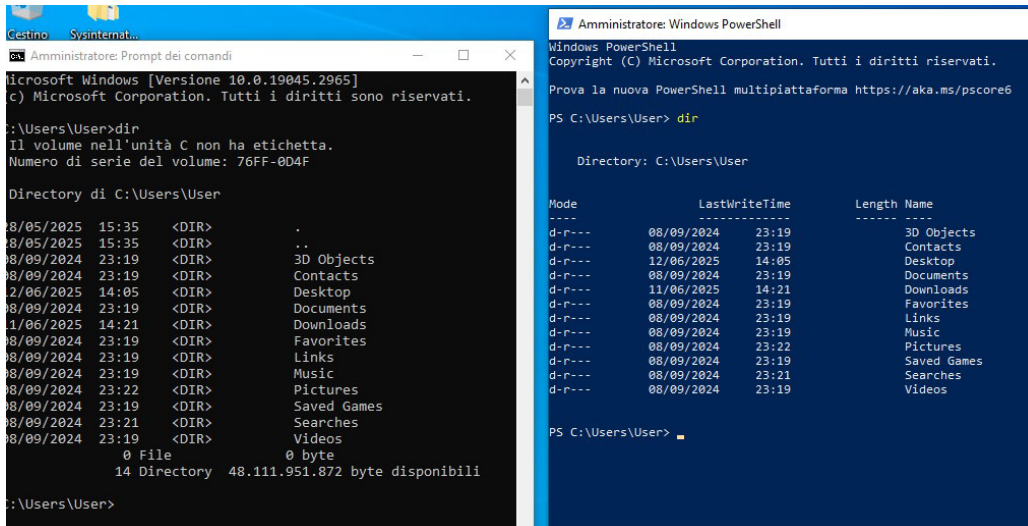


ESERCIZIO 1 - USARE WINDOWS POWERSHELL



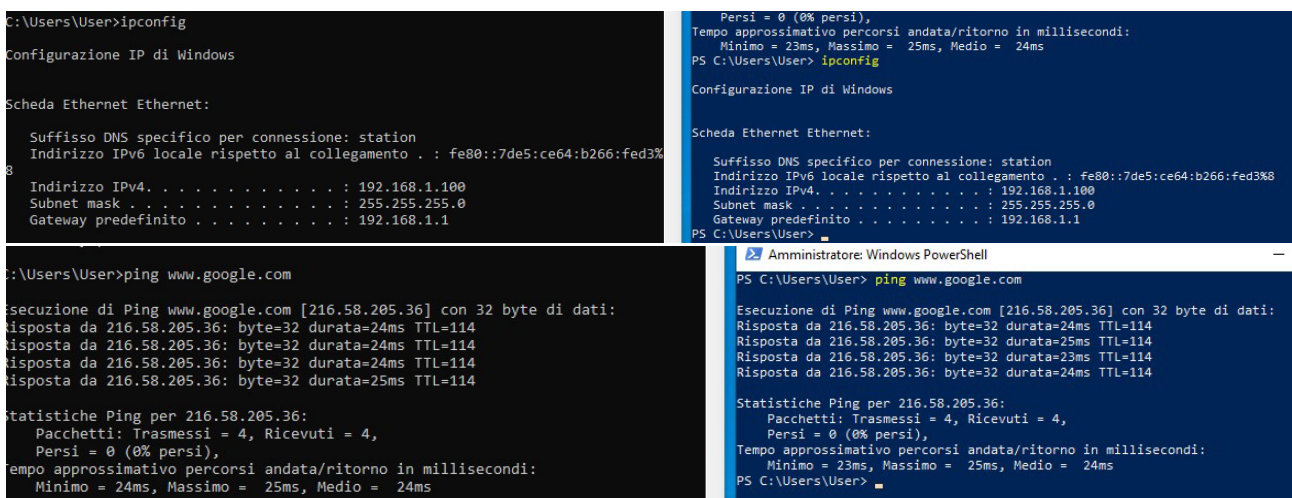
The left screenshot shows the Windows Command Prompt (Prompt dei comandi) running the 'dir' command. The output is in a standard DOS-style text format, listing files and directories with their dates, times, and sizes. The right screenshot shows the Windows PowerShell (Amministratore: Windows PowerShell) running the 'dir' command. The output is more structured, displaying a table with columns for Mode, LastWriteTime, Length, and Name, providing a more detailed view of the directory contents.

- Quali sono gli output del comando dir?

Il comando dir nel Prompt dei Comandi mostra un output in stile DOS, con <DIR> per indicare le directory e informazioni sullo spazio libero. In PowerShell, l'output è più strutturato: visualizza colonne come Mode, LastWriteTime, Length, Name

- Quali sono i risultati?

I comandi ipconfig, ping e cd funzionano sia nel Prompt dei Comandi che in PowerShell. I risultati sono gli stessi in entrambi i casi, anche se PowerShell può presentare l'output in modo leggermente diverso. I comandi di rete (ping, ipconfig) producono informazioni identiche e cd restituisce lo stesso percorso corrente: C:\Users\Users



The top row shows the output of the 'ipconfig' command. The left screenshot (Command Prompt) shows the standard text output for the Ethernet adapter. The right screenshot (PowerShell) shows the same information but with a more structured layout, including a header for the IP configuration and a table for the network statistics. The bottom row shows the output of the 'ping' command. The left screenshot (Command Prompt) shows the standard text output for the ping to www.google.com. The right screenshot (PowerShell) shows the same information but with a more structured layout, including a header for the ping command and a table for the network statistics.

Il comando 'cd'

- Qual è il comando Powershell per dir?

È Get-ChildItem

```
PS C:\Users\User> Get-Alias dir

CommandType      Name                                           Version      Source
-----
Alias             dir -> Get-ChildItem
```

- Qual è il gateway IPv4?

192.168.1.1

Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.100	281
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	192.168.1.100	281
192.168.1.100	255.255.255.255	On-link	192.168.1.100	281
192.168.1.255	255.255.255.255	On-link	192.168.1.100	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	192.168.1.100	281
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	192.168.1.100	281

- Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Dalla scheda Dettagli è possibile ottenere informazioni sul nome del processo, PID, stato, utilizzo delle risorse e utente associato.

Dalla finestra **Proprietà** del PID selezionato si possono vedere dati come il percorso del file, la versione, il produttore e la data di modifica del file eseguibile.

The screenshot shows a Windows desktop with a taskbar containing icons for Microsoft Edge, Wireshark, and an Administrator Windows PowerShell window. The PowerShell window displays the command `netstat -abno` and its output, which includes a table of active connections. One connection is highlighted with PID 900, corresponding to `svchost.exe`. To the right, the Task Manager window is open, showing the 'Processi' tab with a list of running processes. The process `svchost.exe` with PID 900 is selected. The 'Proprietà - svchost' dialog box is open, showing the 'Generale' tab with details about the file `svchost.exe`, including its path, size, and creation/modification dates.

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	900
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	1172
CDPSvc				

Nome	PID	Stato
svchost.exe	448	In esecuzione
csrss.exe	464	In esecuzione
svchost.exe	532	In esecuzione
wininit.exe	540	In esecuzione
csrss.exe	556	In esecuzione
winlogon.exe	632	In esecuzione
services.exe	668	In esecuzione
lsass.exe	688	In esecuzione
svchost.exe	740	In esecuzione
conhost.exe	744	In esecuzione
fontdrvhost.exe	772	In esecuzione
svchost.exe	808	In esecuzione
svchost.exe	900	In esecuzione
svchost.exe	944	In esecuzione
dmv.exe	992	In esecuzione
WmiPvSE.exe	1156	In esecuzione
svchost.exe	1172	In esecuzione
svchost.exe	1300	In esecuzione
svchost.exe	1392	In esecuzione
VRService.exe	1408	In esecuzione

Generale	Firme digitali	Sicurezza	Dettagli	Versioni precedenti
svchost				
Tipo di file: Applicazione (.exe)				
Descrizione: Processo host per servizi di Windows				
Percorso: C:\Windows\System32				
Dimensioni: 54,0 KB (55.320 byte)				
Dimensioni su disco: 56,0 KB (57.344 byte)				
Data creazione: venerdì 5 maggio 2023, 14:22:19				
Ultima modifica: venerdì 5 maggio 2023, 14:22:19				
Ultimo accesso: Oggi 13 giugno 2025, 35 minuti fa				
Attributi: <input type="checkbox"/> Sola lettura <input type="checkbox"/> Nascosto <input data-bbox="1331 1823 1410 1845" type="button" value="Avanzate..."/>				

- **Cosa è successo al file nel cestino?**

Utilizzando il comando `clear-recyclebin` e confermando con `S` il cestino viene svuotato e i file eliminati in modo permanente

- **Riflessione. Registra le tue scoperte.**

PowerShell si è dimostrato uno strumento estremamente utile per la gestione e l'automazione delle attività su un sistema Windows. Durante l'esercizio, ho esplorato diverse funzionalità come ad esempio confrontando i comandi tradizionali del Prompt con i cmdlet specifici di PowerShell, visualizzato connessioni di rete attive tramite `netstat -abno` e associato i processi ai relativi PID attraverso Gestione Attività. Infine, ho appreso come eseguire operazioni di sistema come lo svuotamento del Cestino con il comando `Clear-RecycleBin`, dimostrando come PowerShell possa semplificare azioni che altrimenti richiederebbero più passaggi nell'interfaccia grafica.

PowerShell può essere particolarmente utile anche in ambito cybersecurity e amministrazione, grazie a comandi come `Get-Process`, `Get-Service`, `Get-EventLog` o `Get-LocalUser`, che permettono di monitorare e analizzare lo stato del sistema, i log di sicurezza e l'attività degli utenti.