

ESERCIZIO SETTIMANALE S11L5

LABORATORIO – UTILIZZO DI WINDOWS POWERSHELL

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell:

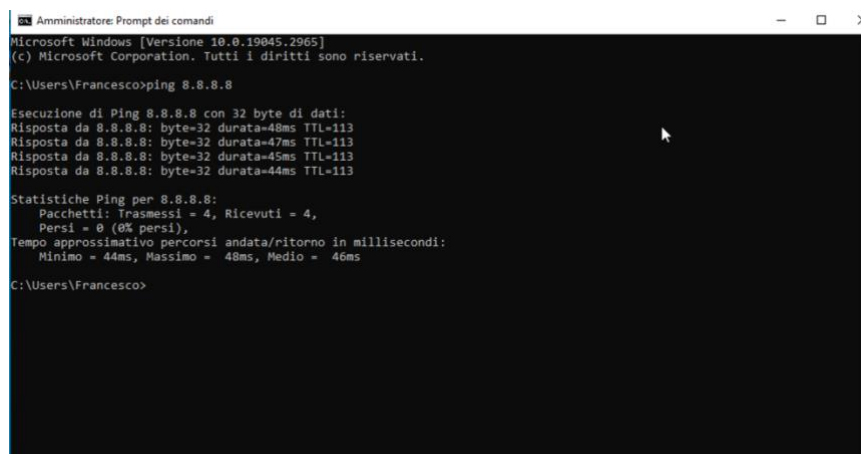
<https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html>

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- **Parte 1: Accedi alla console PowerShell.**
- **Parte 2: Esplora i comandi del prompt dei comandi e PowerShell.**
- **Parte 3: Esplora i cmdlet.**
- **Parte 4: Esplora il comando netstat usando PowerShell.**
- **Parte 5: Vuota il cestino utilizzando PowerShell.**

SVOLGIMENTO:

Nella prima parte di questo esercizio ci assicuriamo di avere la connessione ad internet, avviamo la VM Windows ed accediamo alla console PowerShell:



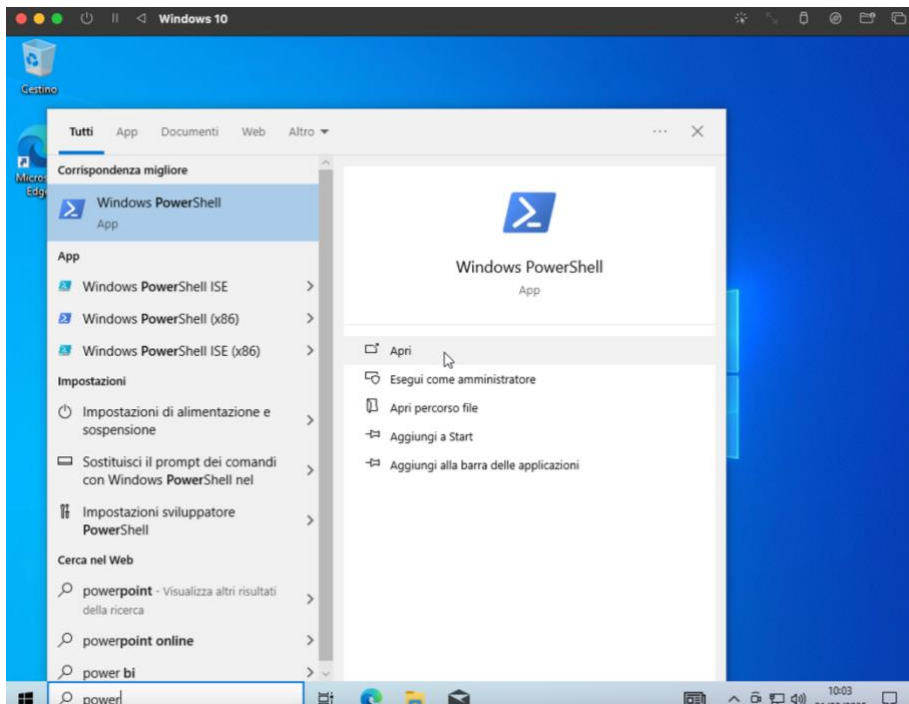
```
Amministratore: Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.2965]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Francesco>ping 8.8.8.8

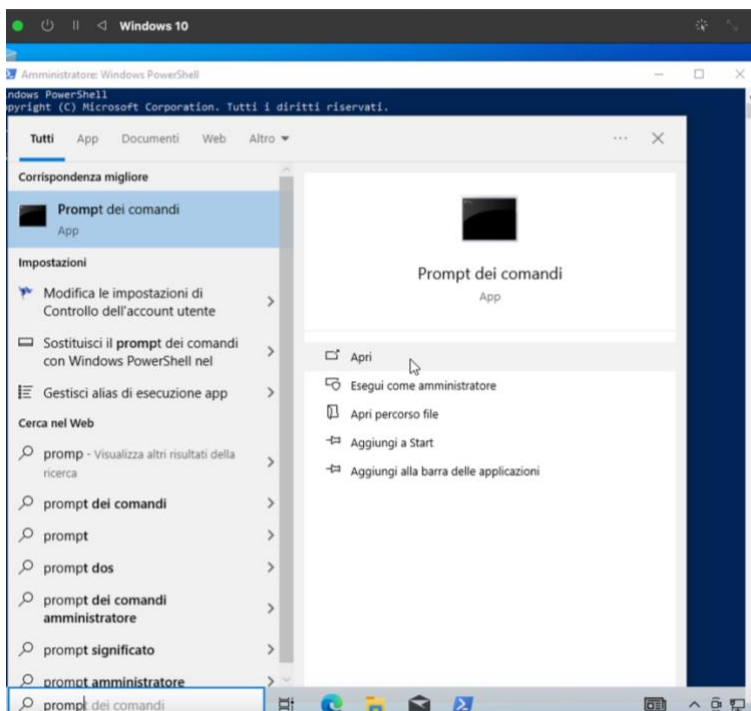
Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=48ms TTL=113
Risposta da 8.8.8.8: byte=32 durata=47ms TTL=113
Risposta da 8.8.8.8: byte=32 durata=45ms TTL=113
Risposta da 8.8.8.8: byte=32 durata=44ms TTL=113

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 44ms, Massimo = 48ms, Medio = 46ms

C:\Users\Francesco>
```



Avviamo anche il prompt dei comandi:



PARTE 2:

Nella seconda parte, utilizzeremo il comando “dir” in entrambe le finestre (powershell e prompt dei comandi) e ne visualizzeremo l’output, avremo modo di vedere che i due output ricevuti saranno molto simili:

```

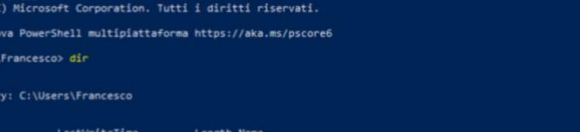
C:\Users\Francesco>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 6460-A030

Directory di C:\Users\Francesco

21/02/2025 10:00 <DIR>      .
21/02/2025 10:00 <DIR>      ..
26/11/2024 18:28 <DIR>      30 Objects
26/11/2024 18:28 <DIR>      Contacts
26/11/2024 18:28 <DIR>      Desktop
26/11/2024 18:28 <DIR>      Documents
26/11/2024 18:28 <DIR>      Downloads
26/11/2024 18:28 <DIR>      Favorites
26/11/2024 18:28 <DIR>      Links
26/11/2024 18:28 <DIR>      Music
26/11/2024 18:30 <DIR>      OneDrive
26/11/2024 18:30 <DIR>      Pictures
26/11/2024 18:28 <DIR>      Saved Games
26/11/2024 18:30 <DIR>      Searches
26/11/2024 18:28 <DIR>      Videos
               0 File             0 byte
               15 Directory    54.097.575.936 byte disponibili

C:\Users\Francesco>

```



Administrator: Windows PowerShell

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

Prova la nuova PowerShell multiplatforma <https://aka.ms/pscore6>

PS C:\Users\Francesco> dir

Directory: C:\Users\Francesco

Mode	LastWriteTime	Length	Name
d-r--	26/11/2024 18:28	30	Objects
d-r--	26/11/2024 18:28		Contacts
d-r--	26/11/2024 18:28		Desktop
d-r--	26/11/2024 18:28		Documents
d-r--	26/11/2024 18:28		Downloads
d-r--	26/11/2024 18:28		Favorites
d-r--	26/11/2024 18:28		Links
d-r--	26/11/2024 18:28		Music
d-r--	26/11/2024 18:30		OneDrive
d-r--	26/11/2024 18:30		Pictures
d-r--	26/11/2024 18:28		Saved Games
d-r--	26/11/2024 18:30		Searches
d-r--	26/11/2024 18:28		Videos

PS C:\Users\Francesco>

Adesso proviamo anche con altri comandi, ad esempio ipconfig:

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

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 . . . . . : fdaf:47cb:dad2:37df:44b9:1883:4c3c:b04a
    Indirizzo IPv6 temporaneo. . . . . : fdaf:47cb:dad2:37df:49:7e55:4a08:e495
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::ecda:b1a:aa61:233a%3
    Indirizzo IPv4. . . . . : 192.168.64.6
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.64.1
PS C:\Users\Francesco>

C:\Users\Francesco>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 . . . . . : fdaf:47cb:dad2:37df:44b9:1883:4c3c:b04a
    Indirizzo IPv6 temporaneo. . . . . : fdaf:47cb:dad2:37df:49:7e55:4a08:e495
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::ecda:b1a:aa61:233a%3
    Indirizzo IPv4. . . . . : 192.168.64.6
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.64.1
C:\Users\Francesco>_
```

Vediamo come ancora una volta gli output sono molto simili.

PARTE 3:

Nella terza parte andremo ad esplorare i cmdlet, l'obiettivo è quello di identificare il comando PowerShell per elencare le sottodirectory e i file in una directory. Per farlo, inseriamo **Get-Alias dir** nel prompt di PowerShell:

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

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

PS C:\Users\Francesco> Get-ChildItem

Directory: C:\Users\Francesco

Mode                LastWriteTime         Length Name
----                -
d-r---           26/11/2024      18:28           3D Objects
d-r---           26/11/2024      18:28           Contacts
d-r---           26/11/2024      18:28           Desktop
d-r---           26/11/2024      18:28           Documents
d-r---           26/11/2024      18:28           Downloads
d-r---           26/11/2024      18:28           Favorites
d-r---           26/11/2024      18:28           Links
d-r---           26/11/2024      18:28           Music
d-r---           26/11/2024      18:30           OneDrive
d-r---           26/11/2024      18:30           Pictures
d-r---           26/11/2024      18:28           Saved Games
d-r---           26/11/2024      18:30           Searches
d-r---           26/11/2024      18:28           Videos
```

Possiamo vedere come powershell risponde al comando indicandoci di utilizzare “Get-ChildItem” per visualizzare le sottodirectory, lo eseguiamo e visualizziamo effettivamente le sottodirectory presenti.

PARTE 4:

Nella parte quattro andremo ad esplorare il comando Netstat su powershell. Aprendo powershell e digitando il comando “netstat -h”, possiamo visualizzare le opzioni disponibili per il comando netstat:

```
PS C:\Users\Francesco> 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 la
  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
  visualizzate 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.
```

Una volta visualizzate le varie opzioni, utilizziamo il comando “netstat -r” per visualizzare le tabelle di routing:

```

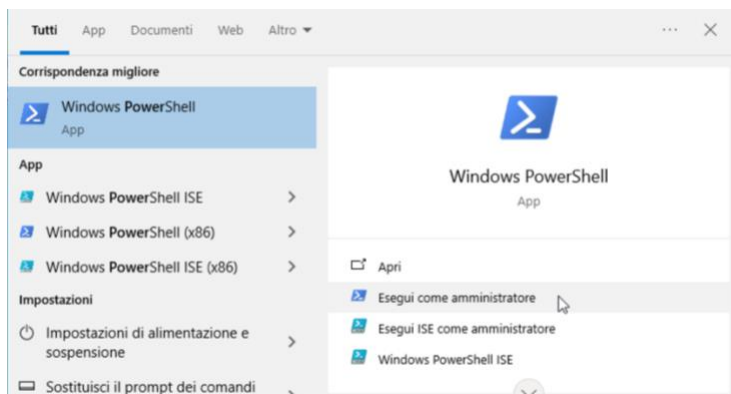
PS C:\Users\Francesco> netstat -r
=====
Elenco Interfacce
3...32 7f e1 3e df 5d .....Intel(R) PRO/1000 MT Network Connection
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia  Metrica
-----
  0.0.0.0             0.0.0.0    192.168.64.1  192.168.64.6  25
  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
  192.168.64.0        255.255.255.0  On-link      192.168.64.6  281
  192.168.64.6        255.255.255.255  On-link      192.168.64.6  281
  192.168.64.255     255.255.255.255  On-link      192.168.64.6  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      192.168.64.6  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      192.168.64.6  281
=====
Route permanenti:
  Nessuna
=====

IPv6 Tabella route
=====
Route attive:
  Interf. Metrica Rete Destinazione Gateway
-----
  1 331 ::1/128 On-link
  3 281 fdaf:47cb:dad2:37df::/64 On-link
  3 281 fdaf:47cb:dad2:37df:49:7e55:4a08:e495/128 On-link
  3 281 fdaf:47cb:dad2:37df:44b9:1883:4c3c:b04a/128 On-link
  3 281 fe80::/64 On-link
  3 281 fe80::ecda:b1a:aa61:233a/128 On-link
  1 331 ff00::/8 On-link
  3 281 ff00::/8 On-link
=====
Route permanenti:
  Nessuna
=====
PS C:\Users\Francesco>

```

Proseguiamo con l'esercizio aprendo un'altra finestra PowerShell ma questa volta con i privilegi di amministratore:



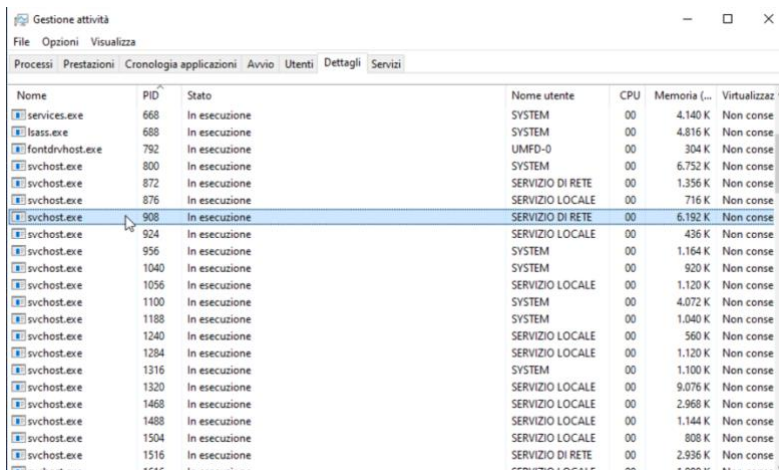
Una volta dentro, utilizziamo il comando “netstat -abno” per visualizzare i processi associati alle connessioni TCP attive.

```

PS C:\Users\Francesco> netstat -abno
=====
Connessioni attive
Proto  Indirizzo locale      Indirizzo esterno      Stato      PID
-----
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING  908
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  5424
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING  4380
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING  688
lsass.exe
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING  532
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING  1100
Schedule
[svchost.exe]
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING  1320
EventLog
[svchost.exe]
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING  2204
spoolsv.exe
TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING  668
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:9843         0.0.0.0:0              LISTENING  2896
[snice-usbdevd.exe]
=====
iphlpsvc
[svchost.exe]
UDP    192.168.64.6:137      *: *                    4
Impossibile ottenere informazioni sulla proprietà
UDP    192.168.64.6:138      *: *                    4
Impossibile ottenere informazioni sulla proprietà
UDP    192.168.64.6:1900     *: *                    4060
SSDPSRV
[svchost.exe]
UDP    192.168.64.6:52002    *: *                    4060
SSDPSRV
[svchost.exe]
UDP    [:]:5353              *: *                    872
Dnscache
[svchost.exe]
UDP    [:]:5355              *: *                    872
Dnscache
[svchost.exe]
UDP    [:]:1900              *: *                    4060
SSDPSRV
[svchost.exe]
UDP    [:]:52001             *: *                    4060
SSDPSRV
[svchost.exe]
UDP    [fe80::ecda:b1a:aa61:233a%3]:1900 *: *                    4060
SSDPSRV
[svchost.exe]
UDP    [fe80::ecda:b1a:aa61:233a%3]:52000 *: *                    4060
SSDPSRV
[svchost.exe]
PS C:\Users\Francesco>

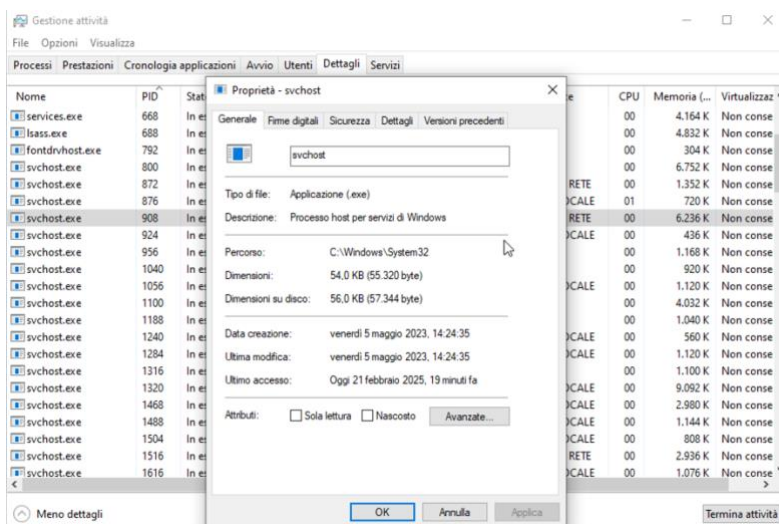
```


Apriamo Task Manager. Andiamo alla scheda dettagli, Facciamo clic sull'intestazione **PID** in modo che i PID siano in ordine. Selezioniamo uno dei PID dai risultati di “netstat -abno”.



Nome	PID	Stato	Nome utente	CPU	Memoria (...	Virtualizzaz...
services.exe	668	In esecuzione	SYSTEM	00	4.140 K	Non conse
lsass.exe	688	In esecuzione	SYSTEM	00	4.816 K	Non conse
fontdrvhost.exe	792	In esecuzione	UMFD-0	00	304 K	Non conse
svchost.exe	800	In esecuzione	SYSTEM	00	6.752 K	Non conse
svchost.exe	872	In esecuzione	SERVIZIO DI RETE	00	1.356 K	Non conse
svchost.exe	876	In esecuzione	SERVIZIO LOCALE	00	716 K	Non conse
svchost.exe	908	In esecuzione	SERVIZIO DI RETE	00	6.192 K	Non conse
svchost.exe	924	In esecuzione	SERVIZIO LOCALE	00	436 K	Non conse
svchost.exe	956	In esecuzione	SYSTEM	00	1.164 K	Non conse
svchost.exe	1040	In esecuzione	SYSTEM	00	920 K	Non conse
svchost.exe	1056	In esecuzione	SERVIZIO LOCALE	00	1.120 K	Non conse
svchost.exe	1100	In esecuzione	SYSTEM	00	4.072 K	Non conse
svchost.exe	1188	In esecuzione	SYSTEM	00	1.040 K	Non conse
svchost.exe	1240	In esecuzione	SERVIZIO LOCALE	00	560 K	Non conse
svchost.exe	1284	In esecuzione	SERVIZIO LOCALE	00	1.120 K	Non conse
svchost.exe	1316	In esecuzione	SYSTEM	00	1.100 K	Non conse
svchost.exe	1320	In esecuzione	SERVIZIO LOCALE	00	9.076 K	Non conse
svchost.exe	1468	In esecuzione	SERVIZIO LOCALE	00	2.968 K	Non conse
svchost.exe	1488	In esecuzione	SERVIZIO LOCALE	00	1.144 K	Non conse
svchost.exe	1504	In esecuzione	SERVIZIO LOCALE	00	808 K	Non conse
svchost.exe	1516	In esecuzione	SERVIZIO DI RETE	00	2.936 K	Non conse
svchost.exe	1616	In esecuzione	SERVIZIO LOCALE	00	1.088 K	Non conse

Nel nostro caso, ho utilizzato PID 908 per questo esempio. Individuiamo il PID selezionato nel Task Manager. Facciamo clic con il pulsante destro del mouse sul PID selezionato nel Task Manager per aprire la finestra di dialogo **Proprietà** per ulteriori informazioni.

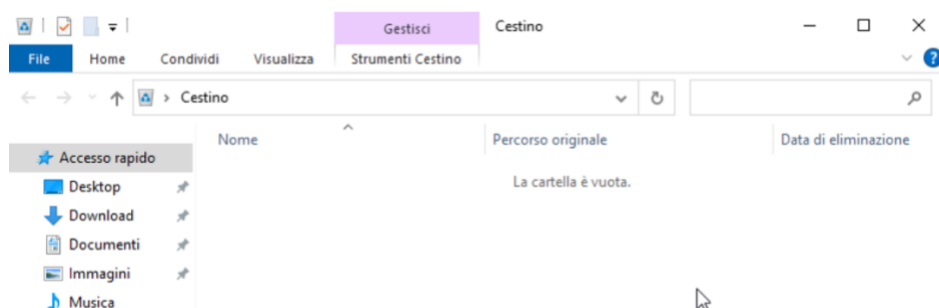
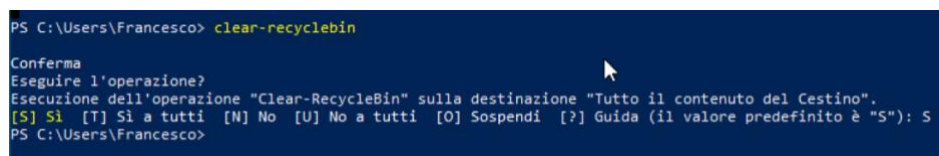
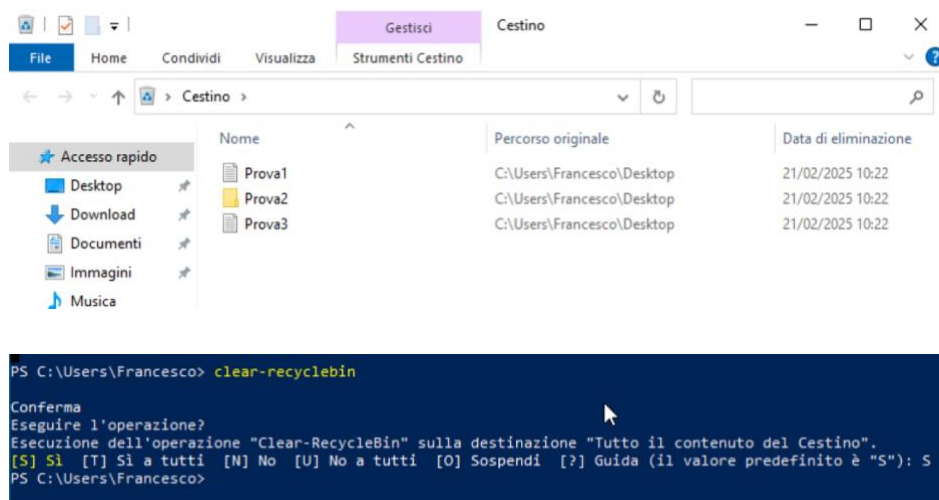


Possiamo quindi vedere che: PID 908 è associato al processo svchost.exe. L'utente per questo processo è NetworkService e sta utilizzando 56.0KB di memoria.

PARTE 5:

Nella parte finale di questo esercizio vedremo come svuotare il cestino utilizzando PowerShell, ci assicuriamo quindi di avere dei file/cartelle o altro all'interno del cestino.

Dopodiché richiamiamo su PowerShell ed utilizziamo il comando "clear-recyclebin" per eliminare gli elementi presenti all'interno del cestino, definitivamente.



Come possiamo vedere, il cestino è stato svuotato.

PARTE 6: PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Utilizzando Internet, cerca i comandi che potresti usare per semplificare le tue attività come analista di sicurezza. Registra le tue scoperte.

PowerShell è uno strumento potente per gli analisti di sicurezza, consentendo l'automazione di attività e la gestione della configurazione.

Ecco alcuni comandi utili che ho trovato cercando su internet, per semplificare le operazioni quotidiane:

- **Get-ExecutionPolicy:** Verifica la politica di esecuzione corrente degli script PowerShell.
- **Set-ExecutionPolicy:** Modifica la politica di esecuzione per consentire o limitare l'esecuzione di script.
- **Get-Service:** Elenca tutti i servizi attivi sul sistema, utile per identificare servizi sospetti.
- **Get-Process:** Mostra i processi in esecuzione, aiutando a individuare attività anomale.
- **Stop-Process:** Termina un processo specificato, utile per fermare attività indesiderate.
- **Get-EventLog:** Recupera i log degli eventi di sistema, essenziale per l'analisi forense.
- **Get-ADUser:** Ottiene informazioni sugli utenti di Active Directory, utile per audit e gestione degli accessi.
- **Resolve-DnsName:** Esegue ricerche DNS per diagnosticare problemi di rete o attività sospette.
- **Get-Acl:** Ottiene i controlli di accesso (ACL) di file o risorse, utile per verificare le autorizzazioni.
- **Set-Acl:** Modifica le ACL di file o risorse, consentendo la gestione delle autorizzazioni.
- **Get-Credential:** Crea un oggetto credenziale per operazioni che richiedono autenticazione.
- **New-FileCatalog:** Crea un catalogo di hash dei file per convalidare l'autenticità dei file.
- **Get-Command:** Elenca tutti i comandi disponibili in PowerShell, utile per scoprire nuove funzionalità.