

# S11L1

## ESERCIZIO 2: Esplorazione di Processi, Thread, Handle e Registro di Windows

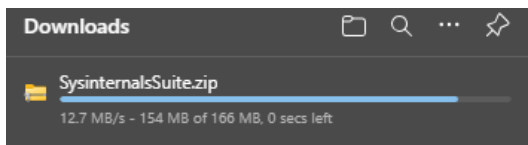
### Obiettivi

In questo laboratorio, esplorerai i processi, i thread e gli handle utilizzando Process Explorer della Suite SysInternals. Utilizzerai anche il Registro di Windows per modificare un'impostazione.

- Parte 1: Esplorazione dei Processi
- Parte 2: Esplorazione di Thread e Handle
- Parte 3: Esplorazione del Registro di Windows

### Parte 1: Esplorazione dei Processi, passo 1

Navigo sul sito Microsoft e scarico Windows SysInternals Suite, dopo averlo scaricato estraggo il file zip.



### Avvio procexp.exe

pendmoves	9/22/2025 2:12 PM	Application	333 KB
pendmoves64	9/22/2025 2:12 PM	Application	431 KB
pipelist	9/22/2025 2:12 PM	Application	332 KB
pipelist64	9/22/2025 2:12 PM	Application	432 KB
portmon	9/22/2025 2:12 PM	Application	441 KB
procdump	9/22/2025 2:12 PM	Application	774 KB
procdump64	9/22/2025 2:12 PM	Application	415 KB
procexp	9/22/2025 2:12 PM	Compiled HTML ...	71 KB
procexp	9/22/2025 2:12 PM	Application	4,425 KB
procexp64	9/22/2025 2:12 PM	Application	2,326 KB

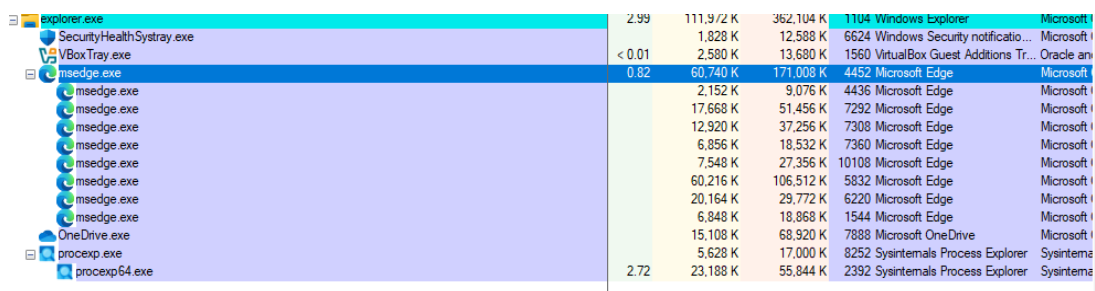
### Passo 2

Una volta aperto, vedremo tutti i processi attivi sul nostro pc, nel seguente modo:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System	0%	40 K	176 K	4	System	Microsoft Corporation
smss.exe	0 K	0 K	0 K	n/a	Hardware Interrupts and DPCs	
csrss.exe	1,116 K	128 K	7,692 K	476	csrss.exe	Microsoft Corporation
svchost.exe	2,036 K	6,768 K	712 K	640	svchost.exe	Microsoft Corporation
services.exe	1,428 K	4,780 K	11,454 K	856	services.exe	Microsoft Corporation
explorer.exe	8,136 K	33,340 K	1000 K	1000	Host Process for Windows S...	Microsoft Corporation
startmenuexperiencehost.exe	81,112 K	101,544 K	1000 K	1000	Host Process for Windows S...	Microsoft Corporation
RuntimeBroker.exe	46,112 K	120,044 K	3508 K	3508	Windows Start Experience H...	Microsoft Corporation
RuntimeBroker.exe	5,328 K	37,420 K	6076 K	6076	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	3,988 K	28,440 K	5200 K	5200	Runtime Broker	Microsoft Corporation
alhost.exe	4,504 K	16,112 K	6272 K	6272	COM Surrogate	Microsoft Corporation
smartscreen.exe	4,096 K	28,024 K	5172 K	5172	Windows Defender SmartSc...	Microsoft Corporation
ApplicationHost.exe	5,396 K	40,280 K	7896 K	7896	Application Host	Microsoft Corporation
RuntimeBroker.exe	5,836 K	27,792 K	10212 K	10212	Runtime Broker	Microsoft Corporation
svchost.exe	2,536 K	12,064 K	9532 K	9532	svchost.exe	Microsoft Corporation
RuntimeBroker.exe	5,232 K	27,416 K	3636 K	3636	Runtime Broker	Microsoft Corporation
svchost.exe	22,668 K	79,396 K	6308 K	6308	svchost.exe	Microsoft Corporation
svchost.exe	5,940 K	10,644 K	572 K	572	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,492 K	11,268 K	928 K	928	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,960 K	12,176 K	1136 K	1136	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,264 K	9,740 K	1152 K	1152	Host Process for Windows S...	Microsoft Corporation
svchost.exe	4,436 K	20,912 K	1180 K	1180	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,508 K	12,620 K	1252 K	1252	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,944 K	14,712 K	1320 K	1320	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,676 K	9,180 K	1380 K	1380	Host Process for Windows S...	Microsoft Corporation
svchost.exe	4,476 K	10,028 K	1596 K	1596	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,760 K	16,000 K	1620 K	1620	Host Process for Windows S...	Microsoft Corporation
svchost.exe	5,724 K	19,252 K	2872 K	2872	Host Process for Windows T...	Microsoft Corporation
svchost.exe	5,032 K	19,320 K	1680 K	1680	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,388 K	13,528 K	1676 K	1676	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,656 K	7,796 K	1688 K	1688	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,960 K	20,240 K	1864 K	1864	Host Process for Windows S...	Microsoft Corporation
svchost.exe	5,592 K	36,540 K	4992 K	4992	Shell Infrastructure Host	Microsoft Corporation
svchost.exe	8,008 K	33,700 K	8236 K	8236	Shell Infrastructure Host	Microsoft Corporation
svchost.exe	6,084 K	29,216 K	9628 K	9628	Shell Infrastructure Host	Microsoft Corporation
svchost.exe	3,068 K	10,784 K	2036 K	2036	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,528 K	8,836 K	1300 K	1300	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,456 K	10,084 K	1712 K	1712	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,012 K	9,952 K	2212 K	2212	Host Process for Windows S...	Microsoft Corporation
svchost.exe	299,260 K	267,184 K	2320 K	2320	Antimalware Service Execut...	Microsoft Corporation
svchost.exe	10,116 K	23,860 K	2540 K	2540	Host Process for Windows S...	Microsoft Corporation
svchost.exe	13,912 K	24,980 K	2844 K	2844	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,124 K	11,000 K	2980 K	2980	Host Process for Windows S...	Microsoft Corporation
svchost.exe	4,288 K	14,080 K	3056 K	3056	Microsoft Network Realtime I...	Microsoft Corporation
svchost.exe	2,828 K	8,580 K	2084 K	2084	VisualBox Guest Additions S...	Oracle and/or its affiliates
svchost.exe	17,232 K	22,696 K	2092 K	2092	Host Process for Windows S...	Microsoft Corporation
svchost.exe	62,572 K	76,496 K	2720 K	2720	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,380 K	7,372 K	2696 K	2696	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,064 K	10,360 K	2716 K	2716	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,840 K	10,544 K	2900 K	2900	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,816 K	10,580 K	3128 K	3128	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,840 K	16,760 K	3212 K	3212	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,540 K	8,896 K	3244 K	3244	Host Process for Windows S...	Microsoft Corporation
svchost.exe	7,760 K	26,560 K	7028 K	7028	svchost.exe	Microsoft Corporation
svchost.exe	1,952 K	12,140 K	3420 K	3420	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,504 K	12,344 K	3432 K	3432	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,800 K	19,352 K	3512 K	3512	Host Process for Windows S...	Microsoft Corporation
svchost.exe	71,836 K	63,348 K	3540 K	3540	Host Process for Windows S...	Microsoft Corporation
svchost.exe	5,276 K	20,240 K	3684 K	3684	Spooler SubSystem App	Microsoft Corporation

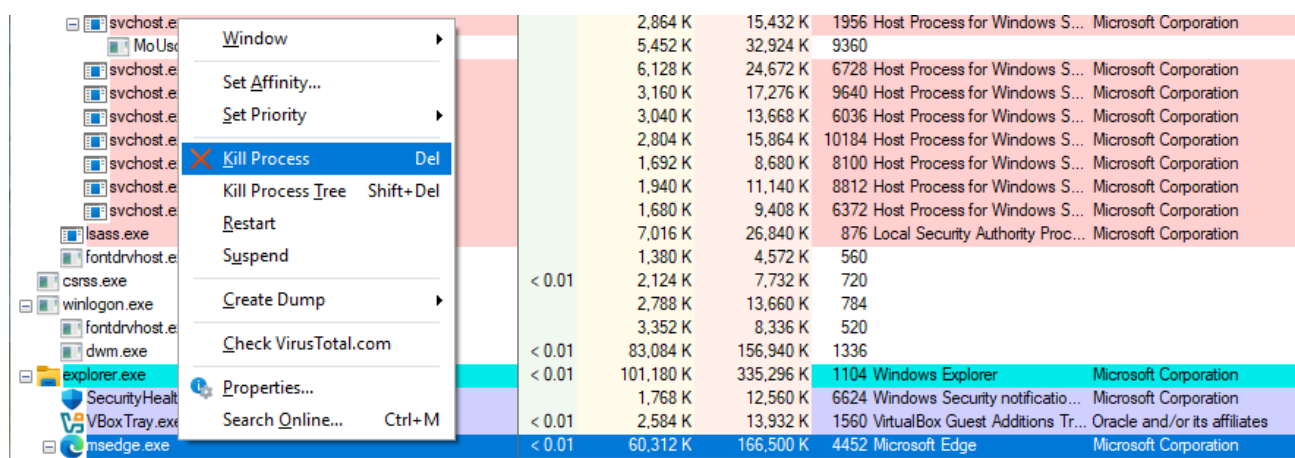
A questo punto, utilizzo il **Find Windows's Process** e lo trascino sulla pagina web di Microsoft Edge utilizzata precedentemente per il download.

Tramite questa funzione possiamo subito identificare il processo del nostro browser.



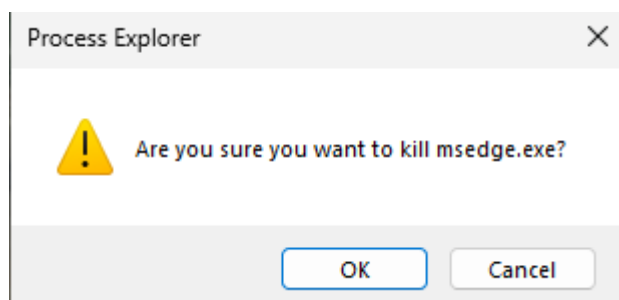
Process Name	Private Bytes	Working Set	Commit Bytes	Process Name	Company Name
explorer.exe	2.99	111,972 K	362,104 K	1104 Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,828 K	12,588 K	6624 Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2,580 K	13,680 K	1560 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
msedge.exe	0.82	60,740 K	171,008 K	4452 Microsoft Edge	Microsoft Corporation
msedge.exe		2,152 K	9,076 K	4436 Microsoft Edge	Microsoft Corporation
msedge.exe		17,668 K	51,456 K	7292 Microsoft Edge	Microsoft Corporation
msedge.exe		12,920 K	37,256 K	7308 Microsoft Edge	Microsoft Corporation
msedge.exe		6,856 K	18,532 K	7360 Microsoft Edge	Microsoft Corporation
msedge.exe		7,548 K	27,356 K	10108 Microsoft Edge	Microsoft Corporation
msedge.exe		60,216 K	106,512 K	5832 Microsoft Edge	Microsoft Corporation
msedge.exe		20,164 K	29,772 K	6220 Microsoft Edge	Microsoft Corporation
msedge.exe		6,848 K	18,868 K	1544 Microsoft Edge	Microsoft Corporation
OneDrive.exe		15,108 K	68,920 K	7888 Microsoft OneDrive	Microsoft Corporation
procexp.exe		5,628 K	17,000 K	8252 Sysinternals Process Explorer	Sysinternals
procexp64.exe	2.72	23,188 K	55,844 K	2392 Sysinternals Process Explorer	Sysinternals

Tramite SysInternals possiamo terminare il processo cliccando con il tasto destro del mouse, kill process.



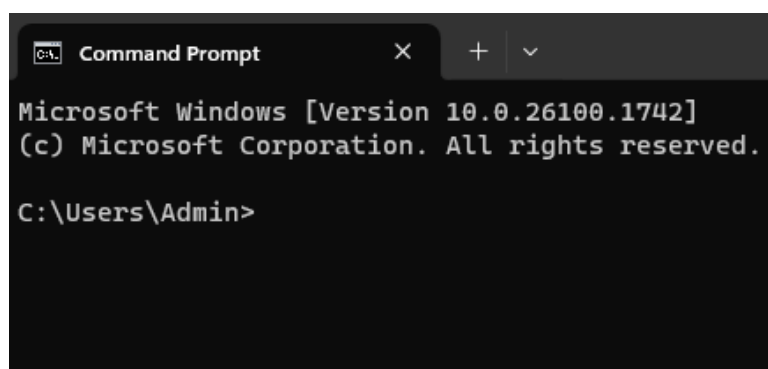
Process Name	Private Bytes	Working Set	Commit Bytes	Process Name	Company Name
svchost.exe		2,864 K	15,432 K	1956 Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,452 K	32,924 K	9360	
svchost.exe		6,128 K	24,672 K	6728 Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,160 K	17,276 K	9640 Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,040 K	13,668 K	6036 Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,804 K	15,864 K	10184 Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,692 K	8,680 K	8100 Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,940 K	11,140 K	8812 Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,680 K	9,408 K	6372 Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,016 K	26,840 K	876 Local Security Authority Proc...	Microsoft Corporation
lsass.exe		1,380 K	4,572 K	560	
fontdrvhost.exe		1,380 K	4,572 K	560	
csrss.exe	< 0.01	2,124 K	7,732 K	720	
winlogon.exe	< 0.01	2,788 K	13,660 K	784	
fontdrvhost.exe	< 0.01	3,352 K	8,336 K	520	
dwm.exe	< 0.01	83,084 K	156,940 K	1336	
explorer.exe	< 0.01	101,180 K	335,296 K	1104 Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe	< 0.01	1,768 K	12,560 K	6624 Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2,584 K	13,932 K	1560 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
msedge.exe	< 0.01	60,312 K	166,500 K	4452 Microsoft Edge	Microsoft Corporation

Chiederà una conferma, dando l'ok la finestra di Microsoft Edge viene chiusa.



### Passo 3

Apro il **Command Prompt** tramite: Start > cercare Prompt dei Comandi > selezionare Prompt dei Comandi



```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>
```

Utilizzo la funzione Find Window's Process per identificare il suo processo.

Come anticipato dalla traccia, il processo per il **Prompt dei Comandi** è **cmd.exe**. Il suo processo genitore è **explorer.exe**. Il **cmd.exe** ha un processo figlio, **conhost.exe**.

OpenConsole.exe		3,120 K	19,368 K	9304	
Windows Terminal.exe	1.82	21,536 K	87,944 K	9720	
RuntimeBroker.exe		2,424 K	13,856 K	2572 Runtime Broker	Microsoft Corporation

Avviando un ping sul **Command Prompt**, possiamo osservare i cambiamenti sotto il processo **cmd.exe**; Viene avviato momentaneamente un processo chiamato **PING.EXE**

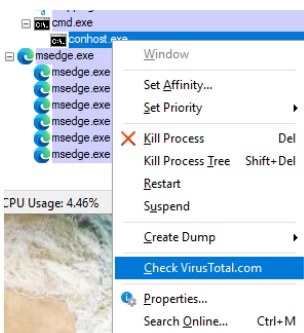
```
C:\Users\Admin>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet (IPv4-only).
  -i TTL      Time To Live.
  -v TOS      Type Of Service (IPv4-only. This setting has been deprecated
              and has no effect on the type of service field in the IP
```

cmd.exe	< 0.01	3,048 K	5,996 K	6116 Windows Command Processor	Microsoft Corporation
conhost.exe		1,456 K	9,884 K	5304 Console Window Host	Microsoft Corporation
PING.EXE	0.25	740 K	4,488 K	9952 TCP/IP Ping Command	Microsoft Corporation

La traccia suggerisce che **conhost.exe** potrebbe essere sospetto. Per verificare la presenza di contenuti malevoli analizziamo il processo tramite **Virus Total**



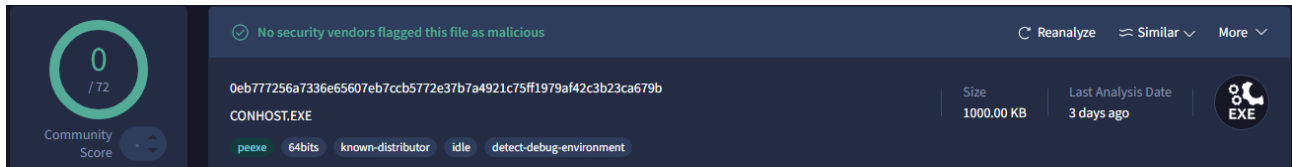
cmd.exe	1,988 K	5,616 K	9680 Windows Command Processor	Microsoft Corporation	
conhost.exe	1,432 K	9,908 K	7248 Console Window Host	Microsoft Corporation	Hash submitted...

conhost.exe		1,404 K	9,892 K	7248 Console Window Host	Microsoft Corporation	0/27
sedge.exe	14.48	59,372 K	174,668 K	1628 Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	2,176 K	9,944 K	3984 Microsoft Edge	Microsoft Corporation	
msedge.exe	5.01	25,912 K	97,744 K	1572 Microsoft Edge	Microsoft Corporation	
msedge.exe	2.78	13,312 K	38,152 K	10032 Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	6,640 K	18,828 K	4904 Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	85,880 K	125,408 K	9584 Microsoft Edge	Microsoft Corporation	
msedge.exe	15.04	276,296 K	336,124 K	5784 Microsoft Edge	Microsoft Corporation	
msedge.exe		9,652 K	20,976 K	6040 Microsoft Edge	Microsoft Corporation	
msedge.exe	1.11	22,788 K	42,320 K	5708 Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	6,452 K	16,822 K	8412 Microsoft Edge	Microsoft Corporation	

Una volta fatto il check con Virus Total, viene mandato l'Hash al sito e successivamente appare 0/77 che sta ad indicare il risultato della ricerca di Virus Total. In altre parole, il risultato 0/77 sta a indicare che:

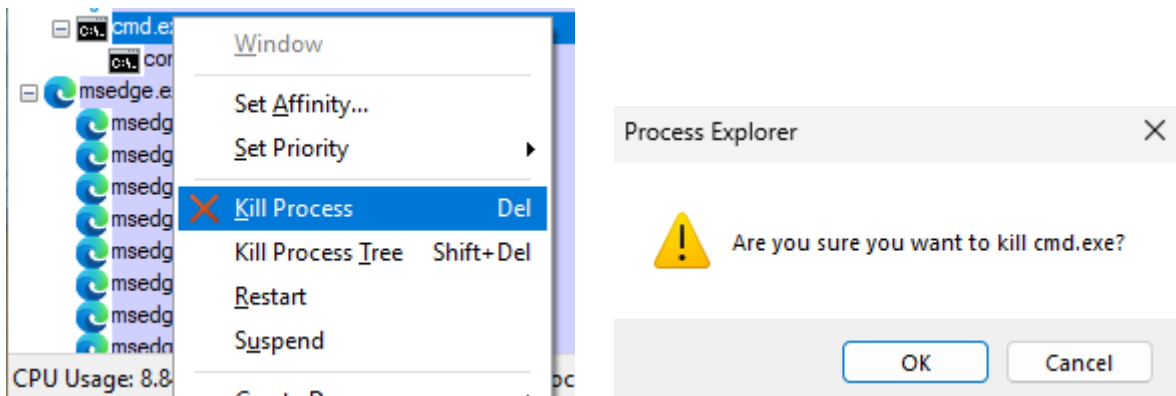
- **0** è il numero di motori che hanno identificato il file come una minaccia.
- **77** è il numero totale di motori antivirus che hanno analizzato il file.

Cliccando sul risultato si aprirà la pagina di Virus Total che ci darà un riepilogo del check fatto



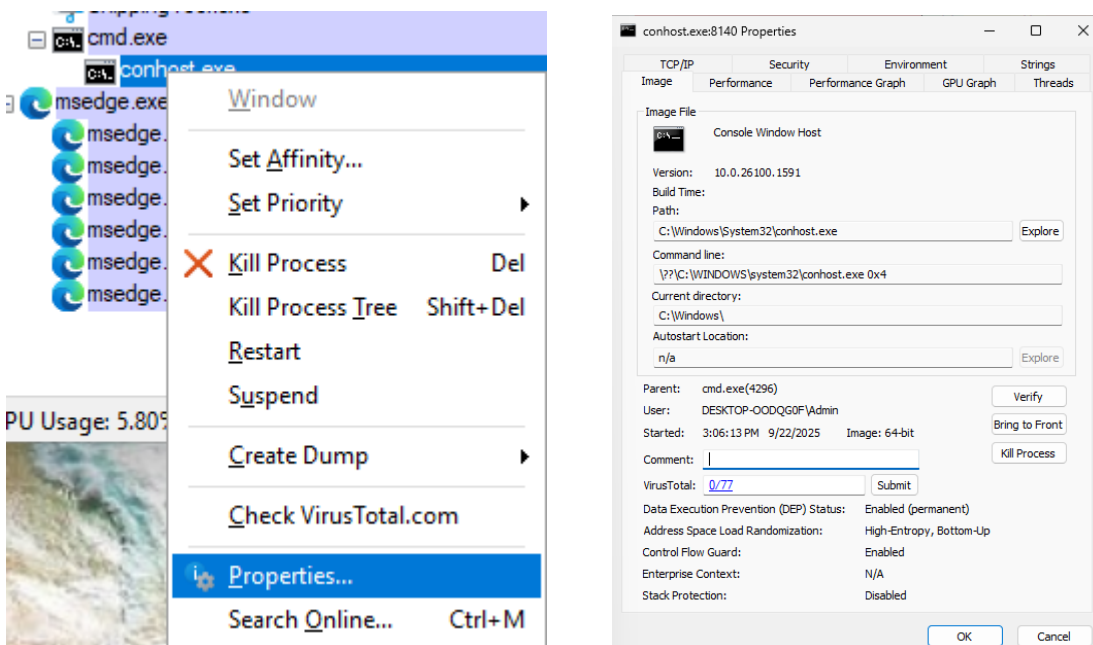
A questo punto terminiamo il processo **cmd.exe** tramite Kill Process.

Dando l'ok all>alert, anche il processo figlio **conhost.exe** viene terminato.



## Parte 2: Esplorazione di Thread e Handle, passo 1

Sempre utilizzando il Command Prompt come esame, andremo ad analizzare le proprietà del processo **conhost.exe**



Tramite le proprietà sono disponibili varie informazioni tra cui:

**Image:** Mostra informazioni sul file del processo stesso, come il percorso, la data di creazione e le firme digitali.

**Performance:** Offre una panoramica delle metriche di utilizzo di CPU e memoria.

**Performance Graph:** Visualizza grafici storici sull'utilizzo di CPU e memoria, utile per identificare picchi di attività.

**GPU Graph:** Se il processo utilizza la scheda grafica, mostra l'attività della GPU.

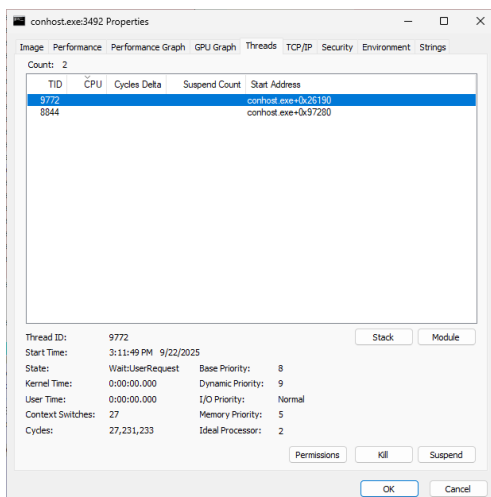
**Threads:** Mostra i singoli thread del processo.

**TCP/IP:** Elenca le connessioni di rete aperte dal processo.

**Security:** Fornisce dettagli sul token di sicurezza del processo, inclusi i permessi e gli account utente.

**Environment:** Mostra le variabili d'ambiente del processo.

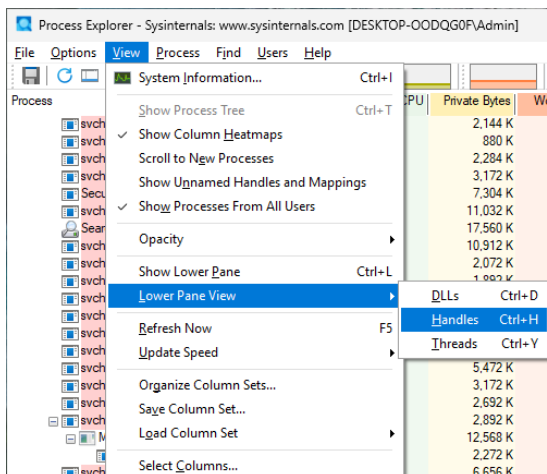
**Strings:** Analizza le stringhe di testo presenti nel file eseguibile del processo, che possono rivelare informazioni su percorsi, nomi di file o altre funzionalità.



**conhost.exe (Thread 9772 e 8844):** Questi sono i thread principali del processo **Console Window Host**. Si occupano direttamente della gestione della finestra della console, dell'input (tastiera) e dell'output (il testo a schermo). In pratica, sono il "motore" che fa funzionare la console.

## Passo 2

Per quanto riguarda l'esplorazione degli Handle, ci basterà fare click su View, Lower Pane View, Handles.



Gli handle sono dei "**segnalibri**" che il processo **conhost.exe** usa per tenere traccia di tutte le risorse che sta utilizzando in quel momento. Gli handle, in questo caso puntano a una vasta gamma di risorse di sistema che il processo sta utilizzando per funzionare correttamente.

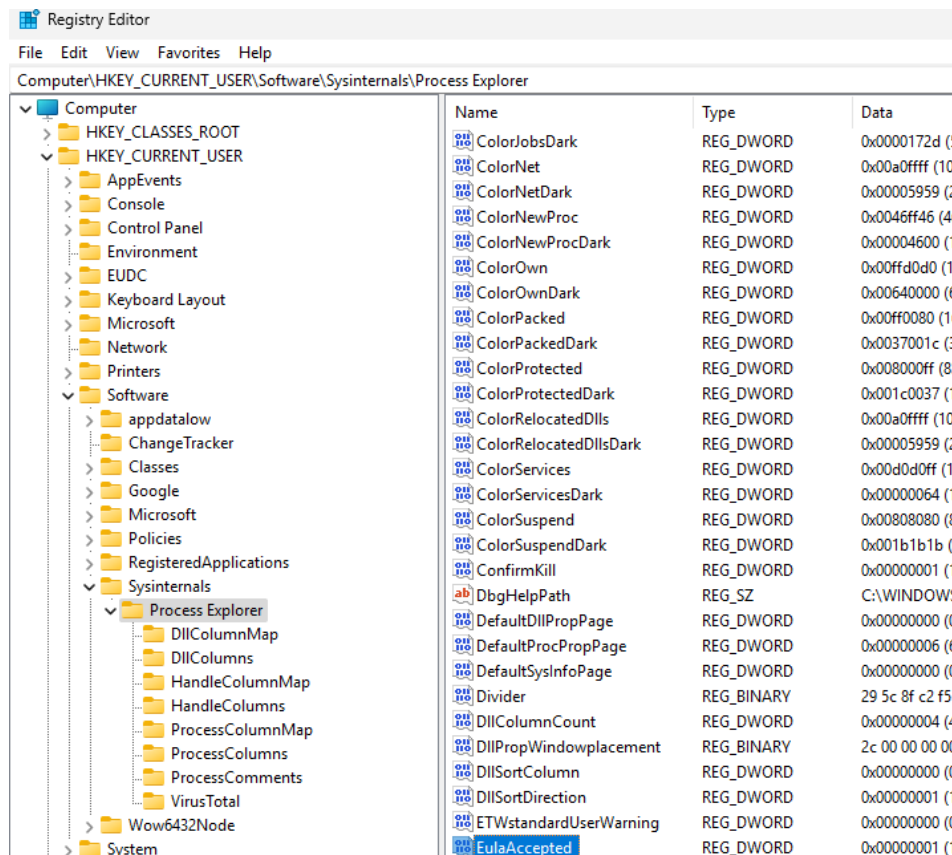
Handles		DLLs	Threads
Type	Name		
ALPC Port	\RPC Control\OLE1054757283E68D48E4659CB6B60D		
Desktop	\Default		
Directory	\KnownDlls		
Directory	\Sessions\1\BaseNamedObjects		
Event	\KernelObjects\MaximumCommitCondition		
File	\Device\ConDrv		
File	C:\Windows		
File	C:\Windows\System32\en-US\Conhost.exe.mui		
File	\Device\CNG		
File	\Device\NamedPipe\		
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions		
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft		
Key	HKCU		
Key	HKLM		
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options		
Key	HKLM\SOFTWARE\Microsoft\Ole		
Key	HKLM		
Key	HKCU\Software\Classes\Local Settings		
Key	HKCU\Software\Classes		
Key	HKCR\PackagedCom		
Key	HKCR\PackagedCom\ClassIndex		
Key	HKCU\Software\Classes\PackagedCom		
Key	HKCU\Software\Classes\PackagedCom\Package		
Key	HKCR\PackagedCom\Package		
Key	HKCU\Software\Classes		
Key	HKCU\Software\Classes		
Key	HKCR\PackagedCom\InterfaceIndex		
Mutant	\Sessions\1\BaseNamedObjects\SM0:3492:304:WinStaging_02		
Mutant	\Sessions\1\BaseNamedObjects\SM0:3492:120:WinError_03		
Section	\BaseNamedObjects\__ComCatalogCache__		
Section	\BaseNamedObjects\__ComCatalogCache__		
Semaphore	\Sessions\1\BaseNamedObjects\SM0:3492:304:WinStaging_02_p0		
Semaphore	\Sessions\1\BaseNamedObjects\SM0:3492:304:WinStaging_02_p0h		
Semaphore	\Sessions\1\BaseNamedObjects\SM0:3492:120:WinError_03_p0		
Semaphore	\Sessions\1\BaseNamedObjects\SM0:3492:120:WinError_03_p0h		
Thread	conhost.exe(3492): 8844		
Thread	conhost.exe(3492): 9772		
Thread	conhost.exe(3492): 9772		
Window Station	\Sessions\1\Windows\Window Stations\WinSta0		
Window Station	\Sessions\1\Windows\Window Stations\WinSta0		

Il processo **conhost.exe** ha chiavi per:

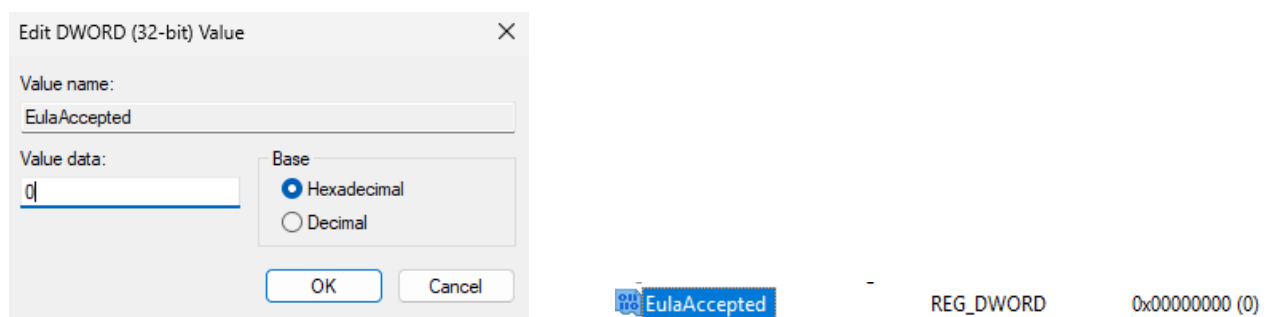
- **File e cartelle:** Per leggere i file di sistema necessari (**File, Directory**).
- **Registro di sistema:** Per leggere impostazioni importanti di Windows (**Key**).
- **Comunicazione:** Per parlare con altri programmi o servizi (**ALPC Port**).
- **Sincronizzazione:** Per coordinare le attività dei suoi stessi thread, assicurandosi che non si intralcino a vicenda (**Semaphore, Mutant, Event**).
- **Finestre e desktop:** Per interagire con l'ambiente grafico (**Desktop**).
- **I suoi stessi thread:** Per monitorare e gestire le sue attività interne (**Thread**).

### Parte 3: Esplorazione del Registro di Windows

Durante lo svolgimento dell'esercizio, abbiamo accettato l'accordo di licenza per Process Explorer. Adesso navigheremo all'interno delle chiavi di registro per individuare la chiave.



Avendo accettato l'accordo, il sistema ha impostato il valore della chiave a 1, adesso modificheremo questo valore in 0 così da dire al sistema che non abbiamo ancora accettato l'accordo. (Passiamo da vero, 1. A falso, 0.)



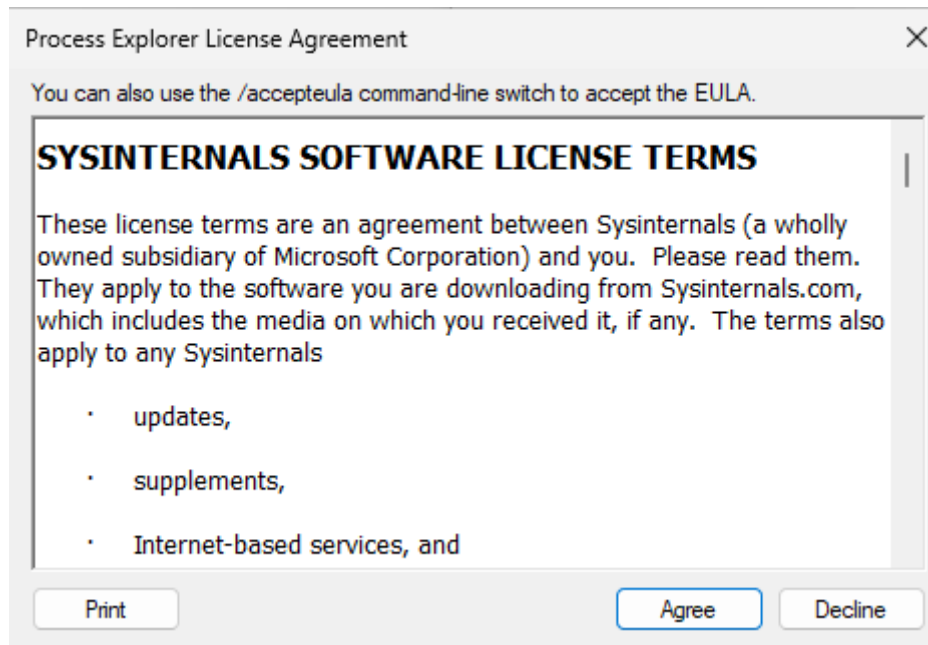
Dopo aver cambiato, il valore nella colonna **Data** è 0.

Adesso proveremo a riaprire nuovamente procexp e dovremmo vedere la richiesta per accettare l'accordo


procdump	9/22/2025 2:12 PM	Application	174 KB
procdump64	9/22/2025 2:12 PM	Application	415 KB
procexp	9/22/2025 2:12 PM	Compiled HTML ...	71 KB
procexp	9/22/2025 2:12 PM	Application	4,425 KB
procexp64	9/22/2025 2:12 PM	Application	2,326 KB
procmon	9/22/2025 2:12 PM	Compiled HTML ...	63 KB



Ci viene chiesto di accettare la licenza. Abbiamo cambiato il valore correttamente e il sistema ci ha chiesto di accettare la licenza. Se lo faremo, il valore della chiave tornerà a 1.



Dopo aver accettato, il valore è tornato 1

 EulaAccepted	REG_DWORD	0x00000001 (1)
--	-----------	----------------