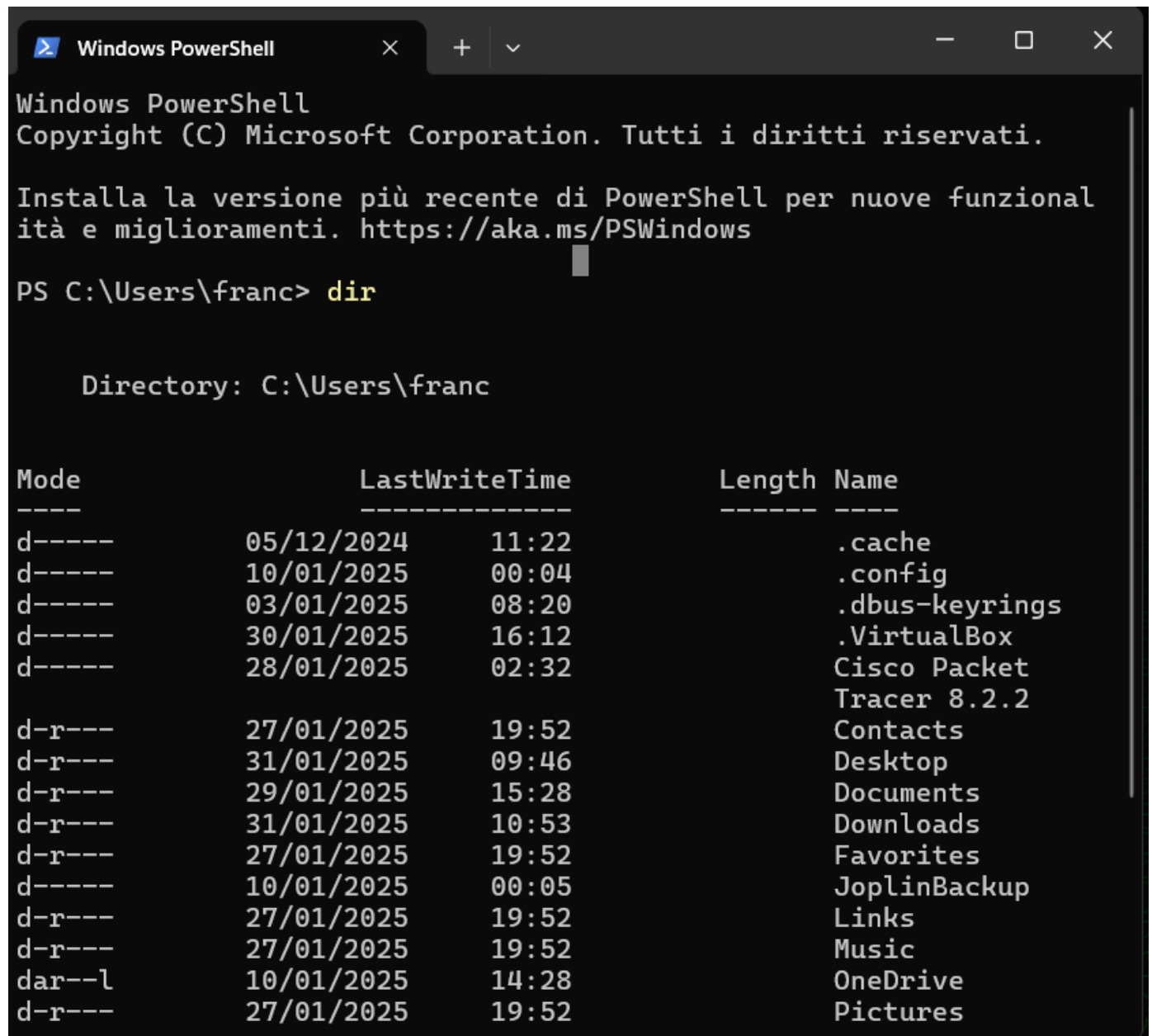


Windows PowerShell

Ho iniziato col dare il comando `dir` che mi ha mostrato tutte le cartelle.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzional
ità e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\franc> dir

Directory: C:\Users\franc

Mode                LastWriteTime         Length Name
----                -
d-----         05/12/2024         11:22         .cache
d-----         10/01/2025         00:04         .config
d-----         03/01/2025         08:20         .dbus-keyrings
d-----         30/01/2025         16:12         .VirtualBox
d-----         28/01/2025         02:32         Cisco Packet
Tracer 8.2.2
d-r---         27/01/2025         19:52         Contacts
d-r---         31/01/2025         09:46         Desktop
d-r---         29/01/2025         15:28         Documents
d-r---         31/01/2025         10:53         Downloads
d-r---         27/01/2025         19:52         Favorites
d-----         10/01/2025         00:05         JoplinBackup
d-r---         27/01/2025         19:52         Links
d-r---         27/01/2025         19:52         Music
dar--l         10/01/2025         14:28         OneDrive
d-r---         27/01/2025         19:52         Pictures
```

poi ho testato il comando `ipconfig`

```
Windows PowerShell
- p      Esegue il ping dell'indirizzo di un provider
- 4      Impone l'utilizzo di IPv4.
- 6      Impone l'utilizzo di IPv6.

PS C:\Users\franc> cd
PS C:\Users\franc> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Ethernet Ethernet 4:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2a04:7
04d:b9a5:d6cc%10
    Indirizzo IPv4. . . . . : 192.168.218.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 3:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:
```

Poi ho testato un comando cmdlet per ottenere le sottodirectory e i file in una directory.

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

CommandType      Name
-----
Alias            dir -> Get-ChildItem

PS C:\Users\franc>
```

Poi ho testato il `netstat -r`

```

PS C:\Users\franc> netstat -r
=====
=====
Elenco interfacce
 13...38 ca 84 c6 a5 0c .....Realtek PCIe GbE Family Controller
 10...0a 00 27 00 00 0a .....VirtualBox Host-Only Ethernet Adapter
r
 15...12 b1 df ce bb 33 .....Microsoft Wi-Fi Direct Virtual Adapter #3
 18...92 b1 df ce bb 33 .....Microsoft Wi-Fi Direct Virtual Adapter #4
 22...10 b1 df ce bb 33 .....Realtek RTL8822CE 802.11ac PCIe Adapter
 1.....Software Loopback Interface 1
=====
=====

IPv4 Tabella route
=====
=====
Route attive:

```

	Indirizzo rete	Mask	Gateway	Interfaccia
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.4
	127.0.0.0	255.0.0.0	On-link	127.0.0.1
	127.0.0.1	255.255.255.255	On-link	127.0.0.1

Poi ho testato anche il manuale di netstat

```

PS C:\Users\franc> netstat -help

Mostra le statistiche del protocollo e le connessioni di rete TCP/IP
correnti.

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

-a          Mostra tutte le connessioni e le porte di ascolto.
-b          Mostra l'eseguibile coinvolto nella creazione di ogni
connessione o porta di ascolto. In alcuni casi, eseguibili noti
ospitano più componenti indipendenti e in questi casi la
sequenza dei componenti coinvolti nella creazione
della connessione o della porta di ascolto viene visualizzata. In
questo caso, il nome dell'eseguibile

```

Dopo ho eseguito la PowerShell come amministratore.



Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive digitando `netstat -abno`.

```

Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows
PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

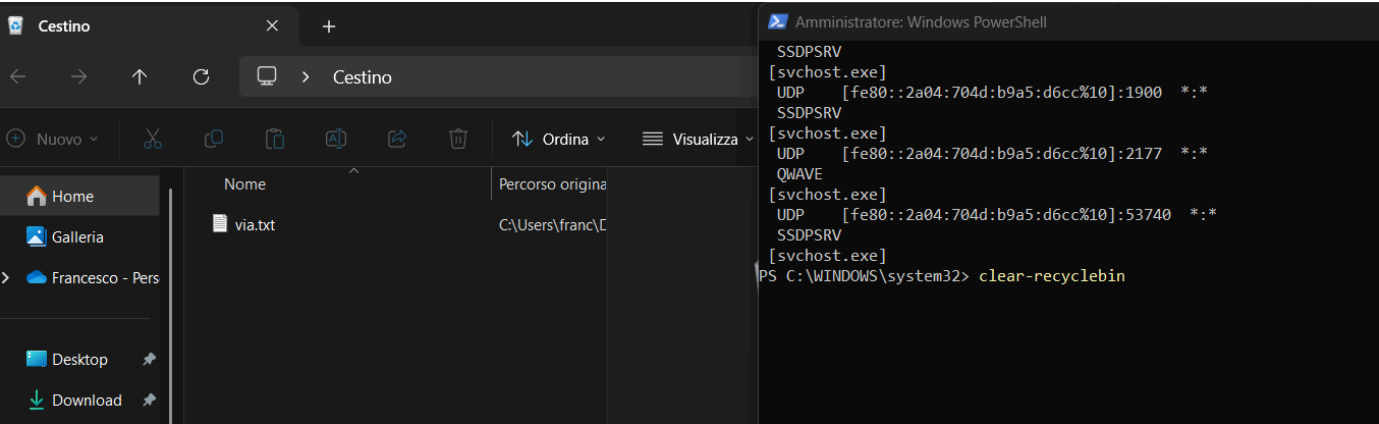
Proto Indirizzo locale      Indirizzo esterno  Stato      PID
TCP    0.0.0.0:135              0.0.0.0:0          LISTENING   1552
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0          LISTENING   4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040             0.0.0.0:0          LISTENING   8140
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680             0.0.0.0:0          LISTENING   7800
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664            0.0.0.0:0          LISTENING   1276
[Sistema]
TCP    0.0.0.0:49665            0.0.0.0:0          LISTENING   1096
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49668            0.0.0.0:0          LISTENING   2632
Schedule
[svchost.exe]
TCP    0.0.0.0:49669            0.0.0.0:0          LISTENING   3368
EventLog
[svchost.exe]

```

Ho visto che mi dava il PID 1552 così col task manager sono andato a verificare di cosa si trattasse.

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID	Processo	Memoria	Architettura	Descrizione
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1552	fontdrvhost.exe	1452	In esecuzione	UMFD-1
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1460	fontdrvhost.exe	1460	In esecuzione	UMFD-0
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1552	svchost.exe	1552	In esecuzione	SERVIZIO D...

Erano dei processi di windows nulla di che. Subito dopo ho provato ad eliminare un file nel cestino con PowerShell.



Ho dato il comando `clear-recyclebin` ed ha funzionato.

