)

FCB – File Control Block

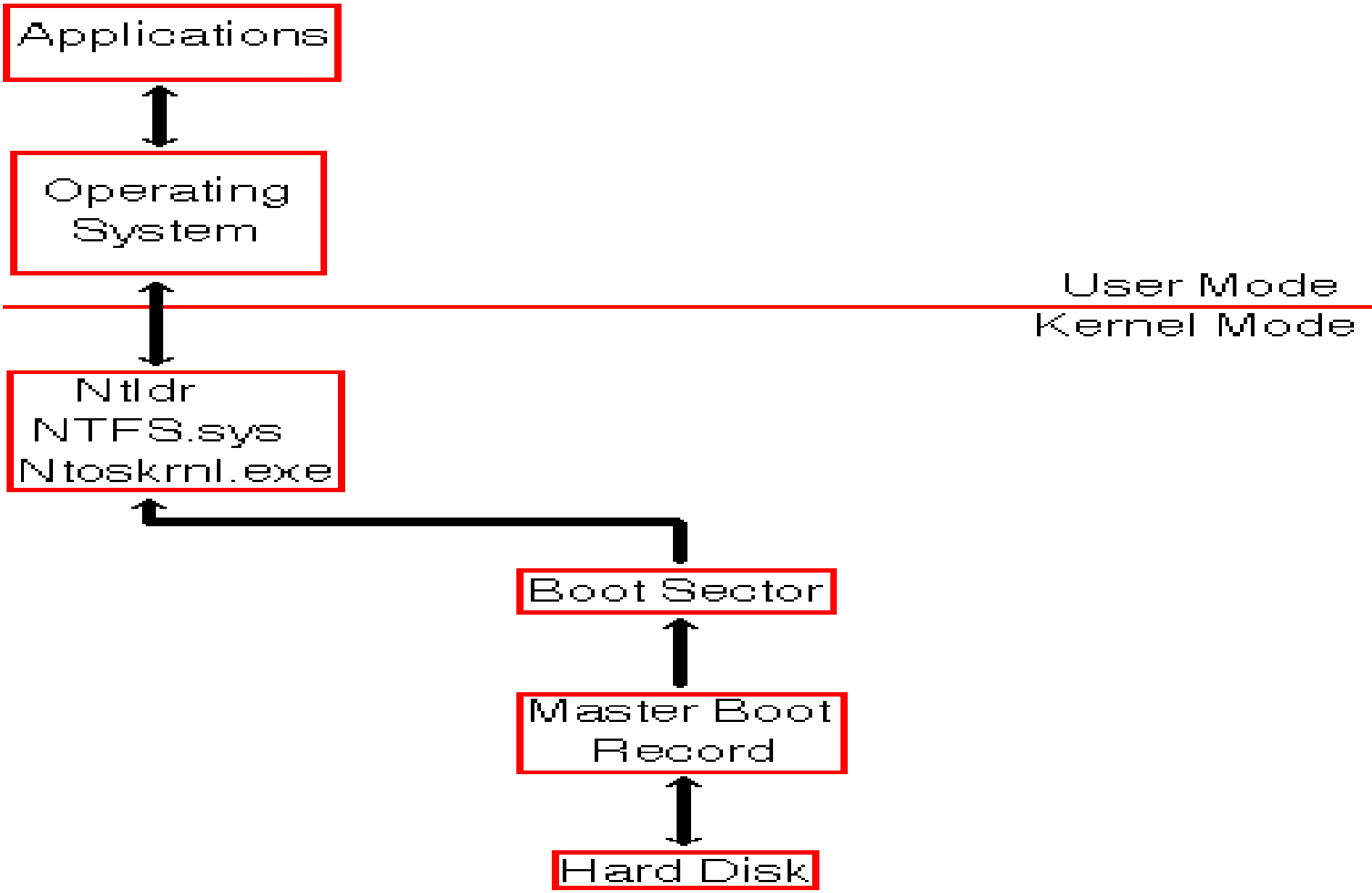
- Contains file attributes + block locations
  - Permissions
  - Dates (create, access, write)
  - Owner, group, ACL (Access Control List)
  - File size
  - Location of file contents
- UNIX File System ➔ I-node
- FAT/FAT32 ➔ part of FAT (File Alloc. Table)
- NTFS ➔ part of MFT (Master File Table)

Boot block

- Dual Boot
  - Multiple OS can be installed in one machine.
  - How system knows what/how to boot?

- Boot Loader
  - Understands different OS and file systems.
  - Reside in a particular location in disk.
  - Read Boot Block to find boot image.

NTFS Architecture



Encrypting File System(EFS)

- Provides security beyond user authentication and access control lists. For example when the attacker has physical access to the computer.
- EFS uses public key cryptography however it is susceptible to brute-force attacks against the user account passwords.

Filename Limitations

Typical Comparison of Legal File Names (Verify Exact Requirements for Your System)

Operating System	Maximum Character Length	Special Characters Disallowed/Discouraged	Case Sensitive	Extension Required
Linux	256	* , ? , $, & , [,] , / , \	Yes	No
Mac OS X	255	: (colon)	Yes	No
Windows 7	255 / 256	Most special characters	No	Yes

File Extensions

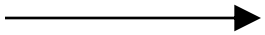
Extensions for a Few File Types	
ASP	Active Server Pages
BAK	Backup File
BAT	Batch File
DLL	Dynamic Link Library
DOC	Document (usually word processing)
CAD	Drawing
EXE	Executable File
JPEG	Graphics File
MP3	Video File
PDF	Portable Document Format
PS	PostScript File
TXT	Text File

File Types – Name, Extension

file type	usual extension	function
executable	exe, com, bin or none	ready-to-run machine-language program
object	obj, o	compiled, machine language, not linked
source code	c, cc, java, pas, asm, a	source code in various languages
batch	bat, sh	commands to the command interpreter
text	txt, doc	textual data, documents
word processor	wp, tex, rtf, doc	various word-processor formats
library	lib, a, so, dll	libraries of routines for programmers
print or view	ps, pdf, jpg	ASCII or binary file in a format for printing or viewing
archive	arc, zip, tar	related files grouped into one file, sometimes compressed, for archiving or storage
multimedia	mpeg, mov, rm, mp3, avi	binary file containing audio or A/V information

MBR

Offset	Purpose
0x00	Bootable flag (0x80)
0x01	Cylinder (10 bits) Head (6 bits) of first sector Sector (8 bits)
0x04	Partition Type
0x05	Cylinder
0x06	Head of last sector
0x07	Sector
0x08	LBA address of first sector
0x0C	Number of sectors



Type	File system
..	…
0x07	NTFS/ex Fat
0x0B	Fat 32
0x83	Linux Ext
0xAF	HFS+
..	…

Network-Based File Systems

- Apple Filing Protocol
- Network File System (NFS)
- Server Message Block (SMB/CIFS/SMB2)
- File Transfer Protocol (FTP)
- Web Distributed Authoring and Versioning (WebDAV)