



S 13 / L 1

WINDOWS SYSINTERNALS SUITE

# CONTENUTI

00

Traccia

01

Exploring processes, threads, handles, and windows Registry

02

Windows Powershell

03

Windows Task Manager

# 00 TRACCIA

## **1) Exploring Processes, Threads, Handles, and Windows Registry**

In this lab, you will complete the following objectives:

- Explore the processes, threads, and handles using Process Explorer in Sysinternals Suite.
- Use the Windows Registry to change a setting.

## **2) Using Windows PowerShell**

In this lab, you will explore some of the functions of PowerShell.

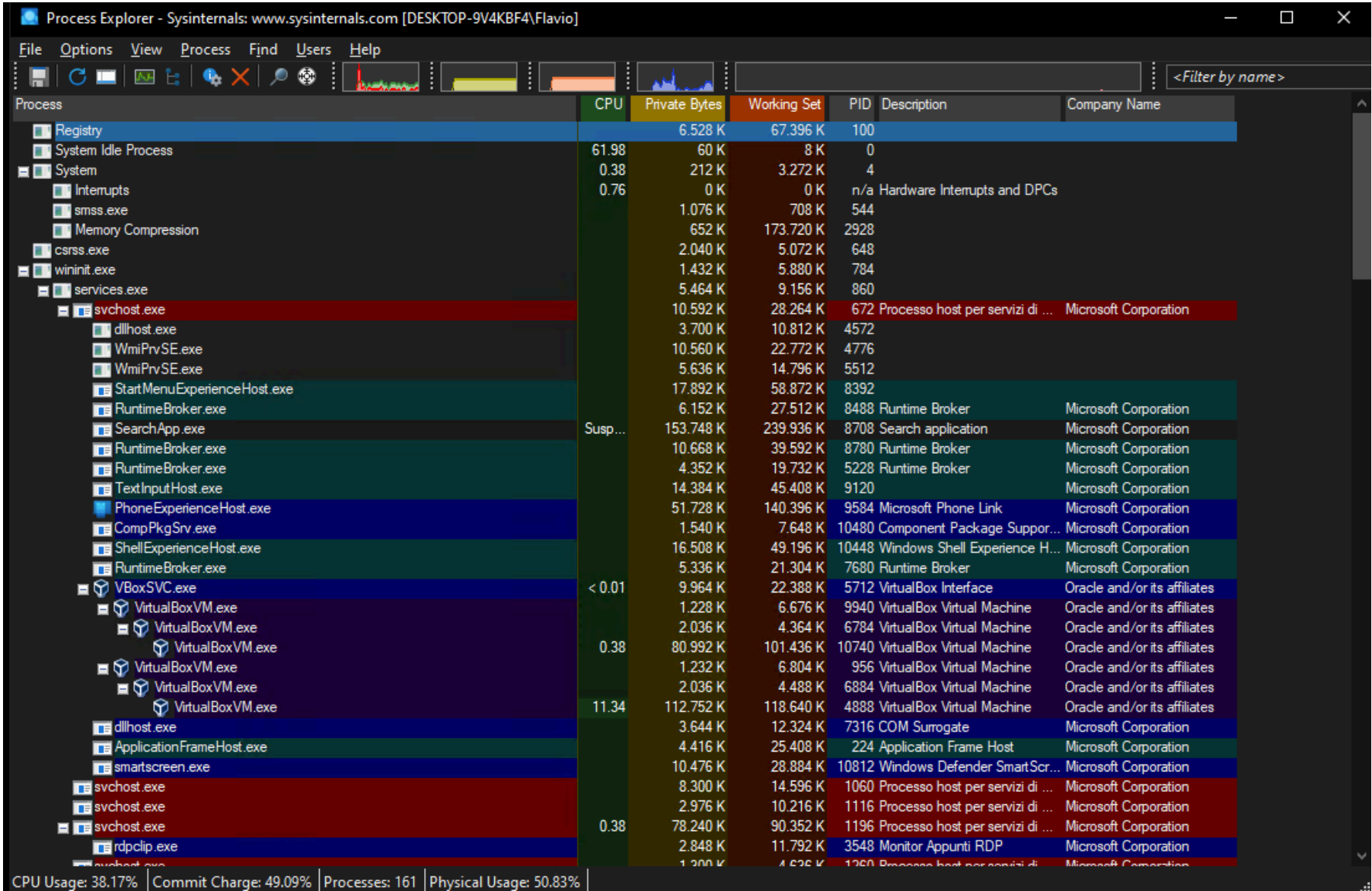
## **3) Windows Task Manager**

In this lab, you will explore Task Manager and manage processes from within Task Manager.

# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

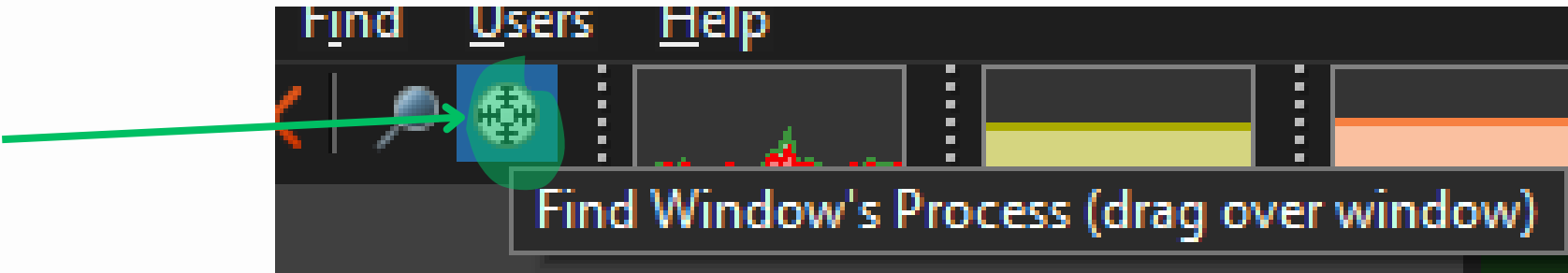
L'esercizio guidato di oggi prevede l'utilizzo di alcune funzioni basilari contenute in **Process Explorer**, uno strumento che fa parte del set Sysinternals, utilizzato per l'amministrazione su Windows.

Abbiamo già avuto modo di conoscerlo nelle settimane precedenti, in particolare durante l'**analisi di malware**.



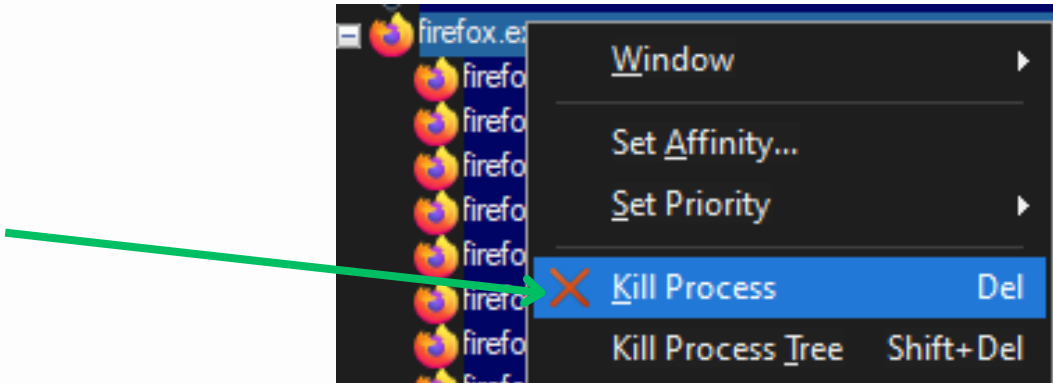
# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

Grazie al pulsante **'Find Window's Process'**, è possibile effettuare un drag and drop, trascinando il pulsante su una finestra aperta nel sistema. Questo mostrerà la corrispondenza esatta del processo all'interno di Process Explorer. Nel mio caso ho puntato al browser **Firefox**.

A screenshot of the Process Explorer window. The 'Processes' list shows several instances of 'firefox.exe'. The first instance is selected and highlighted in blue. The other instances are listed below it. The columns show the process name, CPU usage, private bytes, working set, PID, process name, and company name. The company name for all listed processes is 'Mozilla Corporation'.

firefox.exe	< 0.01	193.208 K	253.884 K	2596	Firefox	Mozilla Corporation
firefox.exe		363.164 K	104.056 K	10532	Firefox	Mozilla Corporation
firefox.exe		21.992 K	15.372 K	4044	Firefox	Mozilla Corporation
firefox.exe		52.408 K	72.000 K	8088	Firefox	Mozilla Corporation
firefox.exe		105.996 K	89.164 K	8900	Firefox	Mozilla Corporation
firefox.exe		27.252 K	12.768 K	1428	Firefox	Mozilla Corporation

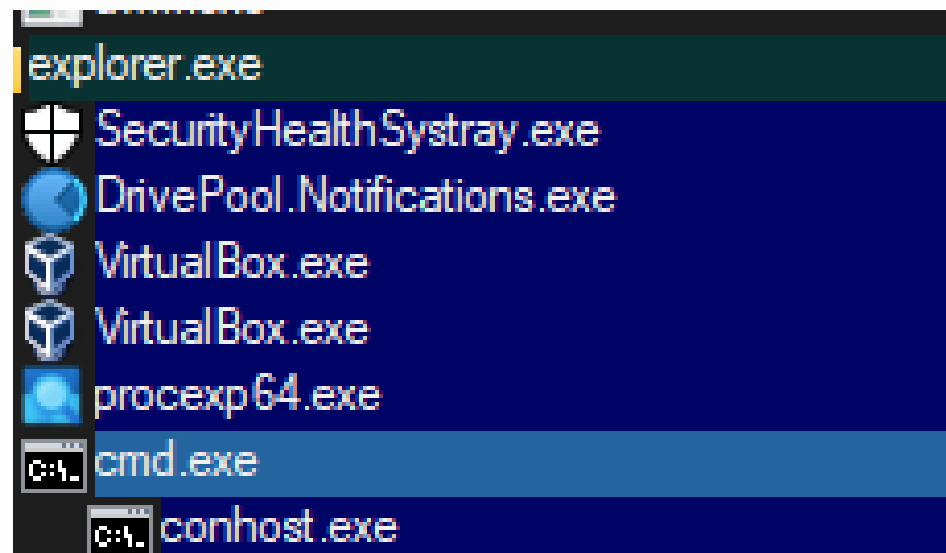
Da qui e ho cliccato con il tasto destro del mouse, aprendo il menu contestuale. Ho scelto di terminare il processo selezionando **"Kill Process"**, che **chiude immediatamente Firefox**.



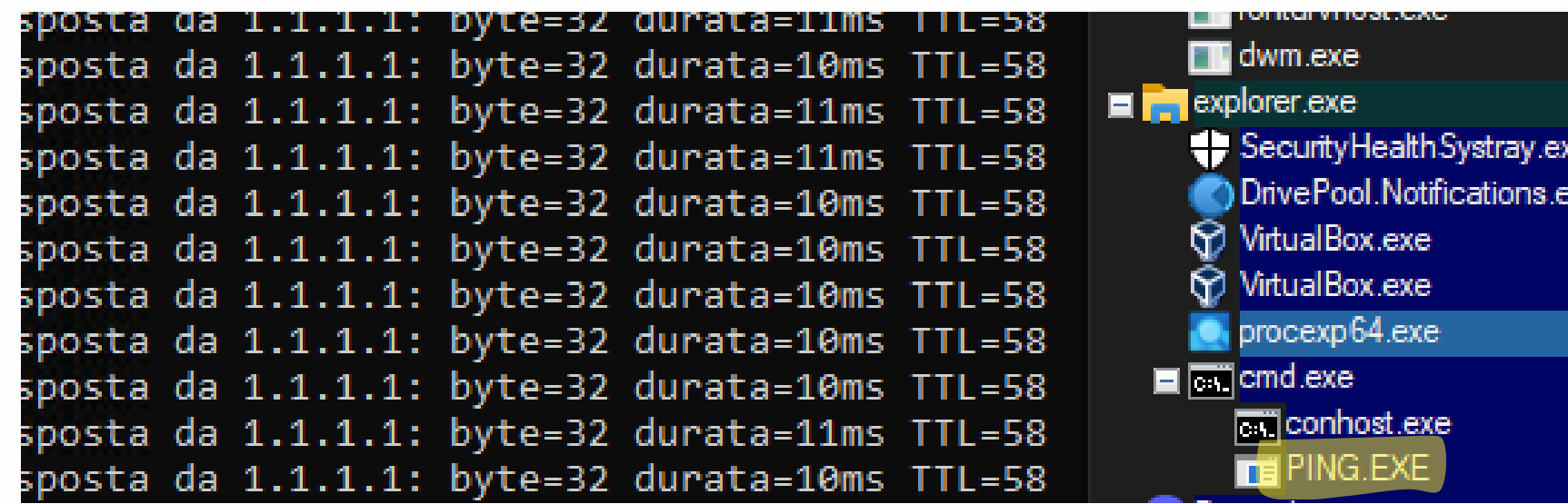
# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

In quest'altro esempio invece ho aperto un **Prompt dei comandi** cercandolo nel menu Start. Successivamente, ho trascinato l'icona "Find Window's Process" nella finestra del Prompt dei comandi per individuare il processo corrispondente, che è "**cmd.exe**". Ho notato che il processo padre è "explorer.exe" e che "cmd.exe" ha un processo figlio chiamato "conhost.exe". Poi, ho eseguito un comando ping dal Prompt dei comandi e ho osservato i cambiamenti nel processo "cmd.exe" durante l'esecuzione del ping.

1



2

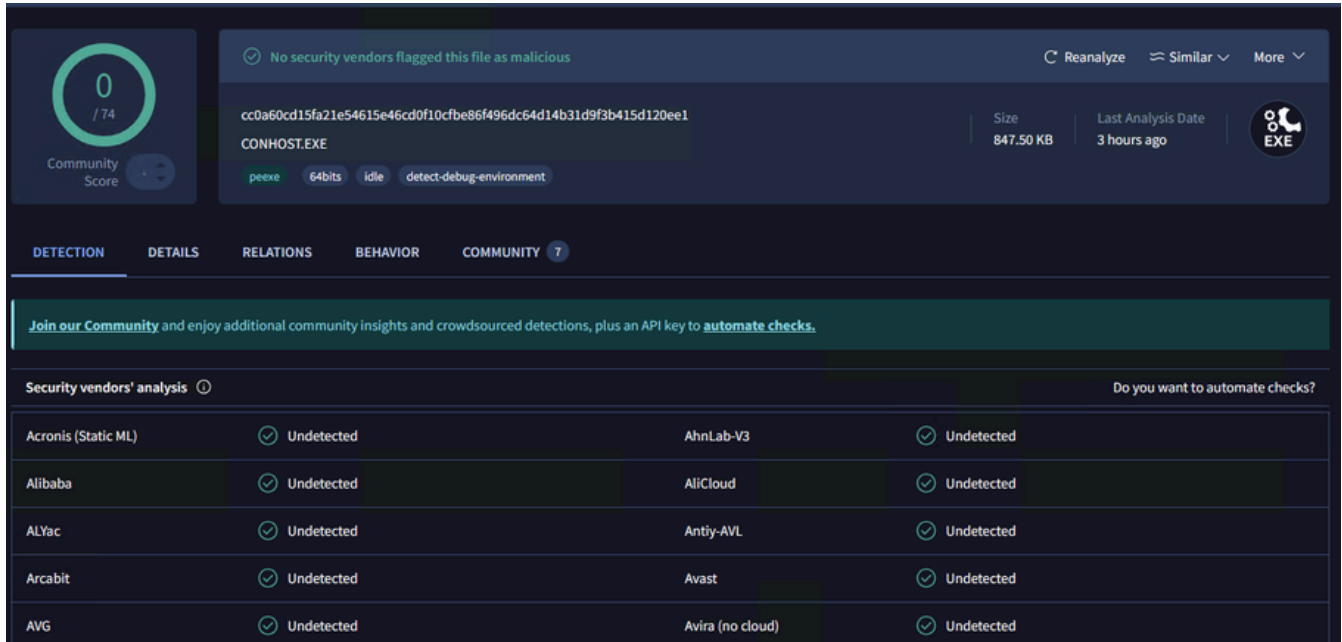
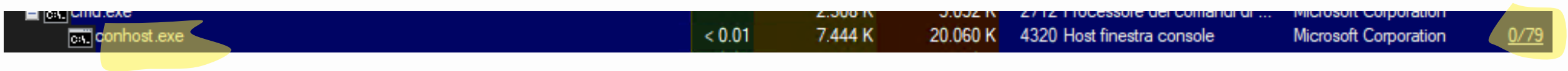


Dopo aver avviato il comando ping, è apparso un nuovo processo "**PING.EXE**" come processo figlio di "cmd.exe" in Process Explorer, indicato chiaramente nella struttura dei processi.

# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

Mentre esaminavo l'elenco dei processi attivi, ho ipotizzato che il processo figlio "conhost.exe" potesse **essere sospetto**. Per verificarne la sicurezza, ho fatto clic con il tasto destro su "**conhost.exe**" e ho selezionato l'opzione "**Controlla VirusTotal**", accettando i Termini di servizio quando richiesto.

Ho quindi espanso la finestra di Process Explorer per visualizzare la colonna VirusTotal e ho cliccato sul link per verificare i risultati. Successivamente, **ho terminato** il processo "cmd.exe" e, di conseguenza, anche il processo figlio "**conhost.exe**" **si è interrotto, poiché dipendeva dal processo padre**.

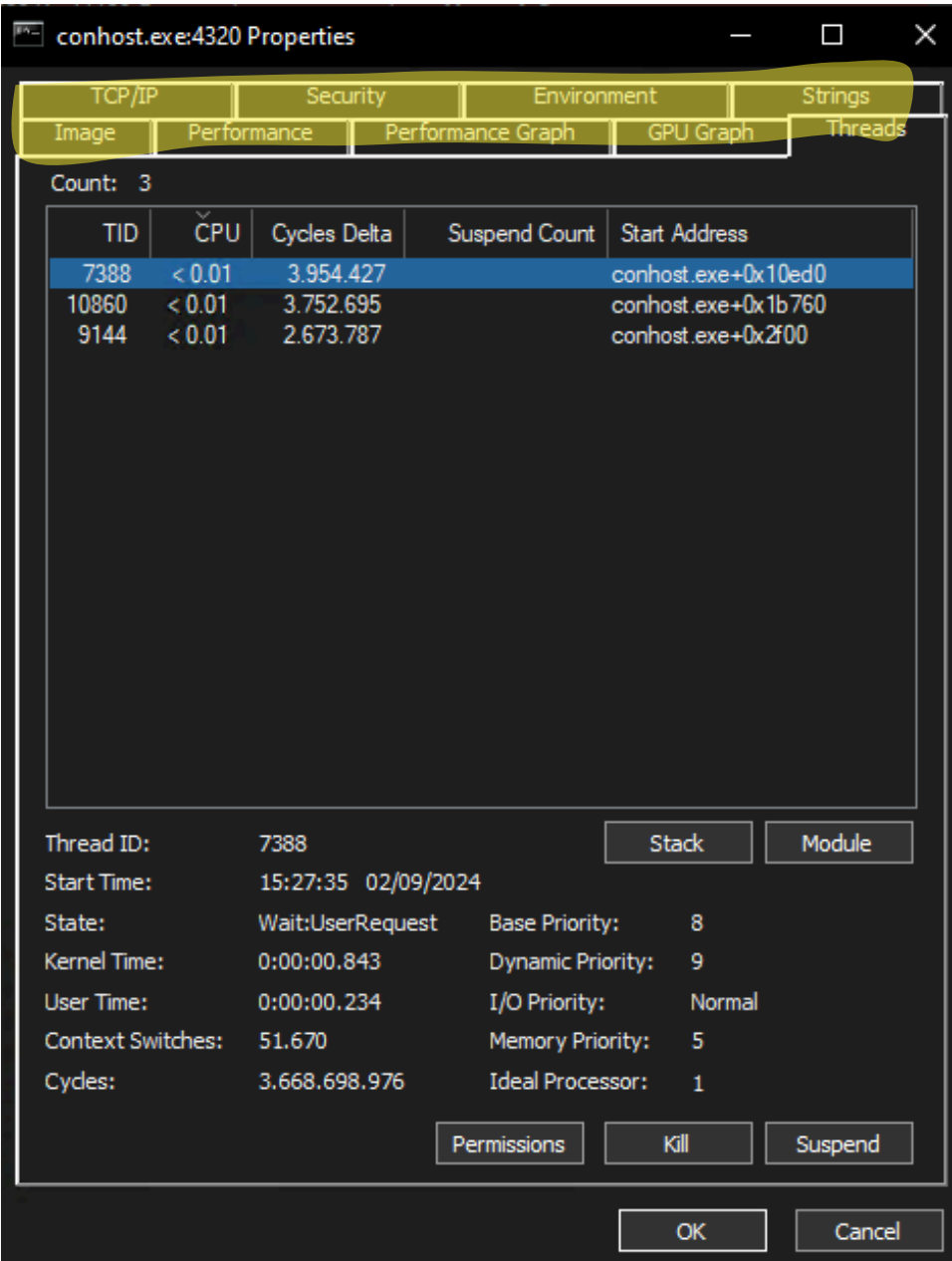


# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

Nella seconda parte del laboratorio, ho esplorato i **thread** e gli **handle** associati ai processi. Dopo aver aperto un prompt dei comandi, ho usato Process Explorer per esaminare i thread attivi del processo "conhost.exe".

Facendo clic con il tasto destro su "conhost.exe" e selezionando "Proprietà", ho aperto la scheda "**Thread**" per visualizzare i dettagli dei thread attivi.

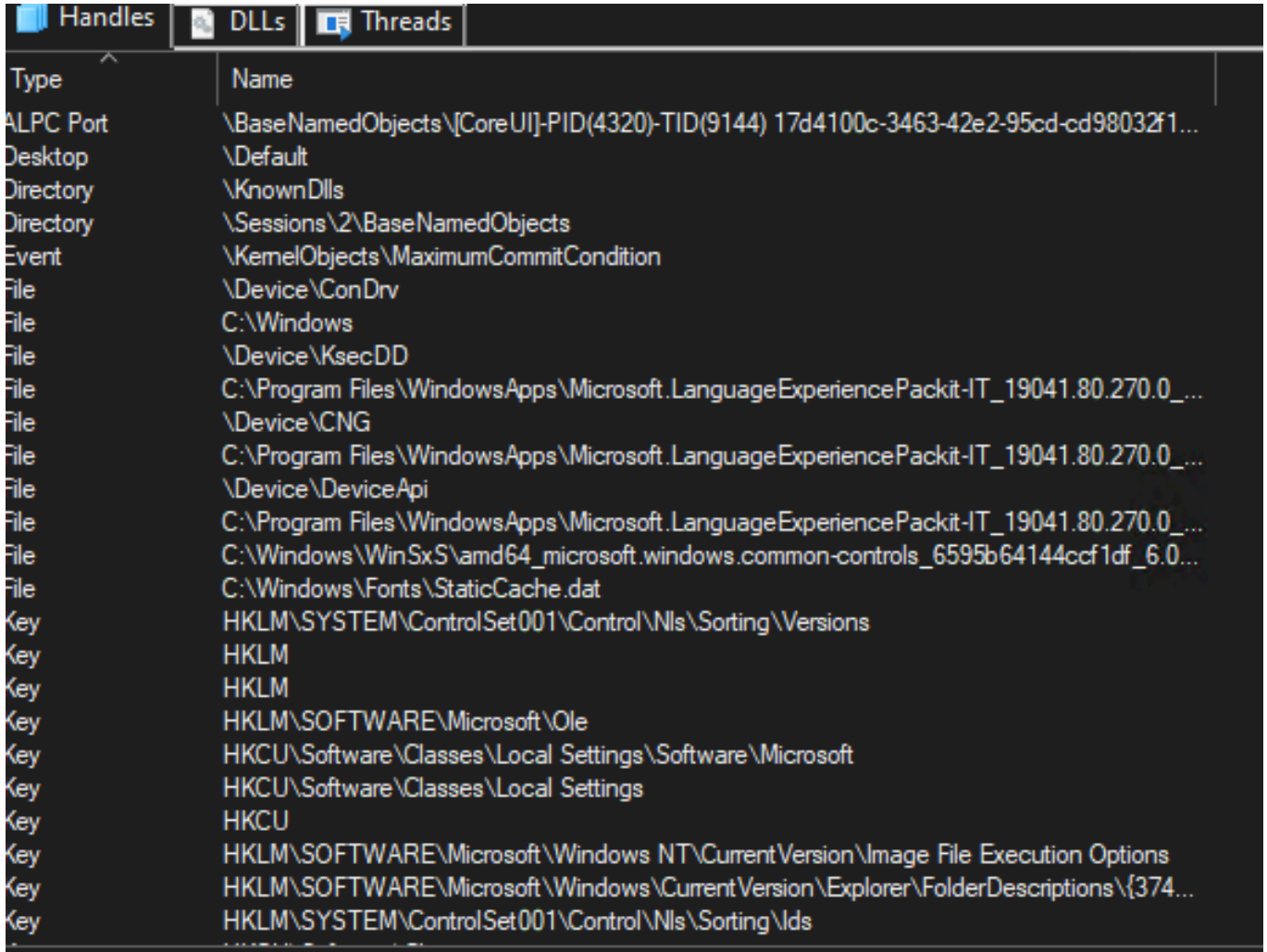
Qui, ho potuto accedere a varie informazioni, come **variabili d'ambiente**, dati sulla sicurezza, dettagli sulle prestazioni e **stringhe**, ottenendo così una visione più approfondita del funzionamento interno del processo.





# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

Nel secondo passaggio, ho esplorato gli handle associati al processo "conhost.exe". In Process Explorer, ho selezionato "**View**" e poi "**Lower Pane View**", scegliendo l'opzione "**Handles**" per visualizzare gli handle correlati. Ho esaminato gli handle e ho notato che puntavano a **file**, **chiavi di registro** e **thread**. Dopo aver completato l'analisi, ho chiuso Process Explorer.

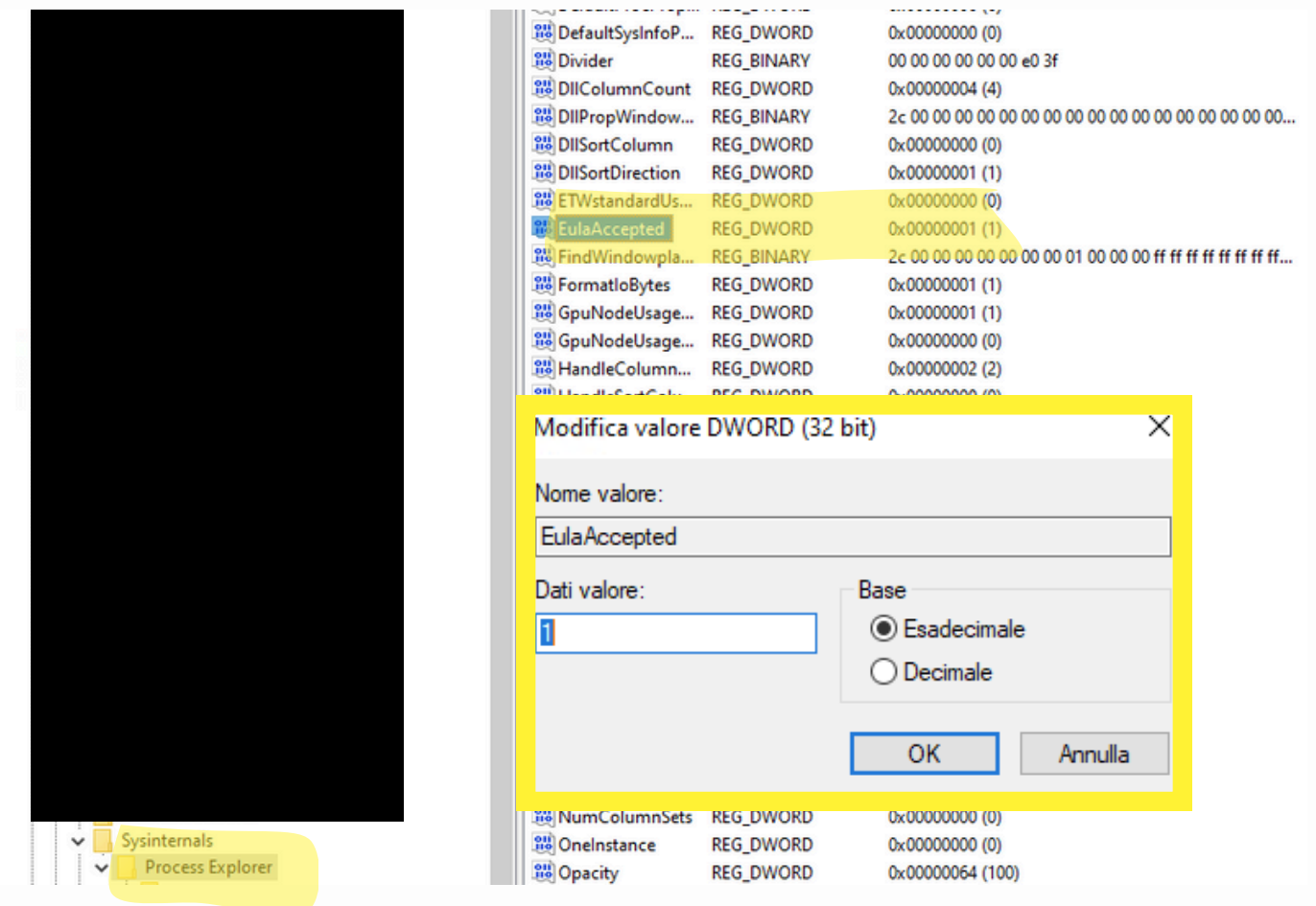


# 01 - EXPLORING PROCESSES, THREADS, HANDLES, AND WINDOWS REGISTRY

Nella terza parte del laboratorio, ho esplorato il Registro di sistema di Windows, che è un database gerarchico che memorizza la maggior parte delle impostazioni di configurazione del sistema operativo e dell'ambiente desktop. Per accedere al Registro di sistema, ho cercato "regedit" dal menu Start e ho aperto l'Editor del Registro di sistema. Questo editor contiene cinque hive principali: **HKEY\_CLASSES\_ROOT**, **HKEY\_CURRENT\_USER**, **HKEY\_LOCAL\_MACHINE**, **HKEY\_USERS**, e **HKEY\_CURRENT\_CONFIG**. Questi hive memorizzano diverse configurazioni e informazioni specifiche per il sistema e per gli utenti.

Successivamente, ho navigato fino alla chiave del registro **"EulaAccepted"** per Process Explorer, situata in **HKEY\_CURRENT\_USER > Software > Sysinternals > Process Explorer**.

Ho verificato che il valore attuale della chiave fosse impostato su **1**, indicando che l'utente ha accettato l'EULA. Ho poi modificato il valore da 1 a **0** per indicare che l'EULA non è stata accettata. Infine, ho riaperto Process Explorer e ho notato che veniva visualizzata di nuovo la finestra di dialogo del Contratto di Licenza, poiché il valore era stato modificato a 0 nel registro.



# 02 - WINDOWS POWERSHELL

Ho aperto la console di **PowerShell**. Ho fatto lo stesso per aprire il Prompt dei comandi. Questo mi ha permesso di confrontare l'output di alcuni comandi comuni in entrambe le console, come il comando dir, che ha mostrato un elenco di sottodirectory e file in entrambe le finestre, con alcune differenze visibili. PowerShell mostra colonne aggiuntive come "**Mode**" e "**Length**", mentre il Prompt dei comandi include dettagli come il numero di serie del volume e lo spazio disponibile.

C:\Users\Flavio>cd Desktop

C:\Users\Flavio\Desktop>dir

Il volume nell'unità C non ha etichetta.  
Numero di serie del volume: D496-6E93

Directory di C:\Users\Flavio\Desktop

02/09/2024	15:03	<DIR>	.
02/09/2024	15:03	<DIR>	..
26/08/2024	16:27		1.254 Adobe Lightroom Classic.lnk
26/08/2024	16:27		1.233 Adobe Photoshop 2024.lnk
26/08/2024	13:12	<DIR>	ajeje
27/08/2024	22:34	<DIR>	BuildWeek
27/08/2024	10:32		114.688 calc-2001.exe
25/08/2024	23:00		137.369.456 DSC01785.psd
13/08/2024	17:19	<DIR>	IOCs
07/08/2024	15:49		204 script-win7.txt
02/09/2024	15:03	<DIR>	sysinternals
26/08/2024	13:14	<DIR>	test
24/08/2024	16:30		1.453 Webex.lnk
			6 File 137.488.288 byte
			7 Directory 48.912.121.856 byte disponibili

C:\Users\Flavio\Desktop>

PS C:\Users\Flavio> cd .\Desktop\  
PS C:\Users\Flavio\Desktop> dir

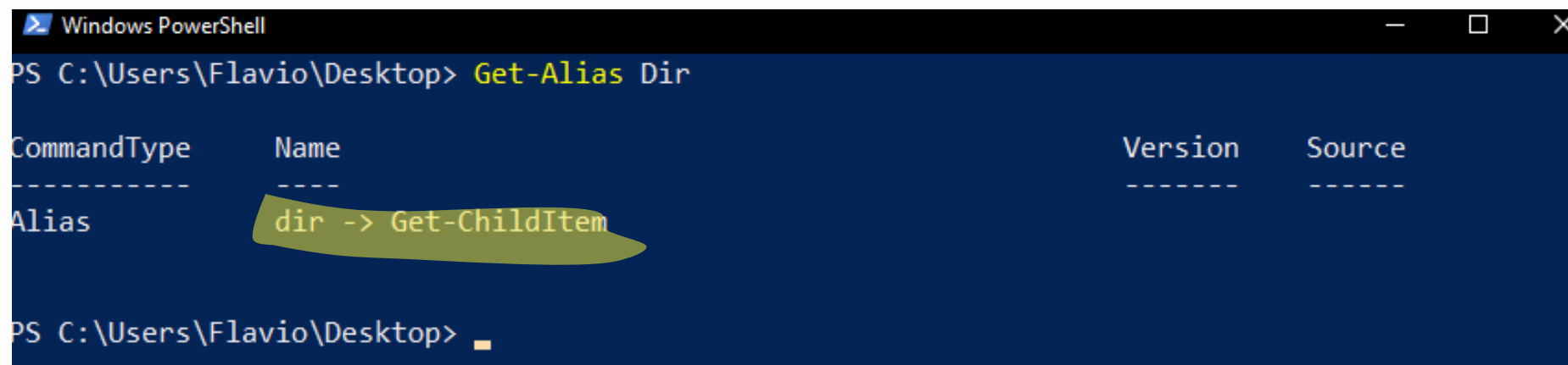
Directory: C:\Users\Flavio\Desktop

Mode	LastWriteTime		Length	Name
d----	26/08/2024	13:12		ajeje
d----	27/08/2024	22:34		BuildWeek
d----	13/08/2024	17:19		IOCs
d----	02/09/2024	15:03		sysinternals
d----	26/08/2024	13:14		test
-a----	26/08/2024	16:27	1254	Adobe Lightroom Classic.lnk
-a----	26/08/2024	16:27	1233	Adobe Photoshop 2024.lnk
-a----	27/08/2024	10:32	114688	calc-2001.exe
-a----	25/08/2024	23:00	137369456	DSC01785.psd
-a----	07/08/2024	15:49	204	script-win7.txt
-a----	24/08/2024	16:30	1453	Webex.lnk

PS C:\Users\Flavio\Desktop>

## 02 - WINDOWS POWERSHELL

Ho eseguito vari comandi, come **ping**, **cd**, e **ipconfig**, sia nel Prompt dei comandi che in PowerShell, notando che l'output era simile in entrambe le console. Inoltre, ho scoperto che il comando PowerShell equivalente a **dir** è **Get-ChildItem**, utilizzando il comando **Get-Alias dir** per verificarlo. Questo ha evidenziato la struttura "**verbo-nome**" tipica dei cmdlet di PowerShell.



```
Windows PowerShell
PS C:\Users\Flavio\Desktop> Get-Alias Dir

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

Successivamente, ho approfondito l'uso dei **cmdlet** di PowerShell, che seguono una struttura di comando del tipo "verbo-sostantivo". Ho utilizzato **Get-Alias** dir per scoprire che il cmdlet PowerShell per **dir** è **Get-ChildItem**. Ho poi effettuato una ricerca online per ottenere maggiori dettagli sui **cmdlet**, ampliando la mia comprensione delle capacità di PowerShell rispetto al Prompt dei comandi. Ho avuto modo di approfondire PowerShell durante l'estate grazie alla certificazione gratuita Blue Team dal sito [securityblue.team](https://securityblue.team)



# 02 - WINDOWS POWERSHELL

Ho esplorato il comando **netstat** in PowerShell, iniziando con **netstat -h** per vedere le opzioni disponibili. Ho poi visualizzato la tabella di routing con **netstat -r** e ho esaminato le connessioni attive utilizzando **netstat -abno**. Successivamente, ho aperto il Task Manager, **ordinato i processi per PID** e ho usato queste informazioni per ottenere maggiori dettagli sul processo associato a uno dei PID elencati, approfondendo le informazioni disponibili nella scheda Dettagli e nella finestra Proprietà.

```
PS C:\Users\Flavio\Desktop> netstat -abno
Per eseguire l'operazione richiesta è necessaria l'esecuzione con privilegi elevati.
PS C:\Users\Flavio\Desktop>
```

svchost.exe	1060	In esecuzione	SERVIZIO DI RETE	00	6.284 K
-------------	------	---------------	------------------	----	---------

```
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   1060
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0          LISTENING   4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:3389             0.0.0.0:0          LISTENING   1196
TermService
[svchost.exe]
TCP    0.0.0.0:5040             0.0.0.0:0          LISTENING   7692
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5985             0.0.0.0:0          LISTENING   4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:7680             0.0.0.0:0          LISTENING   6452
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:27525            0.0.0.0:0          LISTENING   3204
[DrivePool.Service.exe]
TCP    0.0.0.0:28525            0.0.0.0:0          LISTENING   3864
[Scanner.Service.exe]
TCP    0.0.0.0:47001            0.0.0.0:0          LISTENING   4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664            0.0.0.0:0          LISTENING   936
[lsass.exe]
```

## 02 - WINDOWS POWERSHELL

Infine, ho utilizzato PowerShell per **svuotare il Cestino**, un'azione che può essere **automatizzata** per semplificare la gestione del sistema. Dopo aver verificato che il Cestino contenesse file, ho eseguito il comando **clear-recyclebin** per eliminare definitivamente tutti i file al suo interno. Questo comando ha richiesto una conferma prima di procedere, ma una volta confermato, i file sono stati eliminati in **modo permanente**.

```
PS C:\Windows\system32> clear-recyclebin
```

```
Conferma
```

```
Eseguire l'operazione?
```

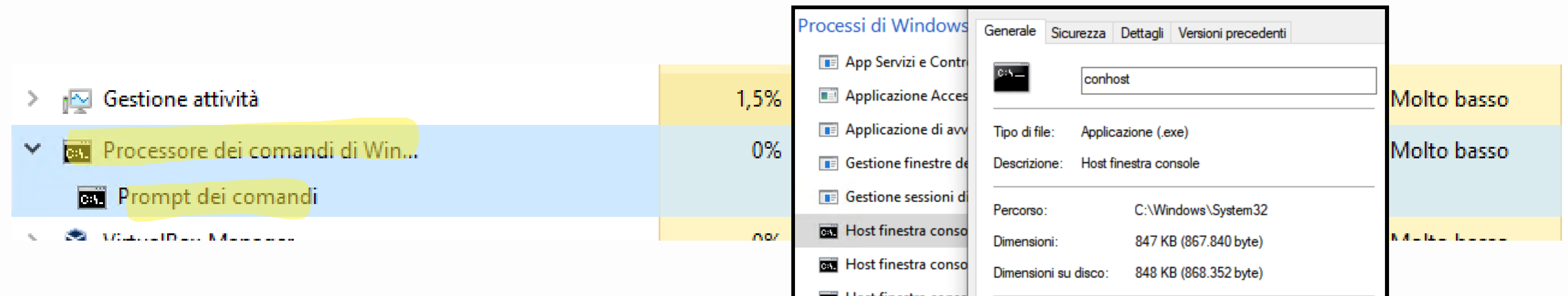
```
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
```

```
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): ■
```

## 03 - WINDOWS TASK MANAGER

Ho aperto il Task Manager per esaminare i processi in esecuzione sul sistema. Dopo aver espanso la voce "**Processore dei comandi di windows**", ho notato che sotto di essa era elencato "**Prompt dei comandi**". Ho esplorato le tre categorie di processi: Applicazioni, Processi in background e Processi di Windows.

Dopo aver chiuso la finestra del Prompt dei comandi, i processi associati, come "**Processore dei comandi di windows**" e "Console Window Host", sono scomparsi dall'elenco. Ho anche ordinato i processi per utilizzo della memoria, visualizzando l'uso della memoria in percentuale per identificare eventuali problemi legati alle risorse. Infine, ho terminato l'attività di Firefox dal Task Manager, chiudendo tutte le finestre del browser.



## 03 - WINDOWS TASK MANAGER

Nella scheda **Servizi** del Task Manager, ho esplorato lo stato dei servizi attivi sul sistema. Ho constatato che i servizi possono avere due stati: "**Arrestato**" e "**In esecuzione**". Questa scheda è utile per gestire e monitorare i servizi di sistema, permettendo di avviare o arrestare manualmente i servizi in base alle necessità.

Nella scheda **Prestazioni**, ho esaminato varie metriche di sistema, come il numero di thread e processi attivi, nonché la memoria fisica totale e disponibile. Ho scoperto che X thread e X processi erano in esecuzione (è chiaro che i valori cambiano a seconda del contesto). Ho anche verificato l'utilizzo della **memoria fisica**. Infine, ho visualizzato la velocità di collegamento **Ethernet** e l'indirizzo IPv4 del PC. Ho poi aperto il Resource Monitor dal Task Manager per un'analisi più dettagliata delle risorse di sistema.

Comprendere il funzionamento del Task Manager è **fondamentale per un amministratore**, poiché offre una visione **dettagliata** delle risorse di sistema e dei processi in esecuzione. Questo strumento è essenziale per risolvere problemi legati all'uso della CPU, della memoria, del disco e della rete, oltre a fornire la possibilità di terminare attività o processi problematici.





# GRAZIE

**Flavio Scognamiglio**