CMD.exe

Command.com, CMD.exe is the command shell used with Windows XP and newer operating systems.

The executable (CMD.exe) is located in the %systemroot% directory as follows:

- 32-bit shell on 32-bit system, located in %systemroot%\system32
- 32-bit shell on 64-bit system, located in %systemroot%\syswow64
- 64-bit shell on 64-bit system, located in %systemroot%\system32

Windows PowerShell

The Windows PowerShell is a full featured command shell that uses “cmdlets” (built-in commands), built-in programming features, and standard command-line utilities. Developed on the .NET Framework, it allows administrators to manage servers and workstations in the enterprise from the command line.

Cmdlets are instances of .NET Framework classes; they are not stand-alone executables. Cmdlets are named using verb-noun pairs in which the verb identifies the action performed and the noun identifies the resource on which the action is performed. For example, the cmdlet “get-command” is used to get all the cmdlets that are registered in the command shell.

A complete list of cmdlets is available from the Windows PowerShell prompt by typing help *-*. Documentation on a specific cmdlet is available by help followed by the cmdlet name, such as “help get-command”.

Windows Management Instrumentation Command-Line

Windows Management Instrumentation Command-Line, or “WMIC” is a command-line and scripting interface that simplifies the use of Windows Management Instrumentation (WMI) and system management through WMI.

- Enables an administrator to enter commands to the interface without native query language knowledge
- Compatible with existing shells and utility commands
- Supported by Windows XP or Server 2003 and newer systems.

Environmental Variables

Environmental variables are strings that are used by Windows to communicate information about the location of system files, folders, and programs as they pertain to the currently logged on user. Systems can be configured differently, either by default or by individual choice. Environmental variables enable universal programming codes to be compatible to the variety of potential system configurations. This is possible because the values of these variables are not hardcoded to specific locations, but are allowed to be changeable based on the system configuration.

System environmental variables, such as the path to the Windows files, are defined by Windows at installation and they apply to all computer users. Changes to the system environment are written to the registry, usually require a restart to become effective, and can only be modified by an administrator. The percent symbol identifies the variable as an environmental variable.

Environmental variables are contained in HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment. These environmental variables are pre-defined. Here are a few commands:

Command	Description
set	Displays all current environmental variables
setx	Creates or modifies environmental variables in the user or system environment, without requiring programming or scripting
echo %systemroot%	shows where Windows files are located
echo %homepath%	shows the \Documents and Settings\“user profile” or \Users\“user profile” in Windows Vista +

Command and Syntax - Redirects

Redirects are used to direct input and output using Windows commands. Using the “greater than” or “less than” special characters, one can send the output of a command to a file or device, for example, command1 > file/device.

A redirect may often involve receiving input or directing output to or from a given path, for example: command > [path]filename. Note that input is represented by the “greater than” symbol, while output is denoted by the “less than” symbol. Information already in the file is overwritten, and if the file does not exist, it will be created.

Double “greater than” or “less than” characters denote that information should be appended to a file instead of overwritten. For example, command>>[path]filename, Command < [path]filename >> [path]filename.

Command and Syntax - Pipes

At the Windows command line, we use “pipes” to send the output of the first command as the input for the second command. Piping allows for multiple redirects in which a number of commands are strung together.

Example, command1 | command2 | command3 denotes that the output of command 1 should be the input for command 2 and the output for command 2 should be the input for command 3.

Command and Syntax – Chaining and Grouping

The ampersand (&) separates multiple commands on one command line. Cmd.exe runs the first command, and then the second command. This is called chaining and looks like this: (command1 & command2).

A double ampersand (&&) runs the command following the symbol only if the command preceding the symbol is successful. Cmd.exe runs the first command, and then runs the second command only if the first command completed successfully: (command1 && command2)

Conversely, a double pipe symbol (||) runs the command following the symbol only if the command preceding the symbol fails. Cmd.exe runs the first command, and then runs the second command only if the first command did not complete successfully (receives an error code greater than zero).

Parentheses () group a set of commands for conditional execution based on success such as ((command1 & command2) && (command3)) or based on failure ((command1 & command2) || (command3)).

Command and Syntax – Escape Characters

The escape character can be used for a few reasons.

- It can be added before a command symbol to allow the command symbol to be treated as ordinary text
- It can be used to make long commands more readable by splitting them into multiple lines and escaping the Carriage Return + Line Feed (CR/LF) at the end of the line.

For example, the command ‘echo <escape>’ will result in an error whereas the command ‘echo **^**<escape**^**>’ will print <escape> to the screen

One thing to note: a stray space at the end of the line (after the escape character) will break the command, which is hard to detect unless you have a text editor that displays spaces and tab characters.

Command and Syntax – Wildcard Characters

A wildcard is a symbol used to replace or represent one or more characters. Wildcards or wild characters are either an asterisk (*), which represents zero or more characters or question mark (?), which represents a single character.

New Technology File System (NTFS)

Components	Description
Sector	Sectors are hardware-addressable blocks on a storage medium. It is typically 512 bytes and is defined in the Partition Boot Sector.
Clusters	Clusters are the addressable blocks that many file system formats use. They are always a multiple of the sector size, typically 4096 bytes, (or 8 sectors), in Windows and are defined in the Partition Boot Sector.
Logical Cluster Number (LCN)	The Logical Cluster Number is the cluster address relative to the storage media.
Virtual Cluster Number (VCN)	The Virtual Cluster Number is the cluster address relative to the start of the file.
File System Format	The file system format defines the way that file data is stored on storage media.
Metadata	Metadata is data stored on a volume in support of file system format management. This includes the data that defines the placement of files and directories on a volume.

NTFS Advanced Features

Components	Description
Multiple Data Streams	With multiple data streams, each unit of information associated with a file is implemented as a file attribute. Each attribute consists of a single stream. This implementation makes it easy to add more attributes.

Unicode-Based Names	Unicode-based names is a 16-bit character coding scheme that allows each character in each of the world languages to be uniquely represented. This makes it easy to move data from one country to another. Each complete filename path can be up to 255 characters in length.
Dynamic Bad-Cluster Remapping	This feature is enabled when a bad cluster is identified and the data is remapped to a new cluster. The process is as follows: the NTFS sends a warning that the cluster is bad, and then a good copy of the sector's data is retrieved. A new cluster is allocated, and the data is copied to the new cluster. The bad cluster is flagged and no longer used.
Per User Volume Quotas	This feature allows for per-user quote specification of quota enforcement, which is useful for usage tracking and tracking when a user reaches warning and threshold limits.
Encryption	This process is transparent to the user and is performed using the Encrypting File System (EFS). Encryption is accomplished using private/public key pairs.
Defragmentation	This feature is enabled when files occupy non-contiguous space on the hard disk. The NTFS has tools to make the files contiguous.
Read-Only Support	This feature was introduced with Windows XP and allows mounted volumes to be read-only.

Commands

For a list of Command Shell commands, please visit the Windows Command-Line Reference Internet site listed below.

Recommended Internet Sites

- Windows Command-Line Reference https://web.archive.org/web/20160719112909/https://technet.microsoft.com/en-us/library/cc754340.aspx
- Windows CMD Shell Command Line Syntax https://web.archive.org/web/20160719112946/http://ss64.com/nt/syntax.html
- NTFS Master File Table https://web.archive.org/web/20160719113043/http://ntfs.com/ntfs-mft.htm
- Master File Table https://web.archive.org/web/20160719113140/https://msdn.microsoft.com/en-us/library/windows/desktop/aa365230%28v=vs.85%29.aspx
- Graphical Identification and Authentication (GINA) https://web.archive.org/web/20160719113218/https://en.wikipedia.org/wiki/Graphical_identification_and_authentication
- Interaction Between Winlogon and GINA https://web.archive.org/web/20160719113259/https://msdn.microsoft.com/en-us/library/windows/desktop/aa376105%28v=vs.85%29.aspx
- Reg import https://web.archive.org/web/20160722132553/https://technet.microsoft.com/en-us/library/cc742021.aspx
- Path https://web.archive.org/web/20160719113521/https://technet.microsoft.com/en-us/library/bb490963.aspx
- Windows Command Line https://web.archive.org/web/20160719113956/http://www.windows-commandline.com/set-path-command-line
- Date Forgery Analysis and Timestamp Resolution https://web.archive.org/save/_embed/http://www.meridiandiscovery.com/articles/date-forgery-analysis-timestamp-resolution/
- Windows Timestamp Tampering https://web.archive.org/web/20160719114109/http://blog.opensecurityresearch.com/2012/01/windows-timestamp-tampering.html
- Windows Management Instrumentation (Retrieved January 11, 2016) https://web.archive.org/web/20160719114138/https://en.wikipedia.org/wiki/Windows_Management_Instrumentation
- What is Windows Management Instrumentation (WMI)? (Retrieved January 11, 2016) https://web.archive.org/web/20160719114209/http://searchwindowsserver.techtarget.com/definition/Windows-Management-Instrumentation
- Wmic (n.d.) https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/wmic

- WMIC Command Cheat Sheet: https://web.archive.org/web/20160719114335/https://projectzme.wordpress.com/2013/03/14/windows-tip-wmic-command-cheat-sheet/
- Windows Command Line Cheat Sheet: https://web.archive.org/web/20160719114406/https://www.sans.org/security-resources/sec560/windows_command_line_sheet_v1.pdf
- WIMIC Snippets: https://web.archive.org/web/20160719114406/https://www.sans.org/security-resources/sec560/windows_command_line_sheet_v1.pdf

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.