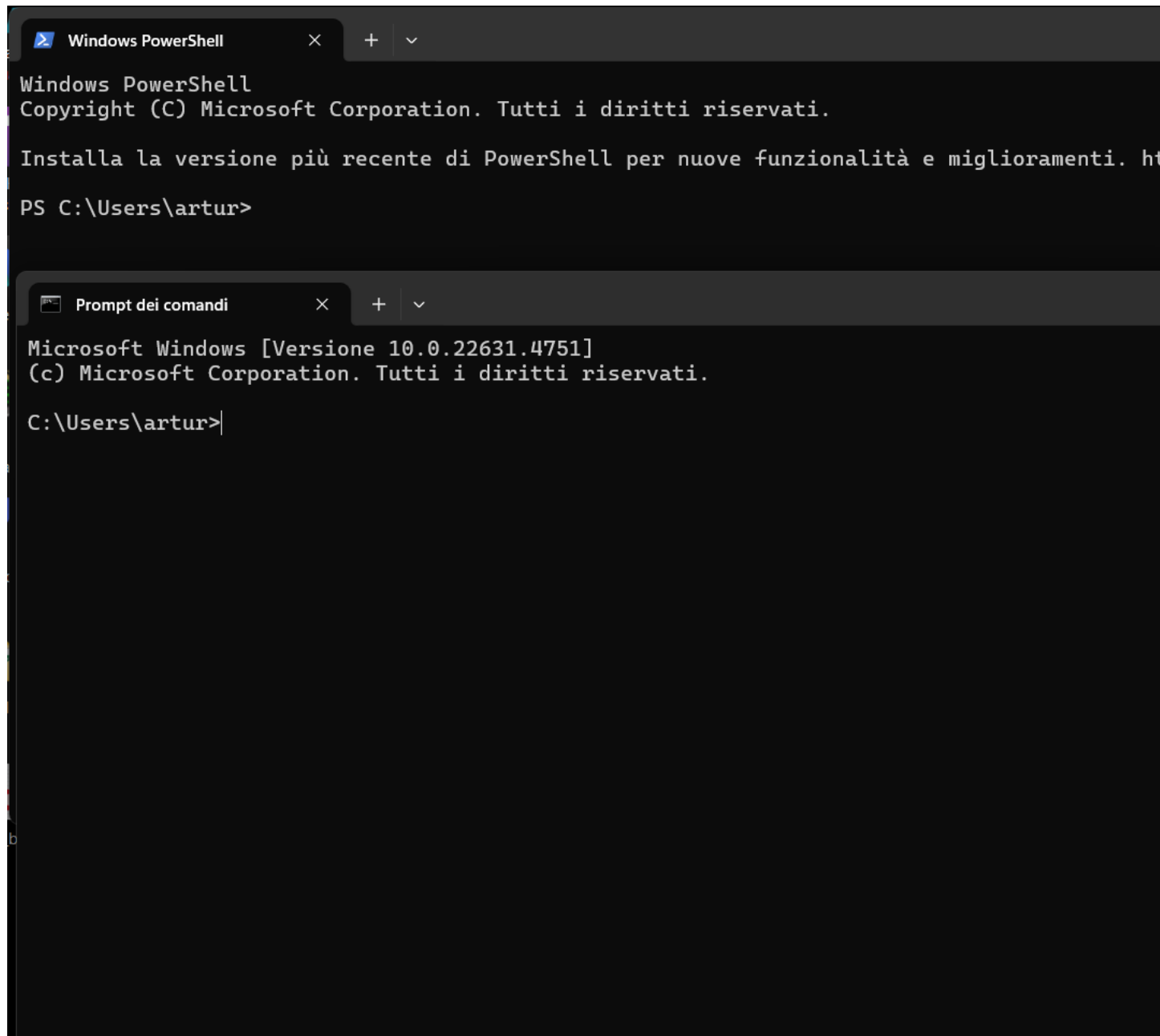


ESERCIZIO S11-L5 (PARTE 1)

1. Accedere alla console Powershell

Per aprire Powershell basta cliccare start e digitare Powershell. Allo stesso modo per aprire il prompt dei comandi basta cliccare start e digitare cmd.



2. Esplorare i comandi del Prompt dei Comandi e di PowerShell

Nel prompt dei comandi ho digitato “dir”

```
Prompt dei comandi
Numero di serie del volume: 7292-305D

Directory di C:\Users\artur

20/01/2025 10:10 <DIR> .
28/11/2023 07:28 <DIR> ..
04/11/2024 18:11      198 .gitconfig
10/12/2023 11:11 <DIR> .km-vm-store
25/11/2024 18:56    176 .packettracer
20/01/2025 10:10 <DIR> .splunk
31/01/2025 09:13 <DIR> .VirtualBox
11/10/2023 18:48 <DIR> 3D Objects
25/11/2024 18:07 <DIR> Cisco Packet Tracer 8.2.2
28/11/2023 07:34 <DIR> Contacts
30/01/2025 15:02 <DIR> Desktop
28/01/2025 10:12 <DIR> Documents
28/01/2025 11:19 <DIR> Downloads
28/11/2023 07:34 <DIR> Favorites
28/11/2023 07:34 <DIR> Links
28/11/2023 07:34 <DIR> Music
12/11/2024 09:18 <DIR> OneDrive
05/11/2024 08:54 <DIR> Pictures
28/11/2023 07:34 <DIR> Saved Games
28/11/2023 07:34 <DIR> Searches
28/11/2023 07:34 <DIR> Videos
31/01/2025 09:12 <DIR> VirtualBox VMs
      2 File      374 byte
     20 Directory 6.405.672.960 byte disponibili

C:\Users\artur>
```

Nella Powershell ho digitato "dir"

```
Windows PowerShell
Install la versione più recente di PowerShell per nuove funzionalità e miglioram
PS C:\Users\artur> dir

Directory: C:\Users\artur

Mode                LastWriteTime         Length Name
----                -
d-----         10/12/2023         11:11         .km-vm-store
d-----         20/01/2025         10:10         .splunk
d-----         31/01/2025         09:13         .VirtualBox
d-r-----        11/10/2023         19:48         3D Objects
d-----         25/11/2024         18:07         Cisco Packet Tracer 8.2.2
d-r-----        28/11/2023         07:34         Contacts
d-r-----        30/01/2025         15:02         Desktop
d-r-----        28/01/2025         10:12         Documents
d-r-----        28/01/2025         11:19         Downloads
d-r-----        28/11/2023         07:34         Favorites
d-r-----        28/11/2023         07:34         Links
d-r-----        28/11/2023         07:34         Music
dar-----        12/11/2024         09:18         OneDrive
d-r-----        05/11/2024         08:54         Pictures
d-r-----        28/11/2023         07:34         Saved Games
d-r-----        28/11/2023         07:34         Searches
d-r-----        28/11/2023         07:34         Videos
d-----         31/01/2025         09:12         VirtualBox VMs
-a-----        04/11/2024         18:11         198 .gitconfig
-a-----        25/11/2024         18:56         176 .packettracer
```

Entrambi i comandi elencano i file e le cartelle presenti nella directory corrente, mostrando dimensioni, date e attributi.

Ho in seguito provato altri comandi comuni come “ipconfig”, “ping” e “cd”. I comandi funzionano in entrambi gli ambienti, ma PowerShell offre più funzionalità avanzate.

```
PS C:\Users\artur> ipconfig
```

Configurazione IP di Windows

Scheda sconosciuta NordLynx:

```
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::723e:7ca:789d:a5aa%46
Indirizzo IPv4. . . . . : 10.5.0.2
Subnet mask . . . . . : 255.255.0.0
Gateway predefinito . . . . . :
```

Scheda Ethernet Ethernet 2:

```
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::ae97:16df:1233:5f8c%13
Indirizzo IPv4. . . . . : 192.168.56.1
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . :
```

Scheda sconosciuta Connessione alla rete locale (LAN):

```
Suffisso DNS specifico per connessione:
Indirizzo IPv4. . . . . : 10.100.0.2
Subnet mask . . . . . : 255.255.0.0
Gateway predefinito . . . . . :
```

Scheda sconosciuta OpenVPN Data Channel Offload for NordVPN:

```
Prompt dei comandi
20 Directory 6.405.672.960 byte disponibili

C:\Users\artur>ipconfig

Configurazione IP di Windows

Scheda sconosciuta NordLynx:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::723e:7ca:789d:a5aa%46
    Indirizzo IPv4. . . . . : 10.5.0.2
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :

Scheda Ethernet Ethernet 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::ae97:16df:1233:5f8c%13
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda sconosciuta Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 10.100.0.2
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :
```

3. Esplorare i cmdlet di PowerShell

Il comando `Get-Alias` dir mi mostrerà che `dir` in PowerShell è un alias per `Get-ChildItem`.

```
Windows PowerShell
Install la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://
PS C:\Users\artur> Get-Alias dir

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

PS C:\Users\artur> Get-ChildItem

Directory: C:\Users\artur

Mode                LastWriteTime         Length Name
----                -
d-----           10/12/2023      11:11             .km-vm-store
d-----           20/01/2025      10:10             .splunk
d-----           31/01/2025       09:13             .VirtualBox
d-r---           11/10/2023      19:48             3D Objects
d-----           25/11/2024      18:07             Cisco Packet Tracer 8.2.2
d-r---           28/11/2023       07:34             Contacts
d-r---           30/01/2025      15:02             Desktop
d-r---           28/01/2025      10:12             Documents
d-r---           28/01/2025      11:19             Downloads
d-r---           28/11/2023       07:34             Favorites
d-r---           28/11/2023       07:34             Links
d-r---           28/11/2023       07:34             Music
dar---           12/11/2024       09:18             OneDrive
d-r---           05/11/2024       08:54             Pictures
d-r---           28/11/2023       07:34             Saved Games
d-r---           28/11/2023       07:34             Searches
d-r---           28/11/2023       07:34             Videos
d-----           31/01/2025       09:12             VirtualBox VMs
-a----           04/11/2024       18:11           198 .gitconfig
-a----           25/11/2024       18:56           176 .packettracer
```

Il comando Get-ChildItem mi mostrerà la stessa lista di file e cartelle di dir, ma con più dettagli.

4. Esplorare il comando netstat con PowerShell

netstat -h mi mostrerà tutte le opzioni disponibili per netstat.

```
PS C:\Users\artur> netstat -h
```

Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

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

-a	Visualizza tutte le connessioni e le porte di ascolto.
-b	Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o porta di ascolto. Alcuni file eseguibili conosciuti includono più componenti indipendenti. In tali casi viene visualizzata la sequenza dei componenti utilizzati per la creazione della connessione o porta di ascolto e il nome del file eseguibile viene visualizzato in fondo, tra parentesi quadre ([]). Nella par e così via, fino al raggiungimento di TCP/IP. Se si utilizza questa opzione, l'esecuzione del comando può richiedere molto tempo e riuscirà solo se si dispone di autor sufficienti.
-e	Visualizza le statistiche Ethernet. Può essere utilizzata insieme all'opzione -s.
-f	Visualizza i nomi di dominio completi (FQDN, Fully Qualified Domain Name) per gli indirizzi esterni.
-i	Visualizza il tempo trascorso da una connessione TCP nel suo stato corrente.
-n	Visualizza indirizzi e numeri di porta in forma numerica.
-o	Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto	Visualizza le connessioni relative al protocollo specificato da "proto", che può essere TCP, UDP, TCPv6 o UDPv6. Se utilizzato insieme all'opzione -s per le statistiche per protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q	Visualizza tutte le connessioni, le porte di ascolto e le porte TCP non di ascolto associate. Le porte non di ascolto associate possono essere a una connessione attiva.
-r	Visualizza la tabella di routing.
-s	Visualizza le statistiche per protocollo. Per impostazione predefinita, vengono visualizzate le statistiche per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare un sottoinsieme dei valori predefiniti, è possibile utilizzare l'opzione -t
-t	Visualizza lo stato di offload della connessione corrente.

Netstat -r mi mostrerà tutte le rotte attive sul computer.

```
Windows PowerShell
verranno visualizzate una volta sola.

PS C:\Users\artur> netstat -r

=====
Elenco interfacce
46.....NordLynx Tunnel
13...0a 00 27 00 00 0d .....VirtualBox Host-Only Ethernet Adapter
18...00 ff b8 32 8a 43 .....TAP-NordVPN Windows Adapter V9
10.....OpenVPN Data Channel Offload
21...22 4e f6 a2 cf 35 .....Microsoft Wi-Fi Direct Virtual Adapter
11...a2 4e f6 a2 cf 35 .....Microsoft Wi-Fi Direct Virtual Adapter #2
20...20 4e f6 a2 cf 35 .....Realtek RTL8821CE 802.11ac PCIe Adapter
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  192.168.1.17  35
    0.0.0.0             128.0.0.0  10.100.0.1   10.100.0.2    25
    10.5.0.0            255.255.0.0  On-link     10.5.0.2      261
    10.5.0.2           255.255.255.255  On-link     10.5.0.2      261
    10.5.255.255       255.255.255.255  On-link     10.5.0.2      261
    10.100.0.0          255.255.0.0    On-link     10.100.0.2    281
    10.100.0.2          255.255.255.255  On-link     10.100.0.2    281
    10.100.255.255      255.255.255.255  On-link     10.100.0.2    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
    128.0.0.0           128.0.0.0     10.100.0.1   10.100.0.2    25
    152.89.206.13       255.255.255.255  192.168.1.1  192.168.1.17  35
    192.168.1.0         255.255.255.0  On-link     192.168.1.17  291
    192.168.1.17        255.255.255.255  On-link     192.168.1.17  291
    192.168.1.255       255.255.255.255  On-link     192.168.1.17  291
    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     10.100.0.2    281
```

Per eseguire PowerShell con privilegi elevati, ho cliccato su Start, cercato PowerShell, clic destro e selezionato esegui come amministratore.

Una volta ottenuti i privilegi da amministratore ho digitato il comando netstat -abno.


```
Seleziona 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  1336
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  3776
CDPSvc
[svchost.exe]
TCP    0.0.0.0:49664            0.0.0.0:0            LISTENING  1064
[lsass.exe]
TCP    0.0.0.0:49665            0.0.0.0:0            LISTENING  980
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666            0.0.0.0:0            LISTENING  1880
EventLog
[svchost.exe]
TCP    0.0.0.0:49667            0.0.0.0:0            LISTENING  2276
Schedule
[svchost.exe]
TCP    0.0.0.0:49668            0.0.0.0:0            LISTENING  4168
[spoolsv.exe]
```

Mi mostrerà tutte le connessioni attive, i programmi che le utilizzano e i relativi Process ID (PID).

Per verificare i PID in Task Manager, ho aperto Task Manager, sono andato alla scheda dettagli, ho ordinato i processi in base al PID e trovato un PID che compare nei risultati di netstat -abno.

5. Svuotare il Cestino con PowerShell

```
PS C:\Users\artur> clear-recyclebin

Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino"
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è Sì)
PS C:\Users\artur> |
```