

MOHAMMED Fahad (sio1)

**Objectif:**

## **SOMMAIRE**

## PARTIE 1 : Étude approfondie des 20 commandes

- 1) Pour chaque commande étudiée, la démarche suivante a été appliquée :
  - **Récupération de l'aide** : commande `/?`
  - **Analyse du fonctionnement** : Compréhension de l'utilité et des options
  - **Exemple pratique** : Application concrète sur le disque D:\
  - **Capture d'écran** : Documentation du résultat obtenu

```
D:\>comp /?
Compare le contenu de deux fichiers ou ensembles de fichiers.

COMP [data1] [data2] [/D] [/A] [/L] [/N=chiffre] [/C] [/OFF[LINE]] [/M]

data1      Spécifie l'emplacement et le(s) nom(s) du (des) premier(s) fichier(s) à comparer.
data2      Spécifie l'emplacement et le(s) nom(s) des deuxièmes fichiers à comparer.
/D         Affiche les différences au format décimal.
/A         Affiche les différences en caractères ASCII.
/L         Affiche les numéros de ligne pour les différences.
/N=chiffre Compare uniquement le premier nombre de lignes spécifié dans chaque fichier.
/C         Ignore le cas des lettres ASCII lors de la comparaison de fichiers.
/OFF[LINE] N'ignorez pas les fichiers avec un ensemble d'attributs hors connexion.
/M         Ne pas demander de comparer d'autres fichiers.

Pour comparer des ensembles de fichiers, utilisez des caractères génériques dans les paramètres data1 et data2.
```

COMP (Compare) est un utilitaire de comparaison binaire qui analyse deux fichiers ou ensembles de fichiers par octet. Cette commande est particulièrement utile pour :

- Vérifier l'intégrité de copies de fichiers
- Détecter des modifications non autorisées
- Comparer des versions de fichiers

```
D:\>comp test.txt test2.txt
Comparaison de test.txt et test2.txt...
Comparaison des fichiers OK

Comparer d'autres fichiers (O/N) ? |
```

Les fichiers présentent une différence, permettant d'identifier précisément où les deux fichiers divergent.

```
D:\>fc test.txt test2.txt
Comparaison des fichiers test.txt et TEST2.TXT
***** test.txt
test 1
***** TEST2.TXT
test2
*****
```

- 2) **FC (File Compare)** est un outil de comparaison plus avancé que COMP. Il compare deux fichiers et affiche les différences de manière détaillée, ligne par ligne.

```
D:\>fc /?
Compare deux fichiers ou ensembles de fichiers et affiche les différences
entre eux.

FC [/A] [/C] [/L] [/LBn] [/N][OFF[LINE]][/T] [/U] [/W] [/nnnn]
[lect1:][chemin1]fichier1 [lect2:][chemin2]fichier2
FC /B [lect1:][chemin1]fichier1 [lect2:][chemin2]fichier2

/A      Affiche la 1ère et dernière ligne de chaque ensemble de
différences.
/B      Effectue une comparaison binaire.
/C      Ignore la casse.
/L      Compare les fichiers en tant que texte ASCII.
/LBn    Définit le nombre maximal de différences consécutives comme égal
au nombre de lignes spécifié.
/N      Affiche les numéros de ligne pour une comparaison ASCII.
/OFF[LINE] Ne pas ignorer les fichiers dont l'attribut hors connexion a été
réglé.
/T      Ne convertit pas les tabulations en espaces.
/U      Compare les fichiers en tant que fichiers texte UNICODE.
/W      Comprime les blancs (tabulations et espaces) pour la comparaison.
/nnnn   Spécifie le nombre de lignes consécutives qui doivent
correspondre après une différence.
[lect1:][chemin1]fichier1
        Spécifie le premier fichier ou ensemble de fichiers à comparer.
[lect2:][chemin2]fichier2
        Spécifie le second fichier ou ensemble de fichiers à comparer.
```

**Résultat obtenu,**

FC affiche clairement le contenu différent entre les deux fichiers, facilitant l'identification des modifications.

```
D:\>fc test.txt test2.txt
Comparaison des fichiers test.txt et TEST2.TXT
***** test.txt
test 1
***** TEST2.TXT
test2
```

- 3) **REPLACE** remplace automatiquement des fichiers dans un répertoire cible par des fichiers du même nom provenant d'un répertoire source.

```
D:\>replace /?
Remplace des fichiers.

REPLACE [lect1:][chemin1]fichier [lect2:][chemin2] [/A] [/P] [/R] [/W]
REPLACE [lect1:][chemin1]fichier [lect2:][chemin2] [/P] [/R] [/S] [/W] [/U]

[lect1:][chemin1]fichier Spécifie le ou les fichiers source.
[lect2:][chemin2]       Spécifie le répertoire dont les fichiers
                        sont à remplacer.
/A                       Ajoute nouveaux fichiers au répertoire destination.
                        Inutilisable avec les commutateurs /S ou /U.
/P                       Demande confirmation avant de remplacer un fichier
                        ou d'ajouter un fichier source.
/R                       Remplace les fichiers en lecture seule ainsi que
                        les fichiers non protégés.
/S                       Remplace les fichiers dans tous les sous-répertoires
                        du répertoire destination. Ne peut pas être utilisé
                        avec le commutateur /A.
/W                       Attend insertion d'une disquette avant de commencer.
/U                       Remplace (met à jour) les fichiers plus anciens
                        que les fichiers source. Inutilisable avec /A.
```

### Résultat obtenu

L'option **/A** a permis d'ajouter le fichier nouveau.txt dans le répertoire de destination sans remplacer les fichiers existants.

```
D:\>replace D:\Source\*.txt D:\Destination /A
Ajout de D:\Destination\test.txt

D:\>|
```

- 4) **ROBOCOPY** (Robust File Copy) est l'outil de copie le plus puissant de Windows.

```
D:\>robocopy /?

-----
ROBOCOPY    ::    Copie de fichiers robuste pour Windows
-----

Démarrage : mardi 7 octobre 2025 20:52:24
          Syntaxe :: ROBOCOPY source destination [fichier
                    [fichier]...] [options]

                    source :: répertoire source (lecteur:\chemin ou
                    \\serveur\partage\chemin).
                    destination :: rép. de destination (lecteur:\chemin ou
                    \\serveur\partage\chemin).
                    fichier :: fichier(s) à copier (noms/caractères
                    génériques : valeur par défaut "*..*").
```

## Résultat obtenu

**ROBOCOPY** a copié l'intégralité de la structure source vers la destination, incluant tous les sous-répertoires et leurs attributs.

```
D:\>robocopy Source Destination /E

-----
ROBOCOPY    ::    Copie de fichiers robuste pour Windows
-----

Démarrage : mardi 7 octobre 2025 20:51:54
Source : D:\Source\
Dest : D:\Destination\

Fichiers : *.*

Options : *.* /S /E /DCOPY:DA /COPY:DAT /R:1000000 /W:30

-----
*Fichier SUPPL.      1      D:\Source\          7      test2.txt
-----

Total      Copié      IgnoréDiscordance      ÉCHEC      Extras
Rép :      1          0          1          0          0
Fichiers :  1          0          1          0          1
Octets :    8          0          8          0          7
Heures:  0:00:00  0:00:00          0:00:00  0:00:00
Fin : mardi 7 octobre 2025 20:51:54
```

- 5) **XCOPY** est un outil de copie avancé qui offre plus d'options que la commande COPY de base. Bien que ROBOCOPY soit plus moderne,

```
D:\>xcopy /?
Copie les fichiers et les arborescences de répertoires.

Source XCOPY [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]
[/C] [/I] [/-I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T]
[/U] [/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z] [/B] [/J]
[/EXCLUDE:fichier1[+fichier2][+fichier3]...] [/COMPRESS]
[/[-]ÉPARGNE] [/NOCLONE]

source      Spécifie le(s) fichier(s) à copier.
destination Spécifie l'emplacement et/ou le nom des nouveaux fichiers.
/A          Copie uniquement les fichiers avec l'attribut d'archive défini,
            ne change pas l'attribut.
/M          Copie uniquement les fichiers avec l'attribut d'archive défini,
            désactive l'attribut d'archive.
/D:j-m-a    Copie les fichiers modifiés à compter de la date spécifiée.
            Si aucune date n'est indiquée, copie uniquement les fichiers dont
            l'heure source est plus récente que l'heure de destination.
/EXCLUDE:file1[+file2][+file3]...
            Spécifie une liste de fichiers contenant des chaînes. Chaque chaîne
            devrait être sur une ligne distincte dans les fichiers. Quand l'un des
            les chaînes correspondent à n'importe quelle partie du chemin absolu du fichier à
            copié, ce fichier sera exclu de la copie. Par
            exemple, spécifier une chaîne comme \obj\ ou .obj exclura
            tous les fichiers sous le répertoire obj ou tous les fichiers avec le
            Extension .obj respectivement.
/P          Vous invite avant de créer chaque fichier de destination.
/S          Copie les répertoires et sous-répertoires sauf ceux vides.
/E          Copie les répertoires et sous-répertoires, y compris les vides.
            Identique à /S /E. Peut être utilisé pour modifier /T.
/V          Vérifie la taille de chaque nouveau fichier.
/W          Vous invite à appuyer sur une touche avant de copier.
/C          Continue la copie même si des erreurs se produisent.
/I          Si la destination n'existe pas et que vous copiez plusieurs fichiers,
            suppose que la destination doit être un répertoire.
/-I         Si la destination n'existe pas et copier un seul fichier spécifié,
            suppose que la destination doit être un fichier.
/Q          N'affiche pas les noms de fichiers lors de la copie.
/F          Affiche les noms complets des fichiers source et de destination lors de la copie.
/L          Affiche les fichiers qui seraient copiés.
/G          Permet la copie de fichiers cryptés vers une destination qui ne le fait pas
            ne prend pas en charge le cryptage.
```

## Résultat obtenu

**XCOPY** a copié l'intégralité de la structure du répertoire source, incluant les sous-répertoires.

```
D:\>echo Copie test > D:\SourceXCOPY\fichier2.txt

D:\>xcopy D:\SourceXCOPY D:\DestXCOPY /E /I /Y
D:\SourceXCOPY\fichier1.txt
D:\SourceXCOPY\fichier2.txt
2 fichier(s) copié(s)

D:\>|
```

## Commandes de gestion du temps et d'affichage

- 1) **TIMEOUT** met en pause l'exécution d'un script batch pendant une durée déterminée. Cette commande est essentielle pour : Créer des délais dans les scripts, Permettre à l'utilisateur de lire des messages,

```
D:\>timeout /?

TIMEOUT [/T] délai_d'attente [/NOBREAK]

Description :
Cet utilitaire accepte un paramètre de délai d'attente qui définit la
période de temps d'attente (en secondes) ou jusqu'à ce qu'une frappe de
touche se produise. Il accepte également un paramètre pour ignorer
l'utilisation d'une touche.

Liste de paramètres :
/T          délai_maximal Spécifie le nombre de secondes d'attente.
                        La plage valide est comprise entre
                        -1 et 99999 secondes.

/NOBREAK    Ignorer l'utilisation des touches et attendre le
            temps indiqué.

/?          Affiche ce message d'aide.

Remarque : une valeur de délai d'attente égale à -1 signifie qu'une
            frappe de touche est attendue.

Exemples :
TIMEOUT /?
TIMEOUT /T 10
TIMEOUT /T 300 /NOBREAK
TIMEOUT /T -1
```

### Résultat obtenu

Les deux variantes de TIMEOUT fonctionnent correctement, avec ou sans possibilité d'interruption par l'utilisateur.

```
D:\>timeout /T 5

Attendre 4 secondes, appuyez sur une touche pour continuer...

D:\>|
```

```
D:\>timeout /T 3 /NOBREAK

Attendre 1| secondes, appuyez sur CTRL+C pour quitter ...
```

- 2) **COLOR** permet de personnaliser l'apparence de la fenêtre CMD en modifiant les couleurs du texte et de l'arrière-plan

```
D:\>color B  
D:\>|
```

La couleur du texte a changé en cyan clair, améliorant la visibilité du terminal.

- 3) **DATE** permet d'afficher ou de modifier la date système. Cette commande est utilisée pour : Vérifier la date actuelle, Modifier la date système , Récupérer la date dans des scripts.

```
D:\>date /t  
07/10/2025
```

```
D:\>date  
La date du jour est : 07/10/2025  
Entrez la nouvelle date : (jj-mm-aa) *|
```

### Résultat obtenu

L'option **/t** affiche proprement la date sans demander de modification, pratique pour les scripts.

- 3) **TIME** affiche ou modifie l'heure système. Similaire à DATE, cette commande permet : Vérifier l'heure actuelle.



```
D:\>time /?
Affiche ou modifie l'heure système.

TIME [/T | heure]

TIME sans paramètres affiche l'heure en cours et demande une nouvelle heure.
Appuyez sur ENTRÉE pour conserver la même heure.

Si les extensions de commandes sont activées, la commande TIME prend en charge
le commutateur /T qui fait que la commande n'indique que l'heure, sans
demander d'en entrer une nouvelle.

D:\>|
```

```
D:\>time
L'heure actuelle est : 21:05:27,68
Entrez la nouvelle heure :
21:05|
```

L'option /T affiche l'heure au format court sans demander de modification.

```
D:\>time /T
21:05

D:\>|
```

## Informations système et Configurations

- 1) **DRIVERQUERY** liste tous les pilotes de périphériques installés sur le système.

```
D:\>driverquery /?

DRIVERQUERY [/S système [/U nom_utilisateur [/P [mot_passe]]]]
                [/FO format] [/NH] [/SI] [/V]

Description :
    Permet à un administrateur d'afficher la liste des pilotes
    de périphériques installés.

Liste de paramètres :
    /S      système          Spécifie le système distant auquel se connecter.

    /U      [domaine\]utili. Spécifie le contexte utilisateur dans
                        lequel la commande doit être
                        exécutée.

    /P      [mot_passe]      Spécifie le mot de passe pour
                        le contexte utilisateur donné.

    /FO      format          Spécifie le type de sortie à afficher.
                        Les valeurs autorisées avec le
                        commutateur sont "TABLE", "LIST" et "CSV".

    /NH                        Spécifie que l'"en-tête de colonne"
                        ne doit pas être affichée. Valide pour
                        les formats "TABLE" et "CSV" uniquement.

    /SI                        Affiche des informations sur les pilotes signés.

    /V                        Affiche les sorties détaillées. Non valide
                        sur les pilotes signés.

    /?                        Affiche ce message d'aide.

Exemples :
    DRIVERQUERY
    DRIVERQUERY /FO CSV /SI
    DRIVERQUERY /NH
    DRIVERQUERY /S adresse_IP /U utilisateur /V
    DRIVERQUERY /S système /U domaine\utilisateur /P mot_passe /FO LIST
```

### Résultat obtenu

La commande affiche une liste complète des pilotes installés avec leurs caractéristiques principales.

```
D:\>driverquery

Nom du module Nom complet Type de pilote Link Date
=====
1394ohci Contrôleur d'hôte comp Kernel
3ware 3ware Kernel 19/05/2015 00:28:03
ACPI Pilote ACPI Microsoft Kernel
AcpiAudioComp Pilote du compositeur Kernel
AcpiDev Pilote d'appareils ACP Kernel
acpiex Microsoft ACPIEx Drive Kernel
acpipagr Pilote d'agrégation de Kernel
AcpiPmi Jauge d'alimentation A Kernel
acpitime Pilote d'alarme de sor Kernel
Acx01000 Acx01000 Kernel
AcxHdAudio ACX HD Audio Driver Kernel
ADP80XX ADP80XX Kernel 09/04/2015 22:49:48
AFD Pilote de fonction con Kernel
afunix afunix Kernel
ahcache Application Compatibil Kernel
amdgpio2 Pilote du service Clie Kernel
amdi2c Service de contrôleur Kernel 07/02/2019 10:32:20
AmdK8 Pilote de processeur A Kernel 20/03/2019 05:57:33
AmdPPM Pilote de processeur A Kernel
amdsata amsdata Kernel 14/05/2015 14:14:52
amdsbs amsbs Kernel 11/12/2012 22:21:44
amdwps Pilote de planificatio Kernel
amdxtata amdxata Kernel 01/05/2015 02:55:35
AppID Pilote AppID Kernel
AppleLowerFil Apple Lower Filter Dri Kernel 15/06/2023 04:16:03
AppleSSD Apple Solid State Driv Kernel 11/11/2019 22:24:17
```

2) **SYSTEMINFO** est l'une des commandes les plus complètes pour obtenir des informations système.

```
D:\>systeminfo /?

SYSTEMINFO [/S système [/U utilisateur [/P mot_de_passe]]] [/FO format] [/NH]

Description :
    Cet outil affiche les informations de configuration du système
    d'exploitation
    pour un ordinateur local ou distant, y compris les niveaux de Service Pack.

Liste de paramètres :

/S      système           Spécifie le système distant auquel se connecter.

/U      [domaine\]utili.  Spécifie le contexte utilisateur sous lequel
                          la commande doit s'exécuter.

/P      [mot_de_passe]   Spécifie le mot de passe pour
                          le contexte utilisateur donné. Est demandé s'il
                          est omis.

/FO     format           Spécifie le format dans lequel la sortie doit être
                          affichée.
                          Valeurs autorisées : "TABLE", "LIST", "CSV".

/NH                                           Spécifie que les en-têtes de colonnes ne
                          doivent pas apparaître dans la sortie.
                          Valide uniquement pour les formats TABLE et CSV.

/?                                           Affiche ce message d'aide.

Exemples :
SYSTEMINFO
SYSTEMINFO /?
SYSTEMINFO /S système
SYSTEMINFO /S système /U utilisateur
SYSTEMINFO /S système /U domaine\utilisateur /P mot_de_passe /FO TABLE
SYSTEMINFO /S système /FO LIST
SYSTEMINFO /S système /FO CSV /NH
```

### Résultat obtenu

**SYSTEMINFO** fournit un rapport exhaustif de plus de 50 lignes d'informations système.

```
D:\>systeminfo

Nom d'hôte: DESKTOP-SDDGPCG
Nom du système d'exploitation: Microsoft Windows 11 Famille
Version du système d'exploitation: 10.0.26100 N/A build 26100
Fabricant du système d'exploitation: Microsoft Corporation
Configuration du système d'exploitation: Station de travail autonome
Type de build du système d'exploitation: Multiprocessor Free
Propriétaire enregistré: F A H A D
Organisation enregistrée: N/A
ID du produit: 00325-80000-00000-AAOEM
Date d'installation originale: 30/11/2024, 13:10:46
Heure de démarrage du système: 06/10/2025, 14:37:04
Fabricant du système: Micro-Star International Co., Ltd.
Modèle du système: Thin GF63 12VE
Type du système: x64-based PC
Processeur(s): 1 processeur(s) installé(s).
[01] : Intel64 Family 6 Model 154 Stepping 3 GenuineIntel ~2000 MHz
American Megatrends International, LLC. E16R8IMS.10D, 27/06/2023
C:\WINDOWS
Répertoire système: C:\WINDOWS\system32
Périphérique de démarrage: \Device\HarddiskVolume1
Paramètres régionaux système: fr;Français (France)
Paramètres régionaux d'entrée: fr;Français (France)
Fuseau horaire: (UTC+01:00) Bruxelles, Copenhague, Madrid, Paris
Mémoire physique totale: 32 469 Mo
Mémoire physique disponible: 19 532 Mo
Mémoire virtuelle : taille maximale: 34 517 Mo
Mémoire virtuelle : disponible: 21 400 Mo
Mémoire virtuelle : en cours d'utilisation: 13 117 Mo
Emplacement(s) de fichier d'échange: C:\pagefile.sys
Domaine: WORKGROUP
Serveur d'ouverture de session: \\DESKTOP-SDDGPCG
Correctif(s) logiciel(s): 4 Corrections installées.
[01]: KB5064401
[02]: KB5048779
[03]: KB5065789
[04]: KB5067437

Carte(s) réseau: 3 carte(s) réseau installée(s).
[01]: Realtek PCIe GbE Family Controller
Nom de la connexion : Ethernet
État : Média déconnecté
[02]: Intel(R) Wi-Fi 6 AX201 160MHz
Nom de la connexion : Wi-Fi
```

- 3) **VER** est une commande simple qui affiche la version du système d'exploitation Windows.

```
D:\>ver /?
Affiche la version de Windows.

VER
```

### Résultat obtenu

La commande affiche la version complète de Windows avec le numéro de build.

```
D:\>ver

Microsoft Windows [version 10.0.26100.6725]
```

- 4) **SHUTDOWN** permet de contrôler l'arrêt, le redémarrage ou la mise en veille du système de manière programmée.

```
D:\>shutdown /?
Syntaxe : shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o] [/hybrid] [/soft] [/fw] [/f]
          [/m \ordinateur] [/t xxx] [/d [p|u:]xx:yy [/c "commentaire"]]

Sans argument    Afficher l'aide. Cela revient à entrer /?.
/?              Afficher l'aide. Cela revient à n'entrer aucune option.
/i              Afficher l'interface utilisateur graphique (GUI).
                Ce doit être la première option.
/l              Fermer la session. Ne peut pas être utilisé avec l'option /m
                ou /d.
/s              Arrêter l'ordinateur.
/sg             Arrêtez l'ordinateur. Au démarrage suivant, si l'authentification de redémarrage automatique
                est activée, se connecter automatiquement et verrouiller le dernier utilisateur interactif.
                Une fois connecté, redémarrez les applications inscrites.
/r              Arrêtez complètement l'ordinateur et redémarrez-le.
/g             Arrêtez complètement et redémarrer l'ordinateur. Une fois le système redémarré,
                si l'authentification de redémarrage automatique est activée, se
                automatiquement et verrouiller le dernier utilisateur interactif.
                Une fois connecté, redémarrez les applications inscrites.
/a             Annuler un arrêt du système.
                Utilisable uniquement pendant le délai imparti.
```

```
D:\>shutdown /S /T 300 /C "Arrêt programmé dans 5 minutes"
```

```
D:\>|
```

```
D:\>shutdown /a
```

```
D:\>|
```

```
/a
```



Fermeture de session annulée  
L'arrêt planifié a été annulé.

### Résultat obtenu

Une notification Windows apparaît indiquant l'arrêt programmé. La commande **/A** permet d'annuler l'opération.

5) **TASKLIST** affiche la liste de tous les processus en cours d'exécution sur le système.

```
D:\>tasklist /?

TASKLIST [/S système [/U utilisateur [/P [mot_de_passe]]]]
          [/M [module] | /SVC | /V] [/FI filtre] [/FO format] [/NH]

Description :
  Cet outil affiche une liste des processus actuellement en cours sur
  un ordinateur local ou un ordinateur distant.
```

## Résultat obtenu

TASKLIST affiche tous les processus actifs avec leur PID, session et utilisation mémoire.

```
D:\>tasklist

Nom de l'image                PID Nom de la sessio Numéro de s Utilisation
=====
System Idle Process           0 Services                0          8 Ko
System                        4 Services                0        6 880 Ko
Secure System                 188 Services              0       110 224 Ko
Registry                      232 Services              0        43 736 Ko
smss.exe                      836 Services              0         1 740 Ko
csrss.exe                     1040 Services             0         7 092 Ko
wininit.exe                   1148 Services             0         9 508 Ko
services.exe                  1224 Services             0        12 388 Ko
lsass.exe                     1244 Services             0         4 576 Ko
svchost.exe                    1252 Services             0        34 440 Ko
svchost.exe                    1468 Services             0        42 980 Ko
fontdrvhost.exe               1500 Services             0         5 196 Ko
WUDFHost.exe                  1608 Services             0        16 068 Ko
svchost.exe                    1632 Services             0        19 368 Ko
svchost.exe                    1692 Services             0        13 800 Ko
WUDFHost.exe                  1860 Services             0        21 760 Ko
svchost.exe                    1952 Services             0         8 156 Ko
svchost.exe                    1972 Services             0        10 576 Ko
svchost.exe                    2024 Services             0         6 968 Ko
```

- 6) **HOSTNAME** est une commande simple qui affiche le nom NetBIOS de l'ordinateur.

```
D:\>hostname /?

Affiche le nom de l'hôte actuel.

hostname
```

#### Résultat obtenu

La commande affiche immédiatement le nom de l'ordinateur sans options supplémentaires.

```
D:\>hostname
DESKTOP-SDDGPCG

D:\>|
```

- 7) **TASKKILL** termine un ou plusieurs processus par leur PID ou nom d'image.

```
D:\>taskkill /?

TASKKILL [/S système [/U utilisateur [/P [mot_passe]]]]
          { [/FI filtre] [/PID ID_processus | /IM image] } [/T] [/F]

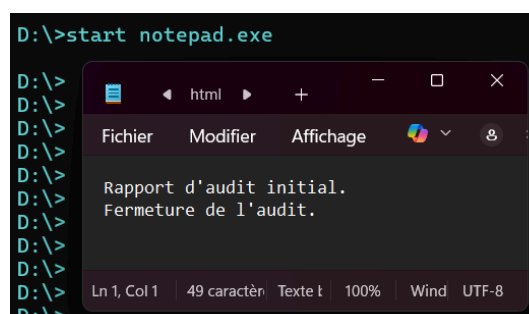
Description :
  Cet outil est utilisé pour arrêter des tâches par id de processus (PID) ou
  nom d'image.
```

#### Résultat obtenu

Le Bloc-notes a été fermé proprement par TASKKILL.

Donc il faut faire un start d'abord pour ouvrir un task, et puis taskkill pour arreter,

```
D:\>taskkill /IM notepad.exe
Opération réussie : un signal de fin a été envoyé au processus "Notepad.exe" de PID 11628.
```



## Commandes réseau

- 1) **PING** est l'outil de diagnostic réseau le plus utilisé. Il envoie des paquets ICMP Echo Request vers une destination pour : Tester la connectivité réseau, Diagnostiquer des problèmes de routage.

```
D:\>ping /?

Utilisation : ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
               [-r count] [-s count] [[-j host-list] | [-k host-list]]
               [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
               [-4] [-6] nom_cible
```

### Résultat obtenu

Le test PING vers le DNS public de Google (8.8.8.8) montre une connectivité parfaite avec une latence moyenne de 47ms.

```
D:\>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=47 ms TTL=117
Réponse de 8.8.8.8 : octets=32 temps=41 ms TTL=117
Réponse de 8.8.8.8 : octets=32 temps=56 ms TTL=117
Réponse de 8.8.8.8 : octets=32 temps=47 ms TTL=117

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 41ms, Maximum = 56ms, Moyenne = 47ms
```

- 2) **GETMAC** affiche l'adresse MAC (Media Access Control) de toutes les cartes réseau physiques et virtuelles.

```
D:\>getmac /?

GETMAC [/S système [/U nom_utilisateur [/P [mot_de_passe]]]] [/FO format]
      [/NH] [/V]

Description :
  Cet outil permet à un administrateur d'afficher l'adresse
  MAC des cartes réseaux d'un ordinateur.
```

### Résultat obtenu

La commande affiche l'adresse MAC unique de la carte réseau principale.

```
D:\>getmac

Adresse physique      Nom du transport
=====
D8-43-AE-05-13-0D    Support déconnecté
30-F6-EF-7A-0F-8F    N/A
0A-00-27-00-00-0C    N/A
```

- 3) **NETSTAT** est un outil puissant d'analyse réseau pour les Connexions réseau actives, Ports en écoute, Processus associés aux connexions.

```
D:\>netstat /?

Affiche les statistiques de protocole et les connexions réseau TCP/IP actuelles.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [intervalle]
```





## Résultat obtenu

NETSTAT affiche toutes les connexions TCP actives avec leurs états et adresses.

```
D:\>netstat -an
```

### Connexions actives

Proto	Adresse locale	Adresse distante	État
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49674	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9100	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9180	0.0.0.0:0	LISTENING
TCP	127.0.0.1:19293	0.0.0.0:0	LISTENING
TCP	127.0.0.1:49677	127.0.0.1:49678	ESTABLISHED
TCP	127.0.0.1:49678	127.0.0.1:49677	ESTABLISHED
TCP	127.0.0.1:49679	127.0.0.1:49680	ESTABLISHED
TCP	127.0.0.1:49680	127.0.0.1:49679	ESTABLISHED
TCP	127.0.0.1:63083	127.0.0.1:63084	ESTABLISHED
TCP	127.0.0.1:63084	127.0.0.1:63083	ESTABLISHED
TCP	127.0.0.1:63085	127.0.0.1:63086	ESTABLISHED
TCP	127.0.0.1:63086	127.0.0.1:63085	ESTABLISHED
TCP	172.20.10.3:139	0.0.0.0:0	LISTENING
TCP	172.20.10.3:49409	98.66.133.186:443	ESTABLISHED
TCP	172.20.10.3:56275	18.97.36.7:443	ESTABLISHED
TCP	172.20.10.3:56289	52.204.247.53:443	ESTABLISHED
TCP	172.20.10.3:56338	34.120.208.123:443	TIME_WAIT
TCP	172.20.10.3:64285	18.97.36.7:443	ESTABLISHED
TCP	172.20.10.3:64287	34.107.243.93:443	ESTABLISHED
TCP	192.168.56.1:139	0.0.0.0:0	LISTENING

## Partie 2: Les commandes DOSKEY

- 1) **DOSKEY** est un utilitaire Windows souvent sous-estimé qui transforme l'expérience de l'invite de commandes.
- 2) DOSKEY mémorise automatiquement les commandes que vous tapez et permet de les utiliser facilement comme :  
**Touches fléchées** (↑ / ↓) : naviguer dans l'historique.  
**F7** : afficher la liste complète des commandes précédentes.  
**F8** : recherche incrémentale dans l'historique.
- 3) Utilisations dans l'invite de commande : Nous allons voir les différentes utilisations de cette commande dans CMD :

**Affichage de l'historique de commandes :**

```
D:\>doskey /history
mkdir D:\Destination
move D:\test.txt D:\Source\
move D:\test2.txt D:\Destination\
dir D:\Source
dir D:\Destination
replace D:\Source\*.txt D:\Destination /A
```

**Création d'une macro :**

Pour pouvoir créer une macro (raccourci), il faut la mettre sous la forme suivante :

Donc si on veut par exemple faire une commande qui s'appelle **retour** et qui va faire remonter au dossier parent du dossier actuel en utilisant la commande **cd ..** :

```
D:\F A H A D>doskey roteur=cd ..
D:\F A H A D>|
```

Si on veut voir toutes les macros enregistrées, on utilise cette commande :

```
D:\F A H A D>doskey /macros
roteur=cd ..

D:\F A H A D>|
```

**Supprimer une macro :**

Pour supprimer une macro, il faut utiliser la commande suivante :

```
D:\F A H A D>doskey retour=

D:\F A H A D>|
```

#### 4) Tests pratiques sur CMD

**Afficher l'historique**

```
D:\F A H A D>doskey /history
xcopy D:\SourceXCOPY D:\DestXCOPY /E /I /Y
mkdir D:\SourceXCOPY
mkdir D:\DestXCOPY
echo Bonjour > D:\SourceXCOPY\fichier1.txt
echo Copie test > D:\SourceXCOPY\fichier2.txt
xcopy D:\SourceXCOPY D:\DestXCOPY /E /I /Y
timeout /?
timeout /T 5
timeout /T 3 /NOBREAK
color B
date
date /t
time /?
time
time /T
```

**Résultat** : L'historique affiche toutes les commandes précédemment tapées.

**Créer une macro simple:**

```
D:\F A H A D>doskey ll=dir /w

D:\F A H A D>ll
Le volume dans le lecteur D s'appelle DATA
Le numéro de série du volume est 18CA-448F

Répertoire de D:\F A H A D

[.]          [Contacts] [Documents] [Downloads] [Favorites] [Links]      [Music]      [Pictures] [Searches] [test_tp] [Videos]
             0 fichier(s)          0 octets
             11 Rép(s)  951 511 801 856 octets libres
```

**Résultat** : La macro `ll` fonctionne et affiche le contenu du répertoire.

**Créer une macro avec paramètre :**

```
D:\F A H A D>doskey backup=copy $1 $1.bak

D:\F A H A D>echo Test > fichier.txt

D:\F A H A D>backup fichier.txt
          1 fichier(s) copié(s).

D:\F A H A D>dir fichier.*
Le volume dans le lecteur D s'appelle DATA
Le numéro de série du volume est 18CA-448F

Répertoire de D:\F A H A D

07/10/2025  21:55                7 fichier.txt
07/10/2025  21:55                7 fichier.txt.bak
              2 fichier(s)              14 octets
              0 Rép(s)  951 511 769 088 octets libres
```

**Résultat** : La macro `backup` crée une copie du fichier avec l'extension `.bak`.

**Lister les macros**

```
D:\F A H A D>doskey /macros
roteur=cd ..
ll=dir /w
backup=copy $1 $1.bak
```

**Résultat** : Toutes les macros créées sont affichées.

**Supprimer une macro**

```
D:\F A H A D>doskey /macros
roteur=cd ..
ll=dir /w
backup=copy $1 $1.bak

D:\F A H A D>doskey backup=

D:\F A H A D>doskey /macros
roteur=cd ..
ll=dir /w

D:\F A H A D>|
```

**Résultat** : La macro **backup** a bien été supprimée avec la commande **doskey =backup .**

## Partie 3: Carte mentale

