Contents

[Introduction 2](#_Toc158276714)

[Theory 2](#_Toc158276715)

[Kommandotolken 2](#_Toc158276716)

[Grundläggande systemdata 3](#_Toc158276717)

[Prestanda och resursnyttjande 3](#_Toc158276718)

[Systemstatus och aktivitetshanteraren 4](#_Toc158276719)

[Network 4](#_Toc158276720)

[Detailed Process View Analysis 4](#_Toc158276721)

[Basprioritet 4](#_Toc158276722)

[Results 6](#_Toc158276723)

[Kommandtolken 6](#_Toc158276724)

[Grundläggande systemdata 8](#_Toc158276725)

[Prestanda och resursnyttjande 9](#_Toc158276726)

[Systemstatus och aktivitetshanteraren 12](#_Toc158276727)

[Performance Tab observation 12](#_Toc158276728)

[Network 13](#_Toc158276729)

[Prioritet 14](#_Toc158276730)

[References 19](#_Toc158276731)

# Introduction

In this assignment, we're going to dive into the world of Windows beyond the usual click-and-drag of the mouse, exploring the command line interface with cmd.exe at the heart of our journey. This lab will guide us through the myriad of commands and options available, including how to use the performance monitor (perfmon.exe) to understand better how Windows manages tasks and memory. Designed with Windows 10 users in mind, this exercise is perfect for both university lab computers and personal devices, offering a hands-on approach to demystify the sometimes-intimidating command prompt. By engaging with this practical exploration, we aim to make the complex workings of Windows more approachable and understandable, equipping you with valuable skills and insights into the operating system's deeper functionalities.

# Theory

## Kommandotolken

1. The `cd` command, standing for "change directory," is an essential tool in the Windows command prompt environment, designed to switch the current working directory. When executed without parameters, it reveals the path of the current directory, whereas specifying a directory path as an argument shifts the working directory to the indicated location. Its primary function is to facilitate the navigation between different folders within the operating system's file system, making it easier to manage files and directories directly from the command line. **[1]**[[1]](#endnote-2) Among its options, `cd ..` is used to ascend one level up in the directory tree, effectively moving to the parent directory. The command `cd \` (or `cd /` on UNIX/Linux systems, but we're focusing on Windows) directs the user to the root directory, simplifying the process of reaching the file system's top level. While options like `cd ~` and `cd -` offer shortcuts to the home directory and toggling between directories in UNIX/Linux, they are not applicable in the Windows context. In summary, the `cd` command is a cornerstone of command line navigation in Windows, offering straightforward pathways to the parent or root directories and thereby streamlining the process of moving around within the file system. [[2]](#endnote-3) **[2]**
2. The `find` command in Windows serves as a powerful utility for searching specific text strings within files, offering a way to pinpoint and display lines where these strings appear. Designed for tasks like text analysis and log file examination, it enhances user efficiency in sifting through content. Among its notable options, `/v` inversely filters search results to exclude the specified string, `/c` tallies the occurrences without listing them, `/n` adds line numbers for precise location identification, and `/i` facilitates case-insensitive searches, broadening the search scope**.[3][[3]](#endnote-4)** These options collectively make `find` an essential tool in the Windows command line arsenal for detailed and flexible text searching, providing users with diverse methods to manage and analyze file content effectively.[[4]](#endnote-5) **[4]**
3. The command "dir" is used in a command-line interface to list the contents of a directory. When executed, it displays a list of files and directories contained within the current directory. Additionally, it shows various details such as file size, creation date, and last modified date. Common options that can be used with the "dir" command include "/w" to display the output in a wide format, "/p" to display one screen at a time, "/s" to include all subdirectories, and "/a" to show all files, including hidden ones. For example, running "dir /s" will display the contents of the current directory as well as all subdirectories recursively.[[5]](#endnote-6) [[6]](#endnote-7) **[5] [6]**

The "where" command is utilized in command-line interfaces to locate the path of executable files matching a specific name pattern. When executed, it returns the paths of all matching executable files found within the system's PATH environment variable. This command is particularly useful for finding the locations of executable files, which can be helpful when multiple versions of a program exist on a system or when troubleshooting issues related to program execution. Common options that can be used with the "where" command include "/R" to search recursively in specified directories, "/T" to set the timeout for the command, and "/Q" to suppress output. For instance, running "where /R C:\Program Files myfile.exe" will search for "myfile.exe" recursively in the "C:\Program Files" directory and its subdirectories.[[7]](#endnote-8) **[7]**

## Grundläggande systemdata

Accessing System Information (msinfo32.exe) allows you to retrieve crucial details about your system, such as the operating system and its version, the amount of physical and virtual memory available, the capacity of secondary memory (storage drives) and the filesystem being utilized, as well as the assigned drive letters for each device. Furthermore, it provides insights into environment variables like PATH, which is a list of directories where executable files reside, aiding in executing programs from any directory without specifying the full path. These pieces of information are indispensable for troubleshooting, system optimization, and ensuring software compatibility, enabling users to understand their system configuration comprehensively and efficiently manage their computing environment.

## Prestanda och resursnyttjande

The Performance Monitor provides insight into CPU activity through various time counters. "% Processor Time" measures the percentage of time the CPU is executing non-idle threads, offering an overview of overall CPU utilization during the sample interval. "% User Time" represents the percentage of CPU time spent executing user-mode processes, encompassing applications like word processors and games. In contrast, "% Privileged Time" signifies the percentage of CPU time spent executing in kernel mode, reserved for critical operating system functions. Finally, "% Idle Time" indicates the percentage of time the CPU remains idle, reflecting periods when no tasks are actively being processed. These counters collectively offer a comprehensive understanding of CPU utilization and workload distribution, aiding in system performance analysis and optimization.[[8]](#endnote-9) **[8]**

## Systemstatus och aktivitetshanteraren

Expected Outcome: Running this command is likely to cause a noticeable increase in both CPU and disk usage. This is because the "tree" command systematically lists out all folders and files within the C: drive, requiring a lot of computing power.

Network  
8.8. 8.8 is the primary DNS server for Google DNS. Google DNS is a public DNS service that is provided by Google with the aim to make the Internet and the DNS system faster, safer, secure, and more reliable for all Internet users. [9][[9]](#endnote-10)

Traceroute tool (IP tracer) allows to detect the route of the IP packets to the given host. Both IPv4 and IPv6 are supported. Traceroute tool displays IP addresses, domains and countries of intermediate hops.

### Detailed Process View Analysis

In our examination of system performance, we first look for the process that's using the most CPU power at the moment. This helps us identify which application is putting the most strain on the processor. Next, we check for the process that's causing the most page faults, which happen when an application tries to access memory that isn't currently available. This could mean the application is using a lot of memory or that there isn't enough physical memory available. Lastly, we search for any processes running in a 32-bit environment. These processes are limited to using a maximum of 4GB of memory, even on a 64-bit system. These investigations give us valuable insights into how our system resources are being used and help us make improvements to optimize performance.

## Basprioritet

The expected outcome involves the idle process, commonly referred to as the "System Idle Process" **[13]** in Task Manager, which typically maintains an exceptionally low priority class. This designation is intentional, ensuring that the System Idle Process utilizes CPU resources only when no other user-initiated or system processes require CPU utilization. By prioritizing other tasks over the idle process, system performance can be optimized, allocating resources efficiently based on immediate demands.[[10]](#endnote-11)

Each priority class in the Windows scheduler determines CPU allocation for processes. Realtime prioritizes immediate CPU needs but is rarely used due to its potential to monopolize resources. High-priority processes rank above normal but below realtime. Above Normal processes have higher priority than normal ones but need fewer resources than high-priority ones. Normal is the default for most processes, Below Normal is less important and gets CPU time less often, and Low-class processes run only when the system is idle, using minimal resources.[[11]](#endnote-12)

The main role of the idle process is simply to hold a spot. Unlike active processes that perform tasks, the System Idle Process represents the portion of the CPU that isn't currently in use. It's like a counter that shows how much of the CPU's capacity is available. So, even though it might show a high CPU usage percentage, it doesn't mean it's using up your CPU's resources. Instead, it just shows that your CPU is ready and waiting to tackle any tasks that come its way.[[12]](#endnote-13)

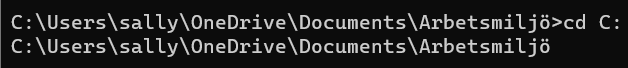
## 

## Results

## Kommandtolken

1. cd is the command used to control directories’ names and current drive.

It can be used in two ways:

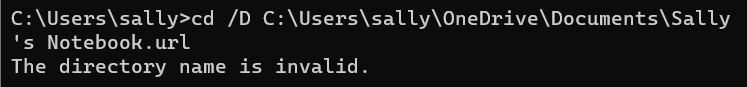
* “CD [Drive]”: displays the current directory according to Drive given.
  + Example
  + 
* “CD” shows the ongoing drive and directory
  + Returns the parent directory
  + Text

    Description automatically generated
  + Navigates to the specified folder
  + Text

    Description automatically generated
* “CD /D [Drive]” switches the current drive and directory
  + Text

    Description automatically generated with medium confidence

Cd extensions are case-insensitive and don’t accept spaces



Graphical user interface, text

Description automatically generated with medium confidence

1. Find is used to search for a text string in files

The command is used with the following parameters:

* /V displays every line except the lines that contain the specified string
  + Example
  + Text

    Description automatically generated
* /C is used to count the number of lines that contain a specific string
  + Example
  + Text

    Description automatically generated
* /N shows the line number next to the displayed lines
* /I searches with case insensitive characters
  + Text

    Description automatically generated
* /OFF[LINE] is to not ignore the files with offline state
* “string” searches the string specified

1. Dir shows the files and subdirectories included in a directory

Dir can be used with parameters such as:

* /B displays files with the minimum format as shown in the following example
  + Example
  + Text

    Description automatically generated with medium confidence
* /O lists files sorted in a specific order
  + N by name
  + A picture containing table

    Description automatically generated
  + D by date (old first)
  + A picture containing text

    Description automatically generated

The previous parameters are not the only parameters that can be used with Dir, it was just an example to show how Dir displays files

1. Where: is the command used to display files’ location matching the search pattern.

Parameter:

* /R recursively displays the files matching the specified pattern.
  + A picture containing text

    Description automatically generated
* /T shows the files size, last modified date and time for all matched files
  + Text

    Description automatically generated

## Grundläggande systemdata

1. The operating system used is “Microsoft Windows 11 Home” and the version is “10.0.22621 Build 22621”

|  |  |
| --- | --- |
| Total Physical Memory | 15,8 GB |
| Available Physical Memory | 4,54 GB |
| Total Virtual Memory | 39,8 GB |
| Available Virtual Memory | 13,9 GB |

1. Storage drives file system is “NTFS” and the capacity/size is “475,64 GB 510 719 422 464 bytes”
2. The unit found is C:

Graphical user interface, text, application

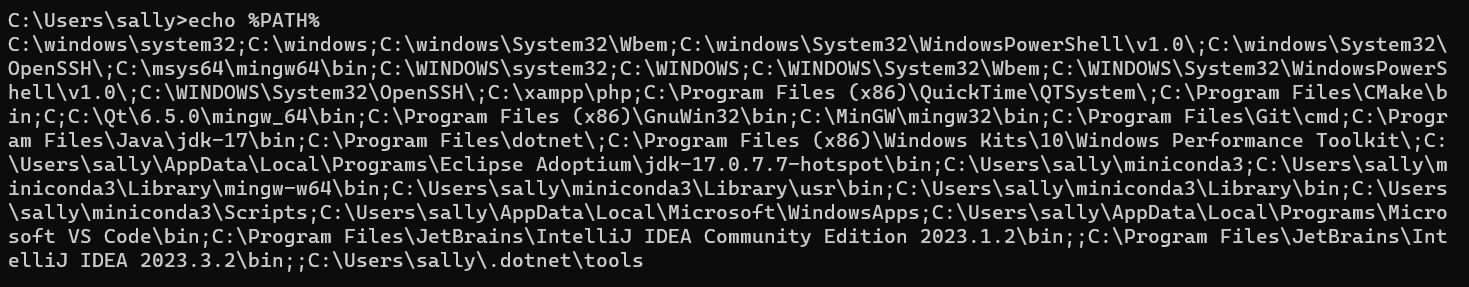
Description automatically generated

1. Vad finns i miljövariabeln PATH? Vad är syftet med PATH?

The PATH environment variable is an essential part of operating systems, especially Unix, Linux, and Windows. It contains a list of directories that the shell searches through to find executable programs when a command is entered by the user. **[14]** Each directory in the PATH variable is separated by a colon (:) in Unix/Linux or a semicolon (;) in Windows.[[13]](#footnote-2)

The primary purpose of the PATH variable is to allow users to run executables or scripts from the command line or terminal without needing to specify the full path to the executable. This convenience speeds up command line navigation and execution, enhancing productivity and easing system administration tasks.

Graphical user interface, text, application

Description automatically generated  


## Prestanda och resursnyttjande

|  |  |
| --- | --- |
| *Time type* | *Average time* |
| *Processor* | *3.840* |
| *Idle* | *87.508* |
| *Privilege* | *2.11* |
| *User* | *1.729* |

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, application

Description automatically generated

A screenshot of a computer

Description automatically generated

Graphical user interface

Description automatically generated  
  
When analyzing data, understanding the different types of time measurements is crucial for evaluating processor performance. "% Processor Time" signifies the total duration the processor spends **actively executing threads**, providing insight into overall processor workload. "% User Time" reflects the portion of processor time dedicated to executing code in **user mode**, with elevated values suggesting a high volume of user applications. Conversely, "% Privileged Time" denotes the duration spent executing in **kernel mode**, indicative of system-level tasks such as memory management. "% Idle Time" represents periods when the processor **remains inactive**, with a high percentage suggesting ample spare capacity. Additionally, certain mathematical relationships between these metrics offer further insights. The sum of '% User Time', '% Privileged Time', and '% Idle Time' should approximate 100%, encompassing all processor time. '% Processor Time' is closely related to '% Idle Time', with the former approaching 100% minus the latter. Moreover, the balance between '% User Time' and '% Privileged Time' elucidates the nature of processor activities, distinguishing between user-level applications and system tasks based on their respective time allocations. These relationships contribute to a comprehensive understanding of processor utilization and workload distribution, facilitating effective performance analysis and optimization strategies.

Processor = priviliged+ user

## Systemstatus och aktivitetshanteraren

### Performance Tab observation

After trying the command, it indeed caused a noticeable increase in both CPU and disk usage. The "tree" command systematically listed out all folders and files within the C: drive, as expected, demanding significant computing power. As it dug through each directory and listed its contents, I observed the CPU working harder, resulting in higher CPU usage. Additionally, the disk showed increased activity, accessing the file system structure extensively to fetch the necessary information. These results align with the expected outcome, highlighting the resource-intensive nature of the "tree" command.

Before

A graph on a white background

Description automatically generated  
  
After:

A screenshot of a computer

Description automatically generated

Before:  
A screenshot of a graph

Description automatically generated

After:

A screenshot of a computer

Description automatically generated

Network  
After running the command "ping 8.8.8.8 /n 10 /l 4096" and observing the load, I noticed a slight increase in CPU and network usage. However, the overall impact on system performance seemed minimal, even though my network bandwidth is limited. This is because the ping command, which sends ICMP echo requests to test host reachability, was used with a buffer size of 4096 bytes, larger than the default. When some packets timed out, suggesting they were too large for the network to handle in one piece, I **reduced the packet size**. Eventually, successful pings confirmed that the issue was indeed due to packet size limitations. Similarly, upon executing the "tracert 8.8.8.8" command and observing the route, I observed a list of hops (intermediate routers) through which packets traveled to reach the destination. The number of hops varied widely, reflecting the diverse network configuration and the specific path to the destination. The packet to 8.8.8.8, which is dns.google, required **30 hops** to reach its destination. The route was determined by examining ICMP times. Overridden messages were returned by intermediate routers, while an echo response message was returned by the destination.

8.8. 8.8 is the primary DNS server for Google DNS. Google DNS is a public DNS service that is provided by Google with the aim to make the Internet and the DNS system faster, safer, secure, and more reliable for all Internet users.

To gather the information available between the source and destination, a traceroute lowers the packet's TTL (time to live) to a minimum (1). When a router receives the information, it decrements the **TTL value to 0,** indicating it should send information **back to the source**. The source gathers the intermediate router information, resets the TTL value to 1, and increments it. Until the final **package reaches the destination IP**.

Task Manager's Detailed Process View Analysis

The process exerting the most strain is Chrome, accounting for 14% of CPU utilization. Utilizing the Resource Monitor, we can identify which applications are **generating** the highest number of **page faults**. In this instance, Chrome is the primary culprit, generating 1 page fault at each interval. Furthermore, Discord operates as a **32-bit platform**, meaning it has a RAM usage limit, specifically **4 GB with Large Address Aware** (LAA) and 2 GB without LAA on an x86 system. However, transitioning to a 64-bit system offers significantly expanded memory capabilities, enabling users to store up to 17 billion GB of RAM. The difference between 32 and 64 is the number of calculations per second they can perform, which affects the speed at which they can complete tasks. 64 can perform multitask.   
  
Appendix has more images for network performance.

## Prioritet

a) Idle has Noll priority or zero priority

(b) Priority levels in the system range from normal to higher and lower than normal, as well as low and high. Many processes can have their priorities adjusted, with most on this computer appearing to be set to normal. A common practice is to assign low priority to background processes and high priority to interactive ones.

Priority classes are:

- low: Graphical user interface, application

Description automatically generated

Below Normal:

Table

Description automatically generated

Normal:

Table

Description automatically generated with medium confidence

Above Normal

Graphical user interface, table

Description automatically generated

High:

Graphical user interface, application, table

Description automatically generated

C) The observed priorities for the Idle process (base priority of 0) and Task Manager (base priority of 8) align with Microsoft's guidelines. The Idle process's [] priority ensures it only uses CPU cycles when no other process does, without interrupting active processes. Task Manager's priority is set to maintain its responsiveness as a user-level application. These settings conform to Microsoft's standards for system performance and stability, highlighting the role of process priorities in efficient system management.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

D) The System Idle Process’ sole purpose is at Halt instruction —literally anything—while it waits for the next computation or process fed into it. The reason this all works is that the idle threads use a zero priority, which is lower than ordinary threads have, allowing for them to be pushed out of the queue when the OS has legitimate processes to be run. Then, once the CPU finishes with that job, it’s ready to handle the System Idle Process all over again. Having idle threads always in a Ready state—if they’re not already running—keeps the CPU running and waiting for anything the OS throws at it.

# References

**[1]** Microsoft, n.d. cd. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/cd> [17/03/2024].

**[2]**GeeksforGeeks, n.d. CD CMD Command. Available at: <https://www.geeksforgeeks.org/cd-cmd-command/> [17/03/2024].

**[3]**How-To Geek, n.d. How to Use Find from the Windows Command Prompt. Available at: <https://www.howtogeek.com/206097/how-to-use-find-from-the-windows-command-prompt/> [17/03/2024].

**[5]**SS64, n.d. FIND. Available at: <https://ss64.com/nt/find.html> [17/03/2024].

**[6]**Microsoft, n.d. you. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/dir> [17/03/2024].

**[7]**Lifewire, n.d. DIR Command. Available at: <https://www.lifewire.com/dir-command-4050018> [17/03/2024].

**[8]**Microsoft, n.d. where. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/where> [17/03/2024].

**[9]**MSSQLTips, n.d. Perfmon Counters for CPU Usage, Memory, Disk, and Network Performance. Available at: <https://www.mssqltips.com/sqlservertutorial/9183/perfmon-counters-for-cpu-usage-memory-disk-and-network-performance/> [17/03/2024].

**[10]**WhatsMyDNS, n.d. What is 8.8.8.8? Available at: <https://www.whatsmydns.net/articles/8-8-8-8.html> [17/03/2024].

**[11]**Wikipedia, n.d. System Idle Process. Available at: <https://en.wikipedia.org/wiki/System_Idle_Process> [17/03/2024].

**[12]**Microsoft, n.d. Scheduling Priorities. Available at: <https://learn.microsoft.com/en-us/windows/win32/procthread/scheduling-priorities> [17/03/2024].

**[13]**Wikipedia, n.d. System Idle Process. Available at: <https://en.wikipedia.org/wiki/System_Idle_Process#:~:text=The%20primary%20purpose%20of%20the,terms%20of%20Windows%20scheduling%20states> [17/03/2024].

**[14]**Baeldung, n.d. An Introduction to the PATH Variable in Linux. Available at: <https://www.baeldung.com/linux/path-variable> [17/03/2024].

1. [↑](#endnote-ref-2)
2. [↑](#endnote-ref-3)
3. [↑](#endnote-ref-4)
4. [↑](#endnote-ref-5)
5. [↑](#endnote-ref-6)
6. [↑](#endnote-ref-7)
7. [↑](#endnote-ref-8)
8. [↑](#endnote-ref-9)
9. Appendix  
   A screenshot of a computer

   Description automatically generated A screenshot of a computer

   Description automatically generated

   A screenshot of a computer

   Description automatically generated

   Text

   Description automatically generated

   A screenshot of a computer

   Description automatically generated A screenshot of a computer screen

   Description automatically generated A screenshot of a computer

   Description automatically generated

   A screenshot of a computer

   Description automatically generated

   1. Graphical user interface, application

      Description automatically generated
   2. Graphical user interface, application

      Description automatically generated
   3. Graphical user interface, table

      Description automatically generated with medium confidence

   [↑](#endnote-ref-10)
10. [↑](#endnote-ref-11)
11. [↑](#endnote-ref-12)
12. [↑](#endnote-ref-13)
13. [↑](#footnote-ref-2)