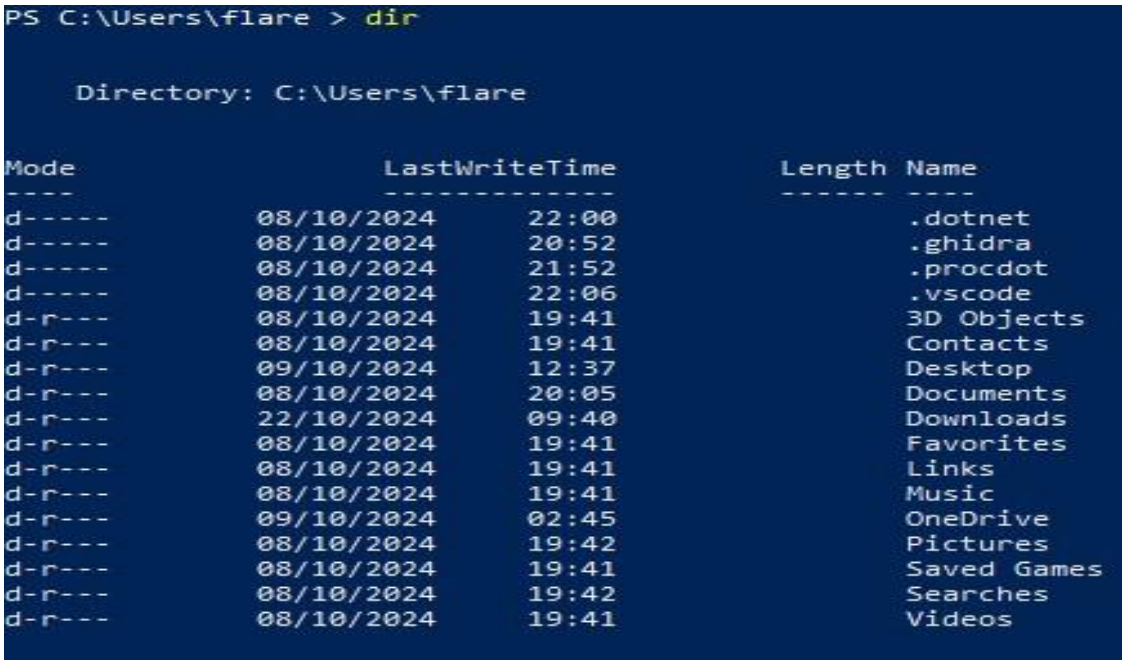
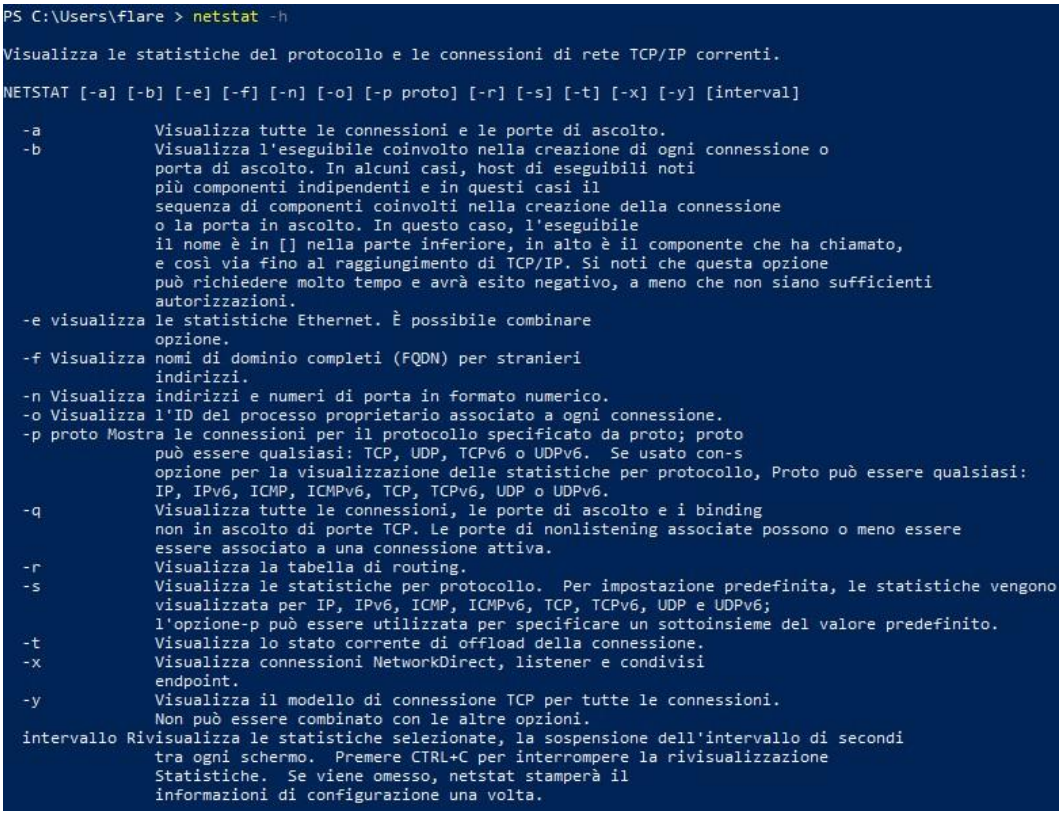
# Relazione Windows Powershell

Nella seguente immagine utilizzo il comando dir sul terminale, di **Powershell** con il quale visualizzo le **sottodirectory e file**, come illustrato di seguito:




Nella seguente immagine utilizzo il comando **Get-Alias** con il quale visualizzo **ChildItem**, come illustrato nell'esempio di seguito:

Dopo aver utilizzato i comandi sopra illustrati e descritti, utilizzo il comando **netstat -h**, con il quale visualizzo le statistiche del protocollo e le connessioni di rete, ad esempio **TCP/IP**, e **netstat -r** per visualizzare la tabella di routing attive, come illustrato di seguito:

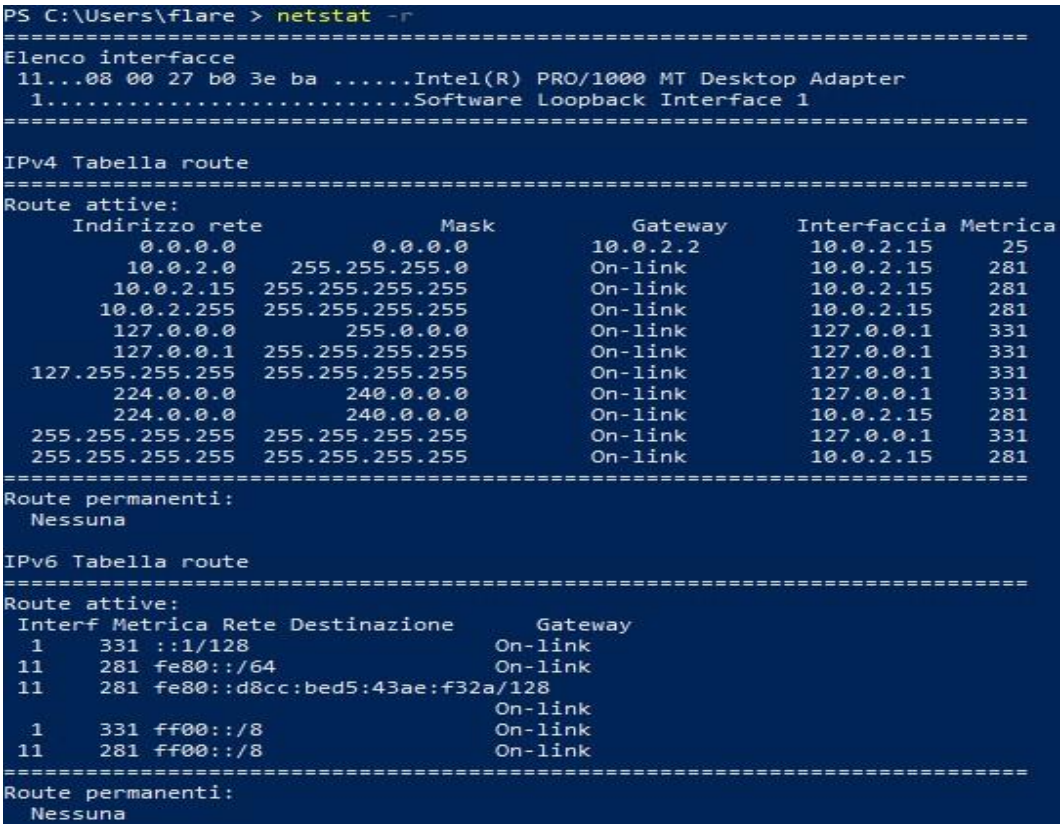


```
PS C:\Users\flare > netstat -h

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

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

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -b            Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
                porta di ascolto. In alcuni casi, host di eseguibili noti
                più componenti indipendenti e in questi casi il
                sequenza di componenti coinvolti nella creazione della connessione
                o la porta in ascolto. In questo caso, l'eseguibile
                il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
                e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
                può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
                autorizzazioni.
  -e visualizza le statistiche Ethernet. È possibile combinare
                opzione.
  -f Visualizza nomi di dominio completi (FQDN) per stranieri
                indirizzi.
  -n Visualizza indirizzi e numeri di porta in formato numerico.
  -o Visualizza l'ID del processo proprietario associato a ogni connessione.
  -p proto Mostra le connessioni per il protocollo specificato da proto; proto
                può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6.  Se usato con-s
                opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  -q            Visualizza tutte le connessioni, le porte di ascolto e i binding
                non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
                essere associato a una connessione attiva.
  -r            Visualizza la tabella di routing.
  -s            Visualizza le statistiche per protocollo.  Per impostazione predefinita, le statistiche vengono
                visualizzata per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
                l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
  -t            Visualizza lo stato corrente di offload della connessione.
  -x            Visualizza connessioni NetworkDirect, listener e condivisi
                endpoint.
  -y            Visualizza il modello di connessione TCP per tutte le connessioni.
                Non può essere combinato con le altre opzioni.
  intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
                tra ogni schermo.  Premere CTRL+C per interrompere la rivisualizzazione
                Statistiche.  Se viene omesso, netstat stamperà il
                informazioni di configurazione una volta.
```



```
PS C:\Users\flare > netstat -r
===========================================================================
Elenco interfacce
 11...08 00 27 b0 3e ba ......Intel(R) PRO/1000 MT Desktop 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         10.0.2.2        10.0.2.15     25
         10.0.2.0    255.255.255.0         On-link         10.0.2.15    281
        10.0.2.15  255.255.255.255         On-link         10.0.2.15    281
       10.0.2.255  255.255.255.255         On-link         10.0.2.15    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
        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         10.0.2.15    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         10.0.2.15    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  1    331 ::1/128                  On-link
 11    281 fe80::/64                On-link
 11    281 fe80::d8cc:bed5:43ae:f32a/128
                                    On-link
  1    331 ff00::/8                 On-link
 11    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
```

Nel prossimo passaggio utilizzo il comando netstat -abno per visualizzare i processi delle connessioni TCP attive:

- **netstat -abno**

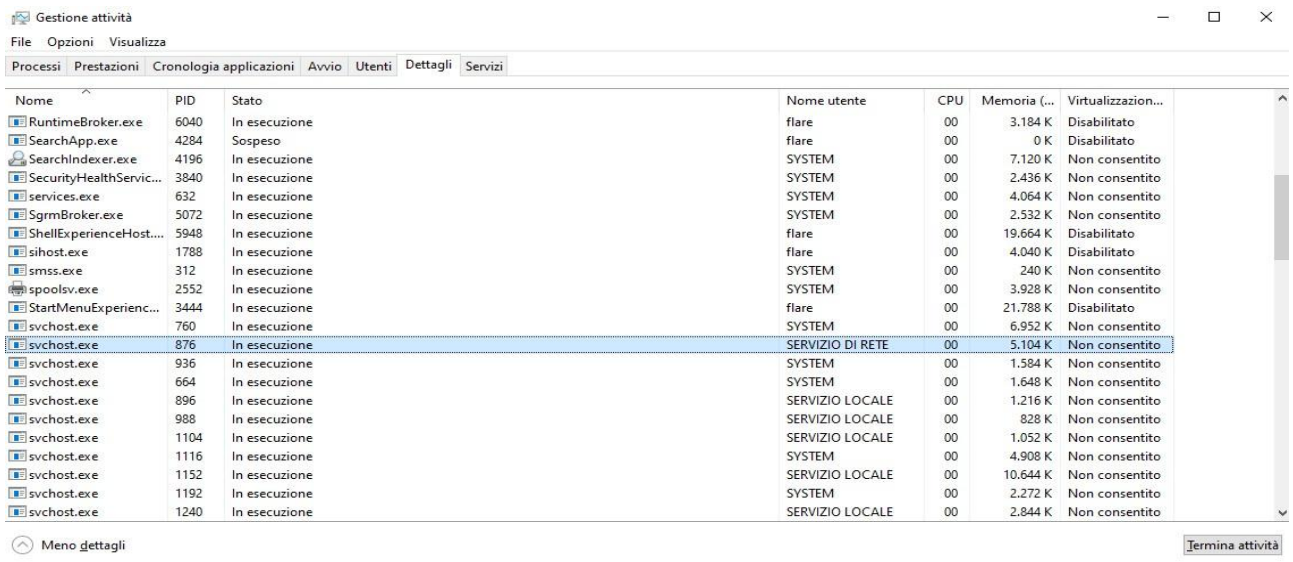
```
PS C:\Windows\system32 > netstat -abno

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:135             0.0.0.0:0              LISTENING       876
  RpcEptMapper
 [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       4952
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:7680            0.0.0.0:0              LISTENING       2200
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49664           0.0.0.0:0              LISTENING       652
 [lsass.exe]
  TCP    0.0.0.0:49665           0.0.0.0:0              LISTENING       488
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49666           0.0.0.0:0              LISTENING       1152
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667           0.0.0.0:0              LISTENING       1116
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668           0.0.0.0:0              LISTENING       2552
 [spoolsv.exe]
  TCP    0.0.0.0:49669           0.0.0.0:0              LISTENING       632
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49670           0.0.0.0:0              LISTENING       2756
  PolicyAgent
 [svchost.exe]
  TCP    10.0.2.15:139           0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:49737         20.54.37.64:443        ESTABLISHED     2440
  WpnService
 [svchost.exe]
  TCP    [::]:135                [::]:0                 LISTENING       876
  RpcEptMapper
 [svchost.exe]
  TCP    [::]:445                [::]:0                 LISTENING       4
```

Dopo aver visualizzato i processi di rete con il comando specifico, netstat -abno, vado sul **Task Manager** per visualizzare il PID specifico del Network Service:

- il **PID** selezionato ed evidenziato nella ricerca con il comando sopra descritto, è: **876**



Nell’ultimo passaggio utilizzo il comando specifico per pulire il cestino, come illustrato di seguito:

- **clear-recyclebin**