

# Laboratorio sull'Utilizzo di Windows PowerShell

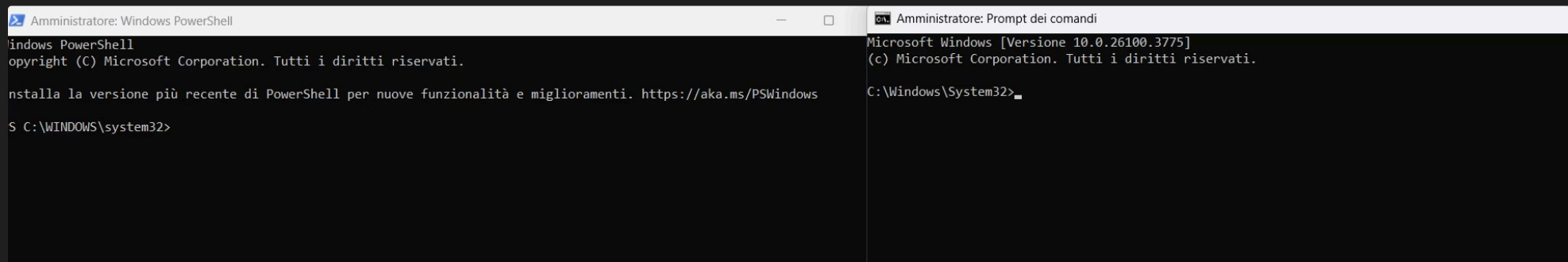
Questo documento riassume le attività svolte durante il laboratorio sull'utilizzo di Windows PowerShell. L'obiettivo principale è esplorare le funzionalità di PowerShell attraverso una serie di esercizi pratici, confrontandole con i comandi tradizionali del Prompt dei Comandi (CMD). Il laboratorio si articola in diverse sezioni, ognuna focalizzata su un aspetto specifico di PowerShell, come l'analisi dei cmdlet, l'uso del comando netstat, e la gestione del cestino.

# Confronto tra PowerShell e Prompt dei Comandi

L'immagine fornita mostra un confronto visivo tra l'interfaccia di PowerShell e quella del Prompt dei Comandi. Entrambi gli strumenti consentono di interagire con il sistema operativo tramite comandi testuali, ma PowerShell offre una sintassi più potente e flessibile.

Mentre il Prompt dei Comandi utilizza comandi semplici e diretti, PowerShell si basa su cmdlet, che sono piccoli programmi scritti in .NET. Questa differenza fondamentale permette a PowerShell di manipolare oggetti complessi e automatizzare compiti in modo più efficiente.

Inoltre, PowerShell supporta il piping, ovvero la possibilità di inviare l'output di un cmdlet come input a un altro, creando flussi di lavoro complessi e personalizzati. Questa funzionalità è limitata nel Prompt dei Comandi.



# Esplorazione dei Comandi: dir e ping

In questa sezione, abbiamo confrontato l'esecuzione dei comandi "dir" e "ping" sia in PowerShell che nel Prompt dei Comandi. Il comando "dir" visualizza l'elenco dei file e delle sottodirectory in una directory.

Mentre in CMD il comando "dir" è nativo, in PowerShell viene tradotto automaticamente nel cmdlet "Get-ChildItem". Entrambi i comandi producono un output simile, ma PowerShell offre maggiori opzioni di formattazione e filtraggio.

Il comando "ping", utilizzato per verificare la connettività di rete, restituisce lo stesso risultato sia in PowerShell che in CMD. Tuttavia, PowerShell consente di manipolare l'output del comando ping tramite cmdlet, ad esempio per estrarre informazioni specifiche come il tempo di risposta medio.

Comando	Prompt dei Comandi	PowerShell
dir	Nativo	Alias per Get-ChildItem
ping	Nativo	Nativo

Amministratore: Windows PowerShell

```
a---- 03/04/2025 19:33 157128 xmlfilter.dll
a---- 03/04/2025 19:32 253416 xmlite.dll
a---- 03/04/2025 19:32 53248 xmlprovi.dll
a---- 03/04/2025 19:33 94208 xolehlp.dll
a---- 03/04/2025 19:32 389120 XpsDocumentTargetPrint.dll
a---- 03/04/2025 19:32 409600 XpsGdiConverter.dll
a---- 03/04/2025 19:32 1236992 XpsPrint.dll
a---- 03/04/2025 19:33 323584 xpspushlayer.dll
a---- 03/04/2025 19:32 1294336 XpsRasterService.dll
a---- 03/04/2025 19:32 2686976 xpsservices.dll
a---- 03/04/2025 19:32 217088 XpsToPclmConverter.dll
a---- 03/04/2025 19:33 118784 XpsToPwgrConverter.dll
a---- 03/04/2025 19:33 102400 XpsToTiffConverter.dll
a---- 01/04/2024 09:22 4014 xwizard.dtd
a---- 03/04/2025 19:32 94208 xwizard.exe
a---- 03/04/2025 19:33 458752 xwizards.dll
a---- 03/04/2025 19:32 151552 xwreg.dll
a---- 03/04/2025 19:32 286720 xwtpdui.dll
a---- 03/04/2025 19:32 167936 xwtpw32.dll
a---- 03/04/2025 19:32 118784 zipcontainer.dll
a---- 03/04/2025 19:32 655360 zipfldr.dll
a---- 03/04/2025 19:33 55184 ztdnsapi.dll
a---- 03/04/2025 19:33 53248 ztrace_maps.dll

S C:\WINDOWS\system32>
S C:\WINDOWS\system32>
```

Amministratore: Prompt dei comandi

```
03/04/2025 19:33 77.824 XInputUap.dll
03/04/2025 19:33 157.128 xmlfilter.dll
03/04/2025 19:32 253.416 xmlite.dll
03/04/2025 19:32 53.248 xmlprovi.dll
03/04/2025 19:33 94.208 xolehlp.dll
03/04/2025 19:32 389.120 XpsDocumentTargetPrint.dll
03/04/2025 19:32 409.600 XpsGdiConverter.dll
03/04/2025 19:32 1.236.992 XpsPrint.dll
03/04/2025 19:33 323.584 xpspushlayer.dll
03/04/2025 19:32 1.294.336 XpsRasterService.dll
03/04/2025 19:32 2.686.976 xpsservices.dll
03/04/2025 19:32 217.088 XpsToPclmConverter.dll
03/04/2025 19:33 118.784 XpsToPwgrConverter.dll
03/04/2025 19:33 102.400 XpsToTiffConverter.dll
01/04/2024 09:22 4.014 xwizard.dtd
03/04/2025 19:32 94.208 xwizard.exe
03/04/2025 19:33 458.752 xwizards.dll
03/04/2025 19:32 151.552 xwreg.dll
03/04/2025 19:32 286.720 xwtpdui.dll
03/04/2025 19:32 167.936 xwtpw32.dll
03/04/2025 19:35 <DIR> zh-CN
03/04/2025 19:35 <DIR> zh-TW
03/04/2025 19:32 118.784 zipcontainer.dll
03/04/2025 19:32 655.360 zipfldr.dll
03/04/2025 19:33 55.184 ztdnsapi.dll
03/04/2025 19:33 53.248 ztrace_maps.dll
4391 File 2.477.557.819 byte
177 Directory 176.733.347.840 byte disponibili

C:\Windows\System32>
```

Amministratore: Windows PowerShell

```
a---- 03/04/2025 19:32 217088 XpsToPclmConverter.dll
a---- 03/04/2025 19:33 118784 XpsToPwgrConverter.dll
a---- 03/04/2025 19:33 102400 XpsToTiffConverter.dll
a---- 01/04/2024 09:22 4014 xwizard.dtd
a---- 03/04/2025 19:32 94208 xwizard.exe
a---- 03/04/2025 19:33 458752 xwizards.dll
a---- 03/04/2025 19:32 151552 xwreg.dll
a---- 03/04/2025 19:32 286720 xwtpdui.dll
a---- 03/04/2025 19:32 167936 xwtpw32.dll
a---- 03/04/2025 19:32 118784 zipcontainer.dll
a---- 03/04/2025 19:32 655360 zipfldr.dll
a---- 03/04/2025 19:33 55184 ztdnsapi.dll
a---- 03/04/2025 19:33 53248 ztrace_maps.dll

S C:\WINDOWS\system32>
S C:\WINDOWS\system32> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=18ms TTL=116
Risposta da 8.8.8.8: byte=32 durata=19ms TTL=116
Risposta da 8.8.8.8: byte=32 durata=19ms TTL=116
Risposta da 8.8.8.8: byte=32 durata=18ms TTL=116

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 18ms, Massimo = 19ms, Medio = 18ms

S C:\WINDOWS\system32>
```

Amministratore: Prompt dei comandi

```
01/04/2024 09:22 4.014 xwizard.dtd
03/04/2025 19:32 94.208 xwizard.exe
03/04/2025 19:33 458.752 xwizards.dll
03/04/2025 19:32 151.552 xwreg.dll
03/04/2025 19:32 286.720 xwtpdui.dll
03/04/2025 19:32 167.936 xwtpw32.dll
03/04/2025 19:35 <DIR> zh-CN
03/04/2025 19:35 <DIR> zh-TW
03/04/2025 19:32 118.784 zipcontainer.dll
03/04/2025 19:32 655.360 zipfldr.dll
03/04/2025 19:33 55.184 ztdnsapi.dll
03/04/2025 19:33 53.248 ztrace_maps.dll
4391 File 2.477.557.819 byte
177 Directory 176.733.347.840 byte disponibili

C:\Windows\System32>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=18ms TTL=116
Risposta da 8.8.8.8: byte=32 durata=18ms TTL=116
Risposta da 8.8.8.8: byte=32 durata=19ms TTL=116
Risposta da 8.8.8.8: byte=32 durata=18ms TTL=116

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 18ms, Massimo = 19ms, Medio = 18ms

C:\Windows\System32>
```



# Esplorazione dei Cmdlet: Get-Alias e Get-Process

I cmdlet sono i comandi fondamentali di PowerShell, strutturati come stringhe verbo-nome. Il cmdlet **Get-Alias** permette di scoprire gli alias definiti per i comandi. Ad esempio, Get-Alias dir rivela che "dir" è un alias per il cmdlet **Get-ChildItem**.

**Get-Process** è un altro cmdlet utile che visualizza l'elenco dei processi attivi sul sistema. L'output include informazioni come il nome del processo, il PID (Process Identifier), l'utilizzo della CPU e della memoria.

Altri cmdlet interessanti includono:

- Get-EventLog: legge i log di sistema.
- Get-Service: visualizza i servizi attivi e il loro stato.

```
Amministratore: Windows PowerShell

Directory: C:\WINDOWS\system32

Mode                LastWriteTime         Length Name
----                -
d-----         01/04/2024        18:38          0409
d-----         03/04/2025        19:35      AccountHealthAssets
d-----         03/04/2025        19:35      AdvancedInstallers
d-----         03/04/2025        19:35          af-ZA
d-----         03/04/2025        19:35          am-ET
d-----         04/04/2025         03:47          AMD
d-----         04/04/2025         03:51      AppLocker
d-----         03/04/2025        19:35      appraiser
d-----         03/04/2025        19:35          ar-SA
d-----         03/04/2025        19:35          as-IN
d-----         03/04/2025        19:35      az-Latn-AZ
d-----         03/04/2025        19:35          be-BY
d-----         03/04/2025        19:35          bg-BG
d-----         03/04/2025        19:35          bn-IN
d-----         09/04/2025         01:00      Boot
d-----         03/04/2025        19:35      bs-Latn-BA
d-----         01/04/2024         09:26      Bthprops
d-----         03/04/2025        19:35          ca-ES
d-----         03/04/2025        19:35      ca-ES-valencia
d-----         03/04/2025        22:54      CatRoot
d-----         10/04/2025        15:48      catroot2
d-----         03/04/2025        19:35      chr-CHER-US
d-----         09/04/2025         01:00      CodeIntegrity
d-----         03/04/2025        19:35          Com
d-----         11/04/2025        10:03      config
d---s-         01/04/2024         09:34      Configuration
d-----         03/04/2025        19:35          cs-CZ
d-----         03/04/2025        19:35          cy-GB
d-----         03/04/2025        19:35          da-DK
d-----         03/04/2025        19:35      DDFs
d-----         03/04/2025        19:35          de-DE
d---s-         04/04/2025         03:47      DiagSvcs
d-----         03/04/2025        19:35          Dism
d-----         01/04/2024         09:26      downlevel
d-----         09/04/2025         01:00      drivers
d-----         01/04/2024         09:26      DriverState
d-----         10/04/2025        15:48      DriverStore
d---s-         03/04/2025        19:29      dsc
d-----         03/04/2025        19:35          el-GR
d-----         04/04/2025         03:43      ElevocConfig
d-----         04/04/2025         03:43      ElevocInstallDriver
d-----         03/04/2025        19:29          en
```



# Analisi delle Connessioni di Rete con netstat

Il comando **netstat** è uno strumento potente per analizzare le connessioni di rete attive sul sistema. In PowerShell, è possibile utilizzare netstat con diverse opzioni per ottenere informazioni specifiche.

**netstat -h** visualizza l'elenco delle opzioni disponibili. **netstat -r** mostra la tabella di routing, che indica i percorsi attivi per il traffico di rete.

```
PS C:\WINDOWS\system32> netstat -h

Socket Handle Count

    PID          Count    Closing Count
    ----          -
    12800         21         0
    4868          4         0
    17160         33         0
    1292          4         0
    3340          7         0
    2064          2         0
    5404          2         0
    20252         1         0
    1824          2         0
    2356          1         0
    5436         61        16
    3392          4         0
    3152         12         0
    14432         1         0
    9572          4         0
    17508         31         8
    10096         1         0
    17028         4         0
    1416          4         0
    3976          4         0
    2444          4         0
    13984         2         0
    9892          6         0
    18340         4         0
    13736         9         0
    5556          3         0
    5304          4         0
    10424         2         0
    1468          4         0
    5324          1         0
    20180         4         0
    14552        35         0
    16344         1         0
    17116        19         6
    9184          1         0
    16612        33         0
    16368         1         0
    1780         11         0
    5368          6         0
    9980          7         0

PS C:\WINDOWS\system32>
```

```
Amministratore: Windows PowerShell
PS C:\WINDOWS\system32> netstat -r

=====
Elenco interfacce
 8...0a 00 27 00 00 08 .....VirtualBox Host-Only Ethernet Adapter
16...ba 1e a4 ab f8 99 .....Microsoft Wi-Fi Direct Virtual Adapter
 9...be 1e a4 ab f8 99 .....Microsoft Wi-Fi Direct Virtual Adapter #2
18...b8 1e a4 ab f8 99 .....Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
 4...b8 1e a4 ab f8 9a .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia  Metrica
  -----
    0.0.0.0           0.0.0.0    192.168.1.1   192.168.1.11    30
    127.0.0.0         255.0.0.0   On-link      127.0.0.1     331
    127.0.0.1       255.255.255.255   On-link      127.0.0.1     331
 127.255.255.255   255.255.255.255   On-link      127.0.0.1     331
    192.168.1.0       255.255.255.0   On-link      192.168.1.11   286
    192.168.1.11     255.255.255.255   On-link      192.168.1.11   286
    192.168.1.255    255.255.255.255   On-link      192.168.1.11   286
    192.168.56.0     255.255.255.0   On-link      192.168.56.1   281
    192.168.56.1    255.255.255.255   On-link      192.168.56.1   281
    192.168.56.255   255.255.255.255   On-link      192.168.56.1   281
    224.0.0.0         240.0.0.0   On-link      127.0.0.1     331
    224.0.0.0         240.0.0.0   On-link      192.168.56.1   281
    224.0.0.0         240.0.0.0   On-link      192.168.1.11   286
 255.255.255.255   255.255.255.255   On-link      127.0.0.1     331
 255.255.255.255   255.255.255.255   On-link      192.168.56.1   281
 255.255.255.255   255.255.255.255   On-link      192.168.1.11   286
=====
Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  ---
 1      331  ::1/128             On-link
 8      281  fe80::/64           On-link
18      286  fe80::/64           On-link
 8      281  fe80::2b5:20:ec62:1b5d/128
                               On-link
18      286  fe80::53df:173b:f060:6c20/128
                               On-link
 1      331  ff00::/8            On-link
 8      281  ff00::/8            On-link
18      286  ff00::/8            On-link
```

```
Amministratore: Windows PowerShell
Route permanenti:
 Nessuna
PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

Proto  Indirizzo locale      Indirizzo esterno      Stato      PID
-----
TCP    0.0.0.0:135           0.0.0.0:0              LISTENING  1780
RpcsS
[svchost.exe]
TCP    0.0.0.0:445           0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040          0.0.0.0:0              LISTENING  9980
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680          0.0.0.0:0              LISTENING  13984
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664         0.0.0.0:0              LISTENING  1468
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665         0.0.0.0:0              LISTENING  1292
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666         0.0.0.0:0              LISTENING  2444
Schedule
[svchost.exe]
TCP    0.0.0.0:49667         0.0.0.0:0              LISTENING  3392
EventLog
[svchost.exe]
TCP    0.0.0.0:49668         0.0.0.0:0              LISTENING  4868
[spoolsv.exe]
TCP    0.0.0.0:49669         0.0.0.0:0              LISTENING  1416
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:6463        0.0.0.0:0              LISTENING  17160
[Discord.exe]
TCP    127.0.0.1:49786      0.0.0.0:0              LISTENING  16612
[ChatGPT.exe]
TCP    127.0.0.1:53515      127.0.0.1:53516       ESTABLISHED 17116
[CiscoCollabHost.exe]
TCP    127.0.0.1:53516      127.0.0.1:53515       ESTABLISHED 17116
[CiscoCollabHost.exe]
TCP    127.0.0.1:53517      127.0.0.1:53518       ESTABLISHED 17116
[CiscoCollabHost.exe]
TCP    127.0.0.1:53518      127.0.0.1:53517       ESTABLISHED 17116
[CiscoCollabHost.exe]
TCP    127.0.0.1:53519      127.0.0.1:53520       ESTABLISHED 17116
[CiscoCollabHost.exe]
TCP    127.0.0.1:53520      127.0.0.1:53519       ESTABLISHED 17116
[CiscoCollabHost.exe]
TCP    127.0.0.1:53521      127.0.0.1:53522       ESTABLISHED 17116
[CiscoCollabHost.exe]
```

**netstat -abno** visualizza i processi associati alle connessioni TCP attive, includendo il PID (Process Identifier) e il nome del processo. Questa informazione è utile per identificare quali applicazioni stanno utilizzando la rete e quali porte sono aperte

"L'analisi delle connessioni di rete è fondamentale per la sicurezza e il monitoraggio delle prestazioni del sistema."

# Correlazione tra netstat e Task Manager

Per correlare le informazioni ottenute con netstat con i processi in esecuzione, è possibile utilizzare il Task Manager di Windows. Il Task Manager, accessibile premendo Ctrl+Shift+Esc, fornisce una panoramica dei processi attivi, inclusi i PID, l'utilizzo della CPU e della memoria.

Dettagli								
	Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Architet...	Descrizione
	Interrupt sistema	-	In esecuzione	SYSTEM	01	0 K		Chiamate di procedura differite e ISR (Interrupt Service Routine)
	Processo di inattività ...	0	In esecuzione	SYSTEM	96	8 K		Percentuale di tempo di inattività del processore
	System	4	In esecuzione	SYSTEM	00	12 K		NT Kernel & System
	Secure System	188	In esecuzione	SYSTEM	00	64.204 K		NT Kernel & System
	Registry	228	In esecuzione	SYSTEM	00	3.212 K		NT Kernel & System
	dasHost.exe	344	In esecuzione	SERVIZIO D...	00	24 K	x64	Device Association Framework Provider Host
	smss.exe	736	In esecuzione	SYSTEM	00	100 K		Gestione sessioni di Windows
	svchost.exe	884	In esecuzione	SYSTEM	00	740 K	x64	Processo host per servizi di Windows
	ApplicationFrameHo...	1124	In esecuzione	lucat	00	1.088 K	x64	Application Frame Host
	csrss.exe	1152	In esecuzione	SYSTEM	00	688 K		Processo runtime client server
	powershell.exe	1164	In esecuzione	lucat	00	25.352 K	x64	Windows PowerShell
	wininit.exe	1292	In esecuzione	SYSTEM	00	8 K		Applicazione di avvio di Windows
	csrss.exe	1300	In esecuzione	SYSTEM	00	704 K		Processo runtime client server
	winlogon.exe	1396	In esecuzione	SYSTEM	00	472 K	x64	Applicazione Accesso a Windows
	svchost.exe	1412	In esecuzione	SYSTEM	00	708 K	x64	Processo host per servizi di Windows
	services.exe	1416	In esecuzione	SYSTEM	00	3.128 K		App Servizi e Controller
	svchost.exe	1444	In esecuzione	SYSTEM	00	284 K	x64	Processo host per servizi di Windows
	Lsalso.exe	1460	In esecuzione	SYSTEM	00	8 K	x64	Credential Guard & VBS Key Isolation
	lsass.exe	1468	In esecuzione	SYSTEM	00	5.240 K		Local Security Authority Process
	dasHost.exe	1496	In esecuzione	SERVIZIO D...	00	32 K	x64	Device Association Framework Provider Host
	svchost.exe	1608	In esecuzione	SYSTEM	00	8.432 K	x64	Processo host per servizi di Windows
	svchost.exe	1624	In esecuzione	SERVIZIO D...	00	3.060 K	x64	Processo host per servizi di Windows
	WUDFHost.exe	1640	In esecuzione	SERVIZIO L...	00	548 K	x64	Windows Driver Foundation - Processo host Framework driver modalità utente
	fontdrvhost.exe	1660	In esecuzione	UMFD-0	00	140 K	x64	Usermode Font Driver Host
	fontdrvhost.exe	1664	In esecuzione	UMFD-1	00	1.660 K	x64	Usermode Font Driver Host
	dllhost.exe	1728	In esecuzione	lucat	00	1.012 K	x64	COM Surrogate
	svchost.exe	1780	In esecuzione	SERVIZIO D...	00	7.768 K	x64	Processo host per servizi di Windows
	svchost.exe	1824	In esecuzione	SYSTEM	00	1.464 K	x64	Processo host per servizi di Windows
	dwm.exe	1952	In esecuzione	DWM-1	00	26.428 K	x64	Gestione finestre desktop
	WUDFHost.exe	1972	In esecuzione	SERVIZIO L...	00	528 K	x64	Windows Driver Foundation - Processo host Framework driver modalità utente
	svchost.exe	2064	In esecuzione	SERVIZIO L...	00	448 K	x64	Processo host per servizi di Windows
	svchost.exe	2092	In esecuzione	SERVIZIO L...	00	1.712 K	x64	Processo host per servizi di Windows
	svchost.exe	2128	In esecuzione	SERVIZIO L...	00	3.112 K	x64	Processo host per servizi di Windows
	chrome.exe	2136	In esecuzione	lucat	00	6.124 K	x64	Google Chrome

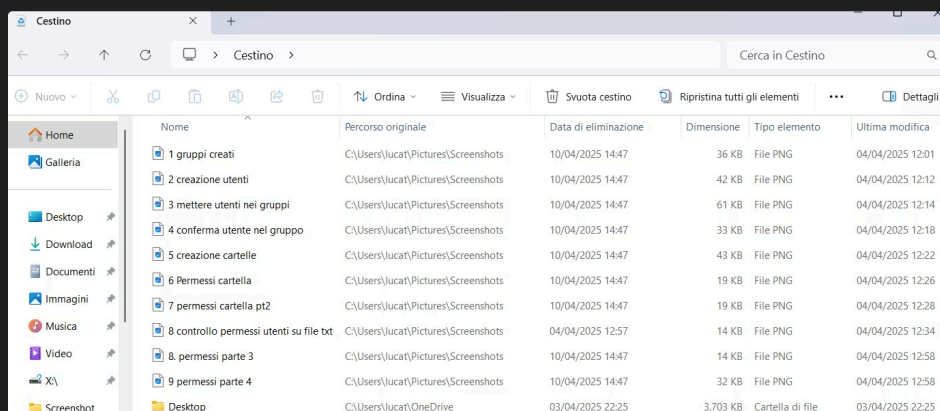
Nella scheda "Dettagli" del Task Manager, è possibile ordinare i processi per PID per individuare facilmente il processo corrispondente a un determinato PID ottenuto con netstat.

Facendo clic con il pulsante destro del mouse su un processo nel Task Manager, è possibile accedere alle "Proprietà" per ottenere ulteriori informazioni, come il percorso del file eseguibile e la firma digitale.

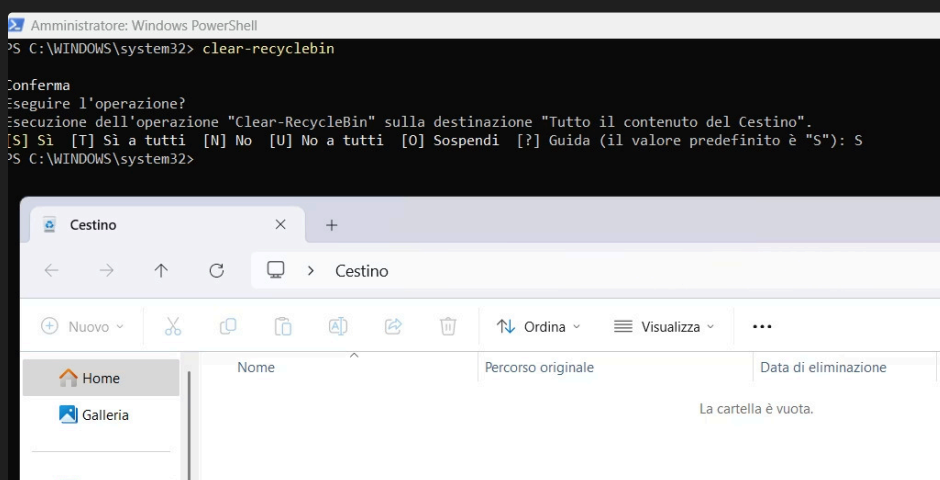


# Gestione del Cestino tramite PowerShell

PowerShell offre un cmdlet dedicato per la gestione del cestino: **Clear-RecycleBin**. Questo cmdlet permette di svuotare il cestino in modo rapido e semplice.



Prima di eseguire il comando, è possibile verificare il contenuto del cestino tramite l'interfaccia grafica di Windows. Dopo aver eseguito **Clear-RecycleBin**, il cestino verrà svuotato e i file eliminati in modo permanente.



È importante notare che **Clear-RecycleBin** richiede conferma prima di svuotare il cestino. È possibile utilizzare l'opzione **-Force** per evitare la richiesta di conferma e svuotare il cestino automaticamente.

# Comandi di PowerShell vs CMD

## CMD

- Sintassi più semplice
- Comandi diretti
- Limitata manipolazione degli oggetti

## PowerShell

- Sintassi verbo-nome
- Cmdlet basati su .NET
- Piping per flussi di lavoro complessi
- Maggiore flessibilità e potenza

PowerShell offre una maggiore flessibilità e potenza rispetto al Prompt dei Comandi.



# Conclusioni

Questo laboratorio ha fornito una panoramica delle funzionalità di Windows PowerShell, confrontandole con i comandi tradizionali del Prompt dei Comandi. Abbiamo esplorato i cmdlet, l'uso del comando netstat, la gestione del cestino, e la correlazione tra PowerShell e Task Manager.

PowerShell si dimostra uno strumento potente e versatile per l'amministrazione di sistemi Windows, offrendo una sintassi flessibile, cmdlet basati su .NET, e funzionalità avanzate come il piping.

Si consiglia di approfondire la conoscenza di PowerShell attraverso ulteriori esercizi pratici e l'esplorazione della vasta gamma di cmdlet disponibili.