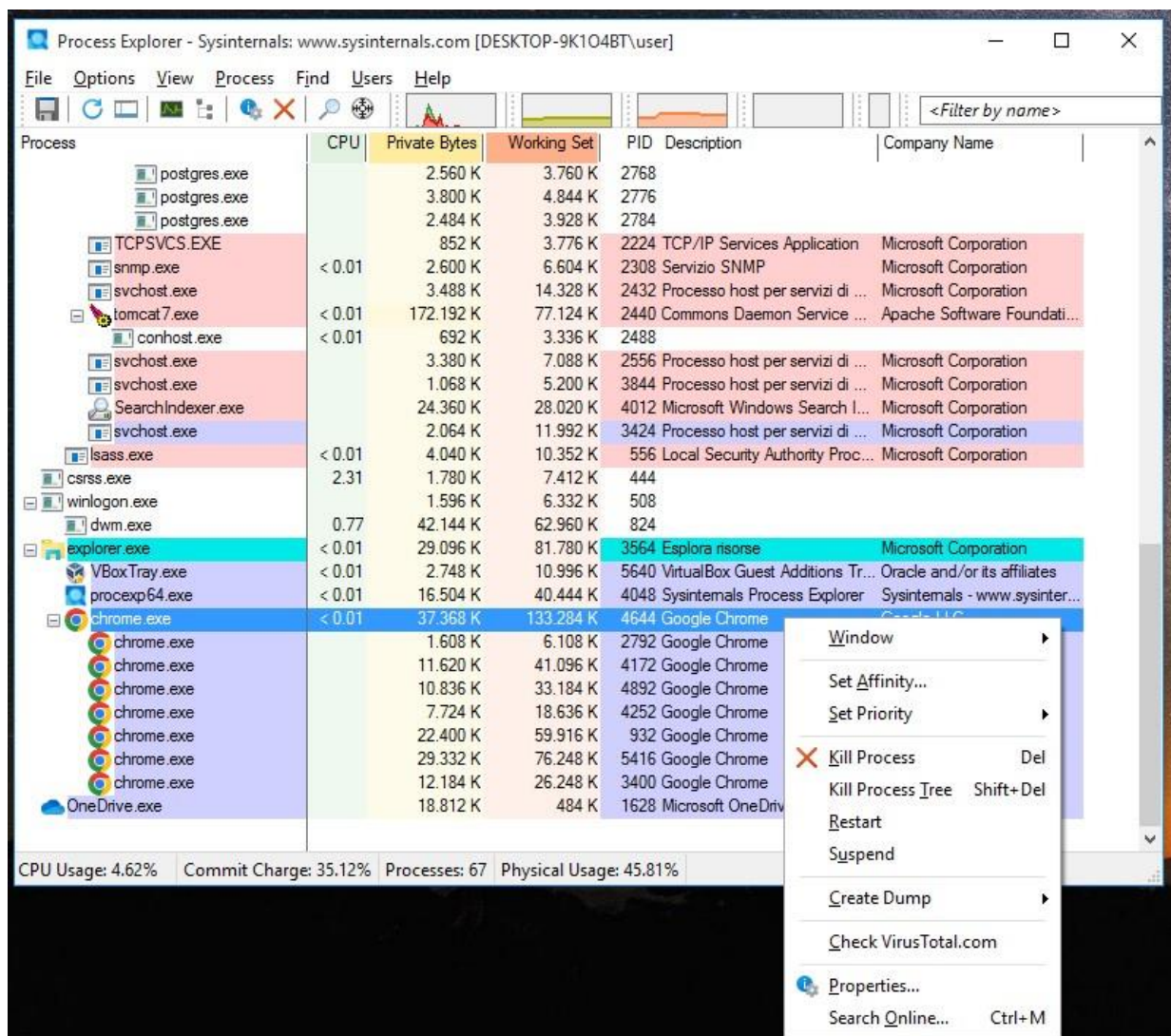


Esplorazione di Processi, Thread, Handle e Registro di Windows

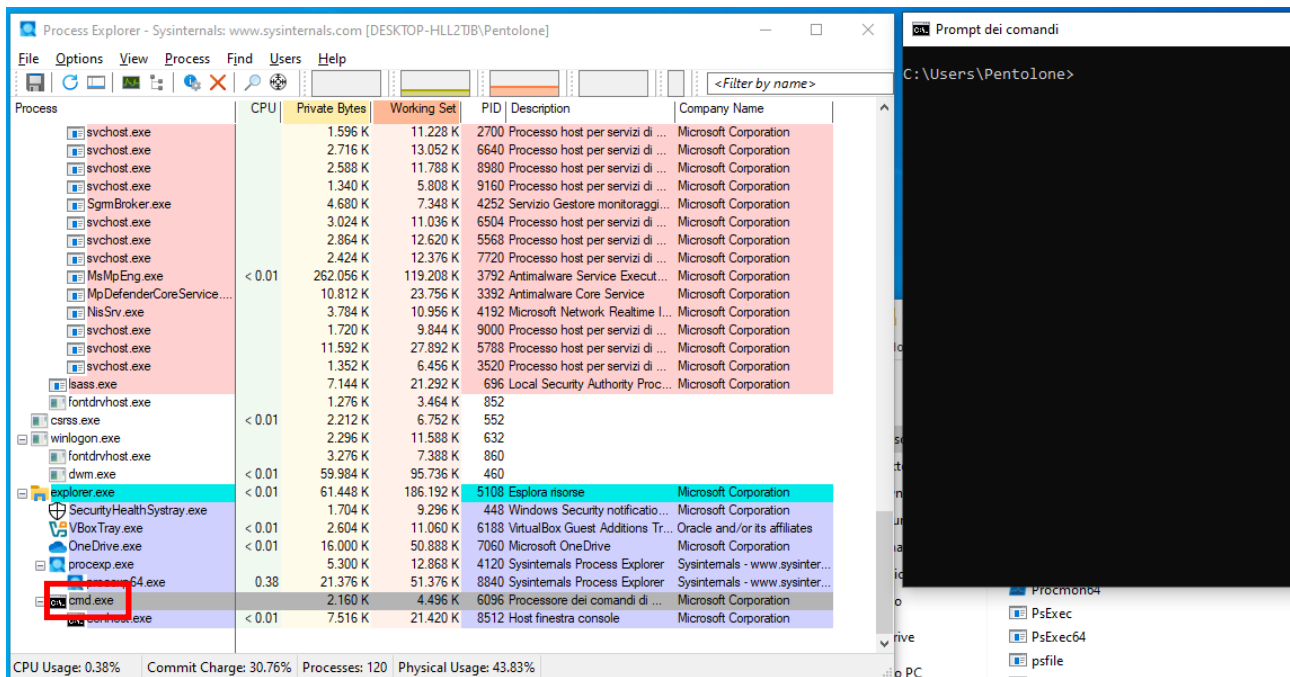
Processi

Un processo è un qualsiasi programma attualmente in esecuzione sulla macchina.

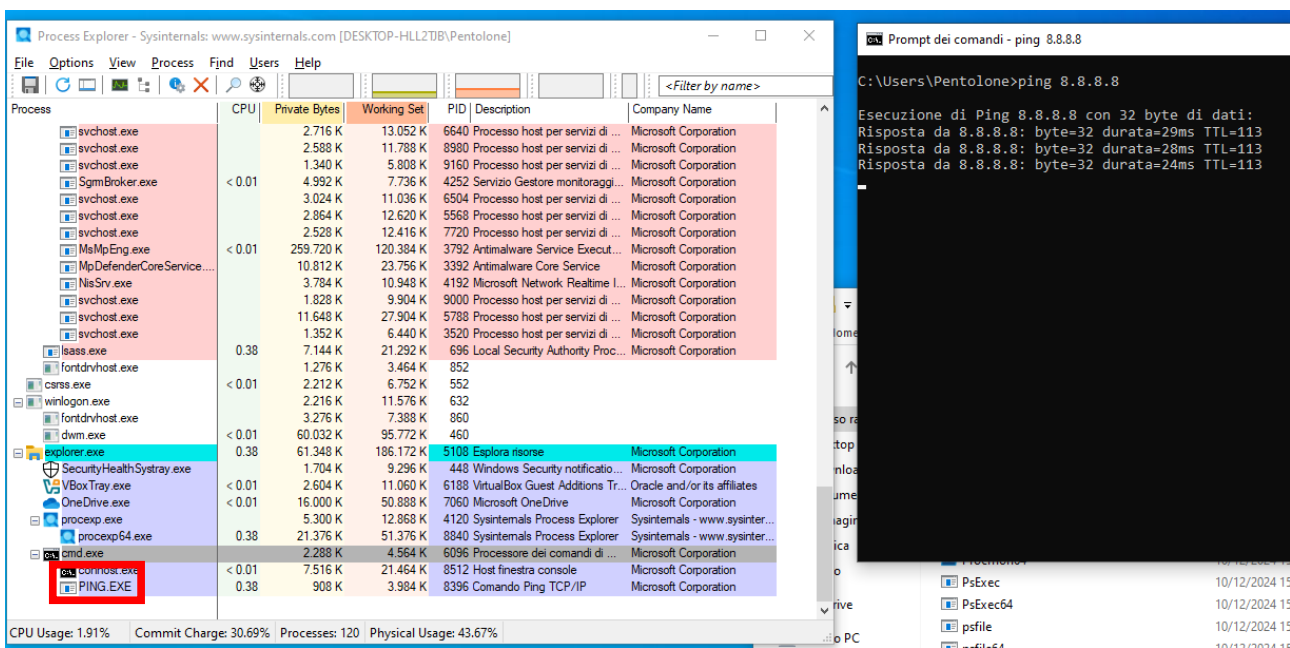
L' esercizio richiede di andare a gestire i processi nel programma *Process Explorer*. Aperto il programma, mostra la lista dei processi attivi in quel momento, tra cui il browser Chrome. Cliccando con il tasto destro sulla voce del processo di Chrome e successivamente su "Kill Process", si vedrà come il processo verrà terminato.



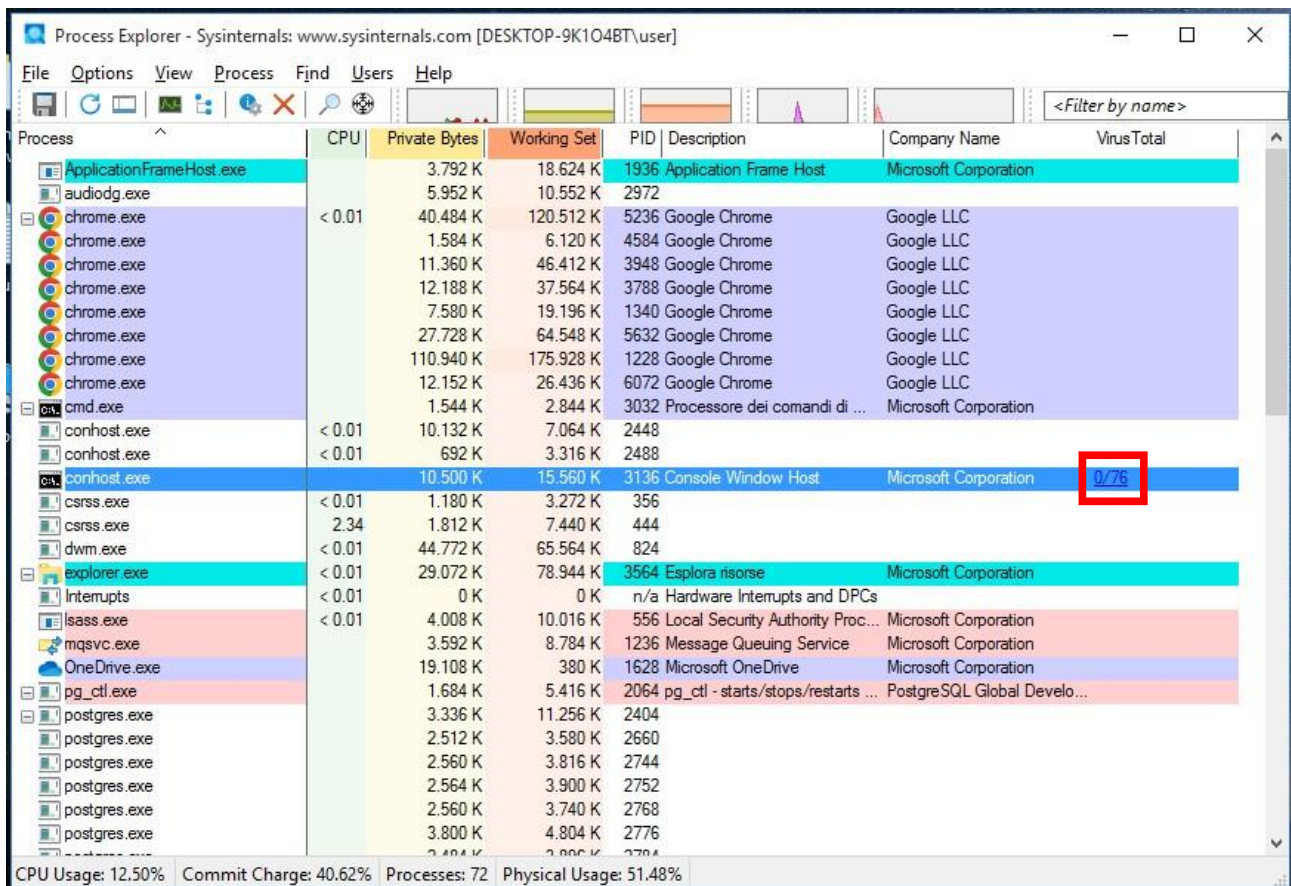
Per vedere un nuovo processo nella lista, bisogna avviare un qualsiasi programma sulla macchina. In questo caso si avvierà il prompt dei comandi. Come si può vedere dall' immagine sottostante compare il processo *cmd.exe*.



Eseguendo un ping sul prompt con Process Explorer aperto, si vedrà aprire e chiudere il processo *ping.exe*, per il tempo necessario di esecuzione del ping.



Se si sospetta che un processo possa essere malevolo, lo si può verificare, cliccando con il tasto destro sul processo e selezionare la voce Check VirusTotal. In questo modo, comparirà una colonna sulla destra che implementa le funzioni del sito virustotal.com, in particolare il punteggio di report del sito.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
ApplicationFrameHost.exe		3.792 K	18.624 K	1936	Application Frame Host	Microsoft Corporation	
audiodg.exe		5.952 K	10.552 K	2972			
chrome.exe	< 0.01	40.484 K	120.512 K	5236	Google Chrome	Google LLC	
chrome.exe		1.584 K	6.120 K	4584	Google Chrome	Google LLC	
chrome.exe		11.360 K	46.412 K	3948	Google Chrome	Google LLC	
chrome.exe		12.188 K	37.564 K	3788	Google Chrome	Google LLC	
chrome.exe		7.580 K	19.196 K	1340	Google Chrome	Google LLC	
chrome.exe		27.728 K	64.548 K	5632	Google Chrome	Google LLC	
chrome.exe		110.940 K	175.928 K	1228	Google Chrome	Google LLC	
chrome.exe		12.152 K	26.436 K	6072	Google Chrome	Google LLC	
cmd.exe		1.544 K	2.844 K	3032	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe	< 0.01	10.132 K	7.064 K	2448			
conhost.exe	< 0.01	692 K	3.316 K	2488			
conhost.exe		10.500 K	15.560 K	3136	Console Window Host	Microsoft Corporation	0/76
csrss.exe	< 0.01	1.180 K	3.272 K	356			
csrss.exe	2.34	1.812 K	7.440 K	444			
dwm.exe	< 0.01	44.772 K	65.564 K	824			
explorer.exe	< 0.01	29.072 K	78.944 K	3564	Esplora risorse	Microsoft Corporation	
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs		
lsass.exe	< 0.01	4.008 K	10.016 K	556	Local Security Authority Proc...	Microsoft Corporation	
mqsvc.exe		3.592 K	8.784 K	1236	Message Queuing Service	Microsoft Corporation	
OneDrive.exe		19.108 K	380 K	1628	Microsoft OneDrive	Microsoft Corporation	
pg_ctl.exe		1.684 K	5.416 K	2064	pg_ctl - starts/stops/restarts ...	PostgreSQL Global Develo...	
postgres.exe		3.336 K	11.256 K	2404			
postgres.exe		2.512 K	3.580 K	2660			
postgres.exe		2.560 K	3.816 K	2744			
postgres.exe		2.564 K	3.900 K	2752			
postgres.exe		2.560 K	3.740 K	2768			
postgres.exe		3.800 K	4.804 K	2776			

CPU Usage: 12.50% Commit Charge: 40.62% Processes: 72 Physical Usage: 51.48%

Threads

Un thread è una parte del processo che può essere eseguita. Un processo può avere uno o più threads.

Sempre con il prompt dei comandi aperto sulla macchina, nella finestra di Process Explorer, cliccare con il tasto destro su *conhost.exe* e selezionare Proprietà. Spostarsi sulla scheda Threads per visualizzare i thread attivi del processo conhost.exe. Se viene visualizzata una finestra di dialogo di avviso, fare clic su OK per continuare. Come mostrato nell' immagine sottostante si possono visualizzare i thread per il processo conhost.exe.

The image shows two windows from Windows Task Manager. The left window is 'Process Explorer' showing a list of processes. The right window is 'conhost.exe:5308 Properties' with the 'Threads' tab selected.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9M...]

Process	CPU	Private Bytes	Working Set
ApplicationFrameHost.exe		3.760 K	18.60
audiodg.exe		5.912 K	10.52
chrome.exe	< 0.01	40.392 K	120.62
chrome.exe		1.584 K	6.12
chrome.exe		11.360 K	46.41
chrome.exe		12.188 K	37.56
chrome.exe		7.580 K	19.20
chrome.exe		27.224 K	64.73
chrome.exe		108.044 K	170.66
chrome.exe		12.152 K	26.43
cmd.exe		1.544 K	2.82
conhost.exe	< 0.01	10.132 K	7.06
conhost.exe	< 0.01	692 K	3.31
conhost.exe		8.800 K	14.62
csrss.exe	< 0.01	1.180 K	3.26
csrss.exe	0.77	1.812 K	7.44
dwm.exe	< 0.01	44.808 K	66.15
explorer.exe	< 0.01	27.376 K	78.20
Interrupts	< 0.01	0 K	
lsass.exe	< 0.01	3.924 K	9.98
mqsvc.exe		3.592 K	8.78
OneDrive.exe		19.108 K	59
pg_ctl.exe		1.684 K	5.41
postgres.exe		3.336 K	11.25
postgres.exe		2.512 K	3.58
postgres.exe		2.560 K	3.81
postgres.exe		2.564 K	3.90
postgres.exe		2.560 K	3.74
postgres.exe		3.800 K	4.80

CPU Usage: 0.77% Commit Charge: 40.12% Processes: 70 Physical U...

conhost.exe:5308 Properties

TCP/IP Security Environment Strings
Image Performance Performance Graph GPU Graph Threads

Count: 2

TID	CPU	Cycles Delta	Suspend Count	Start Address
4628	< 0.01	7.993.159		ConhostV2.dll+0x1c90
5472				ConhostV2.dll\ConsoleCreat...

Thread ID: 5472 Stack Module

Start Time: 15:45:55 10/12/2024

State: Wait:UserRequest Base Priority: 8

Kernel Time: 0:00:00.000 Dynamic Priority: 8

User Time: 0:00:00.000 I/O Priority: Normal

Context Switches: 87 Memory Priority: 5

Cycles: 31.592.028 Ideal Processor: 0

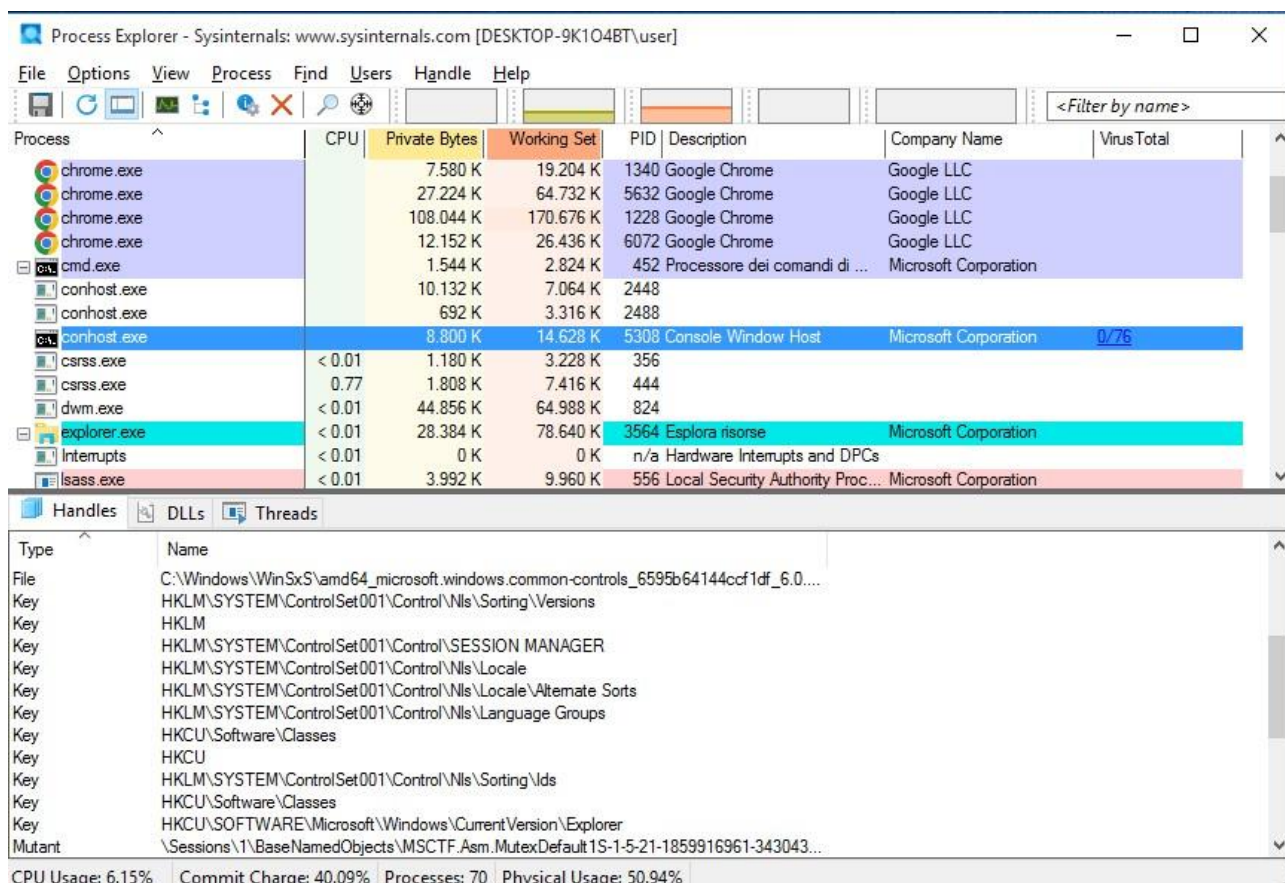
Permissions Kill Suspend

OK Cancel

Handle

Un handle è un riferimento astratto a blocchi di memoria o oggetti gestiti da un sistema operativo.

Nel Process Explorer, fare clic su Visualizza, seleziona *Visualizzazione del riquadro inferiore > Handle* per visualizzare gli handle associati al processo *conhost.exe*.



Registro di Windows

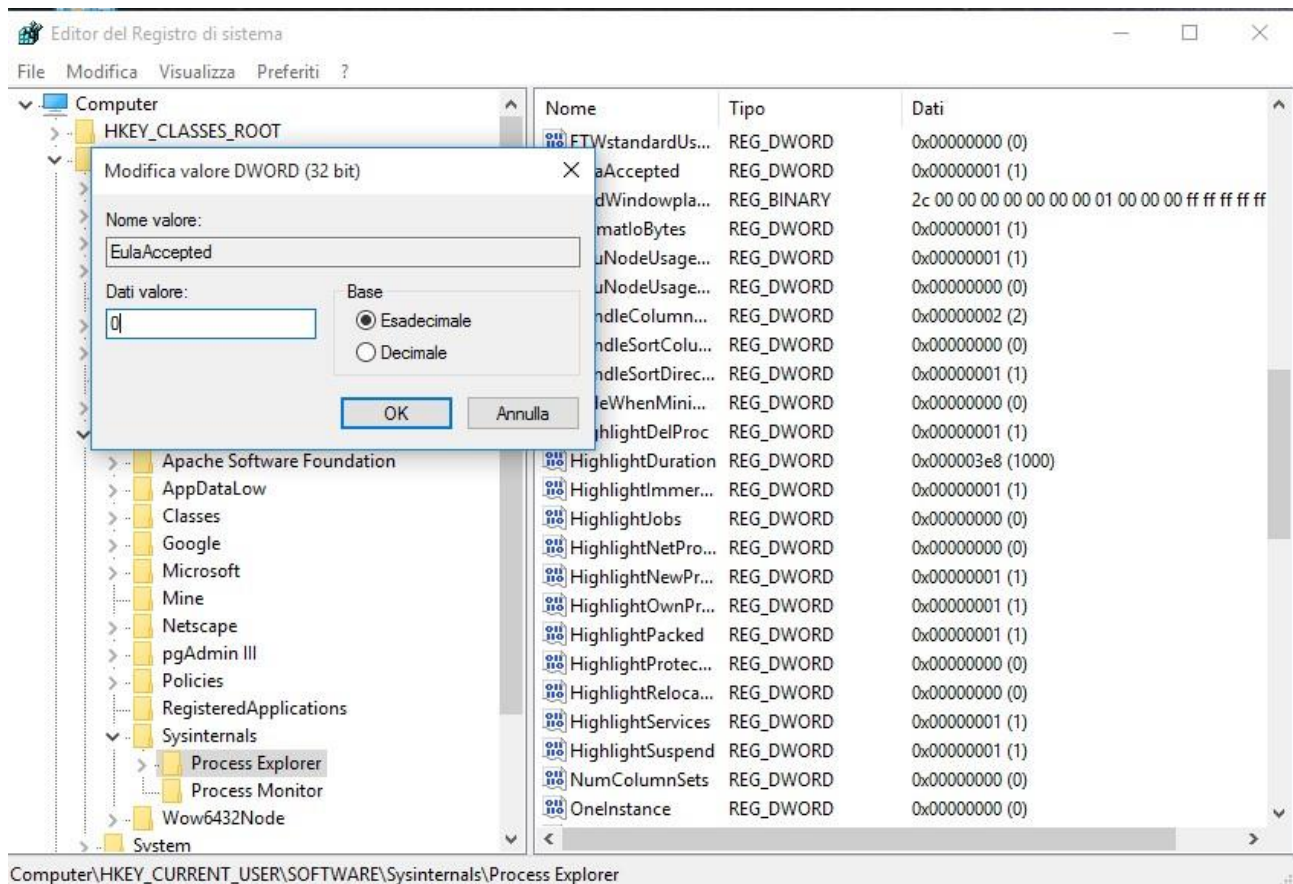
Il Registro di Windows è un database gerarchico che memorizza la maggior parte delle impostazioni di configurazione del sistema operativo e dell'ambiente desktop.

In un passaggio precedente, si è accettato il contratto di licenza (EULA) del Process Explorer. Vai alla chiave di registro *EulaAccepted* per Process Explorer.

Cliccare per selezionare Process Explorer in *HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer*. Scorrere verso il basso per individuare la chiave

EulaAccepted. Attualmente, il valore della chiave di registro EulaAccepted è 0x00000001(1).

c. Fare doppio click sulla chiave di registro EulaAccepted. Attualmente, il valore dei dati è impostato su 1, indica che l'EULA è stato accettato dall'utente. Cambiando il valore 1 in 0 sta a significare che l'EULA non è stato accettato. Fare clic su OK per continuare.



Così facendo, quando si aprirà di nuovo il Process Explorer, chiederà di nuovo di accettare i Termini & Condizioni.

