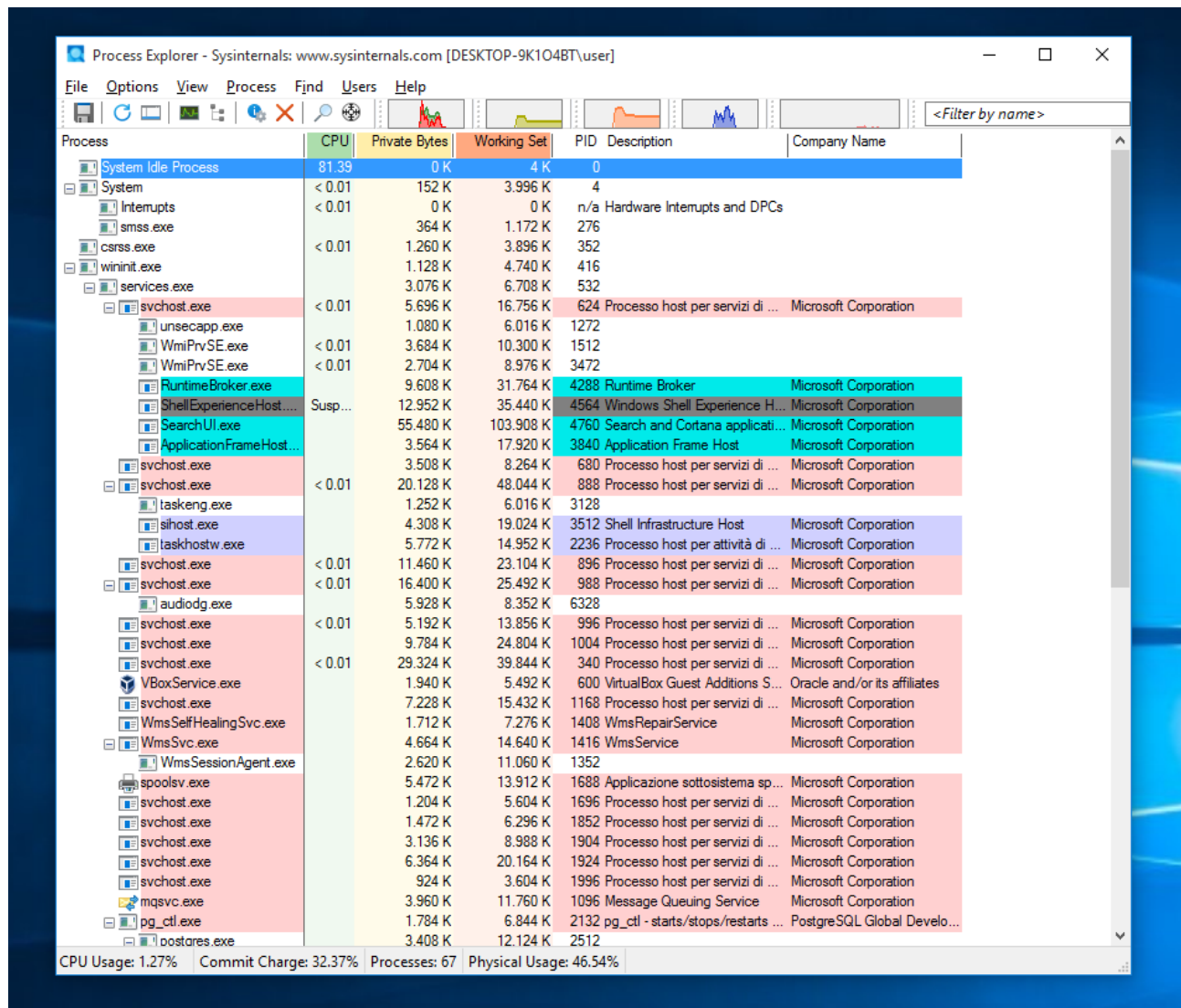


# Process Explorer

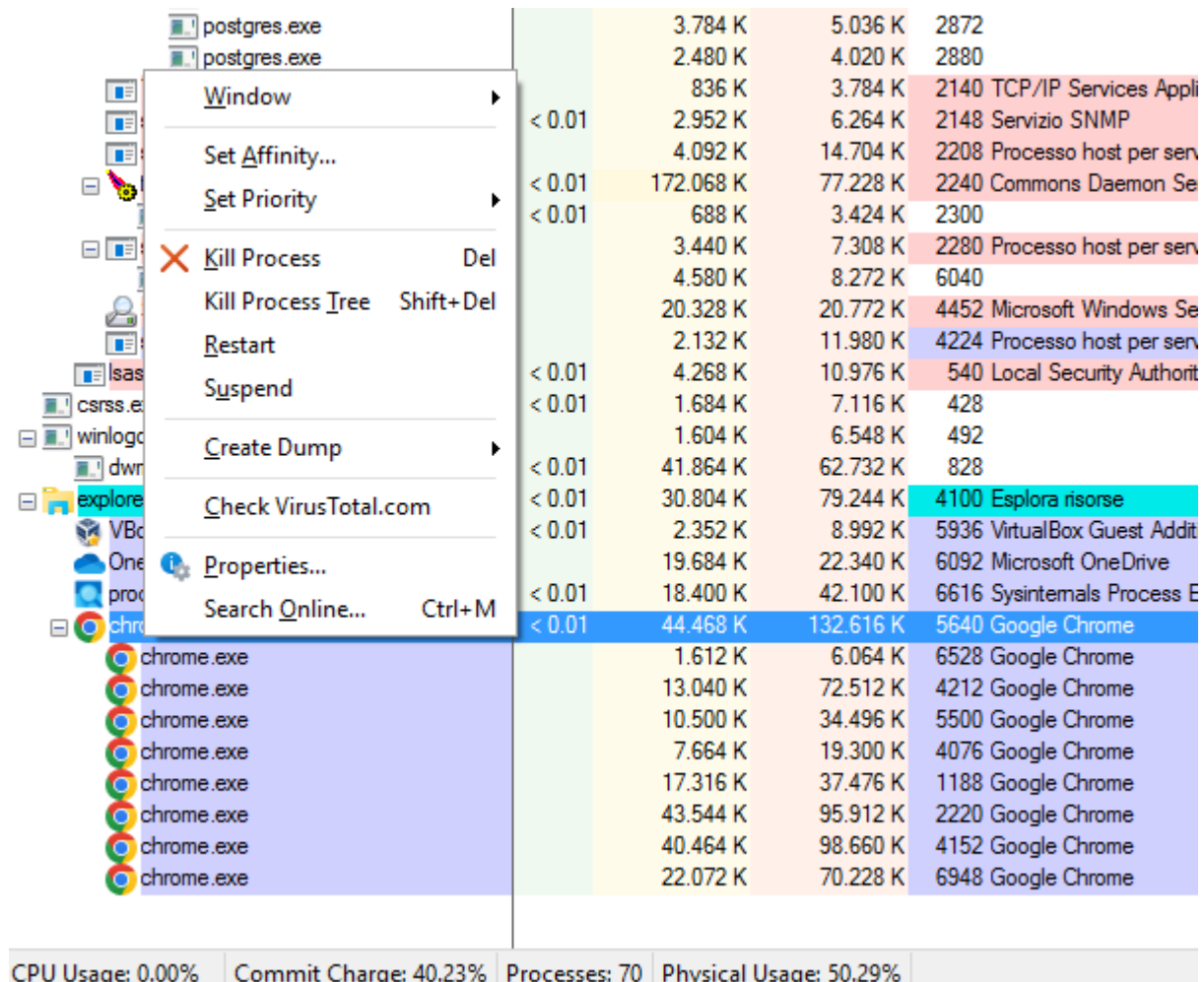
Nell'esercitazione odierna è stato adoperato il tool **Process Manager**, della suite **Sysinternals Suite**, mediante il quale è stato possibile usufruire di funzioni simile a quelle di un task manager, ma più articolate ed esplicative.



Una volta scaricato e installato, questa sarà la schermata principale a cui avremo accesso, nella quale, **come nel classico task manager** ci verranno mostrati **tutti i processi attivi, con le varie opzioni**, quali memoria **CPU occupata, Private bytes, working set, PID e descrizione della task**.

Allo scopo di prendere confidenza con esso, sono stati testati alcuni possibili comandi. Una delle prime prove è stata mediante l'uso del cerchietto esattamente sotto la "User", il quale se

trascinato su un'applicazione, su un software aperto, ci porterà in maniera automatica su Process Explorer, nell'esatta posizione in cui esso si trova.



Name	PID	Private Bytes	Working Set	Session ID
postgres.exe	2872	3.784 K	5.036 K	2872
postgres.exe	2880	2.480 K	4.020 K	2880
TCP/IP Services Appli	2140	836 K	3.784 K	2140
Servizio SNMP	2148	< 0.01	2.952 K	6.264 K
Processo host per serv	2208	4.092 K	14.704 K	2208
Commons Daemon Se	2240	< 0.01	172.068 K	77.228 K
Processo host per serv	2280	< 0.01	688 K	3.424 K
Processo host per serv	2280	< 0.01	3.440 K	7.308 K
Microsoft Windows Se	4452	4.580 K	8.272 K	6040
Processo host per serv	4224	20.328 K	20.772 K	4452
Local Security Authorit	540	2.132 K	11.980 K	4224
Esplora risorse	4100	< 0.01	4.268 K	10.976 K
VirtualBox Guest Addit	5936	< 0.01	1.684 K	7.116 K
Microsoft OneDrive	6092	< 0.01	1.604 K	6.548 K
Sysinternals Process E	6616	< 0.01	41.864 K	62.732 K
Google Chrome	5640	< 0.01	30.804 K	79.244 K
Google Chrome	6528	< 0.01	2.352 K	8.992 K
Google Chrome	4212	< 0.01	19.684 K	22.340 K
Google Chrome	5500	< 0.01	18.400 K	42.100 K
Google Chrome	4076	< 0.01	44.468 K	132.616 K
Google Chrome	1188	1.612 K	6.064 K	6528
Google Chrome	2220	13.040 K	72.512 K	4212
Google Chrome	4152	10.500 K	34.496 K	5500
Google Chrome	6948	7.664 K	19.300 K	4076
Google Chrome	6948	17.316 K	37.476 K	1188
Google Chrome	6948	43.544 K	95.912 K	2220
Google Chrome	6948	40.464 K	98.660 K	4152
Google Chrome	6948	22.072 K	70.228 K	6948

CPU Usage: 0.00% Commit Charge: 40.23% Processes: 70 Physical Usage: 50.29%

Qui sopra, viene mostrato il test mediante **chrome**, sul quale è stato poi aperto un menù a tendina, il quale forniva alcune opzioni, come proprietà **restart**, **suspend** o ancora **kill Process**, il quale ci consente di chiudere istantaneamente un processo.

È stato successivamente effettuato il medesimo test con il **cmd** di windows, con il quale è stato anche effettuato un comando **ping**, anch'esso riportato all'interno di **process explorer** come sottoprocesso.

chrome.exe		44.392 K	132.616 K	5640	Google Chrome	Google LLC
chrome.exe		1.608 K	6.060 K	6528	Google Chrome	Google LLC
chrome.exe		13.040 K	72.512 K	4212	Google Chrome	Google LLC
chrome.exe		10.476 K	34.504 K	5500	Google Chrome	Google LLC
chrome.exe		7.664 K	19.300 K	4076	Google Chrome	Google LLC
chrome.exe		17.316 K	37.476 K	1188	Google Chrome	Google LLC
chrome.exe		43.544 K	95.912 K	2220	Google Chrome	Google LLC
chrome.exe		40.464 K	98.660 K	4152	Google Chrome	Google LLC
chrome.exe		22.328 K	70.488 K	6948	Google Chrome	Google LLC
cmd.exe		1.556 K	2.892 K	7080	Processore dei comandi di ...	Microsoft Corporation
conhost.exe		10.440 K	13.140 K	6148	Console Window Host	Microsoft Corporation
PING.EXE		724 K	3.416 K	1216	Comando Ping TCP/IP	Microsoft Corporation

CPU Usage: 3.12%   Commit Charge: 41.46%   Processes: 77   Physical Usage: 52.69%

Chiudere forzatamente il sottoprocesso **conhost.exe** porta anche alla chiusura del **cmd**.

Proseguendo con i test, è stato in seguito, tramite il menù a tendina, tasto destro del mouse, adoperata la voce “**check virustotal.com**”, opzione fantastica che **implementa le funzioni del servizio virus total all’interno del Process Explorer**, mostrando nel giro di pochi secondi se quel determinato processo ha riscontri all’interno del database di **Virustotal**.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]							
File Options View Process Find Users Help							
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virus Total
postgres.exe		3.412 K	12.140 K	2624			
conhost.exe	< 0.01	10.164 K	7.868 K	2672			
postgres.exe		2.516 K	5.012 K	2756			
postgres.exe		2.560 K	5.416 K	2868			
postgres.exe	< 0.01	2.568 K	5.608 K	2876			
postgres.exe		2.568 K	5.428 K	2884			
postgres.exe		3.796 K	6.444 K	2892			
postgres.exe		2.488 K	5.116 K	2900			
snmp.exe	< 0.01	2.856 K	7.540 K	2332	Servizio SNMP	Microsoft Corporation	
svchost.exe		4.204 K	14.976 K	2460	Processo host per servizi di ...	Microsoft Corporation	
tomcat7.exe	< 0.01	173.848 K	77.544 K	2552	Commons Daemon Service ...	Apache Software Foundati...	
conhost.exe	< 0.01	744 K	3.536 K	2588			
svchost.exe		3.368 K	8.736 K	2684	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		1.124 K	4.840 K	3596	Processo host per servizi di ...	Microsoft Corporation	
SearchIndexer.exe		24.596 K	25.640 K	4132	Microsoft Windows Search I...	Microsoft Corporation	
SearchProtocolHost.e...		1.444 K	5.132 K	4592	Microsoft Windows Search P...	Microsoft Corporation	
SearchFilterHost.exe		1.716 K	5.816 K	5068			
SearchProtocolHost.e...		2.512 K	5.504 K	5108			
svchost.exe		1.304 K	6.084 K	4908	Processo host per servizi di ...	Microsoft Corporation	
spsvc.exe		5.656 K	15.592 K	2568	Servizio piattaforma protezio...	Microsoft Corporation	
svchost.exe		2.332 K	12.104 K	552	Processo host per servizi di ...	Microsoft Corporation	
lsass.exe	< 0.01	4.524 K	12.328 K	544	Local Security Authority Proc...	Microsoft Corporation	
csrss.exe	< 0.01	1.520 K	5.980 K	436			
winlogon.exe		1.996 K	8.212 K	496			
dwm.exe	< 0.01	30.440 K	57.360 K	808			
explorer.exe	< 0.01	22.884 K	69.100 K	3584	Esplora risorse	Microsoft Corporation	
VBxTray.exe	< 0.01	2.376 K	9.384 K	5200	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates	
OneDrive.exe		19.388 K	48.868 K	5280	Microsoft OneDrive	Microsoft Corporation	
proceXP64.exe	< 0.01	18.164 K	39.100 K	5500	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		1.528 K	2.740 K	5732	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		10.556 K	14.276 K	5740	Console Window Host	Microsoft Corporation	0/76
chrome.exe	5.34	48.032 K	151.596 K	6032	Google Chrome	Google LLC	
chrome.exe		1.596 K	6.088 K	6040	Google Chrome	Google LLC	
chrome.exe	< 0.01	11.856 K	57.812 K	5380	Google Chrome	Google LLC	
chrome.exe	2.67	14.112 K	41.900 K	5360	Google Chrome	Google LLC	
chrome.exe		7.796 K	19.548 K	3900	Google Chrome	Google LLC	
chrome.exe	< 0.01	60.224 K	122.008 K	3860	Google Chrome	Google LLC	

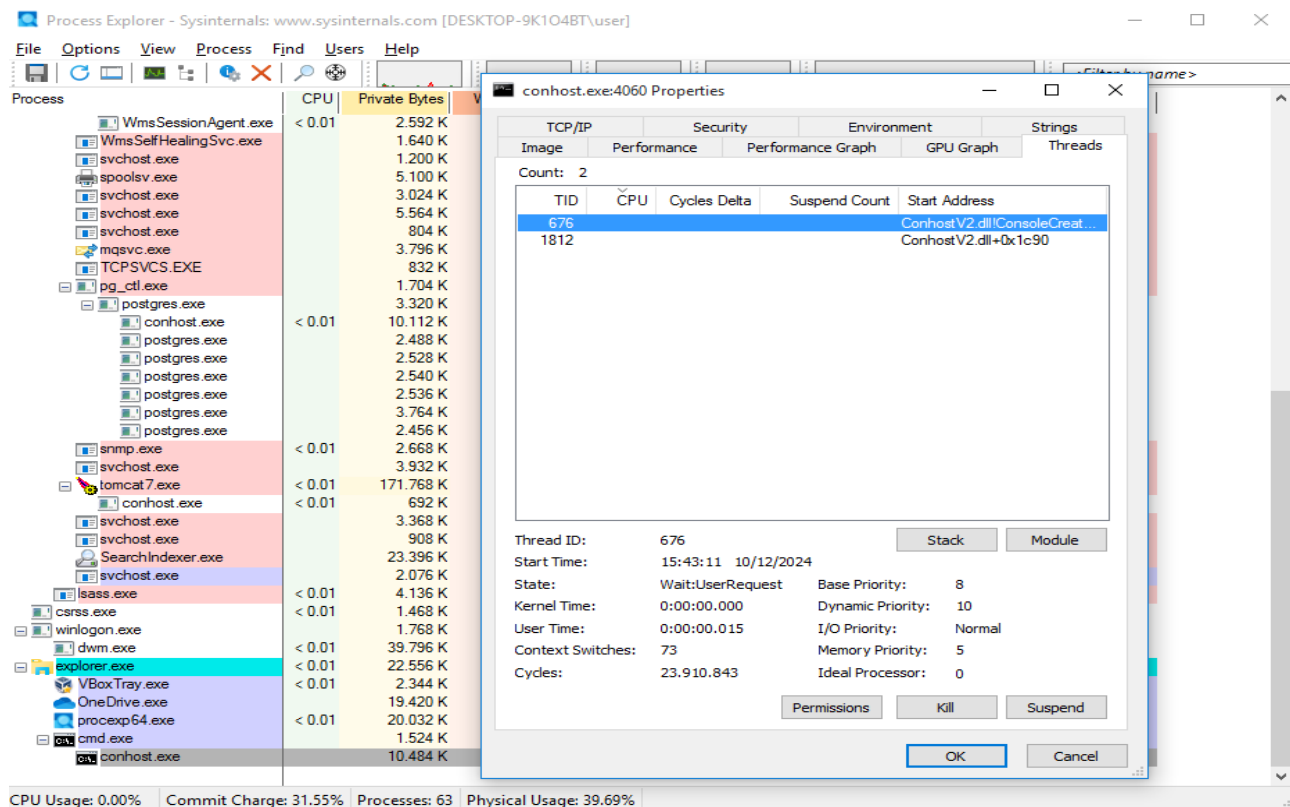
CPU Usage: 9.79%   Commit Charge: 38.89%   Processes: 77   Physical Usage: 58.28%

In questo caso la funzione è stata testata sul **cmd**, il quale ha prodotto come risultato una scansione **0/76**.

# Thread and Handle

Un'altra cosa che **Process Explorer** ci consente di fare, è quello di poter **visualizzare tread ed handle dei singoli processi**.

Tramite le proprietà di essi è infatti possibile dirigersi alla voce **threads** per poter dare un'occhiata.



Ma questo non è l'unico modo, questo perché se invece si adopera l'opzione che ci consente di visualizzare anche una **"barra inferiore"**. Si aprirà una finestra che dividerà in due Process Explorer, mostrando non solo i **thread** ma anche le **handle dei singoli processi**.

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

File Options View Process Find Users Handle Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
VBoxService.exe	< 0.01	1.800 K	5.148 K	344	VirtualBox Guest Additions S...	Oracle and/or its affiliates	
svchost.exe	< 0.01	28.572 K	36.344 K	604	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		6.860 K	12.804 K	1288	Processo host per servizi di ...	Microsoft Corporation	
WmsSvc.exe		4.928 K	12.484 K	1464	WmsService	Microsoft Corporation	
WmsSessionAgent.exe		2.568 K	9.500 K	3528			
WmsSelfHealingSvc.exe		1.640 K	6.552 K	1500	WmsRepairService	Microsoft Corporation	
svchost.exe		1.200 K	5.292 K	1688	Processo host per servizi di ...	Microsoft Corporation	
spoolsv.exe		5.100 K	10.212 K	1888	Applicazione sottosistema sp...	Microsoft Corporation	
svchost.exe		3.024 K	6.876 K	1996	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		5.560 K	16.816 K	2016	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		804 K	3.348 K	1400	Processo host per servizi di ...	Microsoft Corporation	
msgsvcs.exe		3.796 K	9.532 K	1680	Message Queuing Service	Microsoft Corporation	
TCPVCS.EXE		832 K	3.828 K	2252	TCP/IP Services Application	Microsoft Corporation	
pg_ctl.exe		1.704 K	5.896 K	2260	pg_ctl - starts/stops/restarts ...	PostgreSQL Global Develo...	
postgres.exe		3.320 K	12.100 K	2624			
conhost.exe	< 0.01	10.112 K	7.340 K	2672			
postgres.exe		2.488 K	3.804 K	2756			
postgres.exe		2.528 K	4.060 K	2868			

Handles DLLs Threads

Type	Name
Key	HKCU
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Key	HKCU\Software\Classes
Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Mutant	\Sessions\1\BaseNamedObjects\MSCTF_Asm.MutexDefault15-1-5-21-1859916961-343043...
Process	cmd.exe(596)
Section	\BaseNamedObjects\__ComCatalogCache_
Section	\Sessions\1\BaseNamedObjects\windows_shell_global_counters
Section	\Sessions\1\BaseNamedObjects\C:\ProgramData\Microsoft\Windows\Caches\cversions.2.ro
Section	\Sessions\1\BaseNamedObjects\C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-...
Section	\Sessions\1\BaseNamedObjects\C:\ProgramData\Microsoft\Windows\Caches\cversions.2.ro
Section	\Sessions\1\BaseNamedObjects\C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2...
Section	\Windows\Theme1668113713
Section	\Sessions\1\Windows\Theme529532614
Thread	conhost.exe(4060): 1812
Window Station	\Sessions\1\Windows\WindowStations\WinSta0
Window Station	\Sessions\1\Windows\WindowStations\WinSta0

CPU Usage: 3.03% Commit Charge: 31.69% Processes: 64 Physical Usage: 40.09%

## Windows registry

Come ultima task da effettuare, è stato richiesto di modificare un'impostazione dei registri windows, ragion per cui, mediante il comando **regedit**, mi sono diretto all'interno dei registri.

Qui ho individuato proprio **Process Explorer**, in modo da modificare un parametro che non avrebbe causato alcuna possibile problematica.

Editor del Registro di sistema

File Modifica Visualizza Preferiti ?

Nome	Tip	Dati
DbgHelpPath	REG_SZ	C:\Windows\SYSTEM32\dbghelp.dll
DefaultDllProp...	REG_DWORD	0x00000000 (0)
DefaultProcProp...	REG_DWORD	0x00000006 (6)
DefaultSysInfoP...	REG_DWORD	0x00000000 (0)
Divider	REG_BINARY	00 00 00 00 00 00 e0 3f
DllColumnCount	REG_DWORD	0x00000004 (4)
DllPropWindow...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...
DllSortColumn	REG_DWORD	0x00000000 (0)
DllSortDirection	REG_DWORD	0x00000001 (1)
ETWstandardUs...	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000000 (0)
FindWindowpla...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...
FormatIoBytes	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000000 (0)
HandleColumn...	REG_DWORD	0x00000002 (2)
HandleSortColu...	REG_DWORD	0x00000000 (0)
HandleSortDirec...	REG_DWORD	0x00000001 (1)
HideWhenMini...	REG_DWORD	0x00000000 (0)
HighlightDelProc	REG_DWORD	0x00000001 (1)
HighlightDuration	REG_DWORD	0x000003e8 (1000)
HighlightImmer...	REG_DWORD	0x00000001 (1)
HighlightJobs	REG_DWORD	0x00000000 (0)
HighlightNetPro...	REG_DWORD	0x00000000 (0)
HighlightNewPr...	REG_DWORD	0x00000001 (1)
HighlightOwnPr...	REG_DWORD	0x00000001 (1)
HighlightPacked	REG_DWORD	0x00000001 (1)
HighlightProtec...	REG_DWORD	0x00000000 (0)
HighlightReloca...	REG_DWORD	0x00000000 (0)

Computer\HKEY\_CURRENT\_USER\SOFTWARE\Sysinternals\Process Explorer

All'interno di esso, infatti, vi è un valore che si chiama **EulaAccepted**, il quale rappresenta l'accettazione delle policy di utilizzo di questo specifico software. Essa è stata **modificata da 1 a 0**, facendo quindi in modo che risultasse come se l'utente non avesse mai accettato l'accordo di utilizzo.

All'avvio del programma, di fatto, ci è stato **nuovamente** chiesto di accettare l'accordo, in modo da favorire l'utilizzo di quest'ultimo, **come se il software fosse appena stato scaricato per la prima volta**.

